Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date September 30, 2019

Original Release Date May 28, 2019

Superseding Document		
Status	Final	
Series/Number	NIST Interagency or Internal Report (NISTIR) 8183A Volume 2	
Title	Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case	
Publication Date	September 2019	
DOI	https://doi.org/10.6028/NIST.IR.8183A-2	
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8183a/vol-2/final	

Additional Information



DRAFT NISTIR 8183A	1
Volume 2	2
	3
Cybersecurity Framework Manufacturing Profile	4
Low Security Level Example	5
Implementations Guide:	6
Volume 2 – Process-based Manufacturing System Use Case	7
	8
Keith Stouffer	9
Timothy Zimmerman	10
CheeYee Tang	11
Jeffrey Cichonski	12
Neeraj Shah Washay Daymand	13
Wesley Downard	14 15
	16
	17
	18
	19
This publication is available free of charge from:	20
https://doi.org/10.6028/NIST.IR.8183A-2-draft	21
	22
	23



DRAFT NISTIR 8183A Volume 2	24 25
	26
curity Framework Manufacturing Profile	27
Low Security Level Example	28
Implementations Guide:	29
2 – Process-based Manufacturing System Use Case	30
	31
Keith StoufferNeeraj ShahTimothy ZimmermanStrativia, LLCCheeYee TangLargo, MarylandIntelligent Systems DivisionEngineering Laboratory	32 33 34 35 36
Jeffrey CichonskiWesley DownardApplied Cybersecurity DivisionG2, Inc.Information Technology LaboratoryAnnapolis Junction, Maryland	 37 38 39 40 41 42
This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8183A-2-draft	42 43 44 45
	46
May 2019	47 48 49
SORTINENT OF COMMIT	50 51
U.S. Department of Commerce Wilbur L. Ross, Jr., Secretary	52 53
National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology	54 55 56

Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

57 58 59 60 61	National Institute of Standards and Technology Internal Report 8183A, Volume 2 401 pages (May 2019) This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8183A-2-draft
62 63 64 65	Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
66 67 68 69 70 71	There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.
72 73 74	Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <u>https://csrc.nist.gov/publications</u> .
75	
76	Public comment period: May 28, 2019through July 8, 2019
77 78 79	National Institute of Standards and Technology Attn: Applied Cybersecurity Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Email: CSF Manufacturing Profile Implementation@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

84 Abstract 85 This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented 86 87 in process-based manufacturing environments to satisfy the requirements in the Cybersecurity 88 Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept 89 solutions include measured network, device, and operational performance impacts observed 90 during the implementation. Depending on factors like size, sophistication, risk tolerance, and 91 threat landscape, manufacturers should make their own determinations about the breadth of the 92 proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can 93 be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with 94 manufacturing sector goals and industry best practices. The Manufacturing Profile provides a 95 voluntary, risk-based approach for managing cybersecurity activities and cyber risk to 96 manufacturing systems. The Manufacturing Profile is meant to compliment but not replace 97 current cybersecurity standards and industry guidelines that the manufacturer is embracing. 98 100 **Keywords** Computer security; Cybersecurity Framework (CSF); distributed control systems (DCS); 101 102 industrial control systems (ICS); information security; manufacturing; network security; 103 programmable logic controllers (PLC); risk management; security controls; supervisory control 104 and data acquisition (SCADA) systems. 105 Supplemental Content 106 Additional volumes of this publication include: 107 Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low 108 Security Level Example Implementations Guide: Volume 1 – General Implementation 109 Guidance. https://doi.org/10.6028/NIST.IR.8183A-1-draft 110 Draft NISTIR 8183A Volume 3, Cybersecurity Framework Manufacturing Profile Low 111 Security Level Example Implementations Guide: Volume 3 – Discrete-based 112 Manufacturing System Use Case. https://doi.org/10.6028/NIST.IR.8183A-3-draft

Acknowledgments

114	Acknowledgments
116	The authors gratefully acknowledge and appreciate the significant contributions from individuals
117	and organizations in the public and private sectors, whose thoughtful and constructive comments
118	improved the overall quality, thoroughness, and usefulness of this publication. A special
119	acknowledgement to the members of the ISA99, Industrial Automation and Control Systems
120	Security Committee and the Department of Homeland Security Industrial Control System Joint
121	Working Group (ICSJWG) for their exceptional contributions to this publication.
122	
123	Note to Reviewers
124	This guide does not describe the solution, but a possible solution. This is a draft guide. We seek
125	feedback on its contents and welcome your input. Comments, suggestions, and success stories
126	will improve subsequent versions of this guide. Please contribute your thoughts to
127	<u>CSF_Manufacturing_Profile_Implementation@nist.gov.</u>

128

Call for Patent Claims

131 This public review includes a call for information on essential patent claims (claims whose use 132 would be required for compliance with the guidance or requirements in this Information 133 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be 134 directly stated in this ITL Publication or by reference to another publication. This call also 135 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications 136 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents. 137 138 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, 139 in written or electronic form, either: 140 141 a) assurance in the form of a general disclaimer to the effect that such party does not hold and 142 does not currently intend holding any essential patent claim(s); or 143 144 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in 145 146 this ITL draft publication either: 147 148 i) under reasonable terms and conditions that are demonstrably free of any unfair 149 discrimination; or 150 151 ii) without compensation and under reasonable terms and conditions that are 152 demonstrably free of any unfair discrimination. 153 154 Such assurance shall indicate that the patent holder (or third party authorized to make assurances 155 on its behalf) will include in any documents transferring ownership of patents subject to the 156 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on 157 the transferee, and that the transferee will similarly include appropriate provisions in the event of 158 future transfers with the goal of binding each successor-in-interest. 159 160 The assurance shall also indicate that it is intended to be binding on successors-in-interest 161 regardless of whether such provisions are included in the relevant transfer documents. 162 Such statements should be addressed to: CSF_Manufacturing_Profile_Implementation@nist.gov 163

164		Table of Contents	
165		Table of Contents	
166	Ex	ecutive Summary	vii
167	1.	Introduction	1
168		1.1 Purpose and Scope	
169 170		1.2 Audience1.3 Document Structure	
171	2.	Process-based Manufacturing System Low Security Level Use Ca	ase3
172		2.1 Introduction	
173		2.2 Process-based Low Security Level Use Case	3
174	3.	Policy and Procedure Implementations	8
175		3.1 Security Program Document Example	
176		3.2 Security Policy Document Example	
177		3.3 Standard Operating Procedures Document Example	35
178		3.4 Risk Management Document Example	
179		3.5 Incident Response Plan Document Example	
180		3.6 Incident Recovery Plan Document Example	
181	4.	Technical Solution Implementations	
182		4.1 Introduction	100
183		4.2 Open-AudIT	
184		4.3 CSET	
185		4.4 GRASSMARLIN	
186		4.5 Wireshark	
187		4.6 Veeam Backup and Replication	
188		4.7 Security Onion	
189		4.8 Cisco AnyConnect VPN	
190		4.9 Microsoft Active Directory	
191		4.10 Symantec Endpoint Protection	
192		4.11 Tenable Nessus	
193 194		4.12 NamicSoft 4.13 The Hive Project	
194 195		4.13 The five Floject	
195 196		4.15 GTB Inspector	
190		4.16 Graylog	
198		4.17 DBAN	
199		4.18 Network Segmentation and Segregation	
200		4.19 Network Boundary Protection	
200		4.20 Managed Network Interfaces	
201		4.21 Time Synchronization	
202		4.22 System Use Monitoring	
204		4.23 Ports and Services Lockdown	

205	4.24 Media Protection	
206		
207	Appendix A - Acronyms and Abbreviations	
208	Appendix B - Glossary	
209	Appendix C - References	
210		

211 Executive Summary

- 212 This guide provides example proof-of-concept solutions demonstrating how open-source and
- 213 commercial off-the-shelf (COTS) products that are currently available today can be implemented
- 214 in process-based manufacturing environments to satisfy the requirements in the Cybersecurity
- Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed
- 217 during the implementation. Depending on factors like size, sophistication, risk tolerance, and
- threat landscape, manufacturers should make their own determinations about the breadth of the
- 219 proof-of-concept solutions they may voluntarily implement.
- proof-of-concept solutions they may voluntarily implement.
- 220 The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for
- 221 manufacturers and is aligned with manufacturing sector goals and industry best practices. The
- 222 Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity
- activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to
- 224 compliment but not replace current cybersecurity standards and industry guidelines that the
- 225 manufacturer is embracing.
- 226 The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a
- roadmap to identify opportunities for improving the current cybersecurity posture of the
- 228 manufacturing system. The Manufacturing Profile provides a prioritization of security activities
- to meet specific business/mission goals. Relevant and actionable security practices that can be
- 230 implemented to support key business/mission goals are then identified.
- 231 While the proof-of-concept solutions in this guide used a suite of commercial products, this
- 232 guide does not endorse these particular products, nor does it guarantee compliance with any
- 233 regulatory initiatives. Each organization's information security experts should identify the
- 234 products that will best integrate with their existing tools and manufacturing system
- 235 infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these
- 236 guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts
- 237 of a solution. This guide does not describe regulations or mandatory practices, nor does it carry
- any statutory authority.

239 **1.** Introduction

240 The Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [1] directed the

241 development of the voluntary Cybersecurity Framework that provides a prioritized, flexible,

repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for

- those processes, information, and systems directly involved in the delivery of critical
- 244 infrastructure services.
- 245 The Cybersecurity Framework is a voluntary risk-based assemblage of industry standards and

best practices designed to help organizations manage cybersecurity risks [2]. The Framework,

created through collaboration between government and the private sector, uses a common

- 248 language to address and manage cybersecurity risk in a cost-effective way based on business
- 249 needs without imposing additional regulatory requirements.
- 250 To address the needs of manufacturers, a Manufacturing Profile [4] of the Cybersecurity
- 251 Framework was developed, through collaboration between government and the private sector, to
- be an actionable approach for implementing cybersecurity controls into a manufacturing system
- and its environment. The Profile defines specific cybersecurity activities and outcomes for the
- 254 protection of the manufacturing system, its components, facility, and environment. Through use
- of the Profile, the manufacturer can align cybersecurity activities with business requirements,

risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to

257 cybersecurity from standards, guidelines, and industry best practices.

258 **1.1 Purpose and Scope**

259 Many small and medium sized manufacturers have expressed that they are challenged in 260 implementing a standards-based cybersecurity program. This guide provides example proof-of-261 concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) 262 products that are available today can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security 263 264 Level. Example proof-of-concept solutions with measured network, device, and operational 265 performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-266 based manufacturing environment (Volume 3) are included in the guide. Depending on factors 267 like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their 268 own determinations about the breadth of the proof-of-concept solutions they may voluntarily 269 implement. The CSF Manufacturing Profile can be used as a roadmap for managing 270 cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry 271 best practices. The Manufacturing Profile provides a voluntary, risk-based approach for 272 managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing 273 Profile is meant to enhance but not replace current cybersecurity standards and industry

- 274 guidelines that the manufacturer is embracing.
- 275 While the proof-of-concept solutions in this guide used a suite of commercial products, this
- 276 guide does not endorse these particular products, nor does it guarantee compliance with any
- 277 regulatory initiatives. Each organization's information security experts should identify the
- 278 products that will best integrate with their existing tools and manufacturing system

- 279 infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these
- 280 guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts
- 281 of a solution. This guide does not describe regulations or mandatory practices, nor does it carry
- any statutory authority.
- 283 This project is guided by the following assumptions: The solutions were developed in a lab
- 284 environment. The environment is based on a typical small manufacturer. The environment does
- 285 not reflect the complexity of a production environment. An organization can access the skills and
- resources required to implement a manufacturing cybersecurity solution.

287 **1.2 Audience**

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure manufacturing systems.
- System administrators, engineers, and other information technology (IT) professionals
 who administer, patch, or secure manufacturing systems.
- Managers who are responsible for manufacturing systems.
- Senior management who are trying to understand implications and consequences as they
 justify and implement a manufacturing systems cybersecurity program to help mitigate
 impacts to business functionality.
- Researchers, academic institutions and analysts who are trying to understand the unique security needs of manufacturing systems.
- 302 **1.3 Document Structure**
- 303 Volume 2 is divided into the following major sections:
- Section 2 provides an overview of the process-based manufacturing system use case.
- Section 3 provides the detailed policy and procedure documents developed for the
 process-based manufacturing system use case.
- Section 4 provides the detailed technical capability implementations and associated
 performance measurements for the process-based manufacturing system use case.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a list of references used in the development of this document.
- 312

2. Process-based Manufacturing System Low Security Level Use Case

314 **2.1** Introduction

- 315 This use case is a proof-of-concept solution demonstrating how open-source and commercial off-
- the-shelf (COTS) products that are currently available today can be implemented in a
- 317 manufacturing environment to satisfy the requirements in the CSF Manufacturing Profile Low
- 318 Security Level. Depending on factors like size, sophistication, risk tolerance, and threat
- 319 landscape, manufacturers should make their own determinations about the breadth of proof-of-
- 320 concept solution they may voluntarily implement.

321 **2.2 Process-based Low Security Level Use Case**

- 322 The fictional company, Westman Chemical (i.e. Westman), is a chemical manufacturer
- 323 producing commercial grade chemical products for use in the transportation, building and
- 324 construction, and other industrial products. It is headquartered in Westland, a city with
- 325 population of about 100,000 people.
- 326 Westman operates its manufacturing facility 24 hours per day, 7 days per week (24/7), with the
- exception of a schedule maintenance shutdown for about 2 weeks every year, typically scheduled
 at the end of December.
- 329 To increase industrial competitiveness, Westman has introduced process automation equipment
- to improve the production efficiency and to lower production costs. Industrial automation
- 331 equipment like programmable logic controllers (PLC), human-machine-interfaces (HMI), and
- data historians are deployed in the factory to monitor and control the production operation.

333 **2.2.1** Mission

334 To supply high quality chemical products for industrial application.

335 2.2.2 Facility

- 336 Westman facility is a single building about 50,000 square foot, with about 35,000 square foot
- 337 of manufacturing space which includes the production space, a distribution facility, and several
- above ground chemical storage tanks. The remainder of the facility contains the administrativeand engineering office space.
- 340 The perimeter of the facility is fenced, and the main entrance has gate that is open during
- 341 business hours and is locked after hours. There are two entrances to the main building. One is for
- 342 employee's access and is protected by a badge access system. Employees must swipe their
- 343 assigned badge to enter the building. The other entrance is located at the front lobby, staffed by a
- 344 receptionist during normal business hours. Guests and visitors are required to sign in and receive
- 345 proper identification before entering the building or facility. The Westman facility does not have
- any contracted security guards at the gate or entrances.

347 **2.2.3 Employees**

- 348 Westman Chemical has 200 full-time employees, with most of the employees working on the
- 349 manufacturing floor. A small team of full-time manufacturing/control engineers responsible for
- 350 the manufacturing, control and automation equipment controlling manufacturing process. Their
- 351 mission is to ensure the safe and efficient operation of the production system.
- Westman also has a small team of full-time IT personnel responsible for the enterprise ITsystems.

354 Westman Management position and responsibility:

Westman Management	Major Responsibility
CEO/General Manager	Oversight of the company
Director of Operations Oversight of manufacturing operations. Management of the manufacture staff and control engineers. Reports to the CEO/General Manager.	
Director of Product Development	Oversight of product development. Management of the on-site chemists. Reports to the CEO/General Manager.
Director of Marketing	Oversight of marketing and sales. Reports to the CEO/General Manager.
Controller/Finances	Manager of finance staff. Reports to the CEO/General Manager.
General Counsel	Handles all legal matters. Reports to the CEO/General Manager.
IT Manager	Manager of IT staff. Reports to the CEO/General Manager.
HR Manager	Manager of human resources staff. Reports to the CEO/General Manager.

355

2.2.4 Supply Chain

357 Raw materials are utilized continuously to support the continuous operation of the manufacturing

- 358 process. Raw materials are typically supplied through a long-term contract established with
- 359 suppliers and are transported to the facility on a regular basis.

- 360 The end products are typically sold to customers in large quantity. Delivery is sub-contracted to
- 361 several logistics companies which will handle the transportation from the Westman facility to the
- 362 end customers. Westman's products are typically used as raw materials or additives in chemical
- 363 processes performed by other industrial manufacturers.

364 2.2.5 Supporting Services

- 365 The supporting services required by Westman are electricity, natural gas, water, and
- Internet. The broadband Internet connection is a business class service provided by a largenational provider with business class service level agreement.

368 **2.2.6** Legal and Regulatory Requirements

- As a chemical manufacturer, Westman and its employees are required to comply with all federal
 and state legal and regulatory requirements for chemical and hazardous materials. Westman is
- also required to comply with all legal, regulatory and safety requirements.
- 372

373 2.2.7 Critical Infrastructure

- 374 The chemical sector is considered as a critical infrastructure under the Presidential Policy
- 375 Directive 21 (PPD-21).
- 376

377 2.2.8 Manufacturing Process

378 The manufacturing system consists of five major chemical processing components: a reactor, a

379 product condenser, a vapor-liquid separator, a recycle compressor, and a product stripper to

380 separate the end products. The manufacturing system has 12 valves for controlling the flow of

381 chemicals through the system, and 41 sensor measurements for monitoring the chemical process.

- 382 All valves and sensors are connected to the automation equipment (PLCs) through a DeviceNet
- 383 communications bus. Valves are equipped with manual overrides, enabling workers to override
- the automation equipment during an emergency.

Raw materials are fed to the reactor where the materials are mixed and the main reaction takes place. Output from the reactor flows downstream to the product condenser and the vapor-liquid separator. Any output from the reactor still in the gaseous form is recycled through a compressor and fed back into the main reactor. All condensed components continuously flow to the product stripper separate the components into the final products. Quality assurance samples are taken at various stage of the process to validate the product quality and process efficiency.

391

393 2.2.9 Systems

- The administrative office is supported by a small team of IT personnel mainly using general enterprise IT applications (e.g., email, web applications, and enterprise planning applications).
- 396 The IT personnel maintains a central file storage that is used to store source code, chemical
- formulas, drawings, procedures, and diagrams, and is backed up regularly. The product
- 398 development staff and the manufacturing engineers are authorized to access this storage.
- 399 The IT personnel also installed and configured a Historian database on the manufacturing floor
- 400 to record manufacturing process data. IT personnel is responsible for regular data backup of the
- 401 Historian, and the manufacturing engineers are responsible for the configuration and operation of 402 the Historian.
- 403

404 **2.2.10 Data**

- 405 Data transferred over, or stored within the company network include:
- 406 PLC program code
- 407 Chemical formulas and calculations
- Workflow and operating manuals and documentation
- 409 Electrical diagrams
- Network diagrams
- Quality Assurance procedures
- Historical production data
- 413 NOTE: All data listed above are considered to be proprietary, trade secrets, and/or confidential.
- 414

415 **2.2.11 Network**

- 416 The IT systems within the administrative offices are connected to the corporate network, which
- 417 is managed by the IT team. The manufacturing floor has a separate network for automation
- 418 equipment and is managed by the manufacturing engineers.
- The manufacturing network consists of a typical Ethernet based TCP/IP network and otherindustrial protocols, e.g., DeviceNet.
- 421 Some of the production equipment vendors required Westman to provide remote access to the
- 422 equipment. The remote access allows the authorized vendors to connect to the manufacturing
- 423 equipment to provide maintenance and support.
- 424
- 425

426 2.2.12 Mission Objectives

427 Maintain Personnel Safety

428 Westman commits to safe operation of the manufacturing system and to always put personnel

- 429 safety as its highest priority. All manufacturing process, protocols, automation process and
- 430 equipment, operating procedures and guidelines are designed to ensure personnel safety.
- 431

432 Maintain Environmental Safety

433 Westman complies to all applicable regulations regarding environment safety. Westman is

434 committed to ensuring environmentally-friendly operation of its manufacturing process and

435 working to reduce its environment footprint. Environmental impact caused by the manufacturing

- 436 process is measured and reviewed on a quarterly basis.
- 437

438 Maintain Quality of Product

439 Westman has a world-class manufacturing facility and process. It has employed state of the art

440 automation, equipment, and techniques to ensure the high quality of its product. It has developed

441 a quality assurance program using automation equipment, including PLCs, Historian, and high

- 442 precision sensors operating on a high-speed control network to monitor product quality.
- 443

444 Maintain Production Goals

445 Meeting the monthly production goals is an important objective for Westman, and ensures the 446 supply of products to its customers in a timely fashion. It also maintains financial stability for

- 447 Westman.
- 448 Constant 24/7 production enables Westman to plan its manufacturing operation to meet its
- 449 production goals and customer demand. The investment in automation equipment and skilled
- 450 professional assists Westman to maintain the monthly production goals.
- 451

452 **Protect Trade Secrets**

- 453 Westman is committed to protecting its trade secrets, including product development,
- 454 manufacturing processes, product quality, and supply chain management.

455 **3.** Policy and Procedure Implementations

456 This section includes example policy and procedure documents and statements that were

457 developed for the fictional company Westman. Each organization's information security experts

458 should identify the policy and procedure documents and statements that will best integrate with

459 their existing cybersecurity program and manufacturing system infrastructure.

460 **3.1 Security Program Document Example**

461

т			
462		Security Program	
463	for		
464	Westman		
465			
466			
467			
	Document Owner:	Director of Operations, Westman	

468469 Version

470

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

471

472 Approval

474

Approvers	Role	Signed	Approval Date
	CEO		4-22-2018
	Legal Counsel		4-23-2018

475

^{473 (}By signing below, all Approvers agree to all terms and conditions outlined in this document.)

477 3.1.1 Purpose

- 478 The Information Security Program establishes guidelines and principles for initiating,
- implementing, maintaining, and improving cybersecurity management for Westman.
- 480 This program is designed to:
- Ensure the security and confidentiality of employees and business information;
- 482
 483
 Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in
 substantial harm or inconvenience to Westman, its partners, customers, or any member.
- In addition, the Director of Operations oversees the development, implementation, andmaintenance of the information security program.

488 **3.1.2 Who Should use this Document?**

- 489 This document is intended to be used by the CEO/General Manager, IT Manager, Director of 490 Operations and any other members as deemed appropriate by the management. It supports an
- 490 Operations and any other members as deemed appropriate by the management. It 491 agencies responsibility for implementing a cybersecurity program.

492 **3.1.3** Commitment from Management

- 493 Westman's leadership team is committed to the development of this Information Security
- 494 Program. It fully supports and owns the ultimate responsibility of this program. This
- 495 commitment involves allocating necessary funding to information security work and responding
- 496 without delay to new situations. The leadership team will participate in any information security
- 497 related event as organized.

498 **3.1.4 Organization Overview**

499 **Role in the Industrial sector**

- 500 Westman is a chemical manufacturer producing commercial grade chemical products for use in
- 501 the transportation, building and construction, and other industrial products.
- 502 Westman operates its manufacturing facility 24 hours per day and 365 days per year. To increase
- 503 competitiveness, Westman has introduced process automation equipment to improve the
- 504 production efficiency and to lower cost. Industrial automation equipment like Programmable
- 505 Logic Controller (PLC), Human-Machine-Interface (HMI), and Data Historian are deployed in
- 506 the factory to control and monitor the production operation.
- The chemical sector is considered as a Critical infrastructure under the Presidential Policy
 Directive 21 (PPD-21).
- 509

510 Mission Objectives

511512**1. Maintain Personnel Safety**512Westman commits to safe or

Westman commits to safe operation of the manufacturing system and to always put personnel safety as its highest priority. All manufacturing process, protocols, automation process and equipment, operating procedures and guidelines are designed to ensure personnel safety.

515 516 517

518

519

520

521

522 523

530

537

513

514

2. Maintain Environmental Safety

Westman complies to all applicable regulations regarding environment safety. Westman is committed to ensuring environmentally-friendly operation of its manufacturing process and working to reduce its environment footprint. Environmental impact caused by the manufacturing process is measured and reviewed on a quarterly basis.

3. Maintain Quality of Product

Westman has a world-class manufacturing facility and process. It has employed state of
the art automation, equipment, and techniques to ensure the high quality of its product. It
has developed a quality assurance program using automation equipment, including PLCs,
Historian, and high precision sensors operating on a high-speed control network to
monitor product quality.

4. Maintain Production Goals

531Meeting the monthly production goals is an important objective for Westman, and532ensures the supply of products to its customers in a timely fashion. It also maintains533financial stability for Westman. Constant 24/7 production enables Westman to plan its534manufacturing operation to meet its production goals and customer demand. The535investment in automation equipment and skilled professional assists Westman to maintain536the monthly production goals.

538 **5. Protect Trade Secrets**

539Westman is committed to protecting its trade secrets, including product development,540manufacturing processes, product quality, and supply chain management.

541 **Role in the Supply chain**

542 Raw materials are supplied through a long-term contract established with suppliers and are 543 transported to the facility on a regular basis

543 transported to the facility on a regular basis.

544 The end products are typically sold to customers on a large quantity. Delivery is sub-contracted 545 to several logistics companies which will handle the transportation from the Westman facility to 546 the end customers. Westman's products are typically being used as raw materials or addictive for

547 other industrial manufacturers

549 **Communication to Organization**

- 550 All critical and operational aspects of the Manufacturing system, key resources should be
- documented in network diagrams, manuals or other artifacts. The documentation will be
- reviewed on a yearly basis by the Director of Operations with assistance from the IT Manager.
- 553 This information will be shared with all employees, contractors depending on their role in the
- 554 Company.
- 555
- 556 Critical Manufacturing System Components:
- 557

- 558 The following are a list of critical Manufacturing system components:
- Engineering workstation
- Supervisory PLC
- HMI Server
 - OPC and Controller Server
 - Historian Database Server
- Network devices
- 565 Supporting Services:
- 566

562

563

- 567 The supporting services required by Westman are broadband Internet
- 568 connection, electricity, natural gas, and water supply. The broadband Internet connection is a
- 569 business class service provided by a large national provider with business class service level
- 570 agreement
- 571

572 **3.1.5** Information Security Policy

- 573 The purpose of this Information Security Policy is to provide an overview of the policies,
- 574 standards, procedures and Technical controls that make up Westman's Information Security
- 575 Program. This policy is developed and executed by the Director of Operations, and has
- 576 expectations set for protecting Westman's IT and OT assets.

577 **3.1.6** Applicable Laws and Regulations

- 578 As a chemical manufacturer, Westman is required to comply with all federal and state legal or
- 579 regulatory requirements for chemical and hazardous materials. Westman is also required to
- 580 comply with all legal, regulatory and safety requirements being an employer.
- 581

582 **3.1.7** Security Organization and Governance

- 583 Information security is an inherent part of governance and consists of the leadership,
- 584 organizational structures and processes that safeguard Westman's information, its operations, its 585 market position, and its reputation.

Organizational Role	Security Responsibilities
CEO/General Manager	 Reviewing and approving the information security program and supporting policies, at least annually. Assigning the Director of Operations responsibility for organization's policies and procedures for use of any IT/OT assets, implementation, documentation and for meeting its compliance obligations. Serve as Point of Escalation for any incidents. Responsible for data breaches. Comply with Westman security policy
Controller / Finances	 Comply with Westman security policy Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Control Engineers	 Report any security incident and/or concerns to the Director of Operations. Help with the security requirements for their specific area. Comply with Westman security policy Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	 Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Product Development	 Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Operations	 Responsible for overall security of all IT/OT assets. Responsible for remediating vulnerabilities and/or mitigating any risks. Develop, implement and maintain the Security Program and Security Policy documents. Act as a liaison between operators, vendors, and management on matters relating to information security. Acting as a liaison between plant operators, vendors and management on matters relating to information security. Reports to the CEO about the status of the Security Program and security related risks or incidents.

IT Manager and IT Team	 Remediate vulnerabilities as directed by the Director of Operations. Report any security incident and/or concerns to the Director of Operations. Help with the security requirements for their specific business unit and area of expertise. Comply with the Security Policy.
Legal Counsel	 Handling of any legal questions/issues relating to security incidents. Handling of any external communications related to security incidents. Report any security incident and/or concerns to the Director of Operations
HR Manager	 Handling of any personnel and disciplinary issues relating to security incidents. Report any security incident and/or concerns to the Director of Operations

587 All employees, contractors and vendors are responsible for ensuring the security, confidentiality,

and integrity of information by complying with all corporate policies and procedures

589 **3.1.8 Privacy of Personal Information**

590 Employees should not assume any degree of privacy to information they create or store

591 on Westman's systems. Westman is a private organization and any information stored on its

592 information systems may be subject to disclosure under state law. Westman will disclose

593 information about individuals only to comply with applicable laws, regulations or valid legal 594 requests.

595 3.1.9 Operational Security

596 <u>Risk Management:</u>

597 The Organization's Risk Management Strategy can be found in section 3.4 Risk Management

598 Document. The Director of Operations shall conduct yearly risk assessments to identify potential

599 internal and external risks to the security, confidentiality and integrity of Westman.

- 600 Risk assessment involves evaluating risks and their likelihood along with selecting and
- 601 implementing controls to reduce risks to an acceptable level. Each risk assessment documents602 major findings and risk mitigation recommendations.
- All employees are encouraged to report any potential or existing risks to the Director of
- 604 Operations. Once the Director of Operations has identified or acknowledged the risks, the next

605 course of action will be determined (e.g., accept the risk, seek assistance from the IT Team,

606 contact a vendor to remediate the risk). Similarly, a vendor or contractor can also notify the

- 607 Director of Operations if they identify any threats or risks to their equipment. A
- detailed description of risk notification process can be found in Section 3.4 Risk Management
- 609 Document.

610 <u>Physical Security:</u>

- 611 The perimeter of the facility is fenced, and the main entrance has a gate that is open during
- business hours and locked after hours. There are two entrances to the main building. One is for
- 613 Employees only which is normally locked, employees need to swipe their personal
- badges to enter the building. The other entrance located at the front lobby staffed by
- a receptionist during normal business hours. Guests and visitors are required to sign in with
- 616 proper identification. Additional details about Physical security requirements are mentioned in
- 617 the Physical Security Section of the Security Policy document.
- 618 Personnel security is addressed through pre-employment screenings, adequate position
- 619 descriptions, terms of employment, and security education and training.

620 <u>Access Control:</u>

- 621 User access to IT and OT systems is based on the principle of least privilege depending on the
- 622 user's role in the organization. Proper authorization and approval by the Director of
- 623 Operations is required prior to granting access or operating any manufacturing system
- equipment. Sets of controls are in place to restrict access through authentication methods and
- other technical means. Passwords are managed through a formal process and secure log-on
- 626 procedures. Sensitive systems are explicitly identified and audited regularly.
- 627 Appropriate authentication controls are used for external connections and remote users. Physical
- and logical access to critical infrastructure is controlled. Duties are separated to protect systems
- 629 and data. Access rights are audited at regular intervals

630 **3.1.10 Security Awareness Training**

- 631 Security awareness information is provided to new employees at the time of hire. Online
- resources are provided to educate employees on best practices and the importance of reporting
- 633 security incidents. Additionally, the Director of Operations will ensure the employee understands
- their role and responsibilities in Westman's information security program.
- 635 Any information about potential or existing cyber threats to Westman's systems may be
- 636 exchanged routinely between the Director of Operations and external vendors. Likewise, any
- 637 news about email scams, phishing attempts and other malicious actions are posted to inform
- 638 users of possible threats.

639 Training for Users and Managers

- 640 Employees must perform online computer-based training or classroom-based training per
- 641 management approval. Below is a list of training options. Trade organization subscriptions to
- 642 newsletters and magazines will offer more industry specific training classes.

643 644	Computer Based Training
645	• ICS-CERT VLP (Virtual Learning Portal)
646	https://ics-cert-training.inl.gov
647	DHS Recommended Training
648	https://www.dhs.gov/chemical-sector-training
649	• SCADAhacker
650	https://scadahacker.com/training.html
651	In Person Training
652	Sans Industrial Control Systems Training
653	https://ics.sans.org/training/courses
654	
655	Training for Privileged Users
656	Privileged Users in the Organizational Use case:
657	Director of Operations
658	• This user has complete control of the manufacturing process within Westman.
659	IT Manager
660	\circ This user has complete control of the manufacturing process within Westman.
661	Responsibilities:
662	• Any privileged user within manufacturing environment will have two accounts. A primary
663	account used for normal activities, and a privileged "administrator" account for performing
664	privileged functions.
665	
666	• Primary accounts are used for normal daily operations.
667	• Primary accounts will have same rights as a standard Westman user account (e.g., email
668	access, Internet access).
669	• Privileged accounts will have administrative privileges, and must only be used when
670	performing administrative functions within manufacturing system (e.g., system updates
671	of firmware or software, system reconfigurations, device restarts).
672	Privileged users will adhere to securely using Administrative account when performing duties
673	within manufacturing system. If a privilege account becomes compromised this could have a
674	damaging impact on the manufacturing process.
675	Training:
676 677 678 679	• Training for privileged users will include training for regular users. Advance training will be provided from industry trade group specializing in automation process, or other specialty training organization focusing on manufacturing security for ICS environments.

680 681 682	 Examples: International Society of Automation (ISA) <u>https://www.isa.org</u> SANS (Information Security Training) <u>https://www.sans.org</u>
683	Training for Third Party contractors
684 685 686 687 688 689 690 691 692 693 694 695 696	 There are many different training options available. Training can be completed in person at a training facility, or online in a virtual classroom environment. In person training at a facility will have a cost associated and it not always appropriate depending on the level of training required. Online training can also have a cost depending on the level required, but there are also options that are free and provide a good understanding of the difference between a traditional Information Technology (IT) environment and Operations Technology (OT) environment. Payed Training Options. <u>https://www.sans.org/course/ics-scada-cyber-security-essentials</u> (Offers hands on training with experienced instructors). Free Online Training Options. <u>https://ics-cert-training.inl.gov/learn</u> (Offers virtual classroom environment at no cost).
697	3.1.11 Third Party Responsibilities and Requirements
698 699 700 701 702 703 704 705 706 707 708 709 710 711 712	 Third party contactors and vendors are required to be aware of the sensitive information within Westman facility and the steps to ensure propriety information is kept secret. Third party contactors and vendors will be re-evaluated yearly from the date of completion of first security compliance check. During this re-certification all objectives listed in the Security Awareness Training section above will be reviewed again to ensure security compliance with original plan. Remote connections from third party providers will be conducted using a VPN Connection. All third-party remote connections will be monitored and audited. All software and hardware tools used within Westman network will be approved first before service provider can proceed. No data shall leave Westman's network without written approval from President. Network accounts will be limited to only enabled when needed. Accounts used by service for remote access will require approval before being allowed to connect during normal business hours. Refer to Remote Maintenance Approval process in the Security Policy document for additional details.
713	3.1.12 Fire and Safety Regulations
714 715 716	• Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for

- manufacturing system. Fire Protection Systems will be checked minimum once per yearunless shorter intervals are required from superseding regulations.
- Only Industry approved Environmental Controls will be used within manufacturing systems,
 to included compliance with all Local, State, Federal laws. Environmental Control will be
 implemented to place human/community safety first before manufacturing systems.
- Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Fire Protection should be designed and implemented to protect human life first
- and equipment second. Installed fire protection systems will be certified compliant with
- existing/new environment by a licensed and accredited vendor. Check industry standards forany required baselines.
- 727

728 **3.1.13 Emergency Power**

- A short-term uninterruptible power supply (UPS) to facilitate both an orderly shutdown and
- transition of the organization to a long-term alternate power in the event of a major power loss.
- 731

732 3.1.14 Incident Management

- 733 Westman's Incident Response and Recovery Plan describe the detection, analysis, containment,
- radication, recovery and review of security incidents. The process for responding to security
- incident is designated in Incident Response Plan, while the procedures for incident recovery and
- resilience requirements are defined in the Incident Recovery Plan. Security incidents are
- managed by the Director of Operations who ensures that security incidents are promptly
- reported, investigated, documented and resolved in a manner that restores operation quickly and,
- if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The
- 740 Incident Response Plan and Recovery Plans are reviewed annually and updated as needed.
- Lessons learned from cybersecurity events will be used to revise and improve device detectionability while increasing protection for the organization and manufacturing system.

743 **3.1.15 Information Sharing Plan**

- 744 Information sharing with outside entities like trade organizations and local, state, and federal
- agencies can help strengthen cybersecurity. Information sharing, especially when receiving
- information from other outside entities, will improve Westman's situational awareness, and
- result in a more secure manufacturing system.

748 **Trade Organizations:**

- Relationships will be established with trade organizations. These relationships will be used to
- share information regarding cybersecurity incidents detected within the manufacturing facility.
- 751 Information shared with trade organizations regarding cybersecurity incidents must have all
- 752 proprietary information and trade secrets removed. This information will be listed as
- unclassified. Information regarding a cybersecurity incident containing information relating to

- proprietary, customer, or trade secret process will require a Non-Disclosure Agreement before
- data is transmitted; this would be considered classified information requiring approval from
 executive management before being sent.

757 Local Government:

Relationships with any local government organization whose purpose is to share cybersecurity incident data should be established.

760 State Government:

- 761 Relationships with any state government organization whose purpose is to share cybersecurity
- incident data should be established. Trade organizations should be able to provide contact
- information for state government incident sharing organizations, if they exist.

764 Federal Government:

Relationships with federal government agencies whose purpose is to share cybersecurity incident
 data should be established. Some federal government agencies are listed below.

767

- 768 DHS (CISA) Agency for reporting incidents of Phishing, Malware, Vulnerabilities.
- 769 <u>https://www.us-cert.gov/report</u>
- 770 DHS (NCCIC) Agency for reporting cybersecurity incidents relating to Industrial Control
- 771 Systems.
- 772 <u>https://ics-cert.us-cert.gov/Report-Incident</u>
- 773 774

775 **3.1.16 Periodic Reevaluation of the Program**

- The Security Program document will be continuously updated to reflect changes made to
- 777 manufacturing system and to improve cybersecurity. Lessons learned will be incorporated to
- help improve this document in the event a cybersecurity incident occurs.
- The Director of Operations shall reevaluate and modify the Program from time to time as
 deemed appropriate. The Director of Operations shall base such reevaluation and modification
 on the following:
- 782
- The results of the risk assessment and monitoring efforts
- Any material changes to the Westman's operations, business or infrastructure components
- 785 Any cybersecurity incident
- Any other circumstances that the Director of Operations knows or is informed of by the CEO
- 788
- 789

790 **3.1.17 References**

791 792 793	1.	Implementing Effective Information Security Program by SANS Resources <u>https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-</u> <u>effective-information-security-program-protecting-data-assets-of-1398</u>
794 795	2.	InfoSec Program Plan by University of Tennessee Knoxville <u>https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf</u>
796 797 798	3.	GCADA Sample Information Security Procedure http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeg uard%20policy).pdf
799 800	4.	IT Security Program by Old Dominion University https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf
801 802		

803 **3.2** Security Policy Document Example

Ī	1	
804		Security Policy
805		for
806		Westman Chemicals
807		
808		
809	-	
	Document Owner:	Director of Operations, Westman

810

811 Version812

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

813814 Approval

- 815 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 816

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

817

818

819 **3.2.1** Purpose

820 This Security Policy document defines the security requirements for the proper and secure use of

821 IT and OT services in the organization. The goal of the policies defined within is to protect the

822 organization and its users to the maximum extent possible against cybersecurity threats that

823 could jeopardize their integrity, privacy, reputation, and business outcomes.

824 **3.2.2 Scope**

825 Any employee, contractor, or individual with access to the organization's systems or data.

827 3.2.3 Policy Maintenance

- 828
- 829 The Security Policy must be approved by the Director of Operations in consultation with the IT
- 830 Manager and CEO/General Manager before it can be disseminated to employees. Any updates to
- this document will must also be approved by the Director of Operations.
- This policy document will be reviewed by the Director of Operations on an annual basis and willnotify all employees of any updates made to the policy.

834 3.2.4 Role-based Security Responsibilities

835 Security responsibilities vary depending on an individual's role in the company. Each is defined836 below.

Organizational Role	Security Responsibilities
CEO/General Manager	 Serve as Point of Escalation for any incidents. Responsible for data breaches. Comply with Westman security policy
Controller / Finances	 Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Control Engineers	 Often assume responsibility for intrusion detection in Manufacturing system. Report any security incident and/or concerns to the Director of Operations. Help with the security requirements for their specific area. Comply with Westman security policy Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	 Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Product Development	 Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Operations	 Responsible for overall security of all IT/OT assets. Responsible for remediating any detected events and vulnerabilities Implement and maintain Security Policy documents.

837 Employees

	• Serve as a SPOC for any security related incident and keeping upper management in the loop.
IT Manager and IT Team	• Assist in remediating vulnerabilities if asked by the Director of Operations.
	• Report any security incidents, anomalies detected and/or concerns to the Director of Operations.
	• Help with the security requirements for their specific area.
	Comply with Westman security policy
Legal Counsel	• Handling of any legal questions/issues relating to security incidents.
	• Handling of any external communications related to security incidents.
	• Report any security incident and/or concerns to the Director of Operations
HR Manager	• Handling of any personnel and disciplinary issues relating to security incidents.
	• Inform Law Enforcement if security incident involves data breach of sensitive information.
	• Report any security incident and/or concerns to the Director of Operations

839 External Personnel

Role	Security Responsibilities	
Equipment Vendor	 Assist in remediating vulnerabilities, upgrading software or hardware as required. Comply with Westman security policy if called in. 	
Visitor	• Comply with Westman security policy if called in.	

840

841 **3.2.5 Employee requirements**

842	1.	Employees must complete security awareness training and agree to uphold the acceptable
843		use policy.

- 8442. Employees must immediately notify the Director of Operations if an un-escorted or845unauthorized individual is found in the facility.
- 846
 847
 847
 848
 848
 848
 848
 848
 848
 848
 848

- 4. Terminated employees must return all company records, in any format.
- 850 5. Employees must verify with the Director of Operations that authorizations have been851 granted before allowing external personnel to connect to the IT or OT network.
- 6. Employees must report any physical security incidents to the Supervisor.
- 8537. Employees must understand and diligently follow the physical security requirements stated854 in the next section.
- 855 3.2.6 Physical Security
- 856
 1. Employees must always use and display physical identification (ID) provided by the
 company.
- 858
 859
 2. IDs must be designed to enable the immediate visual distinction between employees, external personnel, and visitors.
- 860 3. Sharing of IDs for any reason is strictly prohibited.
- 4. A sign-in sheet will be maintained by the receptionist to record all Visitor visits. These
 log records will be reviewed periodically by the Director of Operations.
- 863 5. Any visitors, contractors and/or maintenance personnel must always be escorted by an
 864 employee.
- 865
 6. Unauthorized removal of any documentation, equipment, or media from any device is
 866 restricted, unless authorized. Authorization can be obtained from the Director of
 867 Operations.
- All activities of visitors, contractors, and maintenance personnel will be subject to
 monitoring while onsite. An employee from the IT team will be assigned to monitor all
 computer activities if the visitor, contractor, or maintenance personnel is connected to
 any company network.
- 8. A supervisor will conduct monthly security status monitoring of the company to check
 873 for any physical security incidents.
- 874 **3.2.7** Information Technology (IT) Assets
- 8751. IT assets must only be used for the business activities they are assigned and authorized to876 perform.
- 8772. Every employee is responsible for the preservation and proper use of the IT assets they878 have been assigned.
- 3. IT assets must not be left unduly exposed.
- 4. Desktops and laptops must be locked if left unattended. This policy should beautomatically enforced whenever possible.
- 5. IT assets must not be accessed by non-authorized individuals. Authorization can beobtained from Director of Operations.
- 6. Configuration changes are to be conducted through the change control process,
 identifying risks and noteworthy implementation changes to security management.
- 886 7. All assets must be protected by authentication technologies (e.g., passwords).
- 887 8. Passwords must follow the password policy.

- 8889. The Director of Operations must be notified immediately after an asset is discovered to889 be lost or stolen.
- 890 10. Use of personal devices to access IT resources is prohibited.
- 891 11. Storage of sensitive information on portable media is prohibited, unless authorized by the892 Director of Operations.
- 893 12. Any sensitive information stored on IT assets, or being transported on a portable device,
 894 must be protected in such a way to deny unauthorized access, and must be encrypted in
 895 line with industry best practices and any applicable laws or regulations.
- 896

Description	Quantity
SuperMicro Servers	6
Allen Bradley 5700 Switches	2
Allen Bradley 8300 Router	1
HP Tower Workstation	1

IT Assets Inventory

898

899 **3.2.8** Operational Technology (OT) Assets

- 900 1. OT assets must not be used for operations they are not assigned or authorized to perform.
- 901
 2. The Director of Operations and Operators are responsible for the preservation and correct
 902
 use of the ICS assets they have been assigned.
- 903
 903 3. Physical access to OT assets is forbidden for non-authorized personnel. Granting access
 904 to the assets involved in the provisioning of a service must be authorized by Director of
 905 Operations.
- 4. All personnel interacting directly with OT assets must have proper training.
- 5. The Director of Operations is responsible for all OT devices. A Control Engineer is
 solely responsible for maintenance/configuration of the device they are assigned. No
 other personnel are authorized to modify OT asset configurations, including any
 modification to interfacing hardware or software.
- 9116. Usage of security tools on the OT network must be approved by the Director of Operations,912 and all affected Control Engineers must be notified.
- 913 7. Concept of least privilege must be followed when authorizing access to OT assets.
- 8. OT assets, such as PLCs, safety systems, etc., should have their keys in the "Run"
 position at all times unless being actively programmed.
- 9169. Accessing IT devices or internet use from the OT network, or OT assets, unless917 authorized, is prohibited.

- 918 10. Accessing IT devices or internet use from the OT network, or OT asset, is prohibited.
- 919 11. Use of personal devices to access OT resources is prohibited.

Description	Quantity
Allen Bradley ControlLogix PLC	1

921

OT Assets Inventory

- 922
- 923 **3.2.9** Lifecycle Accountability of assets
- Any IT or OT asset that needs to be decommissioned must be sanitized of all data, as per
 the manufacturer guidelines. This task will be usually performed by the IT Support staff.
- 926926 2. In case of an employee termination, an IT asset such as desktop PC or laptop must be reimaged prior to assigning it to a different employee.

928 3.2.10 System Maintenance

- Any maintenance tasks involving external resources such as Vendors, Contractors or
 other non-employees must be pre- approved by the Director of Operations. This can be
 coordinated by filling out the Maintenance Order approval form.
- 932
 932
 933
 2. It is the responsibility of Vendors, Contractors and/or Maintenance personnel with access to Westman's resources that due care is ensured to properly secure their own resources.
- 9349359353. It is responsibility of the IT staff that due care is ensured when using vendor devices on networks.
- 4. All systems and/or technical controls must be verified upon the completion ofmaintenance for any cybersecurity related impact.
- 938 5. All systems and/or technical controls must be verified upon the completion of
 939 maintenance for any cybersecurity related impact.
- 6. All maintenance work details will be logged in a Maintenance Tracker Excel sheet. TheSupervisor will update all details of the work performed in the sheet.

943 3.2.11 Data

- 944 1. Access to sensitive data must be authorized by Director of Operations.
- 945
 946
 946
 947
 947
 948
 949
 949
 949
 949
 940
 941
 941
 942
 943
 944
 944
 944
 945
 945
 946
 947
 947
 947
 947
 948
 949
 949
 949
 949
 940
 941
 941
 942
 943
 944
 944
 944
 945
 945
 946
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 947
 948
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
- 948
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
 949
- 4. It is recommended personnel use encrypted portable media or secure protocols while
 transferring data across systems. Director of Operations can provide you with systems or
 devices that fit this purpose. You must not use other mechanisms to handle sensitive data.

- 9535. If you have been permitted to work remotely you, extra precautions must be taken to954ensure sensitive data is appropriately protected.
- 9556. Physical copies of data should be stored in a secure location where unauthorized956 personnel cannot access it.
- 9577. Personnel should ensure physical copies of sensitive data are not left unattended on a printer.
 - 8. Physical copies of sensitive data should be shredded or disposed in a secure manner.
- 959 960

Description	Digital Files	Physical Copies	Databases
PLC program code	✓		
Chemical formulas	~	✓	
Quality Assurance Procedures	~	~	
Operating manuals and documentation	~	~	
Electrical diagrams	✓	~	
Network diagrams	~	✓	
Historical production data	\checkmark		v

Data types considered sensitive, proprietary, or containing trade secrets.

962 **3.2.12 Credentials Management**

- The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, frequency of change and employee expectations.
- 965 All staff, vendors, contractors or other stakeholders who use Westman's IT and OT systems
- 966 should be given authenticated access to those systems by assigning individual credentials
- 967 [username and password]. All access and restrictions to those access will be controlled by these
- 968 credentials.
- 969 The creation and removal of IT system accounts is managed via Microsoft Active Directory. In
- addition, The IT manager will determine and authorize user access to IT or OT systems.
- 971 Westman reserves the right to suspend without notice access to any system or service.

972 **3.2.13 Password Policy for Active Directory Accounts**

- All employee and system passwords must be at least 10 characters long and contain a
 combination of upper-case and lower-case letters, numbers, and special characters.
- 9752. Passwords must be changed every 90 days and cannot match a password used within the976 past 12 months.
- 977 3. Passwords must not be a dictionary name or proper name.
- 978978979979979979
- 5. Employees must choose unique passwords for all company accounts and may not use apassword that they are already using for a personal account.
- 982 6. Whenever possible, use of multi-factor authentication is recommended.
- 983
 984
 7. Default passwords, such as those preconfigured in newly-procured assets, must be removed before the asset is installed or connected to any organizational network.
- 985 8. Sharing of passwords is forbidden.
- 986 9. Passwords must not be revealed or exposed to public sight.
- 987 10. Personnel must refrain from writing passwords down.
- 988 11. Personnel must not use the "remember password" feature prevalent on many applications.
- 989 3.2.14 Privileged Accounts
- 990 **Privileged Users**
- 991 Director of Operations
 - This user has complete control of the manufacturing process within Westman.
- 993 IT Manager
 - This user has complete control of the manufacturing process within Westman.
- 995 **Responsibilities**
- Any privileged user within manufacturing environment will have two accounts. A primary
 account used for normal activities, and a privileged "administrator" account for performing
 privileged functions.
- 999

992

- 1000 Primary accounts are used for normal daily operations.
- 1001oPrimary accounts will have same rights as a standard Westman user account (e.g., email1002access, Internet access).
- Privileged accounts will have administrative privileges, and must only be used when
 performing administrative functions within manufacturing system (e.g., system updates
 of firmware or software, system reconfigurations, device restarts).
- 1006
- Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

1010 **3.2.15** Antivirus

- 1011 1. Antivirus software must be installed on all workstations and servers.
- 1012 2. Virus signatures must be updated daily.
- 1013 3. Antivirus software must provide the capability to push signatures on an ad-hoc basis.

1014 3.2.16 Internet

- 1015 1. Internet access is provided for business purposes.
- 1016
 2. Limited personal navigation is permitted from IT networks if no perceptible consumption
 1017
 of organizational system resources is observed, and the productivity of the work is not
 affected.
- 10193. Only authorized Internet access from the OT network is permitted. Authorized access canbe obtained from Director of Operations.
- 1021 4. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
- 1022 5. All Internal/External communications must be monitored and logged by in-house
 1023 network security tools. Logs must be reviewed regularly by the IT staffs and any
 1024 anomalies detected should be reported to the Director of Operations or IT Manager.
- 6. When accessing the Internet, users must behave in a way compatible with the prestige ofthe organization.

1027 3.2.17 Continuous Monitoring

- Westman will implement a Security Continuous Monitoring program. This will include performing comprehensive network monitoring using Commercial or Open source tools to detect attacks, attack indicators and unauthorized network connections.
- The Manufacturing system will be monitored for any cybersecurity attack indicators or
 IOC's.
- 1033 3. All External boundary network communications will be monitored.
- 4. All cybersecurity incidents must be logged in the Incident Response Management tool fordocumentation purposes.
- 1036
 5. All Local, State, and Federal detection activities applying to organization or manufacturing system will be followed in accordance within the law. Detection activities are to include any industry regulations, standards, policies, and other applicable
 requirements.
- 1040
 6. Monitoring activity levels will be increased during periods of increased risk and/or any other factors as necessitated by Westman's Management.

- 1043 7. All cybersecurity events detected will be communicated to the below list of defined
- 1044 personnel identified by the Director of Operations.
- 1045

Event Severity	List of Personnel
Low (All Events)	Control Engineers
Medium	IT Staff, Control Engineers
High (Requiring Urgent Attention)	IT Manager, Director of Operations

- 10478. Details of cybersecurity events will be shared with ICS-CERT (https://ics-cert.us-1048cert.gov/1049Infrastructure (CISA) is an agency of Department of Homeland Security which provides1050reporting capabilities for manufactures related to cybersecurity events
- 1051

1052 **3.2.18 External Service Provider Communications:**

- 1053 1. All communications from External Service Providers to Westman's systems will be monitored
- 1054 to ensure work provided by service provider is done correctly, including following all
- 1055 cybersecurity best practices and complying with Westman's security policies. Monitoring will 1056 include designated employee to oversee all activities performed.
- 2. Any Indicator of Compromise (IOC's) detected while monitoring external service provider
 communications will be reported and escalated via appropriate communication channels. The
 Director of Operations will reach out to the External service provider upon verifying the threat to
 discuss and seek an immediate remediation path accordingly.
- 1061 **3.2.19 User Access Agreement**
- 1062 Each employee provided with access to any Westman's resources, including Email and HR 1063 system, is required to review and accept the terms of the User Access Agreement.
- 1064 As an employee of Westman:
- You may use Westman's IT, OT systems and networks to which you have been granted access for work related purposes only. Accounts and access are granted based on each individual's roles and responsibilities.
- 10682. You should not expect any privacy on Westman's premises or when using Westman's property or networks either when onsite or accessing remotely
- 1070
 3. You will act responsibly to maintain the security and integrity of the information systems
 1071
 1072
 Westman.

- 4. You agree to co-operate with any audit by us or our Contractors of your access to theSystem.
- 1075 5. You understand your responsibility for respecting other employee's privacy and
 1076 protecting the confidentiality of information to which you have access, and will comply
 1077 with all privacy laws, codes and guidelines including,
- 1078
 6. Internet access must not be used for activities that are not authorized under existing laws,
 1079 regulations, or organization policies.
- 1080
 1081
 7. Any company laptops assigned to you should only be used for the purpose of conducting
 Westman's business. You are expected to take due care while using laptops.
- 1082 8. All laptops must be returned at the end of employment.
- 9. You understand that Transmission or intentional receipt of any inappropriate material or material in violation of law or district policy is prohibited. This includes but is not limited to: copyrighted material; threatening or obscene material: material protected by trade secrets; the design or detailed information pertaining to explosive devices: criminal
- 1087 activities or terrorist acts; gambling; illegal solicitation; racism; inappropriate language.
- 1088 10. You shall be subject to disciplinary action up to and including termination for violating 1089 this agreement or misusing the internet.

1090 3.2.20 Remote Access

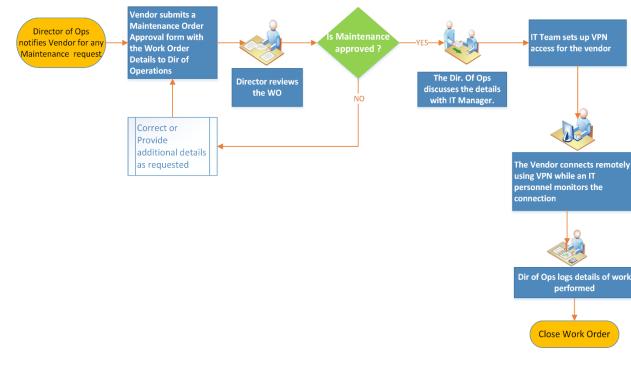
- 1091 This policy applies to the users and devices that need access the organization's internal resources 1092 from remote locations.
- Remote access for personnel requires pre-approval by Director of Operations. The IT manager must also be informed. Vendors requesting remote access must be registered with the company and are required to submit all work order details using the Maintenance Order Approval Form.
- 1097 2. The Director will determine list of authorized users for remote access.
- Remote access to sensitive or confidential information is not permitted on an unencrypted
 connection. Exception to this rule may only be authorized in cases where it's strictly
 required.
- 4. A VPN account will be setup by the IT Team and credentials shared with the vendor. The
 Once connected via a VPN, the vendor will be permitted Remote Desktop Access to
 select systems such as the Engineering Workstation or HMI Server depending on the
 nature of the task. The access will be disabled upon completion of the work.
- 5. All activities will be subject to monitoring by IT staff. Monitoring will start and continue until remote session is no longer required, or work has been completed. Appointed individual will indicate when remote session is active and ensure manufacturing system
- 1108 environment has been returned to same state before remote connection was established
- 11096. Installation of any software such as desktop sharing software etc. on authorized devices1110will be performed by the IT staff.
- 1111 7. Use of remote access technologies on personal devices is prohibited.

- 8. All devices connected via remote access technologies must use the most up-to-date antivirus software and virus signatures.
- 9. During an onsite visit, all activities will be subject to monitoring. Dedicated IT personnel
 will be assigned to monitor the vendor over the shoulder while he/she is working off a
 computer.
- 1117 10. Split tunneling will be disabled. All internet bound traffic will be directed through1118 Corporate network during a VPN session.
- 1119 3.2.21 Usage Restrictions
- To avoid confusing official company business with personal communications,
 employees, contractors, and temporary staff with remote access privileges must never use
 non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct business.
- No employee is to use Internet access through company networks via remote connection
 for illegal transactions, harassment, competitor interests, or obscene behavior, in
 accordance with other existing employee policies.
- Where supported by features of the system, session timeouts are implemented after a
 period of no longer than 30 minutes of inactivity. Where not supported by features of the
 system, mitigating controls are implemented.

1129 **3.2.22 Remote Maintenance Approval Process**

- 1130
- 1131

1132



1134 **3.2.23 Maintenance Approval Form**

Maintenance Order	Approval Form
Vendor Name	
Vendor Address	
Vendor Phone number	
Does the Vendor provide support to Westman currently?	□ YES □ NO
Does the Vendor system intended to be used	
have an Anti-virus installed?	□ YES □ NO
What items will be supported and/or worked upon during this session?	 PC / Laptops Servers Control System Devices Any other IT/OT Device Software Details:
Will any software or program need to be installed on Westman's systems?	□ YES □ NO Details (if YES):
Does this software require licensing to be purchased?	□ YES □ NO
Details of the task to be performed	
Is this a recurring activity	\Box YES \Box NO
Vendor Signature	
Work Approved (To be filled by Director of Operations)	□ YES □ NO
Director of Operations Signature	

1135

1136 **3.2.24 Communicate Information to Organization**

1137 All critical and operational aspects of the Manufacturing system, key resources should be

1138 documented in network diagrams, manuals or other artifacts. The documentation will be

1139 reviewed on a yearly basis by the Supervisor.

1140

1141 This information will be shared with all employees, contractors depending on their role in the 1142 Company.

1144 **3.2.25 Definitions and Acronyms**

Asset	A device owned by the organization
AV	Anti-virus
AV scanning	The act of scanning a device for viruses
Change control process	A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.
Device	Electronic hardware (e.g., machine, computer, laptop, phone, networking equipment)
Employee	An individual directly employed by the organization
External personnel	An individual who is not an employee (e.g., contractor, visitor)
Human machine interface (HMI)	Asset used by personnel to interface and interact with OT (e.g., machines)
ID	Physical identification (e.g., badge)
Industrial control system (ICS)	Typically, the hardware and software used to control processes, or operate machines and manufacturing processes
Information technology (IT)	Hardware devices such as computers, laptops, network switches, firewalls etc.
Least privilege	A user is only authorized to perform the functions necessary to perform their job
Operating system	Software that operates a device (e.g., Windows, Linux); typically, the interface used by the user
Operational technology (OT)	ICS and other devices (typically internetworked) used by the manufacturing process
Personal device	A device owned by an individual; not owned or controlled by the organization

Personnel	All employees and external personnel, excluding visitors
Portable media	USB flash drive, compact disc (CD), external hard drive, laptop
Remote access technologies	Software used to connect a device to the IT or OT network via the Internet, usually performed by personnel located off-site
Sensitive data	Data containing proprietary information or trade secrets pertaining to the operations of the organization; data that could cause damage to the organization if obtained by an attacker
Split tunneling	Split tunneling allows a mobile user access public network (e.g. Internet) and local LAN/WAN Corporate network at the same using same or different network connections
User	Individual using a device
Virus signature	Data used by antivirus software to identify viruses
VPN	Virtual private networking; see 'remote access technologies'.
Vulnerability scanning	Software used to detect common or known vulnerabilities on a device

1146 **3.2.26 References**

1147	1.	Security Policies by SANS Resources <u>https://www.sans.org/security-resources/policies</u>
1148	2.	Template for Security Policy by Project Management Docs
1149		http://www.projectmanagementdocs.com/template/Security-Policy.doc
1150	3.	Data Security Policy by Sophos labs https://www.sophos.com/en-
1151		us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

1152 3.3 Standard Operating Procedures Document Example

1	
1153	Standard Operating Procedures
1154	for
1155	Westman
1156	
1157	
1158	

Document Owner:	Director of Operations, Westman
-----------------	---------------------------------

1159

1160 Version

1161

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

1162

1163 Approval

- 1164 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 1165

Approvers	Role	Signed	Approval Date
	CEO/General		4-22-2018
	Manager		

1166

3.3.1 Introduction 1167

1168 This document defines the procedural steps management and employees will follow ensuring

consistence daily actives along with response to events occurring within the manufacturing 1169 1170 system for Westman. Within this document contains content which should be referred to often

1171 ensuring all employees/individuals performing work within manufacturing system are not 1172

inadvertently compromising cybersecurity posture by not following Standard Operation

1173 Procedures (SOPs).

1174 3.3.2 Purpose

- 1175 To provide a consistent repeatable process that can be followed to perform tasks within
- 1176 manufacturing system.

1177 **3.3.3 Scope**

- 1178 Management, employees, contractors, or individuals requiring access to manufacturing system
- 1179 for changes should be familiar with the contents included within this document.
- 1180

1181 **IDENTIFY**

1182 3.3.4 Asset Inventory

1183 Identifying assets within manufacturing system for Westman is a vital first step in protecting

1184 organization from malicious activates that could result in disruption to production. Westman uses

- 1185 multiple tools for asset inventory, some manual and some automated. Knowing the environment
- and what devices are installed allows the ability to detect non-approved devices on the network
- 1187 which could be an indication of malicious activity. Keeping devices updated with the latest
- 1188 patches ensure to mitigate potential weakness within manufacturing system. All patches will be
- 1189 carefully examined to determine if there could be any performance impact effecting production
- 1190 within manufacturing system.

1191 <u>Manual</u>

- 1192 Devices not able to be automatically scanned will be added to the Excel spreadsheet and updated
- 1193 quarterly. Devices included in manual process would be PLC and machine stations, including
- any additional devices that are unable to be scanned automatically with a tool. All inventory will
- 1195 be conducted during manufacturing system planned down time and inventory will include
- 1196 hardware and software.

1197 <u>Automated</u>

- 1198 Devices with the ability to be scanned will be added to Westman's asset inventory tool and
- scanned quarterly. Scanning quarterly will ensure manufacturing process is not affected. All
- 1200 scanning should be performed when manufacturing system has been placed into a non-
- 1201 production mode (system down time). Westman has chosen an asset inventory tool that has
- 1202 multiple version from open source to enterprise edition. Westman has selected Enterprise edition
- 1203 since this version provides the ability to schedule scans, baseline systems for monitoring
- 1204 changes. For additional information and references see.
- 1205 Westman inventory management tools will be configured for group access to ensure only
- 1206 individuals requiring access are allowed. This ensure that people within the organization only
- 1207 requiring read accesses are not granted a higher level, which could lead to inadvertent changes to
- 1208 tools configuration. See reference for how groups are created.
- 1209 Scans of manufacturing system will be conducted quarterly ensuring not to effect manufacturing
- 1210 process. Scans will audit software including license information, version, and configuration.
- 1211 Devices within the manufacturing systems will have software inventory audited and reviewed
- 1212 quarterly. Changes occurring to devices' software before the next update will trigger a required

- 1213 inventory to remain compliant. See reference for additional details for performing scanning
- 1214 within manufacturing system.
- 1215 Westman will apply updates to asset inventory software as they become available. Updates are
- 1216 required to keep system free from known vulnerabilities while including new features. See
- 1217 reference for additional information

1218 **3.3.5** Network Baseline

- 1219 Network baseline is important as it provides the ability to detect malicious active occurring on
- 1220 manufacturing system network. Westman will periodically perform baseline scans to identify any
- 1221 unusual traffic, which could be indication of malicious activity. All traffic observed during
- 1222 scanning should be reconciled to help create a more secure network. See reference for network
- 1223 baseline performed.

1224 **3.3.6 External Connections**

- 1225 Using company provided network diagram tools all network connection for external
- 1226 communication will be mapped. Mapping will include all relevant information for connection
- 1227 service provided. Example of information required would be assigned IP address for device
- 1228 providing service, support phone number, customer number, person of contact, and support level
- agreement and hours. External providers will include cloud services. Network diagram will beupdated quarterly.

1231 **3.3.7 Baseline Configurations**

- 1232 Baseline configurations was captured using two methods since some ICS devices don't allow
- automated tool scanning; for these devices' spreadsheet tracking is the preferred method.
- 1234 Devices lacking SSH, SNMP, WMI ability will require manual entry in spreadsheet.
- 1235 Steps used to perform automated scanning for Westman.
- 1236 Baseline configurations Westman implemented within Manufacturing systems helps to ensure
- 1237 inadvertent changes are detected before systems' integrity has been compromised.
- 1238 Open-AudIT¹ has been chosen for Westman due to scalable configuration depending on
- 1239 required needs. Instruction are listed for performing scanning. Once scanning has been
- 1240 performed changes with ICS devices are detectable by running reports identifying new software
- 1241 changes.
- 1242 Manufacturing systems was scanned to get initial baseline. Scanning steps used are listed below.
- 1243 Completed scans result scan be exported to CSV file for storage. See end of instructions for
- 1244 exported configuration.

¹ Open-Audit: https://www.open-audit.org

1245 Open-Audit Configuration steps within Process Control System once system has been1246 installed

1247 Initial Configuration:

1250

1258

• Login to Open-AudIT via web portal

• Navigate to \rightarrow Discovery \rightarrow Credentials \rightarrow Create Credentials

Discover -	Report -	Manage -
Credentials	5	List Credentials
Discoveries	s 🕨	Create Credentials

- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop-down during credential creation and select the desired group these credentials will apply to.
- Our environment consists of mainly Windows machine, so Windows will be used for connection type.
- Now create a credential and select **Windows** for the type. Once completed click **Submit**.

ID		?
Name	PCS SCans	?
Organisation	Default Organisation -	?
Description	Perform Windows Scans	?
Туре	Windows -	?
Username	Open-AudIT@lan.lab	
Password	•••••	
Edited By	nmis	?
Edited Date	2018-09-26 14:33:24	?

- 1259 Organization Groups Creation:
- Click on Manage \rightarrow Orgs \rightarrow Create Orgs

	Manage - Applications Attributes Baselines Connections Dashboards Devices Fields Groups Licenses Locations	
1261	Maps Networks Queries Orgs Roles Summaries Users Widgets	List Orgs Create Crgs Import Orgs from CSV
1201	magna	
1262	•	Now enter Name: Description: and click submit at the bottom of the page to save. Name PCS Machines ? Description Process Control Machines ? Parent ID Default Organisation ?
1263		Type Organisation • ?
1264 1265	•	If you have multiple machines / equipment in different locations you can make Organizational groups based on business units, or related task.
1266	Config	gure Discovery Scan:
1267	•	Now click on Discover → Discoveries → Create Discoveries Discover → Report → Manage → Credentials Discoveries List Discoveries
1268		Files Create Discoveries
1269	٠	Enter a meaningful name for discover being created
1270		Name PCS Scans ?
1271	٠	Next, enter the subnet that'll be used for performing this scan. This scan is using
1272		172.16.0.0/22 ^{Subnet} 172.16.0.0/22 ? Search online for additional subnetting
1273		information / calculators if you'd like to learn more.
1274 1275	•	Network address: should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.
1276	•	Now, click on the advanced button to see more options.
1277 1278 1279 1280	•	Once Advanced has been expanded you'll have additional options to select if desired. These options are Org , Type , Devices Assigned to Org , and Devices Assigned to Location . These options aren't required but allow you to organize found devices into groups.

Ê

• Once all are selected click on **Submit** button to continue.

PCS Scans

۲

1282 **Discoveries:**

- Once the above steps have been completed clicking on **Submit** button you'll be taken to a new webpage that will allow you to run discovery process created in the previous step.
- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.
- 1288

- icon to the right. See screen shot for details. Default Organisation subnet Subnet 2000-01-01 172.16.0.0/22 00:00:00
- Once discovery has started you'll be taken to a new page allowing you to view status or cancel.
- 1291 Newly found devices are added to My Devices which is found on the home screen.
- 1292 Process Control System PCS Baseline.zip

- 1293 Detailed baseline reports generated out of Open-AudIT can be obtained from <u>PCS Baseline Data</u>
- 1294 Shown below is an export of the baseline data from one of the devices using Open-AudIT in the 1295 Process Control System.

			ې . ن				Engin	eeringWorkstation-FGS-4	47631ehh.csv - Excel					Shah, I	leeraj A. (Intl	Ctr) 🖽		
ile Ho	ome	nsert	Draw	Page Layout Form	ulas Data Rev	iew View Develop	er Help 🤇	Call me what you wan										
Le Cut te Forr			Calibri B I U	• 11 • Å Å • □ • □ <u>ੈ</u> • <u>A</u> •	= = = + +	eb Wrap Text ∰ Merge & Center →	General \$ • % •	Conditional Formatting →		Bad Calcula		Good Check Cell		insert Dele	te Format	∑ AutoSum ↓ Fill + ♦ Clear +	* AZ▼ Sort & Filter •	
Clipboar	d	r _s		Font 🕠	Alig	nment G	Number	r,		Styles				Cell	s		Editing	
0	• I	\sim	~	f _x														
А	E		С	D	E	F	G	н	I.	J	к	L	М	N	0	Ρ	Q	
id	syster	n id	current	last_seen	first seen	manufacturer	serial	description	smyersion	version	revision	date	asset tag	id				
14		55			3/30/2018 15:38			Default System BIOS	L51 v01.18	HPQOEM			2UA4270V	55				
id	syster	n_id	current	first_seen	last_seen	manufacturer	model	serial	device	caption	hard_drive	interface	partition_c	scsi_bus	scsi_logica	scsi_port	size	stat
16	5	55	у	3/30/2018 15:38	9/24/2018 14:36	(Standard disk drives)	RAIDVOLO	RAIDVOL0	\\.\PHYSICALDRIVE0	RAIDVOLO	0	SCSI	2		0		476929	ок 🖉
39	9	55	У	9/24/2018 14:36	9/24/2018 14:36	(Standard disk drives)	Verbatim STO	RE N GO USB Device	\\.\PHYSICALDRIVE1	Verbatim 9	1	USB	1				15280) Not
id	syster	n id	current	first seen	last seen	name	fqdn	ip	id	ip padded								
14	4	55	v	3/30/2018 15:38	9/24/2018 14:36	fgs-47631ehh	fgs-47631ehł	172.16.3.10	5	5 172.016.0	03.010							

CSF MFG PROFILE LOW SEC LVL EXAMPLE IG PROCESS-BASED MFG SYSTEM USE CASE

	system_id	current	first_seen	last_seen	mac	net_index	ip	netmask	cidr	version	network	set_by	interface	id	ip_padded
74	55	n	3/30/2018 9:26	3/30/2018 15:36			172.16.3.10	255.255.255.0	24	4	172.16.3.0	0/24		5	5 172.016.0
75	55	y	3/30/2018 15:38	*****	40:a8:f0:3d:48:ae	7	172.16.3.10	255.255.255.224	27	4	172.16.3.0)/27		5	5 172.016.0
76	55	y	3/30/2018 15:38	9/24/2018 14:36	40:a8:f0:3d:48:ae	7	fe80::5cca:8dfd:2281:	992e	64	6				5	5
	system_id			last_seen	name	-	-	max_file_size	overwrite						
148				9/24/2018 14:36		C:\Windows			As Needeo						
149				9/24/2018 14:36		C:\Windows			As Needeo						
150			-,,	9/24/2018 14:36		C:\Windows			As Needeo						
151				9/24/2018 14:36		C:\Windows			As Needeo						
152					Key Management Serv				As Needeo						
153				9/24/2018 14:36		C:\Windows			As Needeo						
154				9/24/2018 14:36		C:\Windows			As Needeo						
155					Symantec Endpoint Pro				As Needeo						
156	55	y	3/30/2018 15:38	9/24/2018 14:36	System	C:\Windows	20484	20480	As Needeo	55					
157	55	y		9/24/2018 14:36		C:\Windows		1028	As Needeo	55					
158	55	у	3/30/2018 15:38	9/24/2018 14:36	Windows PowerShell	C:\Windows	68	15360	As Needeo	55					
	system id	current	first_seen	last_seen	serial	bank	type	form_factor	detail	size	speed	tag	id		
10	55	y	3/30/2018 15:38	9/24/2018 14:36	16142323	DIMM4	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55		
11	55	y	3/30/2018 15:38	9/24/2018 14:36	16142314	DIMM3	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55		
12	55	y	3/30/2018 15:38	9/24/2018 14:36	16142322	DIMM2	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55		
13	55	y	3/30/2018 15:38	9/24/2018 14:36	16142352	DIMM1	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55		
	system id	current	first_seen	last seen	manufacturer	model	serial	description	device	manufactu	size	aspect_ratio	edid versi	cost cod	e id
6	55	y	3/30/2018 15:38	9/24/2018 14:36	Dell	DELL P2414H	27HW349M0EDL	1920 x 1080	A09A	14-Oct	24	16:09			55
11	55	v	9/24/2018 14:36	9/24/2018 14:36	Sharp	SHARP HDMI	0	1920 x 1080	1.00E+06	13-Jan	80	16:09			55

1297

1298 List of programs installed:

10661	55 y	3/30/2018 15:38 9/24/2018 14:36 Internet Explorer	9.10.9200.17609		** ** ** ** ** ** **	1/1/2000 0:00 Microsoft Cor
10662	55 y	3/30/2018 15:38 9/24/2018 14:36 Notepad++ (64-bit x64)	7.5.6		C:\Program Files\Notepad	++\un 0000-00-00 00:00 Notepad++ Te
10663	55 y	3/30/2018 15:38 9/24/2018 14:36 Intel(R) Network Connections Drivers	19	C:\Windows\system32	Prounstl.exe	0000-00-00 00:00 Intel
10664	55 y	3/30/2018 15:38 9/24/2018 14:36 OSIsoft MS Runtime Redistributables x64	3.1.1		MsiExec.e: 20150306	0000-00-00 00:00 Rockwell / D:
10665	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft Visual C++ 2010 x64 Redistribution	it 10.0.40219		MsiExec.e: 20150306	0000-00-00 00:00 Microsoft c:\
10666	55 y	3/30/2018 15:38 9/24/2018 14:36 Java 8 Update 60 (64-bit)	8.0.600.27	C:\Program Files\Java\jr	MsiExec.e: 20150928	0000-00-00 00:00 Oracle Cor C:
10667	55 y	3/30/2018 15:38 9/24/2018 14:36 Veeam Agent for Microsoft Windows	2.0.0.700	C:\Program Files\Veeam	MsiExec.e: 20170731	0000-00-00 00:00 Veeam Sof C:
10668	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft SQL Server 2012 Management	O 11.1.3000.0		MsiExec.e: 20170731	0000-00-00 00:00 Microsoft C:\
10669	55 y	3/30/2018 15:38 9/24/2018 14:36 PI Software Development Kit (PI SDK) x64	1.4.2.445	C:\Program Files\Rockw	MsiExec.e: 20150306	0000-00-00 00:00 Rockwell / C:\
10670	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft Visual C++ 2008 Redistributabl	e 9.0.30729.6161		MsiExec.e: 20150306	0000-00-00 00:00 Microsoft c:\
10671	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft .NET Framework 4.6.2	4.6.01590	C:\Windows\Microsoft.I	MsiExec.e: 20180301	0000-00-00 00:00 Microsoft C:\
10672	55 y	3/30/2018 15:38 9/24/2018 14:36 PI AF Client (x64) 2012	2.5.1.5159	C:\Program Files (x86)\R	MsiExec.e: 20150306	0000-00-00 00:00 Rockwell # D:
10673	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft SQL Server Compact 4.0 x64 E	4.0.8482.1	C:\Program Files\Micros	MsiExec.e: 20150306	0000-00-00 00:00 Microsoft D:
10674	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft System CLR Types for SQL Serv	et 11.1.3000.0		MsiExec.e: 20170731	0000-00-00 00:00 Microsoft C:
10675	55 y	3/30/2018 15:38 9/24/2018 14:36 SST DeviceNet Products 3.10	3.10.000	C:\Program Files (x86)\S	MsiExec.e: 20171026	0000-00-00 00:00 Molex Incc C:
10676	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft SQL Server 2012 Express Local	DE 11.3.6020.0		MsiExec.e: 20170731	0000-00-00 00:00 Microsoft C:1
10677	55 y	3/30/2018 15:38 9/24/2018 14:36 Microsoft Message Analyzer	4.0.7948.0		MsiExec.e: 20160519	0000-00-00 00:00 Microsoft E:
10678	55 n	3/30/2018 15:38 3/30/2018 15:41 Symantec Endpoint Protection	14.0.3876.1100	C:\Program Files (x86)\S	MsiExec.e: 20180206	0000-00-00 00:00 Symantec E:\
10679	55 y	3/30/2018 15:38 9/24/2018 14:36 FactoryTalk Historian Site Edition 4.00 Lin	re 4.00.00.0104			0000-00-00 00:00 Rockwell Auto
10680	55 y	3/30/2018 15:38 9/24/2018 14:36 FileZilla Client 3.28.0	3.28.0	C:\Program Files\FileZilla	FTP Client	0000-00-00 00:00 Tim Kosse
10681	55 y	3/30/2018 15:38 9/24/2018 14:36 Redundancy Module Config Tool	8.4.1.0	C:\Program Files (x86)\R	ockwell Sof 20170926	0000-00-00 00:0C Rockwell / C:\
10682	55 y	3/30/2018 15:38 9/24/2018 14:36 AX88772B Windows Drivers	1.0.0.0	C:\Program Files (x86)\A	SIX Electroi 20150914	0000-00-00 00:00 ASIX Electr D:
10683	55 y	3/30/2018 15:38 9/24/2018 14:36 Matrikon OPC Server for Simulation				0000-00-00 00:00:00
10684	55 y	3/30/2018 15:38 9/24/2018 14:36 MatrikonOPC Sniffer				0000-00-00 00:00:00
10685	55 n	3/30/2018 15:38 3/30/2018 15:41 Mozilla Firefox 41.0.2 (x86 en-US)	41.0.2	C:\Program Files (x86)\N	lozilla Firefox	0000-00-00 00:00 Mozilla
10686	55 n	3/30/2018 15:38 3/30/2018 15:41 Mozilla Maintenance Service	41.0.2.5765			0000-00-00 00:00 Mozilla
10687	55 y	3/30/2018 15:38 9/24/2018 14:36 OSSEC HIDS 2.9.2	2.9.2			0000-00-00 00:00:00
10688	55 y	3/30/2018 15:38 9/24/2018 14:36 PI Software Development Kit (PI SDK) x86	21.4.2.445	C:\Program Files (x86)\R	ockwell Software\FactoryT	alk Hi: 0000-00-00 00:00 Rockwell Auto
10689	55 y	3/30/2018 15:38 9/24/2018 14:36 PI Software Development Kit (PI SDK) x64	21.4.2.445	C:\Program Files\Rockw	ell Software\FactoryTalk Hi	storia 0000-00-00 00:00 Rockwell Auto

1299

1300 List of patches installed:

10880	55 y	3/30/2018 15:38	9/24/2018 14:36	Rockwell Automation Generic Safety Mod	9.05.3364.0	20150306	0000-00-00 0
10881	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2764913		1/19/2015	fgs-47631(0000-00-00 0
10882	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2764916		1/19/2015	fgs-47631(0000-00-00 0
10883	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2718695		1/19/2015	fgs-47631(0000-00-00 0
10884	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2670838		1/19/2015	fgs-47631(0000-00-00 0
10885	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2830477		3/6/2018	fgs-47631(0000-00-00 0
10886	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2592687		3/6/2018	fgs-47631(0000-00-00 0
10887	55 y	3/30/2018 15:38	9/24/2018 14:36	KB971033		1/19/2015	fgs-47631(0000-00-00 0
10888	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2479943		1/19/2015	fgs-47631(0000-00-00 0
10889	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2491683		1/19/2015	fgs-47631(0000-00-00 0
10890	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506014		1/19/2015	fgs-47631(0000-00-00 0
10891	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506212		1/19/2015	fgs-47631(0000-00-00 0
10892	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506928		1/19/2015	fgs-47631(0000-00-00 0
10893	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2509553		1/19/2015	fgs-47631(0000-00-00 0
10894	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2511455		1/19/2015	fgs-47631(0000-00-00 0
10895	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2515325		1/20/2015	fgs-47631(0000-00-00 0
10896	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2532531		1/19/2015	fgs-47631(0000-00-00 0
10897	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2533552		1/19/2015	nt authorit 0000-00-00 0
10898	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2533623		1/19/2015	fgs-47631(0000-00-00 0
10899	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2534111		1/19/2015	0000-00-00 0

1301

1303 **3.3.8 Update Baseline after Modifications**

1304 Manufacturing baseline will be reviewed quarterly and updated with any changes that have

1305 occurred since last review. During period between baseline updates any new equipment added,

1306 or configuration changes implemented will initiate a new baseline scan to be performed.

