NIST SPECIAL PUBLICATION 1800-5B

IT Asset Management

Volume B:
Approach, Architecture, and Security Characteristics

Michael Stone
Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

Chinedum Irrechukwu
Harry Perper
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-5

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, 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 or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-5B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-5B, 47 pages, (September 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at financial_nccoe@nist.gov.

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

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

While a physical asset management system can tell you the location of a computer, it cannot answer questions like, “What operating systems are our laptops running?” and “Which devices are vulnerable to the latest threat?” An effective IT asset management (ITAM) solution can tie together physical and virtual assets and provide management with a complete picture of what, where, and how assets are being used. ITAM enhances visibility for security analysts, which leads to better asset utilization and security.

KEYWORDS

asset management; financial sector; information technology asset management; ITAM; personnel security; physical security; operational security

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
FS-ISAC	Financial Services Information Sharing and Analysis Center
Gorrell Cheek	Western Union
Joe Buselmeier	American Express
Sean Franklin	American Express
Ron Ritchey	Bank of America
Sounil Yu	Bank of America
Joel Van Dyk	Depository Trust & Clearing Corporation
Dan Schutzer	Financial Services Roundtable
George Mattingly	Navy Federal Credit Union
Jimmie Owens	Navy Federal Credit Union
Mike Curry	State Street
Timothy Shea	RSA
Mark McGovern	MobileSystem7
Atul Shah	Microsoft
Leah Kauffman	NIST
Benham (Ben) Shariati	University of Maryland Baltimore County
Valerie Herrington	Herrington Technologies
Susan Symington	MITRE Corporation
Sallie Edwards	MITRE Corporation

Name	Organization
Sarah Weeks	MITRE Corporation
Lina Scorza	MITRE Corporation
Karen Scarfone	Scarfone Cybersecurity

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
AlphaPoint Technology	AssetCentral
Belarc	BelManage, BelManage Analytics
Computer Associates	ITAM
Microsoft	WSUS, Server 2012R2 Certificate Authority
Peniel Solutions	Technology/Industry Expertise
PI Achievers	Penetration Testing Services
PuppetLabs	Puppet
RedJack	Fathom
Splunk	Splunk Enterprise
Tyco	iStar Edge
Vanguard Integrity Professionals	Security Manager

Contents

List of Figures

List of Tables

1 Summary

Companies in the financial services sector can use this NIST Cybersecurity Practice Guide to more securely and efficiently monitor and manage their organization's many information technology (IT) assets. IT asset management (ITAM) is foundational to an effective cybersecurity strategy and is prominently featured in the SANS Critical Security Controls [1] and NIST Framework for Improving Critical Infrastructure Cybersecurity [2].

During the project development, we focused on a modular architecture that would allow organizations to adopt some or all of the example capabilities in this practice guide. Depending on factors like size, sophistication, risk tolerance, and threat landscape, organizations should make their own determinations about the breadth of IT asset management capabilities they need to implement.

This example solution is packaged as a “How-To” guide that demonstrates how to implement standards-based cybersecurity technologies in the real world with a risk-based approach. We used open-source and commercial off-the-shelf (COTS) products that are currently available today. The guide helps organizations gain efficiencies in IT asset management, while saving them research and proof of concept costs.

This guide aids those responsible for tracking assets, configuration management, and cybersecurity in a financial services sector enterprise. Typically, this group will comprise those who possess procurement, implementation, and policy authority.

1.1 Challenge

The security engineers we consulted in the financial services sector told us they are challenged by identifying assets across the enterprise and keeping track of their status and configurations, including hardware and software. This comprises two large technical issues:

1. tracking a diverse set of hardware and software. Examples of hardware include servers, workstations, and network devices. Examples of software include operating systems, applications, and files.
2. lack of total control by the host organization. Financial services sector organizations can include subsidiaries, branches, third-party partners, contractors, temporary workers, and guests. It is impossible to regulate and mandate a single hardware and software baseline against such a diverse group.

1.2 Solution

An effective ITAM solution needs several characteristics, including:

- complement existing asset management, security, and network systems
- provide application programming interfaces to communicate with other security devices and systems such as firewalls and intrusion detection and identity and access management systems
- know and control which assets, both virtual and physical, are connected to the enterprise network
- automatically detect and alert when unauthorized devices attempt to access the network, also known as asset discovery
- enable administrators to define and control the hardware and software that can be connected to the corporate environment
- enforce software restriction policies relating to what software is allowed to run in the corporate environment
- record and track attributes of assets
- audit and monitor changes in an asset's state and connection
- integrate with log analysis tools to collect and store audited information

The ITAM solution developed and built at the NCCoE, and described in this document, meets all of these characteristics.