1307 GRASSMARLIN² and Wireshark³ are the tools used for updating baseline after modification
 1308 have occurred. Examples of changes within the manufacturing system would be updating

- 1309 software, license, system patches, firmware updates, new devices like PLCs' or HMIs' and other
- 1310 ICS components required for operations.

1311 **3.3.9** Network Operations Baseline

- 1312 Network baseline will be created within manufacturing system to identify all crucial components
- 1313 required for production to operate. Tools used for this process are as listed, GRASSMARLIN
- and Wireshark. Each tool listed provides slightly different capabilities and detail.
- 1315 GRASSMARLIN generates a diagram for easy visualization, compare to Wireshark which
- 1316 provides data without diagrams. These tools provide the required network operations baseline
- 1317 required for manufacturing process.

1318 **3.3.10** Priorities for Manufacturing Missions

- 1319 The priorities for manufacturing missions have been identified in the "Organization Overview"
- 1320 Section of the Security Program document.

1321 **3.3.11** Critical Manufacturing system components and functions

- 1322 The critical manufacturing system components and functions have been identified in the
- 1323 Organization Overview Section of the Security Program document.
- 1324

1325 **PROTECT**

1326 **3.3.12 Security**

- 1327 Security within the organization including the manufacturing system will be followed at all time
- 1328 to reduce risk of cybersecurity incidents. Sections below contain multiple references to
- 1329 procedures used at Westman for securing the manufacturing system.

² GRASSMARLIN: https://github.com/nsacyber/GRASSMARLIN

³ WireShark: https://github.com/nsacyber/GRASSMARLIN

1330 **3.3.13 Training**

- 1331 Training is a vital role for keeping the company safe for Cybersecurity threats. All employees,
- 1332 contractors and vendors should have completed required training before being allowed to work
- 1333 within manufacturing system. Awareness and Training for Third Party Contractors and Vendors
- 1334 should be reviewed and signed before being allowed to access manufacturing systems.

1335 **3.3.14 Port Security**

1336 Port security allows the ability to configure network ports to be associated with individual

- 1337 device's Media Access Control (MAC) addresses. Enabling port security ensures only designated
- 1338 devices are allowed access, any device not already in the approved list will be denied access.
- 1339 Port Security provides additional protection, when used with defense in depth strategies. See
- 1340 reference for steps required for setup within Westman.

1341 3.3.15 Network Segmentation

- 1342 Westman network for manufacturing systems has been segmented to improve speed and security
- 1343 within the environment. Network segmentation provides ability to control traffic from each
- 1344 network, ensuring only allowed communication can pass between each network. See reference
- 1345 for steps used for Westman.

1346 **Task: Implement network segmentation**.

• The Work Cell consists of the following network hardware.

Туре	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

1348

Network segmentation was implemented using the Allen Bradley Boundary router. The router has the following sub-networks defined.

1351

Interface	IP address of Interface	Network / Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN

1352

One of the Stratix 5700 switches was connected to the Fa 1/1 interface of the 8300 Router
 and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were
 assigned an IP address from the 172.16.1.0/24 subnet

- The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used
- 1358for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP1359address from the 172.16.2.0/24 subnet.

1361Task: Identify and control connections.

1362

	From	То	Direction	Controlled using
Connection	Cybersecurity LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Cybersecurity LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory, Plant and Engineering LAN	Internet	One way	Boundary Firewall (Cisco ASA) in the Cybersecurity LAN

1363

1364

1365 **3.3.16 Monitor Boundary Connections**

Network traffic will be monitored for external and internal communications using a firewall, or other type of device that allows for the ability to control connection traffic. Required network traffic leaving the manufacturing system will be allowed, all other traffic will be explicitly dropped. Traffic to manufacturing system will be limited to only those machines required for monitor from corporate network to manufacturing system and machines won't be allowed internet access. Device monitoring external/ internal connection/communications will forward all logging to internal Syslog server for archival purposes.

• External Boundary communications are monitored using Cisco ASA Firewall in the

1374 Cybersecurity LAN network.

Internal Boundary communications are monitored using Stratix 8300 series Firewall in the
 Work Cell.

1377 **Tool: Boundary Protection Device**

1378 The table below lists the boundary protection devices implemented

Туре	Description
Allen Bradley Stratix 8300	Firewall/Router for Work Cell
Cisco ASA Firewall	Firewall/Router in the Cybersecurity LAN

1379

1380 **Document: Boundary protection device configuration.**

1381 Refer to section 4.19 Network Boundary Protection

1382 **3.3.17** Actions that can be performed with/without Authentication

	Authentication Required to Physically/Logically Interact with Device?									
	Engineering Workstation	Supervisory PLC	HMI	Controller	Local Historian	OPC Server	VLAN switches	Boundary router		
Physical Interaction (All Users*)	Y	N	N	Y	Y	Y	Y	Y		
Logical/Network Interaction (All Users*)	Y	Y	Y	Y	Y	Y	Y	Y		

1383

HMI User Actions Requiring Authentication									
	View Process Status	Modify Process Setpoints	Silence/Clear Alarms						
All Users*	Ν	Y	Y						

Eı	Engineering Workstation User Actions Requiring Authentication									
	Login to Workstation	View/Modify PLC Logic	Access Engineering Files	All Other Actions						
All Users*	Y	Y	Y	Y						

Historian User Actions Requiring Authentication									
	View Historical Data	Modify Historical Data	Modify Configuration	Login to Server Desktop/CLI					
All Users*	Y	Y	Y	Y					

OPC Server User Actions Requiring Authentication					
ModifyLogin toConfigurationDesktop/CLI					
All Users*	Y	Y			

Controller User Actions Requiring Authentication						
	ModifyLogin toModify ControConfigurationDesktop/CLILogic					
All Users*	Y	Y	Y			

VLAN switches User Actions Requiring Authentication					
ModifyView switchConfigurationstatus					
All Users*	Y	Y			

	PLC Actions Requiring Authentication				
				Modify Logic	Change Mode (Run/Config)
All Users*	Ν	N	N	Y	Y

1392 * Authentication for *all users* does not imply authorization has been granted to any specific

1393

1394 3.3.18 Network Connections

All network connection with manufacturing system will be documented to include port numbersand cables will be labeled indicating their designated purpose.

1397 All connection will be reviewed and authorized before being placed into production.

1398 **3.3.19** Remote Maintenance

Remote maintenance activities will be coordinated and approved before vendor access is
allowed. All remote maintenance activities provided by a vendor will be controlled and
monitored to ensure no harmful or malicious activities occur. Any vendors or contractors
connecting to Westman for remote maintenance will require approval before connecting.
Requests will be documented to ensure proper audit trail for activity conducted within

1404 manufacturing system. See reference for detailed plan.

1405 **3.3.20** System Maintenance

1406 Reference System Maintenance within Security Policy

1407 **3.3.21 Change Control**

1408 Changes to manufacturing system will be submitted to a change control process ensuring that all

- applicable parties are aware and agree on actions being performed. Management will have final
- 1410 approval since production could be affected by down time.

- 1411 Changes within the manufacturing systems will be scheduled during non-production hours as not
- 1412 to affect processing within manufacturing system. Changes will be reviewed and authorized
- 1413 before being implemented. Potential system performance issues from the potential change must
- 1414 be determined before the change is made. Once changes have been completed a review will be
- 1415 conducted ensuring same security level continues to be maintained after changes have been
- 1416 implemented.
- 1417
- 1418 Responsible parties will evaluate security impact on change controls being performed within the
- 1419 manufacturing system environment. Change control reviewers will have final say for changes
- 1420 being implemented along with changes having an impact on security.
- 1421
- 1422 Below is a list of items that need to be change controlled

Device Name	Item Type	Details
Engineering Workstation	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (Factory Talk, RSLinx etc.)
	Hardware	Storage and Memory upgrade
OPC Server	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (PI, FactoryTalk Services Platform, RSLINX, Matrikon OPC)
	Hardware	Storage and Memory upgrade
Historian VM	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), SQL Server patches,
	Hardware	Storage and Memory upgrade
Plant Simulator	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.)
	Hardware	Storage and Memory upgrade
Controller Host	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (MATLAB, Matrikon OPC)
	Hardware	Storage and Memory upgrade
HMI Host	Software	OS Patches (Windows), BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (FactoryTalk View Site, FT Services Platform, FT View Studio)
	Hardware	Storage and Memory upgrade

PLC	Software	Firmware upgrade and any type of configuration change
Allen Bradley Boundary Router	Software	Firmware upgrade, Firewall rules and any type of configuration change
Allen Bradley Layer-2 Switches	Software	Firmware upgrade and any type of configuration change
		Firmware upgrade, Firewall rules and any type
Cisco ASA Firewall	Software	of configuration change
Switches	Software	Firmware upgrade and any type of configuration change
Active Directory	Software	Group Policy deployment, User account creation/modification
		Antivirus version upgrades, Any Endpoint
Symantec Antivirus	Software	policy deployment via Symantec Manager
Nessus	Software	Running vulnerability scan(s)

1424 **3.3.22 Media Sanitization for Devices**

Assets / Device type	Method used	Details
		Tool: DBAN ⁴ , Category: Software, Type: Open-Source
		Instructions: (1) Download and create a bootable media of DBAN
		(2) Boot the server using the bootable media
Hard Drives on		(3) Follow the on-screen instructions to run the multiple passes of data wipe.
servers,		(4) Once complete, verify if wipe was successful by booting
workstations	CLEAR	the server without the DBAN media

https://dban.org/

		The below instructions are found in the Allen Bradley manual for Stratix Managed Switches ⁵ <u>Clear:</u> (1) Login to Web Admin console (2) Navigate to Device Management Restart/Reset in the menu (3) Select Reset Switch to Factory Defaults and click on
Allen Bradley 8300 Boundary Router	CLEAR	Submit
Doundary Kouter	CLEAK	The below instructions are found in the Allen Bradley
Allen Bradley 5700		 The below instructions are found in the Anen Bradley manual for Stratix Managed Switches ⁶ <u>Clear:</u> (1) Login to Web Admin console (2) Navigate to Device Management Restart/Reset in the menu (3) Select Reset Switch to Factory Defaults and click on Submit
L2 switch	CLEAR	
HMI	CLEAR	 The HMI program is installed on a Windows 7 system. To uninstall this program (1) Login to the Windows system via an admin account. Go to Control Panel >> Programs and Features (2) Select and Uninstall all "FactoryTalk®" components. Reboot the machine if required.
		 This consists of 2 parts – Historian Suite and SQL Server database. Both are installed on a Windows system. They can be treated as any other program/software on a Windows system. To uninstall Historian program: Login to the Windows system via an admin account. Go to Control Panel >> Programs and Features Select and uninstall all "FactoryTalk®" components. Reboot the machine if required. OR
Historian	CLEAR	>> Factory Talk Site Edition >> Uninstall Factory Talk.

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

		To uninstall the SQL Database (1) From Program and Features select "SQL Server Compact Edition" and uninstall it.
		The Allen Bradley PLC is a modular chassis consisting of different modules such as DeviceNet Scanner, ControlLogix Module, EthernetIP Module and HIPROM time.
		 To reset the HIPROM Time Module: (1) Follow the instructions as per Allen Bradley HIPROM ⁷ manual and set the Rotary Switch to 888.
		 To reset the DeviceNet Scanner Module (2) Follow the instructions as per Allen Bradley DeviceNet ⁸ manual and set the Rotary Switch to 888.
		To clear the ControlLogix 5571 Module, Refer to the below instructions. These are defined in Allen Bradley ControlLogix 5000 Manual ⁹ .
		Clear the Program from On-board NVS Memory If your application allows it, follow these steps to clear the program from the 1756-L7x controller's on-board NVS memory. 1. Remove the ESM from the controller. 2. Remove power from the controller.
		 You can remove power in either of the following two ways: Turn power off to the chassis while the controller is installed in the chassis. Remove the controller from a powered chassis.
Allen Bradley PLC	CLEAR	 3. Reinstall the ESM into the controller. 4. Restore power to the controller in one of two ways.

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um538_-en-p.pdf http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1756-in566_-en-p.pdf http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

NISTIR 8183A VOL. 2 (DRAFT)

1427 3.3.23 Backup Procedures 1428 Servers, Workstations: 1429 Refer Section 9.4.5 Veeam Backup and Replication 1430 Network Devices: 1431 1. Launch the TFTP server on Engineering Workstation 1432 2. SSH to the switch / router and run the below commands Router# enable Router# copy running-config tftp Address or name of remote host ∏? <IP-address of Workstation> Destination filename [router-confg]? <Enter a file-name> 1433 1434 3. Ensure to manually save the configuration backup at a central secure location 1435 **ICS** Devices: 1436 Follow the Manufacturer's product manual to perform a backup 1437 Ensure to manually save the configuration backup at a central secure location

1438**3.3.24Priority Analysis**

- 1439 Manufacturing system will be evaluated quarterly to identify devices importance. Devices
- importance will be used to provide a criticality report containing the minimum pieces ofequipment required to continue productions.
- 1442

1444 **3.3.25 Vendor Requirements**

1445 Service Level Agreements (SLA) will be outlined and discussed, along with the need for

1446 required notification when an employee transfers departments', leaves the company, or is

1447 terminated that had direct network connectivity into Westman's network

1448 Service Level Agreement:

1449	Service Level Agreement (SLA)	٦
1450	for Vendor	
1451	by	
1452	Westman	
1453		
1454	Effective Date: 02-22-2019	
1455		

1455 1456

Document Owner:	Westman President

14571458 Version

1459

Version	Date	Description	Author
1.0	02-22-2019	Service Level Agreement	Westman President

1460

1461 Approval

^{1462 (}By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

Approvers	Role	Signed	Approval Date
Westman	Customer		2-22-2019
Vendor	Service Provider		2-22-2019

1463

1464Agreement Overview

1465This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between1466Westman and Vendor (Service Provider) for the provisioning of IT/OT services required to1467support and sustain the Product or service.

This Agreement remains valid until superseded by a revised agreement mutually endorsed bythe stakeholders.

1470 This Agreement outlines the parameters of all IT/OT services covered as they are mutually
1471 understood by the primary stakeholders. This Agreement does not supersede current processes
1472 and procedures unless explicitly stated herein.

1474 Goals and Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in
place to provide consistent IT/OT service support and delivery to Westman by the Service
Provider(s).

1479 The goal of this Agreement is to obtain mutual understanding for IT/OT services provision
1480 between the Service Provider and Westman.
1481

- 1482 The **objectives** of this Agreement are to:
- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
 Present a clear, concise and measurable description of service provision to the
 - customer.Match perceptions of expected service provision with actual service support and
 - Match perceptions of expected service provision with actual service support and delivery.
- 1488 1489

1486

1487

1473

1475

1491 Stakeholders

1492

1493 The following Service Provider and Westman will be used as the basis of the Agreement and 1494 represent the **primary stakeholders** associated with this SLA:

1495IT Service Provider: Service Provider

1496IT/OT Customer: Westman

1497

1498 Periodic Review1499

1500 This Agreement is valid from the **Effective Date** outlined herein and is valid until further 1501 notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in 1502 lieu of a review during any period specified, the current Agreement will remain in effect.

1503 The **Business Relationship Manager** ("Document Owner") is responsible for facilitating 1504 regular reviews of this document. Contents of this document may be amended as required, 1505 provided mutual agreement is obtained from the primary stakeholders and communicated to 1506 all affected parties. The Document Owner will incorporate all subsequent revisions and obtain 1507 mutual agreements / approvals as required.

- 1508 Business Relationship Manager: Westman (President)
- 1509**Review Period:** Yearly (12 months)
- 1510 **Previous Review Date:** 02-22-2019
- **1511 Next Review Date:** 02-22-2020
- 1512

1513 Service Agreement

1514

1515 The following detailed service parameters are the responsibility of the Service Provider in the 1516 ongoing support of this Agreement.

- 1518 Service Scope
- 1519

1517

1520	The following Services	are covered by this Agreement:
------	------------------------	--------------------------------

1521

• Apply system updates to manufacturing environment per vendor's recommendation

- Apply system updates to IT equipment when patches are released per vendor.
- Backup configure information for all IT/OT equipment within Westman
- Ensure cybersecurity tools are operating correctly within the environment
- Provide liaison service between OT vendor and Westman
- Product recommendation for new equipment being purchased and installed with
 Westman's manufacturing environment
- Manned telephone support
- Monitored email support

1531 1532 1533	 Remote assistance using Remote Desktop and a Virtual Private Network where available Planned or Emergency Onsite assistance (extra costs apply) Monthly system health check
1534 1535 1536	Customer Requirements
1537	Westman's responsibilities and/or requirements in support of this Agreement include:
1538 1539 1540 1541	 Payment for all support costs at the agreed interval. Reasonable availability of customer representative(s) when resolving a service related incident or request.
1542	Service Provider Requirements
1543 1544 1545	Service Provider responsibilities and/or requirements in support of this Agreement include:
1546 1547 1548	Meeting response times associated with service related incidents.Appropriate notification to Customer for all scheduled maintenance.
1548 1549 1550	Service Assumptions
1550	Assumptions related to in-scope services and/or components include:
1552	Changes to services will be communicated and documented to all stakeholders.
1553	Service Management
1554 1555 1556 1557	Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.
1558	Service Availability
1559 1560	Coverage parameters specific to the service(s) covered in this Agreement are as follows:
1561 1562 1563 1564	 Telephone support: 8:00 A.M. to 5:00 P.M. Monday – Friday Calls received out of office hours will be forwarded to a mobile phone and best efforts will be made to answer / action the call, however there will be a backup answer phone service
1565 1566 1567	 Email support: Monitored 8:00 A.M. to 5:00 P.M. Monday – Friday Emails received outside of office hours will be collected, however no action can be guaranteed until the next working day
1568	• Onsite assistance guaranteed within 72 hours during the business week

1569 Service Requests

1571 In support of services outlined in this Agreement, the Service Provider will respond to service 1572 related incidents and/or requests submitted by Westman within the following time frames:

- 0-8 hours (during business hours) for issues classified as **High** priority.
- Within 48 hours for issues classified as **Medium** priority.
- Within 5 working days for issues classified as **Low** priority.
- 1576Remote assistance will be provided in-line with the above timescales dependent on the1577priority of the support request.

1579 **Personal Changes:**

1580When an individual user with remote access leaves service provider, is transferred, or is1581terminated the service provider will notify Westman. If user had access to Westman's1582network, that access will be disabled, or deleted as soon as possible. System account1583passwords the service provider had will need to be changed to ensure user access into the1584network has been completely removed.

1585

1578

1570

1586 **DETECT**

1587 **3.3.26 Event Logging**

1588 Devices within manufacturing system shall be configured to send log data to central repository

1589 (Syslog Server) when supported. Logs sent from devices allow additional forensics analysis,

1590 which will be useful after a cybersecurity event. Westman logs all devices events alerts to central

1591 log server for review and archive purpose. Recorded events help identify any malicious activity

1592 within the manufacturing systems. Logs will be checked periodically looking for abnormal alerts

1593 generated from manufacturing system. See reference for additional information.

1594 **3.3.27 Event Impacts**

- 1595 Logged events will be examined to determine the impact if any against the manufacturing
- 1596 system. Events impacting manufacturing system will be reviewed to determine correlation with
- risk assessment outcomes. Once correlation has been completed action will be taken if required
- 1598 to increase cybersecurity posture to lessen future threats.

1599 3.3.28 Monitor

- 1600 All personnel within the manufacturing system will be required to sign-in upon entering ICS
- 1601 environment with date and time of entry, including when leaving work space. Any person found
- 1602 in violation of mandatory sign-in/sign-out sheet will be escorted out of the manufacturing
- 1603 environment. Individuals will be challenged to ensure they are employees or are being
- 1604 escorted around the environment.

- 1605 All network switches have been configured for port security, so unauthorized devices won't be 1606 allowed access to the manufacturing network without prior approval.
- 1607 Weekly wireless scans will be completed using a laptop within manufacturing system. Rouge or 1608 unknown wireless devices will be brought to management's attention for additional review.
- 1609 Periodic software scans with be performed on devices within manufacturing system to
- 1610 detect any unauthorized software.
- 1611 Switch logs within manufacturing system will be checked regularly to ensure no rogue devices
- 1612 have attempted to connect. Output from switch logs will be compared against hardware
- 1613 inventory performed in.

1614 **3.3.29 Forensics**

- 1615 Syslog server will be used for collection of system logs. Logs can analysis to understand the
- 1616 attack target along with determining the method that was used during the attack against devices
- 1617 within manufacturing system. In addition, tools such as Security Onion and Wireshark may be
- 1618 used to analyze events and packet captures respectively.

1619 **3.3.30 Detect non-essential capabilities**

- 1620 System scanning/auditing tool will be used to identify non-essential software applications
- 1621 installed on devices within manufacturing system. Software not required for operations will be
- 1622 removed and baseline configuration updated to reflect new configuration state.

1623 **3.3.31 Ensure resources are Maintained**

- 1624 Systems performance and resources can have a drastic effect on manufacturing
- 1625 process. Individual in charge of manufacturing system will be responsible for performing daily
- 1626 checks on all systems within the manufacturing system environment (OT). Checks will include,
- 1627 but not limited to physical observation of all operational components ensuring any warning
- 1628 lights or other area of concern are investigated further. System logs of
- all manufacturing devices will be checked at the beginning and end of every shift looking for
- 1630 any deviation from the normal baseline performance.
- 1631

1632 **RESPOND**

1633 **3.3.32 Fire Protection Systems**

- 1634 Fire protection for a manufacturing environment should be designed to safeguard electrical
- 1635 equipment. Manufacturing systems requiring protection can be PLCs', HMIs', Robots,
- 1636 Machining equipment, computers and other required devices. Fire Protection should be designed
- 1637 and implemented to protect human life first and equipment second. Installed fire protection

- 1638 systems will be certified compliant with existing/new environment by a licensed and accredited
- 1639 vendor. Check industry standards for any required baselines.

1640 3.3.33 Emergency and Safety Systems

- 1641 Emergency and Safety Systems will compile with Local, State, and Federal laws. This is to
- 1642 include safety regulations for workers' safety from Occupational Safety and Health
- 1643 Administration (OSHA). Industry regulation for safety will be followed per guidance from
- 1644 regulating industry.
- 1645 Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire
- 1646 Protection Systems specially designed for manufacturing process. Fire Protection System will
- 1647 place emphasis on human safety first and for most, before concern for manufacturing system.
- 1648 Fire Protection Systems will be checked minimum once per year unless shorter intervals are
- 1649 required from superseding regulations.
- 1650 Only Industry approved Environmental Controls will be used within manufacturing systems, to
- 1651 included compliance with all Local, State, Federal laws. Environmental Control will be
- 1652 implemented to place human/community safety first before manufacturing systems.

1653 **3.3.34 Detected Events**

- 1654 Detected cybersecurity event notification will be investigated to determine root cause and
- appropriate remediation steps will be taken to clear events returning the organization /
 manufacturing system to known good operating state.
- 1656 manufacturing system to known good operating state.
- 1657 This can be done by reviewing the logs or events in Graylog and/or Security Onion

1658 3.3.35 Vulnerability Management Process

- 1659 Vulnerability management is an essential component of any information security program and 1660 the process of vulnerability assessment is vital to effective vulnerability management.
- 1661 <u>Vulnerability Scanning and Management Tools</u>
- 1662 Tenable- Nessus will be used to perform vulnerability scans. The Results report generated by
- 1663 Nessus at the completion of the scan, is then fed into NamicSoft which is a vulnerability 1664 management, parsing and reporting tool.
- 1665 NamicSoft can create customized reports and logically group results for a consistent workflow1666 within the organization. The reports are reviewed by the foreman and then shared with the
- 1667 machine operators.
- 1668 <u>Vulnerability Scan Targets</u>
- 1669 All devices connected to both Plant and Supervisory network segments are scanned. The IT Staff 1670 will configure a scan for all network segments of Westman.

- 1671 A new scan can be established, or an existing one changed, by submitting a request to the
- 1672 Director of Operations.
- 1673 Vulnerability Scan Frequency/Schedule
- 1674 Scans are performed by the IT Staff on an on-demand, per-request basis as needed. The IT 1675 manager shall make provisions for an assessment once per month.
- All IT/OT device scans should be scheduled in the 2 weeks of maintenance window in
 December of each year.
- All device scans should be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal operations
- Any new device discovered needs to be classified under its appropriate group.
- 1681 <u>General Rules</u>
- The Engineers or IT staff will not make any temporary changes to information systems, for 1683 the sole purpose of "passing" an assessment. Vulnerabilities on information systems shall be 1684 mitigated and eliminated through proper analyses and repair methodologies.
- No devices connected to the network shall be specifically configured to block vulnerability
 scans from authorized scanning engines.
- Use caution when running vulnerability scans against OT Networks such as the Supervisory
 LAN and Field LAN Network. Scans should be scheduled off hours and during periods of
 maintenance.
- It is recommended to run authenticated scans from the vulnerability scanner.
- 1691 <u>Vulnerability Reporting</u>
- 1692 Upon completion of a vulnerability scan, the data is fed into NamicSoft out of which report is 1693 generated. A report will always be generated as proof that an assessment occurred.
- 1694 All IT/OT devices are organized into appropriate groups in NamicSoft as per the system they
- 1695 reside in. A device may belong to one or more systems. Reporting is done system wise so that
- the devices and vulnerabilities can more easily be distributed to the IT Staff, Manager and
- 1697 Director of Operations. Below is a table of type of reports that will be sent out.

Status Reports	Frequency	Purpose
Host table with affected vulnerabilities	Monthly	Information is presented for each host.
Vulnerability Assessment Report	Monthly	Information is presented for both scanned networks.

Host specific report	Ad-hoc	Information is presented for requested host.
Mitigated vulnerabilities report	Post remediation	Upon re-scanning a host to check if vulnerabilities have been mitigated or not

1699 **Remediation Management and Priorities**

- 1700 All vulnerabilities discovered must be analyzed by the Director, Control Engineers with
- assistance from IT Team and OT Contractor (if needed) to decide on the next course of action.
- 1702 All vulnerabilities discovered should be remediated.
- 1703 The below chart should be used for remediation timelines

Severity	Description	Remediation time
Critical	Nessus uses Common Vulnerability Scoring System (CVSS) for rating vulnerabilities. A Critical vulnerability has a CVSS base score of 9.0 or 10.	15 days of discovery
High	High-severity vulnerabilities have a CVSS score between 7.0 and 8.9.	30 days of discovery
Medium	Medium-severity vulnerabilities have a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	45 days of discovery
Low	Low-severity vulnerabilities are defined with a CVSS score of 1.0 to 3.9. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented	180 days of discovery
Info	Info level do not present security risk and are listed for informational purposes only. It is optional to remediate them.	Not required to remediate

1704

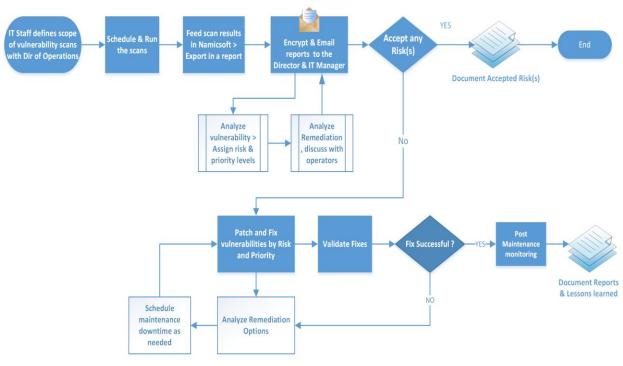
1705 Exceptions Management

Any exceptions to this policy, such as exemption from the vulnerability assessment process mustbe internally discussed and approved by the Foreman.

- 1708 Vulnerabilities may exist in operating systems, applications, web applications or OT devices.
- 1709 While every effort must be made to correct issues, some vulnerabilities cannot be remediated.
- 1710 Vendors may have appliances that are not patched, services may be exposed for proper
- application operations, and systems may still be commissioned that are considered end-of-life by
- 1712 the developer and manufacturer. In these cases, additional protections may be required to
- 1713 mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not
- 1714 identified as items of risk to the system and organization.

1715 False Positives identification may be documented through emails or the NamicSoft tool with the

- 1716 security staff. Acceptable Risk exceptions must be requested through the IT Team with an
- 1717 explanation containing:
- Mitigating controls what changes, tools, or procedures have been implemented to minimize the risk.
- Risk acceptance explanation details as to why this risk is not relevant to the company and systems.
- Risk analysis if the vulnerability is indeed compromised, what risk and systems will be affected.



1724 Process Overview

Westman Chemicals Vulnerability Management Process

1725

1727 **RECOVER**

1728 **3.3.36 Recovery Plan**

1729 **Purpose and Objective:**

- 1730 Westman developed this incident recovery plan (IRP) to be used in the event of a significant
- disruption to the features listed in the table below. The goal of this plan is to outline the key
- recovery steps to be performed during and after a disruption working to return to normal
- 1733 operations as quickly as possible.

17341735 Scope:

- 1736 The scope of this IRP document addresses technical recovery only in the event of a significant
- 1737 disruption. The intent of the IRP is to be used in conjunction with the business continuity plan
- 1738 (BCP) Westman developed. A IRP is a subset of the overall recovery process contained in
- the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies
- 1740 not directly relevant to the technical recovery outlined herein are included in the Business
- 1741 Continuity Plan and/or the Corporate Incident Response and Incident Management
- 1742 plans Westman has in place.
- 1743
- 1744 The specific objectives of this incident recovery plan are to:
- Establish a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage restoration of operations to back full processing capabilities;
- Enable rollback operations once disruption has been resolved and determined appropriate by recovery team.
- 1751
- 1752 Within the recovery procedures there are significant dependencies between and supporting
- 1753 technical groups within and outside Westman. This plan is designed to identify the steps that are
- expected to take to coordinate with other groups / vendors to enable their own recovery. This
- 1755 plan is not intended to outline all the steps or recovery procedures that other departments need to
- 1756 take in the event of a disruption, or in the recovery from a disruption.

1757 Incident Recovery Strategies:

1758 The overall IR strategy of Westman is summarized in Section 3.6 Incident Recovery Plan.

1759 **3.4** Risk Management Document Example

1760		Risk Management Strategy	
1761		for	
1762	Westman		
1763			
1764			
1765			
	Document Owner:	Director of Operations, Westman	

1766

1767 Version1768

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

1769

1770 Approval

1771 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

1772

- 1773 This Risk Management Plan defines how risks associated with the Westman will be identified,
- analyzed, and managed. This document can be used by the Director of Operations and
- 1775 Executives to foresee risks, estimate impacts, and define responses to issues.

1776 **3.4.1 Scope**

1777 Any employee, contractor, or individual with access to the organization's systems or data.

1778 3.4.2 Risk Management Process

1779 **Process**

- 1780 The overall process involves Identifying, Analysis, Categorizing, Reporting and Remediating.
- 1781 Risks will be identified as early as possible in the project to minimize their impact. The steps for
- accomplishing this are outlined in the following sections.

1784 **Risk Identification**

1785 Risk identification will involve the Company's Director of Operations, Control Engineers, IT

1786 Manager, evaluation of environmental factors, organizational culture and the project

1787 management plan including the project scope. There are many different types of threats that

can affect IT and OT infrastructure. These can include: 1788

- 1789 Technical threats — disruption caused by technological advances or failures • Structural threats — anything related to the building that houses your IT infrastructure 1790 •
- 1791
- that could cause it to be harmed 1792 • Financial threats — If the business loses funding or experiences another significant 1793 financial change
- 1794 Human threats — human error or loss of important individual •
- Natural threats weather and natural disasters such as earthquakes, tornadoes, and 1795 • 1796 floods

A Risk Management Log will be generated and updated as needed, a sample of which is shown 1797 1798 in the latter half of this document

- Software tools such as CSET¹⁰ will be used to perform RISK Assessments. The reports 1800 1801 generated will be discussed with the CEO.
- 1802

1799

- 1803 Additionally, the Control Engineers and Director of Operations will subscribe to NVD,
- 1804 USCERT, ICS-CERT and ISACS alert feeds to keep up with the latest vulnerabilities.
- 1805

1817

1806 This is an iterative process. As the program progresses, more information will be gained about 1807 the program and the risk statement will be adjusted to reflect the current understanding. New

1808 risks will be identified as the project progresses through the life cycle.

1809 **Risk Analysis**

- All risks identified either manually or via CSET will be assessed to identify impact on 1810
- 1811 operations. Qualification will be used to determine which risks are the top risks and which ones 1812 can be ignored.

1813 **Qualitative Risk Analysis**

1814 The probability and impact of occurrence for each identified risk will be assessed by the Director 1815 of Operations with input from the control engineers using the following approach:

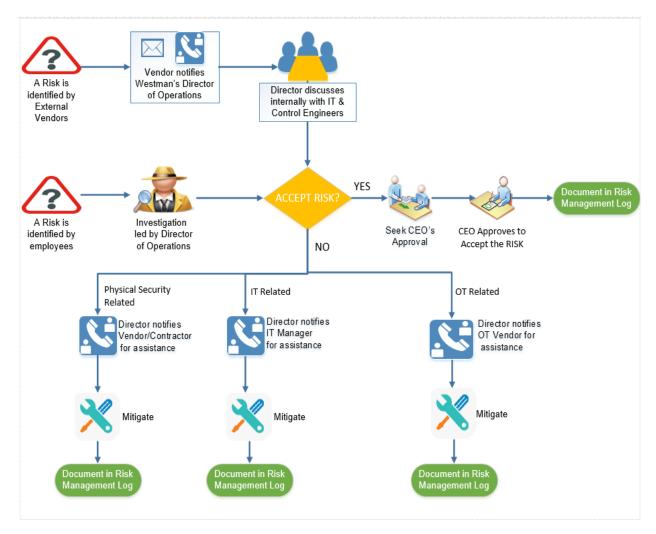
1816 **Probability**

• High – Greater than <70%> probability of occurrence in a year

¹⁰ CSET: <u>https://ics-cert.us-cert.gov/Assessments</u>

1818 1819 1820	 Medium – Between <30%> and <70%> probability of occurrence in a year Low – Below <30%> probability of occurrence in a year
1821	Impact
1822	• High – Risk that has the potential to greatly impact project cost, project schedule or
1822	performance
1823	• Medium – Risk that has the potential to slightly impact project cost, project schedule or
1824	• Medium – Kisk that has the potential to slightly impact project cost, project schedule of performance
1825	 Low – Risk that has relatively minor impact on cost, schedule or performance
1820	• Low – Kisk that has relatively minor impact on cost, schedule of performance
1627	
1828	Quantitative Risk Analysis
1829	This involves assigning a numeric value to the risk calculated as the product of probability of
1830	occurrence and impact score. Analysis of risk events that have been prioritized using the
1831	qualitative risk analysis process and their effect on project activities will be estimated, a
1832	numerical rating applied to each risk based on this analysis, and then documented in the risk
1833	management log.
1834	
1835	3.4.3 Risk Monitor and Control
1836	The Director of Operations and IT Team will conduct yearly risk assessments which includes
1837	CSET assessments, vulnerability scans of the manufacturing system that take into account
1838	vulnerabilities and potential impact to the manufacturing operations. An identified risk can be
1839	bought to Director's attention either by Westman's employees or by external contractors.
1840	
1841	The IT Team will scan the IT and OT assets when called upon; with Nessus to monitor for any
1842	software-based risks. The Nessus results will be fed into NamicSoft. Reports will be generated
1843	out of this tool and shared with the process owners. Any other type of risks like hardware based,
1844	physical, environmental will be identified and documented manually.
1845	
1846	All software-based vulnerabilities discovered using Nessus should be mitigated as per the
1847	Vulnerability Management Plan.
1848	
1849	If a software vulnerability has been remediated; a Nessus scan be re-run to see whether the
1850	situation has changed in a way that affects the manufacturing operations. For any corrective
1851	action has been taken, the risk management log will be updated.
1852	

1853 3.4.4 Risk Notification Process



1854

1855 3.4.5 Risk Response / Remediation Strategy

1856 For each major risk, one of the following approaches will be selected to address it:

- 1857
- Avoid eliminate the threat by eliminating the cause
- **Mitigate** Identify ways to reduce the probability or the impact of the risk
- 1860 Accept Nothing will be done
- **Transfer** Make another party responsible for the risk (buy insurance, outsourcing, etc.) 1862
- For each risk that will be mitigated, the team will identify ways to prevent the risk from reoccurring or reduce its impact or probability of occurring. This may include
- 1865
- 1866 Prototyping.
- Adding tasks to the project schedule
- 1868 Determining and allocating resources.

- 1869 For each risk that needs to be "Accepted", a document containing the list of accepted risks will
- 1870 be maintained by the Director of Operations.
- 1871
- 1872 The Director will reach out to an IT/OT Vendor for any risks and request remediation assistance.

1873 **3.4.6 Risk Appetite**

- 1874 Risk appetite is the broad-based amount of risk an organization is willing to accept in pursuit of 1875 its mission/vision. [4]
- 1876 Risk Appetite scale [5]:
- High the manufacturing system accepts disciplined risk taking because the organization
 has determined the potential benefits outweigh the potential risk.
- Moderate the manufacturing system accepts some risk taking, assuming the organization has reviewed the potential benefits and potential risks.
- Low the manufacturing system accepts minimal risk taking.
- None the manufacturing system accepts no risk taking because the risk is intolerable.

1883 3.4.7 Risk Tolerance

- 1884 Risk tolerance is the acceptable level of variance in performance relative to the achievement of 1885 objectives. In setting risk tolerance levels, management considers the relative importance of the 1886 related objectives and aligns risk tolerance with risk appetite. [4]
- 1887 Risk tolerance scale [6]:
- Low the level of risk will not considerably impact the ability of the manufacturing system to meet its mission objectives.
- Moderate the level of risk may impact the ability of the manufacturing system to meet its mission objectives.
- High the level of risk will significantly impact the ability of the manufacturing system to meet its mission objectives.

1894 **3.4.8 Risk Categories**

- 1895 Risk Categories are used to classify a risk. This table represents a sample of potential categories1896 that may be applied to each risk.
- 1897
- Safety the risk that human and/or environmental safety are compromised by an incident in the manufacturing system.
- Production the risk that product quality and/or production goals are compromised by an incident in the manufacturing system.
- Trade Secrets the risk that intellectual property and sensitive business data are compromised by an incident in the manufacturing system.

1904

Risk Category	Risk Tolerance	Risk Appetite	Mission Objectives
Safety	Moderate	Moderate	Maintain human safety Maintain environmental safety
Production	Moderate	High	Maintain quality of product Maintain production goals
Trade Secrets	Moderate	Moderate	Maintain trade secrets

1905

1906 3.4.9 Risk Reporting

This table describes the frequency and format of how the Director or IT Manager will document,analyze, communicate, and escalate outcomes of the risk management processes.

1909

Reporting Method	Description	Frequency
Risk Management log	A document to report the results of risk identification, analysis, and response planning	Twice a year
CSET Report	A document describing Risk assessment results	Twice a year
NamicSoft report	A document containing results of Nessus vulnerability scans.	Manual/Post vulnerability assessment

1910

1911 The Director will share the results of risk assessments (either the Risk Management Log or

1912 CSET Report) with the CEO.

1914**3.4.10 Sample Risk Management Log**

- 1915 A Risk Log will be maintained by the Director of Operations and IT manager. These will be
- 1916 reviewed in the project team meetings. This log captures the results of a qualitative and
- 1917 quantitative risk analysis and the results of planning for response.

Risk	Category (Technical, Management, Contractual, External)	Probability (High / Likely to occur =3, Medium / May or May not occur =2, Low / Unlikely =1)	Impact (High = 3, Medium = 2, Low =1)	Score (Product of Probability x Impact 1-3 Green 4-6 Yellow 7-9 - Red)	Risk Mitigation Strategy (e.g. Avoid, Transfer, Mitigate or Accept the risk)	Actions required	Status (Open, closed, In Progress)	Due Date

1918

1919 **3.4.11 Periodic Review**

1920 This document will be reviewed and updated annually by the Director in consultation with the IT1921 Manager.

1922 Annual reviews will be conducted determining component value within the manufacturing

1923 process being performed. Values will be used to determine required devices for continued

1924 manufacturing process and the effects if a cyber incident occurs against a device.

1925 **3.4.12 Asset Criticality Matrix**

1926 After a list of Westman assets or systems of value requiring protection have been identified by

the Hardware Inventory process, they will be assigned a value. Asset Value is the degree of

impact that would be caused by the unavailability, malfunctioning or destruction of the asset.

1930 Westman will use the following scale to calculate Asset value.

	ASSET VALUE
Critical	10
High	7-9
Medium	3-6
Low	1-2

1931

1932 Critical – Loss or damage of this asset would have grave / serious impact to the Operations of
 1933 the Manufacturing system directly impacting production. This can result in total loss of primary
 1934 services, core processes or functions. These assets are single point of failure.

1935 **High** - Loss or damage of this asset would have serious impact to the Operations of the

1936 Manufacturing system directly impacting production. This can result in major loss of primary

1937 services, core processes or functions. These assets can also be single point of failure.

- Medium Loss or damage of this asset would have moderate impact to the Operations of the
 Manufacturing system or Production. This can result in some loss of primary services, core
 processes or functions.
- 1941 **Low** Loss or damage of this asset would have minor to no impact on the Operations of the
- 1942 Manufacturing system or Production. This can result in little or no loss of primary services, core
- 1943 processes or functions.
- 1944

1946 A list of assets belonging to Westman with assigned value is presented in the below table.

Asset	Value	Numeric Value
IT / Communication Systems	High	8
OT / Field Devices – PLC, HMI	Critical	10
OT / Machining Stations	High	8
OT / Robots	High	9
Electrical Systems	Critical	10
Utility Systems	Medium	6
Site	Medium	6

1947

1948 **3.4.13 Definition and Acronyms**

IT	Information Technology which includes devices such as servers, laptops, workstations, switches and routers.
ΟΤ	Operational Technology which includes Industrial control system devices that are used by the manufacturing process.
Vulnerability	A weakness or a flaw in the system which an attacker can exploit to gain access.

1949

1950 **3.4.14 References**

1951	1.	Risk Management plan – Maryland Department of Information Technology
1952		doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc
1953		
1954	2.	Sample Risk Management plan – State of North Dakota
1955		https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-
1956		sample.pdf
1957		
1958	3.	Office of Management and Budget, "Management's Responsibility for Enterprise Risk
1959		Management and Internal Control", Office of Management and Budget, OMB Circular
1960		No. A-123, 2016. [Online]. Available:

	https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-
	<u>17.pdf</u> .
4.	United States Agency for International Development, "U.S. Agency for International
	Development Risk Appetite Statement", United States Agency for International
	Development, 2018. [Online]. Available:
	https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-
	Statement_Jun2018.pdf.
5.	Office of the Comptroller of the Currency, "Enterprise Risk Appetite Statement", Office
	of the Comptroller of the Currency, 2016. [Online]. Available:
	https://www.occ.treas.gov/publications/publications-by-type/other-publications-
	reports/risk-appetite-statement.pdf.

1974 **3.5** Incident Response Plan Document Example

	Incident Response Plan	
	for	
	Westman	
L		
Document Owner:	Director of Operations, Westman	

1981

1982Version

1983

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major revision	Director of Operations

1984

1985 Approval

- 1986 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 1987

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

1988

1989 **3.5.1 Statement of Management commitment**

Westman's leadership team is committed to information security and appropriate incident
response to accidental or deliberate incident within the company. Westman has established the
Incident Response Program to establish an actionable information security incident handling
capability that includes preparation, detection, analysis, containment, recovery, and reporting for
information security incidents. Westman's CEO oversees the Incident Response Program as a
whole, supports and funds maintenance of the program and ensures that resources are
appropriately maintained for preparedness.

1997 3.5.2 Purpose

1998 An incident can be defined as any event that, if unaddressed, may lead to a business interruption

1999 or loss. This document describes the plan for responding to information security incidents at

2000 Westman. It defines the roles and responsibilities of participants, characterization of incidents,

- 2001 relationships to other policies and procedures, and reporting requirements. The purpose of this
- 2002 plan is to detect and react to security incidents, determine their scope and risk, respond
- 2003 appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the
- 2004 likelihood of the incident from reoccurring.
- 2005 This Plan is to be executed during or after a cybersecurity incident.
- 2006 **3.5.3 Scope**
- 2007 This plan applies to all the employees of Westman.

2008 **3.5.4** Roles and Responsibilities

2009 The Westman Incident Response Team is comprised of:

ROLE	RESPONSIBILITIES	CONTACT DETAILS
Director of Operations	 Supervise other employees and working of the organization. Serves as a primary point of contact for any type of incident Making sure that all employees understand how to identify and report a suspected or actual security incident Leading the investigation for any type of incident, initiating the Security Incident Response Plan, filling out the Incident Report Form and reporting status to the CEO as needed. Documenting details of all incidents. 	Name: Phone: Email:
Control Engineer(s)	 Reporting a suspected or actual security incident to the Director. Reporting any other operational issues or concerns to the Director Complying with the security policies and procedures of Westman. 	Names: Phone: Email:

IT Manager	 Manages access to systems and applications for internal staff. Complying with the security policies and procedures of Westman. Assist in investigation, troubleshooting and resolving any IT/OT related incident summoned for. Advising the Director for any recommendations to procedures, policies and best practices. 	Name: Phone: Email:
General Counsel	 Handling of any legal questions/issues relating to security incidents. Handling of any external communications related to security incidents. 	Name: Phone: Email:
HR Manager	 Handling of any personnel and disciplinary issues relating to security incidents. Inform Law Enforcement if security incident involves data breach of sensitive information. 	Name: Phone: Email:

2010

2011 **3.5.5 Categories of Incident**

- 2012 Westman defines the following categories/types of incident for internal classification. These 2013 have been mentioned in the Incident Reporting Form as well.
- Intrusion
- 2015 Denial of Service
- 2016 Loss of Power
- Virus / Malware
- Social Engineering (Phishing, Phone, Email etc.)
- 2019 Data Breach
- Hardware Stolen
- User account compromise
- System Misuse
- 2023 Technical Vulnerability

2025 **3.5.6 Severity Classification**

2026 The Severity of an incident is determined based on the impact to the company and the urgency of2027 restoration.

SEVERITY	DEFINITION
High	 All users of the company are affected Work stoppage situation The incident involves sensitive data breach. The incident threatens Westman's operational goals There is no viable workaround
Medium	 There is a viable workaround Moderate to Low impact to the Operations. Service interruption potentially affects specific users and does not involve sensitive or personal data breach.
Low	 No impact to operations. Service interruption potentially affects only one person and does not involve sensitive or personal data breach.

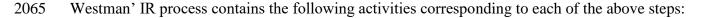
2028

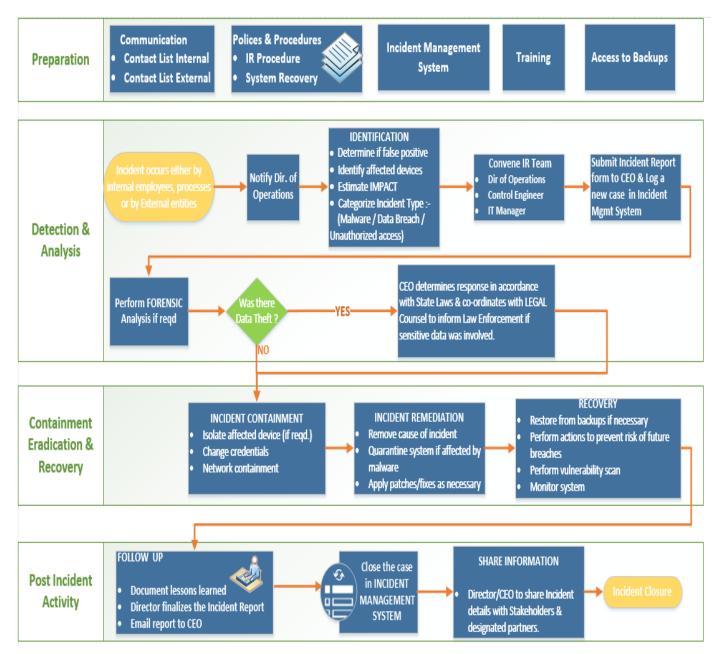
2029 **3.5.7** Restoration Priorities

RESTORATION PRIORITIES	DEFINITION	
High	• Service Restoration must be completed immediately, or significant loss of revenue, reputation, or productivity will occur.	
Medium	• Service Restoration must be completed within two business days or there is a potential for significant loss of revenue, reputation or productivity.	
Low	• Service Restoration can be delayed up to three or more business days without loss of revenue, reputation or productivity.	

2031 **3.5.8** Incident Response Policy

- An incident upon detection or being reported needs to be thoroughly investigated as per the
 process defined under "Detection and Analysis" step of the IR process in the next section.
 The investigation may be performed by the Director or by convening an IR Team.
- 2035 2. The incident needs to be classified as per the categories defined previously.
- 2036 3. Upon Investigation, the impact to the Manufacturing system must be determined. The IR
- 2037 Team may co-relate detected event information with Risk assessment outcomes to achieve 2038 perspective on the incident impact across the Organization. The incident will accordingly be 2039 assigned a Severity level and reported to the CEO. The Incident Report Template form 2040 should be used for this purpose.
- 2041 4. During the "Detection and Analysis" step, detailed troubleshooting or forensic analysis
 2042 should be performed to determine the root cause. This may be done using in place log
 2043 management tools or commercial products such as Wireshark.
- 2044 5. Upon investigation, the incident must be mitigated as per the "Containment, Eradication and2045 Recovery" step of the IR Process.
- 2046 6. The Director of Operations or IT Manager will co-ordinate incident response plan with2047 Westman stakeholders.
- 2048 7. The Director of Operations or CEO will share information about any cybersecurity incidents2049 and its mitigation with its designated sharing partners.
- 8. The overall Incident Response process and plan will be revised or improved after every
 incident. Procedures must be updated regularly to address evolving threats such as APTs,
 Organizational changes, Manufacturing changes and/or after any problems discovered during
 implementation, execution or testing
- 2054 9. User awareness Training and Testing procedures will be updates after every incident.
- 2055 10. The Director will communicate any changes or updates made to this policy.
- 2056 **3.5.9** Incident Plan Response Process / Workflow
- 2057The NIST Computer Security Incident Handling [1] Guide divides the incident response lifecycle2058into the following four steps:
- 2059 1. Preparation
- 2060 2. Detection and Analysis
- 2061 3. Containment, Eradication and Recovery
- 20624. Post-incident Activity
- 2063
- 2064





2066

2067 **3.5.10** Guidelines for Information Sharing

2068 Interactions with Law Enforcement

- All communications with external law enforcement authorities should be made after consulting with the CEO/General Manager.
- The Director of Operations will co-ordinate with the CEO and IT Manager to determine and share the minimum necessary information as required for incident response.

2073 Communications Plan

- The CEO will share information about any cybersecurity incidents and its mitigation with its designated sharing partners. Refer to the Next section for additional details
- All public communications about an incident or incident response to external parties outside 2077 of Westman are made in consultation with the CEO.
- The minimum information necessary to share for a particular incident is determined by the CEO in consultation with Director and other staff.
- 2080 **3.5.11** Guidelines for Reporting to Stakeholders

2081 **Overview:**

- The Director of Operations will compile all the details of incident(s) occurred in consultation 2083 with the IT manager.
- The Director will share the details in the IR Report Template form with CEO/General
 Manager and General Counsel. This will be used to determine level of severity, allowing the
 company to plan according.
- The Company's leadership team consisting of CEO/General Manager, Director of
 Operations, General Counsel, and IT Manager will make sure all facts have been gathered
 relating to the security incident before addressing any concerned with outside parties.
- The Company's response needs to be consistent ensuring message being delivered will not need to be retracted or changed due to lack of clarity.

2092 Who will be responding:

- Depending on the severity of the security incident this role can be filled by CEO/General
 Manager, Directory of Operations or the General Counsel.
- If the severity of a security incident requires additional resources, they should be contacted and brought in to help gather forensic information along with responding to inquiries.
- 2097
 ○
 Examples:

 2098
 ■
 Put

2099

2100

2101

2102

2103

- Public Relation
 - Forensic Investigator
 - IT consultant (Work in conjunction with IT Manager)
- Security Consultant (Work in conjunction with IT Manager and Director of Operations)
- Law Enforcement (Depends on severity)

2104 Notification:

- General Counsel will oversee notification planning since the potential for legal actions against Westman arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.

- General Counsel approval is required for work with any outside agency.
- CEO and General Counsel will both approve all communication being sent out regarding a security incident.

2112 **Communications:**

- CEO/General Manager will contact primary partners/vendors via phone call to inform them of the security incident. This should be done once all information has been gathered and a corporate response has been prepared.
- No voicemails will be left concerning the security incident in question. If recipient is unavailable schedule a follow up call.
- Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT
 Manager are the only Westman employees authorized to call partners/vendors not already
 contacted by CEO/General Manager.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by either
 Director of Operations, Controller/Finance, General Counsel, IT Manager.
- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can ONLY be approved by CEO/General Manager and General
 Counsel.
- 2130

2131 **Restoring Trust:**

- Westman's CEO or Director of Operations with the advice consultants and Forensic experts
 will notify partners/vendors and customers with the steps being taken to restore and strength
 system security.
- Westman IT Manager, Director of Operations will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known Westman leadership
- 2138 team will provide a full report which will be made publicly available containing facts
- 2139 relating to the security incident, along with the steps being taking to safe guard IT
- 2140 infrastructure ensuring this and future events don't happen again.

2141 **3.5.12 Incident Report Form Template**

Incident Reporting Template Form			
Contact information			
Date Reported :			Time Reported:
Name:		Title: Dept:	
Office Phone:			
		Details	
Date of Incident :	:		Time of Incident:
		Type of Incident - Check all that apply	
Intrusion		Social Engineering (Phishing, Phone, Email etc)	Technical Vulnerability
Denial of Service		Data breach	System misuse
Loss of power		Hardware stolen	Others, pls specify
Virus / Malware		User account compromise	
		Incident Description	
Provide a brief de	escription:		
Im	pact / Potent	ial impact - Check all of the following that appl	v to this incident.
Loss / Compromi		Financial Loss	
Damage to system		Other Organizations affected	
Damage to public		Damage to Integrity or Delivery of Goods, Services	
System downtime		Unknown at this time	
Provide a brief de			
		Affected System(s) information	
Host	IP		1
nost	IP	Application (if any)	0.S
nost	IF	Application (if any)	0.\$
nost	112	Application (if any)	0.8
nost		Application (if any)	0.5
nost		Application (if any) nsitivity of Data compromised (incase of Data I	
	Ser		loss)
Public (Informa	Ser tion is already ap	nsitivity of Data compromised (incase of Data I oproved for release & unauthorized disclosure will not caus	oss) e problems for the Company).
Public (Informa	Ser tion is already ap ormation is inter	nsitivity of Data compromised (incase of Data I	e problems for the Company). iated orgnaziations, business partners.
Public (Informa	Ser tion is already ap ormation is inter closure may be	nsitivity of Data compromised (incase of Data I oproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its	e problems for the Company). iated orgnaziations, business partners.
Public (Informa Internal Use (Info Unauthorized dis example: Email o	Ser tion is already ap ormation is inter closure may be ontacts, emails e	nsitivity of Data compromised (incase of Data I oproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its	oss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for	Ser tion is already ap ormation is inter closure may be ontacts, emails e slated to Privacy r access. Unauth	nsitivity of Data compromised (incase of Data I pproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm i	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for	Ser tion is already ap ormation is inter closure may be ontacts, emails e slated to Privacy r access. Unauth	nsitivity of Data compromised (incase of Data I oproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for	Ser tion is already ap ormation is inter closure may be ontacts, emails e slated to Privacy r access. Unauth	nsitivity of Data compromised (incase of Data I pproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm i	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email or Confidential (Re business need for Customers. For examples	Ser tion is already ap ormation is inter closure may be ontacts, emails e lated to Privacy r access. Unauth xample: Trade se	nsitivity of Data compromised (incase of Data I poproved for release & unauthorized disclosure will not caus aded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to cortes, Software code, Citizen's data etc).	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email or Confidential (Re business need for Customers. For examples	Ser tion is already ap ormation is inter closure may be ontacts, emails e lated to Privacy r access. Unauth xample: Trade se	nsitivity of Data compromised (incase of Data I pproved for release & unauthorized disclosure will not caus ided for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised:	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for Customers. For et Provide a descrip	Ser tion is already ap ormation is inter closure may be ontacts, emails e slated to Privacy r access. Unauth xample: Trade se	nsitivity of Data compromised (incase of Data I pproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Infe Unauthorized dis example: Email o Confidential (Re business need foi Customers. For ex Provide a descrip Law enforcement	Ser tion is already ap ormation is inter closure may be ontacts, emails e stated to Privacy r access. Unauth xample: Trade se tion of what	nsitivity of Data compromised (incase of Data I pproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far System disconnected from Network.	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Infe Unauthorized dis example: Email o Confidential (Re business need for Customers. For ex Provide a descrip Law enforcement Restored backupe	Ser tion is already ap ormation is inter closure may be ontacts, emails e stated to Privacy r access. Unauth xample: Trade se tion of what r notified s	nsitivity of Data compromised (incase of Data I oproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm 1 screts, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far System disconnected from Network.	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for Customers. For ex Provide a descrip Law enforcement Restored backup: AV Virus definition	Ser tion is already ap ormation is inter closure may be ontacts, emails e stated to Privacy' r access. Unauth xample: Trade se tion of what r notified s n updated	nsitivity of Data compromised (incase of Data I poproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu porized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far System disconnected from Network. Log files examined Any other action taken, pls specify	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Infe Unauthorized dis example: Email o Confidential (Re business need for Customers. For ex Provide a descrip Law enforcement Restored backupe	Ser tion is already ap ormation is inter closure may be ontacts, emails e stated to Privacy' r access. Unauth xample: Trade se tion of what r notified s n updated	Insitivity of Data compromised (incase of Data I poproved for release & unauthorized disclosure will not caus aded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far System disconnected from Network. Log files examined Any other action taken, pls specify	ioss) e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email or Confidential (Re business need for Customers. For er Provide a descrip Law enforcement Restored backup AV Virus definitio System reimaged	Ser tion is already ap ormation is inter closure may be ontacts, emails e lated to Privacy r access. Unauth xample: Trade se stion of what c notified s in updated i or quarantined	Insitivity of Data compromised (incase of Data I approved for release & unauthorized disclosure will not cause inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far	e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate the Company or its business partners or
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for Customers. For ex Provide a descrip Law enforcement Restored backup: AV Virus definition	Ser tion is already ap ormation is inter closure may be ontacts, emails e lated to Privacy r access. Unauth xample: Trade se stion of what c notified s in updated i or quarantined	nsitivity of Data compromised (incase of Data I poproved for release & unauthorized disclosure will not caus inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu porized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far System disconnected from Network. Log files examined Any other action taken, pls specify	ioss) e problems for the Company). iated orgnaziations, business partners. i business partners or its customers. For st be restricted to those with legitimate
Public (Informa Internal Use (Info Unauthorized dis example: Email o Confidential (Re business need for Customers. For ei Provide a descrip Law enforcement Restored backup: AV Virus definitio System reimaged	Ser tion is already ap ormation is inter closure may be ontacts, emails e lated to Privacy r access. Unauth xample: Trade se stion of what c notified s in updated i or quarantined	Insitivity of Data compromised (incase of Data I approved for release & unauthorized disclosure will not cause inded for internal use within the Company or with other affil against laws, regulations and may harm the Company or its tc). Violation. Information is private & sensitive in nature. It mu orized disclosure is against laws, regulations and will harm to crets, Software code, Citizen's data etc). Details of the Data loss was compromised: Follow up action taken so far	e problems for the Company). iated orgnaziations, business partners. business partners or its customers. For st be restricted to those with legitimate the Company or its business partners or

2143 **3.5.13 Definitions and Acronyms**

СЕО	Head of the organization. Serves as an escalation point.
HR Manager	An employee who deals with recruitment efforts and overall administration.
Incident	An event that is not part of normal operations that disrupts operational processes.
Director of Operations	An employee who supervises other employees and working of the organization.
Vulnerability	A weakness or flaw in the system which an attacker can exploit to gain access to.
Vulnerability Scan	The act of scanning a device or network for vulnerabilities
Control Engineer	An employee who operates the manufacturing equipment and reports to Director of Operations
Legal Counsel	Handles all legal matters. Reports to the CEO.
Stakeholders	Business Owners, System Owners, Integrators, Vendors, Human Resources Offices, Physical and Personnel Security Offices, Legal Departments, Operations Personnel.

2145

2144

2146 **3.5.14 References**

2147 1. NIST Publication for handing Computer Security	y Incident
--	------------

2148 <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf</u>

2150 **3.6** Incident Recovery Plan Document Example

	1		
2151		Incident Recovery Plan	
2152		for	
2153		Westman	
2154			
2155			
2156	1		
2157			
	Document Owner:	Director of Operations, Westman	

2158

2159 Version

2160

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

2161

2162 Approval

- 2163 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 2164

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

2165

2167 **3.6.1 Scope**

- 2168 The scope and purpose of this document is to inventory all of infrastructure and capture
- 2169 information relevant to the Westman's ability to recover its IT/OT environment from a
- 2170 cybersecurity incident. It, in turn also aims to provide an effective and efficient recovery effort.
- 2171
- 2172 **3.6.2** Objectives
- 2173 This plan has been developed to accomplish the following objectives:
- 2174 1. Limit the magnitude of any loss by minimizing the duration of a critical application2175 service interruption.
- 2176 2. Assess damage, repair the damage, and activate the repaired computer center.
- 2177 3. Manage the recovery operation in an organized and effective manner.

²¹⁶⁶

- 4. Prepare technology personnel to respond effectively in an incident recovery situation.
- 2179
- 2180 This IR Plan is to be executed during or after a cybersecurity incident.
- 2181 The person discovering the incident must notify the Director of Operations or IT Manager,
- 2182 who collectively assume responsibility for deciding which if any aspects of the IR plan
- should be implemented, and for establishing communication with employees, management,
- 2184 partners and customers.
- 2185

2186 **3.6.3 RPO and RTO Targets**

- 2187 Westman defines the following SLA's or Restoration times for operations recovery
- 2188

Type of Incident	RTO [2]	RPO [2]	Restoration Priority
Environmental Disasters such as Fire, Flood.	72 hours	24 hours	High
Recovery from Virus/Malware attack	24 hours	24 hours	High
Recovery from user account compromise	24 hours	24 hours	Medium
Recovery from Data Breach	48 hours	24 hours	High
Hardware failure, System Parts Replacement	48 hours	24 hours	High

2189

2190 Westman's Incident Response (IR) Team will consists of the following individuals.

ROLE	RESPONSIBILITIES
Director of Operations	 Lead and oversee the entire IR process Contact any Contractors/Vendors for assistance as needed. Making sure that all employees understand their roles and responsibilities. Update this document as per the Maintenance policy Notify the CEO for any escalation issues.
CEO / President	 Assist the IR Lead (Director) in their role as required. Make any Business decisions that are out of scope for the Director. Serve as point of escalation for any issues.

Control Engineers, IT Staff	 Install, implement or assist in implementing any tools, hardware software and systems as required Escalate any issues related to recovery to the Director. Complying with this plan.
OT Contractors, Vendors	 Assist in Recovery, Troubleshooting and resolving any OT related incident summoned for Advising the Director for any recommendations to procedures, policies and best practices. Complying with this plan

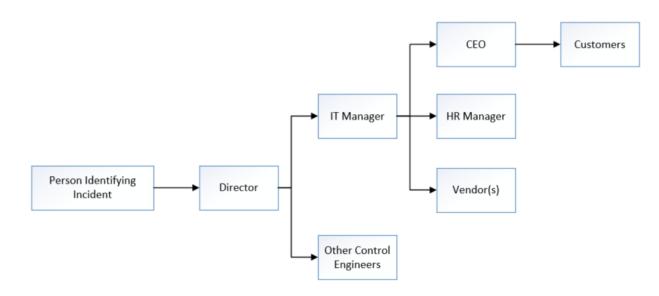
3.6.4 Contact Information

Name	Title	Contact Type	Contact Information
Employee A	ABC	Work	555-555-5555 ext 2
		Mobile	
		Alternate	
		Email	
Employee B	ABC	Work	555-555-5555 ext 3
		Mobile	
		Alternate	
		Email	
Employee C	ABC	Work	555-555-5555 ext 4
		Mobile	
		Alternate	
		Email	

2196 External Contacts

Name	Title	Contact Type	Contact Information
Account #		Mobile	
		Alternate	
		Email	
IT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
OT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
Network Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Telecom Carrier		Work	
Account #		Mobile	
		Alternate	
		Email	
Insurance Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Hardware Provider		Work	
Account #		Mobile	
		Email	

2198 **3.6.5** Notification Calling Tree



- 2199
- 2200

2201 3.6.6 Communications

2202 Notification

- The Director of Operations in consultation with the IT manager and Control Engineers will periodically update the CEO, Executives on the progress of Recovery Activities.
- General Counsel will oversee notification planning since the potential for legal actions against Westman arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.
- General Counsel approval is required for work with any outside agency.

2210 **Communications**

- CEO/General Manager will contact primary partners/customers via phone call to inform them about Recovery activities. This should be done once all information has been gathered and a corporate response has been prepared.
- Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT
 Manager are the ONLY Westman employees authorized to call partners/vendors not already
 contacted by CEO/General Manager.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by either
 Director of Operations, Controller/Finance, General Counsel, IT Manager.

- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can ONLY be approved by CEO/General Manager and General
 Counsel.

2226 Restoring Trust

- Westman's CEO or Director of Operations with the advice consultants and Forensic experts will notify partners/vendors and customers with the steps being taken to restore and strength system security.
- Westman's IT Manager, Director of Operations will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known Westman leadership
 team will provide a full report which will be made publicly available containing facts
 relating to the security incident, along with the steps being taking to safe guard IT
 infrastructure ensuring this and future events don't happen again.
- 2236 **3.6.7** Plan Testing and Maintenance

2237 Maintenance

- The IRP will be revised and updated after every recovery executed following a
 cybersecurity incident, Organizational changes, Manufacturing changes and/or after any
 problems discovered during implementation, execution or testing.
- The Director of Operations will be responsible for updating the document in consultation with Machine Operators and other personnel as required.
- During Maintenance periods, any changes to the IR Team must be accounted for.
- The plan will be updated after any Organizational or Manufacturing System changes.

2245 **Testing**

- Walkthroughs- IR Team members will verbally go through the specific steps as
 documented in the plan to confirm effectiveness, identify gaps or other weaknesses. The
 team should be familiar with procedures, equipment and operations.
- Simulations- An incident is simulated so that normal operations will not be interrupted.
 Hardware, software, personnel, communications, procedures, supplies and forms,
 documentation and utilities should be thoroughly tested in a simulation test.
- Full-Interruption Testing- IR Team members will perform a full-interruption test to activate a total IRP scenario. Caution must be exercised as this type of test disrupts normal operations.

2256 **3.6.8** Hardware Information

SYSTEM TYPE	HARDWARE INFORMATION	
	Hostname: FGS-47631EHH System Model: HP Z230 IP Address: 172.16.3.10 Network: Engineering LAN Location: Cabinet 101 Type: Physical Other: Eng. Workstation, Windows 7 Hostname: FGS-613380SH System Model: Supermicro Z97X IP Address: 172.16.2.5 Network: Supervisory LAN	Hostname: FGS-61338PSH System Model: Supermicro Z97X IP Address: 172.16.2.3 Network: Supervisory LAN Location: Cabinet 101 Type: Physical Other: Plant Simulator, Windows 7 Hostname: FGS-61338CH System Model: Supermicro Z97X IP Address: 172.16.1.5 Network: Control LAN
IT Servers	Location: Cabinet 101 Type: Physical Other: OPC Server, Windows 7	Location: Cabinet 101 Type: Physical Other: Controller, Windows 7
	Hostname: FGS-61338HH System Model: Supermicro Z97X IP Address: 172.16.1.4 Network: Control LAN Location: Cabinet 101 Type: Physical Other: HMI Server, Windows 7	Hostname: WIN- FPVTDCDEUCR System Model: Supermicro Z97X IP Address: 172.16.2.14 Network: Supervisory LAN Location: Cabinet 101 Type: Virtual Other: Controller, Windows 2008
Network Devices	Model: Allen Bradley 8300 Management IP: 10.100.2.8 Location: Cabinet 101 Function: Boundary Router	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Supervisory LAN Switch
	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Control LAN SW	
OT Devices	Model: Allen Bradley Logix 5571 IP Address: 172.16.2.102 Location: Cabinet 101 Function: PLC	

2257 **3.6.9 Backup Strategy**

SYSTEM TYPE	BACKUP STRATEGY
IT Servers Application Code	Frequency Weekdays (M-F): Directory level backup using Veeam Quarterly: Full system image backup using Veeam Source code is checked into a secure central network share. Server hosting the network share is backed up using Veeam.
Network Devices Boundary Router	 Frequency: Quarterly - Manual using Manufacturer Instructions <u>Note</u>: All Allen Bradley devices support Cisco IOS Command line. 1.SSH into the network switch/router from a Windows workstation which has a TFTP server installed. 2. Log in > Enter "enable" mode > Issue a "copy running-config tftp" command > Supply the IP address of TFTP Server > Give the backup file a meaningful name > Hit Enter. 3.The backup file will then be transferred over to the Windows workstation. Once done, copy the file over to a central secure location.
OT Devices	 Frequency: Quarterly - Manual using Manufacturer Instructions. 1.Control Engineer to either download the current image off the PLC using RSLINX Configuration Utility installed on the Workstation or pull out the MicroSD Card from the PLC and access the image using a card reader. For instructions on using RSLINX, refer to the product manual [3]

2.Copy over the image to the central secure location before making any change or upgrading the program.

2258

2259 **3.6.10 Recovery Procedures**

- The Incident Recovery plan will be executed following a cybersecurity incident.
- Any exceptions or issues during the Recovery process must be communicated to the Director 2262 and/or IT Manager.
- Depending on the incident, and on the number and nature of the IT services affected, one or 2264 more of the following IR procedures may be activated by the IR team:

Type of Incident	Plan of Action
Environment Disaster – Fire, Flooding	1. Identify root cause, co-ordinate initial response
	2. Remove damaged systems from the work cell.
	3. Evaluate damage
	4. Review Insurance policies and reach out to Insurance companies.
	5. Procure new hardware systems as required. Reach out to a Data recovery company for data recovery from damaged hard drives.
	1. Disconnect the affected systems from the network.
Virus / Malware – IT / OT Systems	2. Reach out to the IT/OT Contractor for assistance.
	3. Perform a full manual Anti-virus scan on the system
	4. If the Anti-virus software cannot detect or quarantine the infection, you may need to reinstall or restore the entire Operating System. Use Veeam to restore a full image backup, if the system in question is an IT system.

	5. Upon reinstalling the operating system, install all the appropriate patches to fix known vulnerabilities.6. Depending on the nature of the virus attack, change your original passwords as these could have been compromised during the infection.
Data Theft	 Fulfill all legal obligations. The CEO/General Manager to inform law enforcement and other customer protection agencies notifying them of breach. Immediately change system credentials, account passwords to public websites (if personal data is involved) Monitor in-house security controls or tools for any signs of new activity. Identify and erase any new files or programs that may have been installed as part of this attack. Use system baselines for reference. Engage a Contractor or other professional to conduct security audit.
Data Loss - IT Systems	 Browse through the list of directory level backups captured by Veeam for that host to select the backup to restore data from. Initiate a restore of the file or directory from the affected system using Veeam. If the system in question is a virtual machine, restore the most recent full VM image as it is using Veeam. Verify the file, folders and their permissions upon completion of the restore.

Hardware failure – IT Systems	 Follow up with the vendor for getting the faulty hardware replaced. Install and setup the new hardware as per the original baseline configuration. Refer to File system table below to configure any File system dependencies such as NFS mount points. Initiate a Restore operation from the most recent backup using Veeam. The restore procedure varies depending on if the system is physical or virtual. For more details, refer to the Veeam Backup guide. Upon completion of restore, verify connectivity and operations.
Hardware failure –Network Devices	 Order a replacement from a vendor. Setup and configure the new device as per its original counterpart. For more details, refer to the asset inventory database and/or any supporting documentation to reference the original baseline config such as Firewall rules, ACLS, Vlan, etc. Restore system configuration using Manufacturer instructions from the secure central repository. Verify connectivity between devices. Run operations to confirm.

	1. Order a replacement from a vendor.
Hardware failure / Configuration	2. Setup the new device by assigning it the
Restore- OT Systems	original static IP address and restore the
·	configuration on it as per manufacturers
	manual. Following are high level
	instructions for config restore of the Allen
	Bradley PLC
	Pull out the microSD card from the PLC
	and load a previously saved image on it
	using a card reader. A working image can
	be pulled from the central secure location
	used to save backups. Alternatively, a
	new base image can also be obtained
	from the manufacturer.
	► Insert the microSD card back into the
	PLC and power on the device.
	Test Connectivity and operations.

2265 2266

Filesystems as of Sep 2018

2267

Host	Local Drives	Size	Network Drives
		465GB (500GB	
FGS-47631EHH	C:\	HDD)	
		233GB (250GB	
FGS-61338PSH	C:\	HDD)	
		465GB (500GB	
FGS-613380SH	C:\	HDD)	H:\ HMI_Share (\\172.16.1.4)
		233GB (250GB	
FGS-61338CH	C:\	HDD)	
		233GB (250GB	
FGS-61338HH	C:\	HDD)	O:\ OPC_Share (\\172.16.2.5)
		465GB (500GB	
FGS-61338LHH	C:\	HDD)	
WIN-			W:\ Eng_Workstation
FPVTDCDEUCR	C:\	50GB	(\\172.16.3.10)

2268

2269 **3.6.11 Restoration Priorities**

2270 Should an incident occur and Westman need to exercise this plan, this section will be referred to

2271 reference restoration priorities in bringing systems online.

2273 IT Systems

Priority	IT System	Description
High	LAN-AD	Active Directory / DNS Server
High	Veeam	Veeam Backups Server
High	FGS-613380SH	OPC Server
High	FGS-61338CH	Controller Server
High	FGS-61338HH	HMI Server
High	FGS-61338LHH	Local Historian Host server
High	WIN- FPVTDCDEUCR	Local Historian Database Virtual Machine
Medium	FGS-61338PSH	Plant Simulator
Medium	FGS-47631EHH	Engineering Workstation
Medium	PI-DMZ	DMZ Historian Database Server
Medium	SymantecMgr	Symantec Antivirus
Low	Security Onion	Snort IDS
Low	Graylog	Syslog server
Low	GTB Inspector	DLP
Low	Hive	Incident Response Server

2274

2276 Networking Equipment

Priority	Device Info	Description
High	Boundary Router	Allen Bradley Router 8300
High	Supervisory LAN Switch	Allen Bradley Stratix 5700
High	Control LAN Switch	Allen Bradley Stratix 5700

2277

2278 OT Systems

Priority	OT System	Description
High	PLC	Allen Bradley Control Logix 5571
High	HMI Server	Factory Talk View Studio

2279

2280 **3.6.12 Definitions and Acronyms**

SLA	Service Level Agreement
Recovery Time Objective (RTO)	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the Maximum Tolerable Downtime. [2]
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. [2]

2281

2282 **3.6.13 References**

2283	1.	SANS Guide for DR: https://www.sans.org/reading-room/whitepapers/recovery/disaster-
2284		recovery-plan-strategies-processes-564
2285	2.	NIST SP 800-34 Contingency planning guide for Federal Systems
2286		https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

- 2287 3. Allen Bradley ControlLogix 5571 Manual
- 2288https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-2289um001_-en-p.pdf

Technical Solution Implementations 4.

2291 4.1 Introduction

2292 This section includes proof-of-concept technical solution implementations developed for the 2293 fictional company Westman. An overview of these technical solutions is discussed in Section 6 2294 of Volume 1 and potential technical solutions are discussed in Section 7 of Volume 1. Each 2295 organization's information security experts should identify the technical solutions that will best 2296 integrate with their existing cybersecurity program and manufacturing system infrastructure.

- 2297 There are five main areas of performance indicators being collected in the Process Control 2298 System:
- 2299 1. Manufacturing process performance: measures the performance of the manufacturing 2300 process, i.e. the chemical continuous process.
- 2. Network performance: measures the performance of the underlying TCP/IP network. 2301
- 2302 3. Computing resources performance: measures the performance of the computers, 2303 hardware, and software processes.
- 4. Industrial protocol performance: measures the performance of the industrial 2304 2305 communication protocol, i.e. the DeviceNet in the PCS.
- 2306 5. OPC Data Exchange performance: measures the performance of the data exchange 2307 mechanism of the system.
- 2308 Measurements in different areas provide insight of the entire system performance from different 2309 perspectives. The manufacturing process performance provides indicators on how well the high-2310 level manufacturing process and overall system perform. However, this may not be able to provide enough detail on the performance of the sub-systems, therefore measurements are also 2311 performed at sub-system levels. For example, a typical chemical continuous manufacturing is a 2312 2313 relatively slow process in comparison with computer networking. Therefore, a moderate TCP/IP 2314 network delay may not reflect in the measurement of the high-level manufacturing process 2315 performance. However, such TCP/IP delay may have significant impact on the sub-systems. The effects will not be reflected in the high-level measurement until significant delays are 2316 2317
- accumulated in sub-systems. Measurements in multiple levels provide details and in-depth 2318 understanding to key performance areas of the entire system. It helps to understand how the
- 2319 aggregate effects will impact the performance. Aggregate effects will be important to the high-
- level manufacturing performance. 2320
- Each of the technical solution implementation is organized as an experiment. For the 2321
- measurement purpose, each experiment has a fixed runtime of 4 hours (14,400 seconds). 2322
- 2323 Performance metrics and network packet capture are collected during the entire experiment run.
- 2324 After the experiment is completed, all the collected metrics and network packet capture will go
- 2325 through the post processing stage to filter, sort and rearrange data in proper order. The last step is
- 2326 to compute the key performance indicators from the sorted dataset using a set of Python scripts
- 2327 developed by NIST.

More technical detail of the Process Control System and the measurement process is described in
 <u>NISTIR 8188: Key Performance Indicators for Process Control System Cybersecurity</u>
 Performance Analysis.

4.1.1 Implementation Note – Due Diligence Implementing Technical Solutions

2332 It is important to note that the procedures used during this implementation (i.e., install a tool, 2333 then measure the impact) should not be used in a production system. Care must be taken before 2334 using any technical solutions, especially those that actively scan the manufacturing system 2335 network and its devices; manufacturers should first conduct an assessment of how these tools 2336 work and what impact they might have on the connected control equipment [3]. Technology 2337 evaluations may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the 2338 2339 nature of the information or the volume of network traffic. While this impact may be acceptable 2340 in IT systems, it may not be acceptable in a manufacturing system. In general, any operation that 2341 actively scans the manufacturing network should be scheduled to occur only during planned 2342 downtimes. [3]

2344 **4.2 Open-AudIT**

2345 4.2.1 Technical Solution Overview

Open-AudIT is an asset inventory tool providing scanning of hardware and software within the manufacturing environment. Open-AudIT scans are highly customizable to each environment, depending on the level required. The cost depends on the level of functionality desired for your environment. Editions offered by Open-AudIT vary from entry level community edition which is free, all the way up to enterprise edition. Enterprise was chosen since it contains the ability to setup schedule scanning, dashboards, and baselining of equipment.

2352

2353 Open-AudIT is a downloadable OVA which is easy to install. OVA install allows installation in

- a Hyper-Visor environment allowing for installation within an existing virtual environment
- 2355 without requiring purchasing additional hardware. Configure for initial discovery scans are
- straight forward and easy to configure and perform.
- 2357

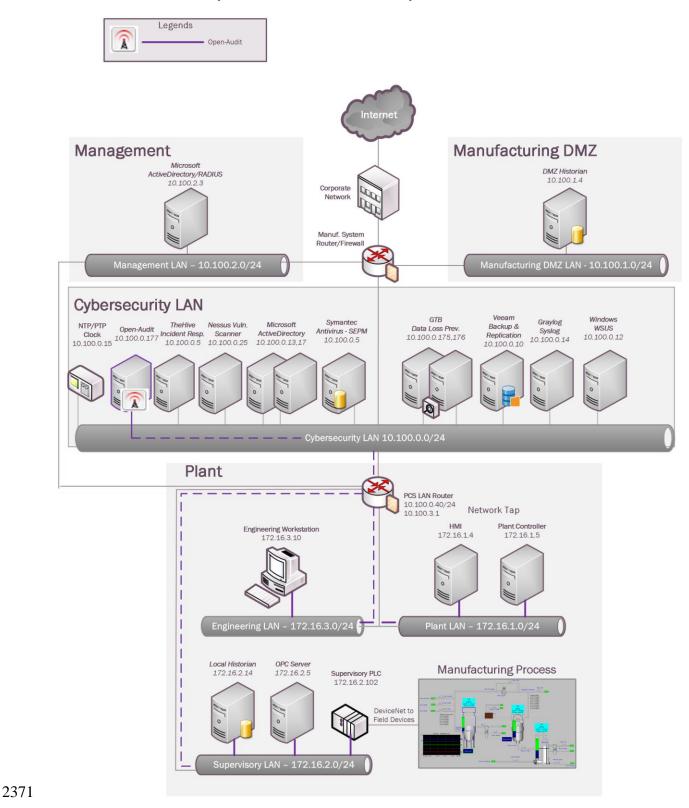
2358 **4.2.2** Technical Capabilities Provided by Solution

- 2359 Open-AudIT provides components of the following Technical Capabilities:
- Hardware Inventory
- Software Inventory
- System Development Lifecycle Management
- Configuration Management
 - Baseline Establishment (Enterprise Edition)
- Change Control
- 2366

2364

2367 **4.2.3** Subcategories Addressed by Implementing Solution

ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4,
PR.IP-6, PR.MA-1, DE.AE-1, DE.CM-7



2370 4.2.4 Architecture Map of Where Solution was Implemented

2372 4.2.5 Installation Instructions and Configurations

2374 2375

- Requirements from Opmantek who developed "Open-AudIT" indicate the specification 2376 •
- 2377 required are low. Please see this link for exact details provided by the vendor link.
- 2378

2379 **Instructions**:

- 2380 Download:
- 2381 1. Download and save **Opmantek Virtual Appliance** from Opmantek website.¹¹

Opmantek Virtual Appliance

8.6.3g

Experience the power of the complete Opmantek suite in one easy-toinstall Virtual Appliance. This package includes NMIS8, Open-AudIT, and all downloadable commercial modules. This package is created by Opmantek and is the easiest way to try out all our apps without the bother of setting up a dedicated server.

Virtual Appliance Release Notes Installation Guide

- 2382
- Once download has completed ".ova" file will need to be extracted to view the contents 2383 • and move to the next step (any tool supporting extracting .ova and .gz can be used). 2384 2385
 - Open the folder where the files were extracted too. There should be a total of four files. •
- 2386 Next, extract the two files with extension (.vmdk.gz) since this file is still •
- 2387 compressed. Once completed two files with the same extension (.vmdk) should now exist.
- 2388 Now two files just extracted need to be convert to "VHDX" format, so we can run these 2389 disk in a Hyper-V environment. See this link for instruction and additional information useful 2390 for converting virtual drive format.
- 2391 • Once both drives have been converted to "VHDX" format proceed to next section.

2392 Virtual Machine Setup:

- 2393 1. On the virtual server host open "Hyper-V Manager" and then right click on server
- 🛾 LAN) 📛 Virtual Machine... New name selecting New Virtual Machine 2394
- 2395 2. Now type in the name you going to give this server.

¹¹ Opmantek Intelligent Network Management Software <u>https://opmantek.com/</u>

		a check in the box " Stor verBuild	e the virtual m	achine in a o	lifferent	t location" click Next	ι.
		older or use an existing folder to store the virtual n nachine is stored in the default folder configured fo					
		al machine in a different location)					
2397	Location: D:\Hype	er-V(Browse.				
2398	4. The st	tep above will place the c	onfiguration an	d hard drive	files for	the newly create	
2399	Virtual M	lachine in D:\Hyper-V\Ne	ewServerBuild	(See Screens	hot)		
2400	5. Leave	Generation 1 selected a	and click Next.	This machine	e doesn't	require additional	
2401	features p	rovided from Generation	n 2.				
2402	6. Now a	assign how much memory	y your new mad	chine will be	given for	r use. For our	
2403	environm	ent we are using "2048"	Click next to co	ontinue.			
2404		the network this virtual		0	lick Next	t.	
2405	8. Now s	select "Attach a virtual	disk later" and	click Next.			
2406		ch a virtual hard disk later this option to skip this step now and attach an exis	sting virtual hard disk later.				
2407	9. Now a	a screen appears displayir	ng a configurati	on summary	click Fi	nish to complete.	
2107	Descripti		ing a configuration	ion sammary	, •11011 1		
	Name:	NewServerBuild					
	Memory	tion: Generation 1 y: 2048 MB					
	Networ Hard Di	12					
2400	To create	e the virtual machine and close the wizard, click Fin	nish.				
2408	10 N (C	1 . 1 1	
						newity created virtual	
2409		open Windows Explorer	-		•	newry created virtual	
2409 2410	machine a	and create a new folder la	beled "Virtual		•		
2410	machine a	and create a new folder la I Hard Disks 3/1/20	-		•	newly created virtual	
	machine a Virtua Virtua	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder	Hard Disk"	,		
2410 2411	machine a	and create a new folder la I Hard Disks 3/1/20	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder	Hard Disk"	w folder		
2410 2411	machine a	and create a new folder la Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder	Hard Disk"	w folder	location just created.	
2410 2411 2412	machine a	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM	Hard Disk" lier to this ne Type Hard Disk Image F	w folder v (Size 7,180,288 KB	location just created.	
2410241124122413	machine a Virtua Virtua Virtua Virtua Virtua Virtua Virtua	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua 11. Now 1 D:\H s 12. Open	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
2410241124122413	machine a Virtua Virtua Virtua 11. Now D Virtua 11. Now D Virtua	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua 11. Now 1 II. Now 1 II. Now 1 II. Open select "Se	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua 11. Now 1 II. Now 1 II. Open select "Se Connect Settings	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua Virtua 11. Now 1 II. Now 1 Virtua Virtu	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V/NewServerBuild/Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri- etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	s 11. Now 1 s 12. Open select "Se Connect Settings Start Checkpoin	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V/NewServerBuild/Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri- etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua Virtua 11. Now 1 II. Now 1 Virtua Virtu	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V/NewServerBuild/Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri- etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	s 11. Now 1 s 12. Open select "Se Connect Settings Start Checkpoin Moye	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V/NewServerBuild/Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri- etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua 11. Now 1 II. Now 1 II. Now 1 II. Open select "See Connect Settings Start Checkpoin Moye Export Rename Delete	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
2410 2411 2412 2413 2414 2415	machine a Virtua Virtua Virtua Virtua 11. Now 1 D:\H S 12. Open select "Set Connect Settings Start Checkpoin Moye Export Rename Delete Enable Rep	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
 2410 2411 2412 2413 2414 	machine a Virtua Virtua 11. Now 1 II. Now 1 II. Now 1 II. Open select "See Connect Settings Start Checkpoin Moye Export Rename Delete	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	
2410 2411 2412 2413 2414 2415	machine a Virtua Virtua Virtua Virtua 11. Now 1 D:\H S 12. Open select "Set Connect Settings Start Checkpoin Moye Export Rename Delete Enable Rep	and create a new folder la I Hard Disks 3/1/20 I Machines 3/1/20 moves the hard drive files yper-V\NewServerBuild\Virtual Hard Disks Name OpmantekVM-disk1.vhdx OpmantekVM-disk2.vhdx Hyper-V Manager and ri etting"	beled "Virtual 018 2:02 PM File folder 018 1:59 PM File folder s converted ear Date modified 3/1/2018 2:12 PM 2/28/2018 11:19 AM	Hard Disk" lier to this ne Type Hard Disk Image F Hard Disk Image F	w folder v (Size 7,180,288 KB 1,708,032 KB	location just created.	

- 2417 13. Memory should be configured for "2048"
- 2418 14. Virtual Processor "2"
- 15. Click on **"IDE Controller 0"** then click on **"Add"** button to attach a virtual hard.
- 2420 16. Click browse button and select the first virtual drive that was moved earlier, click

2421 Apply.

Controller:	Location:	
IDE Controller 0	♥ 0 (in use)	~
Media You can compact, convert, exp by editing the associated file. Si	and, merge, reconnect or shrink a virtual hard	l disk
 Virtual hard disk: 	poer y die fair pach to the file.	

- 2422
 2423
 17. Now click on **"IDE Controller 0"** again and click "**Add**" button to attach a virtual hard.
- 18. Click browse button and select the second virtual drive that was moved earlier, click
- 2425

2426

2429

2434

Appl	у.		
	Controller:	Location:	
	IDE Controller 0	✓ 1 (in use)	~
	Media You can compact, convert, expand, m by editing the associated file. Specify t	arge, reconnect or shrink a virtual hard disk he full path to the file.	
	Virtual hard disk:		
	D:\Hyper-V\NewServerBuild\Virtua	l Hard Disks\OpmantekVM-disk2.vhdx	
	New	Edit Inspect Browse	

- 2427 19. Now, select Network adapter and click the drop down and
- select "vswitch TestBed Lan" or what you have labeled your network.

memory		vswitch_TestBed_LAN V
2048 MB Processor 1 Virtual processor		VLAN ID Enable virtual LAN identification
IDE Controller 0		The VLAN identifier specifies the virtual LAN that this virtual machine
Hard Drive OpmantekVM-disk1.vhdx		network communications through this network adapter.
Hard Drive OpmantekVM-disk2.vhdx		2
E Controller 1		Bandwidth Management
💿 DVD Drive		Enable bandwidth management
None	=	
SCSI Controller		Specify how this network adapter utilizes network bandwidth. Both M Bandwidth and Maximum Bandwidth are measured in Megabits per se
work Adapter		bandwidd i and Maximum bandwidd i are measured in Megabics per se
vswitch_TestBed_LAN		Minimum bandwidth: 0 Mbps

- 2430 20. Click on Name and make sure to add some descriptive information that will allow other
- to easily see this information without having to login into machine.
- 2432 21. Select Integration Service and remove check from **"Time Synchronization"** Time will
- sync using internal NTP server via DNS pointer. Click "Apply" and then "OK".

Servi	ues -
-	Operating system shutdown
	Time synchronization
~	Data Exchange
~	Heartbeat
-	Backup (volume checkpoint)
	Guest services

2435 Configure Virtual Machine Networking:

- 2436 1. Open Hyper-V Manager and then right click on newly created machine and select start.
- 2437 2. Double click on machine being configured to open a Console window.

- 2438 3. Now type in **"root"** and then hit enter. Now type in Password which is
- 2439 \rightarrow "NM1\$88" without the quotes. Additional information for default login credentials can be 2440 found <u>here</u>.
- 4. Now type this command without the quotes to copy a static configuration for
- 2442 networking. cp ifcfg-eth0.static /etc./sysconfig/network-scripts/ifcfg-eth0 if prompted to
- 2443 overwrite file type "Yes"
- 5. Now type this command without the quotes "sudo nano /etc./sysconfig/network-
- 2445 scripts/ifcfg-eth0"
- 6. Now use the arrow keys to change the highlighted fields to your desired network
- configuration.

ı	iiguiulloll.
	DEVICE="eth0"
	NM_CONTROLLED="yes"
	ONBOOT=yes
	TYPE=Ethernet
	BOOTPROTO=static
	IPADDR=192.168.1.7
	NETMASK=255.255.255.0
	BROADCAST=192.168.1.255
	GATEWAY=192.168.1.1
	IPV4_FAILURE_FATAL=yes
	IPV6INIT=yes
	IPV6_AUTOCONF=yes
	IPV6_DEFROUTE=yes
	IPV6_PEERDNS=yes
	IPV6_PEERROUTES=yes
	IPV6_FAILURE_FATAL=yes
	NAME=eth0

2451

2452 2453

2454 2455

2456

- 2449 7. Once all fields have been updated use **Ctrl** + **O** "^**O**" to write the file and then **Ctrl** +
- 2450 **X** "^**X**" to

exit.					
Ğ Get Help	🔼 WriteOut	R Read File	Y Prev Page	🔭 Cut Text	^C
^X Exit	^J Justify	^W Where Is	🗘 Next Page	^U UnCut Text	^7

8. Now type **"service network restart"** These restarts networking services with the newly configured settings.

- 2457 Complete Additional Setup via Web Browser:
- 2458 1. Now with any web browser navigate to "IP Configured Earlier" example would
 2459 be "10.100.0.177"
- 2460 2. If prompted to proceed to untrusted site, select "Yes". This error is produce since SSL
- has not been configured and Open-AudIT redirects HTTP sessions over to HTTPS.
- 2462 3. Once this page opens you'll see lots of different options this tool provides. We're using
- 2463 "Open-AudIT Enterprise" This version allows for up to 20 nodes to be audited / monitored for free.

Opmantek Documentation and Community

NMIS8 Dashboard
opCharts - interactive Charts and Dashboards
opEvents - Event Management
opFlow - NetFlow Analysis
opConfig - Configuration and Compliance Management
opReports 3.0 - Network Reporting
Open-AudIT Enterprise

Open-AudIT V2 Dashboard
Open-AudIT Documentation and Community

2465

- 4. You'll now be prompted for login with username and password. This default information
 is provided above "username / password".
- 5. Once logged in we need to make some required changes to allow this produce to functionin our environment.
- 2470 6. Click on "Admin → LDAP Server → Create LDAP Servers" This will allow
- 2471 integration with Active Directory using LDAP authentication for logging into this
- 2472 application.

Licenses - Ad	min 👻	Help 🗕	<u> </u>	User: nr
Enterprise	•			
Community	►			
Collectors	►			
Database	►	lat Saa	n far	20
LDAP Servers		List LD	AP Sei	vers
Tasks	•	Create	LDAP	Servers
Logs	•			

2474 7. Required setting for LDAP server connection. Screen shot provide for 2475 reference.

Name	TestConnection	?
Description	Documentation	?
Organisation	Default Organisation •	?
Domain	LAN.LAB	?
Host	10.100.0.17	?
Port	389	?
Use Secure (LDAPS)	No 🗸	?
Version	3	?
Use LDAP for Roles	Yes	?
Туре	Active Directory	?
Base DN	CN=Users,DC=lan,DC=lab	?

2476 2477

2478

2480

2488

- a. Name TestConnection
- b. Description -- Documentation
- c. Domain LAN.LAB 2479
 - d. Host **10.100.0.17**
- 2481 e. Use LDAP Roles -- Yes (Additional configuration is required in AD Groups. See 2482 section below in this document for additional steps.
- 2483 f. Base DN – "cn=user,dc=lan,DC=lab"
- 2484 8. Click "Submit" once all information has been entered.

2485 **Active Directory Groups for LDAP Integration:**

- 1. Groups listed below are required for integration to work with Open-AudIT and 2486 Active Directory. 2487
 - a. Admin "open-audit_roles_admin"
- 2489 b. org_admin "open-audit_roles_org_admin"
- 2490 c. reporter "open-audit_roles_reporter"

d. user "open-audit roles user"

2491

2492

2493 2. Create each group listed within quotes in your Active Directory. Each group should be 2494 created with Group Scope (Global) Group Type (Security) 3. Once each group has been created and the appropriate users add you can now login with 2495 2496 your Active Directory credentials. **Discover Credentials and Discover Scans** 2497 1. From the home screen click on Discover >> Discoveries >> Create Credentials. 2498 Discover -Report -Manage -List Credentials Credentials Discoveries **Create Credentials** Ы 2499 2500 2. Now enter in the requested information. 2501 a. Name – Name of the Credentials being used. Example (SSH) 2502 b. Organization – Default Organization is selected. Pickup another if 2503 your configuring more the one organization. 2504 c. Description – Description of item being added. 2505 d. Type – Select which type of credentials will be used. (SNMP (v1 / v2), SNMP v3, SSH, SSH Key, or Windows) 2506 SNMP (v1 / v2) SNMP v3 SSH SSH Key Windows 2507 2508 e. Credentials – enter the appropriate credentials for the select type from above. 2509 f. Click submit to save this entry. 2510 **Discovered Scan:** 1. Click Discover button [] Discoveries [] Create Discoveries. 2511 Discover -Report -Manage -Credentials Þ Discoveries List Discoveries Create Discoveries Files 2512 2513 2. Name – The name for this scan which should be unique. 3. Subnet – The network discovery will be performed on. 2514 4. Click submit to save and return to main discovery screen. 2515 2516 5. Main discovery screen allows you to start a scan at any time. Scans can also be 2517 configured to run on a schedule interval. 2518 2519 2520 110

e. Default Organization "open-audit orgs default organisation"

2521 Useful information and links:

- Default password were not changed, so remember to change all default password before
 this is put into production. (THIS IS VERY IMPORTANT)
- 2525 this is put into production. (**THIS IS VERY INPORTANT**) 2524 2. Software Vendor webpage. \rightarrow https://opmantek.com
- 2525 3. Community forums. \rightarrow https://community.opmantek.com
- 252625264. Software is Open Source. Your able to use Professional Edition for up to 20 machines
- after that there is a cost which is relatively inexpensive.
- 2528 5. Comparison Chart

Both the community and enterprise products share a common code base, however, Open-AudIT Enterprise includes additional modules that improve discovery, simplify administration and increase reporting ability. Use the comparison chart below to decide which version best suits your organization's requirements.

	Community	Professional	Enterpris
Network Discovery	Yes	Yes	Yes
Device and Software Auditing (including Device Port and Storage Appliances)	Yes	Yes	Yes
Configuration Changes Detection and Reporting	Yes	Yes	Yes
Hardware Warranty Status	Yes	Yes	Yes
Inventory Management	Yes	Yes	Yes
Custom Fields	Yes	Yes	Yes
Interactive Dashboard		Yes	Yes
Geographical Maps		Yes	Yes
Devices Export		Yes	Yes
Scheduling – discovery and reporting		Yes	Yes
Enhanced Reports including Tine based, Historical and Multi Reporting		Yes	Yes
High Scale			Yes
High Availability			Yes
File Auditing			Yes
Baselines			Yes
Configurable Role Based Access Control including Active Directory and LDAP			Yes
Integration with agents and CMDB			Yes
Commercial Support		Yes	Yes

- 6. Ability to perform baseline scan on devices is provided by Enterprise edition. This could
- be very useful for determining changes over a period of time.

2535 Install Steps for Process Control

2536 Open-Audit Configuration steps within Process Control System once system has been2537 installed

2538 Initial Configuration:

• Login via web portal

• Navigate to \rightarrow Discovery \rightarrow Credentials \rightarrow Create Credentials

Discover 🗸	Report -	Manage -			
Credentials	5	List Credentials			
Discoveries	s 🕨	Create Credentials			

- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop down during credential creation and select the desired group these credentials will apply to.
- Our environment consists of mainly Windows machine, so Windows will be used for connection type.
- Now create a credential and select **Windows** for the type. Once completed click **Submit**.

ID		?
Name	PCS SCans	?
Organisation	Default Organisation -	?
Description	Perform Windows Scans	?
Туре	Windows -	?
Username	Open-AudIT@lan.lab	
Password	•••••	
Edited By	nmis	?
Edited Date	2018-09-26 14:33:24	?
	Submit	

2549

- 2550 **Organization Groups Creation:**
- Click on Manage \rightarrow Orgs \rightarrow Create Orgs

	Manage 🛩
	Applications
	Attributes > Baselines >
	Connections > Dashboards >
	Devices
	Fields Groups
	Licenses Locations
	Maps
	Networks Queries
	Orgs List Orgs Roles Create Orgs
	Summaries b Import Orgs from CSV
2552	Users / Widgets /
2553	• Now enter Name: Description: and click submit at the bottom of the page to save.
	Description Process Control Machines ?
	Parent ID Default Organisation • ?
2554	Type Organisation - ?
2555	• If you have multiple machines / equipment in different locations you can make
	• • • • •
2556	Organizational groups based on business units, or related task.
2557	Configure Discovery Scan:
2558	• Now click on Discover \rightarrow Discoveries \rightarrow Create Discoveries
	Discover - Report - Manage -
	Credentials
	Discoveries List Discoveries
2559	Files Create Discoveries
2560	Enter a magningful name for discover being created
2300	• Enter a meaningful name for discover being created
2561	Name PCS Scans ?
2561 2562	• Next, enter the subnet that'll be used for performing this scan. This scan is using
2563	172.16.0.0/22 ^{Subnet} 172.16.0.0/22 ? Search online for additional subnetting
2564	information / calculators if you'd like to learn more.
2565	• Network address: should already be defaulted to Open-AudIT installed location, if this
2566	is not true, click the drop-down arrow and select your installed location.
2300	
2567	• Now, click on the advanced button to see more options.
2568	• Once Advanced has been expaned you'll have additional options to select if desired.
2569	These options are Org, Type, Devices Assigned to Org, and Devices Assigned to
2570	Location. These options aren't required, but allow you to place found devices into
2571	different Organzations groups.
2572	• Once all selection have been made click on Submit button to continue.
2312	• Once an selection have been made ener on Submit button to continue.
2573	
-	
2574	

2575 **Discoveries:**

- Once the steps above have been completed clicking on **Submit** button you'll be taken to a new webpage that'll allow you to run discovery process created in the previous step.
- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.

		-					
	PCS Scans	Default Organisation	subnet	Subnet -	2000-01-01	×	1
				172 16 0 0/22	00.00.00		

- Once discovery has started you'll be taken to a new page allowing you to view status, or cancel if needed.
- Newly found devices are added to **My Devices** which is found on the home screen.
- 2585

2581

2586 Lesson Learned:

2587 Ensure default password are changed

Use Secure LDAP (LDAPS) If unable to use LDAPS make sure account being used for syncing
 groups has least privilege rights. (Not an Administrator and not a Domain Administrator)

2590 When configuring SNMP make sure to use SNMP V3 if possible

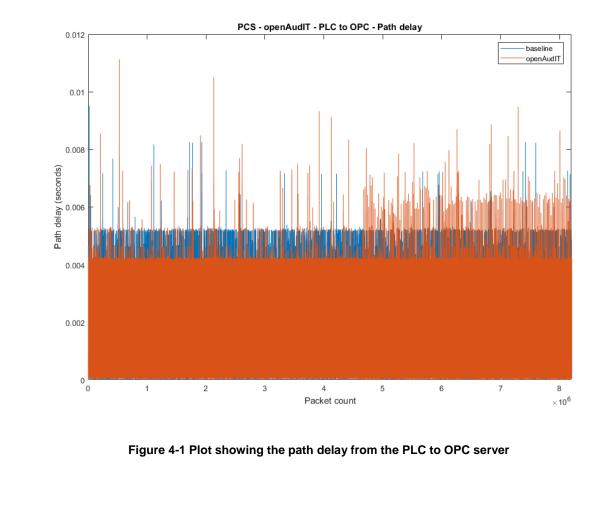
2591 **4.2.6** Highlighted Performance Impacts

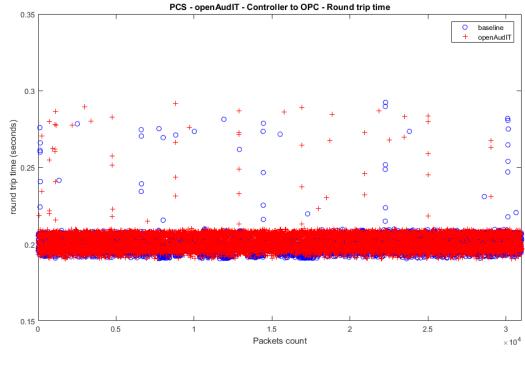
The following performance measurement experiment was performed for the Open-AudIT tool while the manufacturing system was operational:

2594 Experiment PL003.1- Open-AudIT asset inventory tool network scan and authenticated scan

A small performance impact to the network behavior was observed in the PCS system during the Open-AudIT scan. The network traffic was slightly increased in part of the PCS system during the scan. For example, the path delay from PLC to OPC was slightly higher especially in the latter part of the experience when Open-AudIT was performing the authenticated scan. However, the round trip time from the Controller to the OPC was mostly the same throughout the scan. It

appears that some part of the system has a more noticeable impact than the other parts.





2607

Figure 4-2 Plot of the packet round trip time from Controller to OPC

2608

A small impact to the manufacturing process was observed. The product flow of the

2610 manufacturing process was slightly higher than the optimal level. The reactor pressure was

slightly higher than the optimal level specially at the latter part of the experiment when Open-

2612 AudIT was performing the authenticated scan. However, the impact was small within the

tolerance of the system.

2614 It is hypothesized that the impacts were caused by increased network delays between the hosts of

the system. There is a time delay before the network impact will start impacting the

2616 manufacturing process due to the iterative nature of the process simulation and sensor and

actuator values exchange.

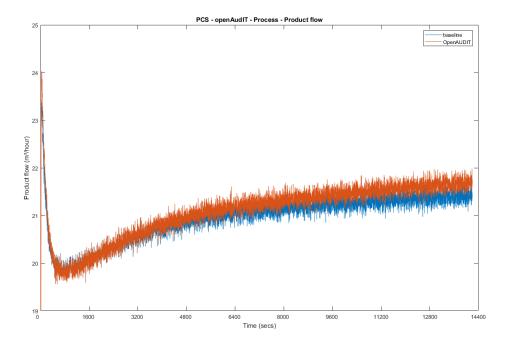
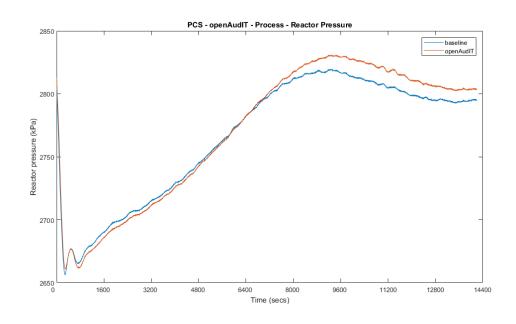






Figure 4-3 Plot of the production flow of the manufacturing process



2620 2621

- Figure 4-4 Plot of the reactor pressure of the manufacturing process
- 2622 **4.2.7** Link to Entire Performance Measurement Data Set
- 2623 Open-AudIT KPI data
- 2624 **Open-AudIT measurement data**

2625 **4.3 CSET**

2626 **4.3.1 Technical Solution Overview**

Cyber Security Evaluation Tool (CSET) is a tool provide by Department of Homeland Security
 for performing Cybersecurity evaluation against an organization. This evaluation is completely
 manual process of answering multiple questions to determine organizational security posture in
 regard to implemented current cybersecurity practices against current security status. This
 evaluation will help identify area within the organization that required more attention and
 resources.

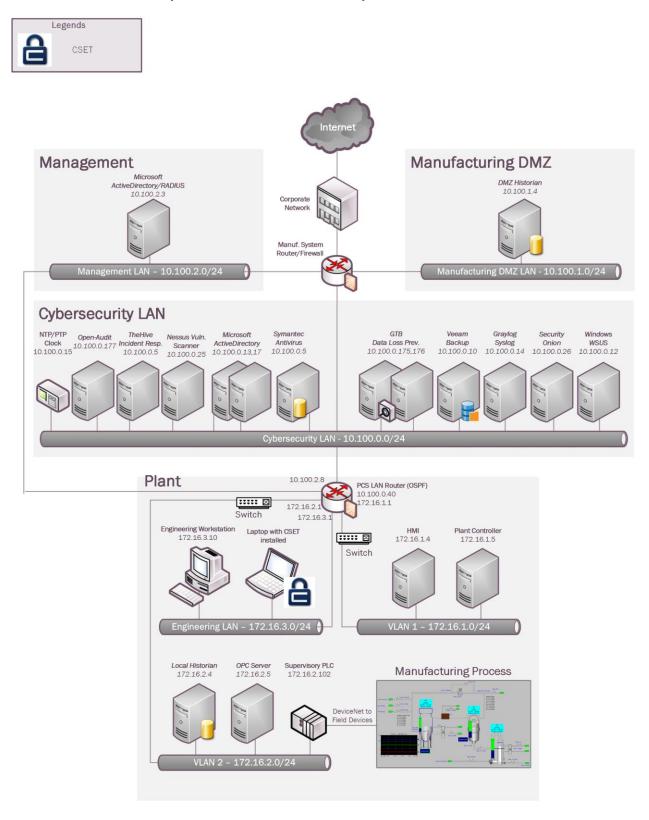
2633 **4.3.2** Technical Capabilities Provided by Solution

- 2634 CSET provides components of the following Technical Capabilities described in Section 6 of2635 Volume 1:
- Network Architecture Documentation
- Risk Assessment

2638 **4.3.3** Subcategories Addressed by Implementing Solution

2639 ID.RA-1

2640 **4.3.4** Architecture Map of Where Solution was Implemented



2642 **4.3.5** Installation Instructions and Configurations

2643 CSET Installation and Configuration

2644 **Download and Installation Instructions: Provided by DHS**

2645

2646 Download CSET using the link at the bottom of this page or by clicking <u>here</u>. After clicking the 2647 link, you will be asked to identify yourself and will then be given the opportunity to download 2648 the file *CSET_x.x.iso* (where x.x represents the download version).

The CSET download is in a file format known as "ISO." This file is an "image" of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

- Decompressing the File Open the file using any one of the newer compression utility software programs.
- 2654
 2. Mounting the File this method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
- Burning the file to CD this method uses CD-burn software and the ISO file to burn the
 files onto your own CD to create a physical disk identical to the CSET original.
- These methods require separate software utilities. There are a variety of both free and purchased utility programs available through the Internet that will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step by step instructions for each method are provided below:

2663 **Decompressing the File**

- CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
- 2666
 2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive)
 2667 maintaining the file name and extension (.iso).
- 2668
 3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
- 2670 4. COMPLETE the *Installing the CSET Program* instructions below.

2671 Mounting the File

- CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
- 2674
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675
 2675</l
- RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE
 the instructions within the utility software to create a virtual drive using the ISO file. If

- 2678 you do not have an ISO utility application, you will need to find and install one before 2679 continuing with these instructions.
- 2680 4. COMPLETE the *Installing the CSET Program* instructions below.

2681 Burning the file to CD

- CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
- 26842. SAVE the file to the hard drive on your computer maintaining the filename and extension (.iso).
- 2686 3. INSERT a blank, writable CD into the computer's CD drive.
- 2687
 4. RUN your CD-burn utility program. COMPLETE the instructions on your utility
 2688
 2689
 2690
 2690
 4. RUN your CD-burn utility program. COMPLETE the instructions on your utility
 2689
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 2690
 <li
- 2691 5. COMPLETE the *Installing CSET Program* instructions below.

2692 Installing the CSET Program

- FIND the CSET_Setup.exe file in the folder, virtual drive, or CD containing the CSET
 files.
- 2695
 2. DOUBLE-CLICK the CSET_Setup.exe file to execute. This will initiate the installer program.
- 2697 3. COMPLETE the instructions in the installation wizard to install the CSET program.
- 2698
 4. READ the material within the ReadMe document for a summary explanation of how to use the tool. Help is also available through the User Guide, screen guidance text,
- and video tutorials.

2701 Video Tutorials

- A number of video tutorials are available to help you better understand how to use this tool. They
- are designed to play within YouTube, therefore, you must have an active internet connection to
- view them. You can access these videos by navigating to the CSET YouTube channel (https://www.youtube.com/c/CSETCyberSecurityEvaluationTool)
- 2705 (https://www.youtube.com/c/CSETCyberSecurityEvaluationTool).
- 2706 To view close captioning in YouTube, click on the "cc" icon on the video window.

2707 System Requirements

- 2708 In order to execute CSET, the following minimum system hardware and software is required:
- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- CD-ROM drive if creating a physical CD
- 5 GB free disk space
- 3 GB of RAM

- Microsoft Windows 7* or higher
- A Microsoft Office compatible (.docx) document reader is required to view reports in .docx format
- A Portable Document Format (PDF) reader such as Adobe Reader is required to view supporting documentation. The latest free version of Adobe Reader may be downloaded from <u>http://get.adobe.com/reader/</u>
- Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)
- 2721 **NOTE:** For all platforms, we recommend that you upgrade to the latest Windows Service Pack
- and install critical updates available from the Windows Update website to ensure the bestcompatibility and security.
- 2724 CSET Hash Values
- 2725 SHA-256:
- 2726 B7061B169E3461A298E58B99FADC9978D9F6CE22A0747669A538BDAF39C214ED
- 2727 MD5: 53f2f71eb6e3bb54471e75318eaa64ee
- 2728 SHA-1: f2b020e3a73db9b72ff85bd9b5e158449f6c003a
- 2729 To download CSET, select the following link:
- 2730 **Download CSET**
- 2731 If you are unable to download or install CSET from the link, you may request a copy be shipped.
- To request a copy, please send an email to: <u>cset@hq.dhs.gov</u>. Please insert "CSET" in the subject line and include the following in your email request:
- Your name
- Organization name
- Complete street address (no P.O. boxes)
- Telephone number
- The error or installation issue you encountered when attempting the download
- 2739
- 2740 **Running CSET for First time:**
- Once install of CSET has been completed find the application just installed and double
 click to run. Concentration
- 2743 2. Once program has launched you will see the home screen.
- 2744 3. Click on File and select "New Assetment" New Assessment Ctrl+N

- 4. Now, click on Start Here button in the lower right corner of program. Start Here \gg
- 5. Next, enter all required information

Assessment Name		Assessment Date	
Process Control		4/22/2019	贷
Facility Name			
Westman Chemical Company			
City or Site Name			
Gaithersburg			
State, Province, or Region			
Maryland			
Assessor Name	Assessor Email	Assessor Telephor	10
John Doe			10

2748 6. Click continue to proceed.

2747

27497. Now click on drop down menu and select the appropriate choices. Change any highlight2750 options required.

Sector		
Chemical Sector (Not Oil and Gas)	•	
Industry		
Other	•	
What is the gross value of the	e assets you are trying to protect?	
< \$1,000,000	▼	
What is the relative expected	effort for this assessment?	
Small (1-2 hours)		
V Privacy is a significant conce	rn for the assets I am trying to protect.	
My organization is concerne	d with the cybersecurity integrity of our procureme	ent supply chain.
🗹 My organization uses 🏟	rial control systems (ICS).	

- 2751✓ My organization uses ithjustrial control system27528. Click continue to proceed.
- 9. If you want to create a network diagram click the button, otherwise click "**Continue**".
- 2754 10. Change Mode Selection to "Advanced" and "Cybersecurity Frame-based Approach"
 - O Basic Generate a basic assessment using the provided demographic information

Advanced - Let me choose which cybersecurity standard(s) the assessment will be based on:

efore	sel	ecting which cybersecurity standards your assessment is based on, please choose one of the following options.
	0	Questions-based Approach The questions-based approach uses simple questions and allows for partial credit.
	0	Requirements-based Approach
		The requirements-based approach uses the exact wording of the standard and is best for those industries that are regulated by a specific standard.
	0	Cybersecurity Framework-based Approach
		The cybersecurity framework-based approach uses allows you to define a custom profile based on the Cybersecurity Framework.

2756 11. Click continue.

2755

- 2757 12. Click continue to use default profile or create a new profile.
- 2758 13. Click continue again.
- 14. Now answer the questions as they appear.
- 2760 15. Complete all questions and generate a final report.

2761 Lessons Learned:

• The tool is only as good as information entered. Make sure each answer is thought out before answering.

- Mark any answer for review as needed so there will be follow up.
- When completed your organization will receive a 0 to 100 score depending on readiness. 2766

2767 **4.3.6 Highlighted Performance Impacts**

- 2768 No performance measurement experiments were performed for CSET due to its typical
- installation location (i.e., external to the manufacturing system).

2770 **4.3.7** Link to Entire Performance Measurement Data Set

- 2771 N/A
- 2772

2773 **4.4 GRASSMARLIN**

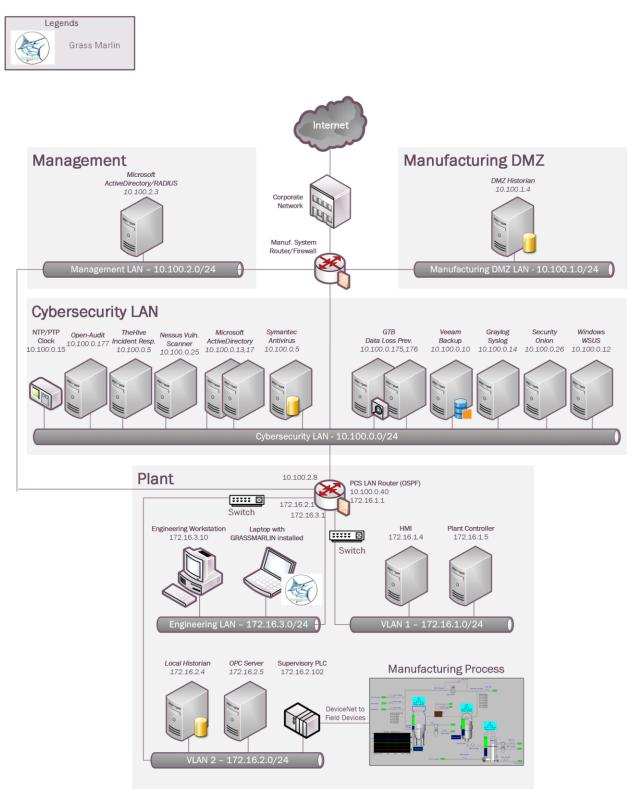
2774 **4.4.1 Technical Solution Overview**

GRASSMARLIN is an open source, passive network mapper dedicated to industrial networks
and developed by the National Security Agency (NSA). GRASSMARLIN gives a snapshot of
the industrial system including:

- Devices on the network
- Communications between these devices
- Metadata extracted from these communications
- 2781 Points to consider:¹²
- Passive IP network mapping tool
- Hardware agnostic portable Java based tool
- Can only see and map hosts where you are capturing data from.
- 2785 **4.4.2** Technical Capabilities Provided by Solution
- GRASSMARLIN provides components of the following Technical Capabilities described inSection 6 of Volume 1:
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- **4.4.3** Subcategories Addressed by Implementing Solution
- 2792 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.CM-7

¹² GRASSMARLIN Briefing Powerpoint 2017: <u>https://github.com/nsacyber/GRASSMARLIN /blob/master/GRASSMARLIN /blob/mas</u>





4.4.5 Installation Instructions and Configurations 2795

2796 Details of the solution implemented:

	Name	Version	
	GRASSMARLIN	3.2.1	
7	Setup		1
)) 2 3 4 5 5 5 7 7 3))	 GRASSMARLIN is supported on the fermi Microsoft Windows (64bit, 7 8 and 10) Fedora Linux Ubuntu (14.04 ,15.10) Kali Linux 2.0 CentOS (6,7) Debian (8) Download GRASSMARLIN from http://per the OS version of your system. Upor additional programs such as Java and V GRASSMARLIN can operate in a real importing a recorded pcap file. Data in contains imported files and visual state A temporary Windows 10 laptop would required with GRASSMARLIN installed 	s://github.com/ns on download, run Vireshark during time passive moo GRASSMARLIN information. I be setup in the I	acyber/GRASSMARLIN/releases as the installer. The installer will install the setup. le by sniffing the live traffic or by N is stored in a Session. The Session
ļ	Using the Software:		
5 7 3 9	 A captured pcap file from the system we network baseline. The pcap was capture system which had a network connection Aggregator was configured with mirror network segments such as Supervisory 	ed by the running n from a Network port connections LAN and Contro	the tcpdump command on a Linux aggregator device. This in coming from the different
2	tcpdump -i <mirror-port interface=""> -w</mirror-port>	турсар.рсар	
	For example : tcpdump -i eth1 -w /hor Where eth1 is our mirror port connection		р
	• To run GRASSMARLIN on a Window click on the "GRASSMARLIN" shortc	•	

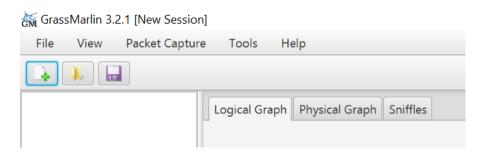
¹³ GRASSMARLIN User Guide: <u>https://github.com/nsacyber/GRASSMARLIN</u>

2828 Linux system without a Desktop, type the command "GRASSMARLIN" or "sudo 2829 GRASSMARLIN" and the interface should load up.

2830

2833

• To Import a pcap in GRASSMARLIN, click on the **Import** icon in the toolbar (or select **Import files** from the File Menu)



2834 • Click on Add Files. Browse to the PCAP

	Pending Imports					👻 🔍 Start 📓 St
	File Name		Size Typ	Timesta	·	
				16:37:37.284	Unable to load user Fingerprints	
				16:37:37.177	Unable to load manufacturer database	
				16:37:37.263	Unable to initialize JNetPCap; packet c	
				16:37:37.179	Unable to create application directorie	
				16:37:36.613	This session cannot be logged to disk:	
				16:37:37.093	Loading Geold -> Name Mapping fron	
		No content in table			Loading Cidr -> Geold Mapping from:	
					Loaded plugin 'iadgov.svgexport'	
				16:37:37.949	Loaded plugin 'iadgov.offlinepcap'	
				16:37:37.094	Geold -> Name Mapping load comple	
				16:37:37.088	Cidr -> Geold Mapping load complete	
				16:37:37.263	Cannot locate Wiresharl; please verify	
Timesta▼	Add Files Load Quickli	Save Quicklis	t Import Selecte	d <	>	
6:37:37.284 Unable to load user Fingerprints	Running and Completed Im	ports				
6:37:37.177 Unable to load manufacturer database fro	om Wireshar Progress	File	Size			
6:37:37.263 Unable to initialize JNetPCap; packet capt	ture function	THE	SIL			
6:37:37.179 Unable to create application directories: 0	C\Program F					
5:37:36.613 This session cannot be logged to disk: C/	Program File					
6:37:37.093 Loading Geold -> Name Mapping from: 0	C:\Program F		No content in tak	le		
6:37:36.627 Loading Cidr -> Geold Mapping from: C:	Program File					
20 MAD / AS MAD						

2835

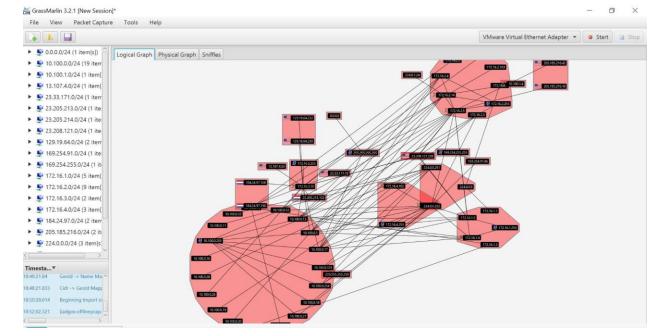
The Pcap will now show up under Pending Imports. Select the file and click on "Import
 Selected". Hit the Close button upon completion to back to the Main interface. The Import
 process can take several minutes to hours depending on the size of the pcap file.

Import

cap	16:37:37.284 16:37:37.177 16:37:37.263 16:37:37.179 16:37:36.613	Unable to load user Fingerprints Unable to load manufacturer database Unable to initialize JNetPCap; packet o Unable to create application directorie
	16:37:37.263 16:37:37.179	Unable to initialize JNetPCap; packet o Unable to create application directorie
	16:37:37.179	Unable to create application directorie
	and the second second	
	16:37:36.613	
		This session cannot be logged to disk:
	16:37:37.093	Loading Geold -> Name Mapping from
	16:37:36.627	Loading Cidr -> Geold Mapping from:
	16:37:37.95	Loaded plugin 'iadgov.svgexport'
	16:37:37.949	Loaded plugin 'iadgov.offlinepcap'
	16:37:37.094	Geold -> Name Mapping load comple
	16:37:37.088	Cidr -> Geold Mapping load complete
	16:37:37.263	Cannot locate Wireshark; please verify
	Selected	16:37:37.95 16:37:37.949 16:37:37.094 16:37:37.088 16:37:37.263

2839

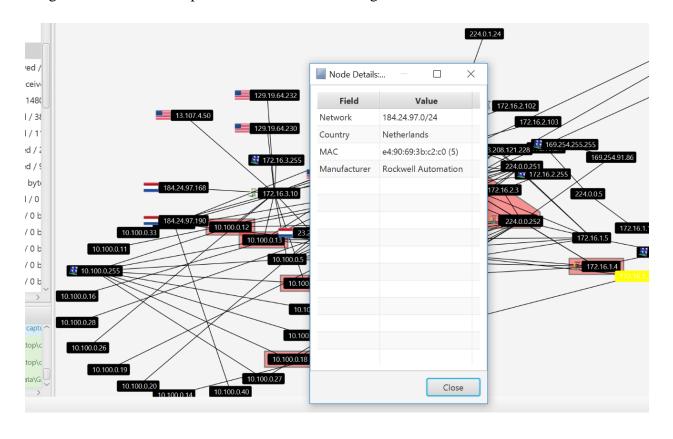
Upon the completion of Import, the main screen will display a Logical Graph of the network
 topology as shown below.



- Take a moment to review the logical graph. The public IP addresses will also be highlighted with their respective Country's flag. This can be useful in finding out information about any external IP's that your network is communicating with.
- 2846

Right-click on any external IP address in question >> View Details. For instance, the below image shows a host with ip172.16.3.10 communicating with an IP address from Netherlands.

2849



2850 2851

- To Generate a list of all nodes in the Logical Graph, click on View (Top Menu) >> Logical
 Nodes Report. By default, only a single column (IP) is present, although additional columns
 can be added with any Property present in the set of Nodes.
- 2856 To add a column, select the Property Name from the drop-down and click the Add button.

 Destination Source and 	Destination			Add Browser Protocol.Domain/Workgroup
IP	ICSProtocol	EtherNetIP.ICSProtocol	Service	Browser Protocol.MicrosoftProtocol
			Authentication File Replication Service	Domain Controller.Role
72.16.3.10	Allen Bradley Rockwell PLC Allen Bradley Rockwell PLC ETHERNETIP	(-/	LDAP Authentication File Replication Service	Domain Controller.Service Operating System.OS Role
72.16.2.102	ETHERNETIP	ETHERNETIP (5)		Windows Version
72.16.2.4			LDAP Authentication	os
72.16.4.5	Allen Bradley Rockwell PLC Allen Bradley Rockwell PLC ETHERNETIP	ETHERNETIP (5)	File Replication Service	Domain/Workgroup MicrosoftProtocol
72.16.4.102	ETHERNETIP	ETHERNETIP (5)		
72.16.1.4			LDAP Authentication File Replication Service	
72.16.2.14			LDAP Authentication	

- To Generate a Report of all connections in the pcap file, click on View (Top Menu)>>
- 2859 Logical Connections Report

2860

File	View		ket Ca		То	0.0	Help		
*	Cur								
- 81	💁 1 📕 Logical Nodes Report						Logical Graph		
▶ 10	 10. Logical Connections Report 10. Inter-Group Connections Report 								
▶ 10									
, ¥ 1	New Filtered Logical View								
S 1	92.108.1	1.0/24	(8 iter	n[s])		1			

- This will generate an output similar to below shown image. Click on **Export CSV** for further analysis of all the communications happening on your network.
- 2865

			Export CS	V	
Source	Destination	Bytes Sent	Bytes Received		
172.16.1.5	172.16.2.5	64545600	5062420		â
172.16.3.10	172.16.2.102	28147182	45873018		
172.16.2.4	172.16.3.10	1280520	0		U
172.16.4.5	172.16.4.102	3000132	9207080		
172.16.1.4	172.16.2.5	2157735	12923885		
172.16.2.5	172.16.2.14	5872436	864720		
172.16.2.4	172.16.2.5	852840	0		
0.0.0	255.255.255.255	171021	0		
172.16.2.103	10.100.0.15	200160	0		
10.100.1.4	172.16.2.14	138504	1056789		
172.16.2.1	224.0.0.5	818100	0		
172.16.1.1	224.0.0.5	408780	0		
172.16.1.5	10.100.0.5	96711	153960		
172.16.2.5	255.255.255.255	94920	0		
172.16.1.4	172.16.1.255	78488	0		
172 16 2 14	255 255 255 255	104440	0		~

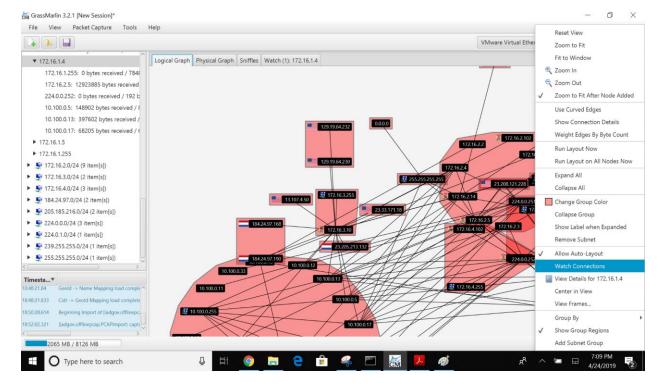
To view all the logical communications for a specific host for capturing a baseline, under the left-side explorer right-click on a Node >> View Frames. This opens a new screen as shown below displaying all the different IP addresses that particular host is communicating with including Port and Protocol information. You may click further on "Export CSV"
 button to export this data to a csv file.

2873 2874

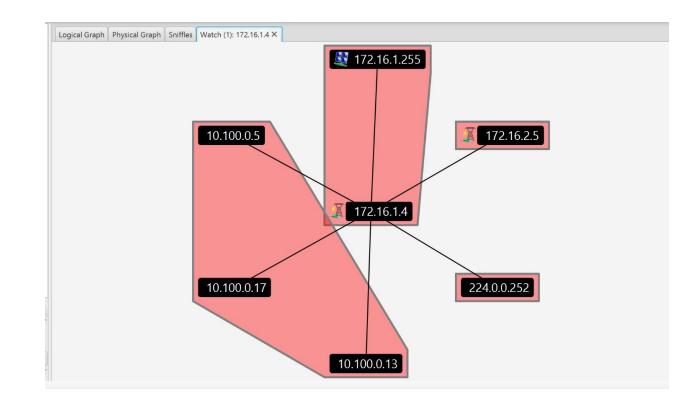
Note: This process needs to be repeated for every node.

🖌 👠 📊	K Connections involving 172	.16.1.3						
♥ 0.0.0.0/24 (1 item[s])								Export CSV
➡ 10.100.0.0/24 (19 item[s])	Timestamp	Source IP	Source Port	Destination IP	Destination Port	PCAP File	Frame	Protocol
▲ 10.100.1.0/24 (1 item[s])	2019-03-22T14:35:44.440Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	81395	UDP
₩ 13.107.4.0/24 (1 item[s])	2019-03-22T14:35:44.440Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	81396	UDP
§ 23.33.171.0/24 (1 item[s])	2019-03-22T14:36:49.445Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	90784	UDP
§ 23.205.213.0/24 (1 item[s])	2019-03-22T14:36:49.445Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	90785	UDP
🐓 23.205.214.0/24 (1 item[s])	2019-03-22T14:37:54.449Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	100249	UDP
🐓 23.208.121.0/24 (1 item[s])	2019-03-22T14:37:54.449Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	100250	UDP
🐓 129.19.64.0/24 (2 item[s])	2019-03-22T14:55:01.459Z	172.16.1.3	123	10.100.0.15	123	capture.pcap	248453	UDP
 169.254.91.0/24 (1 item[s]) 169.254.255.0/24 (1 item[s]) 172.16.1.0/24 (5 item[s]) 172.16.1.1 224.00.5: 0 bytes received / 408780 172.16.1.3 10.100.0.14: 0 bytes received / 408780 172.16.1.4 10.100.0.15: 0 bytes received / 3456 172.16.1.4 > 	010.100.0.15 010.100.0.15 168 112 56 0 30.100 ¹ 109 ¹ 109 ¹ 109 ¹ 20		019-03-22716.	19-03-221516:30'	0022 2019-03-2 2019-03-2	2019-03-22	-••	و بل Close

• Another interesting feature is Watch-Graphs. A Watch Graph is a subset of Logical graph, created for a particular node and shows all the different nodes connected to it. This can be generated using **Watch-connections** menu. Right-click a node >> select **Watch Connections**. This will generate a graph in a new window "**Watch <IP address**>"







- 2886
- 2887

2888 **4.4.6** Highlighted Performance Impacts

2889 No performance measurement experiments were performed for the use of GRASSMARLIN due 2890 to its installation location and how it was used (i.e., the software performed offline analysis of

2891 PCAP files captured by other software).

2892 **4.4.7** Link to Entire Performance Measurement Data Set

2893 N/A

2895 **4.5** Wireshark

2896 **4.5.1 Technical Solution Overview**

Wireshark is a free and open-source packet analyzer. It is user friendly, simple to implement, just
need to ensure network connection plugged in is configured to display traffic correctly i.e. Port
mirroring.

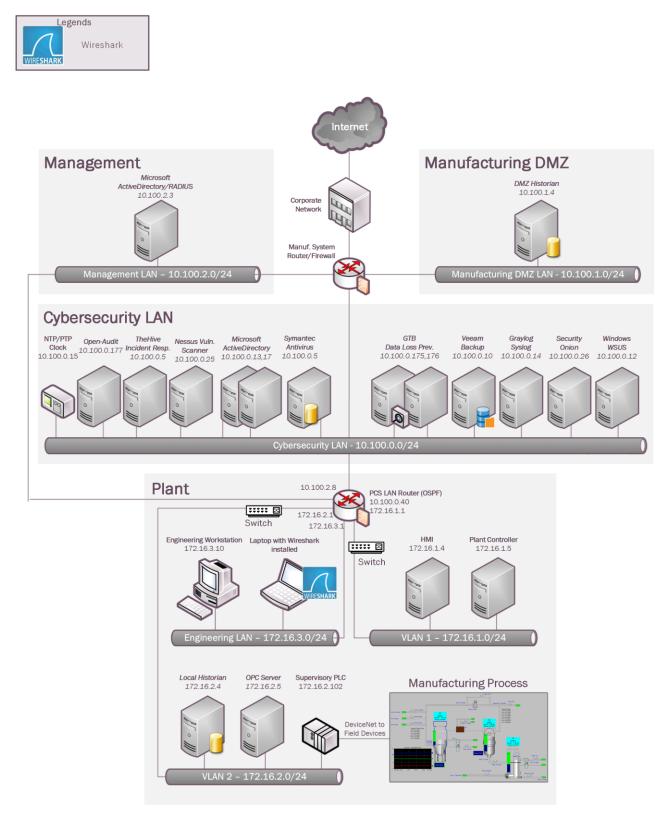
2901 **4.5.2** Technical Capabilities Provided by Solution

- Wireshark provides components of the following Technical Capabilities described in Section 6of Volume 1:
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- Forensics

2908 **4.5.3** Subcategories Addressed by Implementing Solution

- 2909 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.AE-2,
- 2910 DE.CM-7, RS.AN-3
- 2911

2912 **4.5.4** Architecture Map of Where Solution was Implemented



2914 **4.5.5** Installation Instructions and Configurations

2915 Steps for installing Wireshark

2916 **Download and Installation instructions:**

- 1. Only download Wireshark from https://www.wireshark.org (Select 32bit or 64 bit)
- 2918 2. Once download has completed locate the executable just downloaded and double click to 2919 start install process. C:\Users\johndoe\Downloads\Wireshark-win64-3.0.1.exe
- 2920 3. If prompted for password enter administrator account on local machine.
- 2921 4. When first Screen appears click "**NEXT**"

🚄 Wireshark 3.0.1 64-bit Setup	×
	Welcome to Wireshark 3.0.1 64-bit Setup
	This wizard will guide you through the installation of Wireshark.
	Before starting the installation, make sure Wireshark is not running.
	Click 'Next' to continue.
51	5
	Next > Cancel

2922

- 2923 5. Click "Agree" to continue.
- 2924
 6. Leave default selected and click "Next" five times to continue install. (Make changes if
 all features aren't required. This will be uncommon)
- 2926 7. When prompted for Npcap install click "I Agree" to continue.
- 2927 8. Leave default and click "Install".
- 2928 9. Now click "**Next and Finish**" to start process.
- 2929 10. Click next and then select "Reboot Now" or "I want to manually reboot later"
- 2930 11. Click "Finish" to complete.
- 2931

2932 Running Wireshark and configure

- 2933 1. Click start button and find program labeled "Wireshark".
- 2934 2. Once Wireshark is found right click on icon and select More→Run as Administrator
- (Windows 10) Older operating system can just hold down "Shift + Right Click" menu
 will appear for run as, select administrator to continue.
- 29373. Wireshark requires administrative privileges to be fully functional, otherwise there will2938 be undesired results.

2939 4. Once Wireshark is running the initial interface will appear that the screen shot provided.

File Edit View	w Go Capture Analyze Statistics Telephony Wireless Tools Help	
🖌 🔳 🎊 🛞	📕 🖹 🗴 🕼 🗰 🎬 🖉 🗶 🜉 🜉 🔍 Q, Q, II	
Apply a display fil		
	Welcome to Wireshark	
	Capture	
	using this filter: 📕 Enter a capture filter	✓ All interfaces shown ▼
	Npcap Loopback Adapter	
	Ethernet 3 A	
	Local Area Connection* 10 Ethernet	
	Wi-Fi	
	Local Area Connection* 7	
	Local Area Connection* 6 Local Area Connection* 8	
	Ethernet 4	
	Learn	
	User's Guide Wiki Questions and Answers Mailing Lists	
	You are running Wireshark 3.0.1 (v3.0.1-0-gea351cd8). You receive automatic updates.	
		No Packets
Ready to load		

5. Select the interface to be monitored.

2940

2942 Wireshark provide lots of information and can be hard to decipher <u>https://www.wireshark.org</u> 2943 provides documentation along with searches for additional command syntax.

2944 Capturing Network Baseline using Wireshark

- Launch Wireshark. Click **Open** to load a previously captured pcap file or run a "**Start Capture**" as explained in the previous section to record traffic.
- 2947 2. Upon loading the pcap or capturing live traffic; click on **Statistics** >> **Conversations**
- This will generate a window similar to the one below which will list all the different
 types of communications happening between all endpoints in your traffic. Click COPY
- 2950 >> **as Csv** to save this data as a Csv file for further analysis.

CSF MFG PROFILE LOW SEC LVL EXAMPLE IG PROCESS-BASED MFG SYSTEM USE CASE

Ethernet · 95	IPv4 · 75	IPv6 • 22	TCP	• 853 UDP	• 670							
Address A	Address B	Packets	Bytes	Packets A \rightarrow I	B Bytes A → B	$Packets \; B \to A$	Bytes $B \to A$	Rel Start	Duration	$Bits/s\:A\toB$	Bits/s B \rightarrow A	A ^
10.100.0.16	224.0.0.251	2	174		2 174	4 0	0	0109.13388	3600.1009	0		0
10.100.0.17	172.16.1.4	342	33 k	1	71 17	c 171	16 k	9235.241245	5111.8544	27		25
10.100.0.17	172.16.3.10	349	81 k	10	53 34 1	c 186	47 k	9341.621642	4829.8745	57		77
10.100.0.17	172.16.2.4	1,097	305 k	4			181 k	9360.223089	4796.3020	206		303
10.100.0.17	10.100.0.255	74	9571		74 9571		0	9391.429714	4801.4406	15		0
10.100.0.17	224.0.0.252	4	264		4 264		-	9475.946375	3600.5112	0		0
10.100.0.17	172.16.2.14	1,106	332 k	5				9529.909699		214		366
10.100.0.17	172.16.2.5	2,534	298 k	1,2				9656.383446	4381.4873	311		234
10.100.0.17	172.16.2.3	688	203 k		95 78			9773.279386		139		221
10.100.0.17	172.16.1.5	228	45 k		02 18			0868.02465	1285.4367	114		170
10.100.0.18	10.100.0.255	13	2456		13 2456		-	9272.279839		4		0
10.100.0.18	224.0.0.252	4	264		4 264		-	9272.280802		0		0
10.100.0.19	224.0.0.251	1	87		1 87	-	-	1365.30458		_		-
10.100.0.27	10.100.0.255	114	10 k	1				9271.772421		16		0
10.100.0.27	224.0.0.252	2	132		2 132			1061.46345		2572		0
10.100.0.28	224.0.0.251	1	87		1 87	-		1828.86474		_		-
10.100.0.33	224.0.0.251	1	81		1 81		-	1229.03123		-		-
10.100.0.101	224.0.0.252	47	3248		47 3248		-	2215.07204		15		0
10.100.0.101	239.255.255.250	77	16 k		77 16		-	2215.69742		61		0
10.100.0.101	224.0.0.251	6	492		6 492		-	2219.20341		1308		0
10.100.0.101	10.100.0.255	116	13 k		16 13 1		•	2223.70201		55		0
10.100.0.234	239.255.255.250		62 k	3				9213.476484		96		0
10.100.0.234	224.0.0.252	6	394		6 394			0471.43449		0		0
10.100.0.234	10.100.0.255	6	552		6 552		-	0591.45248		1		0
10.100.1.4	172.16.2.14	9,390	638 k	6,2				9213.771229		626		357
23.205.214.21	172.16.3.10	39	2522		0 () 39	2522	2536.51692	1523.2062	0		13 🗸
Name resoluti	ion 🗌 I	Limit to displa	ay filter	A	solute start time						[Conversation Types 🔻
						Copy	y 🔻 Fo	llow Stream	Gra	aph	Close	Help
172.16.2.10	2				172.16.3.1	0 as	CSV				555 [TCF	Retransmissio
72.16.2.5					172.16.1.4						60 6522	

2951

2952 2953 2954

2955

4. To get a list of ports used, Click on Statistics >> IPv4 Statistics >> Destination and Ports. This will generate a list of ports used by all the IP addresses in the traffic. Click Copy, to copy the results to a word document or click Save as to save as a plain text file. Hit Close when done.

opic / Ite	m	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start		
	VDP	244				0.0000	100.00%	0.0100	577.838		1
	138	16				0.0000	6.56%	0.0100	577.838		
	137	228				0.0000	93.44%	0.0100	646.796		
× 1	72.16.3.10	280703				0.0195	17.75%	0.4400	5542.363		
	> UDP	108				0.0000	0.04%	0.0200	655.814		
	> TCP	259177				0.0180	92.33%	0.4400	5542.363		
	NONE	21418				0.0015	7.63%	0.0600	718.162		
	0	21418				0.0015	100.00%	0.0600	718.162		
> 1	72.16.2.5	420916				0.0292	26.61%	2.3600	8443.682		
× 1	72.16.2.4	42194				0.0029	2.67%	0.7000	4838.174		
	> UDP	84				0.0000	0.20%	0.0600	4838.074		
	TCP	6554				0.0005	15.53%	0.6700	4838.174		
	54702	27				0.0000	0.41%	0.2100	14141.953		
	54701	27				0.0000	0.41%	0.2100	13241.934		
	54700	42				0.0000	0.64%	0.2100	12821.873		
	54699	30				0.0000	0.46%	0.2100	12341.911		
	54698	30				0.0000	0.46%	0.2100	11441.890		
	54697	21				0.0000	0.32%	0.2100	11084.048		
	54696	21				0.0000	0.32%	0.1500	11084.039		
	54695	15				0.0000	0.23%	0.0900	11083.531		
play filter:	Enter a display fi	iter								Apply	

2957 4.5.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Wireshark tool 2958 2959 while the manufacturing system was operational:

2960 Experiment PL015.2-wireshark

2961 Significant performance impact on computing resources was observed when using Wireshark for

2962 network traffic capture. Both the processor and memory utilization of the host were significantly 2963 higher than normal. There was no performance impact to the manufacturing process observed.

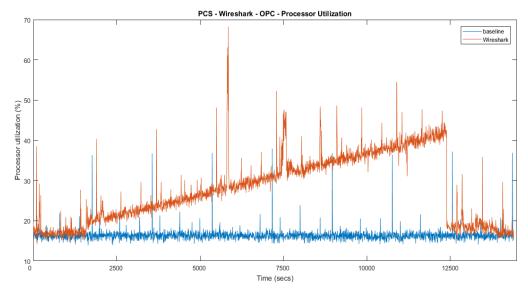
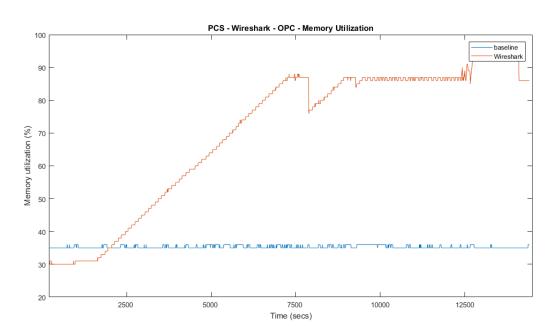


Figure 4-5 Processor utilization of the OPC computer during Wireshark network capture



2964 2965

Figure 4-6 Memory utilization of the OPC computer during Wireshark network capture

Wireshark started at around 1900 seconds experiment time and continued to capture network traffic for about 3 hours. During this period of time, the processor utilization of the OPC

2970 computer kept going up. Wireshark has a sizeable impact to the processor utilization. The

2971 Wireshark data file was about 2.3GB in this case.

2972 The memory utilization has a similar impact to the processor utilization, except the memory

- 2973 utilization stayed high after Wireshark has stopped capturing the network traffic. It is
- 2974 hypothesized that Wireshark stored the captured data in memory until the data was saved into the

- 2975 hard drive. Therefore, the memory utilization stayed high even after the Wireshark has stopped
- 2976 the network capture. Even though the processor and memory utilization were significantly
- higher, they were still below the full capability of the computer and therefore did not have major
- impact to the manufacturing process. However, for the manufacturing system that has a high utilization in normal run time, the use of Wireshark may cause a performance impact.
- 2980 The PCS system uses an external computer to use Wireshark to perform network traffic capture 2981 for this reason. Care should be taken if using Wireshark on a production system.