1.3 Risks

In addition to being effective, the ITAM solution must also be secure and not introduce new vulnerabilities into an organization. To reduce this risk, the NCCoE used security controls and best practices from NIST [3], the Defense Information Systems Agency (DISA) [4] and International Organization for Standardization (ISO) [5], and the Federal Financial Institutions Examination Council (FFIEC). How these individual controls are met by individual components of this solution can be seen in Table 4-2.

Some of the security controls we implemented include:

- access control policy
- continuous monitoring and tracking of assets connected to a network
- event auditing
- anomalous activity detection and reporting
- vulnerability scanning

By implementing an ITAM solution based on controls and best practices, implementers can tailor their deployment to their organization's security risk assessment, risk tolerance, and budget.

1.4 Benefits

The build described here employs passive and active data collectors/sensors across an enterprise to gather asset information and send it to a centralized location. The data collectors/sensors specialize in gathering information from different devices, no matter their operating system. Machines used by direct employees receive software agents that report on configuration, while temporary employees and contractors receive “dissolvable” agents and more passive sensing. Dissolvable agents are automatically downloaded to the client, run, and are removed. All of this information is gathered at a central location for analysis and reporting. You can choose to view all the activity in an enterprise, or configure the system to choose which machines are monitored, how much data is collected, and how long the data is retained.

The example solution described in this guide has the following benefits:

- enables faster responses to security alerts by revealing the location, configuration, and owner of a device
- increases cybersecurity resilience: help security analysts focus on the most valuable or critical assets
- improves and reduces reporting time for management and auditing
- provides software license utilization statistics (to identify cost reduction opportunities)
- reduces help desk response times: staff already know what is installed and the latest pertinent errors and alerts
- reduces the attack surface of machines by ensuring that software is correctly patched/updated

Other potential benefits include, but are not limited to rapid, transparent deployment and removal using consistent, efficient, and automated processes; improved situational awareness; and an improved security posture gained from tracking and auditing access requests and other ITAM activity across all networks.

This NIST Cybersecurity Practice Guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations as well as the Federal Financial Institutions Examination Council IT Examination Handbook and Cyber Assessment Tool (CAT) guidance
- provides
    - a detailed example solution with capabilities that address security controls

    - instructions for implementers and security engineers, including examples of all the necessary components and installation, configuration, and integration
- is modular and uses products that are readily available and interoperable with your existing IT infrastructure and investments

Your organization can be confident that these results can be replicated: We performed functional testing and submitted the entire build to verification testing. An independent second team verified the build documentation based on the information in this practice guide.

While we have used a suite of open source and commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee regulatory compliance. Your organization's information security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

2 How to Use This Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate all or parts of the build created in the NCCoE ITAM Lab. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-5A: *Executive Summary*
- NIST SP 1800-5B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-5C: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Financial services sector leaders, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-5A*, which describes the following topics:

- challenges that financial services sector organizations face in implementing and using ITAM systems
- example solution built at the NCCoE
- benefits of adopting a secure, centralized ITAM system, and the risks of a lack of visibility into networked IT assets

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-5B*, which describes what we did and why. The following sections will be of particular interest:

- Section 4.5, Risk Assessment and Mitigation, where we identify the steps we took to protect and monitor the ITAM system
- Section 4.5.1, Assessing Risk Posture, where we identify the security measures used in this implementation
- Section 4.5.2, Security Characteristics and Controls Mapping, where we map the security characteristics of this example solution to cybersecurity standards and best practices
- Section 4.6, Technologies, where we identify the products and technologies we used and map them to the relevant security controls

You might share the *Executive Summary, NIST SP 1800-5A*, with your leadership team members to help them understand the importance of adopting standards-based IT Asset Management (ITAM) which is foundational to an effective cybersecurity strategy and is prominently featured in the SANS Critical Security Controls [1] and NIST Framework for Improving Critical Infrastructure Cybersecurity [2].

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-5C*, to replicate all or parts of the build created in our lab. The How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products in financial services sector organizations. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of IT Asset Management (ITAM) which is foundational to an effective cybersecurity strategy and is prominently featured in the SANS Critical Security Controls [1] and NIST Framework for Improving Critical Infrastructure Cybersecurity [2]. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 4.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to financial_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/financial-services.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Introduction

In order for financial services sector institutions to make informed, business-driven decisions regarding their assets, they must first know what assets they possess, and their status. This information provides the visibility into license utilization, software support costs, unauthorized devices, vulnerabilities, and compliance. IT assets include items such as servers, desktops, laptops, and network appliances. Technology and policy constraints make it difficult to collect and analyze IT asset data in a large enterprise composed of multiple organizations (subsidiaries and partners) spread out over diverse geographic locations.