2982 **4.5.7** Link to Entire Performance Measurement Data Set

- 2983 Wireshark KPI data
- 2984 Wireshark measurement data
- 2985
- 2986

2987 **4.6 Veeam Backup and Replication**

2988 4.6.1 Technical Solution Overview

Veeam Backup and Replication is a proprietary backup and incident recovery software
developed by Veeam for virtual environments. It is built on VMware vSphere and Microsoft
Hyper-V hypervisors. The software provides backup, restore and replication functionality for
virtual machines. Veeam® Backup and Replication suite delivers availability for all workloads virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V) -from a single
management console. It provides fast, flexible and reliable recovery of your applications and
data, and brings backup and replication together into a single software solution [1].

The Veeam Backup Free Edition lets you back up your VMs on the fly and provides you with flexible storage options, including file-based (NFS) primary storage, for easy archiving and quick recovery. Veeam also has products such as "Veeam agent for Windows" and "Veeam agent for Linux" for backing up physical Windows and Linux servers respectively.

- 3000 Points to consider:
- Free backup edition available for virtual and physical servers.
- Support for file level backups as well as system image type of backups.
- Backups can be run without having to shut down the system. This can be very critical in
 ICS/SCADA environments.
- Tech support available for Free edition users.
- Easy to setup and use. Lot of documentation available online to get started.

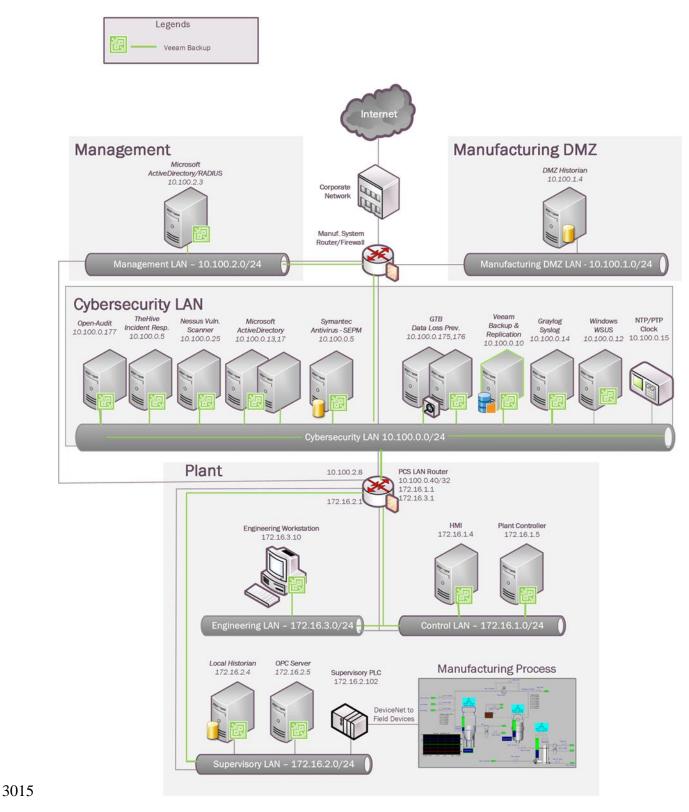
3007 **4.6.2** Technical Capabilities Provided by Solution

3008 Veeam Backup and Replication provides components of the following Technical Capabilities3009 described in Section 6 of Volume 1:

- 3010 Data Backup
- Data Replication

3012 **4.6.3** Subcategories Addressed by Implementing Solution

3013 PR.IP-4



3014 **4.6.4** Architecture Map of Where Solution was Implemented

(Free version)

3016 **4.6.5** Installation Instructions and Configurations

3017 <u>Setup</u>

- The following products from Veeam were implemented
- 3019

	-	
Name	Purpose	Version
Veeam Backup and	Veeam Backup Server and Repository	9.5
Replication		
Veeam Agent for Windows	For backup/recovery of Physical	3.0.0.748

Windows Systems in Process Control

- 3020
- A Windows 2012 Virtual Machine was setup in the Cybersecurity LAN for installing
 Veeam Backup and Replication Server. Around 4TB of storage was allocated to this VM
 for backup storage.

Network

- The Free Edition of Veeam Backup and Replication lets you manage virtual machine
 backups from the Central Veeam Backup and Replication Console. However, any physical
 servers configured for backup using the Veeam agent cannot be managed from the Central
 console in the Free edition. These need to be managed locally on the endpoint or client
 system itself.
- A parent folder called "backups" was created on the 4TB storage drive for saving the
 backups. Within this folder, different sub folders were created as per the Server names of
 Process Control System. Each system's backup was configured to save its data into its
 corresponding server name folder. The backups folder was then configured as a network
 share.
- A service account named "veeamuser" was created in Active Directory (Cybersecurity
 LAN) for backup and recovery purposes. This user was granted Read/Write permissions on
 the above share.

3037 Backups

- All Windows systems of Process Control Network were configured for Backup using
 Veeam Agent for Microsoft Windows [2].
- The Veeam agent was installed on all Windows clients (systems). Connectivity between
 each client and the Veeam Server was verified by accessing the "backups" share folder
 (created in the above section) from each client.
- In the Free version, a backup or restore operation needs to be initiated from the client
 system. Once the agent is installed on the client system, double click the "Veeam backup
 icon" in the System tray to launch the wizard.

Backup	•		
Restore	•		
Control Panel			
Exit			4:42 PM
	-	🐼 🐠 🄽 🖽	4/11/2019

304c

3052

3054

3055

- If this is your first time, the setup wizard will prompt to create a "Recovery Media" which is
 required for Bare metal backup and restore operations. It is recommended to create this
 Media if your backup mode is a Full Computer image.
- 3053 This media creation wizard can also be launched manually by running
 - Veeam.Endpoint.RecoveryMedia.exe program under C:\Program Files\Veeam\Endpoint Backup directory. Once launched, select one of the 3 options under Available Bootable Media Types as per your requirement
- 3056 3057

Recovery M Specify bare	ledia metal recovery media options			
Recovery Media	Available bootable m	edia types:		0
mage Path	Name	Туре	Capacity	
Ready to Apply	D:\	DVD RW Drive (D:) SST_DN	<unknown></unknown>	
ready to Apply		Removable Disk (E:)	1.9 GB	
Progress	Image	ISO image file		
	Include hardware	onnections settings from this computer drivers from this computer (recommend ing additional storage and network hard	ded)	Add
				Remove
		< Previous	lext > Finish	Cancel

3058 3059 3060

• If ISO option is selected, enter the name and location to save the ISO.

Create Recovery Media Image Path Specify when	
Recovery Media Image Path	ISO file name and location: C:\Users\Administrator\Documents\VeeamRecoveryMedia_FGS-47631EHH.iso Browse.
Ready to Apply Progress	This share requires access credentials: Username: Password:

- The system will need to be booted off the ISO when performing a Restore / Recovery option
 of the Entire Computer or Volume based backups.
- There are 3 types of backup jobs supported –
- 3065 (1) Entire Computer which is the system image
- 3066 (2) Volume level
- 3067 (3) File level backup.
- 3068 However, only one type of backup job can be scheduled in the Free version.
- To configure a backup job, Right-click on the Veeam Tray, select "Control Panel >>
- 3070 Backup" >> Click on Add New Job
- 3071

📃 🗹 Veeam Agent		×
 Veeam Agent Add New Job Settings Support About 	gured Backup Now	×

• Enter a Name for the Backup Job

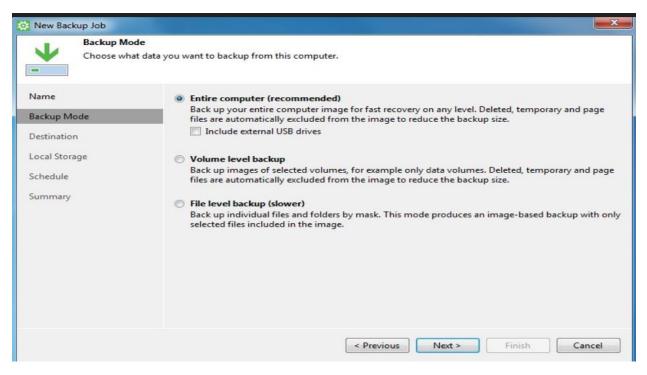
3077

🔅 New Backup Job		×
Name Type in a name a	nd description for this backup job.	
Name	Name:	
Backup Mode	Full-backup	
Destination Local Storage Schedule Summary	Description: Created by FGS-47631EHH\Administrator at 4/11/2019 4:45 PM.	
	< Previous Next > Finish	Cancel

3078 3079 3080 3081

3082

• Select a Backup Mode. For instance: Entire Computer



Select a Backup Destination. Choose "Shared folder" if saving the backups to a network
 share as in our case.

New Backup Job	
	e you want to backup your data to. We highly recommend that you do not store your backups on the same at you are protecting.
Name Backup Mode Destination Shared Folder	 Local storage Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended. Shared folder Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.
Backup Cache Schedule Summary	 Veeam backup repository Choose this option to back up to a backup repository managed by Veeam Backup & Replication 9.5 Update 4 or later server. Veeam Cloud Connect repository Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider. Microsoft OneDrive Choose this option to back up to the Microsoft OneDrive or Microsoft OneDrive for Business.
	< Previous Next > Finish Cancel

• Enter the path of the Network share and the Active Directory user credentials created earlier. Select the Number of Restore Points as per your retention policy.

Shared Fold Specify a sha	er ared folder to backup to, and account to connect to a shared folder with.
Name	Shared folder:
De aleva Marda	\\10.100.0.10\backups\workstation Browse
Backup Mode Destination	n/a Populate
Shared Folder	This share requires access credentials:
Backup Cache Schedule Summary	Vsername: LAN\veeamuser Password:
	Keep backups for the past: 14 🚔 days when the computer was running Click Advanced to enable periodic full backups, configure encryption and other

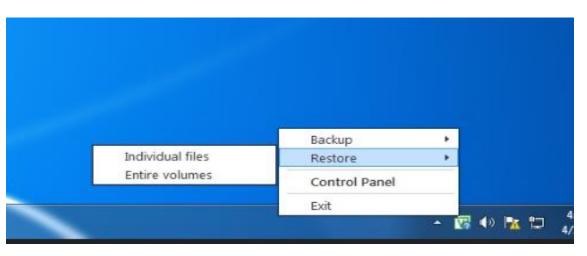
• Configure a Schedule. Hit **Apply** when done.

Choose whe	en you want backup job to be started automatically.			
Name Backup Mode	Periodically We will wake your computer from sleep to tal is enabled. Normally, this model is only enabl			power mod
Destination	Daily at 12:3	0 AM 🚔	Everyday 👻	Days
Local Storage	If computer is powered off at this time	[Backup once powered o 💌	
Schedule	Once backup is taken, computer should	1	Keep running 👻	
Summary	At the following events			
	C Lock			
	Log off			
	When backup target is connected 🕦			
	Eject removable storage once backup		I (CryptoLocker protection)	
	Back up no more often than every 2 🗼	lour	*	
	< Pre	vious	Apply Finish	Cancel

3096 **<u>Recovery:</u>**

- Recovery of Individual files or Volumes can be done using the Veeam agent in the System
 Tray itself. Double click on the Agent icon >> Restore >> Select <Type> >> Follow the
 steps.
- 3100 Note: This is dependent on having a successful File-level or Volume-level Backups captured3101 previously.
- 3102

3095

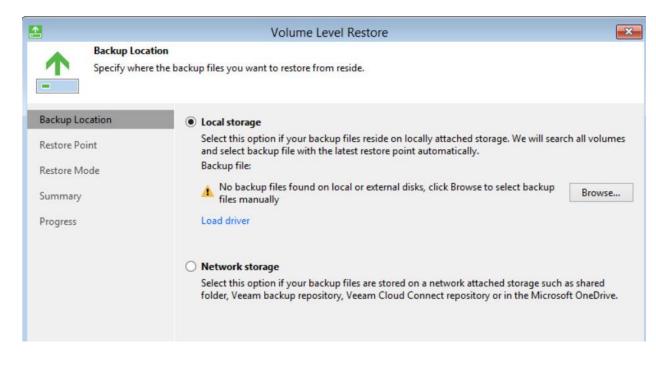


- To perform a Bare Metal restore of the Entire Computer, Boot the system using the
- 3105 Recovery media created earlier. Click on "Bare Metal Recovery"
- 3106

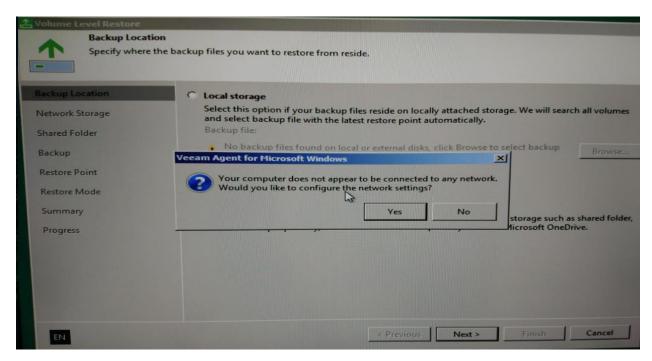


3110

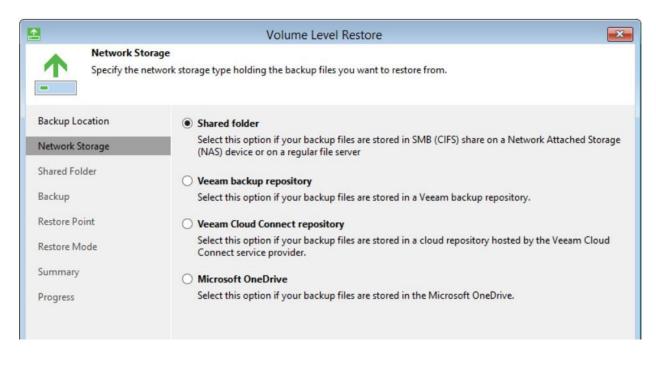
• Select "Local Storage" if restoring backups from an External USB Drive or "Network Storage" if restoring from a network share as in our case.



An option will be presented to configure Network Settings. Choose either DHCP or Static
 IP and hit Continue.



- Under "Network Storage", select Share folder. Hit Next



• Enter the path of Share folder to restore from. For instance:

3123

3124

Shared Fold Specify a sha	er red folder to backup to, and account to connect to a shared folder with.	
Name	Shared folder:	
Backup Mode	\\10.100.0.10\backups\workstation	Browse
Destination	n/a	Populate
Shared Folder	This share requires access credentials:	
Backup Cache	Username: LAN\veeamuser	
Schedule	Password:	

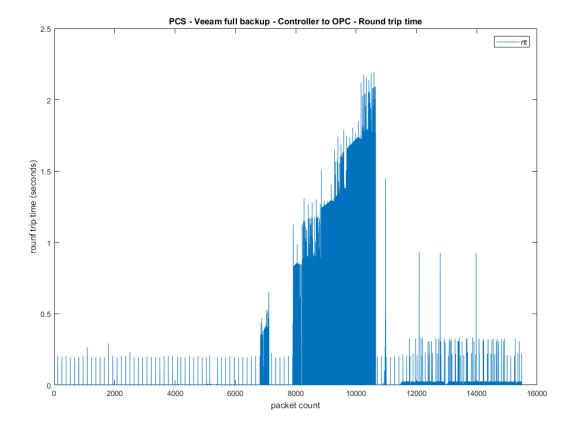
- Next, assuming the wizard is able to connect to the Network share, it will populate a list of
 Backups. Select a Backup and hit Next.
- Under **Restore Points** select a restore point from which you want to recover data. Veeam
 Agent for Microsoft Windows displays only restore points of volume-level backups.
- Select a Restore Point and hit Next.
- Under Restore Mode, choose a Restore Mode. If the disk type and layout on the system has
 not changed select "Entire Computer". There is a Manual restore available for advanced
 users.

	Volume Level Restore
Restore Mode Specify a restore r	mode.
Backup Location Network Storage Shared Folder Backup Restore Point	 Entire computer Restores the entire computer backup. All data on existing volumes of this computer will be overwritten with the data from backup file. System volumes only Restores only system volumes required for the operating system to function. Recommended in situations when your computer does not boot up. Manual restore (advanced)
Restore Mode Disk Mapping Summary Progress	Restores selected volumes only, with the ability to re-allocate partitions and volumes. This restore mode should be used by advanced users only.
EN	< Previous Next > Finish Cancel

- Under **Disk Mapping**, Map restored drives as per your system layout. For detailed
- 3135 instructions on how to map, refer to
- 3136https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.htm31371?ver=30
- Under **Summary** Page, review the summary. Hit **Restore** to start the restore process.
- 3139 **References:**
- 3140 [1] Veeam Backup and Replication <u>https://www.veeam.com/vm-backup-recovery-replication-</u>
 3141 <u>software.html</u>
- 3142 [2] Veeam agent for MS Windows Free edition <u>https://www.veeam.com/windows-endpoint-</u>
 3143 server-backup-free.html

3144 **4.6.6 Highlighted Performance Impacts**

- 3145 The following performance measurement experiment was performed for the Veeam Backup tool
- 3146 while the manufacturing system was operational:
- 3147 Experiment PL009.2- Veeam full backup
- 3148 Experiment PL010.1- Veeam incremental backup
- A small performance impact to the manufacturing process was observed in, however, a more
- 3150 noticeable impact was observed in the network traffic. For example, the round trip time from the
- 3151 Controller to the OPC was increased significantly during the backup. The path delay from the
- 3152 OPC to HMI was also increased significantly during the backup. The amount of backup traffic
- 3153 could take up a large portion of the available bandwidth.
- Also, there is storage consideration, example of backup size in the PCS system: HMI: 96GB,
- 3155 OPC: 29GB, Controller: 31GB, Historian: 194GB
- 3156 Network usage should be taken into consideration on when to perform a full backup, a low
- 3157 network utilization time is likely to reduce the impact to the system One important feature of the
- 3158 Veeam backup is its ability to throttle to adapt to the network utilization in order to avoid taking
- 3159 up all the available bandwidth for the backup traffic.
- 3160 Incremental backup should be considered for periodic backup instead of full image backup.
- 3161 During the full backup, the network traffic increased dramatically, in one case, the backup of the
- 3162 HMI and Controller hosts represented 99.6% of the total traffic verse 0.4% of the normal traffic.
- 3163





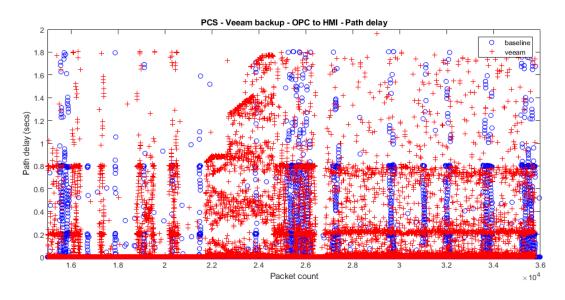
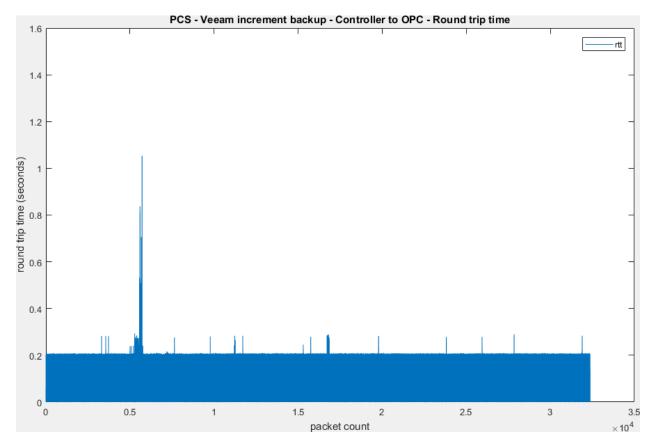


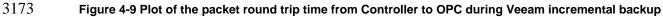


Figure 4-8 Plot of the path delay from OPC to HMI during Veeam full backup

- 3168 Increment backup should be considered, the amount of network resources consumed was much
- 3169 lower compare with full backup. The round trip time from Controller to OPC during an
- 3170 incremental backup was increased only for a short amount of time.
- 3171







There was a small performance impact to the manufacturing process observed during the full
backup. The product flow was slightly lower and the reactor pressure overshot their normal
levels in the experiment.

3177 It is hypothesized that the impacts were caused by increased network latency and traffic which 3178 caused a delay of the sensor and actuator information exchange between the Controller and the 3179 simulated plant. Therefore, a degrade performance of the control loop causing a slight impact to 3180 the performance of the system. The ability of the Veeam backup to throttle the rate of backup 3181 according to the network condition helped reduce the impact to the network traffic and latency 3182 during the full backup.

- 3183
- 3184

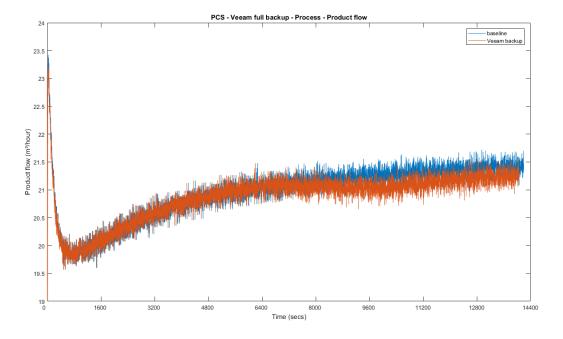
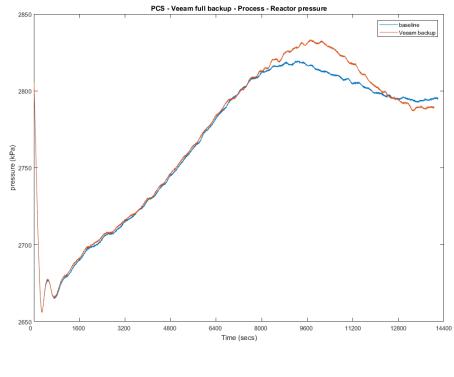




Figure 4-10 Plot of the production flow of the manufacturing process during Veeam full backup



3188 Figure 4-11 Plot of the reactor pressure of the manufacturing process during Veeam full backup

3189

- **4.6.7** Link to Entire Performance Measurement Data Set
- 3191 Veeam full backup KPI data
- 3192 Veeam full backup measurement data
- 3193 Veeam incremental backup KPI data
- 3194 Veeam incremental backup measurement data
- 3195
- 3196

3197 4.7 Security Onion

3198 **4.7.1 Technical Solution Overview**

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise
security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort,
Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools.¹⁴ Security
Onion combines three core functions:

- full packet capture;
- network-based and host-based intrusion detection systems (NIDS and HIDS, respectively);
- and powerful analysis tools
- 3207 Points to consider:
- Open source software, available as an ISO distribution to deploy in any type of environment (physical or virtual).
- Collection of different open-source tools such as SNORT, BRO, OSSEC SGQUIL,
 KIBANA, ELSA etc. integrated into one product which otherwise would require lot of manual work to integrate.
- Support for standalone instance and distributed deployment for large organizations.
- Provides a front-end to Snort and BRO IDS which natively are command line-based tools.
- Fully customizable rule-set. Has inbuilt detection rules to detect a variety of cyber-attacks and anomalies for both IT and OT environments.
- Learning curve associated. Familiarity with SNORT and BRO IDS rule-set.
- Hardware Resource intensive.
- No reporting capabilities out of the box.

3221 **4.7.2** Technical Capabilities Provided by Solution

3222 Security Onion provides components of the following Technical Capabilities described in3223 Section 6 of Volume 1:

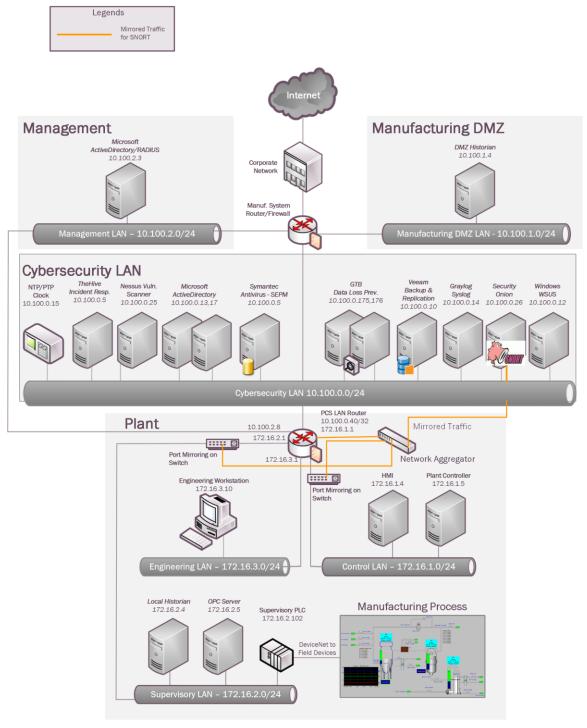
- Network Boundary Protection
- Network Monitoring
- Event Logging
- Forensics

¹⁴ Security Onion: <u>https://securityonion.net/</u>

3228 Subcategories Addressed by Implementing Solution

- 3229 PR.DS-5, PR.PT-4, DE.AE-2, DE.CM-1, DE.CM-6, DE.CM-7
- 3230

3231 **4.7.3** Architecture Map of Where Solution was Implemented



3233 4.7.4 Installation Instructions and Configurations

Setup 3234

- 3235 An ISO image of the Security Onion was downloaded from their website
- (https://securityonion.net/) and deployed on a Microsoft Hyper-V virtual host in the 3236
- Cybersecurity LAN network. Ensure to assign appropriate hardware resources as 3237
- recommended in the product documentation.¹⁵ 3238
- 3239 Details of the solutions implemented:

Name	Version	Hardware details
Security Onion	16.04.5.2	Virtual Machine with 4 virtual cores, 20GB Memory, 400GB Disk

3240

3241 Ours is a standalone single server deployment. For larger environments, Security Onion • supports a distributed deployment mode consisting of multiple remote sensors. Detailed setup 3242 documentation is available on their wiki.¹⁶ 3243 3244 3245 Security Onion requires 2 physical network connections as follows -٠ 3246 3247 (i) (eth0) for management IP address (ii) (eth1) for the monitoring interface. This interface needs to be configured in 3248 promiscuous mode to leverage the SNORT and BRO IDS components for monitoring 3249 network traffic. 3250 3251 3252 For (i) a virtual switch connection was provisioned from the Cybersecurity LAN and 3253 assigned to the Security Onion VM. This is for setting up an IP address to login to 3254 Security Onion interface or the server itself. 3255 3256 For (ii) Port Mirroring was configured on the two network switches and the Boundary Firewall. These mirrored port(s) were further connected to a Network Aggregator device. 3257 3258 3259 The Network Aggregator device is used for aggregating traffic from these network 3260 devices of the Process Control System. An outbound connection from its Aggregated 3261 interface was made to the monitoring interface (eth1) of the Security Onion VM. 3262 Figure 1 below shows the setup of security onion in our environment. 3263

¹⁵ Security Onion Documentation: https://securityonion.readthedocs.io/en/latest/

¹⁶ Security Onion WIKI: https://github.com/Security-Onion-Solutions/security-onion/wiki

- Once the two network connections are connected, power on the virtual machine and complete
 the default Linux OS setup as per the instructions on the screen. Upon a system reboot, login
 to the console locally and click on the Setup icon on the "Desktop" to configure the network
 interfaces. This step includes assigning a static IP address for management and setting up the
 monitoring port of the instance. Ensure to select the correct interfaces for each role. A
 Reboot is required upon completion.
- Reboot the system and click on the Setup icon again to complete the next phase of the setup.
- 3271 It will display the below message. Click **YES**, **Continue!** and then select **Evaluation Mode** 3272 in the next screen for standalone deployments.
- 3273

Security Onion Setup (se	econion) ×
Welcome to Security Onion E	Elastic Setup!
Elastic Setup will configure th	e following services:
Elasticsearch Logstash Kibana Squert Sguil Bro Snort/Suricata netsniff-ng Would you like to continue?	
No, Quit.	Yes, Continue!

- 3274 3275
- 3276 3277

3285

- Follow the on-screen options and complete the wizard. A system reboot would again be required.
- Security Onion by default allows SSH only from localhost. To connect to it remotely, run the command "sudo so-allow" to configure the appropriate firewall rules for remote connectivity. Select "a analyst" option and whitelist the IP address or ip-range of client-pc where you intend to access security onion interface from. Instructions to setup the firewall can be found here: <u>https://github.com/Security-Onion-Solutions/security-</u> <u>3284</u>
 - Upon completion of both setup phases, security onion should now be accessible using any of the 3 methods below:
- SQUERT Web Interface: This is the web interface to the backend Sguil database. The
 URL is <u>https://IP address-of-security-onion/</u>
- Kibana: Kibana is an open source data visualization plugin for Elasticsearch. It can be accessed via https://ip-address-of-security-onion/app/kibana
- Sguil client: A windows-based client is available for querying the Sguil database at https://bammv.github.io/sguil/index.html for installing on a remote workstation.
- The credentials to login to the above URLs should be the one that were created earlier during the setup process.

- Ensure to set the OS time-zone to UTC as Security Onion uses UTC by default. Changing
 time-zone can cause other issues.
- The command sudo nsm_sensor_ps-status can be used to check the status of each
 Security Onion component/service.
- 3299

3300 **Configuring Updates:**

- Register on SNORT.org for an account to be eligible for downloading the "Registered" Rule
 set. Upon registration, note down the OINK code tied to your account. Copy-paste the OINK
 code in the "rule_url" parameter in /etc./nsm/pulledpork/pulledpork.conf file of the server
 and save the changes.
- 3305 rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|<oink-code> 3306
- 3307 Security Onion by default requires internet access to download Snort signatures. If your
 3308 Security Onion server has internet access, uncomment and set
- 3309 "LOCAL_NIDS_RULE_TUNING=no" in /etc./nsm/securityonion.conf file. Run the "sudo
 3310 rule-update" command to update the rule set. This will download new rules from Snort.org
 3311 and save them in /etc./nsm/rules/downloaded.rules file.
- 3312
- For Air-Gapped environments (w/o Internet), set LOCAL_NIDS_RULE_TUNING=yes in the securityonion.conf file and the snort updates would have to be manually downloaded on a different system and transferred via USB device or network to /tmp folder on the
- 3316 Security Onion server. Once done run the **sudo rule-update** command.

3317 SNORT IDS Setup:

- Define the network variables such as \$HOME_NET, \$EXTERNAL_NET etc. as per your environment in the snort configuration file (snort.conf) located at /etc./nsm/<hostname-
 MonitorInterface>/. Once done, the snort service should be restarted by running the command:
- 3322 sudo nsm_sensor_ps-restart --only-snort
- Below is a snippet of the **snort.conf** in our instance
- 3325

3330

33313332

33333334

3335 3336

3337

```
# Step #1: Set the network variables. For more information, see README.variables
   ******
   # Setup the network addresses you are protecting
   ipvar HOME NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
   ipvar NETWORK DEVICES [172.16.1.3,172.16.3.1,172.16.2.2,192.168.0.239,192.168.0.2,192.168.1.2]
   ipvar ICS DEVICES [172.16.2.102,172.16.4.102,192.168.0.30,192.168.0.60]
   ipvar PCS ICS DEVICES [172.16.2.100/30]
   # Set up the external network addresses. Leave as "any" in most situations
   ipvar EXTERNAL NET !$HOME NET
   # List of DNS servers on your network
   ipvar DNS SERVERS [10.100.0.17]
   # List of SMTP servers on your network
   ipvar SMTP SERVERS $HOME NET
   The Snort module uses the downloaded.rules under /etc./nsm/rules/ directory for its IDS
•
   rule set in addition to any local rules defined under /etc./nsm/rules/local.rules file. All
   custom rules should be defined under this local.rules file. Upon adding a custom rule, the
   snort rule set must be updated using this command: sudo rule-update
   This command will also result in local rules getting merged into downloaded.rules file.
   Additionally, you can manually verify the same by running tail -n 100 downloaded.rules. If
   the defined local rules do not appear in the downloaded.rules file; the
   /etc./nsm/<interface>/snortu-1.log file must be reviewed for any syntax errors.
   Below are some of the rules we setup to detect common IT and ICS-specific anomalies.
```

alert UDP any any -> SPCS_ICS_DEVICES any (msg: "NmAP UDP Scan"; sid:10000002; rev:1;) alert icmp any any -> SHOME_NET any (msg: "NMAP ping sweep Scan"; dsize:0; sid:10000004; rev:1;) alert icmp any any -> SHOME_NET any (msg: "Ping Large ICMP Packet"; dsize:>800; classtype:bad- unknown; sid:10000030; rev:1;) alert tcp any any -> SHOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recor; sid:10000005; rev:1;) * Detect FTP Attempt to Public IP-address & other FTP events alert tcp SHOME_NET any -> SEXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000002; rev:1;) alert tcp SHOME_NET any -> SEXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000002; rev:1;) alert tcp SHOME_NET any -> any 21 (msg: "FTP file successfully uploaded"; content: "[54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert tcp any 21 -> SHOME_NET any (msg: "FTP file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) * Detect Gredit curd number in cleartext alert tcp any any ~> any any (pcre:"/5id{3}(sl-)?/d{4}(sl-)?/d{4}(sl-)?/d{4}//"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) * Detect Gredit curd number in cleartext alert tcp any any ~> any any (pcre:"/3id{3}(sl-)?/d{4}(sl-)?/d{4}(sl-)?/d{4}//"; msg: "WasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any compt."//aid{3}(sl-)?/d{4}(sl-)?/d{4}//"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Password in Clear text"; content "Password"; sid:10000010; rev:1;) alert tcp SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "I73 77 69 74 63 68]"; sid:10000008; rev:1;) alert tcp SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Pas		AP scan, ICMP attack , TCP-SYN Flood attack
alert icmp any any -> SHOME_NET any (msg: "Ping Large ICMP Packet"; dsize:>800; classtype:bad- unknown; sid:10000030; rev:1;) alert top any any -> SHOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recor; sid:10000005; rev:1;) * Detect FTP Attempt to Public IP-address & other FTP events alert top SHOME_NET any -> SEXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000002 rev:1;) alert top SHOME_NET any -> any 21 (msg: "FTP upload attempt"; content: "[53 54 4f 52]"; sid:10000020; rev:1;) alert top SHOME_NET any -> any 21 (msg: "FTP file successfully uploaded"; content: "[54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert top any 21 -> SHOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) * Detect Credit card number in cleartext alert top any any <> any any (pcre:"/3d{3}(\si-)?\d{4}(\si-)?\d{4}(\si-)?\d{4}\d{*}"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert top any any <> any any (pcre:"/3d{3}(\si-)?\d{4}(\si-)?\d{4}(\si-)?\d{4}\d{*}"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000014; rev:1;) alert top any any <> any any (pcre:"/3d{3}(\si-)?\d{4}(\si-)?\d{4}(\si-)?\d{4}(\si-)?\d{4}\d{*}"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert top SHOME_NET any -> STELNET_SERVERS 23 -> SHOME_NET any (msg: "Telnet Password in Clear text"; content "Password"; sid:10000010; rev:1;) alert top SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "I/3 77 69 74 63 68["; sid:10000008; rev:1;) alert top SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "I/3 77 69 74 63 68["; sid:1000008; rev:1;) alert top SHOME_NET any -> STELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content:		
unknown; sid:10000030; rev:1;) alert tcp any any -> SHOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recor; sid:10000005; rev:1;) *** Detect FTP Attempt to Public IP-address & other FTP events alert tcp SHOME_NET any -> SEXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000002 rev:1;) alert tcp SHOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> SHOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert tcp any 21 -> SHOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) ** Detect Credit card number in cleartext alert tcp any any \diamondsuit any any (pcre: "/5/d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any \backsim any any (pcre: "/3/d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any \backsim any any (pcre: "/4/d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp \$HOME_NET any -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "13 77 69 74 63 68["; sid:10000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "17 37 76 97 46 36 8["; sid:1000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation		
alert tcp any any -> \$HOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recon; sid:10000005; rev:1;) # Detect FTP Attempt to Public IP-address & other FTP events alert tcp \$HOME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: "[53 54 4f 52]"; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: "[54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any any (pcre:"/5\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:1000001; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}/"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "[73 77 69 74 63 68]"; sid:1000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "[73 77 69 74 63 68]"; sid:1000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "[73 77 69 74 63 68]"; sid:1000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Autom		
<pre>flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recor; sid:10000005; rev:1;) // Detect_FTP_Attempt to Public IP-address & other_FTP_events alert tcp \$HOME_NET any -> SEXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000002 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) // Detect_Credit_card_number in cleartext alert tcp any any <> any any (pcre: "/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number_detected in clear text"; content: "number"; nocase; sid:1000013; rev:1;) alert tcp any any <> any any (pcre: "/4\d{3}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre: "/4\d{3}(\s -)?\d{4}(\s -)?\d{4}/\s]/"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) // Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "[73 77 69 74 63 68]"; sid:10000008;rev:1;) alert tcp \$HOME_NET any -> \$TELNET login failed"; flow:from_server,established; content: "Logi alert tcp \$1 OMME_NET any -> \$TELNET login failed"; flow:from_server,established; content: "Logi</pre>		
<pre>sid:10000005; rev:1;) # Detect FTP Attempt to Public IP-address & other FTP events alert tcp \$HOME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pre: "/5\d{3}(\sl-)?\d{4}(\sl-)?\d{4}\\sl-)?\d{4}//"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pre: "./3\d{3}(\sl-)?\d{4}(\sl-)?\d{4}\\sl-)?\d{4}/"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pre: "./3\d{3}(\sl-)?\d{4}(\sl-)?\d{4}\\sl-)?\d{4}/"; msg: "WasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pre: "./4\d{3}(\sl-)?\d{4}(\sl-)?\d{4}\\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:1000001;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000007; rev:1;) alert tcp \$HOME_NET any any (msg: "TELNET login failed"; flow:from_server,established; content: "Logi alert tcp \$HOME_NET any any (msg: "TELNET login failed"; flow:from</pre>		
<pre># Detect FTP Attempt to Public IP-address & other FTP events alert tcp \$HOME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 66 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}\'"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any any (pcre:"/5\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}\'"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/d\d{3}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}(\sl-)?\d{4}\'"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "173 77 69 74 63 68]"; sid:10000008;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "173 77 69 74 63 68]"; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: "173 77 69 74 63 68]"; sid:10000008;rev:1;) alert tcp \$HOME_NET any any any (msg: "TELNET login failed"; flow:from_server,established; content: "Logi alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Ro</pre>		
alert tcp \$HOME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; content "Password"; sid:1000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_login failed"; flow:from_server,established; content: "Logi		
alert tcp \$HOME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003 rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; content "Password"; sid:1000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_login failed"; flow:from_server,established; content: "Logi		
rev:1;) alert tcp \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 6e 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d {3}(\s -)?\d {4}(\s -)?\d {4}(\s -)?\d {4}/\"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d {3}(\s -)?\d {6}(\s -)?\d {6}(\s -)?\d {4}/\"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d {3}(\s -)?\d {4}(\s -)?\d {4}(\s -)?\d {4}/\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) # Telnet activity monitorng alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; content "Password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:1000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008; rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server, established; content:"Logi		
alert top \$HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: " 53 54 4f 52 "; sid:1000020; rev:1;) alert top any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 66 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert top any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert top any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert top any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000014; rev:1;) alert top any any <> any any (pcre:"/3\d{3}(\s -)?\d{4}(\s -)?		ME_NET any -> \$EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:1000000
sid:10000020; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 66 7 66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number"; nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\"; msg: "Visa number detected in clear text"; content:"number"; nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s		ME_NET > 21 ("ETD1
alert tcp any 21 -> \$HOME_NET any (msg: "FTP file successfully uploaded"; content: " 54 72 61 66 7 66 65 72 20 63 6f 6d 70 6c 65 74 65]"; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any \Leftrightarrow any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "MasterCard number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any \diamondsuit any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{6}\"; msg: "American Express number detected in clear text"; content: "number"; nocase; sid:10000013; rev:1;) alert tcp any any \diamondsuit any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000014; rev:1;) alert tcp any any \diamondsuit any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "Visa number detected in clear text"; content: "number"; nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008; rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server, established; content: "Logi		
66 65 72 20 63 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;) alert tcp any 21 -> \$HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf"; sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{6}(\s -)?\d{4}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008; rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
<pre>sid:10000031; rev:1;) # Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login </pre>	66 65 72 20 6	3 6f 6d 70 6c 65 74 65 "; sid:10000027; rev:1;)
# Detect Credit card number in cleartext alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login		
alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi	sid:10000031	rev:1;)
alert tcp any any <> any any (pcre:"/5\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "MasterCard number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}\"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi	# Detect Cred	it eard number in claartext
number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;) alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:1000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
alert tcp any any <> any any (pcre:"/3\d{3}(\s -)?\d{6}(\s -)?\d{5}/"; msg: "American Express number detected in clear text"; content:"number";nocase; sid:10000014; rev:1;) alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/"; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:1000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
<pre>alert tcp any any <> any any (pcre:"/4\d{3}(\s -)?\d{4}(\s -)?\d{4}(\s -)?\d{4}/\s ."; msg: "Visa number detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login</pre>		
<pre>detected in clear text"; content:"number";nocase; sid:10000015; rev:1;) # Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:1000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login </pre>		
# Telnet activity monitoring alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content: "Login		
alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content: "Logi	detected in cle	ar text"; content:"number";nocase; sid:10000015; rev:1;)
alert tcp \$TELNET_SERVERS 23 -> \$HOME_NET any (msg: "Telnet Password in Clear text"; conte "Password"; sid:10000010;rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content: "Logi	# Telnet activ	ty monitoring
alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "TELNET login attempt"; classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content: "Logi		
classtype:default-login-attempt; sid:10000007; rev:1;) alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
alert tcp \$HOME_NET any -> \$TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
Password"; content: " 73 77 69 74 63 68 "; sid:10000008;rev:1;) alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		
alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Logi		

3343 Snort Rules for ICS/ SCADA¹⁷

3344

#ICS-SCADA specific rules [4]
alert tcp \$HOME_NET any -> \$ICS_DEVICES 44818 (msg: "PROTOCOL-SCADA Rockwell firmware
change attempt"; flow:to_server,established; content:" 6F 00 "; content:" 00 00 00 00 "; within:4; distance:6;
content:" 00 00 00 00 "; within:4; distance:8; pcre:"/(\x20\xa1 \x21\x00\xa1\x00)(\x24[\x01-
\xff] \x25\x00[\x01-\xff]\x00)/smi"; reference:cve,2012-6437;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=27868; classtype:policy-violation;
sid:10000019; rev:1;)
alert tcp \$HOME_NET any -> \$ICS_DEVICES \$HTTP_PORTS (msg: "ICS-SCADA PLC Web access
attempted "; sid:10000033; rev:1;)
alert tcp any any -> \$HOME_NET 22350 (msg: "PROTOCOL-SCADA TwinCAT PLC DOS attempt";
flow:to_server,established; dsize:>2000; content:" A2 1D CB AA AA 75 48 B4 91 DB F4 06 B0 B0 2D ";
fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop;
reference:url,www.beckhoff.com/english.asp?twincat/overvw.htm; classtype:attempted-dos; sid:41743;
rev:2;)
alert tcp any any -> \$ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15074; rev:5;)
alert tcp any any -> \$ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15075; rev:5;)
alert tcp any any -> \$ICS DEVICES 502 (msg: "PROTOCOL-SCADA Modbus read multiple coils - too
many inputs"; flow:to_server, established; modbus_func:read_coils; byte_test:2,>,2000,10;
reference:url,www.modbus.org/docs/Modbus Application Protocol V1 1b.pdf; classtype:protocol-
command-decode; sid:15077; rev:6;)
alert tcp any any -> \$ICS DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple registers
from external source"; flow:to server,established; modbus func:write multiple registers;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17782; rev:4;)
alert tcp any any -> \$ICS DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write single coil from
external source"; flow:to_server,established; modbus_func:write_single_coil;
reference:url,www.modbus.org/docs/Modbus Application Protocol V1 1b.pdf; classtype:protocol-
command-decode; sid:17784; rev:4;)
alert tcp any any -> \$ICS DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple coils from
external source"; flow:to server, established; modbus func:write multiple coils;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17785; rev:4;)

¹⁷ Snort Rules for ICS/ SCADA: <u>https://github.com/ITI/ICS-Security-</u> Tools/blob/master/configurations/rules/talos-snort.rules

I	# Accessing switch via Web URL & use of default password
	alert tcp_any -> \$NETWORK_DEVICES 80 (msg: "WEBAPP Netgear Default Password";
	flow:established,to_server; content:"POST"; nocase; http_method;
	uricontent:"/base/cheetah_login.html"; content:"password"; nocase; sid:1000009; rev:1;)
	alert tcp \$HOME_NET any -> \$NETWORK_DEVICES \$HTTP_PORTS (msg: "WEBAPP Rockwell
	Automation default password login attempt"; flow:to_server,established; content:"Authorization 3A ";
	nocase; http_header; content:"YWRtaW5pc3RyYXRvcjptbDE0MDA="; fast_pattern:only; http_header;
	metadata:service http; classtype:default-login-attempt; sid:10000011; rev:1;)
	# SSH Activity monitoring
	alert tcp any any -> \$EXTERNAL_NET 22 (msg: "SSH Attempt to Public Host"; sid:10000018; rev:1;)
	alert tcp any any -> \$HOME_NET 22 (msg: "Potential SSH Brute Force Attack"; flow:to_server,
	established; flags:S+; detection_filter:track by_src, count 30, seconds 10; classtype:attempted-dos;
	priority:1; sid:10000006; rev:1;)
	# DNS traffic to social media websites
	alert udp \$HOME NET any -> \$DNS SERVERS 53 (msg: "DNS Request to Twitter.com Detected";
	content: " $ 6e 69 73 74 $ "; sid:10000016; rev:1;)
	alert udp \$HOME_NET any -> \$DNS_SERVERS 53 (msg: "DNS Request to Facebook.com Detected";
	content: " 66 61 63 65 62 6f 6f 6b "; sid:10000017; rev:1;)
	# File upload activity to a public web server
	alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg: "WEB-PHP file upload
	attempt"; flow:to_server, established; uricontent:"/upload.php"; nocase; content:"filename=";
	reference:bugtraq,3361; reference:cve,2001-1032; classtype:attempted-admin; sid:10000029; rev:1;)
	alert tcp \$Robotics_devices any -> \$EXTERNAL_NET \$HTTP_PORTS (msg: "Web Access to Public
	IP attempted"; sid:10000039; rev:1;)

3347 **Tuning Security Onion:**

- The default database retention period for Sguil database is 30 days. This can be changed by editing the **DAYSTOKEEP** parameter in the /etc./nsm/securityonion.conf file.
- A number of rules defined in the downloaded.rules file are commented out by default. This is intentional to reduce the volume of alerts and leaving the onus on the end user to customize it depending on the environment. To use any of the commented-out rules from downloaded.rules file, note down the Generator ID (GID) and Signature ID (SID) value defined in the rule that's commented out and list them in
- 3355 /etc./nsm/pulledpork/enablesid.conf file. Avoid directly uncommenting them. This will
 3356 enable that rule and will be persistent next time when the downloaded.rules gets updated.
- Likewise, to silence any false alerts note down the Generator ID (GID) and Signature ID
 (SID) value of the rule that is generating the alert and define them in the
 /etc./nsm/pulledpork/disablesid.conf file. Detailed instructions are available on the Snort
- 3360 documentation [5] under "Managing alerts".
 3361 Shown below is a snippet from our **disablesid.conf** file showing the SIDs we have disabled.
- 3362
- 3363
- 3364

	# example disablesid.conf V3.1
	# Example of modifying state for individual rules
	# 1:1034,1:9837,1:1270,1:3390,1:710,1:1249,3:13010
	3:19187
	119:19 # http_inspect: LONG HEADER
	123:8 # frag3: Fragmentation overlap
_	128:4 # ssh: Protocol mismatch
	129:4 # stream5: TCP Timestamp is outside of PAWS window
	129:5 # stream5: Bad segment, overlap adjusted size less than/equal 0
	129:7 # stream5: Limit on number of overlapping TCP packets reached
	129:12 # stream5: TCP Small Segment Threshold Exceeded

PCAPS can fill up the storage space on server. Follow the instructions on the wiki to manage
 the pcap files.

3382 **BRO IDS Setup:**

- Security Onion also uses BRO IDS alongside SNORT for network monitoring. The BRO logs are stored in /nsm/bro/logs directory. Similar to local.rules in SNORT, any custom scripts for BRO must be placed in /opt/bro/share/bro/policy/ directory. Please refer to the security onion wiki [3] for additional reference on BRO.
- To leverage BRO capabilities for Windows SMB File share monitoring, add the below line at
 the end of /opt/bro/share/bro/site/local.bro file
- 3389
- 3390 @load policy/protocols/smb
- 3391

ioad policy/protocols/s

3392 Once done restart BRO using the command: sudo nsm_sensor_ps-restart --only-bro

3393 OSSEC Setup:

 OSSEC server (now replaced with Wazuh) comes along with Security Onion. Ossec is a Host Intrusion Detection System (HIDS). The OSSEC server module is installed and running by default in the Security Onion server. OSSEC alerts can be viewed either from Kibana or Squert web interface.

 To configure additional client systems for monitoring using OSSEC, download the agent installer from OSSEC website (http://www.ossec.net/) specific to your Operating System, copy over the agent to the client system and run the setup process using the instructions mentioned on the Ossec website. During the install, mention the IP address of Security Onion server as the IP address of Ossec server. Ensure to open firewall ports on Security Onion server to receive data from Ossec clients.

- It is beyond the scope of this document to explain detailed working of the OSSEC product.
 The Ossec official website and other documentation links under References can be a useful
- source.
 Similar to Snort and Bro, any custom OSSEC rules for monitoring should be added in
 local_rules.xml file under /var/ossec/rules directory. If a decoder is required to parse
 custom logs, it should be defined under in local_decoder.xml file under /var/ossec/etc.
 directory.
- On Windows systems, OSSEC agents can be configured to monitor Event Viewer logs,
 Rootkit Detection, File Integrity Monitoring (FIM), Registry changes and any other custom
 application logs. Instructions are available on OSSEC website.
- Similarly, on Linux systems, OSSEC can perform File Integrity Monitoring, Process
 Monitoring, Rootkit changes and any other host intrusion attempts such as failed SSH logins.
- Ossec agent was installed on the Engineering workstation in Process Control System to detect following anomalies:
 - USB Drive detection [5].
 - Allen Bradley Factory Talk Administration Console login failures.
- 3420 Monitoring Unauthorized Assets.

3421 USB Drive Detection:

• The following lines were added to the local **ossec.conf** file on the Agent side (Engineering Workstation) where an USB drive would be monitored for

3424

3418

3419

<agent_config os="Windows"> <localfile> <log_format>full_command</log_format> <command>reg QUERY HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command> <alias>usb-check</alias> </localfile> </agent_config>

3425 3426

- Next, the following lines were added to the /var/ossec/rules /local_rules.xml file on the
- 3428 Security Onion server to generate an alert

<rule id="140125" level="7"> <if_sid>530</if_sid> <match>ossec: output: 'usb-check':</match> <check_diff /> <description>New USB device connected</description> </rule>

3430 3431

3432 Detecting Allen Bradley-Factory Talk Login failures:

3433

The Factory Talk Administration Console (installed on the Engineering Workstation) logs all authentication attempts and other diagnostic events under Windows Event Viewer as shown below.

3437

• 🔿 🚺 🚺 🚺					
Event Viewer (Local)	FactoryTalk Diagnosti	cs Number of events: 2,080			
Custom Views	Level	Date and Time	Source	Event ID	Task Category
Application	(i) Information	4/23/2018 4:04:28 PM	RSLinx Enterprise	1001	Operator
Security	Information	4/23/2018 4:03:19 PM	FactoryTalk Service	1001	Operator
Setup	(i) Information	4/23/2018 4:03:19 PM	FactoryTalk Service	1001	Operator
System	(i) Information	4/23/2018 4:03:10 PM	FactoryTalk Service	1001	Operator
Forwarded Events	(i) Information	4/23/2018 4:03:10 PM	FactoryTalk Service	1001	Operator
🗎 Applications and Services Lo	(i) Information	4/23/2018 4:02:56 PM	RSLinx Enterprise	1001	Operator
FactoryTalk Diagnostics	(i) Information	4/23/2018 4:02:56 PM	RSLinx Enterprise	1001	Operator
Hardware Events	(1) Information	4/23/2018 4:02:56 PM	RSLinx Enterprise	1001	Operator
Internet Explorer	(1) Information	4/23/2018 4:02:56 PM	FactoryTalkDiagn	1001	Engineer
Key Management Service					

3438 3439

 To alert on login failures from Factory Talk Admin console, the below config was placed in the local ossec.conf file of the windows workstation. This line tells Ossec to look for event ID 1001 under "Factory Talk Diagnostics" category also referenced as "FTDiag" in Event Viewer and forward those events to Ossec server. ossec.conf - Notepad File Edit Format View

3444

• Next on the Ossec server, the following lines were added in **local_rules.xml** file to generate an alert.

3447

<group name="syslog,"> <rule id="110001" level="0"> <if_sid>18104</if_sid> <match>FactoryTalkDiagnostics</match> <description>FactoryTalk Audit Event</description> </rule> <rule id="110002" level="7"> <if_sid>110001</if_sid> <match>failure</match> <description>FactoryTalk Administration Console login failure</description> </rule>

3448

3449 Monitoring for Unauthorized assets:

3450

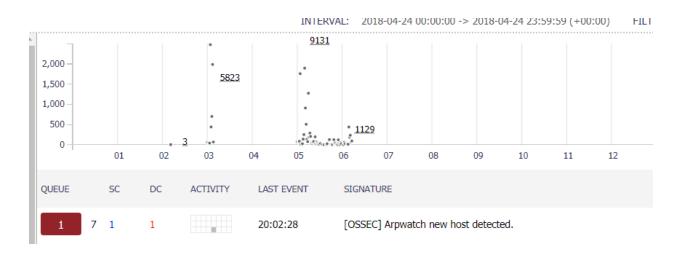
Rogue/Unauthorized Asset discovery can be implemented using Arpwatch and Ossec. To configure this, install the "arpwatch" package on the Security Onion server. Arpwatch package is available in all Linux distributions. Upon installation start the arpwatch service and configure it to listen to the network interfaces using the arpwatch -i <interface>
 command.

- 3457 For instance: arpwatch -i eth1 where eth1 is monitoring port.
- The Security Onion server already has an inbuilt decoder and a rules file for arpwatch located at /var/ossec/etc./arpwatch_decoder.xml and
 /var/ossec/rules/arpwatch_rules.xml. A new rule was added to our local_rules.xml file as shown below which references this inbuilt decoder and alerts when a new/bogon device is
- 3462 plugged into our network.

<rule id="110003" level="7"> <if_sid>7200</if_sid> <match>new|logon</match> <description>Arpwatch new host detected. </description> <group>new_host,</group> </rule>

3463

- Once done, restart the OSSEC server upon adding any local rules.
- The below image shows a sample alert in Squert Web Interface, when a new system was physically connected to the network:
- 3467



- 3468 3469
- 3409
- 3470

3471 Note: This package relies on ARP cache of the local system to detect new devices. It is
 3472 possible for an intruder to spoof this system's mac-address or poison arp-cache and remain
 3473 un-noticed.

3474 Lessons Learned:

- The full packet capture feature in Security Onion can fill up the hard disk space quickly
- 3476 depending on the amount of network traffic in your environment. Ensure to plan and allocate
- 3477 substantial amount of storage for the server along with configuring the necessary data
- retention options in securityonion.conf file. Trimming your pcaps can allow you to store pcapfor longer periods of time. For an example, please
- 3480 see <u>https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-</u>
 3481 Files---Trim-Them
- 3482

3484 **4.7.5** Highlighted Performance Impacts

No performance measurement experiments were performed for the use of Security Onion due to its installation location and how it was used (i.e., the software performed passive analysis of

its installation location and how it was used (i.e., the senetwork traffic external to the manufacturing system).

3488 **4.7.6** Link to Entire Performance Measurement Data Set

- 3489 N/A
- 3490

3491 **4.8 Cisco AnyConnect VPN**

3492 **4.8.1 Technical Solution Overview**

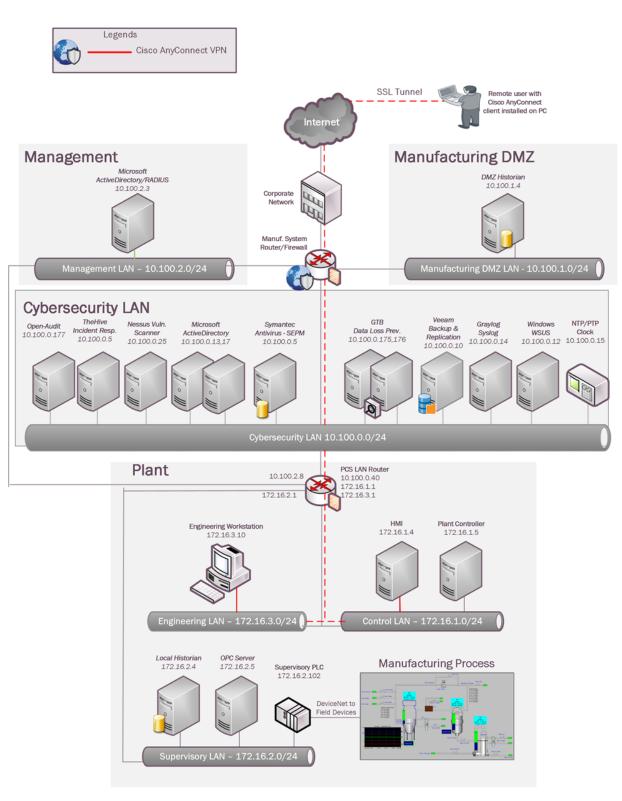
The AnyConnect Secure Mobility Client is a modular endpoint software product by Cisco. It not only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules. These modules provide services such as compliance through the VPN with ASA or through wired, wireless, and VPN with Cisco Identity Services Engine (ISE), web security alongside Cisco Cloud Web Security, network visibility into endpoint flows within Stealth watch, or off-network roaming protection with Cisco Umbrella. AnyConnect clients are available across a broad set of platforms, including Windows, macOS,

- 3500 Linux, iOS, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.¹⁸
- 3501 Points to consider
- Provides additional security in the form of Web Security and DNS-Based security.
- OS Platform independent: The VPN clients are supported on Windows, Mac and Linux.
- Administrators can control which networks or resources for endpoints to connect. It provides an IEEE 802.1X supplicant that can be provisioned as part of authentication, authorization, and accounting (AAA) capabilities along with some unique encryption technologies such as MACsec IEEE 802.1AE.
- Cisco Proprietary Product. This replaces the earlier free product called AnyConnect VPN client. You must either have a Cisco Adaptive Security appliance(ASA) Firewall or Cisco
 Firepower Services Appliance and an active AnyConnect Secure Mobility Client license.
- 3511 **4.8.2** Technical Capabilities Provided by Solution
- 3512 Cisco AnyConnect VPN provides components of the following Technical Capabilities described3513 in Section 6 of Volume 1:
- Secure Remote Access
- 3515 Data Replication
- 3516 **4.8.3** Subcategories Addressed by Implementing Solution
- 3517 PR.MA-2
- 3518

¹⁸ Cisco AnyConnect VPN <u>https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf</u>

3519 **4.8.4** Architecture Map of Where Solution was Implemented

3520



3522 4.8.5 Installation Instructions and Configurations

- 3523 Secure Remote Access was implemented for PCS system using the Cisco AnyConnect VPN. 3524 The AnyConnect VPN was configured on the top-level firewall - Cisco ASA in the 3525 Cybersecurity LAN network.
- 3526
- 3527 Overview 3528
- 3529 The following devices are involved in this setup
- 3530

Device	Function	OS / Version
Cisco ASA 5512 with Firepower services	Firewall	FTD 6.2.3
AnyConnect VPN	VPN Client software	4.7.01076
A Server in the Management LAN	Active Directory, Radius	Windows 2012 R2

3531 3532

3534

3537

- 3533 Setup of Radius server
- 3535 A Windows server was setup in the Management LAN for hosting Active Directory and 3536 Radius Authentication services for VPN clients.
- 3538 **Configuration Steps:**
- 3539 3540 Install the following roles on the server. Different servers can be used to separate out the 3541 Roles and for redundancy.
 - Active Directory Services
- o DNS Server 3543
 - Network Policy Server
- 3544 3545

3547

3548

3542

3546 All the above 3 roles can be installed using Windows Server Manager >> Add Roles and • Features wizard. Below image shows the role to be installed for Network Policy server

b	Add Roles and Features Wizard	_ _ ×
Select server rol Before You Begin Installation Type Server Selection	ES Select one or more roles to install on the selected server. Roles	DESTINATION SERVER Mgmt-AD.mgmt.lab
Server Selection Server Roles Features Confirmation Results	DNS Server (Installed) Fax Server File and Storage Services (2 of 12 installed) Hyper-V Network Policy and Access Services (1 of 3 installed) Health Registration Authority Host Credential Authorization Protocol Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services V	Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
	< Previous Next	> Install Cancel

Create a security group in Active Directory for VPN users and add those users to this group requiring VPN Access. A group called VPN-users was created in our AD server and a user vpnuser01 was added to this group.

	Active Directory Users and Computers	 x
File Action View Help Active Directory Users and Saved Queries Managed Service Action Managed Service Action Users	Active Directory Users and Computers General Members Member Of Managed By Members: Name Active Directory Domain Services Folder Name Active Directory Domain Services Folder Image: Name Member Of Members Members: Members Members Members: Member Of Members Members: Members Members <t< td=""><td></td></t<>	
< III	OK Cancel Apply	~

Open up the "Network Policy Server" console, click on Radius Clients and create a client
 for your firewall device. Below image shows a Radius client created for our Cisco-ASA
 firewall.

>		Network P	olicy Server				×
File Action View Help							
Þ 🔿 🙍 🖬 🚺							
	RADIUS Clients						
 RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Policies 	RADIUS clients	allow you to s	pecify the network acce	ess servers, that	provid <mark>e access</mark> to y	our network.	
Policies Network Access Protection	Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status		
	RuggedCOM-CRS	10.100.2.7	RADIUS Standard	No	Enabled		
Accounting	Allen Bradley-8300		RADIUS Standard	No	Enabled		
> 💐 Templates Management	Cisco-ASA	10.100.2.1	RADIUS Standard	No	Enabled		
¢ m >							

3560

3561

- While creating the Client, enter the IP address of the Interface on the ASA. This is typically
 the Default Gateway of the subnet where the AD/Radius server is in. Enter a strong password
 for Shared secret. This secret will later be used during the setup of a AAA group on the
 Firewall.
- Hit **OK** when done.

ettings Advanced	
Enable this RADIUS client	£
Select an existing template	e:
Name and Address	
Friendly name:	
Cisco-ASA	
Address (IP or DNS):	
10.100.2.1	Verify
Shared Secret	
Select an existing Shared Se	ecrets template:
None	
Manual Shared secret:	⊖ Generate
Confirm shared secret:	
•••••	
	OK Cancel A

- Under **Policies** >> Click on **Network Policies**. Create a Network Policy here corresponding
- to the Radius client setup earlier. Below image shows network policy created for the Cisco-
- 3583 ASA client. Ensure the policy is enabled.

		CISC	co-ASA Acco		2			
verview Condition	ns Constraints S	ettings						
^o olicy name:	Cisco-ASA	Access						
Policy State	valuates this policy	while performing a	authorization. If d	isabled, NPS does	not evaluate this	policy.		
Policy enabled	1							
Access Permissio								
	constraints of the access permission		hatch the connec	tion request, the p	policy can either	grant acces	ss or deny	
								
Grant access.	Grant access if the	connection reque	<mark>st matches this</mark> p	olicy.				
O Deny access.	Deny access if the o	connection reques	st matches this po	blicy.				
Ignore user ac	count dial-in properti	es.						
	on request matches ith network policy or					nts access,	perform	
addition2ation w	an nerwork policy of	ny, do not evalua	te the diamin prop	ferties of user acco	Junits .			
Network connect	on method							
Select the type of	on method network access se							
Select the type of or Vendor specific	on method network access se ; but neither is requ							
Select the type of	on method network access se ; but neither is requ							
Select the type of or Vendor specific select Unspecifie	on method network access se ; but neither is requ							
Select the type of or Vendor specific select Unspecifie	on method network access se ; but neither is requ d.							
Select the type of or Vendor specific select Unspecifie Type of netwo	on method network access se c, but neither is requ d. ırk access server:		ork access serve					
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified	on method network access se c, but neither is requ d. rk access server: c:		ork access serve					
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve					
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve			or wireless		
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,
Select the type of or Vendor specific select Unspecifie Type of networ Unspecified Vendor specifi	on method network access se c, but neither is requ d. rk access server: c:		ork access serve		nenticating switch	or wireless	access poi	int,

- Under Conditions tab, click ADD to add the following two conditions. More conditions can
 be added as per your requirement.
- 3597 **VPN-Users** security group created earlier.
- 3598 Client IPv4 Address: IP address of the Radius client created earlier.

				co-ASA Accces					
Overview	Conditions	Constraints	Settings						
If conditio	ns match the		equest, NPS uses ti	nis policy to authorize other policies, if add			ditions do n	ot match the	
Con	dition	Va	alue						
Win	dows Group	s M	GMT\VPN-Users						
Real Property in the second	nt IPv4 Addr).100.2.1						
	description: lows Groups	condition spe	cifies that the conne	cting user or compu	ter must belon <u>c</u>	to one of the se	lected grou Edit.		Remove

3599

- Under Authentication Methods, select the methods shown below. This is as per Cisco documentation.¹⁹
- 3603 3604

Constraints	nods	Allow access only to those clients that authenticate with the specified methods	ú.
Idle Timeout Session Timeout		EAP types are negotiated between NPS and the client in the order in which the listed. EAP Types:	ey are
Called Station ID	tions	Mo	ve Up
Image: Solution of the soluti	Aloris.	Move	e Down
		Add Edit Remove	
		Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) Jer can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP)	
		User can change password after it has expired	
		 Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) 	
		Allow clients to connect without negotiating an authentication method Perform machine health check only	

¹⁹ Cisco ASA VPN User Authentication: <u>https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html</u>

- 3608 Under Settings >> Radius Attributes >> Standard set the following attributes •
- 3609 \circ Framed Protocol= **PPP**
- 3610 • Service-Type=Framed
- 3611 \circ Class = **Name of group policy**>. This policy is configured in the Firewall for VPN

Overview Conditions Constraints S	CISCO-ASA A	access Properties
Configure the settings for this network p If conditions and constraints match the Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection	To send additional at then click Edit. If you	olicy grants access, settings are applied. ributes to RADIUS clients, select a RADIUS standard attribute, and do not configure an attribute, it is not sent to RADIUS clients. See ocumentation for required attributes.
 NAP Enforcement Extended State Routing and Remote Access Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Encryption IP Settings 	Attributes: Name Class Framed-Protocol Service-Type	Value DfltGrpPolicy PPP Framed
	Add	EditRemove
		OK Cancel A

3617

3615	Below are the high-level steps for configuring Remote Access VPN in the FMC (Firepower
3616	Management Console)

- 3618 Go to Licenses >> Smart Licenses >> Verify if either AnyConnect Plus or AnyConnect • 3619 **VPN** license has been enabled (if not already). 3620
- To enable license (assuming an AnyConnect license has been procured and tied to your Cisco 3621 3622 smart account), Click Edit Licenses >> Select the corresponding firewall device from the left side window "Devices without license" and move it to the right side under "Devices 3623 with license". Hit Apply. 3624
- 3625
- 3626

3628

3629

					?
Malware Threat URL	Filtering AnyConnect	Apex AnyConne	ect Plus AnyCon	nect VPN Only	
Devices without license 🔮		E	Devices with license	. (1)	
🔍 Search			占 Cisco-ASA		6
Cisco-ASA		Add			

Go to Objects menu >> Object Management >> Radius Server Group >> Add Radius
 Server Group (if not already configured)

Overview Analysis	Policies Devices Objects AMP Intelligence	Deploy 📀 System Help 🔻 admin 🔻
Object Management	Intrusion Rules	
RADIUS Server Grou RADIUS Server Group objec	P s contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.	Add RADIUS Server Group
Network	▲ Name	Value
Minterface Tunnel Zone Application Filters	No records to display	
Security Group Tag		
Time Range		
S Variable Set		

- Under Add Radius Server Group >> Enter a Name and Description >> Under Radius
 Servers in the bottom menu >> Click on + to add one.
- Under New Radius Server wizard >> Enter the IP address of the Radius Server. Shared
 Secret. Hit Save.

Nam	e:*	Mgmt-Radius			
Desc	ription:	Radius server on Mgmt AD			
Gre	New RADIUS Server	(? :	×
Ret					
Rea	IP Address/Hostname:*	10.100.2.3 Configure DNS at Threat Defense Platform Settings to	resolve hostna	me	
	Authentication Port:*	1812	(1-65535)		
	Key:*	•••••			
	Confirm Key:*	•••••			
	Accounting Port:	1813	(<mark>1-65535</mark>)		
RAI	Timeout:	10	(1-300) See	conds	
	Connect using:	Routing O Specific Interface (1)			
1		Default: Diagnostic Interface	~	0-	
	Redirect ACL:		~		
		Save	Cance		

- Next, go to **Devices** menu >> **VPN** >> **Remote** Access >> Wizard >> Add a new
- 3641 Configuration.
 3642
 3643 <u>Step 1: Policy Assignment</u>
 3644
 3645 Define a Name, Description.
 3646 Select a protocol (SSL, IPSec-IKEv2). It is possible to select both.
 3647 Move the appropriate firewall device under "Available Devices" (left-side) to "Selected
 - Devices" right-side window

Device Management NAT	VPN ► Remote Access Qo	S Platform Settings FlexCo	onfig Certifi	cates		
Remote Access VPN F	Policy Wizard					
1 Policy Assignment	2 Connection Profile	3 AnyConnect > 4 Acc	ess & Certific	ate 🔪 5 Summa	ary	
	This wizard will gui a new user-defined	de you through the required minimal s	teps to configure	the Remote Access VPN p	olicy with	1 Before You Start
	a new user-defined	connection prome.				Before you start, ensure the following configuration elements to be in place to
	Name:*	AnyconnectRemoteAccessVPN				complete Remote Access VPN Policy.
	Description:					Authentication Server Configure <u>Realm</u> or <u>RADIUS Server Group</u>
	VPN Protocols:	SSL IPsec-IKEv2				to authenticate VPN clients. AnyConnect Client Package
	Targeted Devices:	Available Devices		Selected Devices		Make sure you have AnyConnect package for VPN Client downloaded or you have
		Search		Cisco-ASA	6	the relevant Cisco credentials to download it during the wizard.
		Cisce-A5A				Device Interface
						Interfaces should be already configured or targeted <u>devices</u> so that they can be used as a security zone or interface group to enable VPN access.

3649

3651 <u>Step 2: Connection Profile</u>

• Choose Authentication Method – For instance AAA.

shbbards Reporting Summary emote Access VPN Policy Wizard Policy Assignment Of Connection Profile Onection Profile SuperStructure Connection Profile Name: Automotication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connection. Authentication Method: Authentication Server: Muthentication Server: Muthentication Server: Orecomment is tried in the order of AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pools. Use DHCP Servers Ver DHCP Servers First Address Pools IPv4 Address Pools: IPv6 Address Pools:	
Policy Assignment Image: Connection Profile Augeonnect Access & Certificate Summary Connection Profile and how address are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* AryconnectRemoteAccess/VN Connection Profile Name:* AnyconnectRemoteAccess/VN This name is configured as a connection alias, it can be used to connect to the VPW gateway Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: AAA Only (Raalmor RADIUS) Authorization Server: Use same authentication server (RaDIUS) Accounting Server: Use same authentication server (RADIUS) Client Address Assignment: Client Address Assignment: Client Paddress can be assigned from AAA server, DHCP server and IP address pools. Use DHCP Servers Use SAAA Server (RADIUS only) (Use DHCP Servers) (Use DHCP Servers) Use IP Address Pools: IPV4 Address Pools: IPV4 Address Pools: (PIH-Pool	
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* AnyconnectRemoteAccessVPN This name is configured as a connection alias, it can be used to connect to the VPN gateway. Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: AAA only (Realm or RADIUS) Authentication Server: Mgmt-Radius (RADIUS) Authorization Server: Use same authentication server (RADIUS) Accounting Server: Use same authentication server (RADIUS) Client Address Assignment: Client Praddress can be assigned from AAA server, DHCP server and IP address pools. Use AAA Server (RADIUS only) (RADIUS) Lie DHCP Servers Use DHCP Servers Use IP Address Pools: IPv4 Address Pools: IPv6 Address Pools: IPv6 Address Pools: IPv6 Address Pools:	
accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* AnyconnectRemoteAccessVPN This name is configured as a connection alias, it can be used to connect to the VPN gateway Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: AAA Only Authentication Server: Mgmt-Radius Authentication Server: Mgmt-Radius Authorization Server: Use same authentication server (RADIUS) Authorization Server: Use same authentication server (RADIUS) Client Address Assignment: Client P address can be assigned from AAA server, DHCP server and IP address pools. Use AAA Server (RADIUS only) Use BAAB Servers Use DHCP Servers Use DHCP Servers Use IP Address Pools: IPv6 Address Pools: IPv6 Address Pools: IPv6 Address Pools:	
This name is configured as a connection alias, it can be used to connect to the VPN gateway Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: Authentication Server: Mgmt-Radius Authentication Server: Use same authentication server (RADIUS) Accounting Server: Use same authentication server (RADIUS) Accounting Server: Client Address Assignment: Client Paddress can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pools. When multiple options are selected, IP address Use AAA Server (RADIUS only) Use AAA Server (RADIUS only) Use DHCP Servers Use IP Address Pools: IPv4 Address Pools: IPv6 Address Pools: IPv6 Address Pools:	5
Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: Authentication Server: Authentication Server: Mgmt-Radius Authorization Server: Use same authentication server (RADIUS) Accounting Server: Client Address Assignment: Client Address Assignment: Client Paddress can be assigned from AAA server, DHCP server and IP address pools. Use AAA Server (RADIUS only) Use DHCP Servers Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: Pv6 Address Pools: Authorization Server: Accounting Server: Accounting Server: Authorization Server: Authorization Server: Authorization Server: Accounting Server: Authorization Server: Authorization Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Authorization Server: Authorization Server: Accounting Server: Authorization Server: Authorization Server: Authorization Server: Accounting Server: Accounting Server: Accounting Server: Authorization Server: Authorization Server: Authorization Server: Authorization Server: Authorization Server: Authorization Server: Accounting Server: Authorization	
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: AAA Only Authentication Server: Mgmt-Radius (Realm or RADIUS) Authorization Server: Use same authentication server (RADIUS) Accounting Server: (RADIUS) Client Address Saignment: Client P address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is fried in the order of AAA server, DHCP server and IP address pool. (Use AAA Server (RADIUS)) Use AAA Server (RADIUS only) (Use DHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use DHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use DHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address pool. (Use AAA Server (RADIUS only)) (Use CHCP Server and IP address Pools) (Use AAA Server (RADIUS Address Pools) (Use CHCP Server (RADIUS Address Pools) (Use AAA Server (RADIUS Address Pools) (Use CHCP Server (RADIUS Address Pools) (Use CHCP Server (RADIUS (Use CHCP Server (RADIUS Server (RADIUS CHCP Server (RADIUS Server (RADIUS Server (RADIUS	
Authentication Method: AAA Only Authentication Server:* Mgmt-Radius Authorization Server: Use same authentication server Accounting Server: (RADIUS) Accounting Server: (RADIUS) Client Address Assignment: (RADIUS) Client P address and be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool. Use AAA Server (RADIUS only) Use AAA server Use IP Address Pools Use IP Address Pools IPv6 Address Pools: IPv6 Address Pools:	
Authentication Server: Mgmt-Radius (Realm or RADIUS) Authorization Server: Use same authentication server (RADIUS) Accounting Server: (RADIUS) (RADIUS) Client Address Signment: (RADIUS) (RADIUS) Client P address can be assignment: (RADIUS) (RADIUS) Client Address Assignment: (RADIUS) (RADIUS) Use same authentication server (RADIUS) (RADIUS) Client Address soginment: (RADIUS) (RADIUS) (RADIUS) (RADIUS) (RADIUS) Use AAA Server (RADIUS only) (Use DHCP Servers) (Use IP Address Pools) (IPv6 Address Pools): (IPv6 Address Pools): (IPv6 Address Pools): 	
Authorization Server: Use same authentication server Accounting Server: Client Address signment: Client IP address question assignment from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool. Use AAA Server (RADIUS only) Use DHCP Servers Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: Question and P address Pools: Pv6 Address Pools: Question and P address Pools: Pv6 Address Pv06 Address Pv0	
Accounting Server: Client Address Assignment: Client IP address assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool. Use AAA Server (RADIUS only) Use DHCP Servers Use DHCP Servers Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: Q	
Client Address Assignment: Client IP address can be assigned from AAA server, DHCP server and IP address pool. Use AAA Server (RADUS only) Use DHCP Server Use DHCP Server Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: 2000	
Client Address Assignment: Client IP address can be assigned from AAA server, DHCP server and IP address pool. Use AAA Server (RADUS only) Use DHCP Server Use DHCP Server Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: 2000	
Client IP address can be assigned from AAA server, DHCP server and IP address pool. Use AAA Server (RADIUS only) Use AAA Server (RADIUS only) Use DHCP Servers Pools Use IP Address Pools: IPv4 Address Pools: IPv6 Address Pools: IPv6 Address Pools: IPv6 Address Pools: IPv6 Address Pools:	
Use AAA Server (RADIUS only) Use DHCP Servers Use IP Address Pools IPv4 Address Pools: VPN-Pool IPv6 Address Pools:	
Use DHCP Servers Use IP Address Pools IPv4 Address Pools: IPv6 Address Pools: 2	
IPv4 Address Pools: VPII-Pool IPv6 Address Pools: Image: Content of the second	
IPv6 Address Pools:	
Group Policy	
A group Policy. A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Se or create a croup Policy object.	ct
Group Policy:* DiftGrpPolicy	
Edit Group Policy	
	Back

- Under Authentication Server, select the Radius Server configured earlier under. 3656
- 3657 Select "Use IP Address Pool", click to Create a New IPv4 Address Pool. Below image our 3658 **VPN-Pool**
- 3

'	050	
3	659	

dd IPv4 Pool			? :
Name:*	VPN-Pool		
IPv4 Address Range:*	192.168.100.10-192.168.100.20		
	Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150		
Mask:	255.255.255.0		
Description:	1]	
Allow Overrides: 🕑 Configure device ove shared across multip	errides in the address pool object to avoid IP address o le devices		object is
Override (0)			Ŧ
		12.020	

Under Group Policy >> Edit the Default Group Policy or Create a new one as per your 3663 requirement. This is the policy name to be referenced on the Radius server setup on 3664 3665 Windows. 3666 The following changes were put in our Default Group Policy 3667 3668 3669 • Under General >> VPN Protocols >> SSL • Under **General**>> **Banner** >> Enter a custom welcome message 3670 • Under **General** >> Split Tunneling >> Allow all traffic over tunnel (Split tunnel was 3671 3672 disabled)

Name:*	DfltGrpPol	icy		
Description:				
General /	AnyConnect	Advanced		
VPN Protocols		IPv4 Split Tunneling:	Allow all traffic over tunnel	
IP Address Pools Banner	5	IPv6 Split Tunneling:	Allow all traffic over tunnel	
DNS/WINS		Split Tunnel Network List Type:	Standard Access List Standard Access List	
Split Tunneling		Standard Access List:	~	
		DNS Request Split Tunneling		
		DNS Requests:	Send DNS requests as per split tunnel policy	
		Domain List:		

3675

3673

3676 • Under AnyConnect, Create a new Client Profile (if not already)

dit Group Policy		?
Name:* Dfl	GrpPolicy	
Description:		
General AnyCo	nect Advanced	
Profiles	AnyConnect profiles contains settings for the VPN client fur	onality and optional
SSL Settings	features. FTD deploys the profiles during AnyConnect clien	
Connection Settings	Client Profile:	× ()
	Standalone profile editor can be used to create a new or m profile. You can download the profile editor from <u>Cisco Soft</u>	

3677

3679

3680

3678 Under Advanced >> Session Settings >> Idle Session Timeout was set to 30 minutes

Name:*	DfltGrpP	olicy			
Description:					
General	AnyConnect	Advanced			
Traffic Filter		Access Hours:	Unrestricted	*	0
Session Sett	ings	Simultaneous Login Per User:	3	(Range 0-	-2147483647)
		Connection Time			
		Max Connection Time:		Minutes	(Range 1-4473924)
		Alert Interval:	1	Minutes	(Range 1-30)
		Idle Time			
		Idle Timeout:	30	Minutes	(Range 1-35791394)
		Alert Interval:	1	Minutes	(Range 1-30)

3681 <u>Step 3: AnyConnect:</u>

3683

• Select the AnyConnect Image for OS Supported (Windows, Linux, MacOS)

/ -	e 3	AnyConnect 4	Access & Certificate	> 5 Summar		
					AAA	
	AnyConn	ect Client Image			000	
	The VPN ga	teway can automatically dow				V connection is
1	nitiated. Mi	nimize connection setup time	by choosing the appropriate	OS for the selected pack	kage.	
	Download A	nyConnect Client packages fro	m Cisco Software Download			
	-			2	Show Re-order buttor	<u>15</u>
	U Select a	at least one AnyConnect Client	: image			
	AnyC	onnect File Object Name	AnyConnect Client Pac	kage Name	Operating System	n
	Anyco	nnect-Win-Image	anyconnect-win-4.7.010	76-webdeploy-k9.pkg	Windows	*
	Anyco	nnect-Linux-image	anyconnect-linux64-4.6.	04056-webdeploy-k9	Linux	•

• The Image files can be added manually by clicking on + icon.

Download AnyConnect Client			
Select at least one AnyC	Name:*	Anyconnect-Linux-image	
AnyConnect File Obje	File Name:*	anyconnect-linux64-4.6.04056-webdeploy-ks	Browse
	File Type:*	AnyConnect Client Image	
	Description:		
		Save	Canc

3687 <u>Step 4: Access and Certificate:</u>

3688 • Interface group/Security Zone: Select your outside interface

D.			
Re	emote Access VPN Policy Wizard		
(1) Policy Assignment $ ightarrow$ 2 Connection Profile $ ightarrow$	3 AnyConnect 4 Acce	ss & Certificate 5 Summary
			AAA
		Network Interface for Incom	
		Select or create an Interface Group connections.	or a Security Zone that contains the network interfaces users will access for VPN
		Interface group/Security Zone:*	fake_public_nccoe
			Enable DTLS on member interfaces
		Device Certificates	
		Device certificate (also called Ident certificate which is used to authent	ity certificate) identifies the VPN gateway to the remote access clients. Select a cate the VPN gateway.
		Certificate Enrollment:*	 O
	• Device Certificates: Se	elect a Name and C	Certificate can be imported manually or Clic
			÷ •
			÷ •
	to create a Self-signed (Network Interface for Incomir	Certificate. A self-	signed certificate was used in our environm
	to create a Self-signed (Network Interface for Incomir	Certificate. A self-	signed certificate was used in our environm
	to create a Self-signed (Network Interface for Incomir Select or create an Interface Group of	Certificate. A self-	signed certificate was used in our environm
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections.	Certificate. A self- ng VPN Access r a Security Zone that con fake_public_nccoe	AAA tains the network interfaces users will access for VPN
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections.	Certificate. A self- ng VPN Access r a Security Zone that con	AAA tains the network interfaces users will access for VPN
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections.	Certificate. A self- ng VPN Access r a Security Zone that con fake_public_nccoe	AAA tains the network interfaces users will access for VPN
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections. Interface group/Security Zone:*	Certificate. A self- ng VPN Access r a Security Zone that con fake_public_nccoe	AAA tains the network interfaces users will access for VPN
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections. Interface group/Security Zone:*	Certificate. A self- ng VPN Access r a Security Zone that con fake_public_nccoe Enable DTLS on memb	AAA tains the network interfaces users will access for VPN
	to create a Self-signed C Network Interface for Incomir Select or create an Interface Group or connections. Interface group/Security Zone:*	Certificate. A self- og VPN Access r a Security Zone that con fake_public_nccoe Enable DTLS on memb	tains the network interfaces users will access for VPN

Name:*	Self-Signed	
Description:		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Self Signed Certificate	~
Allow Overrides:		

3698 Step 5: Summary:

• Review the **Summary**. If all OK, click **Finish** to apply the changes.

Remote Access VPN Policy Wizard			 	
	AnyconnectRemoteAccessVPN AAA Only Mgmt-Radius Mgmt-Ra	 WAT Exemption INAT is enabled on the targeted devices, you must define a <u>NAT Policy</u> to exempt VPN traffic. ONS Configuration Torsolve hostname specified in AAA Servers or CA Servers, configure DNS using <u>FleeConfig</u> Policy on the targeted devices. OPT Configuration SL, will be enabled on port 443. Please ensure that these ports are not used in <u>NAT Policy</u> or other services before deploying the configuration. Make sure to add interface from targeted devices to SecurityZone object 'fake_public_nccce' 		

3701 <u>Further Configuration Requirements:</u>

Once the Wizard is completed, the following configuration requirements need to be done for RAVPN to work on all device targets:

Access Control Policy: An ACL rule must be defined to allow VPN traffic on to whichever
 network segments you wish to permit.

3706

- 3707 The image below shows an ACL configured to allow VPN traffic from outside to only a couple
- 3708 of internal servers in the Process Control system over Remote Desktop Port 3389.

	Source	Destination	Selection
Zones	Outside	Inside	
Networks	VPN_Pool (Network)	HMI Server (Host) Workstation (Host)	
Ports	Any	3389 TCP	
Action			Allow
Inspection			Enabled. Balanced connectivity over Security.

			CEL Doli	Nono			I	lonti	ty Dolicy: Nono		
diting Ru	ıle - VPN-Ru	le									1
Name VPI	N-Rule				🕑 Enable	d	Move				
Action 🖌	Allow			• • • 26	ı D						
Zones	Networks	VLAN Tags	🛆 Users	Applications	Ports	🛆 URLs	SGT/ISE Attributes		Inspection Lo	gging	Comment
vailable N	letworks 🖒		٢		Source N	etworks (1)			Destination Networks (2)		
💫 Search l	by name or value	9			s	ource	Original Client		PCS-HMI		
Net	works	Geolocati	on		VPN-P	ool		8	PCS-Workstation		
any any-ipv4 any-ipv4 CRS-NA DMZ-Ne DMZ-Se Esxi-Hos Graylog	6 T-IP vtwork vrvers st.mgmt			Add To Source Networks Add to Destination							
Hyper-V			•		Enter an	IP address	Ad	ld	Enter an IP address		Ad
нуper-v	Servers		· ·						Enter an IP address		Can

3711

lame VPN-Rule				Enabled	Move			
Allow			• U D 2 t	1 D				
Zones Networks	VLAN Tags	🛆 Users	Applications	Ports 🛆 URLs	SGT/ISE Attributes	Inspection	Logging	Comments
vailablePorts 🔮		٢		Selected Source Port	s (0)	Selected Destination F	Ports (1)	
👃 Search by name or value				any		ADP-Windows		
AOL AOL DINS_over_TCP DINS_over_UDP FTP HTTP HTTPS IMAP			Add to Source Add to Destination					
✤ LDAP♠ NetBIOS-TCP		-		Protocol TCP (6)	Port Enter Add	Protocol	Y Port	Enter a A

Device Certificate: Associate the certificate created earlier with the Firewall device.

	Analysis	Policies	Devices	Objects	AMP I	ntelligence						Deploy	System	Help 🔻	admin v
Device Manag	gement	NAT VP	PN ▼ Qo	S Platforn	n Settings	FlexCon	ig Certificates								
														\odot	Add
Name				Do	omain		Enrollment Type	Status							
4 🗐 Cisco-A	SA														
Self-Sig	ned			Add Ne	ew Certifi	cate					? X			P	Φ 🖥
				Add a ne identify	ew certificate certificate.	e to the devic	e using cert enrollme	nt object which	is used to	generate C/	A and				
				Device*:	:	Cisco	-ASA		•						
				Cert Enr	ollment*:	Self-	Signed		~ 🔾						
				Cert Enr	ollment Deta	ails:									
				Name:		Self-S	Signed								
				Enrollme	ent Type:	Self-	Signed								
				SCEP UF	RL:	NA									
									Add	Can	el				

- 3718 Create a NAT Exemption rule: If NAT is enabled on the firewall, you must define a NAT rule
- 3719 to exempt VPN traffic.
- 3720 Go to Devices Menu >> NAT >> Select <NAT Policy> >> Add Rule.
- 3721 Below images show a NAT Rule created to exempt VPN Traffic

NAT Rule: Ma	nual NAT Rule	*	Insert:	In Category	▼ NAT Rules Before ▼
Type: Sta	itic	👻 🗹 Enab	le		
Description:					
Interface Objects Tr	anslation PAT F	ool Advanc	ed		
Available Interface Object	ts C		Source Interface Object	cts (1)	Destination Interface Objects
🔍 Search by name			击 inside	i	📩 fake_public_nccoe
🏭 dmz					
击 fake_public_nccoe		Add to Source			
🚠 inside					
👬 management		Add to Destination			
击 outside					

NAT Rule:	Manual NAT Ru	ile 💙	Ins	sert:	In Category	▼ NAT Rules B	efore 💙	
Type:	Static	~	🕑 Enable					
Description:								
Interface Objects	ranslation	PAT Pool	Advanced					
Original Packet					Translated Packet			
Original Source:*	PCS-Netv	vork		~	Translated Source:	Address		~
Original Destination:	Address			×		PCS-Network		~
original Destination.								
	VPN-Pool			× (Translated Destination:	VPN-Pool		*
Original Source Port:				~	Translated Source Port:			~
Original Destination Port	t:			~ C	Translated Destination Port:			~

3725

Edit NAT Rule					? ×
NAT Rule:	Manual NAT Rule	Insert:	In Category	▼ NAT Rules Before	*
Туре:	Static	Enable			
Description:					
Interface Objects	Translation PAT Pool	Advanced			
Translate DNS replies	s that match this rule				
Fallthrough to Interfa	ace PAT(Destination Interfac				
IPv6					
Net to Net Mapping					
Do not proxy ARP on	Destination Interface				
Perform Route Looku	p for Destination Interface				
Unidirectional					
				0	K Cancel

3726

3728 <u>Client Connection:</u>

Clients can use a web browser to connect to the Outside interface of the device. Once they login,the AnyConnect image is automatically downloaded or updated. After that, clients can connect

3731 using the AnyConnect software installed on their device, which already has the AnyConnect

3732 XML profile with all the parameters for the RA VPN connection.

Accessing the outside interface should give a similar page as shown below. Enter the Active
 Directory user credentials created earlier to Logon.

🖻 🖅 🗖 129.6.1.5	× + ~ -		\times
\leftrightarrow \rightarrow \odot \Leftrightarrow	▲ Certificate error https://129.6.1.5/+CSCOE+/logon.html#f 🛄 📩 🏂	L B	
	Group AnyconnectRemoteAccessVPN \ Username vpnuser01 Password . Logon		

• Download the Client software and Install it.

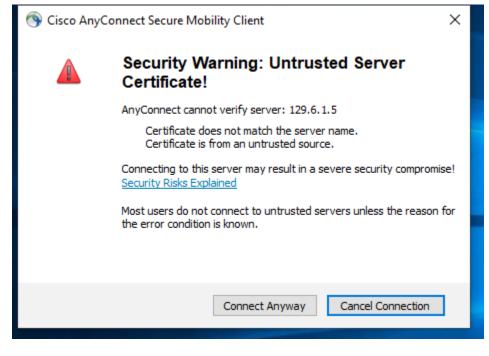
E ←□ AnyConnect Installation × + ∨	<u> </u>		\times
\leftarrow \rightarrow \circlearrowright \bigtriangleup Certificate error https://129.6.1.5/CACHE/stc/1/index.html \square \bigstar	l-	Ŕ	
Download & Install			
Download Cisco AnyConnect Secure Mobility Client and install it on your computer. Download for Windows			
Instructions			
anyconnect-win-4.7.01076-core-vpn- webdeploy-k9.exe finished downloading. Run Open folder View do	wnload	s ×	~

3738

3741

3737

If using a self-signed certificate as in our case, you will be presented with this warning. Hit
 Connect Anyway



• Enter the AD user credentials

		Cisco AnyConne	ct 129.6.1.5		×	
		Group: Username: Password:	AnyconnectRemot vpnuser01	eAccessVPN		
			ОК	Cancel		
3744						
3745 3746 3747	• When c	onnected, a pop	-up message a	opears showing	g the Client a	s Connected
	4	Conn	AnyConne ected: 129.0	5.1.5	Client	nc
		CISCO #	AnyConnect Se	cure mobility	Client	ed
				Build 17/63.rs	crelease.180	
			مج	^ 🖏 🔩	3:21 PM	E.
3748 3749			~		A/17/3010	
3750						

- Upon establishing the connection, the two servers in Process Control System whitelisted
- arlier in the ACL Rule were accessed using RDP to perform Remote Maintenance.

r								_	
		Noodhead DeviceNet Ne	twork Analyzer					_	
e	File View	Setup Capture Help							
	🖻 🔒 🗉	X 💷 🖇 🎟 📥	🕨 🌮 😼 Can Dn Hex 🚟 [8 A A 8	8				
	Index	Timestamp	Date/Time	MAC ID	Group	Msg I	D CAN ID	Size	Data
	1	159885.374	04/17/19 07:30:37.285374	40	2	5	545	4	00 00 00 0
	2	159886.029	04/17/19 07:30:37.286029	39	1	15	3E7	4	6A 9A 3E
e	3	159886.685	04/17/19 07:30:37.286685	40	1	15	3E8	4	72 0D 57 4
	4	159887.373	04/17/19 07:30:37.287373	41	2	5	54D	4	00 00 00 0
	5	159888.077	04/17/19 07:30:37.288077	42	2	5	555	4	FE 2D 7E 4
	б	159888.725	04/17/19 07:30:37.288725	41	1	15	3E9	4	59 F1 2F 4
	7	159889.437	04/17/19 07:30:37.289437	42	1	15	3EA	4	00 00 00 0
5	8	159890.069	04/17/19 07:30:37.290069	43	2	5	55D	4	C7 8E 5A
	9	159890.741	04/17/19 07:30:37.290741	44	2	5	565	4	4C 81 C6
	10	159891.453	04/17/19 07:30:37.291453	43	1	15	3EB	4	00 00 00 0
	11	159892.157	04/17/19 07:30:37.292157	44	1	15	3EC	4	00 00 00 0
	12	159892.813	04/17/19 07:30:37.292813	45	2	5	56D	4	BE 54 7E 4
	13	159893.525	04/17/19 07:30:37.293525	46	2	5	575	4	00 00 00 0
	14	159894.221	04/17/19 07:30:37.294221	45	1	15	3ED	4	00 00 00 0
	15	159894.924	04/17/19 07:30:37.294924	46	1	15	3EE	4	00 00 00 0
<	16	159895.581	04/17/19 07:30:37.295581	47	2	5	57D	4	82 38 22 4
	17	159896.244	04/17/19 07:30:37.296244	48	2	5	585	4	40 6D 1C
	18	159896.948	04/17/19 07:30:37.296948	47	1	15	3EF	4	00 00 00 0
	19	159897.645	04/17/19 07:30:37.297645	48	1	15	3F0	4	00 00 00 0
	20	159898.284	04/17/19 07:30:37.298284	49	2	5	58D	4	36 DF 3D
	21	159898.988	04/17/19 07:30:37.298988	50	2	5	595	4	00 00 00 0
	22	159899.676	04/17/19 07:30:37.299676	49	1	15	3F1	4	00 00 00 0
	23	159900.373	04/17/19 07:30:37.300373	50	1	15	3F2	4	00 00 00 0
	24	159901.004	04/17/19 07:30:37.301004	51	2	5	59D	4	CA C7 32
	75	150001.684	04/17/10 07:20:27 201694	57	7	5	545	А	FF (7 83 /
	<u> </u>								
					RX: 5,597,253		HEX DeviceNet	Filter OFF	ER: 0 N

3754 3755 3756

3758 <u>Session Termination</u>

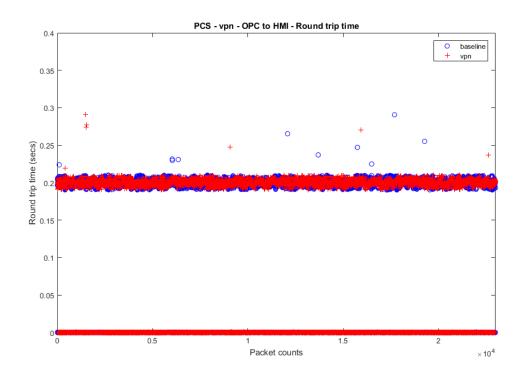
- 3759
- To terminate a VPN Session, log on to the Cisco FMC Web interface, go to **Analysis** >> **Users**
- 3761 >> Active Sessions. Select the session and click Logout
- 3762 3763

Overview Anal	ysis Policies	Devices Obje	cts Al	MP Intelli	gence					
Context Explorer	Connections 🔻	Intrusions 🔻	Files 🔻	Hosts 🔻	Users ► Active	Sessions	Correlat	ion 🔻 🛛 Ad	vanced 🔻	Search
Active Sess Table View of Activ	e Sessions > Activ	<u>ve Sessions</u>								
Jump to 🔻										
_ <mark>▼ Login</mark>	Time X La	ast Seen 🗙	<u>User</u> X			<u>Authentica</u> <u>Type</u>	ntion X	Current IP	× <u>R</u> e	alm ×
↓ Ø <u>2019-04</u>	<u>-19 15:25:16</u> <u>20</u>	<u>19-04-19 15:25:16</u>	E Discov	ered Identitie	<u>vpnuser01 (LDAP)</u>	VPN Authent	<u>tication</u>	<u>192.168.1</u>	<u>100.10</u> <u>Dis</u>	covered Ider
View	Displaying	row 1 of 1 rows			ected VPN sessions					
View All			Y VP	N. Other ses	sions will be remov	ved from the Contir		sions list. Cancel		

- ----
- 3766 References:
- 3767 [1] Cisco AnyConnect VPN
- 3768 https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-
- 3769 <u>client/at_a_glance_c45-578609.pdf</u>
- 3770 [2] Cisco ASA VPN User Authentication:
- 3771 https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-
- 3772 <u>firewalls/117641-config-asa-00.html</u>
- 3773
- 3774

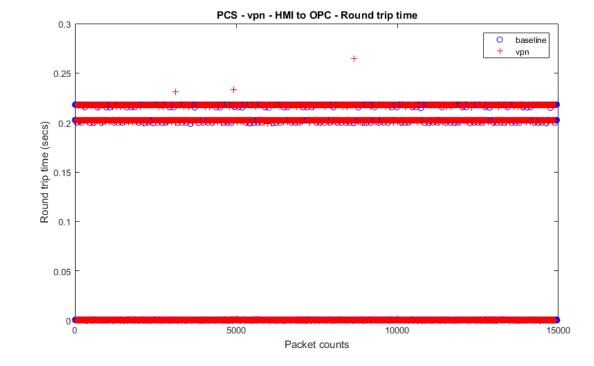
3775 **4.8.6** Highlighted Performance Impacts

- 3776 The following performance measurement experiment was performed for the Cisco AnyConnect
- 3777 VPN tool while the manufacturing system was operational:
- 3778 Experiment PL012.1- VPN connection from testbed LAN
- 3779 In this experiment, a remote user was accessing the HMI from a remote computer through the
- 3780 VPN connection. A remote computer was first connected to the testbed LAN through the VPN,
- then used the Remote Desktop to connect to the HMI computer to access the HMI screen.
- 3782 Although there was slightly increased network traffic between the testbed LAN and the PCS
- 3783 system due the Remote desktop session, there was no significant performance impact observed in
- the PCS system. The packet round trip time between the HMI and OPC remained mostly
- 3785 constant with and without the VPN connection.



3786

3787
3788Figure 4-12 Plot of packet round trip time from OPC to HMI computer during the use of VPN connection from
a remote computer

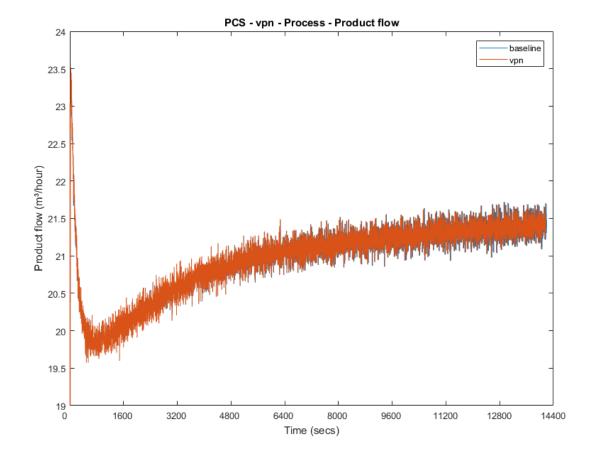


3790
3791Figure 4-13 Plot of packet round trip time from HMI to OPC computer during the use of VPN connection from
a remote computer

3792

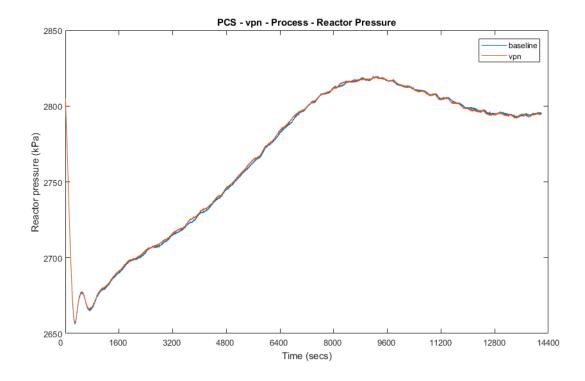
- 3793 The manufacturing process also remained stable without any significant performance impact
- 3794 observed. The reactor pressure and product flow rate remained constant with and without the

3795 VPN connection.



3797 3798

Figure 4-14 Manufacturing process product flow rate during the use of VPN connection from a remote computer



3799

3800
3801Figure 4-15 Manufacturing process reactor pressure during the use of VPN connection from a remote
computer

- 3802 **4.8.7** Link to Entire Performance Measurement Data Set
- 3803 Cisco VPN KPI data
- 3804 Cisco VPN measurement data

3805 **4.9 Microsoft Active Directory**

3806 **4.9.1 Technical Solution Overview**

3807 Active Directory (AD) is a directory service developed by Microsoft for Windows 3808 domain networks. A directory is a hierarchical structure that stores information about objects on 3809 the network. A directory service, such as Active Directory Domain Services (AD DS), provides 3810 the methods for storing directory data and making this data available to network users and 3811 administrators. For example, AD DS stores information about user accounts, such as names, 3812 passwords, phone numbers, and so on, and enables other authorized users on the same network to 3813 access this information. A server running Active Directory Domain Services (AD DS) is called 3814 a domain controller. It authenticates and authorizes all users and computers in a Windows 3815 domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory uses Lightweight Directory Access Protocol (LDAP) 3816 versions 2 and 3, Microsoft's version of Kerberos and DNS.²⁰ 3817

3818 Points to consider

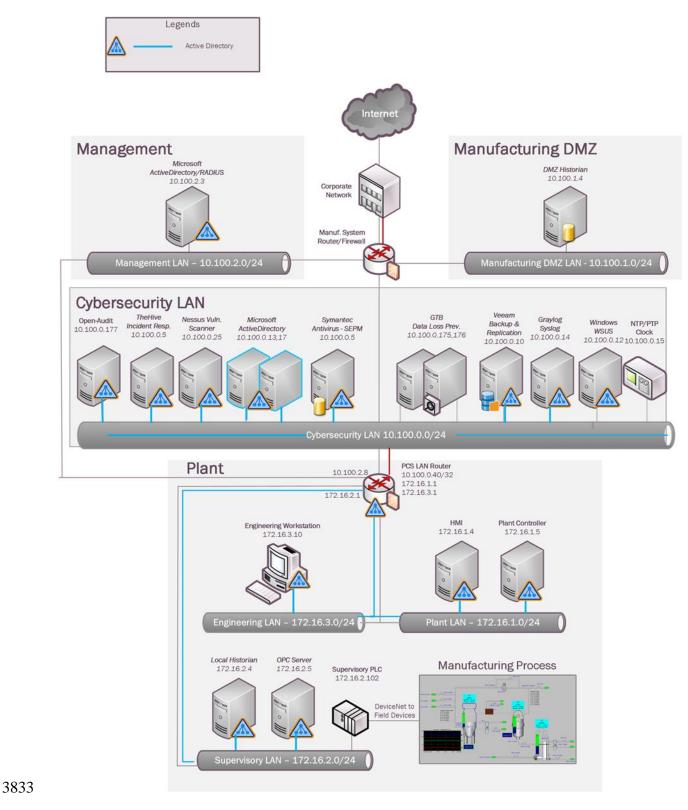
3819	3819 •	Cost	Cost of infrastructure can get high.													
2020		р	•		· •			1	• ,	•	n ,	•	1	1 / 11	1 1	•

- Requires expertise to setup and maintain. Setup involves detailed planning.
- It is prone to being hacked.
- 3822
- 3823 **4.9.2** Technical Capabilities Provided by Solution
- 3824 Microsoft Active Directory provides components of the following Technical Capabilities3825 described in Section 6 of Volume 1:
- Credential Management
- Authentication and Authorization

3828 **4.9.3** Subcategories Addressed by Implementing Solution

- 3829 PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3
- 3830
- 3831

²⁰ https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-servicesoverview



3832 4.9.4 Architecture Map of Where Solution was Implemented

3834 **4.9.5** Installation Instructions and Configurations

3835 Setup:

3836 Our setup consists of two separate Active Directory domain environments; one for the

3837 Cybersecurity -LAN network and other for the Management network. For security reasons, The

3838 AD domain in the Cybersecurity LAN network is separate from the domain that's in the

3839 Management network. A pair of Domain Controllers (DC) running on Windows 2012 R2 were

3840 setup in the Cybersecurity LAN network for authenticating Windows/Linux devices and another

3841 separate DC on Windows 2012 R2 was setup in the Management network for authenticating

3842 VPN users and network devices such as boundary routers. This DC in the Management network

is used in conjunction with a Windows NPS (Radius) server for authenticating the networkdevices.

Hostname	IP address	Roles	Domain Name
LAN-AD	10.100.0.17	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
LAN-AD02	10.100.0.13	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
Mgmt-AD	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

3845

3846 **Installation:**

Below are high level instructions for installing Active Directory services (ADDS) on a
 Windows 2012 R2 server.

• It is recommended to have 2 servers running AD for redundancy. Ensure the servers are up to date with patches and have meaningful hostnames as per their role. Begin by configuring a

3851 static IP address on the network interface of your server. Since the server will also act as

3852 DNS server, for DNS server field you can use local host address 127.0.0.1

Internet Protocol Version	4 (TCP/IPv4) Properties						
General							
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.							
Obtain an IP address automatical	у						
Use the following IP address:							
IP address:	10 . 100 . 0 . 17						
Subnet mask:	255.255.255.0						
Default gateway:	10 . 100 . 0 . 1						
Obtain DNS server address autom	natically						
 Use the following DNS server add 	resses:						
Preferred DNS server:	127.0.0.1						
Alternate DNS server:							
Validate settings upon exit Advanced							
	OK Cancel						

- Launch "Server Manager" and click on "Add Roles and Features"
- 3855

	Serve	er Manager
Cor •• Dashb	oard	🕶 🗭 🚩 Manage Tools View Help
🔛 Dashboard	WELCOME TO SER	VER MANAGER
 Local Server All Servers File and Storage Services 		1 Configure this local server
	QUICK START	2 Add roles and features
	WHAT'S NEW	3 Add other servers to manage
		4 Create a server group5 Connect this server to cloud servic
		Hide

3859 • Click "Next" at the first page

00.00	
3860	
5000	

a	Add Roles and Features Wizard
► Before you begin Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Image: Comparison of the computing needs of your organization, such as sharing documents, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again. To continue, click Next.
	< Previous Next > Install Cancel

3861 3862 3863

• Select "Role Based or Feature Based Installation" under Installation Type

3864

	Add Roles and Features Wizard				
elect installatio	on type	DESTINATION SERVER SymTest.lan.lab			
Before You Begin	Select the installation type. You can install roles and features on a run machine, or on an offline virtual hard disk (VHD).	ning physical computer or virtual			
Installation Type					
erver Selection	Role-based or feature-based installation				
	Configure a single server by adding roles, role services, and feature	25.			
	Remote Desktop Services installation				
onfirmation	Install required role services for Virtual Desktop Infrastructure (VDI or session-based desktop deployment.) to create a virtual machine-base			

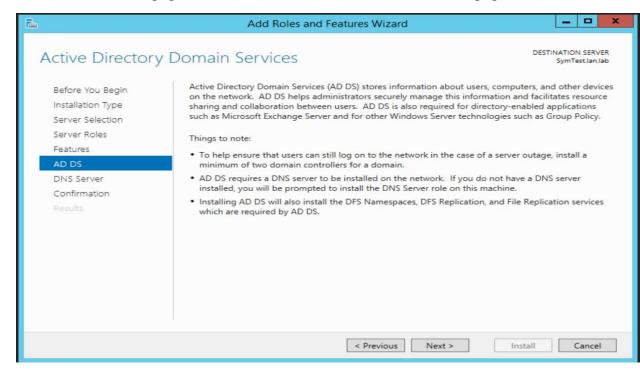
• Select "Active Directory Domain Services" and "DNS Server" to install. Click Next

	Add Roles and Features Wizard	
elect server ro	les	DESTINATION SERVER SymTest.lan.lab
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection		Active Directory Domain Services
Server Roles	Active Directory Certificate Services	(AD DS) stores information about
eatures	Active Directory Domain Services	objects on the network and makes this information available to users
	Active Directory Federation Services	and network administrators. AD DS
	Active Directory Lightweight Directory Services	uses domain controllers to give
NS Server	Active Directory Rights Management Services	network users access to permitted resources anywhere on the network
onfirmation	Application Server	through a single logon process.
esults	DNS Server	
	Fax Server	
	File and Storage Services (1 of 12 installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Desktop Services	
	v	
	< Previous Nex	kt > Install Cancel

3869

• Under "Features", leave the default options selected and click Next.

Select features		DESTINATION SERVE SymTest.lan.la	
Before You Begin Installation Type	Select one or more features to install on the selected server.	Description	
Server Selection Server Roles	INET Framework 3.5 Features INET Framework 4.5 Features (2 of 7 installed)	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for	
Features AD DS DNS Server Confirmation Results	▷ Background Intelligent Transfer Service (BITS) □ BitLocker Drive Encryption □ BitLocker Network Unlock	building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and	
	BranchCache Client for NFS Data Center Bridging	secure communication, and provid the ability to model a range of business processes.	
	Direct Play Enhanced Storage Failover Clustering		
	Group Policy Management		



3874

3873

3871

• Verify your settings on the "Confirmation" page. Click Install to proceed.

a	Add Roles and Features Wizard	- 🗆 X
Confirm installati	on coloctions	IATION SERVER SymTest.lan.lab
Before You Begin	To install the following roles, role services, or features on selected server, click Install.	
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on this page because	
Server Roles	been selected automatically. If you do not want to install these optional features, click Pre- their check boxes.	vious to clear
Features		
AD DS	Active Directory Domain Services	Ê
DNS Server	DNS Server	
Confirmation	Group Policy Management	
Results	Remote Server Administration Tools Role Administration Tools	
	AD DS and AD LDS Tools	=
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	Active Directory Administrative Center	
	AD DS Snap-Ins and Command-Line Tools	~
	Export configuration settings Specify an alternate source path	
	< Previous Next > Install	Cancel

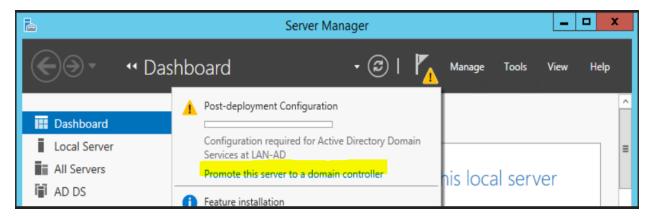
3876

3879

The installation process will run and will show an "Installation succeeded" message upon
 completion. Hit Close button.

b	Add Roles and Features Wizard	_ _ ×
Installation prog	gress	DESTINATION SERVER
	View installation progress	
	1 Feature installation	
	Configuration required. Installation succeeded on LAN-AD.	
	Active Directory Domain Services	^
AD DS	Additional steps are required to make this machine a domain controller.	
	Promote this server to a domain controller	
	DNS Server	=
Results	Group Policy Management Remote Server Administration Tools	-
	Role Administration Tools	
	AD DS and AD LDS Tools	
	Active Directory module for Windows PowerShell AD DS Tools	
	Active Directory Administrative Center	~
	You can close this wizard without interrupting running tasks. View task pro page again by clicking Notifications in the command bar, and then Task D Export configuration settings	
	< Previous Next > Clo	Cancel

3880 > Launch "Server Manager" again and click on "Promote this server to a domain 3881 controller"



3882

3886

- On the "Deployment Configuration" step, select "Add a new forest" as this would be a new
- domain controller in a new forest. Mention a Root Domain name as applicable to yourenvironment.

	Active Directory Domain Services C	Configuration Wizard	_ D X
Deployment Conf	iguration		TARGET SERVER LAN-AD
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment operation Add a domain controller to an existin Add a new domain to an existing for Add a new forest Specify the domain information for this of Root domain name:	est	
	More about deployment configurations	evious Next > Install	Cancel

• Set a Directory Services Restore Mode password in the next step. Click Next

Oomain Controll	er Options		TARGET SEI
Deployment Configuration	Select functional level of the new	forest and root domain	
Domain Controller Option	s		
DNS Options	Forest functional level:	Windows Server 2012 R2	•
Additional Options	Domain functional level:	Windows Server 2012 R2	•
Paths	Specify domain controller capabi	lities	
Review Options	✓ Domain Name System (DNS)		
Prerequisites Check	Global Catalog (GC)	arbeit # beit	
Installation	Read only domain controller	(RODC)	
	Type the Directory Services Resto	ore Mode (DSRM) password	
	Password:		
	Confirm password:		

• Under "DNS Options" leave the default options selected. Click Next

a	Active Directory Domain Services Configuration Wizard		X
DNS Options		TARGET SER LAN	RVER I-AD
A delegation for this DN	IS server cannot be created because the authoritative parent zone cannot be found Sho	ow more	×
Deployment Configuratio Domain Controller Option	Specify DNS delegation options		
DNS Options	Create DNS delegation		
Additional Options			
Paths			

3892

• Under "Additional Options", confirm the NETBIOS domain name. Click Next.

B	Active Directory Domain Services	Configuration Wizard	_ 🗆 🗙
Additional Optior	IS		TARGET SERVER LAN-AD
Deployment Configuration Domain Controller Options DNS Options	Verify the NetBIOS name assigned to t The NetBIOS domain name:	he domain and change it if necessary LAN	
Additional Options			
Paths			
Review Options			
Prerequisites Check			
Installation			
Results			

- 3894
- Under "Paths", leave the default folder paths as it is. Click Next

a	Active Directory Domain Services (Configuration Wizard	_ 🗆 X
Paths			TARGET SERVER LAN-AD
Deployment Configuration Domain Controller Options	Specify the location of the AD DS databa	ase, log files, and SYSVOL	
DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths	SYSVOL folder:	C:\Windows\SYSVOL	
Review Options			
Prerequisites Check			
Installation			
Results			

3897

• On the "**Review Options**" page, confirm all the settings and click **Next**.

Review Options Review your selections: Deployment Configuration Configure this server as the first Active Directory domain controller in a new forest. DNS Options Configure this server as the first Active Directory domain controller in a new forest. DNS Options Configure this server as the first Active Directory domain controller in a new forest. Paths Configure this server as the first Active Directory domain controller in a new forest. Prerequisites Check The NetBIOS name of the domain: LAN Installation Forest Functional Level: Windows Server 2012 R2 Domain Functional Level: Windows Server 2012 R2 Domain Functional Level: Windows Server 2012 R2 Display Create DNS Delegation: No These settings can be exported to a Windows PowerShell script to automate additional installations	la /	Active Directory Domain Services Configuration Wizard	×
	Review Options Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation	TARGET SE LA Review your selections: Configure this server as the first Active Directory domain controller in a new forest. The new domain name is "LAN.LAB". This is also the name of the new forest. The NetBIOS name of the domain: LAN Forest Functional Level: Windows Server 2012 R2 Domain Functional Level: Windows Server 2012 R2 Additional Options: Global catalog: Yes DNS Server: Yes	N-AD
More about installation options		additional installations View scrip	ət 🗌

3899

3901

• On the "**Prerequisites Check**", click Install to launch the installation process.

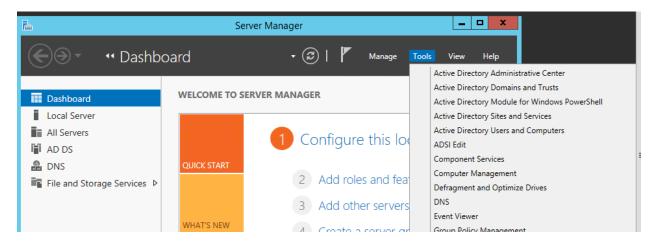
a	Active Directory Domain Services Configuration Wizard
Prerequisites Che	ck TARGET SERVER LAN-AD
 All prerequisite checks pass 	sed successfully. Click 'Install' to begin installation. Show more
Deployment Configuration Domain Controller Options	Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
DNS Options	Rerun prerequisites check
Additional Options	 View results
Paths Deview Options	Windows Server 2012 R2 domain controllers have a default for the security setting
Review Options Prerequisites Check	named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
Installation Results	For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?LinkId=104751).
	A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "LAN.LAB". Otherwise, no action is required.
	1 If you click Install, the server automatically reboots at the end of the promotion operation.
	More about prerequisites
	< Previous Next > Install Cancel

3904

The installation process will now run displaying the Progress bar. Upon completion, the ٠ server should auto reboot.

2	Active Directory Domain Services Configuration Wizard
Installation	TARGET SERVER LAN-AD
Deployment Configuration	Progress
Domain Controller Options	Securing machine\software\microsoft\enterprisecertificates
DNS Options	 View detailed operation results
Additional Options	Windows Server 2012 R2 domain controllers have a default for the security setting named
Paths	"Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
Review Options	For more information about this setting, see Knowledge Base article 942564 (http://
Prerequisites Check	go.microsoft.com/fwlink/?LinkId=104751).
Installation	A delegation for this DNS server cannot be created because the authoritative parent zone
Results	cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "LAN.LAB".

3905 Upon reboot, login with domain administrator credentials. Open "Server Manager" and click ٠ 3906 on "Active Directory Users and Computers" under Tools to manage your AD.



Configurations: 3908

3909 All windows systems were domain joined to the AD domain in the Cybersecurity LAN 3910 network. The initial domain join process is a onetime task and involves a system restart. In 3911 addition to authentication piece, the Domain Controllers also have DNS role installed. They 3912 also act as internal DNS servers. Any system that is joined to AD, will automatically create a 3913 DNS record for itself. For any system that isn't joined to AD such as a switch or a router the 3914 DNS record for these would have to be manually created. 3915 3916

- The procedure to integrate or join Windows machines to AD can be found here.
- 3917

- Once the machines were domain joined, different user accounts with varying levels of privileges were provisioned depending on the role i.e. machine operators, process owners and service accounts. On Windows systems, the accounts used by the process owners were granted administrator privileges on each Windows system by adding them to the local Administrators group while the operator user accounts were only granted "Remote Desktop" rights. The individual user accounts are subjected to a password policy whereas the service accounts are set to not expire.
- 3925

On the OPC server, we are running a Matrikon OPC server. The Microsoft Distributed
 Component Object Model (DCOM) service plays a vital role in integration the OPC server
 with AD. Having the correct DCOM settings in place when using AD is critical for plant
 operations. We have followed the steps documented in this Matrikon OPC guide ²¹ to apply
 the necessary DCOM settings. Please refer to the section below "OPC Server DCOM
 Configuration" for our settings.

- 3932
- For using AD authentication against network devices, we leveraged Microsoft Network
 Policy Services (NPS) to use as a Radius server along with AD DS. Within the Radius server,
 a connection request policy and a network policy was created for each network device.
 Please refer to the section below "Radius Server Setup"
- A physical network connection was made to the Management port of the Boundary Firewall This port was then assigned a static IP address from the Management subnet on each device so that it could communicate with the above Radius and AD server. Typically, each network device has an option to configure Radius authentication. In addition, we enabled the auditing feature on the DC to track for successful/failed logins. Once the setup is done, you should be able to use AD user accounts to login to your network devices.

OPC Server DCOM Configuration

- 3945 Pre-requisites:
- All windows systems participating need to be domain joined to the AD server.
- Ensure all systems are getting their time synced from the AD server and verify the time on
 each server is consistent with the time on the AD (Domain Controller). Time sync is
 critical.
- Verify TCP port 135 is open between all OPC clients and the OPC server.
- 3951 Shown below are the changes implemented

²¹ Matrikon OPC DCOM Setup: <u>https://www.matrikonopc.com/downloads/1128/whitepapers/index.aspx</u>

- Created 2 domain users "opcadmin" and "opcuser" in our AD. The "opcadmin" will be the
- admin user. The other "opcuser" will be treated as a non-admin user and is optional to
 configure. Add the opcadmin user to the Local Administrators group on the OPC Server and
 client.
- 3956
- 3957 Systems taking part in the OPC setup:
- 3958

Hostname	IP address	Roles	Administrators
OPC Server	172.16.2.5	OPC_Server	opcadmin
Controller	172.16.1.5	OPC Server + Client	opcadmin, opcuser

For example: Below is a snap from one of the OPC clients.

lame	Descrip	ption		
Administrators	Admin	nistrators have com	plete an	
Backun Oner	Administrators P General	roperties inistrators Administrators ha to the computer/ gent User ator hain Admins admin	ave complete and unres	up membership

3961

On the OPC Client, make the following changes to DCOM properties. Launch the "Control Panel >> Administrative Tools >> Component Services snap-in to open the DCOM console. Alternatively, you can also run "dcomcnfg" (without quotes) command from command prompt to launch the DCOM snap-in.

• Expand Console Root > Component Services > Computers, Right-click My Computer and then click **Properties**. Ensure the settings are as follows

and then click **Properties**. Ensure the settings are as following the setting of the setting of

Default Protocols	COM Security	MSDTC
General	Options	Default Properties
Enable Distributed CO	M on this computer	
Enable COM Internet	Services on this compute	er
efault Distributed COI	M Communication Propert	ties
he Authentication Le	vel specifies security at th	ne packet level.
Default Authenticatio	an Level	
Connect		•
who is calling them, an	el specifies whether appli id whether the application ity.	
who is calling them, an	nd whether the application ty.	
who is calling them, an using the client's identi Default Impersonatio Identify Security for reference 1	nd whether the application ty.	 can do operations if authentication is used
who is calling them, ar using the client's identi Default Impersonatio Identify Security for reference I and that the default im	nd whether the application ity. In Level:	 can do operations if authentication is used nonymous.
who is calling them, ar using the client's identi Default Impersonatio Identify Security for reference I and that the default im	nd whether the application ity. In Level: tracking can be provided personation level is not a	 can do operations if authentication is used nonymous.
who is calling them, ar using the client's identi Default Impersonatio Identify Security for reference I and that the default im	nd whether the application ity. In Level: tracking can be provided personation level is not a	 can do operations if authentication is used nonymous.
who is calling them, ar using the client's identi Identify Security for reference I and that the default im Provide additiona	id whether the application ity. In Level: tracking can be provided personation level is not an al security for reference tra	 can do operations if authentication is used nonymous.
who is calling them, ar using the client's identi Default Impersonatio Identify Security for reference I and that the default im	id whether the application ity. In Level: tracking can be provided personation level is not an al security for reference tra	 can do operations if authentication is used nonymous.

3969 3970

3971

Click on "COM Security" tab. Under "Access Permissions" >> "Edit Limits" button >>
 Add the opcadmin user to the list and check on the Allow boxes for both "Local Access" and
 "Remote Access" categories. You can add the "opcuser" as well if needed and grant it
 Allow permission for only "Local Access".

General	Options	Default	Properties
Default Protocols	COM Se	ecurity	MSDTC
cess Permissions			
Access Permission			2
Security Limits			
Group or user name	ec.		
& Everyone			
👗 opcadmin (LA)	N\opcadmin)		
👗 opcuser (LAN)	(opcuser)		
🞎 Performance L	og Users (FGS-6	1338CH\Perform	nance Log I
Stributed CO		338CH\Distribut	ed COM U:
Sector Distributed CO	IM Users (FGS-61	338CH\Distribut	ed COM U:
See Distributed CO			•
See Distributed CO		Add	
Permissions for opc			•
•		Add	Remove
Permissions for opc		Add	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access		Add (Allow	Remove
Permissions for opc Local Access	m admin	Add	Remove

- Under "Access Permissions" >> "Edit Default" button >> Ensure that "<server-
- name>\Administrators" group has all the boxes checked. The opcadmin user was made part
 of this Administrators group earlier.
- 3980 If you are adding the **opcuser**, grant it Allow permissions for "Local Access" only.

Default Security		
Group or user names:		
SELF		
SYSTEM		
Sopcuser (LAN\opcuser)		
& Administrators (FGS-61338C	H\Administrators)	
	Add	Remove
Permissions for Administrators	Add	Remove Deny
Permissions for Administrators		
	Allow	
Local Access	Allow	
Local Access	Allow	
Local Access	Allow	

- Under the "Launch and Activation Permissions" >> "Edit Default" button >> ensure the
- 3983 "Administrators" group has ALLOW Permissions for all 4 categories. The other "opcuser"
 3984 should have ALLOW only for "Local Launch"

General	Options	Defau	It Properties
Default Protocols	COM S	ecurity	MSDTO
Launch and Acti	vation Permission		8
Default Security			
Group or user	names:		
SYSTEM			
	LAN\opcuser)	A destruction of the	
	ators (FGS-61338CH\ CTIVE	Ruministratorsj	
			14
	[Add	Remove
Permissions for	r Administrators	Add Allow	Remove
Permissions for			
Local Laund Remote Lau	ch Inch	Allow V V	Deny
Local Launo Remote Lau Local Activa	ch inch ation		Deny
Local Laund Remote Lau	ch inch ation	Allow V V	Deny
Local Launo Remote Lau Local Activa	ch inch ation		Deny
Local Launo Remote Lau Local Activa	ch inch ation		Deny
Local Laund Remote Lau Local Activa Remote Act	ch Inch Ition ivation	Allow V V V	Deny
Local Laund Remote Lau Local Activa Remote Act	ch inch ation	Allow V V V	Deny

- This completes the OPC client-side configuration. Reboot the system after these changes are
 made. Repeat the process on each client.
- On each OPC Server machine, make the following changes to DCOM properties. Launch the
 "Control Panel >> Administrative Tools >> Component Services" snap-in to open the
 DCOM console.

- 3992 3993 3994
- Expand Console Root > Component Services > Computers, right-click **My Computer** and then click Properties. Ensure the settings are as follows
 - My Computer Properties ? X Default Protocols COM Security MSDTC **Default Properties** General Options Enable Distributed COM on this computer Enable COM Internet Services on this computer Default Distributed COM Communication Properties The Authentication Level specifies security at the packet level. Default Authentication Level: Connect • The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level: Identify • Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous. Provide additional security for reference tracking

• Click on the "COM Security" tab >> Access Permissions >> "Edit Default" >> Add the opcadmin user and grant it ALLOW permissions for Local Access and Remote Access boxes.

3999 4000

General	Options	Defa	ult Properties		
Default Protocols	COM Se	ecurity	MSDTC		
Access Permissions					
You may edit who i: also set limits on ap					8
	lodifying access per ions to start, conner		Default Security Group or user names:		
	Edit Limits	E	SELF SYSTEM Administrator (FGS-613		
Launch and Activation	n Permissions		Opcadmin (LAN\opcad Minimum CAN\opcad Minimum CAN\opcad	min)	
You may edit who is activate objects. Yo				III	•
determine their own		o on applicatio		Add	Remove
	lodifying launch and ability of application			Allow	Deny
and/or run			Local Access	V	
			Bemote Access	V	100

- Similarly, under "Launch and Activation Permissions" >> "Edit Default" >> Add the ٠ "Administrators" group and check on ALLOW Boxes for all 4 categories. If adding the other opcuser, it will only have Local Launch permissions. 4007
- 4008

General	Options	Defau	It Properties	
Default Protocols	COM Se	curity	MSDTC	
coese Permissions				
Launch and Activatio	on Permission		2	×
Defects Consults				_
Default Security				_
Group or user name	es:			
Serveryone				
SYSTEM				
all and an	FGS-613380SH\	and the second		
		Administrators		
		Add	Remove	
]
		Add	Remove]
Remissions for Adm		Add Allow	Remove]
Remissions for Adm		Add Allow	Remove	
Remote Launch	ninistrators	Add Allow V	Remove]
Permissions for Adm Local Launch Remote Launch Local Activation	ninistrators	Add Allow V	Remove]
Permissions for Adm Local Launch Remote Launch Local Activation	ninistrators	Add Allow V	Remove	
Permissions for Adm Local Launch Remote Launch Local Activation	ninistrators	Add Allow V	Remove	
Permissions for Adm Local Launch Remote Launch Local Activation	ninistrators	Add Allow V V V	Remove	

4009 4010

- Note down the names of the opc-server software installed in your environment and make the 4011 • below shown DCOM changes on each of their application folders. In our case, the list of the 4012 4013 s/w is as follows
- 4014 • Harmony (Installed on OPC Server)
- 4015 • RSLINX (Installed on OPC Server)
- MATLAB (Installed on the Controller) 4016

4017

4018 We will start with the main OPC-Server and then move on to the Controller host. Launch the ٠ DCOM console and browse to **Console Root** > **Component Services** > **Computers** > **My** 4019 **Computer > DCOM Config.** In the list of applications in the right pane, right-click your 4020 4021 OPC server (application folder) and choose PROPERTIES.

JZZ Component Services	
A File Action View Win	dow Help
🗢 🔿 🚺 🚺 🗶 🗎 🖸	🛛 🗔 11 🛄 🗄 🏛 🏛
🧰 Console Root	
a 💩 Component Services	
a 🚞 Computers	
a 🜉 My Computer	
DOM+ Applic	
a 🧰 DCOM Config	
	loot%\system32\appwiz.cpl pot%\system32\colorui.dll
	oot%\System32\fveui.dll
	bot%\system32\intl.cpl
-	oot%\system32\lpksetup.exe
🧆 File Action View 🕅	Vindow Help @ 🛛 🗊 12 🖭 📰 🏢 🧾
b ♣ FTTop	ologyExtension
🔈 🚔 FwCpli	
	Reporting
> 🚔 Harmo	
Health	K View 🕨
> 🚔 Home	Gr New Window from Here
🔈 🏯 Home	3r
> 🏯 Home	3r Properties
👂 🚔 Home	Gr Help
025 🛛 🔊 🊔 Home	Broup i toviuci ocivice
026	en en el se en el se en el se el s

For example, find the "Harmony" folder, right click to view its Properties. On the General tab, 4027

set Authentication Level to Default. 4028

General	Location Secu	rity Endpoints Identity
Gener	al properties of th	is DCOM application
Appli	ication Name:	Harmony
Appli	ication ID:	{DAA085E0-F341-11CE-B4B5-C46F03C10000}
Appli	ication Type:	Local Service
Auth	entication Level:	Default
Serv	ice Name:	Harmony
Learn m	ore about <u>setting</u>	these properties.

• On the Location tab, Select - **Run application on this computer**.

ieneral	Location	Security	Endpoints	Identity		
applica	tion. Îf you i	nake more	e than one s		et computer for DCOM uses th lections.	
🔲 Rur	application	on the co	omputer whe	re the data is	located.	
🔽 Rur	application	on this co	omputer.			
Rur	application	on the fo	llowing com	outer:		
					Browse	

- 4038 OPC users: (opcuser)
 - Launch and Activation Permissions: Use System Defaults

- 4040 Access Permissions: Use System •
- 4041 Configuration Permissions: Allow Read •
- 4043 OPC administrators: (opcadmin)
- Launch and Activation Permissions: Use System Defaults 4044 •
- Access Permissions: Use System Defaults 4045 •
- 4046 • Configuration Permissions: Customize Full Control as shown below. (Note opcadmin is a 4047 member of Administrators group)

4042

ieneral Location Security Endpo	Change Configuration Permission
Launch and Activation Permissio Use Default Customize Access Permissions Use Default	Security Group or user names: CREATOR OWNER SYSTEM Administrators (FGS-613380SH\Administrators) Users (FGS-613380SH\Users)
Customize	Add Remove Permissions for Administrators Allow Denv
Configuration Permissions O Use Default O Customize	Full Control Image: Control Read Image: Control Special permissions Image: Control
Learn more about setting these prope	For special permissions or advanced settings, Advanced click Advanced. Learn about access control and permissions

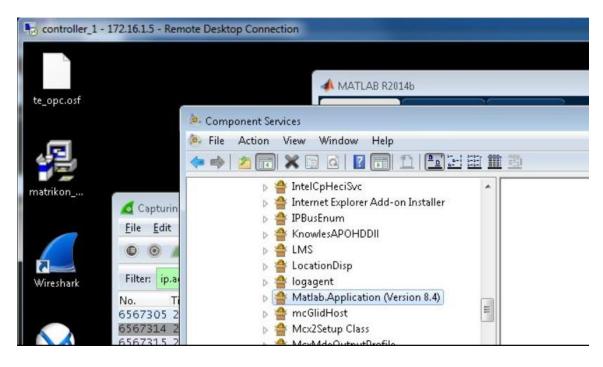
4049 4050

On the Identity tab, choose the "This user" option and enter the user name and password for 4051 • 4052 the AD user you created. We will select opcadmin as the user in our case. Click OK to save your settings. Reboot system.

General	Location	Security	Endpoints	Identity		
Which	user accou	nt do you v	want to use t	o run this app	blication?	
C The	interactive	user.				
0 The						
	launching	user.				
	launching	user.				
The	launching		LAN\opcadr	in	Brows	e
TheThis	launching user.		LAN\opcadr	in •••••	Brows	e

• Repeat the above steps 3.e.1 to 3.e.5 on the "RSLINX" folder (on the OPC Server) and on the MATLAB Application folder (on the Controller Server). Reboot system when done. Some screenshots for the MATLAB folder are shown below.

Note: These settings may not be necessary for the RSLINX folder and depends on the environment.



ieneral Location Secu	urity Endpoints Identity
General Location Secu	
Application Name:	Matlab.Application (Version 8.4)
	{D309A656-4B0B-47F2-9A27-0C4E9D8735C4}
Application ID:	di d
Application Type:	Local Server
Authentication Level:	J
Local Path:	C:\Program Files\MATLAB\R2014b\bin\win64\I
Learn more about <u>setting</u>	these properties.
Learn more about <u>setting</u>	
Learn more about <u>setting</u>	these properties.
Learn more about <u>setting</u>	
	OK Cancel Apply
lab.Application (Versio	OK Cancel Apply
lab.Application (Versionersel Location Security	OK Cancel Apply
ab.Application (Versic meral Location Secu he following settings allo pplication. If you make r pplicable one. Client app	OK Cancel Apply on 8.4) Properties wity Endpoints Identity ow DCOM to locate the correct computer for this more than one selection, then DCOM uses the firs
ab.Application (Version Ineral Location Security	OK Cancel Apply on 8.4) Properties P wity Endpoints Identity ow DCOM to locate the correct computer for this more than one selection, then DCOM uses the firs plications may overide your selections. e computer where the data is located.
The following settings allo application. If you make n applicable one. Client app	OK Cancel Apply on 8.4) Properties wity Endpoints Identity ow DCOM to locate the correct computer for this more than one selection, then DCOM uses the firs plications may overide your selections. e computer where the data is located. is computer.
Iab.Application (Version and the second s	OK Cancel Apply on 8.4) Properties wity Endpoints Identity ow DCOM to locate the correct computer for this more than one selection, then DCOM uses the firs plications may overide your selections. e computer where the data is located. is computer.

OK

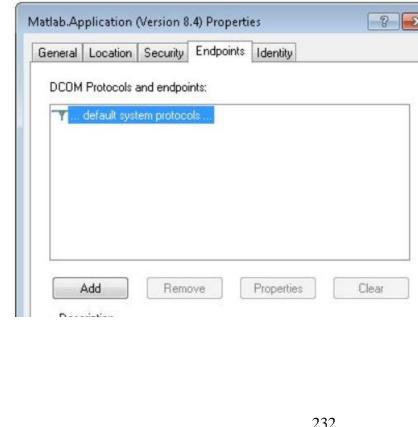
Cancel

Apply



aeneral Location Security Endpo	Change Configuration Permission		? ×
- Launch and Activation Permissio	Security		
Use Default	Group or user names:		
	& CREATOR OWNER		
Customize	SYSTEM		
	Administrators (FGS-61338CH)	Administrators	
Access Permissions			
() Use Default			
	ſ	Add	Remove
Customize			
	Permissions for Administrators	Allow	Deny
	Full Control		
Configuration Permissions	Read Special permissions	1	
🔘 Use Default	Special permissions	10	
Customize			
	En en sid e univiene er ed en er	d an Winnes	
	For special permissions or advanced click Advanced.	a settings,	Advanced
	Learn about access control and per	missions	
		missions	
Learn more about setting these prop		OK	Cancel
0	K Cancel Apply		

 $\begin{array}{c} 4070\\ 4071 \end{array}$



2440-00 C	urity Endpoints Identity	
Which user account do	you want to use to run this appli	cation?
The interactive user.		
The launching user.		
This user.		
User:	LAN\opcadmin	Browse
Password:	•••••	
Confirm password:	•••••	
The system account	(services only).	
Learn more about <u>setting</u>	these properties.	

4083

4085

4078 Radius Server Setup

A Windows 2012 R2 server running Active Directory and Windows Network Policy Server (NPS) was setup in the Management LAN to authenticate the boundary firewall and VPN users. Technically both the roles can be on the same server but its recommended to keep them separate for redundancy.

- 4084 High level setups
 - Setup the AD Server
- 4086 Create an AD Domain
- 4087 o Setup the Radius Server
- 4088 Join Radius server to the AD Domain
- 4089 o Register Radius Server with AD
- 4090 Details of the AD Server and Domain in Management Network

Hostname	IP address	Roles	Domain Name
Mgmt-AD	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

- 4091 4092
- To setup Radius services on Windows 2012 R2, install the Network Policy Server role. This can be done from Server Manager >> Add Roles and Features Wizard as shown below

ē.	Add Roles and Features Wizard	_ _ ×
Select server role Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results		DESTINATION SERVER Mgmt-AD.mgmtlab Description Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
	Windows Deployment Services	
	< Previous Next >	Install

4095

- Open the Network Policy Server Console, Click on **Register Server in Active Directory**
 - 6 Network Policy Server File Action View Help (= =) 🗖 ? NIDE (L-🚱 NPS (🗠 (Les) Import Configuration ⊿ 🔛 R/ Export Configuration Ē Server (NPS) allows you to create and enforce organization Start NPS Service **I** Po nection request authentication, and connection request au Þ Stop NPS Service N Þ Register server in Active Directory A ration ιт Properties scenario from the list and then click the link below to open View ۲ Help Lction (NAP) Network Access Protection (NAP) When you configure NPS as a NAP health policy server, you create health policie configuration of NAP-capable client computers before they connect to your netwo with health policy can be placed on a restricted network and automatically update Configure NAP Learn more

L.,

- 4098• <u>Create user accounts in AD.</u> A User account called "icsuser01" and a Security Group "Network
- 4099 Admins" were created in our Mgmt.lab domain. The icsuser01 user was added to the Network4100 Admins group.
- 4101

	Active Directory U	sers and Comp	uters	_	×
 Active Directory Users and Com Saved Queries mgmt.lab 	C C C C C C C C C C C C C C C C C C C	Type User Security Group	Description Built-in account for ad Members in this group c		
 ▷ I Builtin ▷ Ormputers ▷ Domain Controllers ▷ ForeignSecurityPrincipal: ▷ Managed Service Accour □ Users 	 Cert Publishers Cloneable Domain Contro Denied RODC Password R DnsAdmins DnsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Guests Enterprise Read-only Dom Group Policy Creator Own 	Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Members of this group Members of this group t Members of this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain guests Members of this group Members in this group c		
< 111 >	Subscription Guest Gues	User User Security Group Security Group Security Group	Built-in account for gue Members of this group Servers in this group can		

4102 4103

- 4104
- 4105 4106

4107

4108 4109

4110 4111

- Create Radius Clients and Policies in NPS:
- Launch the Network Policy Server snap-in to create a Radius client for the Network Device you did like to integrate. A Radius client was created for the Boundary Firewall (Allen Bradley) of the Process Control System.

File Action View Hel	р					
🗢 🔿 🙍 🖬 🖬						
NPS (Local) RADIUS Clients and S RADIUS Client			s allow you to	specify the network acc	ess servers, that	t provide access
Remote RADIU	New Export List					
Connection R	VIEW	-	IP Address 10,100,2,6	Device Manufacturer	NAP-Capable No	Status Enabled
Network Polic Health Policie	Refresh		10.100.2.7	RADIUS Standard	No	Enabled
Network Access F	Help	300	0 10.100.2.8		No	Enabled
here a counting the second sec						

- 4114 o Enter a matching name of the Network Device, IP address of the management interface
 4115 and create a "passphrase ". Hit OK when done. This will create the Radius client.
 4116 Make sure you can ping the Management IP of the network device from the Radius
 4117 server
- 4118

	AllenBradley8300 Properties	
ttings	Advanced	
Enab	e this RADIUS client	
Sele	ct an existing template:	
		~
Name	and Address	
	v name:	
AllenE	radley8300	
Addres	s (IP or DNS):	
10.10		/
None		~
	nually type a shared secret, click Manual. To automatically generate a	
secret, secret	click Generate. You must configure the RADIUS client with the same s entered here. Shared secrets are case-sensitive. nual O Generate	
secret secret	click Generate. You must configure the RADIUS client with the same s entered here. Shared secrets are case-sensitive. nual O Generate I secret:	
 Ma Shared 	click Generate. You must configure the RADIUS client with the same s entered here. Shared secrets are case-sensitive. nual O Generate I secret:	
 Ma Shared Confim 	click Generate. You must configure the RADIUS client with the same s entered here. Shared secrets are case-sensitive. nual O Generate I secret:	

- 4123 Next, under Policies >> Network Policies >> Create a new policy for the radius client.
- 4124 The below image shows the network policy created for the Allen Bradley firewall

	AllenBradley-access Properties
Overview Conditions Constraints Settings	
Policy name: Allen Bradley-acc	ess
s	performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled	
Access Permission If conditions and constraints of the netwo access. <u>What is access permission?</u>	rk policy match the connection request, the policy can either grant access
 Grant access. Grant access if the conner 	ction request matches this policy.
 Deny access. Deny access if the connect 	tion request matches this policy.
Ignore user account dial-in properties.	
	nditions and constraints of this network policy and the policy grants access, p not evaluate the dial-in properties of user accounts .
Network connection method	
	at sends the connection request to NPS. You can select either the network a f your network access server is an 802.1X authenticating switch or wireless a
• Type of network access server:	
Unspecified	v
◯ Vendor specific:	

Under "Conditions", click on the ADD button, look for "user/groups option", select the
"Network-Admins" security group we setup earlier in our AD. This will allow users
from this group to login as admins for managing the switch. Also add another condition
to check for the IP address of our Allen-Bradley. Look for "Client IPv4 address"
option, enter the IP address of our Allen-Bradley and add it. Below is how the
Conditions page should like once both conditions are added. Hit Next to proceed to the
next screen.

₽ 10.100.2.4	4 - Remote Desktop Connection		_		\times
		AllenBradley-access Properties			
/iew Hel	Overview Conditions Constrait				
ients and S S Clients re RADIUS S	If conditions match the connecti	on request, NPS uses this policy to authorize the connection request. If conditions do n his policy and evaluates other policies, if additional policies are configured.	ot match	the	
e loadios s	Condition	Value			
ction Requ	Ser Groups	MGMT\NetworkAdmins			
rk Policies	Client IPv4 Address	10.100.2.8			
Policies Vccess Prot 9 ; Managem					
	Condition description: The Client IP Address condition	specifies the IP address of the RADIUS client that forwarded the connection request to	NPS.		
		Add Edit.		Remov	ve

• Under Authentication methods choose the "**PAP**, **SPAP**" method as Cisco IOS supports these ones. Click **Next** to proceed to the Settings page.

	AllenBradley-access Properties
Overview Conditions Constraints Setting	8
Configure the constraints for this network poli If all constraints are not matched by the conn	
Constraints:	
Authentication Methods	Allow access only to those clients that authenticate with the specified
Idle Timeout Idle Station Timeout Idle Called Station ID Pay and time restrictions	EAP types are negotiated between NPS and the client in the order in th
NAS Port Type	Add Edit Remove
	Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication meth Perform machine health check only

- Under Settings >> Radius Attributes >> Standard >> Remove the 2 default attributes. Click ADD to add a new attribute with Name = "Service-Type" and Value = "Login" as shown below.

	AllenBradl	ey-access Properties
Overview Conditions Constraints Setting	s	
Configure the settings for this network policy If conditions and constraints match the conn		e policy grants access, settings are appli
Settings:		
RADIUS Attributes	To send additional	attributes to RADIUS clients, select a R.
🚯 Standard	then click Edit. If y	rou do not configure an attribute, it is not nt documentation for required attributes.
🗾 Vendor Specific	your hADIOS ciler	it documentation for required attributes.
Network Access Protection		
NAP Enforcement	Attributes:	
🕎 Extended State	Name	Value
Routing and Remote Access	Service-Type	Login
Multilink and Bandwidth Allocation Protocol (BAP)		
TP Filters		
🔒 Encryption		
🔏 IP Settings		
	Add	Edit Remove
		T INTINETS

Under Vendor Specific Attributes, add a new attribute by selecting "Cisco-AV-pair" from the list, Vendor= "Cisco" and value = "shell:priv-lvl=15". This will allow the user to login with privilege level =15 meaning admin privileges. Click on OK/Apply button to save the changes

					AllenBradle	ey-acce	ss Properties
	Overview	Conditions	Constraints	Settings			
			for this netwo traints match t		ction request and the	e policy gra	ants access, settings are applied.
	Settings:						
	BADIU St.	IS Attributes andard	\$		then click Edit. If ye	ou do not	to RADIUS clients, select a Vendor ! configure an attribute, it is not sent to ntation for required attributes.
	🗾 Ve	ndor Specific	5		your RADIUS clien	il documer	itation for required attributes.
	Netwo	r <mark>k Acce</mark> ss F	Protection				
	- 🛃 N/	P Enforceme	ent		Attributes:		
	💌 Ex	tended State	:		Name	Vendor	Value
	Routin	g and Rem	ote Access		Cisco-AV-Pair	Cisco	shell:priv-lvl=15
	💑 Mu Ali	ultilink and Ba ocation Proto	andwidth Icol (BAP)				
	TP	Filters					
	🔒 Er	cryption					
	🔒 iP	Settings					
					Add	Edit	Remove
Co	onfiguring	g Bounda	ry Firewa	ll for R	adius Authenti	cation:	
0		U			n on the Allen dius server.	Bradle	y Boundary firewall to ena

4	1	49

4150 • 4151	Configuring Boundary Firewall for Radius Authentication:
4151 4152 4153 4154	• The following commands were run on the Allen Bradley Boundary firewall to enable it to authenticate against the above Radius server.
4155 4156 4157 4158 4159 4160 4161 4162 4163 4164	<pre># enable # configure terminal # aaa new-model # aaa authentication login default group radius local # aaa authorization exec default group radius local # radius server host < IP address of our radius server> # radius server-key <passphrase> # quit # wr mem</passphrase></pre>
4165	

4167 **4.9.6** Highlighted Performance Impacts

- The following performance measurement experiment was performed for the Active Directoryservice while the manufacturing system was operational:
- 4170 PL002.1 Active Directory service active with non-OPC accounts being configured as non-
- 4171 Administrator privilege.
- 4172 There was no performance impact to the manufacturing process observed during the experiment.
- 4173 However, performance impact was observed at the implementation of the Active Directory (AD)
- 4174 service. At the initial implementation, the team focused on the Active Directory installation and
- 4175 user configuration, but not knowing the need for DCOM configuration initially, causing
- 4176 unplanned production interruption. DCOM and user account configuration for every OPC client
- 4177 have to be modified to use AD instead of local authentication. Without modification, the OPC
- 4178 client failed to communicate with the OPC DA server and caused all OPC data exchange to cease
- 4179 operation. This failure caused the manufacturing process entered the emergency shutdown state.
- 4180 Another impact observed at implementation was the **time synchronization** source with the AD.
- 4181 Authentication failed due to time discrepancy between hosts and AD. It is because the hosts were

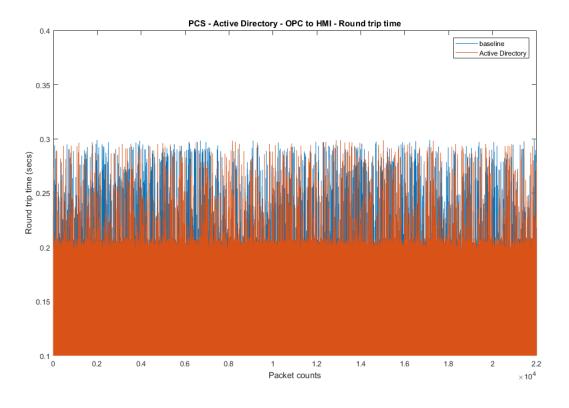
4182 synchronized to a different time source than the AD and the time difference was greater than 5

4183 minutes. When the host joins the AD domain, each host should use the same time source as AD.

- 4184 For example, all hosts in PCS use AD as the time source, and AD uses an external NTP server as 4185 its time source
- 4185 its time source.
- 4186 Care should be taken to ensure proper operation of the Active Directory service. Failure in
- 4187 authentication causes error in operation of the OPC server, which handles all the data exchange
- 4188 of the controller and the plant operation. The manufacturing process entered emergency
- 4189 shutdown state because the controller lost the ability to communicate to the sensors and
- 4190 actuators. Redundancy and backup is highly recommended. Ability to switch between primary
- 4191 and secondary AD should be seamless to avoid impact to the system.

4192 There was no significant impact to the network performance observed. For example, the round

4193 trip time from OPC to HMI is mostly the same with the Active Directory.



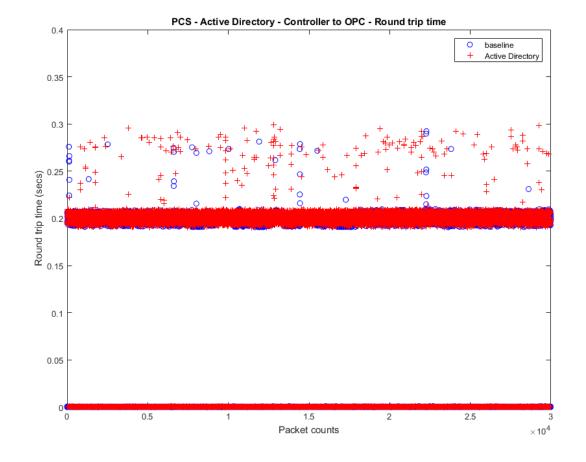
4195

Figure 4-16 Packet round trip time from OPC to HMI with Active Directory.

4196

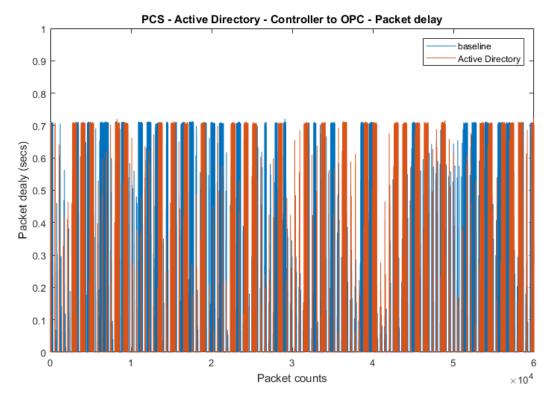
4197 The controller is another major component required modification to use Active Directory. The 4198 Controller authenticates against the AD server. The controller also has the updated DCOM so 4199 that it can continue to communicate with the OPC server. The packet round trip time from the 4200 Controller to OPC was slightly elevated, with a small number of packets had a slightly increased 4201 round trip time. There was no significant increase in inter packet delay from the Controller to

4202 OPC observed.



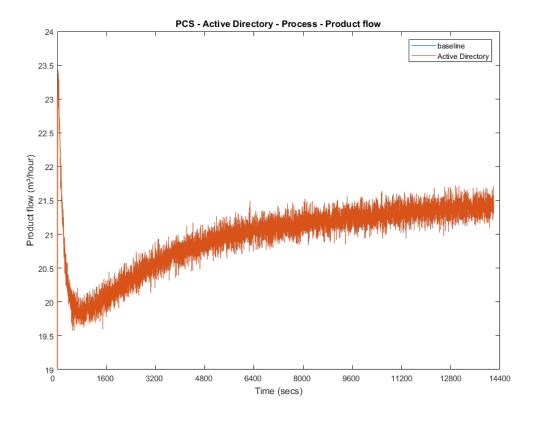
4204

Figure 4-13 Packet round trip time from Controller to OPC with the Active Directory enabled (red)



4206 Figure 4-14 Inter packet delay of Controller to OPC with the Active Directory enabled (red)

4207 There was no significant performance impact to the manufacturing process observed with the use
4208 of Active Directory. For example, the product flow rate remained consistent with and without the
4209 use of Active Directory.

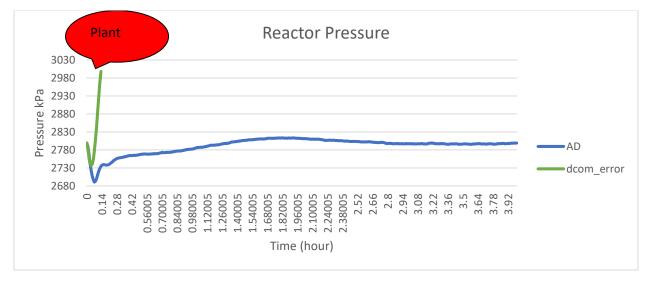


4212 Figure 4-19 Manufacturing process product flow rate during the use of Active Directory (red)

4213 A misconfiguration on the Active Directory cased the manufacturing process to enter the

4214 emergency shutdown state in about 600 seconds of the experiment time due to the reactor

4215 pressure too high



4217
4218Figure 4-20 Plot of the manufacturing process reactor pressure. The process entered emergency shutdown
mode when DCOM communication failed.

4220 **4.9.7** Link to Entire Performance Measurement Data Set

- 4221 Active Directory KPI data
- 4222 Active Directory measurement data
- 4223

4224 **4.10** Symantec Endpoint Protection

4225 **4.10.1 Technical Solution Overview**

4226 Symantec Endpoint Protection:

4227 Symantec Endpoint Protection (SEP) is a complete endpoint protection solution from Symantec.

4228 It delivers superior, multilayer protection to stop threats regardless of how they attack your

4229 endpoints. SEP integrates with existing security infrastructure to provide orchestrated responses

4230 to address threats quickly. Its lightweight SEP agent offers high performance without

- 4231 compromising end-user productivity. SEP also defends against ransomware and other emerging
- 4232 threats with multilayered protection that fuses signatureless technologies like advanced machine

4233 learning, behavior analysis and exploit prevention with proven protection capabilities like 4234 intrusion prevention, reputation analysis and more.²²

- 4235
- 4236 Points to Consider:
- 4237 Next Generation Antivirus / Endpoint protection solution to prevent against virus attacks
 4238 and emerging cyber threats such as zero-day attacks, ransomware etc.
- OS Platform independent: The endpoint agents are supported on Windows and Linux.
- 4240 Comes with a lightweight agent and virus definition sets that require minimal network
 4241 bandwidth.
- Diverse Feature set: Core capabilities include Antivirus, Host Firewall, Intrusion
 Prevention, Host Integrity, System lockdown, Application White listing and USB Device
 Control.
- 4245
 Centralized Management: All endpoints, rule sets, policies can be centrally managed from the Symantec Endpoint Manager console.
- The Symantec Manager component is supported only on Windows OS.
- The Linux agent requires the OS kernel on Linux systems to be at a certain level for
 installation. In addition, the Linux agent is a 32-bit installer. If installing on a 64-bit Linux
 system, it requires certain 32-bit packages/libraries to be installed as a pre-requisite. This
 may conflict with some of the existing packages on the system.
- The endpoint agent on each system by default needs to communicate outbound with a range of public IP addresses for its Reputation analysis and Global Threat intelligence feature. It is recommended to allow this traffic from your firewall to leverage the advanced features of the product.
- 4256
 Important: System reboot is required to complete the installation process on clients/endpoints. Plan ahead of time.

 $[\]frac{^{22} \text{ Symantec Endpoint Protection: } \underline{\text{https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf}}{\text{content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf}}}$

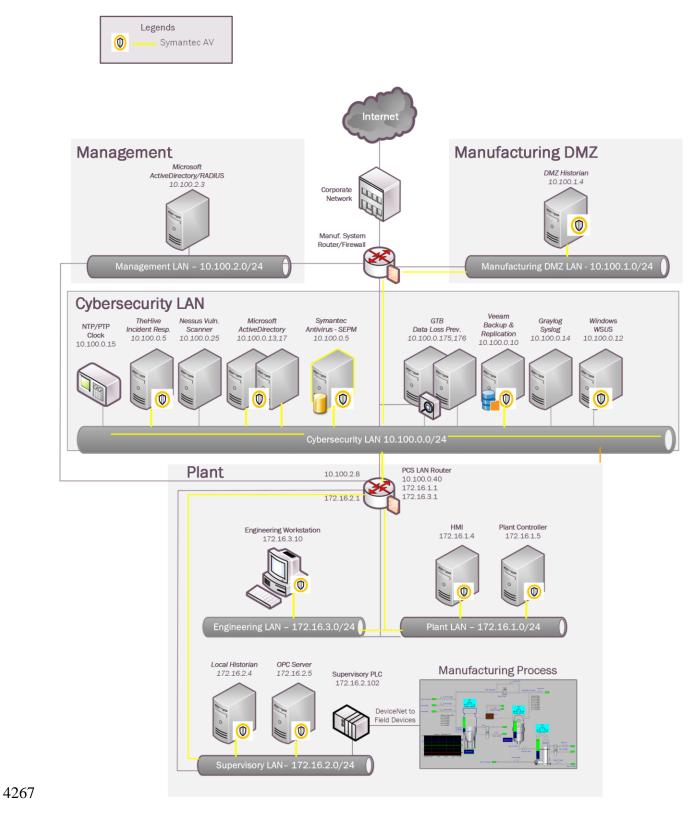
4259

4260 **4.10.2** Technical Capabilities Provided by Solution

- 4261 Symantec Endpoint Protection provides components of the following Technical Capabilities4262 described in Section 6 of Volume 1:
- 4263 Anti-virus/malware

4264 **4.10.3** Subcategories Addressed by Implementing Solution

4265 PR.AC-1, DE.CM-3, DE.CM-4



4266 **4.10.4** Architecture Map of Where Solution was Implemented

4268 **4.10.5** Installation Instructions and Configurations

4269 Setup Overview:

4270 Setup consists of a single Symantec Endpoint Protection Manager (SEPM) instance in the

4271 Cybersecurity LAN network. This central instance communicates with all the endpoint agents4272 deployed on to the Process Control systems. Likewise, all endpoints report their status to the

4273 Manager server. The communication ports required to be opened are different for Windows

4274 clients as compared to Mac/Linux clients. Detailed list of firewall ports can be obtained from

- 4275 Symantec website. The SEP Manager server downloads its daily signature updates from the
- 4276 Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufacturing
- 4277 System Firewall.
- 4278 Details of the software used

Product Name	Version
Symantec Endpoint Protection Manager (SEPM)	14.2 Build 758
Symantec Endpoint agent for Windows (Client)	14.2.758.0000

4279

4280 **Installation of SEP Manager:**

0

SEPM is supported only on Windows server platforms. A Windows Server 2012 R2 virtual
 machine was setup in the Cybersecurity LAN to install the SEPM component.

Upon purchase, there will be a license file emailed to you along with the link to download
 the install binaries. Download the zip bundle from the Symantec website. Extract the zip
 file which will be like the one below depending on whatever is the latest version available.

4286 4287 Symantec_Endpoint_Protection_14.2.0_Full_Installation_EN.exe

- Open the extracted folder and run the Setup.exe file. Mid-way during the setup, the install
 wizard will prompt to select a password for the admin user. Enter a strong password and hit
 Next.
- On the Backed Database selection page, there are two options "Embedded" and "MS
 SQL Server". Choose the Embedded database if you do not have a MS SQL Server.
 Follow the on-screen instructions and complete the installation wizard. Reboot the server
 once done.
- Launch the SEP Manager console and login with the admin user created earlier.
- 4296

•	Symantec Endpoint Protection Manager	_ 🗆 X
_		
	Symantec.	
	Symantec Endpoint Protection Manager	
	Endpoint Protection Manager	
	User name: admin	
	Password:	
	Server: SymantecMgrVM:8443	
	Forgot your password?	
	Log On Exit Options >>	
	Copyright © 2018 Symantec Corporation. All rights reserved.	
	This Symantec product may contain open source and other third party materials that are subject to a separate license.	

- Upon completing the installation of Symantec Endpoint Manager, the next steps are to
 activate the license, configuring client groups to group devices and installing the antivirus
 agent on each endpoint/client system.
 - Link to Official Symantec Endpoint Protection v14 installation guides https://support.symantec.com/en_US/article.DOC9449.html
- 4304
 Ensure to open the necessary ports on the firewall for communication between the SEPM server and endpoints. A complete list of ports is available at https://support.symantec.com/en_US/article.HOWTO81103.html
- 4307 Custom Configuration of SEPM server

- 4309 The following client groups were created to group devices from each of the systems.
 4310 Upon installing the AV agent on the endpoints, the devices were moved to their
- 4311 respective groups.
- 4312

D	Symantec Endp	point Prote	ection Manager			
Symantec Endpoint Protecti	on Manager			Lates	st Alerts Refres	ih Help LogO
Clients My Company Default Group DMZ	Process Contro	ol		Policy serial r	umber: D575-11/29	/2018 15:33:34 712
Monitors – LAN Network – Process Control	Clients Policies I View: Client status	Details Insta	II Packages All users a	nd computers		Filter
Reports	Name	Health State	Logon User or Computer			Last Time Sta
12	FGS-47631EHH	Online	Administrator	172.16.3.10 172.16.2.4	14.2.758.0000 14.2.758.0000	April 23, 2019 1 April 23, 2019 1
Policies		Online	cheet	172.16.1.5	14.2.758.0000	April 23, 2019 1
Ω	GS-61338HH	Online	cheet	172.16.1.4	14.2.758.0000	April 23, 2019 1
Clients Tasks	GS-613380SH	Online	cheet	172.16.2.5	14.2.758.0000	April 23, 2019 1
	GS-61338PSH	Online	cheet	172.16.2.3	14.2.758.0000	April 23, 2019 1
Admin Minport Organizational Unit or Conta	WIN-FPVTDCDEUCR	Online	Administrator	172.16.2.14	14.2.758.0000	April 23, 2019 1
Cloud Command on the group						
Cloud 🤤 Set display filter						

- For integrating SEP Manager with AD/LDAP server, click on ADMIN >> Servers >> Local Site >> <Server Name> >> Edit Server Properties >> Directory servers. Click further on "ADD" button as shown below to configure domain details. Once done, logout and try logging in back with your AD credentials.

🛡 s	ymantec Endpoint Protection	Manager	🔔 Latest News Refresh He	lp Log Off
	Servers Servers Servers Superv	 Server Properties for Symantec File Fingerprint Update Full Definitions Download General Email Server Directory Servers Directory Servers 	MgrVM X	
Monitors		Name Type Properties	Add Edit Delete	
Policies <u>Clients</u>	Tasks ✓ Edit the server properties Source Delete Selected Server ✓ Manage Server Certificate ✓ Configure SecurID Authentication Import Server Properties Export Server Properties	Synchronized Directory Settings Synchronize with Directory Servers Schedule Auto-schedule (occurs every 24 hours) Synchronize every: hours		
(Domains Se	OK ptember 27, 2017 11:10:42 AM EDT: Retry timestamp is over the maximum ret ptember 27, 2017 11:00:42 AM EDT: LiveUpdate retry failed. Will try again. [5 ptember 27, 2017 11:00:42 AM EDT: LiveUpdate encountered one or more en III	try window, switching to regular schedul Site: Site SymantecMgrVM] [Server: Sym SymantecMgrVM] [Server: SymantecMgr	nantecMgi≡ rVM]

- 4320 4321
 - Similarly, Email server can be configured by clicking on the "Email Server" tab.

4322 Getting started with Endpoint installs

4323 High level steps:

- 4324
 4324
 4325
 Create a deployment package specific for a client group
 4325
 Deploy the package from the SEPM server to the endpoint using Network Deployment options or manually copy over the package to the endpoint for installation.
- Restart the endpoint. Verify the device shows up in the SEPM console.

4328 Creating a deployment package:

- Login to the Symantec Manager console, click on CLIENTS >> <Group Name> where the device needs to be in >> Click on Install client under TASKS. For instance, to create a deployment package for the group "Process Control", click on that group name followed by Install Client option.
- Select "New Package Deployment" if this is your first agent installation of that group.
 If you have already deployed the agent on other systems of this group, you can re-use the same package and skip this wizard completely.

)	Client Deployment Wizard
Select	Deployment Type Symante
Welcom	e to the Client Deployment Wizard
-	wizard to install the protection client on computers in your network or update existing client communication settings. k to view the Install Client tour
	or instructions to install the client on a computer that runs Symantec Mail Security or Symantec Scan Engine, see the Symantec al Support knowledge base article:
Click	k here
۲	New Package Deployment
	Select packages from the server and specify client group and features.
	Existing Package Deployment
	Choose from previously exported packages that are located on your hard drive.
	Browse
C	Communication Update Package Deployment
	Create a package that changes the communication settings on an existing Symantec Endpoint Protection client installation. Use this option to restore communication between the client and Symantec Endpoint Protection Manager, to connect the client to a new Symantec Endpoint Protection Manager, or to convert an unmanaged client to a managed client.
	🔿 Create a package for Symantec Endpoint Protection clients that run on Windows. 😂
	🔿 Create a package for Symantec Endpoint Protection clients that run on Mac. 🐗
	< Back Next > Cano

- 4338
- Click "Next" >> Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of Install Packages. You will notice the Group Name is already pre populated. This ensure the client will be placed directly in that group upon install. Under
 Content Options; Select "Include virus definitions in the client installation package"
 Click Next.

0	Client Deployment Wizard	X
Select Group a	nd Install Feature Sets	Symantec.
Install Packages:	Windows - Symantec Endpoint Protection version 14.2.758.0000 - English Windows - Symantec Endpoint Protection version 14.2.758.0000 - English Linux - Symantec Endpoint Protection version 14.2.758.0000 - English Windows - Symantec Endpoint Protection version 14.2.758.0000 - English Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English Linux - Symantec Endpoint Protection version 14.0.3929.1200 - English Linux - Symantec Endpoint Protection version 14.0.3929.1200 - English Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English Windows - Symantec Endpoint Protection version 14.0.3929.1101 - English Windows - Symantec Endpoint Protection version 14.0.3892.1101 - English	
Group:	My Company\Process Control	Browse
Install Feature Sets:	Full Protection for Clients Recommended for laptops and desktops - Includes all protection technologies. Some security features are not supported on some platforms. Please refer to product documentation for details.]
Install Settings:	Default Standard client installation settings for Windows	Options
Content Options:	Include virus definitions in the client installation package. Uncheck this option to create a smaller client installation package that does not include virus definitions but does other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definition	
	< Back Next :	Cancel

4345

On the next page, choosing the "Save Package" will create a local installer which needs to
be copied over the target machine manually and the "Remote Push" will make the SEPM
server perform a network deployment to the target machine(s). Choose your preferred option
and hit Next.

Choose y	our preferred installation method.	Symante Symante
 Save 	Package	
	Creates an executable installation package, but does not distribute protection software to remote computers.	
◯ Rem	ote Push	
	Creates a client installation package and pushes the package onto client computers. The package installs automat	tically on the computers.
	Preparing for Remote Push Installation	
O Web	Link and Email	
	Creates a client installation package and an email template so you can send an email notification with download in	nstructions to users.

4351 Installing the AV on Process Control System

- An installation package was first created as described in the previous section by selecting
 "Process Control" group and install package as "Windows". The executable installer was
 then manually copied over to each Windows system in the network and run.
- Upon installation, the system requires a **restart**. All systems were rebooted post installation.
- 4356 The SEPM console on the central server was checked to confirm all the clients from the
 4357 group were reporting green ONLINE and their Virus Definitions were current.
 4358

0		Symantec End	dpoint Pro	otection Manager		_ D X
🛡 s	symantec Endpoint Protec	tion Manager			Latest Alerts Refr	esh Help LogOf
₩ <u>H</u> ome	Clients My Company Default Group	Process Cont	trol		Policy serial number: D575-06/2	28/2018 18:42:16 123
Monitors	LAN Network Process Control	Clients Policies	Details Ins	stall Packages		
Eeports	Robotics Transportation	View: Default view	V Health State		nd computers Last Time Status Changed	Filter Virus Definition
		GS-47631EHH	Online Online	Administrator	October 1, 2018 1:31 PM October 1, 2018 1:37 PM	10/01/2018 r2 10/01/2018 r2
Policies		GS-61338CH	Online Online	cheet	October 1, 2018 1:37 PM	10/01/2018 r2 10/01/2018 r2
Clients	Tasks	FGS-613380SH	Online	cheet	October 1, 2018 1:37 PM October 1, 2018 1:37 PM	10/01/2018 r2
ري Admin	Install a client	GS-61338PSH	Online R Online	cheet Administrator	October 1, 2018 1:34 PM October 1, 2018 1:51 PM	10/01/2018 r2 10/01/2018 r2

 The official install guide for Windows systems can be found at https://support.symantec.com/en_US/article.DOC9445.html

4363 Additional Configuration

Symantec AV on each system by default blocks any port scan related traffic. If you have a vulnerability scanner or security tools in your environment, ensure those IP addresses are whitelisted in the SEPM console. The recommended way to do this is by creating a policy under Policies >> Intrusion Prevention >> Excluded Hosts and linking it to the appropriate client group. The figure below shows the settings page of excluded hosts.

0	Symantec Endpoint Protection Manager					
🔘 s	ymantec Endpoint I	Intrusion Prevention Policy	x			
企	Policies	Intrusion Prevention Policy				
Home	Virus and Spyware Protection	Overview Intrusion Prevention				
M	ntrusion Prevention Application and Device Control	Intrusion Prevention Windows Settings Intrusion Prevention Exceptions Intrusion Prevention automatically detects and blocks network attacks. Browser	Intrusi			
Monitors	Host Integrity	Exceptions blocks browser attacks.	_			
<u>R</u> eports	Memory Exploit Mitigation	Enable Network Intrusion Prevention Enable excluded hosts Excluded Hosts				
11	Exceptions Policy Components	Excluded Hosts vention for Windows				
Policies	Policy components	Host List Hosts to exclude from Intrusion Prevention:				
Clients	Tasks	Enab Group Name Content P address:10.100.0.25 P address:10.100.0.28				
තු	 Edit the policy Delete the policy 	✓ IP address: 10.100.0.20 ✓ IP address:10.100.0.177				
Admin	Delete the policy					

- 4370 4371
- 4372
- To setup device control such as restricting USB devices, create a policy under "Application and Device Control". Detailed instructions can be found <u>here</u>. Below shown image shows the USB policy implemented in our use case.

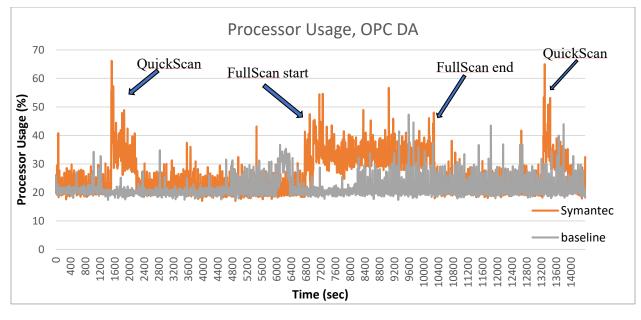
0		Application and Dev	rice Control Policy	×		
Application and E	Device	Control Policy				
Overview Application Control		Windows Device Control	<u> </u>			
Windows Settings	~					
Device Control		Blocked Devices Use this pane to manage the list of devices to which you want to block access.				
Mac Settings	\sim					
		Device Name	Identification			
		USB	Class: {36fc9e60-c465-11cf-8056-444553540000}			
		Devices Excluded From Blocking Use this pane to manage the list of devices	o which you want to allow access.	Add Delet		
		Device Name	Identification			
		Human Interface Devices (Mice, Joysti	Class: {745a17a0-74d3-11d0-b6fe-00a0c90f57da}			
				Add Delet		
		 Log detected devices 				
		 Notify users when devices are blocked 	r unblocked Specify Message Text			
		4	III	•		
				Cancel Help		

4377 Lessons learned

Using Symantec's Firewall: SEP also provides a firewall for clients. Firewall rules control how the client protects the client computer from malicious traffic. When you install the console for the first time, it adds a default Firewall policy to each group automatically.
Similarly, a client typically gets default firewall settings if a firewall policy is not configured from the console. Ensure to disable Windows OS or Host OS firewall if using Symantec's firewall.

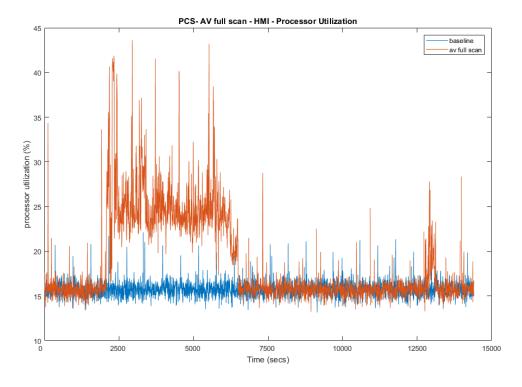
4384 **4.10.6 Highlighted Performance Impacts**

- The following performance measurement experiment was performed for the Symantec anti-virustool while the manufacturing system was operational:
- 4387 Experiment PL008.2- Symantec AV scan
- 4388
- 4389 During the Symantec anti-virus scan, sizeable performance impact was observed on the host
- 4390 processor Utilization. However, no significant performance impact was observed on the
- 4391 manufacturing process. A full Symantec scan can take up a considerable amount of processor
- 4392 power.
- 4393



4395
4396Figure 4-21 Plot of processor utilization of the OPC computer during the Symantec anti-virus scan (Red), and
the baseline processor utilization (gray)

4397 No significant performance impact to the network was observed. For example, the packet round4398 trip time between the OPC and PLC remained mostly the same.



4399

4400 Figure 4-22 Plot of processor utilization of HMI computer during a Symantec scan (red) and without a Symantec scan (blue)

- 4402 No significant performance impact to the network was observed. For example, the packet round
- trip time between the OPC and PLC remained mostly the same.

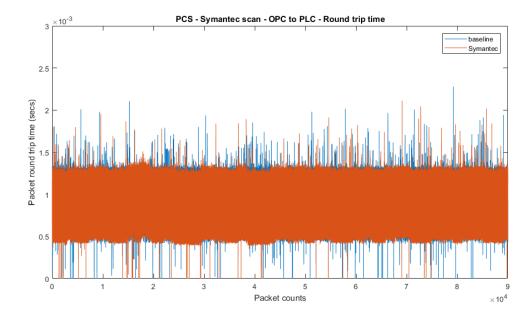
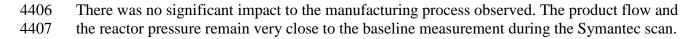
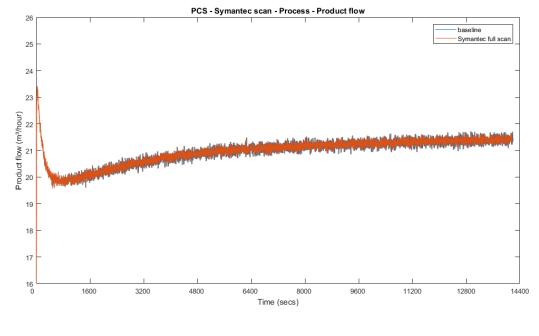
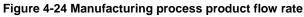


Figure 4-23 Packet round trip time between OPC and PLC during Symantec scan (red)









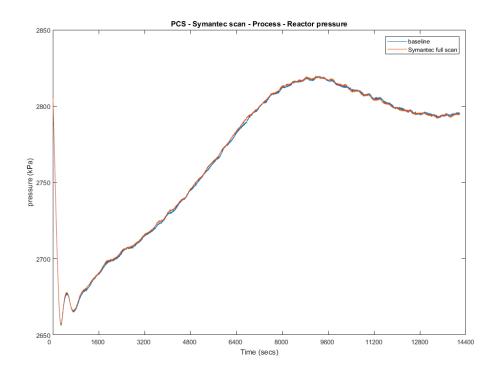


Figure 4-25 Manufacturing process Reactor pressure

4412 It is hypothesized that the impact to the processor utilization was caused by the Symantec AV

4413 during the scan. In the case of the PCS system, the normal processor utilization is relatively low

4414 and therefore the increased usage did not cause any performance impact to the manufacturing

4415 process. If the normal utilization of the host is close to 100%, there is potential performance

4416 impact due to the increase utilization during scan time.

4417 **4.10.7** Link to Entire Performance Measurement Data Set

- 4418 Symantec AV KPI data
- 4419 Symantec AV measurement data

4420 **4.11 Tenable Nessus**

4421 **4.11.1 Technical Solution Overview**

Nessus Professional is a vulnerability assessment software from Tenable. It features high-speed
asset discovery, configuration auditing, target profiling, malware detection, sensitive data
discovery and more. Nessus supports technologies such as scanning operating systems, network
devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure
for vulnerabilities, threats and compliance violations.²³ It supports both authenticated and
unauthenticated scans.

- 4428 Points to consider:
- Easy to setup, User friendly dashboard, fast scanning and can be configured to work in a distributed environment.
- Support for Industrial Protocols such as MODBUS, DNP3 etc. It has the necessary plugins to detect vulnerabilities on ICS/SCADA systems making it ideal to use in OT environments.
- Comes with a variety of Out-of-box policy and configuration templates.
- No limit on number of IPs or number of assessments you can run.
- Support for scanning devices behind a firewall.
- No integration available with LDAP or AD in the Professional edition.
- Multiple user accounts not supported for logging in to the Web UI.
- 4438

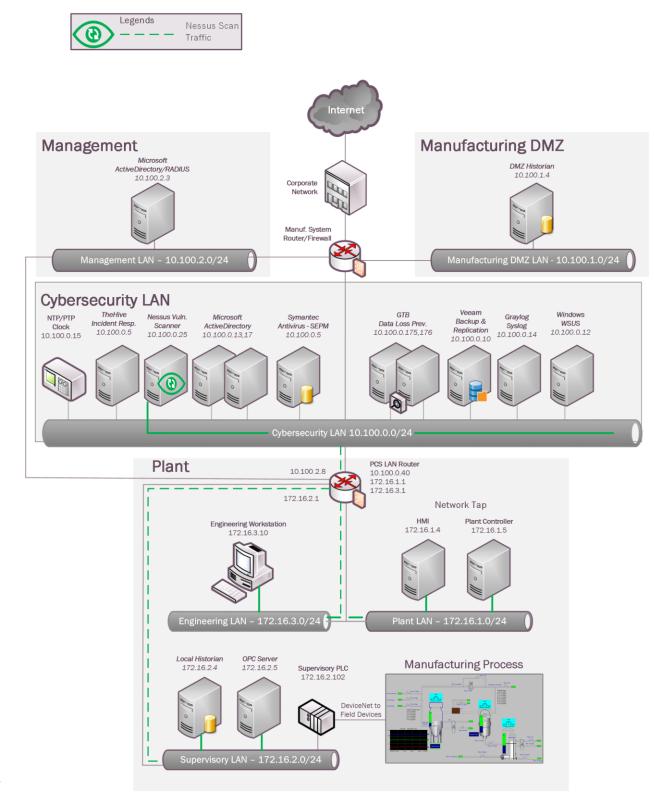
4439 **4.11.2 Technical Capabilities Provided by Solution**

- 4440 Tenable Nessus provides components of the following Technical Capabilities described in4441 Section 6 of Volume 1:
- Vulnerability Scanning
- Vulnerability Management

4444 **4.11.3** Subcategories Addressed by Implementing Solution

4445 ID.AM-3, ID.AM-4, ID.RA-1, DE.CM-4, DE.CM-8

²³ Nessus Professional: <u>http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf</u>



4446 **4.11.4** Architecture Map of Where Solution was Implemented

4448 **4.11.5** Installation Instructions and Configurations

4449 Details of the solutions implemented:

Name	Version
Nessus Professional	7.2.0

4450

4456

4460

4451 Setup Overview:

- A Nessus Professional 7.x version package file was downloaded from Tenable website and was installed on a Windows 2012 R2 Virtual machine in the Cybersecurity-LAN network.
 Nessus is supported on Windows, Linux and Mac OS platforms. Detailed installation instructions can be found in official product guide. ²⁴
- Ours was a single instance deployment. For distributed environments, Nessus supports
 distributed architecture of having multiple Nessus servers called as remote scanners linked to
 a central Nessus manager instance.
- During the setup, the wizard will prompt for registration. The Registration process and updates can be configured either in online or offline mode. An online mode is suitable for environments where Nessus server is connected to the internet while an offline mode is for air-gapped environments. Detailed instructions for registering Nessus offline can be found in the product guide. Upon completion, Nessus can be accessed via https://<IP address of Nessus server>:8834
- 4467
- The Nessus server needs to have network connectivity from whichever networks or subnets that are intended to be scanned. In addition, if performing authenticated scans then appropriate firewall rules should be in place to allow SSH, WMI or SNMP traffic depending on the type of hosts. If performing unauthenticated scan, the firewall should be allowed for any-any communication between the Nessus server and target network.
- 4473

4474 **Configuration:**

The Process Control Network has direct network connectivity with the Cybersecurity-LAN network, therefore no additional configuration was required other than allowing ports for
 WMI communication for scanning the Windows systems located in the Process Control network.

²⁴Nessus Official Documentation: <u>https://docs.tenable.com/nessus/Content/GettingStarted.htm</u>

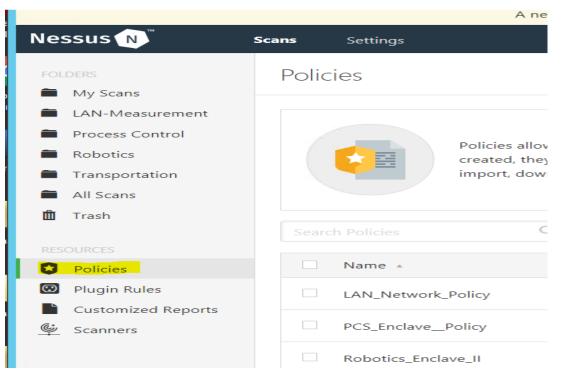
4479 The following is a list of settings that must be true for credentialed (authenticated) scans to • 4480 run successfully on Windows systems. All of these were enabled on the client (target) 4481 machines of Process Control System. 4482 4483 1. The Windows Management Instrumentation (WMI) service must be enabled on the 4484 target. (https://technet.microsoft.com/en-us/library/cc180684.aspx) 4485 4486 2. The **Remote Registry** service must be enabled on the target. 4487 4488 3. File and Printer Sharing must be enabled in the target's network configuration. 4489 4490 4. An SMB account must be used that has local administrator rights on the target. (You can 4491 use a domain account, but that account must be a local administrator on the devices being 4492 scanned.) 4493 4494 5. Ports 139 (TCP) and 445 (TCP) must be open between the Nessus scanner and the target. 4495 4496 6. Ensure that no Windows security policies are in place that block access to these services. See below for more information. 4497 4498 4499 7. The default administrative shares (i.e. IPC\$, ADMIN\$, C\$) must be enabled (AutoShareServer = 1). These are enabled by default and can cause other issues if 4500 4501 disabled (http://support.microsoft.com/kb/842715/en-us). 4502 4503 Run all commands from an elevated Command prompt or PowerShell (Right click CMD > • 4504 **Run as administrator**) on a host in the same network as the target 4505 4506 1. This command will see if we can access the IPC\$ share without a username (This is how 4507 Nessus tests to see if SMB is running): *Change x.x.x.x with the target's IP address.* net use \\x.x.x.x\ipc\$ /user:"" 4508 4509 4510 2. If this returns "Failed to connect to the IPC\$ share anonymously." then SMB is not 4511 running correctly. 4512 For SMB log-on test, run the following commands, with "username" being the username of 4513 • 4514 the account and "password" as the password for the account being used for the scan: 4515 4516 net use <u>\\x.x.x.x\ipc</u>\$ /user:username password 4517 4518 net use \\x.x.x.x\admin\$ /user:username password 4519 These commands should return "The command completed successfully." If it does not, then the 4520 4521 credentials did not work or do not have sufficient privileges. 4522

• Run the following command to check if the remote registry is running:

- 4524 reg query $\underline{x.x.x.}hklm$
- 4525

4526 If this returns registry keys, the service is running and accessible. If this returns "ERROR: The

- 4527 network path was not found." then the service is not running and must be enabled.4528
- 4529 To have a successful credential scan, these commands should not return errors.
- 4530
- It is recommended to use the "Policy" feature of Nessus for performing credentials checks,
 A Policy lets you create a scan template where in device credentials and other custom
 settings can be saved for scanning assets. Once created, a policy can then later be assigned to
 a scan.
- To create a policy, Click on "**Policies**" from the left-side explorer bar and further click on
- 4536 "**New Policy**" button.
- 4537



- Choose from any on the default templates available. The "Advanced Scan" template was selected for our use. Click on "Credentials" tab under a template to configure host based credentials (SSH, Windows, SNMP, etc.). Hit Save when done.
- 4543
- Next, Create a Scan. On the home-page, click "Scans" from left-side explorer bar >> New
 Scan >> User Defined >> Select <Policy> >> Enter a Name, Description and Network
 Range or Host IP addresses. Hit Save.
- 4547

Nessus N	Scans Settings	5		
FOLDERS My Scans	Scan Temp < Back to Scans	olates		
LAN-Measurement	Scanner	User Defined		
Process Control				
Robotics		•		
Transportation		£	1	±
All Scans	LAN Netv	vork Policy	PCS Enclave Policy	Robotics Enclave II
🛍 Trash	A user defined policy.		A user defined policy.	Advance scan policy template
RESOLIRCES				

- Click "All Scans" >> Click on the <Scan> created above >> Under Policy, Select the appropriate Policy from the drop down list to associate the scan with a policy. Click Save.
- The figure below shows the different policies created in our Nessus Manager specific to each system. The policy for this Process Control system is named "PCS_Enclave_Policy"
- 4555

Nessus 🔊 🕺 s	cans Settings		
FOLDERS My Scans LAN-Measurement Process Control Robotics Transportation All Scans Trash	created, they can b	to create custom templates defining what actions an be selected from the list of scan templates. From this edit, and delete policies.	
Trash RESOURCES	Search Policies Q 3	Policies	
Dolicies	Name 🔺	Template	Last Modified
Plugin Rules Customized Reports	LAN_Network_Policy	Advanced Scan	10/10/17 at 2:44 PM
Scanners	PCS_Enclave_Policy	Advanced Scan	10/10/17 at 2:47 PM
	Robotics_Enclave_II	Advanced Scan	10/10/17 at 2:50 PM

4556 4557

- The figure below shows the corresponding scan job settings which has the
- 4560 "PCS_Enclave_Policy" assigned to it
- 4561

Nessus Professional	I/Sca ×			
← → C ▲ Not	secure https://localho	st:8834/#/scans/report	s/63/config/settings/basic/general	Q
Nessus N	Scans Settings			🐥 a
FOLDERS My Scans LAN-Measurement Process Control	PCS_Enclave_Scat < Back to Scan Report Settings	n / Configuration		
 Robotics Transportation All Scans Trash RESOURCES Policies Plugin Rules Customized Reports 	BASIC ~ • General Schedule Notifications	Name Description Folder Policy	PCS_Enclave_Scan Process Control PCS_Enclave_Policy	
Scanners		Targets	172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24	

4565

• To kick-off a manual on-demand scan, click on the launch button next to the scan.

Search Scans Q 11 S	cans		
Name	Schedule	Last Modified 🔹	Launch
Process Control PCS_Enclave_Scan	Once on October 18 at 7:00 PM	V March 27 at 10:02 AM	►
Robotics Robotics_Enclave	On Demand	✓ 2018-12-10 at 1:29 PM	

4569

4566

4567

4570 **4.11.6 Highlighted Performance Impacts**

4571 The following performance measurement experiment was performed for the Nessus vulnerability 4572 assessment tool while the manufacturing system was operational:

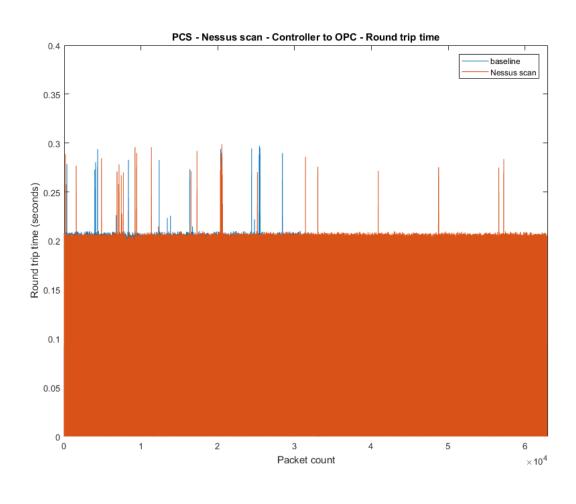
- 4573 Experiment PL006.1- Nessus vulnerability network scan
- 4574

4575 There was no significant performance impact to the manufacturing process was observed during 4576 the Nessus vulnerability scan. No significant network traffic increased during the Nessus scan

4577 was observed. For example, the packet round trip time from the Controller to OPC stayed mostly

4578 constant throughout the Nessus scan.

4579



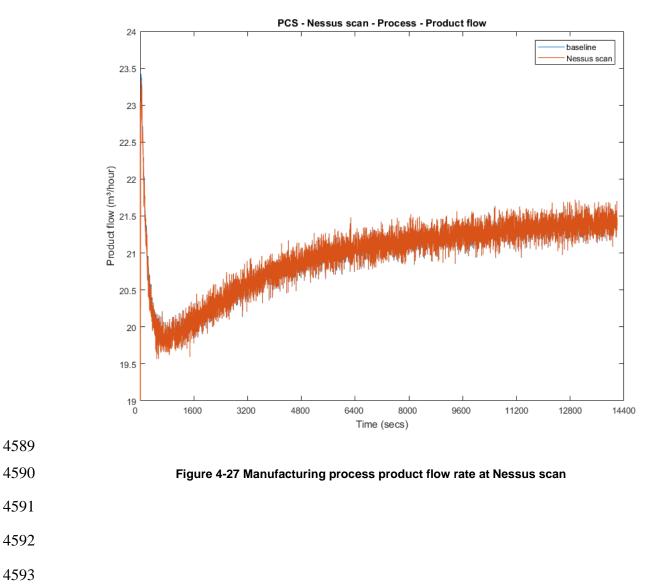
4580



Figure 4-26 Packet round trip time from Controller to OPC during Nessus scan

Some part of the system recorded a slightly increased network traffic, for example, the network
utilization and average bit rate from OPC to HMI during the Nessus scan was about 14.11% and

- 4584 1.41Mbit/sec respectively, while the baseline is 13.81% and 1.38Mbit/sec respectively The
- 4585 network utilization from PLC to OPC during the Nessus scan was about 2.2% higher than4586 baseline.
- 4587 The performance of the manufacturing process mostly remained the same. For example, the
- 4588 product flow and the reactor pressure remained align with the baseline measurement.



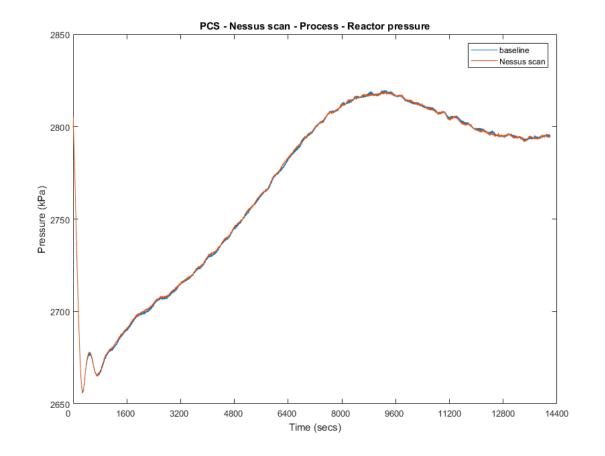




Figure 4-28 Manufacturing process reactor pressure at Nessus scan

- 4596
- 4597 **4.11.7** Link to Entire Performance Measurement Data Set
- 4598 Nessus KPI data
- 4599 Nessus measurement data
- 4600
- 4601

4602 **4.12** NamicSoft

4603 **4.12.1 Technical Solution Overview**

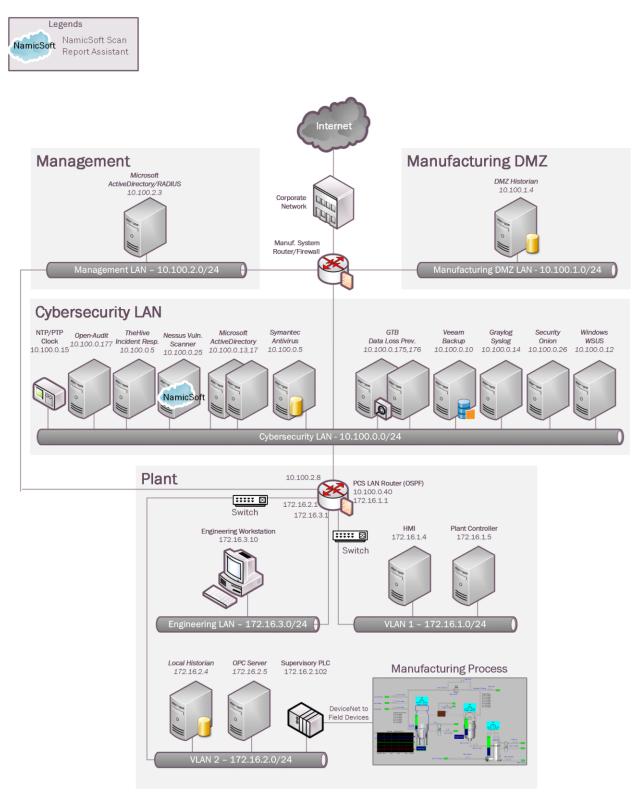
- 4604 NamicSoft Scan Report Assistant, a parser and reporting tool for Nessus, Burp, Nexpose
 4605 OpenVAS and NCATS.²⁵
- 4606 **4.12.2 Technical Capabilities Provided by Solution**
- 4607 NamicSoft provides components of the following Technical Capabilities described in Section 64608 of Volume 1:
- Vulnerability Management

4610 **4.12.3 Subcategories Addressed by Implementing Solution**

4611 ID.RA-1, DE.CM-4, RS.MI-3

²⁵ Namicsoft <u>https://www.namicsoft.com/</u>

4612 **4.12.4** Architecture Map of Where Solution was Implemented



4614 **4.12.5** Installation Instructions and Configurations

4615 Details of the solutions implemented:

	Name	Version	
	NamicSoft Scan Report Assistant	3.5.0	
4616		1	1
4617	Setup:		
4618 4619 4620 4621 4622 4623 4623 4624 4625	 Download NamicSoft from <u>https://www</u>PC. NamicSoft is currently supported of The installation is tied to a user account a different user logging in to the same set. If using for the first time, the installation entered, it runs in free mode. The free reference out on the Nessus our Process Control System. 	on 64-bit Window t. Any changes m system. on will prompt for node is limited to	as with .Net Framework 4.5 installed ade by a user would not be visible to a license file. If a license is not five hosts.
4626	Configuration for reporting Nessus scans:		
4627 4628 4629	 Export a Scan Report of nessus format Launch NamicSoft Report Assistant. C 		

4630 • Click on **Choose** button to import files

4631

4			NamicSoft Scan Report Assistant	_ 🗆 X
8	Dashboard	File Settings Tools Import	About	
	Overview Vulnerability age	Tool Description Choose file(s) to import	Nessus Import your Nessus scan results to using Nessus export to XML (.nessus format). Nessus file format v2 supported. Choose	T
쁆	Hosts	Number of files to read		
▦	Vulnerabilities	Import vulnerabilities	with the following severities	
Ð	Import	Informational 🗹 Low 🔽		
G	Export	Medium 🗹 High 🗹 Critical 🗹		
Đ	Report	Status		
٩	Actions	Elapsed time 0 Status		
		Job Id File	File size (kB) Time to import Status Hosts Vulnerabilities	
Versi	on 3.0.5.0			Import

- Browse to the nessus scan report. Under Import Vulnerabilities with following
- 4634 vulnerabilities, Check / Un-check whichever severity of vulnerabilities you wish to be
 4635 included in the report. Click Import

4636

4637 The below image shows "Informational" type being excluded. When the Import finishes, the
4638 Status bar should display All files read

4639

	K.			NamicSoft Scan Report Assistant	_ 🗆 X
	::	Dashboard	File Settings Tools Import	About	
П		Overview	Tool	Nessus	•
Ш		Vulnerability age	Description	Import your Nessus scan results to using Nessus export to XML (.nessus format). Nessus file format v2 supported.	
Ш			Choose file(s) to import	Choose 📾	
Ш	緣	Hosts	Number of files to read	1	
Ш			Files read	1	
I	⊞	Vulnerabilities	Import vulnerabilities	with the following severities	^
Ш	÷	Import	Informational		
I		import	Low 🗹 Medium 🔽		
Ш	G	Export	High 🔽		
I		Export	Critical		
I	Đ	Report	Status		
Ш			Elapsed time 7		
Ш	٩	Actions	Status All files re	ead	
l			Job Id File	File size (kB) Time to import Status Hosts Vulnerabiliti	
			Job la File	riie size (KD) Time to import Status Hosts vuinerabilitie	5
Ņ	Versi	on 3.0.5.0			Import

4640

- Upon completion of Import, go to **Hosts** page to view all the hosts level summary. Similarly,
- 4643
- clicking on **Vulnerabilities** page shows all the vulnerabilities
- 4644

-			N	amicSoft Scan Report Assistant		_ □	x
	<u>^</u>	File Settings Tools	s About				
1 ==	Dashboard	Name	IP	Operating System	MAC	NetBIOS	
	Overview	172.16.2.103	172.16.2.103				ŕ
	Vulnerability age	172.16.2.102	172.16.2.102	Digital UNIX 4.0			_
		WIN-FPVTDCDEUCR	172.16.2.14	Microsoft Windows Server 2008 R2 Standard Service Pack 1	08:00:27:AE:99:58	WIN-FPVTDCDEUCR	
윪	Hosts	fgs-61338osh.lan.lab	172.16.2.5	Windows 6.1	0C:C4:7A:32:B3:00 0C:C4:7A:32:B3:01		
		fgs-47631lhh.lan.lab	172.16.2.4	Microsoft Windows 7 Professional Service Pack 1		FGS-47631LHH	
■	Vulnerabilities	fgs-61338psh.lan.lab	172.16.2.3	Microsoft Windows 7 Professional Service Pack 1		FGS-61338PSH	
Ð	Import	172.16.2.2	172.16.2.2	CISCO IOS Cisco IOS XE			
G	Export	172.16.2.1	172.16.2.1	CISCO IOS 15.2(4a)EA5	E4:90:69:3B:C2:81 E4:90:69:3B:C2:82 E4:90:69:3B:C2:85 E4:90:69:3B:C2:C0 E4:90:69:3B:C2:C1 E4:90:69:3B:C2:C2 E4:90:69:3B:C2:C3 E4:90:69:3B:C2:C6		
Ê	Report	((1000	170 17 1 5		E4:90:69:3B:C2:C7	500 (10000)	
	V	fɑs-61338ch.lan.lab ←	172.16.1.5	Microsoft Windows 7 Professional Service Pack 1	0C:C4:7A:31:3E:D7	FGS-61338CH	→
Versi	on 3.0.5.0	Total: 13 Selected: 0					

4				NamicSoft Scar	n Report Assistant		_ 🗆 X
🚦 Dashboar	rd	File Settings Tools A	About			Optimize colums for	ALL 🔻
Overview		Host name		Host Name	Synposis	Description	Solution
Vulnerabilit	y age	fgs-47631ehh.lan.lab	^	fgs-47631lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has 1
		172.16.2.103		fgs-47631lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
윪 Hosts		172.16.2.102		fgs-47631lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
		WIN-FPVTDCDEUCR		fgs-47631lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
🖽 Vulnerabi	ilities	fgs-61338osh.lan.lab		fgs-47631lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
	_	fgs-47631lhh.lan.lab		fgs-47631lhh.la	The Microsoft Outlook application i	The Microsoft Outlook application i	Microsoft has
된 Import		fgs-61338psh.lan.lab		fgs-47631lhh.la	The Microsoft Outlook application ii	The Microsoft Outlook application i	Microsoft has
		172.16.2.2		fgs-47631lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
G→ Export		172.16.2.1		fgs-47631lhh.la	The Microsoft Excel Products are m	The Microsoft Excel Products are m	Microsoft has
		fgs-61338ch.lan.lab		fgs-47631lhh.la	The Microsoft Skype for Business o	The Microsoft Skype for Business o	Microsoft has
🔒 Report		fgs-61338hh.lan.lab		fgs-47631lhh.la	The Microsoft Outlook application ii	The Microsoft Outlook application in	Microsoft has
	V	172.16.1.3	4	fgs-47631lhh.l≀ ←	The Microsoft Outlook application ii	The Microsoft Outlook application ii	Microsoft has √ →
Version 3.0.5.0		Total: 557 Displayed: 176	Selecte				

4648 To mark a Vulnerability as Fixed, select the Vulnerability >> Right Click >> Vulnerability 4649 Fixed.

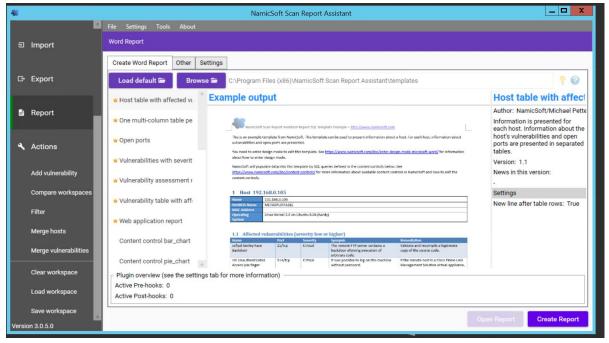
-			NamicSoft Sca	an Report Assistant		_ 🗆 X
	↑ Dealth a sud	File Settings Tools About				
	Dashboard				Optimize colums for	ALL 🔻
	Overview	Host name	Host Name	Synposis	Description	Solution
	Vulnerability age	fgs-47621-66 In- In6 🔨	f 47€31lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has $^{\wedge}$
		172.16 Edit	31lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
윦	Hosts	172.16 Delete	31lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
		WIN-FF Vulnerability fixed	31lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
⊞	Vulnerabilities	fgs-61338osh.lan.lab	fgs-47631lhh.la	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
	_	fgs-47631lhh.lan.lab	fgs-47631lhh.la	The Microsoft Outlook application i	The Microsoft Outlook application i	Microsoft has
Ð	Import	fgs-61338psh.lan.lab	fgs-47631lhh.la	The Microsoft Outlook application i	The Microsoft Outlook application in	Microsoft has
		172.16.2.2	fgs-47631lhh.la	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
G	Export	172.16.2.1	fgs-47631lhh.la	The Microsoft Excel Products are m	The Microsoft Excel Products are m	Microsoft has
- بال		faa 61220ah lan lah	fas-476311hh la	The Microsoft Skyne for Business o	The Microsoft Skype for Rusiness o	Microsoft has

4650 4651 4652

4653

4654

- Under Actions, click on Save Workspace. Ensure to Save your workspace after every change made. When running NamicSoft the next time, you can load this saved workspace file.
- 4655 4656
- To generate a Report, click on **Report.** You can select one of the default reporting templates from the list or create a custom one. To use a default template, select one from the list >>
 Create Report.



4660 • To view the Report, click **Open Report.**

4	NamicSoft Scan Report Assistant	_ D X				
Dashboard	File Settings Tools About Word Report					
Overview	Create Word Report Other Settings					
Vulnerability age	Load default 🗃 🛛 Browse 🚔 C:\Program Files (x86)\NamicSoft Scan Report Assistant\templates	9 Ø				
	Host summary table with e	ICS-LAB-Host summa				
쁆 Hosts	ICS-LAB-Host summary	Author: NamicSoft/Michael Petters A summary table of each host's vulnerabilities. The total CVSS				
Ulnerabilities	S One table per vulnerability v This is an example template from NamicSoft. This template presents an overview of the scanning result for each host. The total CVSS score is also presented each host.					
	Remediations with affected adout to enter design mode to estit this temptate. See https://www.namissoft.com/doc/enter-design-mode-microsoft-word/ for information adout how to enter design mode.	Version: 1.0 News in this version:				
된 Import	Repeat information for eacl controls. New context controls below. See	0:##/acc				
G→ Export	Ipp Iour Medium High Critical Houd (959 Vulnerabilities with highest 102.346.3307 1 0 0 224.33 193.046.0307 1 0 0 2 233.3 193.046.0309 1 0 0 0 3.3 193.046.0310 1 0 0 6.2 193.046.0310 1 0 0 6.2	Settings New line after table rows: True				
🖹 Report	Plugin overview (see the settings tab for more information) Active Pre-hooks: 0 Active Post-hooks: 0					
Actions	Status Done, report saved in C:\Users\Administrator\Downloads\Host Summary.docx					
	Time to create report 0min and 5s					
Version 3.0.5.0		Open Report Create Report				

4661

To create a custom template, copy one of the template files located under C:\Program
 Files(x86)\NamicSoft Scan Report Assistant\templates and save it to a different folder.
 Open the copied file in MS Word to begin editing. The image below shows a customized
 template file created for CRS system. This report generates a summary of hosts and their
 respective vulnerabilities based on the Severity level.

4667

4668



Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
<u>DummyValue</u>	DummyValue	<u>DummyValue</u>	<u>DummyValue</u>	DummyValue	<u>DummyValue</u>	DummyValue
queryTable y WHE	RE severitynumber ueryTable y WHER	r=2 AND y.ip=x.ip),(9 E severitynumber=(SELECT COUNT(*) FRC	ERE severitynumber=3 DM queryTable y WHER ECT ROUND(SUM(cvssE	E severitynumber=1 A	ND y.ip=x.ip), (SELECT
A summary table o	f each host's vulne	erabilities. The total	CVSS base score is als	so presented for each h	iost.	

NamicSoft/Michael Pettersson Solutions AB Host summary table Image.PNG

- Detailed instructions for creating custom reports are available on the NamicSoft website
 under <u>https://www.namicsoft.com/doc/content-controls/</u>
- Save your changes and give the file a suitable name. Copy this file back to the "Templates"
- directory. For instance, the below image shows our customized file PCS- Host Summary
 copied back to the templates folder.

🏨 l 🚅 🐘 = l		templates		_ 0	x
File Home Sha	re	View			~ ?
€ ⊚ - ↑ 👢 «	Nar	micSoft Scan Report Assistant 🕨 templates	~ ¢	Search templates	Q
☆ Favorites	^	Name	Date modified	Туре	^
Desktop		Host summary table with exploitable vul	8/20/2017 8:46 PM	Office Open XML Document	
🐌 Downloads		📄 Host summary table	8/19/2017 9:33 PM	Office Open XML Document	
🐉 Recent places		Host table with affected vulnerabilities	8/19/2017 9:54 PM	Office Open XML Document	
sec_550		ICS-LAB-Host summary	9/18/2018 10:59 A	Office Open XML Document	
		📄 One multi-column table per vulnerability	8/19/2017 9:52 PM	Office Open XML Document	
😽 This PC	=	One table per vulnerability with affected	8/19/2017 9:38 PM	Office Open XML Document	
C on PN108214		Open ports	12/9/2017 8:46 PM	Office Open XML Document	
📜 Desktop		PCS-Host summary	4/24/2019 10:05 A	Office Open XML Document	
Documents		Remediations with affected hosts	12/27/2017 8:28 PM	Office Open XML Document	
🗼 Downloads		Repeat information for each host	8/19/2017 9:42 PM	Office Open XML Document	=
b Music		Vulnerabilities with highest total Cvss	8/19/2017 9:44 PM	Office Open XML Document	
E Pictures		Vulnerabilities with severity medium or hi	8/20/2017 8:47 PM	Office Open XML Document	
Videos		Vulnerability assessment report	1/14/2019 7:46 PM	Office Open XML Document	
🤩 Local Disk (C:)		Vulnerability table with affected hosts	8/20/2017 9:11 PM	Office Open XML Document	~
	\sim	< T			>
27 items 1 item sele	ected	46.9 KB			

4675 Launch NamicSoft again. The custom report should now appear under the list. Select it and click on Create Report.

4		NamicSoft Scan Report Assistant	_ 🗆 X				
		File Settings Tools About					
-	Dashboard	Word Report					
	Overview	Create Word Report Other Settings					
	Vulnerability age	Load default 🗃 Browse 🖀 C:\Program Files (x86)\NamicSoft Scan Report Assistant\templates	?				
		Host summary table with e Texample output	ICS-LAB-Host summa				
쁆	Hosts	ICS-LAB-Host summary	Author: NamicSoft/Michael Petters A summary table of each host's vulnerabilities. The total CVSS				
⊞	Vulnerabilities	One table per vulnerability \ This is an example template from NamicSet. This template presents an overview of the scanning result for each host. The total CVSS score is also calculated per host.	base score is also presented for each host.				
		You need to enter design mode to exit this template. See https://www.namicsoft.com/doc/enter-design-mode-microsoft-word/ for information Remediations with affected advances of the set of	Version: 1.0 News in this version:				
Ð	Import	Repeat information for each on the second of					
G	Export	Image: Control of the state of the	New line after table rows: True				
Û	Report	Plugin overview (see the settings tab for more information) Active Pre-hooks: 0 Active Post-hooks: 0					
٩	Actions	Status Done, report saved in C:\Users\Administrator\Downloads\Host Summary.docx					
		Time to create report 0min and 5s					
Versi	on 3.0.5.0	-	Open Report Create Report				

• The output should appear as per your changes.



National Institute of Standards and Technology U.S. Department of Commerce

Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
172.16.1.1	172.16.1.1	4	6	2	0	58.6
172.16.1.3	172.16.1.3	1	6	0	0	36.2
172.16.1.4	fgs- 61338hh.lan.lab	3	26	39	6	542.3
172.16.1.5	fgs- 61338ch.lan.lab	3	24	42	5	547.6
172.16.2.1	172.16.2.1	4	6	2	0	58.6
172.16.2.2	172.16.2.2	0	6	0	0	33.6
172.16.2.3	fgs- 61338psh.lan.lab	2	23	41	5	538.3
172.16.2.4	fgs- 47631lhh.lan.lab	3	40	122	11	1420.3
172.16.2.14	WIN- FPVTDCDEUCR	3	18	92	11	1047.5
172.16.3.10	fgs- 47631ehh.lan.lab	0	0	0	1	10

4679

4680	• To report on Vulnerabilities remediated based off the previous vulnerability scans, use the
4681	"Compare Workspaces" feature under Action Menu
4682	• Load Nessus result from your previous scan. Save as a workspace.
4683	• Clear the workspace in the GUI (or restart NamicSoft)
4684	 Load Nessus results from the latest scan
4685	• Open Actions> Compare workspaces. Choose Compare with current workspace
4686	and point Workspace 2 to your workspace saved earlier.
4687	• Choose Excel output file (target)
4688	 Click "Compare Workspaces"
4689	4.12.6 Highlighted Performance Impacts
4690	No performance measurement experiments were performed for the use of NamicSoft due to its
4691	installation location and how it was used (i.e., the software performed offline analysis of
4692	vulnerability data captured by other software at a location external to the manufacturing system).

4693 **4.12.7** Link to Entire Performance Measurement Data Set

4694 N/A

4696 **4.13 The Hive Project**

4697 **4.13.1 Technical Solution Overview**

A scalable, open source and free Security Incident Response Platform, tightly integrated with
 MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs,
 CERTs and any information security practitioner dealing with security incidents that need to be
 investigated and acted upon swiftly.²⁶

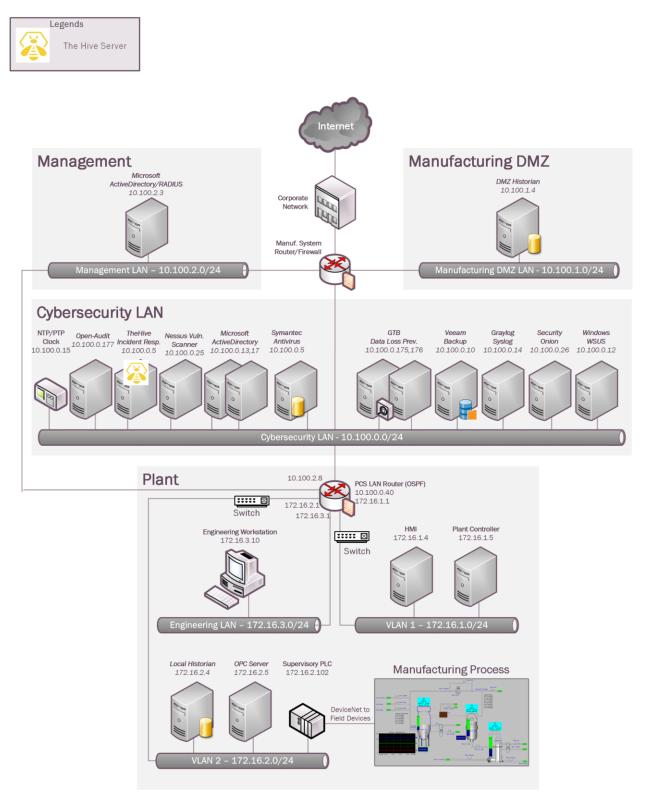
4702

4703 **4.13.2 Technical Capabilities Provided by Solution**

- 4704 The Hive Project provides components of the following Technical Capabilities described in4705 Section 6 of Volume 1:
- 4706 Incident Management
- 4707 **4.13.3** Subcategories Addressed by Implementing Solution
- 4708 RS.MI-2 and RS.MI-3
- 4709

²⁶ The Hive Project: https://thehive-project.org/

4710 **4.13.4** Architecture Map of Where Solution was Implemented



4712 **4.13.5** Installation Instructions and Configurations

4713 Setup:

- The Hive Project's website provides detailed setup <u>guide</u> for Linux platform. Additionally,
 there is a preconfigured training VM available for non-production environments. This can be
 downloaded from https://github.com/TheHive-Project/TheHive
- The preconfigured VM was deployed in our environment. Deploy the ova file on a
 Hypervisor and assign the VM a static IP address. Once done, the URL of application is
- 4719 http://IP_OF_VM:9000
- The first time you access TheHive, you'll need to create the associated database by clicking
 on the Update Database button as shown below:
- 4722

0 9000/index.html#/maintenance	< ☆ ■ ■ ■ ■
TheHive needs to update its datab	ase
Update Database	

- 4723 4724
- Follow the wizard to setup a user account. Login to TheHive url with these credentials.
- 4726

Q Case

- The default page will show you a List of Cases assigned to your account 4728 ٠
- 4729

%TheHive	+ New Case ▼	My tasks 1	Waiting tasks 🧿	Alerts 0	Lan Dashboards

list of cases (1 of 1)						
Y Quick Filters ► \$ Sort by ►			Lill Stats	Q Filters	15	per pag
filter(s) applied: status: Open 🗙 Clear filters						
Title	Severity	Tasks	Observat	oles Assig	gnee Date	
#1 - Outage 🗞 None	•	2 Tasks	0	I	09/20/1	8 13:07

- 4730 4731
- User accounts can be created by going to **Admin** >> **Users** >> **User Management** page. 4732 • Click on "+Add User" to create a new user. 4733
- 4734

4735 4736

ser mana	agement				
Add user					10 v p
Login	Full Name	Roles	Password	API key	Ad
icssec	icssec	read, write, admin	New password	Create API Key	≜ Lock
seconion	seconion	alert	New password	Renew Revoke Reveal	≜ Lock

- To create a new Incident / case, click on the "New Case" menu option and fill in all the
- 4739 details. Hit "Create Case" button when done.
- 4740

Create a n	ew case				
Case details					
Title ≭	Title		Date ≭	07-03-2019 16:37	now
Severity ≭	L M H		TLP ≭	WHITE GREEN AMBER RED	
Tags	Tags		Description	Case description	
			Ŧ		
Case tasks					
Task title					Add task
		No tasks hav	ve been specified		
Cancel *	Required field				+ Create case

4/42		
4743	٠	Once you've created a case, you can create, assign, and track tasks within a case. A task can
4744		be useful to track status updates or notes within a case. Click on "+Add Task" to add a task
4745		description under a case. Each task can be individually assigned to an analyst for the work to
4746		be performed. By default, a task doesn't have an owner until someone clicks into it, or
4747		"takes" it from the Waiting tasks queue in the top menu bar.
4748		
4749	٠	Custom Case templates can be created via the Case Template Management Screen. Click on
4750		+New Template button to create a new template of your own.
4751		
4752	٠	Custom "Observables" such as domain names, IP addresses, files, filenames etc. can be
4753		added to a case by clicking on "Observables" tab >> +Add Observables. In addition,
4754		observables can also be marked as Indicators of Compromise (IOC).
4755		

TheHive + New Case	🗕 My tasks 🚺 Waiting tasks 💿 Alerts 💿 🖬	<u>H</u> Dashboards	Q 0
Case # 1 - Outage			Merge case
Created by icssec 🗯 Thu, Sep 2	0th, 2018 13:07 -04:00	⊘ Close	🍽 Flag 💉 Merge 🗙 Remove
Tasks 2	★ Observables 0		
Action Action		Laal Stats Q Fil	Iters 15 v per page
Observable List (0 of 0)			
	No	o records.	

·) → C û [] /	2 🔏 10.100.0.51:9000/ind	ex.html#/case/AWX388aSI	Ds-nH_5cBT_H/observables	▣ ♡ ☆	\ ⊡
•*************************************	ate new observab		Q. ca	e, user, URL, hash, IP, domain 👻 🔷	Admin 🗕 🚺
M Case # 1 - Outage	Туре 🗰	domain 🗸		🖾 Open in n	ew window 🛛 🗕
🚨 Created by icssec 🗮 Thu, Sep 2	Value 🗱	autonomous-system domain		ry icssec r to replace R pleted	©5m obot
🖀 Details 🛛 🗃 Tasks 🔕		file		E Call vendor to r	
Action - + Add observable(s)	TLP 🗰	fqdn hash		cssec	© 5 m
	Tags 🗚	ip mail		Outage	
Observable List (0 of 0)	Description **	mail_subject other regexp		cssec ure gress	©5 n
		registry uri_path url	≭ Required field ≭≭ At le	ast, one required field	©6 m
Cane	el	user-agent	+0	reate observable(s) reate observable(s)	obot
				🖀 #1 - Outage 🔜 Call vendor to r	
				+ Added by icssec	©6 m

4760 Analysts can use "Cortex" engine to perform detailed analysis on observables or IOCs such ٠ 4761 as domain names, IP addresses, hashes. This can be achieved by enabling or creating 4762 Analyzers in Cortex. The default URL for Cortex Web UI is http://<CORTEX_IP>:9001 4763 4764 The high-level steps in configuring Cortex are: 4765 i. Setup Cortex Create an Administrator account 4766 ii. 4767 iii. Create an Organization Create an Organization Administrator account 4768 iv. 4769 Enable or Configure Analyzers v. 4770 vi. Integrate with the Hive instance 4771 4772 Detailed instructions on setting up Cortex are available at https://github.com/TheHive-4773 Project/CortexDocs 4774

4775 Integration with Security Onion

Integration with other products can be done via API keys to connect with the Hive. A
 dedicated user account was created for this purpose with permissions to "Allow alerts
 creation". Ensure Roles: None is set for security purposes of this user account.

4779

Add user		
Login ≭	seconion	
Full name 🗱	seconion	
Roles 🗱	none 🗸	
Additional Permissions	✓ Allow alerts creation	
Cancel		Save user

4780 4781

4783 • An API key was created for this user, by clicking on "Create API Key" for this dedicated 4784 user account

17	85
4/	0.0

user account				
User management				
Add user				
Login	Full Name	Roles	Password	API key
icssec	icssec	read, write, admin	New password	Create API Key
seconion	seconion	read, write, alert	New password	Create API Key

4786 4787

Our Security Onion instance was integrated with the Hive Instance to create a case for IDS alerts generated by Security Onion. This was accomplished by creating a new rules file
 hive.yaml under the /etc./elastalert/rules directory of the Security Onion server. Detailed instructions are available at https://securityonion.readthedocs.io/en/latest/hive.html#thehive.

4792 4793

Extract from our hive.yaml

4794

hive.yaml # Elastalert rule to forward IDS alerts from Security Onion to a specified TheHive instance. # es host: elasticsearch es port: 9200 name: TheHive - New IDS Alert! type: frequency index: "*:logstash-ids*" num events: 1 timeframe: minutes: 10 buffer time: minutes: 10 allow buffer time overlap: true filter: - term: event type: "snort" alert: hivealerter hive connection: hive host: https://10.100.0.51 hive port: 9000 hive apikey: APIKEY

4796 **4.13.6 Highlighted Performance Impacts**

4797 No performance measurement experiments were performed for the use of the Hive Project due to4798 its typical installation and usage location (i.e., external to the manufacturing system).

4799 **4.13.7** Link to Entire Performance Measurement Data Set

- 4800 N/A
- 4801
- 4802

4803 **4.14 Microsoft EFS**

4804 **4.14.1 Technical Solution Overview**

4805 EFS is file level encryption tool provided by Windows. The Encrypted File System, or EFS,
4806 provides an additional level of security for files and directories. It provides cryptographic
4807 protection of individual files on NTFS file system volumes using a public-key system.²⁷

4808 **4.14.2 Technical Capabilities Provided by Solution**

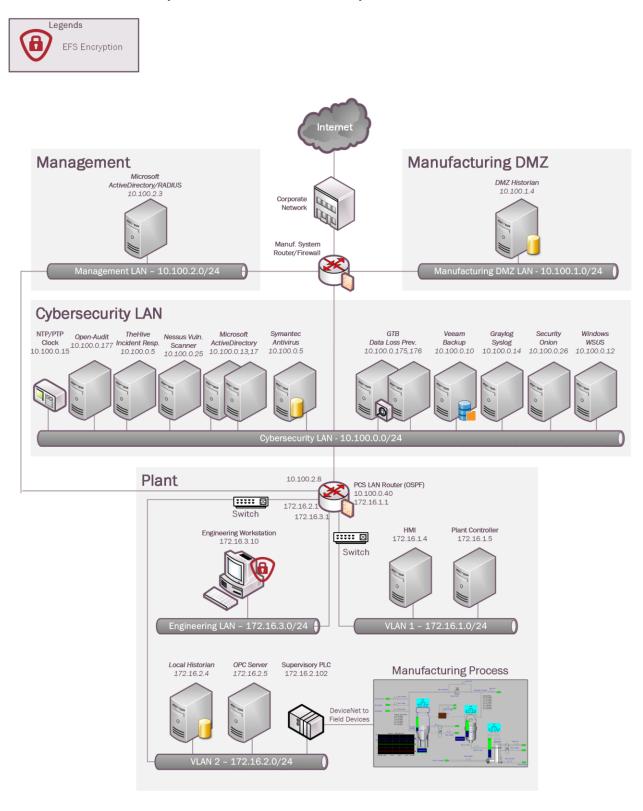
- 4809 Microsoft EFS provides components of the following Technical Capabilities described in Section4810 6 of Volume 1:
- 4811 Encryption

4812 **4.14.3** Subcategories Addressed by Implementing Solution

4813 PR.DS-5

²⁷ <u>https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption</u>

4814 **4.14.4** Architecture Map of Where Solution was Implemented



4816 **4.14.5** Installation Instructions and Configurations

- 4817 **Setup:**
- 4818 Note: These steps were performed on the below system

Hostname	IP_Address	OS
Engineering Workstation	172.16.3.10	Windows 7 Professional 64bit

4819

- Windows EFS was used to encrypt confidential folders on the Windows workstation of
 Process Control System.
- 4822 To begin encrypting, select a parent folder which you wish to encrypt. Right Click on the
 4823 Folder Name >> Click **Properties** >> General Tab >> Click Advanced

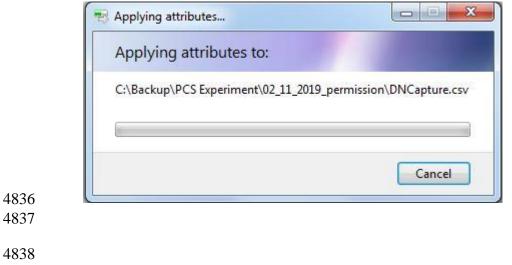
eneral Shari	ng Security Previous Versions Customize
	PCS Experiment
Туре:	File folder
Location:	C:\Backup
Size:	13.4 GB (14,399,209,230 bytes)
Size on disk:	13.4 GB (14,399,840,256 bytes)
Contains:	280 Files, 50 Folders
Created:	Today, April 16, 2019, 4 hours ago
Attributes:	Read-only (Only applies to files in folder)
	Hidden Advanced.
Attributes:	

4826

- Under Confirm Attribute Changes, choose how extensive you want the encryption to be,
- 4828 click **OK**. We recommend selecting the option of "Apply changes to folder, subfolders and
 4829 files"
- 4830
- 4831



- Click **Apply.** This will begin the encryption process.
- 4835



4839 Upon encryption, the subfolders or file names would change to Green color as shown below
 4840 Any new folder added to this parent folder will be automatically encrypted.

Name	Date modified	Туре	Size
02_11_2019_permission	4/16/2019 3:23 PM	File folder	
闄 02_14_2019_openAudit	4/16/2019 3:24 PM	File folder	
D2_24_19_firewall	4/16/2019 3:25 PM	File folder	

4841

4842 Backing up the Encryption Key

- When a file or folder is encrypted for the first time, a pop-up message saying "Backup your encryption key" should appear in the task-bar. Double click to launch the backup process.
- Alternatively, this process can also be launched manually by going to **Control Panel** >> All
- 4846 Control Panel Items >> User Accounts >> Manage your encryption certificates
- 4847 **Note**: This process is different for a Windows 10 system.



4848

4850 • Click **Next**

Manage y	our file encryp	otion certificates		
associated	decryption key o			on certificate and its You can't access your
Use this wiz	ard to:			
- Select or o	reate a file encry	vption certificate an	d key.	
- Back up th	e certificate and	key to avoid losing	g access to your er	ncrypted files.
- Set Encry	oting File System	to use a smart car	d.	
- Update pr	eviously encrypte	ed files to use a dif	ferent certificate ar	id key.
What is End	rypting File Syste	em?		

4852 • Select existing Certificate or Create a new one. It is safe to go with the default option
4853

🚱 🕺 Encrypting File System	×
Select or create a file encryption certificate	
Select an existing file encryption certificate or create a new encrypted files, you can update them to use this certificate.	one. If you have already
Use this certificate If you are using a smart card, select the certificate on the Certificate details:	smart card.
Issued to: Administrator Issued by: Administrator Expires: 3/23/2119	View certificate Select certificate
© Create a new certificate	
Why do I need a certificate for file encryption?	
	Next Cancel

4854

• Select "Backup the Certificate and Key Now". Click Browse to choose a destination for

4856 saving the pfx bundle file. For instance: a USB drive. Enter a password for added protection.

4857

his helps you avoid lo ey are lost or damage	osing access to your encrypted file ed.	s if the original certificate and
Current certificate:	Issued to: Administrator	View certificate
	the certificate and key to removab	
Backup location:	E:\efskey.pfx	Browse
Password:	•••••	
Confirm password:	•••••	
Back up the certifica Windows will remind	ate and key later I you the next time you log on.	

4858 4859 4860

4861 • Select the appropriate folder to associate with the new certificate and key OR Alternatively
 4862 select "I'll update my encrypted files later". Click Next

	ously encrypted files
	taining encrypted files that you want to associate with the new odating now helps you avoid losing access to your encrypted files to and key are lost
Folders:	
	5.)
l'll update my encry	pted files later
	ght take some time, depending on how many files you update. If
	your smart card during the process, your files will not be updated.

- A confirmation message as below will be shown next. This completes the backup of the • Recovery key 4866
- 4867

	View certificate
Issued to: Administrator Issued by: Administrator	view certificate
Expires: 3/23/2119	View log
Certificate and key backup location: E:\efskey.pfx	
L. (eiskey.pix	

4868

4869

Using Encrypted files on a Different Computer 4870

4871 If you want to use your encrypted files on another computer, you need to export the EFS

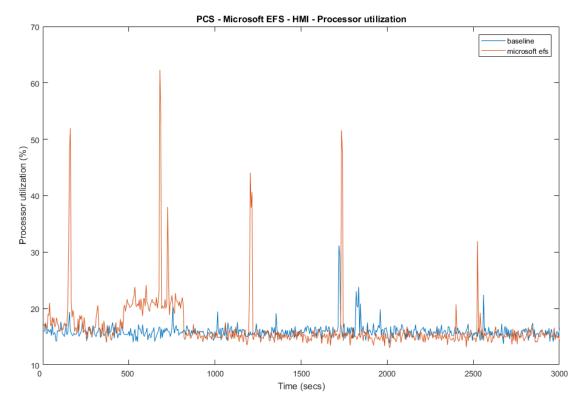
certificate and key from your computer or the USB backup and then import it at the other 4872 4873 computer.

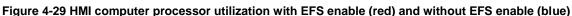
4875 **4.14.6 Highlighted Performance Impacts**

- 4876 The following performance measurement experiment was performed for the Microsoft EFS tool 4877 while the manufacturing system was operational:
- 4878 Experiment PL013.1- Enable file level encryption on HMI host

4879 The FactoryTalk HMI application has a designated file folder to contain the log files for the HMI4880 data. EFS tool was used to encrypt the data log file in this experiment.

- 4881 There were noticeable performance impacts to the computing resources observed when the EFS
- 4882 was activated for the data log files, especially at the initial operation of the HMI. The processor
 4883 utilization was noticeable higher from 450 seconds to 750 seconds experiment time and
- 4884 occasionally higher throughout the first 3000 seconds. The disk write operation was significantly
- 4885 higher in the first 800 seconds of the experiment time. The HMI application attempted to access
- 4886 the data log files at the initialization stage and therefore most of the impacts were observed at the
- 4887 beginning of the operation.
 - 4888 On the network side, no significant performance impact was observed. The packet round trip
 - 4889 time between the HMI and OPC in both directions reminded mostly constant before and after the
 - 4890 EFS was enabled.





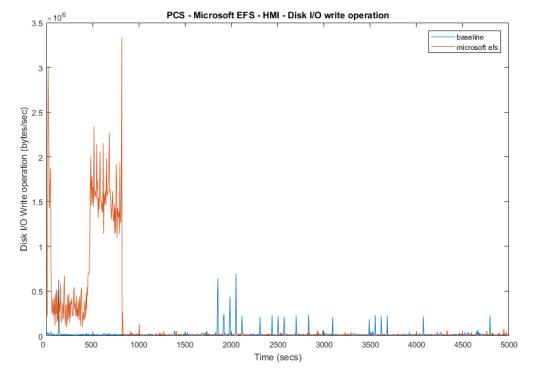
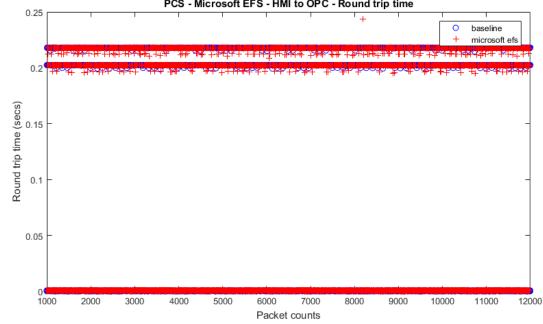
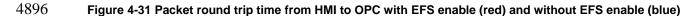
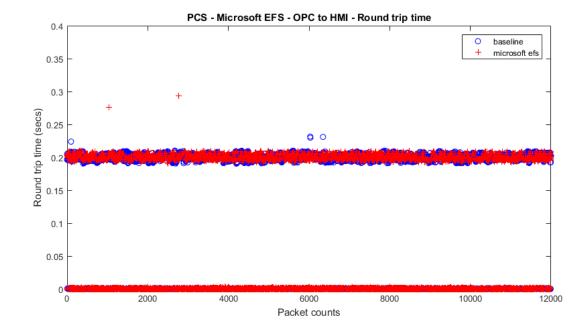


Figure 4-30 HMI computer disk write operation with EFS enable (red) and without EFS enable (blue)



PCS - Microsoft EFS - HMI to OPC - Round trip time

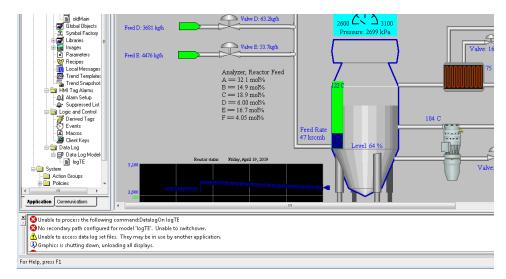




4898 Figure 4-32 Packet round trip time from OPC to HMI with EFS enable (red) and without EFS enable (blue)

4899 The HMI application was not able to access the data log files and new data from operation was 4900 not logged. The HMI flagged an error/warning message to the operator.

- 4901 Care should be taken for encrypting application specific files or folders. There is performance
- 4902 impact to the manufacturing process in the form of losing the ability to log data files in the HMI.





4904

Figure 4-33 HMI screen with warning message "Unable to access data log set files"

- 4906 **4.14.7** Link to Entire Performance Measurement Data Set
- 4907 File Encryption KPI data
- 4908 File Encryption measurement data
- 4909

4910 **4.15 GTB Inspector**

4911 **4.15.1 Technical Solution Overview**

4912 GTB Inspector by GTB Technologies is a DLP solution that has been evaluated in our lab

4913 environment for low baseline manufacturing profile. GTB Inspector's built in ability to detect,

4914 log, and block network traffic trying to leave premise. Inspector detects and blocks FTP, Email,

4915 HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured

4916 exfiltration methods. GTB Inspector is the main component that analyzes all network traffic and

depending on the configuration Bridge (In-Line), Monitoring (OOL), TAP, Transparent Proxy
(TPROXY), and Load Balancing if required. GTB Central Console which is the device Inspector

4919 reports back to, so there is always a log of violation that occurred. Central Console allows for

- 4920 groups and escalation paths depending on the alerting required.
- 4921 GTB is configured within the corporate network. This option was chosen to ensure we could get4922 the best protection for the entire environment.

4923 All DLP products have a high cost to implement, but GTB Technologies provides a product that4924 can grow as your company does.

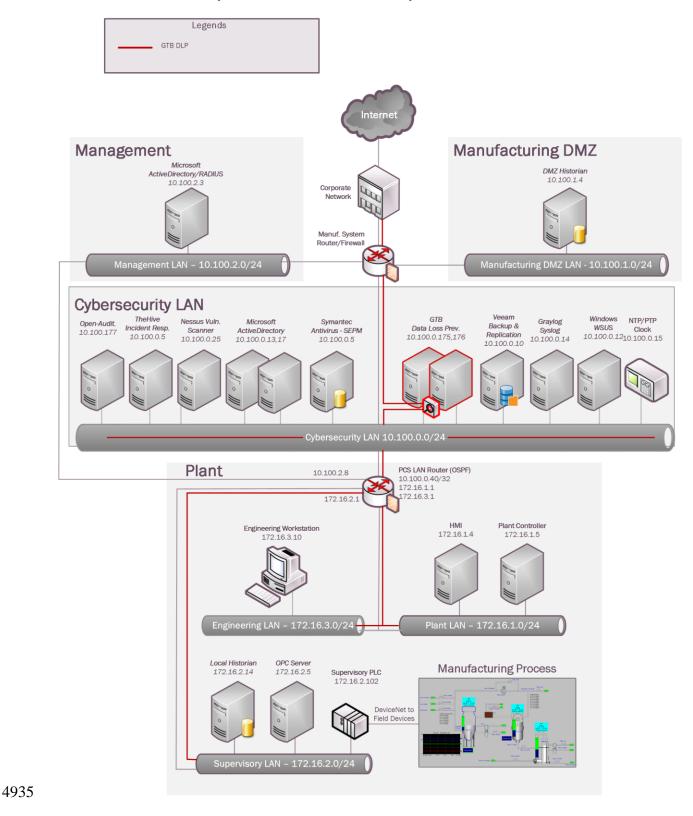
- 4925 Once installed and configured system requires little maintenance.
- 4926 Install time within the lab was approximately 16 hours for configuration, but for simple data4927 capture setup took about an hour.

4928 **4.15.2 Technical Capabilities Provided by Solution**

- 4929 GTB Inspector provides components of the following Technical Capabilities described in4930 Section 6 of Volume 1:
- Data Loss Prevention

4932 **4.15.3 Subcategories Addressed by Implementing Solution**

4933 PR.DS-5



4934 **4.15.4** Architecture Map of Where Solution was Implemented

4936 **4.15.5** Installation Instructions and Configurations

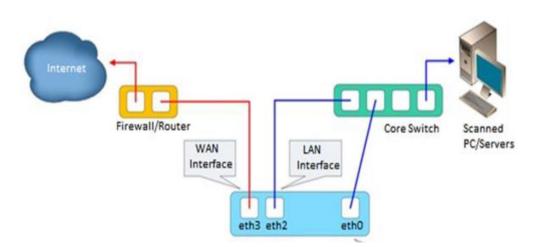
4937 Steps for installing GTB Central Console and Inspector

- Both products are virtual machines and downloadable from <u>https://gttb.com/downloads/</u>
 select desired product for download.
- Once downloaded extract each zip file to its own folder.
- 4941
 Inside newly created folders there'll be a "installation guide" along with the extracted files for each product.
- 4943 See attached PDF for current "system requirements" for each component being installed.



GTB DLP Installation Requirements for a G

4946
 Currently "GTB Inspector" network configuration is enabled in "Bridge [Inline]"
 4947
 4948
 methods. Displayed is Bridge [Inline] mode which monitors.



4950

4945

4949

4951 Hyper-V Install Configuration

4952 Create two virtual machines (See below for current specification of our environment) 4953 GTB Inspector (VM #1) • VHDX -- D:\Hyper-V\GTB InspectorVirtual Hard Disks\GTB Inspector.vhdx 4954 • Memory – 16GB (16384MB) 4955 \circ Processor – 4 CPU 4956 4957 • Network Adapter 4958 "vswitch TestBed LAN" Management Port Management port IP is (10.100.0.175) 4959 • 4960 "Eth2 for GTB Inspector" Connects to Monitor Port 1 on Tap Device 4961 "Eth3 for GTB Inspector" Connects to Monitor Port 2 on Tap Device • 4962 GTB Central Console (VM #2)

4963	0	VHDX D:\Hyper-V\GTB Central Console\Virtual Hard Disks\GTB Central Console.vhdx
4964	0	Memory – 16GB (16384MB)
4965	0	Processor – 4 CPU
4966	0	Network Adapter
4967	-	"vswitch TestBed LAN" Management Port / Connection
4968		• Management Port / Connection IP is (10.100.0.176)
4969	Install Instru	uctions for Each Virtual Machine and any additional configuration
4970	• Inspe	ector
4971	0	See install guide for most updated instructions, or attachment below. Changes
4972		made within our environment are included below.
4973	0	Each network connection was installed and rebooted to ensure they were assigned
4974		correct name / location, and if not, this command can be used to rename the
4975		network to reflect and needed changes. /usr/local/gtb/libexec/manage_nics -i ethX -o ethX
4976		(This syntax is included within installation guide)
4977	0	IP Address (10.100.0.175)
4978	0	Hostname = gtbinspector / gtpinspector.lan.lab
4979	0	Created DNS A record for "gtbinspector" along with reverse lookup
4980	0	Configured LDAP integration with Active Directory (10.100.0.17)
4981	0	UPN is required for username
4982	0	Configured email
4983		 SMTP Server Hostname (postmark.nist.gov)
4984		 Send email from (<u>GTBInspector@nist.gov</u>)
4985		 SMTP Server Port (25)
4986	0	Check and ensure LAN and WAN interfaces are configured for eth2 (WAN) eth3
4987		(LAN)
4988		 Configuration tab, Network, #-3 and #-4
		PDF
		GTB Inspector
4989		Installation Guide.pdf
4990	Centr	ral Control
4991	0	See install guide for most updated instructions or attachment below. Changes
4992		made within our environment are included below.
4993	0	IP Address (10.100.0.176)
4994	0	Hostname = gtbcc / gtbcc.lan.lab
4995	0	Created DNS A record for "gtbcc" along with reverse lookup
4996	0	Configured LDAP integration with Active Directory (10.100.0.17)
4997	0	UPN is required for username
4998	0	Configured email
4999		 SMTP Server Hostname (postmark.nist.gov)
5000		 Send email from (<u>GTBInspector@nist.gov</u>)

SMTP Server Port (25)



Installation Guide.pdf 5002 Install information for VMware 5003 • 5004 Install 0 5005 Installed a separate physical machine with vSphere (10.100.0.180) for testing 5006 since problems were observed with Hyper-V ability to block rule violations 5007 with HTTP/HTTPS traffic. Configured two network cards in vSphere for pass thru access. This was 5008 . 5009 completed to give the virtual machine access to physical network cards to 5010 eliminating possible configuration issues being observed in Hyper-V. (Will try 5011 to confirm if possible still exist with Hyper-V since new release from GTB 5012 has been released) 5013 GTB's Inspector (10.100.0.181) is currently at release 15.4 and contains an 5014 option under "Configuration → Network" labeled (Failover Mode). In our 5015 environment this option is set to "NO" since we don't have a bypass card 5016 installed. This setting allows all web traffic to be filter via scanning engine. Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode. 14 Failover mode 5017 Email filtering is designed to use "MTA" from Inspector and then forward 5018 along to intended recipient after been scanning for any rule violations. 5019 Added GTTB Certificate to "Default Domain Policy" so any machine within 5020 5021 the domain will update with the required Trusted Certificate Authority so as 5022 not to get a warning message. (Confirmed working) 5023 5024 Lesson learned: 5025 Microsoft Hyper-V solution detects and logs traffic, however even when configured for blocking, only detection occurs. Support has 5026 5027 indicated that this is since we're not using a bypass network card stated earlier with a physical box. 5028 5029 5030 **Performance Impact:** 5031 This tool has not been configured and ran against ICS enclaves currently, so there has been no performance impact that were aware of. 5032 5033 5034

5035	Specific configuration steps for GTB's Inspector and Central Console					
5036 5037 5038 5039	This section contains information for configuration within our environment. If scanning email for content violation, you'll need to configure email clients to point SMTP to 10.100.0.175 (Inspector - MTA) for email scanning. For additional configuration information please see vendors Administrator Guides which are included in download package from vendor.					
5040	Inspector					
5041	Generating and applying License:					
5042	• Generating					
5043	 Click on middle top web page once logged into Inspector 					
5044	License expires in 349 days ●					
5045	• You will now be directed to a page that allows you to download, email, or					
5046	upload a license file.					
5047	• License files should be emailed to support@gttb.com . Support will reply					
5048	with an updated file to be uploaded.					
5049	When to generate a new license file					
5050	• Anytime a network change effects the MAC (Media Access Control) address for					
5051	Inspector you'll need to generate a new license key an email support@gttb.com.					
5052	Before emailing change the extension from ".dat" to ".txt". Example: Inspector					
5053	– " <mark>7-31-2018-sysinfo_inspector.dat to 7-31-2018-sysinfo_inspector.txt</mark> ". This					
5054	change may be required if your email provider blocks ".dat" file extension.					
5055	Configuration Setting					
5056	 Login into GTB Inspector web page and click "Configuration" tab. 					
5057	Events Rule Viewer Quarantine Configuration Logs Statistics Administration					
5058	• All setting are accessible via "Groups" located on left side of webpage.					
5059	 Central Console = "gtbcc.lan.lab" 					

Network

CSF MFG PROFILE LOW SEC LVL EXAMPLE IG PROCESS-BASED MFG SYSTEM USE CASE

5060

• Network = Screenshot below

1	Inspector location	GTBInspector.lan.lab	The location or hostname the Inspector appliance.
2	Deployment mode	TPROXY	Deployment mode of the Inspector: "OOL" for Out-of-Line, "BRIDGE" for Inline, "TAP" for a Tap connection, "TPROXY" for Transparent Proxy.
3	LAN interface	eth2	LAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming from. It is being used in all Inspector modes.
4	WAN interface	eth3	WAN Interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming to. It is being used in TAP, BRIDGE, and TPROXY modes.
5	OOL LAN	10.100.0.0/24, 172.16.3.0/24	List of source IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode.
6	OOL WAN		List of destination IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode. An empty entry accepts all WAN packets.
7	TPROXY LAN	10.100.0.0/20,192.168.0.0 /20,172.16.0.0/20	List of source IP addresses or subnets separated by commas which HTTP/HTTPS traffic is being inspected in the TPROXY mode.
8	TPROXY source exceptions	10.100.0.14, 10.100.0.11	List of source IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line
9	TPROXY destined exceptions		List of destination IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
10	TPROXY IP address	10.100.0.175	IP address of TPROXY NIC device.
11	TPROXY netmask	255.255.255.0	Subnet mask of TPROXY NIC device.
12	TPROXY gateway	10.100.0.1	Default gateway of TPROXY NIC device.
13	TPROXY routing	10.100.0.0/24 via 10.100.0.1 dev eth0 192.168.0.0/20 via 10.100.0.1 dev eth0 172.16.0.0/20 via 10.100.0.1 dev eth0	Static routing rules each on a separate line. Example: 192.168.0.0/24 via 191.168.0.1 dev eth0. Where 192.168.0.0/24 is destination host/subnet, 191.168.0.1 is a gateway, eth0 is a NIC device of the Inspector.
14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.
15	OOL/TAP blocking	Yes	Select "Yes" to enable blocking in OOL/TAP modes.
16	Blocking interface	eth2	Network interface name for sending TCP Reset or FIN packets in "TAP" mode (ie. eth0, eth1, eth2, or eth3).
17	DNS servers	10.100.0.17, 10.100.0.13	DNS servers IP addresses separated by commas.
18	Network Overload Protection	No	Enable skipping stream inspection (BRIDGE mode only) due to excessive network traffic.
19	Network MTU	9000	The maximum transmission unit size for inspection ports (LAN and WAN), this can be up to 16110.

5061 5062 5063

o **Emai**l

Emails Alerts = Screenshot below

1	Security Respondents	wesley.downard@nist.gov,neeraj.shah @nist.gov	Default Security Respondents - list of email addresses separated by commas.
2	Special Case Security Respondents		Format: [Policy: list of email addresses separated by commas]. Example: PCI: demo@gttb.com
3	MD5 Recipients		Email address receiving MD5 of triggered events.
4	System Administrator Email	wesley.downard@nist.gov,neeraj.shah @nist.gov	System Administrator email address(es) separated by commas.
5	Notify about system errors by email	Yes	Select "Yes" to notify System Administrator about system errors by email.
6	Send Emails From	GTBInspector-ICSLab-220- A230@nist.gov	Email address, appears as the source of the email notification.
7	SMTP Server Hostname	postmark.nist.gov	The IP address or domain name (FQDN) of the SMTP server. This address is required in order for the Inspector to send emain notifications.
8	SMTP Server Port	25	The SMTP server port number. Typically, it is port 25.
9	Use SSL/TLS	No	Select "Yes" to use SSL/TLS encrypted connection.
10	Email Username		Authenticated Email Username.
11	Email Password		Authenticated Email Password.
12	Time between Alerts	60	Minimum interval in seconds, between alert emails.
13	Enable HTTP Block Response	Yes	Select "Yes" to return an alert page to a web browser when HTTP request is blocked.
14	HTTP Response Message	http://testpage.gtbtechnologies.com:	Response message in HTML or redirect URL returned when the HTTP session is blocked.

• LDAP Intergration = Screenshot below

1	LDAP Server Hostname	10.100.0.17	IP address or hostname of the corporate LDAP server.
2	LDAP Server Port	389	LDAP server port.
3	LDAP Username (bind DN)	gttbldap@lan.lab	Example: Domain\Username (for MS Active Directory), cn=Admin,o=MyOrganization (for Novell eDirectory or OpenLDAP).
4	LDAP Password	*****	LDAP password.
5	LDAP SSL	No	Select "Yes" to use SSL connection to the LDAP server.
6	LDAP Cache Refresh Period	1800	Period in seconds used for LDAP objects cache periodic refreshes. Zero means no periodic refreshes.
7	Hostnames Cache Refresh Period	3600	Period in seconds used for hostnames cache periodic refreshes. Zero means no periodic refreshes.
8	NRH UDP Port	2222	UDP port for receiving reports from Name Resolution Helpers (the device acts as server).
9	Cache Persistence Timeout	450	User names cache persistence timeout in seconds. If the system is stopped for more than timeout specified, cache becomes obsolete and is dropped. Zero means "never obsoleted".

5068

CSF MFG PROFILE LOW SEC LVL EXAMPLE IG PROCESS-BASED MFG SYSTEM USE CASE

5069

• Mail Transfer Agent = Screenshot below Mail Transfer Agent

1	List Of Allowed Hosts	*	Allowed hosts for email processing. Insert hostnames or IP addresses in separate rows. Insert * to accept emails from any host. A blank field means emails are rejected from any host.
2	Route Emails	Yes	Select "Yes" to have MTA route all emails to the next email hops listed in the "Domain Routing Rules" field.
3	Email Username		Authenticated next email hop Username. Example: demo@gttb.com.
4	Email Password		Authenticated next email hop User Password.
5	Domain Routing Rules	* 129.6.16.94	This entry contains routing rules per email domain on separate lines. Each rule consists of a domain pattern and a list of hostnames to which MTA will attempt to relay emails for this pattern. Use a colon to separate hostnames. Use double colon to specify a port number. Example: *.com 192.168.0.1192.168.0.100, *.net 192.168.1.1:2525
6	Excluded domains		Emails destined to these domains will be passed without inspection. Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
7	Bcc domain inspection		List of email domains for inspection only (without routing). Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
8	MTA Listening Ports		List of listening TCP port numbers separated with colons. Default is 25. Example: 25:465
9	Email Size Limit	20	Maximum allowed email size in MBytes which is accepted for delivery and inspection. Value "0" means unlimited size.
10	Alert on Queue Above	4	System will alert Administrator hourly, when the number of email messages in the MTA queue is above this value. Set 0 to disable it.
11	Backup Emails	None	Enable email backup system.
12	Reject Email on fail	No	Select "Yes" to enable email rejection when inspection fails.

5070 5071

5072

\circ SIEM = Screenshot below

SIEM			

1	SIEM Receiver Hostname	10.100.0.27	IP address or hostname of the corporate SIEM receivers separated by commas.
2	Log Content	Yes	Select "Yes" to include security events triggers into the SIEM message.
3	Arcsight CEF	Yes	Select "Yes" to use Arcsight Common Event Format in the SIEM messages.

• SSL Proxy = Screeshot below

SSL Proxy		
General		
Enable SSL Proxy	Yes No	Select "Yes" to enable SSL Proxy.
Proxy Port	3128	SSL Proxy listening port.
Transparent Proxy HTTP Ports	80	List of HTTP ports separated by commas for transparent proxy. Works only in the TPROXY mode. Example 80, 81, 82.
Transparent Proxy HTTPS Ports	443	List of ports separated by commas for which HTTPS decryption is preformed transparently. Works only in TPROXY mode. Example: 443, 444, 445,
Transparent Proxy Source IP	Yes No	Select "Yes" to enable source IP address in TPROXY mode (allows user client IP to the firewall).
Enable RESPMOD	Yes O No 🖲	Enables server response inspection.
RESPMOD for internal servers	4	Inspects responses of external requests to internal servers such as OWA, WEB-Servers, etc. Make sure traffic is forwarded on the same port to the Inspector. Example: 192.168.0.10:444, owa.gttb.com:445.
RESPMOD for internal users	4	List of IP addresses or subnets for which responses inspection is enabled. Example: 192.168.0.0/24, ws12.local
Bypass inspection on failure	Yes No	Select "Yes" to bypass on failure and forwards traffic without inspection.
Proxy Server Identity	gtbinspector	The Inspector name, which is shown in user browsers in case of SSL Proxy errors.
System Administrator		Email address of System Administrator shown in SSL Proxy errors.
Append domain name		Appends local domain name to hostnames without any dots in them. Must begin with a period. Example: .foo.net
Access Control		Example: .roo.net
		List of source IP address or subnets which are restricted to use the SSL Proxy.
Restricted Sources		Example: 192.168.1.10, 192.168.2.0/24.
Restricted Destinations		List of destined domains which are basically blocked by SSL Proxy. Example: foo.net, www.bar.net.
Allowed ports		List of ports which are allowed SSL Proxy to connect to. Example: 21.80.443
SSL Decryption		
	Issued to: www.gttb.com CA	
Current Certificate	Issued by: www.gttb.com CA Issued by: www.gttb.com CA Valid from 06.15.2012 to 05.28.2024	Detailed information about the certificate used for the HTTPS decryption.
Download Certificate	Public certificate Key and certificate	Save and view the certificate used for HTTPS decryption.
Upload Certificate	Browse No file selected.	Customer defined SSL Certificate in PEM format to be used for HTTPS decryption. The file should include both RSA private key and public certificate in plain text.
Block Invalid Sites	Yes 🔿 No 💿	Select "Yes" to block destined domains with invalid certificates.
Exception Source List	b.	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: 192.168.1.10, 192.168.2.0/24.
Exception Source List file (Upload empty file to clear list)	Browse No file selected.	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each sourse should be on a separate line no other separators are needed. Example: 192.168.2.0/24 foo.net www.bar.net
Exception Source List Download	Source exceptions file was not uploaded.	List of sources IP and domain addresses file download.
Exception Destinations List		List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: www.bar.net, .foo.net, . 192.168.1.10,192.168.0.1/24.
Exception Destinations List File (Upload empty file to clear list)	Browse No file selected.	List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each source should be on a separate line no other separators are needed. Example: 192.168.1.0 192.168.2.0/24 .foo.net www.bar.net
Exception Destinations List Download	Destination exceptions file was not uploaded.	List of destination IP and domains address file download.
Enable SSLv2	Yes O No 🖲	Select "Yes" to enable SSLv2.
Enable SSLv3	Yes O No 💿	Select "Yes" to enable SSLv3.
Enable TLSv1.0	Yes No	Select "Yes" to enable TLSv1.0.
Enable TLSv1.1	Yes • No O	Select "Yes" to enable TLSv1.1.
Enable TLSv1.2	Yes No	Select "Yes" to enable TLSv1.2.
	Apply Settings Discard Setting	15

5077	•	Administration setting
5078		Events Rule Viewer Quarantine Configuration Logs Statistics Administration
5079		• Licensing = Used for download and uploading license information.
5080		• Health Check = Ability to perform "Self-Test" to check Inspector install health.
5081		• Account Manager = Used to add new personal who will be administrating
5082		Inspector or responding to alerts for further investigation.
5083		 System Time = Screenshot below
		System Time
		Edit Date/Time: 08/02/2018 11:30:10
		Edit NTP Server: 10.100.0.15
		Select Timezone: (GMT-05:00) Eastern Time (US & Canada)
5084		
5085	<u>Centr</u>	al Console
5006		
5086		Generating and applying License:
5087	٠	Generating
5088		• Click on middle top web page once logged into Central Console
		Please acquire Endpoint licenses (support@gttb.com)
5089		•
5090		• You will now be directed to a page that will allow you to download, email,
5091		or upload a license file.
5092		• License files should be emailed to support@gttb.com . Support will reply
5093		with an updated file to be uploaded.
5094	•	When to generate a new license file
5095		• Anytime a network change effects the MAC (Media Access Control) address for
5096		Central Console you'll need to generate a new license key and email it to
5097		support@gttb.com. Before emailing change the extension from ".dat" to ".txt".
5098		Example: Central Console - 7-31-2018-sysinfo_cc.dat to 7-31-2018-
5099		<pre>sysinfo_cc.txt</pre> . This change may be required if your email provider blocks ".dat"
5100		file extension.
5101	•	System settings
5102		• Click on "DLP Setup" tab
5102		-
		 Network (Located under Categories)
5104		Enter required information. See below for screenshot Parameter Value
		This Console's IP or Domain name: 10.100.0.176
-10-		DNS Server IP : 10.100.0.17,10.100.0.13 Test Connection
5105		
5106		• Click save to continue.
5107		

5108	o LDAP	•				
5109	•	Enter information	n for screenshot below. This	s user ha	s been crea	ated and
5110		only has Domain	User right. Check for passy	word in	database.	
		LDAP				
5111		ID LDAP Server I 10.100.0.17	Port Is Forest ? Domain\Username 389 gttbidap@km.lab		Password	Use SSL Refresh, Hrs 24
5112	•	User name = gttb	lab@lan.lab			
5113	•	Password = check	k database			
5114	•	LDAP Server $= 1$	0.100.0.17			
5115	o Email	and alerts				
5116	•	Enter information	n from screenshot below			
		Parameter	Value			
		Email Server:	10.100.0.175	±.	Send Test E	mail
		Email Port:	25		(i)	
		Email User Name:		0	•	
		Email Password: Email Originator:	GTBCC-ICSLab-220-A230@nist.gov	P	(i) (i)	
		Encryption:	None	~	() ()	
		Alert manager:	Network (SMTP only)		(i)	
		-	Save Cancel		-	
5117						
5118	•	Email Server $= 1$	0.100.0.175			
5119	•	Email Originator	= <u>GTBCC-ICSLab-220-A2</u>	230@nis	st.gov	
5120	•	Click save				
5121	○ Data a	and Time				
5122	•	NTP Server $= 10$.100.0.15 (Click set time to	sync)		
5123	•	Time Zone = Eas	stern Time (US and Canada)) (Click	Apply to sa	ave)
5124	•	Click Save				
5125	Other settings under l	DLP Setup \rightarrow Sys	stem aren't currently config	ured Th	nese setting	will be
5126	updated an included v			urea. II	lebe betting	, , , , , , , , , , , , , , , , , , , ,
5127			ve Directory using LDAP it		nmended to) use
5128	Secure LDAP to ensu	re user name and	password are not sent in pla	untext.		
5129	How	ACL rules are cr	reated for use with GTB D	LP Insp	ector.	
5130 5131	GTB DLP Inspector configured rules.	views data as it j	passes thru the device and	respon	ds based o	n
5132	GTB Central Conso	le is the portal we	ere all policy rules and oth	er setti	ngs are co	nfigured.
5133	ACL Rules:					
5134	• Login into to	Central Console v	ia web browser (E.g. 10.10	0.0.176)		

- 5135 • Now click on **DLP-Setup** → **Network DLP** to access rules.
 - Dashboard All Events Network Events Discovery Events Cloud Events Endpoint Events Reports Network Status Accounts Manager DLP Setup Network DLP Discovery
- 5136 • Now, look to the left of window under categories and select your Inspector installation. 5137 Categories Inspectors (1)

GTBInspector.lan.lab

- 5138 Once selected you will see on the right current ACL Rules being applied. 5139
- Click Add button. +Add 5140 •
- 5141 A new window will appear titled "Add New ACL Rule" •

Source:	Any				
Protocol*: Source:					
Source:					
	Any				
estination:	Any				
ile type:	None				
ile size:	Any				
Comment:					
Enforcement: + Add X Delete Policy/Sets	1	Action	Alerts	File capture	
		Log	Alerta		* +
		5			

5142

- Now type in a name for the new rule being created. 5143
- Change Protocol to desire setting. This can be left to "ANY" which will look at all 5144 • protocols passes thru the Inspector (This may cause a performance impact on you 5145 Inspector installation depending on the number of clients within your organization). 5146
- Source: Choices are \rightarrow Any, IP Address, Hostname, Hostname (Custom), and 5147
 - Group (User/Computer).
- 5149 • Destination: Choices are \rightarrow Any, IP Address, Hostname, Hostname (Custom), and 5150 Group (User/Computer).
- File type: Choices are \rightarrow None, All Files, Encrypted, and Extension. 5151
- File Size: Choices are \rightarrow Any, and Not more than. 5152 ٠

• **Comments:** Give a description of the rule being applied then click **Add** button.

lame*: ∕rotocol×:	CRS				
ource:	Any				
estination:	Any				
ile type:	None				
ile size:	Any				
Enforcement:		o Collaborative F	oodus system		
Enforcement: + Add X De Policy/Sets	lete	Action	Alerts	File capture	
Enforcement:	lete			File capture	î i
Add X De	lete	Action	Alerts		±+
Add X De	lete	Action	Alerts		Ŷ.

- 5154 Cancel
 5155 Once Add has been clicked you'll have an option to select a "Policy/Sets" to enforce.
 5156 Default policies that are enforce are (Credit Card Number CCN and Social Security
 5157 Numbers SSN).
 5158 Next, select the action to be taken. There are four choices, Log, Block, S-Block, and
 5159 Pass.
- Now select if you would like additional personal to be notification upon rule violations.
- Finally, place a check in **File Capture** if you want to retain a copy of the offending data.
- Click **Save** to complete.
- Last step is to click on **Deploy all** button. This sends newly created policy to Inspector.
 This button will have a red blinking box around it indicating required action.
- 5165 Geploy all
- 5166

5167 **Useful Information:**

- Once a new rule has been created double click on that rule to adjust the ordering from top to bottom by click the UP or Down arrows towards the right.
- 6 Remember rules work from Top → Down, so think about ordering process. If unsure move the rule all the way to the top and then click Deploy all again.
- 5172
- 5173

5174 How to Fingerprint Files using GTB Security Manager for DLP Protection

5175 Download:

- First download "GTB Security Manager" by clicking on Help tab within Central Console server web portal then select "GTB Security Manager" link to start download.
 Dashboard Al Events Network Events Discovery Events Cloud Events Endpoint Events Network Status Accounts Manager OLP Setup Mantenance Logs Help
 GTB Security Manager (19 MB) - Fingerprinting Management System
 Select location to save file being downloaded.
- Double click to start install for "GTBSecurityManager_15.3.0.msi" from location 5182 where file was saved to (version number might be different than one listed above).
- Once first screen appears click on "Next" to continue.

		_	×	
	Velcome to the GTB S Setup Wizard	ecurity Manager		
Manager and Manage	he Setup Wizard allows you to d lanager features are installed on ' om your computer. Click Next to etup Wizard.	our computer or to remove		
GTB Technologies Data Loss Prevention				
	Back	Next Cancel		
Salaat Vaa ta Li	aanaa A aana	amont and	aliale (N	ant? to cont
_	cense Aggre	ement and		ext" to cont
률 GTB Security Manager Setup		ement and	click "N ×	ext" to cont
		ement and		ext" to cont
GTB Security Manager Setup End-User License Agreement Please read the following license a	: ngreement carefully	ement and		ext" to cont
GTB Security Manager Setup End-User License Agreement Please read the following license a G End User License and Warrant	greement carefully TB Technologies, Inc. by Terms & Conditions For: G1	-		ext" to cont
Please read the following license a	The service of the se	E's Information Leak and Waranty Terms & and Waranty Terms & nologies ("GTB") for the burger? either embedded and for the waranties for ware's to be homedded screek to be homedded screek to be homedded		ext" to cont

Print Back Next Cancel

5186

• Leave Destination Folder as default and Click "Next"

GTB Security Manager Setup		-	×
Destination Folder			
Click Next to install to the default folder of	or dick Change to choose anothe	r.	8
Taskill CTD Casarita Massaraha			
Install GTB Security Manager to:			
C.) Deserver Files (+OC) CTD To the dealer	Count Manage		-
C:\Program Files (x86)\GTB Technologies	Security Manager\		
<u>C</u> hange			

- 5188 5189
 - 9 Click "Install" to continue.

TB Security Manager Setup	-		2
eady to install GTB Security Manager		(õ
Click Install to begin the installation. Click Back to review or settings. Click Cancel to exit the wizard.	r change any of you	r installation	
Back	Install	Cano	al

5190

5196

5197

5198

5199

5200 5201

- When prompted by User Access Control (UAC) enter administrator password to continue install.
- If prompted to close Open Applications, select either option. Reboot is required if second option is selected.
- Click "**OK**" to continue.
 - Once install has completed click "Finish" to complete install.
 - If prompted to reboot, select "Yes". MAKE SURE TO SAVE ALL OPEN FILES BEFORE SELECTING "YES"

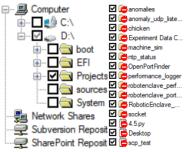
뤻 GTB Se	curity Manager Setup	\rightarrow	$\langle \rangle$
i	made to GTB Security Mar	tem for the configuration changes nager to take effect. Click Yes to lan to manually restart later.	
	<u>Y</u> es	No	

- Once machine has completed rebooting open "GTB Security Manager" by right click and selecting "Run as administrator"
 - When prompted enter administrator password for application to start.

- Once "GTB Security Manager" has opened, click on setting button on menu bar.
- 5204 File Profiles View Command Settings Window Help
- Now enter the IP Address of where "Central Console" is installed. Login and password are already populated with default credentials from vendor. Both can be changed. See foot notes for additonal steps required to change Fingerprint Inspections login an password.

Slobal Settings	
Connection Advanced Network	
Device Connection	
Database IP Address 10 · 100 · 0 · 175	
Login (Customer Code) myfingerprints	
Password	
OK Cancel	

- Once IP Address has been enter click "**OK**" to save changes.
- Now, click on File from menu bar and select New → New File Profile
 File Profiles View Command Settings Window
 New →
 New File Profile
 Open Profile
 New Query Profile
- 5212 A new window will appear allowing the ability to select files to be added. Files can be copied to Local Machine, or accessed from a Network Share, Subversion
 5215 Description
- 5215 **Repositories,** or **SharePoint Respositories.**
- Select the folder, or files that need fingerprinting. Once a folder is selected all files within selected folder will recive a check mark indicating which files will be fingerprinted.



- Now click on floppy disk icon to save.
- Select location to save newly created profile.

- Now the profile has been saved click the **padlock** icon to start fingerprinting process
- 5222 (Depending on the number of files being fingerprinted this can take a few minutes).
 5223 To view the process see the Output screen that will display what files have been
- To view the process see the Output screen that will display what files have been 5224 processed and there status. Once completed click **Close**

Fingerprinting				
4	Processed 570 Fingerprinti	Skipped 140 ng : 100,00 %	Total 570	
[Close	Stop		

- Now look to the right side window for a tab labeled "Profiles" if this is missing click on
 "View" from menu bar and select "Profiles Window". Click on Profile tab and a slide
 out appears show all the Profiles that can be monitored.
- Now select the Profile that was created earlier and right click, then select Start
 Monitoring.
 - Once monitoring is enabled it'll appears under "Currently Monitoring" under help. Currently Monitoring ProjectsFromCRS.pf
- Files that were included in fingerprinting profile will now have ACL rules applied from
 Network DLP section from Central Console.
- Login to Central Console and navigate to Account Manager Tab and click Refesh
 Polices.
- Dashboard
 All Events
 Network Events
 Discovery Events
 Cloud Events
 Endpoint Events
 Reports
 Network Status
 Accounts Manager

 5237
 Scient Filters
 Reset View
 Create User Account
 Refersh Policies
 Vou'll see a message indicating Fingerprint polices successfully synchronized.



5225

5231

- 5240 How to add policy to GTB Central Console for detecting fingerprinted files
- Login to Central Console
- Click on DLP Setup tab. DLP Setup
- Now select Policy Management tab. Policy Management
- Now double click on Default to launch a new window.
- Click Add Policy. + Add Policy
- Click drop down and select File. File

- Now click save button for setting to be applied.
- All fingerprinted files from above steps will automatically be added to default Network DLP
 policy applied ACL. New Default values are "SSN, CCN, and File"

5251 Additional Information for Fingerprinting:

- Recommended to configured GTB Security Manager to connect to IP address of DLP
 Inspector.
- Fingerprint only allows for one active Profile at a time. If another profile is set to Start
 Monitoring you'll receive a warning asking if you'd like to disable the active profile.

Profile × GTB Security Manager is currently monitoring files from another profile. By clicking Yes, monitoring will stop for C:\Users\wnd1\Documents\GTB Information\Finger Printing\ProjectsFromCRS.prf profile and start for current profile. Do you wish to continue?

Recommendation would be to install GTB Security Manager on a machine that can be the central repositoiry for all fingerprinted files. Creating a large folder were the files can placed into for fingerprinting. Files don't have to remain in saved location once the profile has been fingerprinted and uploaded to Central Console. Access to fingerprinted files is only required when changes are made to profile containing said files.

<u>N</u>o

Yes

- Although only one profile is able to monitored at a time you are able to define multiple
 Polices within that profile. This is useful since when a fingerprint violation is triggered it
 will be tagged with the Defined Policy name, which allows for easier usability.
- Fingerprinted files follow ACL Rules: created within Central Console under DLP
 Setup → Network DLP. Rules are processed in order from top to bottom. This means
 the first rule with a matching violation takes precedence over rules below.

	Dashboard All Ev	vents No	etwork Events D	scovery Event	s Cloud Events	Endpoint Events Repo	orts Net	twork Status Accou	ints Manager	DLP Setup	Maintenan	e Logs
	Network DLP	Discovery	Endpoint & Dev	ice Control	App Control IRM	M Policy Management	Inspectio	on System				
	Categories		ACL Rules: GTBI	spector.lan.la	ab							
	Inspectors (1)		🛨 Add 🛛 📉	Delete 🚖	Load 🕴 📩 Save all	🔁 Deploy all						
	GTBInspector.lan.la	ab	Name	Protocol	Source	Destination	Files	Policy/Sets	Action	Alerts	Files capt	
5268			E Any	Any	Any	Any		All	Block	Security		î↓⁄X
5269												
5270												
c_ / c												
5271												
5211												

5272 **4.15.6 Highlighted Performance Impacts**

- 5273 No performance measurement experiments were performed for the installation of GTB into the
- 5274 PCS due to its location within the network topology. No manufacturing process components
- 5275 across the boundary on a regular basis while the system is operational.

5276 **4.15.7** Link to Entire Performance Measurement Data Set

- 5277 N/A
- 5278

5279 **4.16 Graylog**

5280 4.16.1 Technical Solution Overview

5281 Graylog is an open source log management tool. It can collect, parse and enrich logs, wire 5282 data, and event data from any data source. Graylog also provides centralized configuration 5283 management for 3rd party collectors such as beats, fluentd and nxlog. The processing 5284 pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching 5285 messages in real-time as they enter Graylog. It has a powerful search syntax to help query 5286 exactly what we are looking for. With Graylog one can even create dashboards to visualize 5287 metrics and observe trends in one central location.²⁸

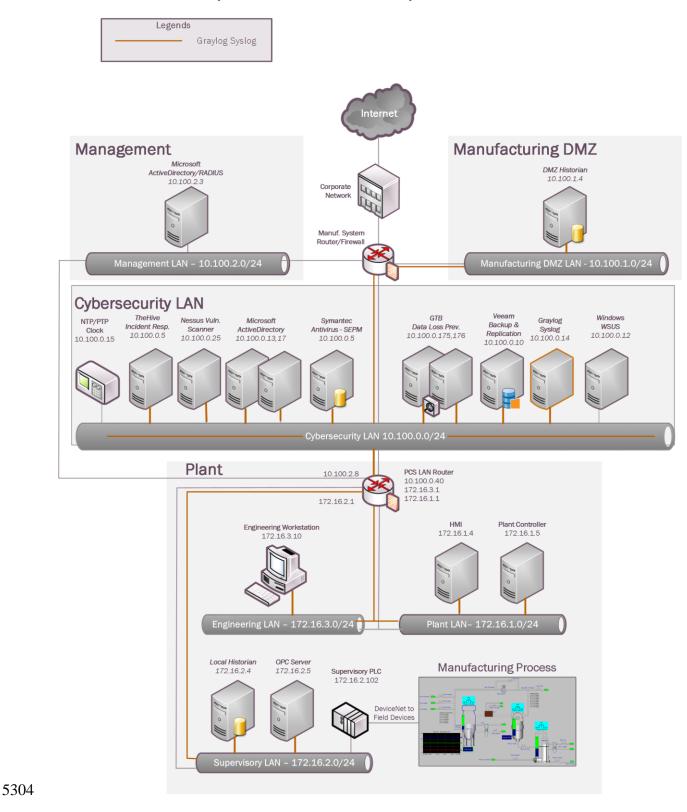
5288 Points to consider

- Open source product with good community support
- Easy to setup and customize. Support log collection from any OS platform.
- It is packaged for major Linux distributions, has a VM ready for use and Docker images are
 also available.
- The dashboard part, even if though well integrated and useful, lacks many features and visualizations contained in other elastic search tools such as Kibana (like aggregations).
- 5295 4.16.2 Technical Capabilities Provided by Solution
- 5296 Graylog provides components of the following Technical Capabilities described in Section 6 of 5297 Volume 1:
- Network Monitoring
- Event Logging
- Forensics

5301 **4.16.3 Subcategories Addressed by Implementing Solution**

5302 PR.DS-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

²⁸ Graylog Documentation <u>http://docs.graylog.org/en/3.0/</u>



5303 **4.16.4** Architecture Map of Where Solution was Implemented

5306 **4.16.5** Installation Instructions and Configurations

5307 Details of the solutions implemented:

Name	Version	Daily volume of logs	Server
Graylog Enterprise	2.4.6	< 5GB per day	Ubuntu 14

5308

5309 Setup:

- Download the installation package from the Graylog website (<u>https://www.graylog.org/</u>).
- 5311Graylog can be installed on any flavor of Linux. In addition, Graylog also provides a5312preconfigured virtual machine for **non-production** environments. This virtual machine5313template (OVA) file was used in our environment.
- The OVA file was deployed on a Microsoft Hyper-V host server in our Cybersecurity LAN network.
- The Graylog server at a minimum requires UDP port 514 which is the default syslog port to
 be opened. Accordingly, UDP 514 was permitted in the firewall rules. Additional ports such
 as UDP 5415 and 12202 are also used if configuring other features of Graylog as described in
 the documentation.
- Upon deploying the OVA file, the virtual machine will default to a DHCP IP address. Login to the system to assign it a static IP address as per below shown instructions.

Assign a static IP

Per default the appliance make use of DHCP to setup the network. If you want to access Graylog under a static IP please follow these instructions:

\$ sudo ifdown eth0

Edit the file /etc/network/interfaces like this (just the important lines):

```
auto eth0
iface eth0 inet static
address <static IP address>
netmask <netmask>
gateway <default gateway>
pre-up sleep 2
```

Activate the new IP and reconfigure Graylog to make use of it:

\$ sudo ifup eth0
\$ sudo graylog-ctl reconfigure

Wait some time until all services are restarted and running again. Afterwards you should be able to access Graylog with the new IP.

5324 5325

5327

5333

5334

5335

5336 5337

5323

• Login to the Web Interface using the default credentials and change the admin password.

 Active Directory (AD)-integration is supported in Graylog. To configure, on the Top Menu Bar, Click on System >> Authentication. On the Authentication Management page, click on LDAP / Active Directory and fill out the AD server details. Detailed instructions can be found in product documentation.²⁹

Note: Any AD domain user that's added is assigned "Reader" access by default. This can be changed by configuring Group Mapping options in the same page. Change the Default User Role depending on your requirement. Adding permissions can be assigning by clicking on LDAP Group Mapping button on the same page

²⁹ Configuring External Authentication in Graylog

http://docs.graylog.org/en/2.3/pages/users and roles/external auth.html?highlight=ldap

4. Group Mapping (optional)

Group Search Base	Group Search Base
DN	The base tree to limit the LDAP group search query to, e.g. cn=users,dc=example,dc=com.
Group Search Pattern	Group Search Pattern
	The search pattern used to find groups in LDAP for mapping to Graylog roles, e.g. (objectClass=groupOfNames) or (&(objectClass=groupOfNames)(cn=graylog*)).
Group Name Attribute	Group ld Attribute
	Which LDAP attribute to use for the full name of the group, usually cn .
Default User Role	Reader - basic
	The default Graylog role determines whether a user created via LDAP can access the entire system, or has limited access. You can assign additional permissions by mapping LDAP groups to Graylog roles,
	or you can assign additional Graylog roles to LDAP users below.

5339 **Configuration:**

5340 Syslog from Windows servers:

NXLOG (<u>https://nxlog.co/</u>) was used to forward logs from the Windows hosts in the Process
 Control System. The free community edition of NXLOG was installed on each windows
 host. In addition, it was also installed on Active Directory servers in Cyber-security LAN
 network.

5345

- Once NXLOG is installed, edit the nxlog.conf file located at C:\Program Files
- 5347 (**x86**) $nx\logconf$ directory as per whichever category of events you want to forward to your
- 5348 Graylog server. Detailed instructions on NXLOG configuration can be found on its website.³⁰
- 5349Below is a sample nxlog.conf from one of the Windows hosts in the Process Control system
- 5350

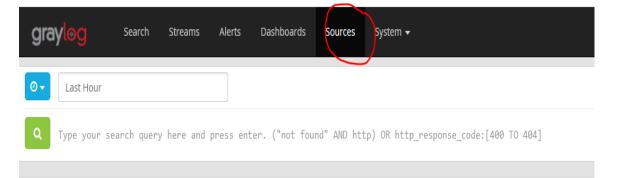
³⁰ <u>https://nxlog.co/documentation/nxlog-user-guide/</u>

Please set the ROOT to the folder your nxlog was installed into, ## otherwise it will not start. #define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog Moduledir %ROOT%\modules CacheDir %ROOT%\data Pidfile %ROOT%\data\nxlog.pid SpoolDir %ROOT%\data LogFile %ROOT%\data\nxlog.log <Extension_syslog> Module xm_syslog </Extension> <Input in> Module im msvistalog ReadFromLast True Query <QueryList>\ <Query Id="0">\ <Select Path="System">*[System[(EventID=1074)]]</Select>\ <Select Path="Application">*[System[(EventID=1034)]]</Select>\ <Select Path="Security">*[System[(EventID=4625)]]</Select>\ <Select Path="Security">*[System[(EventID=4689)] and EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files (x86)\Common Files\Rockwell\RsvcHost.exe')]]</Select>\ <Select Path='Microsoft-Windows-TerminalServices-LocalSessionManager/Operational'>*</Select>\ <Select Path="Veeam Agent">*[System[(EventID=190)]]</Select>\ <Select Path="FTDiag">*[System[(EventID=1001)]]</Select>\ </Query>\ </QueryList> </Input> <Output out> Module om udp Host 10.100.0.14 Port 514 Exec to_syslog_bsd(); </Output> <Route 1> Path in => out

5351 5352

5353 As per the screenshot above, we have configured it to forward the below types of events

- 5357 ➤ Event ID 4689 from "Security" category and ProcessName= to notify us when the
 5358 process for Rockwell Automation software stops.
- 5359 All events [*] from "*Microsoft-Windows-TerminalServices-LocalSessionManager*"
 5360 category to notify us when a user logs in or logs out of the system.
- 5362 > Event ID 1001 from FTDiag category which is a custom event ID generated by Factory
 5363 Talk Administration Software where there is an authentication failure.
- You can add other categories like "Application" or "System" should you need to collect
 those events as well. Ensure to balance out the type of events you are sending from your
 host. Too much noise will eventually make it difficult to search for meaningful logs in
 Graylog.
- Save the nxlog.conf once edited and restart the NXLOG windows service. The device will
 now begin sending syslog (events) to the Graylog server. If the service fails to start, please
 check the syntax of your nxlog.conf file for any blank spaces or missing parenthesis.
 Nxlog.conf file is very sensitive to proper indentation.
- Login to Graylog Web UI and you should start seeing the events from these windows hosts.
 Click on "Sources" in the Top menu bar to verify if the windows host shows up under the list of "Selected sources". Any device which you configure to send syslog data should begin showing up here under "Selected Sources" assuming your configuration is correct. If you don't see your device in here, verify the nxlog config and network connectivity between the end device and Graylog server.



Sources

This is a list of all sources that sent in messages to Graylog. Note that the list is cached for a few seconds so you might have to wait a bit until a new sourc

👔 Use your mouse to interact with the table and graphs on this page, and get a better overview of the sources sending data into Graylog.

Selected sources			
Search			Show: 100
Name	Perce	ntage Message (count
Top sources			
lan-ad.lan.lab	53.40	% 636	C
ciscoasa	31.40	% 374	Œ
ruggedcom	8.82%	105	œ
fgs-47631ehh.lan.lab	5.12%	61	Q
vcontroller1	0.25%	3	Q
mintaka	0.25%	3	Q
polaris	0.25%	3	Q

5380

5385

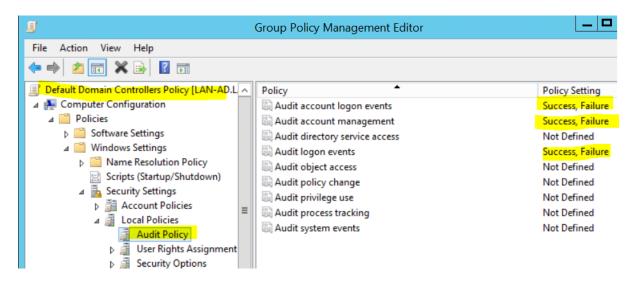
5386

- Search for events from a host by entering a search query and selecting the appropriate time interval in the home page.
- 5383 For example: To search for events by hostname, enter *"source: <windows hostname>"*5384 (without quotes) in the Search *box* as shown below

grayl⊚g	Search	Streams	Alerts	Dasl	nboards	Sources	System 🗸
Ø ▼	last 5 minu	<mark>utes</mark>	•				
Q source:fgs-47	7631ehh.l	an.lab					
Search result Found 93 messages in 2: Results retrieved at 2017			G.			ogram	Week, Day, Hour, Minut e
Add count to dashboar	rd 🗕 🛛 Sar	ve search crite	eria		30		
More actions 🗸					20		
Fields Decorat	ors				10-		

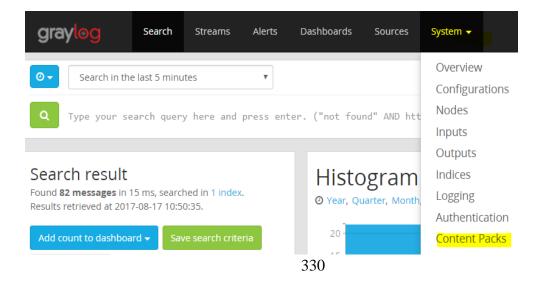
5388 Syslog from Active Directory Domain Controllers

- The nxlog.conf configuration remains same on the Domain Controllers as that for a member server except the PORT number to send the data on. In addition, there is a Content pack available at Graylog Marketplace, which if installed can parse Active Directory events and generate useful graphs. This content pack requires a different UDP Port (5414).
 Accordingly, this port was used in the nxlog.conf of the Domain Controllers instead of the default 514. The AD content pack can be downloaded from: https://marketplace.graylog.org/addons/750b88ea-67f7-47b1-9a6c-cbbc828d9e25
- Ensure to first enable Auditing on Domain Controllers (as mentioned in the Requirements section of the Content pack) prior to importing this content pack. This can be done using the
 "Default Domain Controllers Policy" in the Group Policy Management Console on the Domain Controller.
- 5401



5402 5403 5404

• Next, login to the Graylog Web UI. Click on "System" >> "Content Packs"



Download the Active Directory Content pack. Next, click on "import content packs" to
 import it. Once import is completed you should see "Active Directory" under "Select
 Content packs". This is the pack we just imported.

Search Streams Alerts Dashboards Sources System / Content Packs 👻 graylog Content packs Content packs accelerate the set up process for a specific data source. A content pack can include inputs/extractors, streams, and dash Find more content packs in the Graylog Marketplace. 0 Select content packs Active Directory, Windows, Operating Systems, Security Appliance Grok Import content pack

5410

5409

• Click on "**Dashboards**" to view the new graphs of the AD user and group activities. The graphs will begin populating data assuming the AD server is successfully sending over the events to Graylog server.

grayl⊚g	Search	Streams	Alerts	Dashboards	Sources
Dashboard Use dashboards to cre Take a look at	eate specific v	-	0	Create a new dash ther useful tips.	board here and
AD Compute AD Computer Obje AD DNS Objet AD DNS Object Sur	ct Summary (7d)		1)	
AD Group Ol	-	mmary	(7d)		
AD Logon Su		(2h)			
AD Summary (7d)	/ (7d)				

• On the main dashboard look for events from the AD server. Use the search query as explained in previous steps to look for events using the server hostname.

grayl⊚g	Search	Streams	Alerts	Dashboards	Sources	System 🗸
				2017-08-17	11:09:09.711	ciscoasa
Search result				Failed to	locate egress	s interface for UDP from lab_lan:10.100.0.17/55980 to 192.58
ound 95 messages in 19 r				2017-08-17	11:09:08.000	LAN-AD.lan.lab
esults retrieved at 2017-0	8-17 11:10	0:15.		An account	t was logged o	off.
Add count to dashboard	- Sav	e search crite	ria	Subject:		
More actions 🗸				Security 1	ID: 5-1-5-21-	
More dealons +					11:08:59.690	ciscoasa
				Failed to	locate egress	s interface for UDP from lab_lan:10.100.0.17/57580 to 198.41
Fields Decorator	rs			2017-08-17	11:08:59.000	LAN-AD.lan.lab
Default All None	Filter fie	lds		An account	t was logged o	off.
Derugie Ville Home	The file	105		Subject:		
AuthenticationPacka	ageName		A	Security 1	ID: 5-1-5-21-	
Category				2017-08-17	11:08:56.000	LAN-AD.lan.lab
🕨 🗆 Channel				An account	t was logged o	off.
🕨 🔲 EventID				Subject:		
EventReceivedTime				Security 1	ID: S-1-5-18	
EventType				2017-08-17	11:08:56.000	LAN-AD.lan.lab
▶ □ facility				Special pr	rivileges assi	igned to new logon.
from_syslog				Subject:		

5418

5417

- Note: Likewise, there are lot of useful Content packs and plugins available at <u>Graylog</u>
 Marketplace for vendor specific technologies / devices such as Cisco, Microsoft DNS, Bro
 IDS, Cacti, Symantec etc. Download and install each as per the infrastructure in your
 environment.
- 5423 Syslog from Boundary Firewall/Network Devices:
- All network devices such as switches and boundary routers from Process Control system
 were configured to send their syslog data to the Graylog server. There is a device specific
 setting in each network device to log to a Syslog server. This can be done either via Web UI
 or CLI of the device.
- 5429 The below commands were used on the Boundary Router of the system which is an Allen5430 Bradley Stratix firewall.
- 5431 5432
- 5433
- 5434
- logging enable

➤ Enable

➢ logging 10.100.0.14

 \succ configure terminal

- (Optional) To limit the messages sent based on priority level, enter:
- logging trap informational
- ▶ end
- ➢ wr mem

- It was observed that these messages however ended up in Graylog under the device's
- 5436 **IP address** as the **Source** instead of its hostname. This an expected behavior as different
 5437 vendor devices log in different formats.
- 5439To overcome this, Graylog offers native features such as Pipelines, Rules, Grok Patterns and5440Lookup Tables to get around this. Their documentation offers details on creating these5441http://docs.org/on/2.4/no.coc/ninclines.html
- 5441 <u>http://docs.graylog.org/en/2.4/pages/pipelines.html</u>
- 5442 Additional guidance on creating pipelines can be found at <u>https://jalogisch.de/2018/working-</u> 5443 with-cisco-asa-nexus-on-graylog/
- 5444 Configuring Pipelines /Rules for Network devices:
- The following screenshots show some pipelines and rules that were created.
- 54465447 Pipelines can be created by clicking on System/Pipelines >> Pipelines option in the TOP
- 5448 Menu bar
- 5449

Pipelines overview Pipelines let you transform and process mes applied. Messages can go through one or m	0 0 1	es consist of stages where rules are evaluated ar	Manage pipelines Manage rules Simulato
Read more about Graylog pipelines	s in the documentation.		
ilter pipelines	Filter Reset		Add new pipelin
Pipeline	Connected to Streams	Processing Timeline	Actions
Correct ASA Name Correct ASA Name Throughput: 0 msg/s	All messages	Stage 0	Delete
Correct PCS 8300 Router Name Throughput: 0 msg/s	All messages	Stage 0	Delete
Correct PCS Vlan01 Switch Name	All messages		Delete E di

Pipeline Rules ules are a way of applying changes to messag decutes the actions if the condition is satisfier	ges in Graylog. A rule consists of a condition and a list o d.	f actions. Graylog evaluates t	he condition against a message a		age pipelines Manag	e rules Simulato
Read more about Graylog pipeline ru	iles in the documentation.					
lter Rules	Filter Reset					Create Rul
Title	Description	Created	Last modified	Throughput	Errors	Actions
Correct CiscoASA hostname	Correct CiscoASA hostname	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	Delete Edit
Correct PCS 8300Router Name	Correct PCS 8300Router Name	4 months ago	4 months ago	1 msg/s	0 errors/s (0 total)	Delete
Correct PCS Vian01 Switch	Correct PCS Vlan01 Switch Name	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	Delete
Correct PCS Vian02 SwitchName	Correct PCS Vlan02 Switch Name	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	Delete
Correct Siemens Switch hostname	Correct i800 SwitchName	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	Delete

5455

The following screenshots show details of one such pipeline "Correct PCS 8300 Router 5456 • 5457 Name" and its corresponding rule "Correct PCS 8300 Router Name" that was created to make the Allen Bradley Boundary Router display its hostname correctly. 5458

Pipelines let you transfo	DIFFECT PCS 8300 R rm and process messages coming from o through one or more stages.	OUTER NAME n streams. Pipelines consist of stages where rules are evaluate	Manage pipelin	es Manage rules Si	mulator
		ssages matching all or one of the rules continue to the nex	xt stage.		
Details				Edit pipeline	e details
Title:	Correct PCS 8300 Router Name				
Description: Created:	4 months ago				
Last modified:	4 months ago				
Current throughput:	1 msg/s				
This pipeline is processi	ng messages from the stream "All mess	20222 .			
Pipeline Stage	S			Add ne	ew stage
Stages are groups of cor	ditions and actions which need to run	in order, and provide the necessary control flow to decide wh	ether or not to run the rest of a pipeline.		
Stage 0 Contains	1 rule			Delete	Edit
There are no further sta Throughput: 1 msg/s	ges in this pipeline. Once rules in this s	stage are applied, the pipeline will have finished processing.			
Title		Description	Throughput	Errors	
Correct PCS 8300Route	r Name	Correct PCS 8300Router Name	0 msg/s	0 errors/s (0 total)	

5462 Rule: C

5463

Rule: Click on "Manage Rule" to create a rule to associate with the pipeline.

Rule source

1	rule "Correct PCS 8300Router Name"
2	when
3	has_field("source") AND contains(to_string(\$message.source), "10.100.0.40")
4	then
5	<pre>set_field("source", "PCS-AB8300");</pre>
6	end

5464

• End Result in the "Search" pane now shows the hostname "PCS-AB8300" as configured in the Rule.

5468

graylog Search St	treams Alerts Dashboa	rds Sources	System v	In 0 / Out 0 msg/s	Help 🗸	Admi
Search result	2019-03-28 12:20:28.980 %SEC-6-IPACCESSLOGP: list	PCS-AB8300 plant-vlan-acl perm	nitted tcp 172.16.1.4	(51211) → 172.16.2.5(1332	2), 1 packet	
Found 141 messages in 12 ms, searched in 1 index. Results retrieved at 2019-03-28	2019-03-28 12:20:26.371 %SEC-6-IPACCESSLOGRL: acc	PCS-AB8300	e-limited or missed	61 packets		
12:20:39. Add count to dashboard 🗸	2019-03-28 12:20:26.371 %SEC-6-IPACCESSLOGP: list	PCS-AB8300 plant-vlan-acl perm	nitted tcp 172.16.1.4	(3389) -> 172.16.3.10(5686	€), 481 pac	kets
Save search criteria	2019-03-28 12:20:26.371 %SEC-6-IPACCESSLOGP: list	PCS-AB8300 : Manf-vlan-ACL permi	.tted tcp 172.16.2.5(50006) -> 172.16.1.5(56551	L), 1292 pac	kets
More actions •	2019-03-28 12:20:26.371 %SEC-6-IPACCESSLOGP: list	PCS-AB8300 Manf-vlan-ACL permi	.tted tcp 172.16.2.5(3389) -> 172.16.3.10(5118)	7), 546 pack	ets

5469 5470

5471 <u>Configuring Email Notifications for Alert conditions:</u>

You can create email alerts for any custom events, alert condition as per your requirement.
 Below process show how our Graylog was configured to send out email notifications, for any
 Veeam backup events that it received from the Windows clients. Follow this process to
 define your custom alert conditions
 There are multiple configuration settings required for email notification to work. Creating a

• There are multiple configuration settings required for email notification to work – Creating a stream, adding an alert condition and creating a notification.

- To create a stream, click on Streams on the Top-Menu >> Create a Stream >> Enter Title,
 Description, and Index Set which should default to "Default index set"
- Click **Save** to save the changes

	Editing Stream	
	Title	
	Backup Notifications	
	Description	
	Backup Messages	
	Index Set	
	Default index set × 💌	
	Messages that match this stream will be written to the configured index set.	
	Remove matches from 'All messages' stream	
	Remove messages that match this stream from the 'All messages' stream which is assigned to every message by default.	
	Cancel Save	_
•	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >> on Add new condition to define a condition.	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition"	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli	> ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition" Condition	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition" Condition Define the condition to evaluate when triggering a new alert.	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition" Condition Define the condition to evaluate when triggering a new alert. Alert on stream	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition" Condition Define the condition to evaluate when triggering a new alert. Alert on stream Backup Notifications	> (ck
	Next, click on "Alerts" options on the top menu >> Click on Manage conditions >: on Add new condition to define a condition. Click drop menu under "Alert on Stream" and select the stream created earlier. Cli "Condition Type" menu drop down and select "Message Count Alert Condition" Condition Define the condition to evaluate when triggering a new alert. Alert on stream Backup Notifications Select the stream that the condition will use to trigger alerts.	> (ck

- Click "Add Alert Condition". Once window appears fill out the required information.

• Click **Save** to complete (See below for example of current Message Count Alert Condition).

Message Count Alert Condition descrip	ption	
This condition is triggered when the number of threshold in a given time range.	messages is higher/lower than a defined	
Title		
Veeam Backup Alerts		
The alert condition title		
Time Range		
2	٢	
Evaluate the condition for all messages received	d in the given number of minutes	
Threshold Type		
more than	~	
Select condition to trigger alert: when there are	more or less messages than the threshold	
Threshold		
0	\$	
Value which triggers an alert if crossed		- 0
Grace Period		
1	۵	
Number of minutes to wait after an alert is reso	lved, to trigger another alert	
Message Backlog		
1	۲	
The number of messages to be included in alert	t notifications	
Repeat notifications (optional)		
Check this box to send notifications every time f regardless of its state.	the alert condition is evaluated and satisfied	

5495 5496 5497

5494

• Now create a **notification**.

• Click on "Manage notifications" blue button in upper right-hand corner. • Click green button for "Add new notification" 5498 Under "Notify on Stream" select notification created earlier from drop down 5499 0 5500 menu. 5501 Under "Notification type" select "Email Alert Callback" from drop down 0 5502 menu. Click "Add alert notification" button 5503 0 5504 Title: "Veeam Backup Alerts" 0

5505	• Email Subject: "Successfull Veeam Backup source: \${foreach backlog
5506	message}\${message.source}\${end}" without the quotes, see below for screen
5507	shot of current callback wording.
5508	• Sender: < sender address >
5509	• E-mail Body: "This can be adjusted as required"
5510	
5511	Alert Description: \${check_result.resultDescription}
5512	Date: \${check_result.triggeredAt}
5513	Stream ID: \${stream.id}
5514	Stream title: \${stream.title}
5515	Stream description: \${stream.description}
5516	Alert Condition Title: \${alertCondition.title}
5517	
5518	\${if backlog}Last messages accounting for this alert:
5519	{foreach backlog message} {message}
5520	
5521	\${end}\${else} <no backlog=""></no>
5522	\${end}
5523	
5524	• User Receivers: "Select a Graylog user if desired"
5525	• Email Receivers: "Enter email address for individuals receiving these
5526	alerts"
5527	• Click Save
5528	
5529	• Test new Streams / Alerts / Notifications to ensure they are configured correctly.
5530	
5531	4.16.6 Highlighted Performance Impacts
5532	No performance measurement experiments were performed for the use of the Graylog due to its
5533	typical installation and usage location (i.e., external to the manufacturing system).
5534	4.16.7 Link to Entire Performance Measurement Data Set

- 5535 N/A
- 5536

5537 **4.17 DBAN**

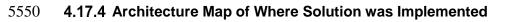
5538 4.17.1 Technical Solution Overview

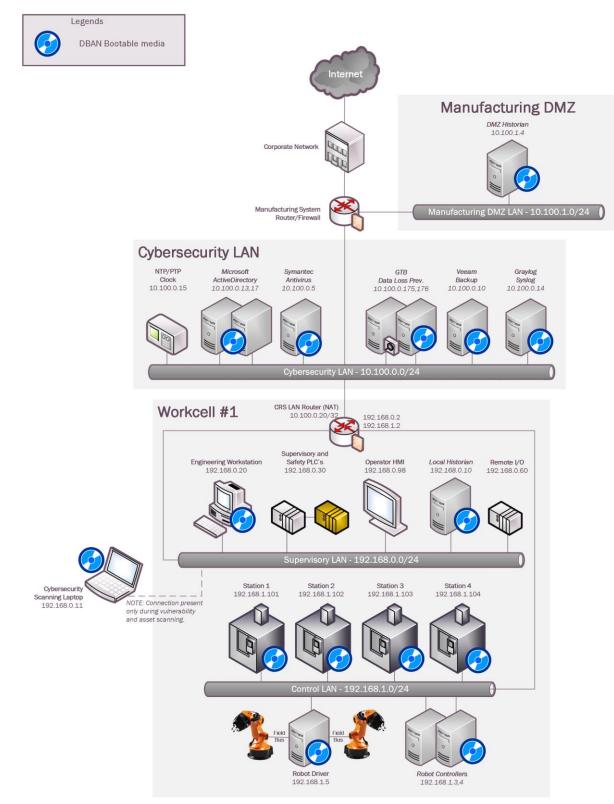
5539 DBAN is a free open source data wiping utility allowing the ability to sanitize hard drives to

- ensure data is not left behind when drives are beginning decommissioned and prepared for
- removal from on-premise. DBAN and other hard drive sanitization tools only work with spinning
- hard drives, SSD hard drives and other flash media refer to vendors for specific directions for
- sanitizing media before removing from company control.
- 5544 **4.17.2 Technical Capabilities Provided by Solution**
- 5545 DBAN provides components of the following Technical Capabilities described in Section 6 of5546 Volume 1:
- Media Sanitization

5548 **4.17.3 Subcategories Addressed by Implementing Solution**

5549 PR.DS-3, PR.IP-6





5552 **4.17.5 Installation Instructions and Configurations**

5553	Instructions for installing DBAN and use
5554 5555 5556 5557 5558 5559 5560	Download: DBAN can be downloaded from <u>https://dban.org</u> Click download link which redirects the page and a pop will appear to start download process for ISO image file " dban-2.3.0_i586.iso ". Download ISO file and burn to CD/DVD, or USB drive using widely available ISO bootable utilities.
5561	Instructions:
5562	1. Once ISO has been burned to bootable media go to device requiring sanitization.
5563	2. Power on machine and boot from USB or CD/DVD depending on the install option
5564	from earlier steps above. (Change Boot order in BIOS if no option for Boot
5565	Menu is available during machine power-up)
5566	3. Once machine has booted from media select desire option for media sanitization.
	<pre>Darik's Boot and Nuke Warning: This software irrecoverably destroys data. This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is". http://www.dban.org/ * Press the F2 key to learn about DBAN. * Press the F3 key for a list of guick commands. * Press the F4 key for troubleshooting hints. * Press the F4 key for start DBAM in interactive mode. * Enter autonuke at this prompt to start DBAN in automatic mode. boot: _</pre>
5567	
5568	4. Select option to continue. Default sanitization mode is "short DoD 5520.22-M",
5569	but this can be changed depending on the level your security program indicates.
5570	5. Follow menu options to start wiping process.
5571	6. Once the wipe has completed, you will see a screen like the image below.

ardнаre clock operation finish date: Sun Aug 13 15:27:80 2006 aving log file to floppy disk a floppy disk in DOS format наs not found BAN finished. Press ENTER to save the log file	ving log file to floppy disk a floppy disk in DOS format was not found.	rdware c	BBAN boot	tion star	t date:	Sun Aug	13 15:24	:36 2006		
HM TINISNEG, Press EMIER to save the log Tile	IN TINISAEU. Press ENIER to save the log Tile	ving log	file to f	loppy dis	k a f	loppy di:	sk in DOS		was not	found.
		AN finis	thed. Press	ENTER to	save th	e log fi	1e			

55737. Once sanitization has completed, remove hard drive from device and label wiped ready for disposal.

5575 Lesson Learned and things to know:

Not all hard drives are able to be wiped clean using this sanitization method. Media that is either
SSD or flash memory is written differently than spinning drives, so follow SSD/Flash media
vendors' recommendations for proper media sanitization for all non-spinning hard drives.

5579 **4.17.6 Highlighted Performance Impacts**

- 5580 No performance measurement experiments were performed for the use of DBAN due to its
- 5581 typical installation and usage location (i.e., external to the manufacturing system).

5582 **4.17.7** Link to Entire Performance Measurement Data Set

- 5583 N/A
- 5584

5585 **4.18** Network Segmentation and Segregation

5586 4.18.1 Technical Solution Overview

5587 Network segmentation and segregation solutions enable a manufacturer to separate the

5588 manufacturing system network from other networks (e.g., corporate networks, guest networks), 5589 segment the internal manufacturing system network into smaller networks, and control the

5590 communication between specific hosts and services.

5591 Each Router's native capabilities were leveraged to implemented network segmentation.

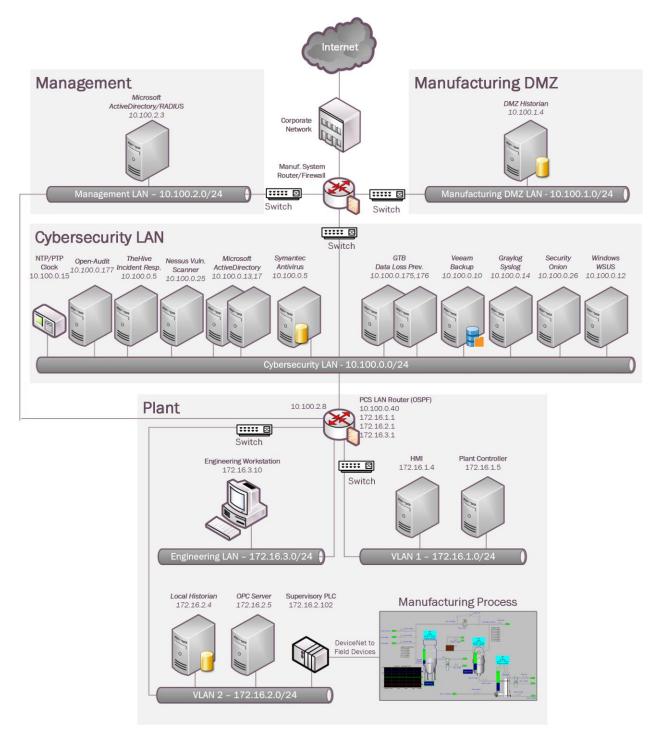
5592 **4.18.2 Technical Capabilities Provided by Solution**

- 5593 Network Segmentation and Segregation provides components of the following Technical
- 5594 Capabilities described in Section 6 of Volume 1:
- Network Segmentation and Segregation

5596 **4.18.3 Subcategories Addressed by Implementing Solution**

5597 PR.AC-5





4.18.5 Installation Instructions and Configurations

5603 The following devices were involved in implementing Network Segmentation

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell

• Segmentation in the Cybersecurity LAN:

Following is a list of interfaces created on the Boundary Router/Firewall – Cisco ASA of the
 Cybersecurity LAN network

Interface	IP address of Interface	Subnet	Description
GE 0/0	129.6.66.x	129.x.x.x/x	Uplink to Corporate
GE 0/1	10.100.0.1	10.100.1.0/24	Cybersecurity LAN
GE 0/2	129.6.1.x	129.x.x.x/x	VPN users
GE 0/3	10.100.2.1	10.100.2.0/24	Management LAN
GE 0/4	10.100.1.1	10.100.0.0/24	Manufacturing DMZ LAN

- Segmentation in the Plant:
- The Work Cell consists of the following network devices.

Туре	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

🏫 Dashboa

5615 5616 • Following is a list of interfaces created on the Boundary Router – Allen Bradley 8300

Interface	IP address of Interface	Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN
Gi 1/1	10.100.2.8		Management interface

5617

Allen-Bradley

V	Stratix 0300		
y	Device Manager - Switch		

	_	
Physical	Port	Table
,		

1	/ Edit				
	Port Name	Description	Port Status	Speed	Duplex
0	Fa1/1	Supervisory VLAN1 Switch	۲	Auto-100Mb/s	Auto-Full
\bigcirc	Fa1/2	Control VLAN2 Switch	•	Auto-100Mb/s	Auto-Full
\bigcirc	Fa1/3	Engg LAN Workstation	•	Auto-100Mb/s	Auto-Full
0	Fa1/4	Uplink to Cybersecurity LAN	•	Auto-100Mb/s	Auto-Full
\bigcirc	Gi1/1	Mgmt	۲	Auto-1000Mb/s	Auto-Full
\bigcirc	Gi1/2			Auto	Auto

5618 5619

5623

5627

- One of the Stratix 5700 switches was connected to the Fa1/1 interface of the 8300 Router and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were assigned an IP address from the 172.16.1.0/24 subnet
- The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used 5625 for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP 5626 address from the 172.16.2.0/24 subnet.

5628 **4.18.6 Highlighted Performance Impacts**

No performance measurement experiments were performed for network segmentation and
 segregation due to it being implemented on the PCS before the Manufacturing Profile
 implementation was initiated.

5632 **4.18.7** Link to Entire Performance Measurement Data Set

5633 N/A

5634 **4.19 Network Boundary Protection**

5635 4.19.1 Technical Solution Overview

5636 Boundary Protection devices are implemented to monitor and control connections and

- 5637 communications at the external boundary and key internal boundaries within the organization.
- 5638 Boundary protection mechanisms include for example, Routers, Firewalls, Gateways, Data
- 5639 diodes separating system components into logically separate networks and sub networks.

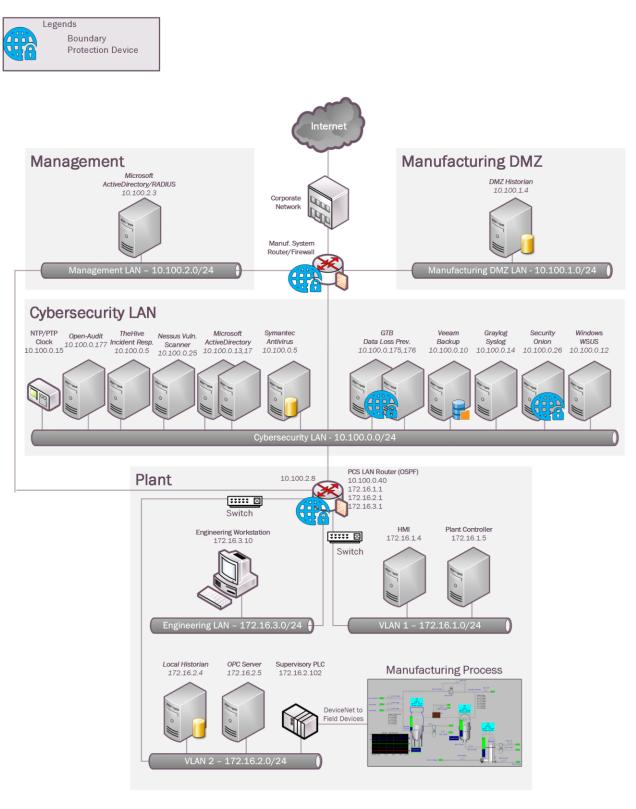
5640 **4.19.2 Technical Capabilities Provided by Solution**

- 5641 Network Boundary Protection provides components of the following Technical Capabilities5642 described in Section 6 of Volume 1:
- Network Boundary Protection

5644 **4.19.3 Subcategories Addressed by Implementing Solution**

5645 PR.AC-5, PR.PT-4, DE.CM-1





5648 **4.19.5** Installation Instructions and Configurations

- 5649 **Setup:**
- 5650 The following devices were implemented for Boundary protection in the PCS System

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell
GTB Inspector	Data Loss Prevention (DLP) virtual appliance	Cybersecurity LAN
Security Onion	Running Snort, BRO IDS	Cybersecurity LAN

5651

- **5652** Configuration on Cisco-ASA:
- 5653 The following features, settings were enabled on the ASA firewall
- 5654 Network Segmentation
- 5655 ACL Rules
- NAT policy for Internet access
- 5657 Snort Inspection
- 5658 DMZ network
- 5659 Network Segmentation

5660 Separate network interfaces were configured for the different network segments as listed below

- Inside Interface (Network: 10.100.0.0/24)
- 5662 DMZ Interface (Network: 10.100.1.0/24)
- Outside Interface (Network:129.6.91.x/24, Uplink to NIST Corporate for Internet)
- Public interface (Network:129.6.1.x/24 For VPN Users)
- 5665 Access Control List (ACL) rules
- 5666 The following rules were put in place on the ASA with a default Action to **Block all traffic**.

Source	Source Port	Destination	Dest Ports	Protocol	Action
10.100.0.0/24, 172.16.0.0/22	Any	DMZ network	SSH,RDP,ICMP	ТСР	Trust
PCS-Historian (172.16.2.14)	TCP_High_Ports	DMZ-Historian	5450	ТСР	Trust
DMZ Historian	TCP_High_Ports	PCS-Historian	5450	ТСР	Trust
CRS-NAT (10.100.0.20)	TCP_High_Ports	DMZ-Historian	5450, 5460, 5671, 5672	ТСР	Trust
DMZ Historian	TCP_High_Ports	CRS-NAT (10.100.0.20)	5457, 5450	ТСР	Trust
DMZ Historian	Any	Active Directory (10.100.0.17)	53	UDP	Allow
Veeam Server	Any	Hyper-V Host servers, Esxi Host Server	NETBIOS, ICMP, HTTPS, 445, TCP_High_ports, 2500-5000, 6160- 6163	ТСР	Trust
Hyper-V Host Servers, Esxi Host Server	Any	Veeam Server	ICMP, 2500-5000	ТСР	Trust
inside_interface	Any	outside_interface	Any	Any	Allow
DMZ Historian	Any	Symantec Server	SMB (445), HTTPS	ТСР	Trust
Symantec Server	Any	DMZ Historian	HTTP, HTTPS, 8014	ТСР	Trust
DMZ Historian	Any	Graylog Server	514	UDP	Trust
VPN_Pool (192.168.100.1020)	Any	PCS-HMI-Server, PCS-Workstation	3389	ТСР	Allow

CSF MFG PROFILE LOW SEC LVL EXAMPLE IG PROCESS-BASED MFG SYSTEM USE CASE

se Access Control Policy													Save Save	8 C
filter Policy: Default Prefilter Policy		SSL Policy: None		Id	entity Policy:	None						📑 Inher	itance Settings 🖳 Policy Assig	ignme
tules Security Intelligence HTTP Re	sponses Logging Advanced								Show Rule Conflicts 😣	🔘 Add	Category	🔾 Add Rule Se	earch Rules	
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat	Source Ports	Dest Ports	URLs	ISE/S	-	U 🕞 🤌 🖢 🗉 🛡	
 Mandatory - AC-Policy (1-13) 														
Allow-SSH-RDP-DMZ	Any	Any	Testbed-LAN-Networ	🕯 🚊 DMZ-Network	Any	Any	Any	Αηγ	x [®] ICMP (1) ∂ SSH ∂ RDP-Windows	Any	Any	⇒ Trust	Ū 🗅 🔒 🔒 🖡 o	ø
PI-To-PI	Any	Any	RCS-Historian	PI-Server-DMZ	Any	Any	Any	// TCP_high_ports	🎤 PI-to-PI	Any	Any	⇒ Trust	V 🗅 🔏 📩 🖉 o	6
PI-to-PI-PCS	Any	Any	PI-Server-DMZ	🖶 PCS-Historian	Any	Any	Any	// TCP_high_ports	🎤 PI-to-PI	Any	Any	⇒ Trust	U D 2 1 0	6
CRS-PI-PI	Any	Any	CRS-NAT-IP	💂 PI-Server-DMZ	Any	Any	Any	# TCP_high_ports	☆ TCP (6):5671 ☆ TCP (6):5672 > PI-Connector > PI-DCM	Any	Any	⇒Trust	0 🗅 🔒 📩 🖬 o	b
CRS-PI-To-PI-2	Any	Any	PI-Server-DMZ	CRS-NAT-IP	Any	Any	Any	TCP_high_ports	v TCP (6):5457 → PI-to-PI	Any	Any	⇒ Trust	V D 2 to C •	6
Allow-DNS-DMZ	Any	Any	DMZ-Network	💂 LAN-AD01-DNS-Se	nı Any	Any	Any	Any	DNS_over_UDP	Any	Any	🖌 Allow	0 0 2 2 2 0	6
Veeam-Mgmt-Hoots	Any	Any	💂 Veeam	Hyper-VServers Esxi-Host.mgmt	Any	Any	Any	Απγ	<pre>% ICMP (1) % TCP_high_ports % Veeam-channel-port % NetBIOS-TCP (4 more)</pre>	s Any	Any	⇒ Trust	062660	ø
HyperV-Hosts-Veeam	Any	Any	Esxi-Host.mgmt	👼 Veeam	Any	Any	Any	Any	x [®] ICMP (1) <i>P</i> Veeam-channel-port	s ^{Any}	Any	⇒ Trust	V 🗅 🔒 🖆 🖡 o	6
Internet-Access	🚠 inside	🚠 outside	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	🤴 🖒 🔏 🖄 📕 o	6
0 Symantec-DMZ-1	Any	Any	📄 SymantecMgr	PI-Server-DMZ	Any	Any	Any	Απγ	№ TCP (6):445 > SMB-Windows > HTTPS	Any	Any	🖌 Allow	002000	6
Symantec-DMZ-2	Any	Any	PI-Server-DMZ	SymantecMgr	Any	Any	Any	Any	 HTTPS HTTP Symantec 	Any	Any	🖌 Allow	VD.26.C •	6
2 DMZ-Syslog	Any	Any	PI-Server-DMZ	👮 Graylog	Any	Any	Any	Any	SYSLOG	Any	Any	🖌 Allow	UD2610	6

5672

5673 NAT Policy

• A Dynamic NAT policy was configured to allow internet access.

Type of NAT rule	Auto NAT [1]
Source Interface	inside
Destination Interface	outside
Original sources	10.100.0.0/8
Translated Source	Destination Interface IP
Options	Translate DNS Replies that match this Rule: False

Edit NAT Rule							3
NAT Rule:	Auto NAT Rule	~					
Туре:	Dynamic	~	🗹 Enable				
nterface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:*	IPv4-Priva	te-10.0.0.0-8		v 📀	Translated Source:	Destination Interface IP	~
Original Port:	TCP	¥			Translated Port:	The values selected for Destination Inter Objects in 'Interface Objects' tab will be	used
						ОК Са	ancel

5677 Snort Inspection

• Snort Inspection was enabled on the following ACL rules

Name of the ACL	Intrusion Policy
Allow-DNS-DMZ	Balanced connectivity and security
Internet-Access rule	Balanced connectivity and security
VPN-Rule	Balanced connectivity and security

5679

Name	Internet-Access				🕑 Ena	bled	Move	
Action	Allow 🗸		💌 🔍 🗋 💌	èn 🗾				
Zone	s Networks	VLAN Tags	🛆 Users	Applications	Ports	🛆 URLs	SGT/ISE Attributes	Inspection Loggi
Intrusion	Policy						Variable Set	
Balanced	d Security and Co	nnectivity				*	Default Set	
File Policy None	·							

5683 **DMZ Network**

- 5684 A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the DMZ
- 5685 Historian server.

Overvie	w Analys	sis Policie	s Device	es Obje	ects AMP	Intel	ligence			Deploy	0	System
Device M	lanageme	nt NAT	VPN 🕶	QoS	Platform Sett	tings	FlexConfig	Certificates				
Cisco ASA5	ASA 512-X Threa	t Defense										
Device	Routing	Interfaces	Inline Sets	DHCP								
									🔍 dmz		×	Sync Device
Inte	rface	Logical N	ame	Туј	pe	Securit	y Zones	MAC Add	· IP Ad	ldress		
🚰 G	igabitEthern	_{et} dmz		Phy	rsical	dmz			10.10	0.1.1/24(Sta	tic)	

5686

• Configuration of Allen Bradley Firewall:

- 5688 The following features, settings were enabled on this firewall
- 5689 Network Segmentation
- 5690 ACL Rules

5691 Network Segmentation

- 5692 Separate network interfaces were configured for the different network segments as listed below
- Supervisory VLAN1 (Network: 172.16.1.0/24)
- Control VLAN2 Interface (Network: 172.16.2.0.0/24)
- Engineering LAN (Network: 172.16.3.0/24)
- Uplink (IP:10.100.0.40, Uplink to Cybersecurity LAN)
- Management interface (IP:10.100.2.8)

AB	Allen-Bi	radley	Stratix 830 Device Mana	ratix 8300 evice Manager - Switch								
S Net	Network Port Settings											
Phy	sical Port Ta	ble										
-		bie										
<u>/</u>	Edit											
	Port Name	Description		Port Status	Speed	Duplex						
\circ	Fa1/1	Supervisory V	LAN1 Switch	۲	Auto-100Mb/s	Auto-Full						
\bigcirc	Fa1/2	Control VLAN	2 Switch	•	Auto-100Mb/s	Auto-Full						
\circ	Fa1/3	Engg LAN Wo	orkstation	•	Auto-100Mb/s	Auto-Full						
0	Fa1/4	Uplink to Cyb	ersecurity LAN	•	Auto-100Mb/s	Auto-Full						
\bigcirc	Gi1/1	Mgmt		•	Auto-1000Mb/s	Auto-Full						
\bigcirc	Gi1/2				Auto	Auto						

5699 Access Control List (ACL) rules

5700 Three ACLs of Extended type were created as shown below. Each one was associated to a5701 specific network interface as an Inbound ACL

Allen-Bradley	Stratix 8300			
Anon Drauley	Device Manager - Switch	🏠 Dashl	ooard Configure 🔻	Monitor 🔻 Admin 🔻
Security ACL				
ACL List Apply ACL				
ACL List Apply ACL	/ Import / Export			
	/ Import / Export Description	Туре	Interface/Direction	n Number of Statem
<pre>e Add ∮ Edit X Delete</pre>		Type Extended IP	Interface/Direction Fa1/3 Inbound	n Number of Statem
Add ACL Name/Number				

Allen-Bradley	Device Manager - Switch	🏦 Dashboard	Configure 💌	Monito	
Security ACL					
	_				
ACL List Apply ACL					
Port Name	Inbound ACL	Outbound ACL			
Fa1/1	plant-vlan-acl	None			
Fa1/2	Manf-vlan-ACL	None			
Fa1/3	EnggWkstn-ACL	None			
Fa1/4	None	None			
permit ip host 172.16.3.10 permit tcp host 172.16.3.1					
	10 172.16.1.0 0.0.0.15 eq 3389				
	10 172.16.2.0 0.0.0.15 eq 3389				
permit icmp host 172.16.					
permit ip host 172.16.3.1	10 host 172.16.2.102 eq 44818 0 host 172 16 3 1				
permit ip host 172.16.3.1					
permit ip host 172.16.3.10					
permit tcp host 172.16.3.	10 host 10.100.1.4 eq 3389				
permit tcp host 172.16.3.	10 host 129.6.1.2 eq ftp				
	10 host 120 6 1 2 og 22				
permit tcp host 172.16.3.	10 110st 129.0.1.2 eq 22				
	10 host 129.6.1.2 eq www				
permit tcp host 172.16.3. permit tcp host 172.16.3.	10 host 129.6.1.2 eq www 10 host 172.16.2.102				
permit tcp host 172.16.3. permit tcp host 172.16.3. permit tcp 192.168.100.0	10 host 129.6.1.2 eq www				

ip access-list extended Manf-vlan-ACL

permit ip 172.16.2.0 0.0.0.15 172.16.1.0 0.0.0.15 log permit icmp 172.16.2.0 0.0.0.255 any log permit tcp 172.16.2.0 0.0.0.255 host 172.16.3.10 gt 49000 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.5 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.10 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.13 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.17 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.25 log permit ip 172.16.2.0 0.0.0.255 host 10.100.0.177 log permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.234 log permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq www log permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 443 log permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.14 eq syslog log permit udp 172.16.2.0 0.0.0.255 host 10.100.0.14 eq syslog log permit tcp host 172.16.2.14 host 10.100.1.4 gt 49000 log

5706

ip access-list extended plant-vlan-acl

permit ip 172.16.1.0 0.0.0.15 172.16.2.0 0.0.0.15 log permit icmp 172.16.1.0 0.0.0.255 any log permit tcp 172.16.1.0 0.0.0.255 host 172.16.3.10 gt 49000 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.5 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.10 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.13 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.17 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.25 log permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.234 log permit udp 172.16.1.0 0.0.0.255 host 10.100.0.14 eq syslog log permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq www log permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 443 log permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 8530 log permit ip 172.16.1.0 0.0.0.255 host 10.100.0.177 log permit tcp 192.168.100.0 0.0.0.255 host 172.16.1.4 eq 3389 log permit tcp host 172.16.1.4 192.168.100.0 0.0.0.255 gt 49000 log

5707

5708 • Configuration of GTB Inspector:

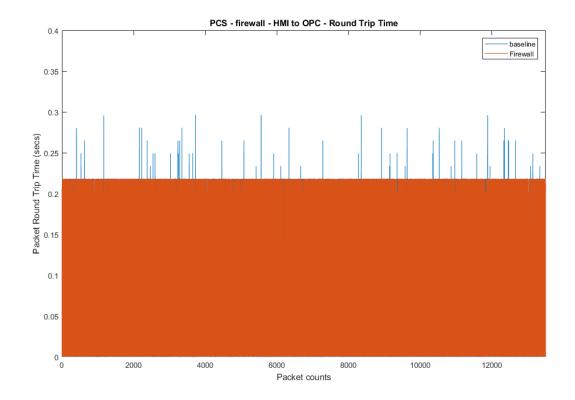
5709 Refer to Section 4.15 for details.

5710 • Configuration of Security Onion:

5711 Refer to Section 4.7 for details

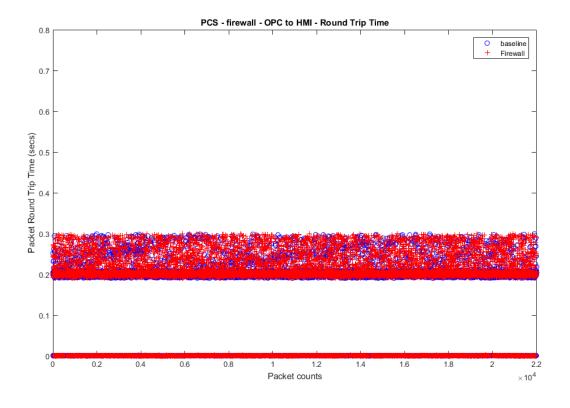
5712 **4.19.6 Highlighted Performance Impacts**

- 5713 The following performance measurement experiment was performed for the network boundary
- 5714 protection while the manufacturing system was operational:
- 5715 Experiment PL004.1- Firewall rules are activated at the PCS boundary router
- 5716 There was no significant performance impact observed when firewall rules were activated. For
- 5717 example, the packet round trip time between the HMI and OPC remained mostly constant before
- 5718 and after the firewall rules were activated.
- 5719 Care needs to be used for implementation of the rules and a thorough understanding of the
- 5720 system is important. A misconfigured firewall rule can block a legitimate connection and cause
- 5721 system failure.
- 5722 In the PCS system implementation, a thorough analysis on network connections was performed
- to identify all the legitimate connections in order to implement the firewall rules. Some network
- 5724 connections are legitimate but not obvious or only stayed connected for a short amount of time.
- 5725 Validation test was performed to ensure all the legitimate network connections for normal
- operation are allowed. The implementation and validation test was completed during a planned
- 5727 system down time.



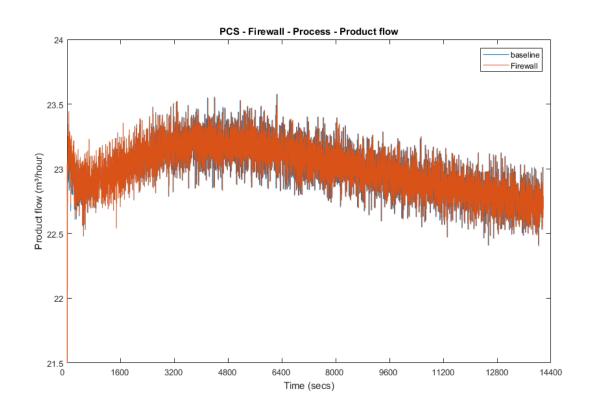
5729

Figure 4-35 Packet round trip time from HMI to OPC before and after firewall rules were activated



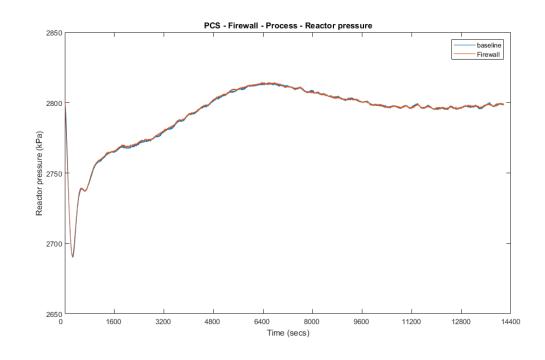
5731 Figure 4-36 Packet round trip time from OPC to HMI before and after firewall rules were activated







5734 Figure 4-37 Manufacturing process product flow rate before and after firewall rules were activated





5736

Figure 4-38 Manufacturing process reactor pressure before and after firewall rules were activated

- 5737
- 5738 **4.19.7** Link to Entire Performance Measurement Data Set
- 5739 Firewall KPI data
- 5740 Firewall measurement data
- 5741
- 5742

5743 **4.20 Managed Network Interfaces**

5744 **4.20.1 Technical Solution Overview**

5745 Managing network interfaces controls what network devices are plugged into switches within

- 5746 manufacturing system, along with physical labeling connections to help with system
- 5747 identification and classification. Required actions will be performed directly on the exterior of
- the switch. Switch port in use will be labeled logically within switch console itself, along with
- 5749 the corresponding network cable for easy identification. All cable should be labeled/identified at
- 5750 the switch and at the opposite end of the network cable. Switch Port Security should be
- 5751 configured to restrict access to only allowed preconfigured Media Access Control (MAC)
- addresses devices.
- 5753 Minimal cost for labeling. Effort of implement is high, but not difficult. The effort will be spent 5754 taking the required time to accurately identify cabling connections.
- 5755 Most switches have built in Port security. Since this technical control is built into switches there
- 5756 is no additional cost for implementation. Configuration for Port security is well documented and
- 5757 easily configured

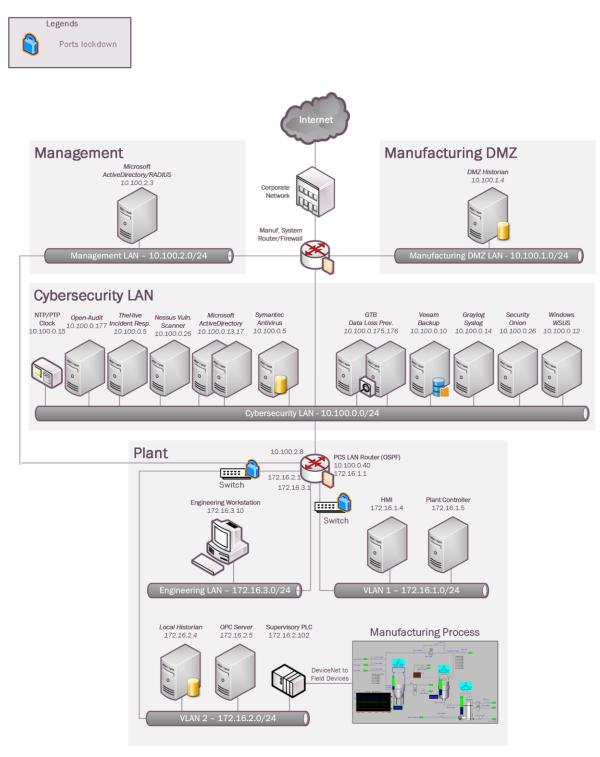
5758 **4.20.2 Technical Capabilities Provided by Solution**

- 5759 Managed Network Interfaces provides components of the following Technical Capabilities 5760 described in Section 6 of Volume 1:
- Managed Network Interfaces

5762 **4.20.3 Subcategories Addressed by Implementing Solution**

5763 PR.AC-5





5767	4.20.5 Installation Instructions and Configurations
5768	Managing Network Interface Instructions
5769	Overview:
5770 5771 5772	Port labeling provides ability for others to understand and know what network devices belong where. Managing your switches with correct labeling and classification makes troubleshooting simpler along with improving cybersecurity.
5773	Labeling ports within switch:
5774	Router/Switches within PCS: Allen-Bradley
5775	Stratix 8300 (Router) 172.16.3.1
5776	Stratix 5700 (Switch) Vlan1 172.16.1.3, Vlan2 172.16.2.2
5777	
5778 5779	 Login to switch/router via web browser. https://x.x.x.x Once logged in click on Configure → Port Settings Configure ▼ ■ Network
5780 5781 5782 5783 5784	 Smartports Port Settings Select port that will be labeled and click edit. A window will appear, now type into box next to Description and enter desired label. Description Engg Workstation Click OK to save change and exit.
5785	Same steps apply to Switches/Router within Process Control
5786	
5787	Port Security Configuration for Process Control Enclave
5788	Overview:
5789 5790 5791 5792 5793	Port security prevents unauthorized devices from being plugged into a network switch while trying to obtaining sensitive information, which could be used for mapping out network connections for possible data exfiltration. When an unauthorized device is plugged into a protected port a warning message is logged and sent to a syslog server if supported by switch vendor.
5794	
5795	

1

Selected 0 | Total 10 🎬 🖕

5796 **Process Control Enclave:**

- 5797 • Enclave contains two different switches/routers.
- 5798 • Allen Bradley Router (8300)
- 5799 Allen Bradley Switch (5700) 0

5800 Allen Bradley Router 8300: Has multiple ports which are individual configurable depending on 5801 desired network topology.

5802 Ports Fa1/1, Fa1/2, Fa1/3(Port Security Enabled), Fa1/4, Gi1/1 = Enabled •

5803

Phy	Port Gi1/2 = Disabled Physical Port Table Selected 0 Total 8 @ . / Edit												
	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode				
0	Fa1/1	Plant subn	۲	Auto-100Mb/s	Auto-Full	10/100BaseTX		routed					
\bigcirc	Fa1/2	Manf- Vlan	•	Auto-100Mb/s	Auto-Full	10/100BaseTX		routed					
0	Fa1/3	Engg Work	•	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	1	Access				
\bigcirc	Fa1/4	Uplink to L	۲	Auto-100Mb/s	Auto-Full	10/100BaseTX		routed					
0	Gi1/1	Mgmt	۲	Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/10	Static access	3	Access				
\bigcirc	Gi1/2		•	Auto	Auto	AUTO-SELECT Not Pr	Down		Trunk				

5804

Enabling port security for connection are only allowed when configuring a switching 5805 • 5806 port. If a port has been configured for routing port security cannot be enabled.

5807 Allen Bradley 5700 (172.16.1.3): Layer 2 switch (Vlan1)

- 5808 • Ports Fa1/1, Fa1/2, Fa1/5, Fa1/6, Gi1/1 are all configured for switching.
- 5809 Ports Fa1/3, Fa1/4, Fa1/7, Fa1/8, Gi1/2 are currently disabled. •

🕫 Edit	t									
P	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode	
) F	a1/1		۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	101	Access	
) F	a1/2		۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	101	Access	
) F	a1/3		•	Auto	Auto	10/100BaseTX	Down	101	Dynamic auto	
) F	a1/4		۲	Auto	Auto	10/100BaseTX	Down	101	Dynamic auto	
) F	a1/5		۲	Auto-10Mb/s	Auto-Full	10/100BaseTX	Static access	104	Access	
) F	a1/6		۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	104	Access	
) F	a1/7		۲	Auto	Auto	10/100BaseTX	Down	101	Dynamic auto	
) F	a1/8		٠	Auto	Auto	10/100BaseTX	Down	101	Dynamic auto	
) (Gi1/1		۲	Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/10	Static access	101	Access	
) (Gi1/2		٠	Auto	Auto	AUTO-SELECT Not Pr	Down	1	Dynamic auto	

5810

5811 Allen Bradley 5700 (172.16.2.2): Layer 2 switch (Vlan2)

5812 Ports Fa1/1, Fa1/4, Fa1/5, Fa1/6, Fa1/7, Gi1/1 are all configured for switching.

Ports Fa1/2, Fa1/3, Fa1/8, Gi1/2 are currently disabled. 5813 •

Physical Port Table

/ Edit							
Port Name Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
○ Fa1/1	۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
○ Fa1/2	•	Auto	Auto	10/100BaseTX	Down	102	Access
○ Fa1/3	•	Auto	Auto	10/100BaseTX	Down	102	Dynamic auto
○ Fa1/4	۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
○ Fa1/5	•	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
○ Fa1/6	۲	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	\$ ₁₀₂	Access
○ Fa1/7	•	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
○ Fa1/8	•	Auto	Auto	10/100BaseTX	Down	102	Dynamic auto
O Gi1/1	۲	Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/10	Static access	102	Access
O Gi1/2	•	Auto	Auto	AUTO-SELECT Not Pr	Down	1	Dynamic auto

5815 Enable Port Security (Allen Bradley 5700 and 8300, switch ports only)

- 5816 • Login into Allen Bradley device via web browser.
- 5817 • Click, "Configure→Security→Port Security"



- Select desired port requiring security and click "Edit" button. Fal/1 5819
- Place a check in box next to "Enable" and then click "Add Learned MAC Addresses" 5820 5821 or add the Addresses manually.

Port Name	Fa1/1	
Enable	\checkmark	
Maximum MAC Count	1]
0cc4.7a31.3ed7]	
	Add Learned MAC Addresses	
		Add
	Remove	
	Remove All	

- 5822
- Once MAC addresses have been added click "OK" to save changes. 5823

OK Cancel

- If more than one MAC addresses are required to be added change "Maximum MAC 5824
- Count" to the required MACs being assigned to this port. 5825
- 5826

Disable unused ports 5827

- While on the homepage select "Configure→Port Settings" 5828 •
- Find all Operational Mode labeled as down to identify ports being disabled. 5829 Operational Mode Static access

Down	
Down	
Static	access
Down	
Static	access
Dansa	

- 5830
- Now select on of the down ports and click on "Edit" 5831
- Once "Edit Physical Port" window appears remove check for enable from 5832 Administrative and click OK. Administrative 🗌 Enable 5833

- Port now is disabled. Any device plugged into this port or other disabled ports will not work.
- 5836 Lessons Learned
- A Router don't allow Port Security via MAC on a routed port. This is because a routed port uses IP Address and not MAC Addresses.
- When enabling Port Security turn on one port at a time to limit changes within the environment.
- 5841 Snippet from Allen Bradley Vlan1 Switch Running-Config File

```
interface FastEthernet1/1
switchport access vlan 101
switchport mode access
switchport port-security mac-address 0cc4.7a31.3ed7
switchport port-security
ī
interface FastEthernet1/2
switchport access vlan 101
switchport mode access
switchport port-security mac-address 0cc4.7a31.4447
switchport port-security
interface FastEthernet1/3
switchport access vlan 101
shutdown
interface FastEthernet1/4
switchport access vlan 101
shutdown
interface FastEthernet1/5
switchport access vlan 104
switchport mode access
switchport port-security mac-address 0cc4.7a32.b300
switchport port-security
interface FastEthernet1/6
switchport access vlan 104
switchport mode access
switchport port-security mac-address 001d.9cbf.78b3
switchport port-security
interface FastEthernet1/7
switchport access vlan 101
shutdown
interface FastEthernet1/8
switchport access vlan 101
shutdown
1
```

```
interface GigabitEthernet1/1
switchport access vlan 101
switchport mode access
switchport port-security mac-address e490.693b.c2c6
switchport port-security
interface GigabitEthernet1/2
shutdown
interface FastEthernet1/1
switchport access vlan 102
switchport mode access
switchport port-security mac-address 0cc4.7a32.b301
switchport port-security
interface FastEthernet1/2
switchport access vlan 102
switchport mode access
shutdown
interface FastEthernet1/3
switchport access vlan 102
shutdown
interface FastEthernet1/4
switchport access vlan 102
switchport mode access
switchport port-security mac-address fcaa.147a.aa42
switchport port-security
interface FastEthernet1/5
switchport access vlan 102
switchport mode access
switchport port-security mac-address 001d.9cc9.6d42
switchport port-security
I.
interface FastEthernet1/6
switchport access vlan 102
switchport mode access
switchport port-security maximum 2
switchport port-security mac-address 0800.27ae.9958
switchport port-security mac-address 0cc4.7a31.44bd
switchport port-security
т
interface FastEthernet1/7
switchport access vlan 102
switchport mode access
switchport port-security mac-address 0060.3520.c156
switchport port-security
1
interface FastEthernet1/8
switchport access vlan 102
shutdown
```

interface GigabitEthernet1/1 switchport access vlan 102 switchport mode access switchport port-security mac-address e490.693b.c2c7 switchport port-security

interface GigabitEthernet1/2 shutdown

! interface Vlan1 no ip address shutdown

5844 5845

5846

5847

Snippet from the Allen Bradley Boundary Router Running-Configuration file

interface FastEthernet1/3 description Engg LAN Workstation switchport mode access switchport port-security mac-address 40a8.f03d.48ae switchport port-security ip access-group EnggWkstn-ACL in

5848

5849

5850 **4.20.6 Highlighted Performance Impacts**

5851 No performance measurement experiments were performed for the managed network interfaces

due to their implementation method (i.e., manually disable unused network interfaces inconfiguration).

5854 **4.20.7** Link to Entire Performance Measurement Data Set

5855 N/A

5857 **4.21 Time Synchronization**

5858 **4.21.1 Technical Solution Overview**

- 5859 Ability to have all devices sync from a reliable time source. Time synchronization is vital for 5860 system logins, event tracking and all other time sensitive events occurring with a manufacturing 5861 system.
- 5862 No additional cost since services are included.
- 5863 Ease of use simple
- 5864 Effort and time required = minimal

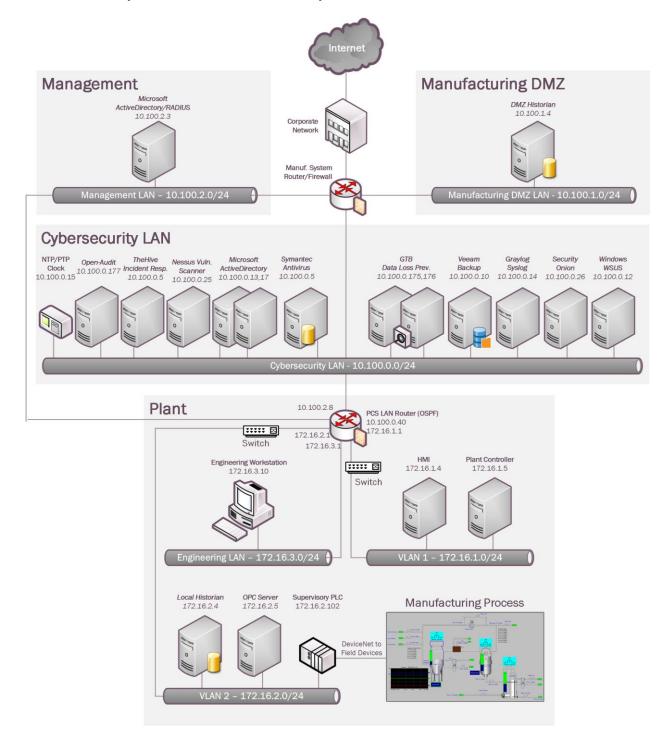
5865 **4.21.2 Technical Capabilities Provided by Solution**

- 5866 Time Synchronization provides components of the following Technical Capabilities described in5867 Section 6 of Volume 1:
- 5868 Time Synchronization

5869 **4.21.3 Subcategories Addressed by Implementing Solution**

5870 PR.PT-1

5871 **4.21.4** Architecture Map of Where Solution was Implemented



5873

5874 **4.21.5** Installation Instructions and Configurations

5875 Details of the NTP server implemented:

Name	IP address	Purpose
Meinberg M9000 Lantime	10.100.0.15	NTP/PTP Clock

5876

5877 Computers:

All windows computers within process control environment for Westman are joined to a domain.
Domain joined machines automatically update their time by contacting local domain controller.

5880 **Domain Controller:**

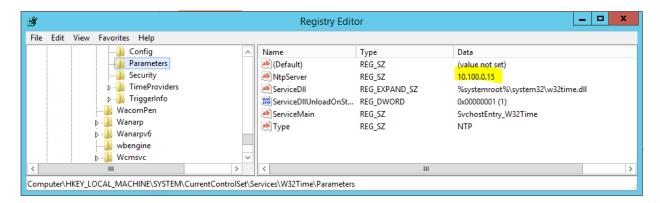
5881 Domain controller obtains time from Meinberg Lantime M900 device. W32tm.exe is used to 5882 configure Windows Time service settings. Change the following registry key on the Domain

5883 Controller to have w32Time sync its time from an external source IP address.

5885 Controller to have w5211me sync its time from an external source iP address.

5884 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer

5885 The image below shows our Domain Controller pointing to the IP address of Meinberg LAN5886 Time clock



5887

5888 **Other Devices:**

5889 All other devices within manufacturing system contact Meinberg Lantime M900 using NTP to 5890 sync time.

5891 Allen Bradley Boundary Router:

- Login to the web UI by browsing to https://172.16.3.1
- 5893 Click on Configure \rightarrow NTP

• Click Add button to add new time server.												
		🖭 Add 🏼 🦯 Edit 🔰	Add 🖋 Edit 💥 Delete									
		Status	Configured	IP Address	Prefer	Ref Clock	Stratum	When	Poll	Delay	Off Set	
5895		O sys.peer	Yes	10.100.0.15		129.6.15.28	2	558	1024	0.767	-0.334	
5896	•	Save chan	ge									
5897	•	Logout										
	~											
5898	Switc	hes:										

• Steps for switches Vlan1 (172.16.1.3) and Vlan2 (172.16.2.2) are the same as above.

5900 Lesson Learned: The master time reference selected should be as close to your physical location5901 as possible. This should reduce the Off Set.

5902

5903 **4.21.6 Highlighted Performance Impacts**

No performance measurement experiments were performed for time synchronization due to itsinstallation in the system before the Manufacturing Profile implementation was initiated.

5906 **4.21.7** Link to Entire Performance Measurement Data Set

5907 N/A

5909 **4.22 System Use Monitoring**

5910 **4.22.1 Technical Solution Overview**

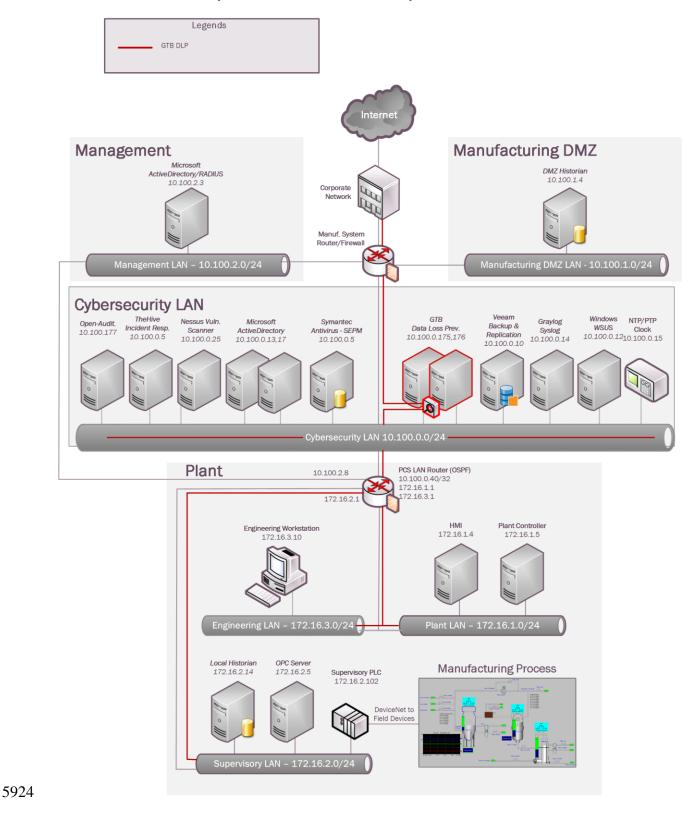
- 5911 System use monitor is accomplished by multiple tools to protect manufacturing system
- 5912 environment from harmful actives using data loss protection, auditing and syslog server for
- 5913 monitoring, store and auditing. Each tool provides a different level required to protect the
- 5914 manufacturing system.
- 5915 Implementation effort is moderate requiring understand of Linux and Windows systems, along
- 5916 with virtual machine experience. Time required to install and configure all components 10 to 20
- 5917 hours depending on skill level.

5918 **4.22.2** Technical Capabilities Provided by Solution

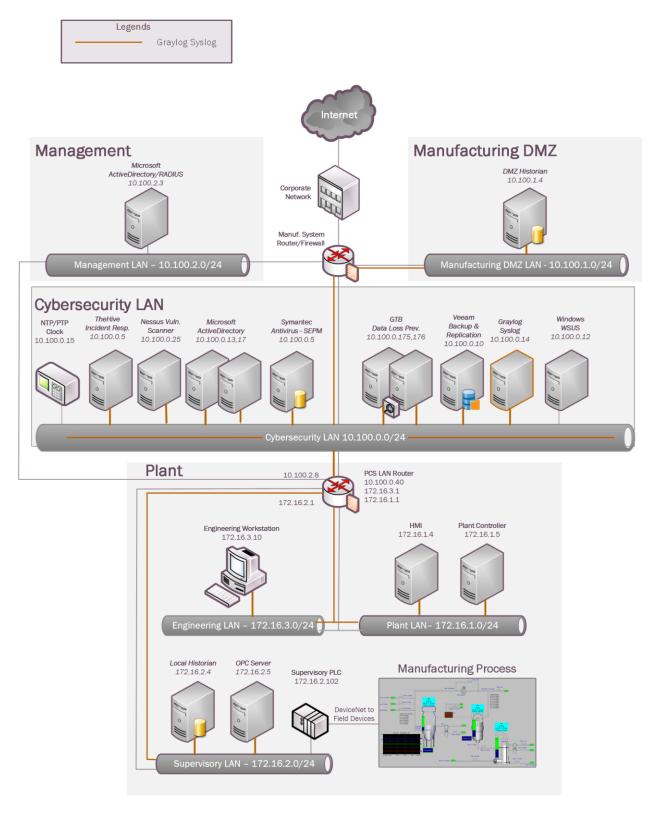
5919 System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and 5920 Graylog.

5921 **4.22.3** Subcategories Addressed by Implementing Solution

5922 PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3



5923 **4.22.4** Architecture Map of Where Solution was Implemented



NISTIR 8183A VOL. 2 (DRAFT)

5927 **4.22.5** Installation Instructions and Configurations

- 5928 System use monitoring was implemented using a combination of tools such as GTB Inspector,
- 5929 Graylog and native Windows Server Capabilities such as enabling Auditing, restricting 5930 administrative user accounts.
- 5931 **GTB DLP**: See Section 4.15.5 for instructions.
- 5932 **Graylog**: See Section 4.16.5 for instructions

5933 Auditing Logon events:

- 5934 Open Group Policy manager on domain controller.
- 5935 Right click on Group Policy and select edit.

or oup i oney management	
	_ 8
OPC_Security01 Scope Details Settings Delegation Status	
OPC_Security01	~
Data collected on: 5/2/2019 10:41:27 AM	show all
Computer Configuration (Enabled)	<u>hide</u>
Policies	<u>hide</u>
Windows Settings	<u>hide</u>
Security Settings	<u>hide</u>
Local Policies/Audit Policy	<u>hide</u>
Policy Setting	
Audit account logon events Success, Failure	
Audit logon events Success, Failure	
Audit object access Success, Failure	
User Configuration (Enabled)	hide
No settings defined.	

5937 Navigate to Computer Configuration→Polices→Windows Settings→Security Settings→Local
 5938 Polices→Audit Policy

5939 Now change setting to reflect Success, Failure

5940 Auditing Process Termination:

- 5941 While in Group Policy manager navigate to Computer Configuration→Polices→Windows
- 5942 Settings→Security Settings→Advanced Audit Configuration→
- 5943 Change Detailed Tracking and Logon/Logoff to Success / Success, Failure (See Image)

	5_Audit_Policy Oetails Settings Delegation Status		
Proce	ess_Audit_Policy		
Data co	ollected on: 5/2/2019 10:39:45 AM		show all
Comput	ter Configuration (Enabled)		hide
Polici	ies		<u>hide</u>
Wir	ndows Settings		<u>hide</u>
S	ecurity Settings		<u>hide</u>
	Advanced Audit Configuration		<u>hide</u>
	Detailed Tracking		<u>hide</u>
	Policy	Setting	
	Audit Process Termination	Success	
	Logon/Logoff		<u>hide</u>
	Policy	Setting	
	Audit Logon	Success, Failure	
User C	Configuration (Enabled)		<u>hide</u>
	No settings defined.		

5945 **Restricting Administrative Users:**

- 5946 The local Administrators group on each system was reviewed and only those accounts that 5947 needed to have Administrative privileges on the system were added to this group.
- 5948 For instance: An active directory user account "opc-admin" was created to run OPC-server 5949 services and was granted Administrative privileges on the below 2 servers:
- 5950 OPC Server
- Controller Server
- 5952 Remote Access to PLC is only permitted through Engineering workstation.

5953 **4.22.6 Highlighted Performance Impacts**

- 5954 No performance measurement experiments were performed for the installation of GTB into the
- 5955 PCS due to its location within the network topology. No manufacturing process components
- 5956 across the boundary on a regular basis while the system is operational.
- 5957 No performance measurement experiments were performed for the use of the Graylog due to its 5958 typical installation and usage location (i.e., external to the manufacturing system).

5959 **4.22.7** Link to Entire Performance Measurement Data Set

5960 N/A

5962 **4.23** Ports and Services Lockdown

5963 4.23.1 Technical Solution Overview

5964 Ports and services lockdown solutions enable a manufacturer to discover and disable nonessential logical network ports and services. A logical port is a number assigned to a 5965 "logical" connection. Port numbers are assigned to a service, which is helpful to TCP/IP in 5966 5967 identifying what ports it must send traffic to. Hackers use port scanners and vulnerability scanners to identify open ports on servers. By revealing which ports are open, the hacker can 5968 5969 identify what kind of services are running and the type of system. Closing down unnecessary 5970 ports by uninstalling un-necessary programs considerably reduces the attack surface. These 5971 actions need to be performed manually.

5972

5975

Native OS capabilities, Open-Audit and Nessus scanner were leveraged to inventory list of portsand applications currently running on each device of the plant.

5976 **4.23.2 Technical Capabilities Provided by Solution**

5977 Ports and Services Lockdown provides components of the following Technical Capabilities 5978 described in Section 6 of Volume 1:

- 5979
- Ports and Services Lockdown

5981 **4.23.3 Subcategories Addressed by Implementing Solution**

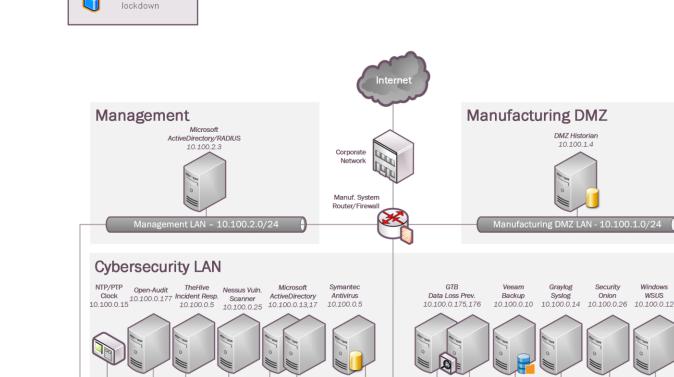
5982 PR.IP-1, PR.PT-3

Ports & Services

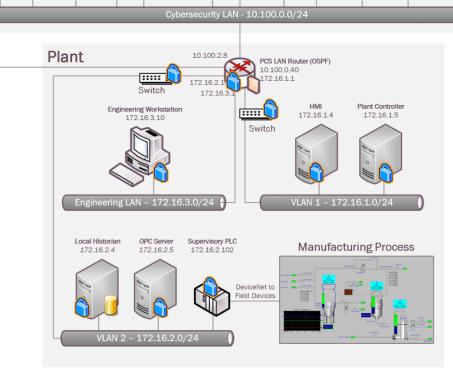
Legends

Windows

WSUS



5983 4.23.4 Architecture Map of Where Solution was Implemented



5985 **4.23.5** Installation Instructions and Configurations

- 5986 The following steps were performed on all Windows systems of the Plant
- Removal of Un-wanted programs
- 5988 Disable unsecure services
- 5989 <u>Removal of Un-wanted programs:</u>

A software inventory of each system was performed using Open-Audit. The inventory reports
were reviewed, and a list of unwanted programs were identified. These includes some software
that's comes by default with the OS. These programs were then uninstalled.

- Netstat utility was used to gather information about which applications are running or usingwhich TCP/IP ports on each system
- 5995 For instance: netstat -aon | more will generate a list of processes, PID

	t Windows [Version t (c) 2009 Microsof	6.1.7601] t Corporation. All righ	ts reserved.	
::\Users	\Administrator>nets	tat —aon ¦ more		
Ictive C	Connections			
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	976
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1332	0.0.0.0:0	LISTENING	2552
TCP	0.0.0.0:3060	0.0.0.0:0	LISTENING	3844
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1412
TCP	0.0.0.0:4241	0.0.0.0:0	LISTENING	2756
TCP	0.0.0.0:5241	0.0.0.0:0	LISTENING	2812
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:6000	0.0.0.0:0	LISTENING	1204
TCP	0.0.0.0:6002	0.0.0.0:0	LISTENING	2892
TCP	0.0.0.0:6160	0.0.0.0:0	LISTENING	8288
TCP	0.0.0.0:6183	0.0.0.0:0	LISTENING	8532
TCP	0.0.0.0:6185	0.0.0.0:0	LISTENING	8532
TCP	0.0.0.0:7001	0.0.0.0	LISTENING	2856
TCP	0.0.0.0:7002	0.0.0.0:0	LISTENING	2856
TCP	0.0.0.0:8082	0.0.0.0	LISTENING	2664
TCP	0.0.0.0:9395	0.0.0.0:0	LISTENING	8532

- 5997 The PID from the above output can be used with Windows Task Manager for further analysis.
- 5998 Within Task Manager (Windows 7), enable the PID column by clicking on View >> Select
 5999 Columns.
- 6000 Next, you might have to use the option to Show Processes for All Users, and then you'll be able
- to find the PID in the list. Once you're there, you can use the End Process, Open File Location,
- 6002 or Go to Service(s) options to control the process or stop it.

plications Proces	ses Se	rvices F	Performance	Network	king Users					
Image Name	PID	User	Name	z	Memory (Pri	ivate W	Handle	s	Description	-
System Idle P	0	SYSTE	EM	99		24 K		0	Percentage of time th	
System	4	SYSTE	EM	00		212 K	850	0	NT Kernel & System	
IAStorDataMg	304	SYSTE	EM	00		8,952 K	350	0	IAStorDataSvc	-
smss.exe	392	SYSTE	EM	00		628 K	3	0	Windows Session Mai	1
svchost.exe	484	LOCA	L SERVICE	00		13,964 K	62	0	Host Process for Win	
svchost.exe	512	SYSTE	EM	00	2	231,432 K	66	0	Host Process for Win	
csrss.exe	536	SYSTE	EM	00		2,960 K	1,29	0	Client Server Runtime	
wininit.exe	624	SYSTE	EM	00		1,420 K	8	. 0	Windows Start-Up Ap	
services.exe	696	SYSTE	EM	00		7,136 K	355	0	Services and Controll	
lsass.exe	720	SYSTE	EM	00		8,960 K	1,14	0	Local Security Author	
jusched.exe *32	724	Admir	nistrator	00		2,712 K	16	9	Java Update Schedul	
lsm.exe	732	SYSTE	EM	00		3, 196 K	286	0	Local Session Manage	
svchost.exe	892	SYSTE	EM	00		6,556 K	42	0	Host Process for Win	
svchost.exe	912	LOCA	L SERVICE	00		8,392 K	44	0	Host Process for Win	
svchost.exe	976	NETW	ORK SERVI	. 00		7,252 K	42	0	Host Process for Win	
svchost.exe	1040	SYSTE	EM	00		31,224 K	1,46	0	Host Process for Win	
svchost.exe	1176	SYSTE	EM	00		5,204 K	19	0	Host Process for Win	
FTLDIntAgent	1204	0.0	en File Locati	ion		2,604 K	100	0	FactoryTalk Historian	
igfxCUIServic	1320	Op	en ne cocac	ion		2,096 K	100	0	igfxCUIService Modu	
Imgrd.exe *32	1356	Enc	Process			2,120 K	130	0	Flexera Software, In	
svchost.exe	1412	Ene	Process Tre			25,380 K	789	0	Host Process for Win	
spoolsv.exe	1528			e		5,060 K	31	. 0	Spooler SubSystem A	
svchost.exe	1568	Dek	bug			8,912 K	34	: 0	Host Process for Win	
FTSysDiagSvc	1704	UA	C Virtualizati	on		2,472 K	119	0	Rockwell Automation	
armsvc.exe *32	1824	Cre	ate Dump Fi	le		1,192 K	8	0	Adobe Acrobat Upda	
svchost.exe	1884	0.0	are builtpri			3,004 K	16	0	Host Process for Win	
FuantCarvar	1016	Set	Priority		>	4 584 V	181	0	Event Server	-
* L	_	Set	Affinity							_
Show processes	s from	Sec	, arring you						End Process	
		Pro	perties							-

6004 Other alternatives are using **Resource Monitor** (resmon.exe) and **TCPView** from SysInternals6005 [1].

6006 TCPView:

6003

ile Options Process View Help									
🖬 🛪 🏁 😰									
Process	PID	Protocol	Local Address	Local Port	Remote Add	Remote Port	St ∇	Sent Packets	S
RdcyHost.exe	2552	TCP	127.0.0.1	1332	127.0.0.1	49192	ESTABLISHED		
RsvcHost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	49193	ESTABLISHED		
RsvcHost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65156	ESTABLISHED		
RsvcHost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65157	ESTABLISHED		
RsvcHost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65160	ESTABLISHED		
RsvcHost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	49174	ESTABLISHED		
Imgrd.exe	1356	TCP	127.0.0.1	27000	127.0.0.1	49172	ESTABLISHED		
🖸 nxloq.exe	2332	TCP	127.0.0.1	49166	127.0.0.1	49167	ESTABLISHED		
🖸 nxloq.exe	2332	TCP	127.0.0.1	49167	127.0.0.1	49166	ESTABLISHED		
🖸 flexsvr.exe	2404	TCP	127.0.0.1	49170	127.0.0.1	49171	ESTABLISHED		
🖸 flexsvr.exe	2404	TCP	127.0.0.1	49171	127.0.0.1	49170	ESTABLISHED		
🖾 flexsvr.exe	2404	TCP	127.0.0.1	49172	127.0.0.1	27000	ESTABLISHED		
🛾 RSLinxNG.exe	2756	TCP	127.0.0.1	49174	127.0.0.1	5241	ESTABLISHED		
RdcyHost.exe	2552	TCP	127.0.0.1	49192	127.0.0.1	1332	ESTABLISHED		
RdcyHost.exe	2552	TCP	127.0.0.1	49193	127.0.0.1	5241	ESTABLISHED		
mstsc.exe	4864	TCP	172.16.3.10	51955	172.16.1.4	3389	ESTABLISHED		
mstsc.exe	7996	TCP	172.16.3.10	51956	172.16.2.5	3389	ESTABLISHED		
WinSCP.exe	8732	TCP	172.16.3.10	58958	10.100.0.16	22	ESTABLISHED		
P putty.exe	3456	TCP	172.16.3.10	60520	10.100.0.16	22	ESTABLISHED		
P putty.exe	4944	TCP	172.16.3.10	60522	10.100.0.16	22	ESTABLISHED		
P putty.exe P putty.exe	3884	TCP	172.16.3.10	60526	10.100.0.16	22	ESTABLISHED		
mstsc.exe	9052	TCP	172.16.3.10	64301	172.16.2.3	3389	ESTABLISHED		
mstsc.exe	8308	TCP	172.16.3.10	64317	172.16.2.4	3389	ESTABLISHED		
mstsc.exe	2296	TCP	172.16.3.10	64328	172.16.1.5	3389	ESTABLISHED		
EventClientMultiplexer.exe	3864	TCP	127.0.0.1	65156	127.0.0.1	5241	ESTABLISHED		
RnaDirServer.exe	3844	TCP	127.0.0.1	65157	127.0.0.1	5241	ESTABLISHED		
RNADirMultiplexor.exe	4340	TCP	127.0.0.1	65160	127.0.0.1	5241	ESTABLISHED		
RdcyHost.exe	2552	TCP	172.16.3.10	65109	172.16.2.4	1332	SYN_SENT		

6007

6009	The following steps were performed on all network devices of the Plant
6010 6011 6012 6013	 Disabling unsecure services such as Telnet, SNMP (1 and 2) If SNMP is required, change the default community string Setting a password for enable Cisco commands to set a password for enable:
6014 6015 6016 6017	router1(config)# enable router1(config)# configure terminal router1(config)# enable secret <password></password>
6018	• Restrict ssh access to select machines.
6019	Cisco commands to restrict access [2]:
6020	router1(config)# enable
6021	router1(config)# configure terminal
6022	router1(config)# access-list 1 permit 172.16.0.0 0.0.255.255
6023	<pre>router1(config)# line vty 0 15</pre>
6024	<pre>router1(config-line)# access-class 1 in</pre>
6025	

- 6026 The following steps were performed on the PLC
- Disabled unsecure services such as Telnet, SNMP and HTTP
- Remote Access to the PLC was permitted only through the Engineering Workstation.
- 6029 **4.23.6 Highlighted Performance Impacts**
- 6030 No performance measurement experiments were performed for the managed network interfaces
- due to their implementation method (i.e., manually disabled network ports and removed
- 6032 unwanted Windows programs and services).
- 6033 **4.23.7** Link to Entire Performance Measurement Data Set
- 6034 N/A

6035 **4.24 Media Protection**

6036 4.24.1 Technical Solution Overview

Port locks provide a low-cost solution for protecting USB ports. Implementation and ease of use
provide for quick install and easy removal. USB Port locks provide a simple yet effective
solution to restrict USB use. Once USB Port lock has been inserted and engaged there is no way
of removing lock device without damaging USB port unless key is used. Each USB Port lock can
block up to two ports. These ports are the inserted port, and the port directly to either side
depending on the blocking plate direction. USB Port Lock can be purchased with a collar that

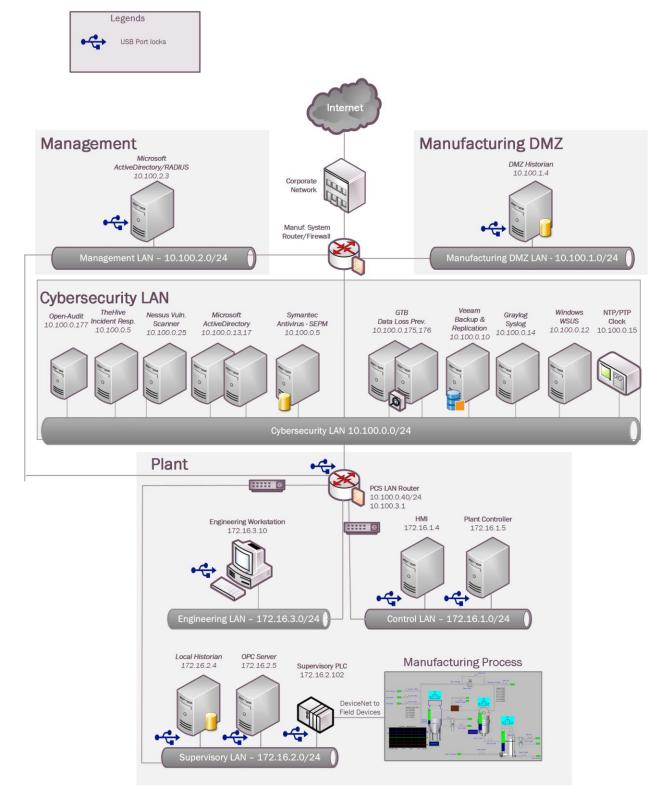
6043 protects attached USB Mice and Keyboards from removal without prior approval.

6044 **4.24.2 Technical Capabilities Provided by Solution**

- 6045 Media Protection provides components of the following Technical Capabilities described in
- 6046 Section 6 of Volume 1:
- 6047
- 6048 Media Protection

6049 **4.24.3 Subcategories Addressed by Implementation**

- 6050 PR.PT-2
- 6051



6052 **4.24.4** Architecture Map of Where Solution was Implemented

6054	4.24.5 Installation Instructions and Configurations
6055	Products / Tools found to meet capability:
6056	 Kensington USB Port Locks
6057	 Symantec Endpoint Protection (USB Policy Enforcement)
6058	 Group Policy Management (GPO) Active Directory
6059	Product / Tools selected to be implemented in testbed:
6060	• Kensington USB Port Locks (Protects Linux Machines)
6061	• Symantec Endpoint Protection (USB Policy Enforcement - Protects Windows
6062	Machines)
6063	 Group Policy (GPO) Active Directory (Protects Windows Machines)
6064	Products Overview:
6065	• USB Port locks from Kensington provide an alternative for small manufactures
6066	that don't have the resources or primarily run Linux machines within their
6067	environment to have a solution that protections from rogue USB devices being
6068	used without approval.
6069	Pros: Quick solution, Hardware only solution, inexpensive
6070	 Cons: Feels like having to force device into USB Port first few times
6071	Insert USB Port lock then push locking button in to secure. Kensington provides inserts to block
6072	multiple ports including locks designed for securing USB Keyboards and Mice.
6073	Lessons learned:
6074	Patience is required when using this product so as not to inadvertently damage USB port

6075 **4.24.6 Highlighted Performance Impacts**

6076 No performance measurement experiments were performed for the USB port locks due to their 6077 implementation method (i.e., physically restricting access to USB ports).

- 6078 **4.24.7** Link to Entire Performance Measurement Data Set
- 6079 N/A
- 6080
- 6081

6082 Appendix A - Acronyms and Abbreviations

- 6083 Selected acronyms and abbreviations used in this document are defined below.
- 6084 **CSF** Cybersecurity Framework
- 6085 **FIPS** Federal Information Processing Standards
- 6086 HMI Human Machine Interface
- 6087 ICS Industrial Control System
- 6088 ICS-CERT Industrial Control Systems Cyber Emergency Response Team
- 6089 **ISA** The International Society of Automation
- 6090 IT Information Technology
- 6091 LAN Local Area Network
- 6092NCCICNational Cybersecurity and Communications Integration Center
- 6093 NIST National Institute of Standards and Technology
- 6094 **NVD** National Vulnerability Database
- 6095 **OT** Operational Technology
- 6096 PLC Programmable Logic Controller
- 6097 US-CERT United States Computer Emergency Readiness Team
- 6098 **VPN** Virtual Private Network

Appendix B - Glossary 6099 6100 Selected terms used in in this document are defined below. 6101 Business/Mission Objectives - Broad expression of business goals. Specified target outcome 6102 for business operations. 6103 6104 **Capacity Planning -** Systematic determination of resource requirements for the 6105 projected output, over a specific period. [businessdictionary.com] 6106 6107 **Category** - The subdivision of a Function into groups of cybersecurity outcomes closely tied to 6108 programmatic needs and particular activities. 6109 Critical Infrastructure - Essential services and related assets that underpin American society 6110 6111 and serve as the backbone of the nation's economy, security, and health. [DHS] 6112 6113 Criticality Reviews - A determination of the ranking and priority of manufacturing system 6114 components, services, processes, and inputs in order to establish operational thresholds and 6115 recovery objectives. 6116 6117 Critical Services - The subset of mission essential services required to conduct manufacturing 6118 operations. Function or capability that is required to maintain health, safety, the environment and 6119 availability for the equipment under control. [62443] 6120 6121 Cyber Risk - Risk of financial loss, operational disruption, or damage, from the failure of the 6122 digital technologies employed for informational and/or operational functions introduced to a 6123 manufacturing system via electronic means from the unauthorized access, use, disclosure, 6124 disruption, modification, or destruction of the manufacturing system. 6125 6126 **Cybersecurity** - The process of protecting information by preventing, detecting, and responding 6127 to attacks. [CSF] 6128 6129 Defense-in-depth - The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security 6130 6131 technologies in the common attack vectors to ensure that attacks missed by one technology are 6132 caught by another. [62443 1-1] 6133 6134 Event - Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, 6135 capabilities, or reputation). [CSF] 6136 6137 6138 Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with 6139 the other computer hardware. [Techterms.com] 6140 6141

- 6142 Framework - The Cybersecurity Framework developed for defining protection of critical
- 6143 infrastructure. It provides a common language for understanding, managing, and expressing
- cybersecurity risk both internally and externally. Includes activities to achieve specific 6144
- 6145 cybersecurity outcomes, and references examples of guidance to achieve those outcomes.
- 6146
- 6147 Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity 6148 activities at their highest level.
- 6149

6150 **Incident** - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or 6151 availability of an information system or the information the system processes, stores, or transmits 6152 or that constitutes a violation or imminent threat of violation of security policies, security 6153 procedures, or acceptable use policies. [CSF]

6154

6155 Integrator - A value-added engineering organization that focuses on industrial control and

- 6156 information systems, manufacturing execution systems, and plant automation, that has
- 6157 application knowledge and technical expertise, and provides an integrated solution to an
- 6158 engineering problem. This solution includes final project engineering, documentation,
- procurement of hardware, development of custom software, installation, testing, and 6159
- 6160 commissioning. [CSIA.com]
- 6161
- 6162 Manufacturing Operations - Activities concerning the facility operation, system processes, 6163 materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to 6164
- the manufacturing enterprise. 6165 6166
- 6167 **Network Access** - any access a network connection in lieu of local access (i.e., user being 6168 physically present at the device).
- 6169

6170 **Operational technology** - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. 6171 [Gartner.com] 6172

6173

6174 **Programmable Logic Controller** - A solid-state control system that has a user-programmable 6175 memory for storing instructions for the purpose of implementing specific functions such as I/O 6176 control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data 6177 and file processing. [800-82]

6178

6179 Profile - A representation of the outcomes that a particular system or organization has selected 6180 from the Framework Categories and Subcategories. [CSF]

- 6181
- Target Profile the desired outcome or 'to be' state of cybersecurity implementation _ _ 6182 Current Profile – the 'as is' state of system cybersecurity
- 6183

6184 **Protocol** - A set of rules (i.e., formats and procedures) to implement and control some type of 6185 association (e.g., communication) between systems. [800-82]

- 6187 **Remote Access -** Access by users (or information systems) communicating external to an 6188 information system security perimeter. Network access is any access a network 6189 connection in lieu of local access (i.e., user being physically present at the device). [800-53] 6190 6191 **Resilience Requirements** - The business-driven availability and reliability characteristics for the 6192 manufacturing system that specify recovery tolerances from disruptions and major incidents. 6193 6194 Risk Assessment - The process of identifying risks to agency operations (including mission, 6195 functions, image, or reputation), agency assets, or individuals by determining the probability of
- 6196 occurrence, the resulting impact, and additional security controls that would mitigate this impact. 6197 Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability 6198 analyses. [800-82] 6199
- 6200 Risk Tolerance - The level of risk that the Manufacturer is willing to accept in pursuit of 6201 strategic goals and objectives. [800-53] 6202
- 6203 **Router** - A computer that is a gateway between two networks at OSI layer 3 and that relays and 6204 directs data packets through that inter-network. The most common form of router operates on IP 6205 packets. [800-82] 6206
- 6207 Security Control - The management, operational, and technical controls (i.e., safeguards or 6208 countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability 6209 of the system, its components, processes, and data. [800-82]
- 6210
- 6211 **Subcategory** - The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are 6212 catalogued," "Data-at-rest is protected," and "Notifications from detection systems are 6213 6214 investigated." [CSF]
- 6215
- 6216 Supporting Services - Providers of external system services to the manufacturer through a 6217 variety of consumer-producer relationships including but not limited to: joint ventures; business 6218 partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of 6219 business arrangements); licensing agreements; and/or supply chain exchanges. Supporting 6220 services include, for example, Telecommunications, engineering services, power, water, 6221 software, tech support, and security. [800-53]
- 6222
- 6223 **Switch** - A device that channels incoming data from any of multiple input ports to the specific 6224 output port that will take the data toward its intended destination. [Whatis.com]
- 6225
- 6226 **System Categorization** - The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or 6227 6228 confidentiality would have on organizational operations, organizational assets, or individuals. 6229 [FIPS 199]

- 6230 Third-Party Relationships relationships with external entities. External entities may include,
- for example, service providers, vendors, supply-side partners, demand-side partners, alliances,
 consortiums, and investors, and may include both contractual and non-contractual parties.
- 6232 [DHS]
- 6234 Third-party Providers Service providers, integrators, vendors, telecommunications, and
- 6235 infrastructure support that are external to the organization that operates the manufacturing6236 system.
- 6237
- Thresholds Values used to establish concrete decision points and operational control limits to
 trigger management action and response escalation.

6240 Appendix C - References

6241 6242 6243 6244 6245	1.	Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. <u>https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915</u>
6246	2.	National Institute of Standards and Technology (2014) Framework for Improving Critical
6247		Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and
6248		Technology, Gaithersburg, MD), February 12, 2014.
6249		https://doi.org/10.6028/NIST.CSWP.02122014
6250		
6251	3.	Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial
6252		Control Systems (ICS) Security. (National Institute of Standards and Technology,
6253		Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2.
6254		https://doi.org/10.6028/NIST.SP.800-82r2
6255		
6256	4.	Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2017)
6257		Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and
6258		Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183, Includes updates
6259		as of May 20, 2019. <u>https://doi.org/10.6028/NIST.IR.8183</u>
6260		