While many financial services sector companies label physical assets with bar codes and track them in a database, this approach does not answer questions such as, "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?" The goal of this project is to create an integrated system that can quickly provide answers to questions like these by connecting existing systems for physical assets, physical security, IT systems, and network security into a comprehensive ITAM system. Another key consideration is the need for companies to demonstrate compliance with industry and regulatory standards.

In our lab at the NCCoE, we constructed an ITAM solution that spans traditional physical asset tracking, IT asset information, physical security, and vulnerability and compliance information. Users can now query one ITAM system and gain insight into all four of these types of information regarding their entire IT asset portfolio.

Financial sector companies can employ this ITAM system to dynamically apply business and security rules to better utilize information assets and protect enterprise systems and data. In short, the ITAM system described in this practice guide gives companies the ability to monitor and report on an IT asset throughout its entire life cycle, thereby reducing the total cost of ownership by reducing the number of man-hours needed to perform tasks such as incident response and system patching.

4 Approach

4.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions in financial services organizations. Current decentralized systems often require connecting to multiple systems (assuming you have access), performing multiple queries, and then assembling a report. This centralized ITAM system provides data and metadata analysis, data aggregation, and reporting and alerting, all from an automated platform. The technical components will appeal to system administrators, IT managers, IT security managers, and others directly involved in the secure and safe operation of business operations and IT networks.

4.2 Scope

The scope of this guide encompasses the implementation of numerous products to centralize IT asset management. The scope concentrates on centralizing the following capabilities:

1. receiving a new physical IT asset
2. transferring a physical IT asset
3. migrating a virtual machine
4. detecting, preventing, and responding to incidents
5. continuously monitoring for unapproved hardware and software
6. continuously monitoring for vulnerabilities and applying corporate-approved patches/updates

The objective is to perform all of the above actions using a centralized system with interfaces designed for each task.

4.3 Assumptions

This project is guided by the assumptions described in the following subsections.

4.3.1 Security

This ITAM system provides numerous security benefits including increased visibility and faster remediation. We assert that the benefits of using this ITAM system outweigh any additional risks that may be introduced. A key assumption is that all potential adopters of the build or any of its components already have system and network security in place. Therefore, we focused on what potential new vulnerabilities were being introduced to systems if the solution (or any part of the solution) was implemented. One of the goals of this solution is to not introduce additional vulnerabilities, however there are always risks when adding systems, or adding new features into an existing system.

4.3.2 Modularity

Financial services sector companies already have ITAM solution(s) in place. Our philosophy is that a combination of certain components or a single component can improve ITAM functions for an organization, and that they need not remove or replace existing infrastructure. This guide provides a complete top-to-bottom solution and is also intended to provide various options based on need.

4.3.3 Technical Implementation

This practice guide is written from a “how-to” perspective, and its foremost purpose is to provide details on how to install, configure, and integrate the components. The NCCoE assumes that an organization has the technical resources to implement all or parts of the build, or has access to companies that can perform the implementation on its behalf.

4.3.4 Tracking and Location

The ITAM system described in this guide can provide an organization with location information for specific assets. This location information is typically in the form of building, room number, rack number, etc. The location information is usually manually entered into one or more asset databases. The location information in this project is not obtained via the global positioning system or other wireless/radio frequency tracking.

4.3.5 Operating Systems

This project uses Ubuntu Linux, CentOS Linux, RedHat Enterprise Linux, Windows Server 2012R2, and Windows 7 operating systems. Operating systems were chosen based on the requirements of the software. For example, BelManage and CA ITAM need to run on Windows 2012R2.

Operating systems were securely configured based on the Department of Defense standard configuration guidance known as the Security Technical Implementation Guidelines (STIGs) and Security Requirements guides. They are publicly available at http://iase.disa.mil/stigs/Pages/index.aspx. Each STIG includes a set of rules and guidelines for configuring the operating system implementation. For example, the Microsoft Windows 2012R2 STIG (http://iase.disa.mil/stigs/os/windows/Pages/index.aspx) was used to configure the Windows servers used in the build. The specific percentage of STIG compliance for each operating system used in the build is listed in NIST SP 1800-5C of this publication, How-To Guides. Note that the lab instantiation of the build did not require or allow implementation of every rule and guide in each STIG.

4.4 Constraints

This project has the constraints described in the following subsections.

4.4.1 Limited Scalability Testing

The NCCoE is a laboratory environment and is, therefore, constrained in terms of replicating a sizeable user base, such as that in most financial services sector companies. However, the products used in the build do not have that constraint and are designed for enterprise deployments.

4.4.2 Limited Assets

The NCCoE lab has access to a limited number and variety of IT assets. The assets at the NCCoE were included in the ITAM system, and the components used in the build do not have a limitation on the amount or variety of assets.

4.4.3 Mobile Devices

Due to scoping constraints, mobile devices were not included in the ITAM project. The NCCoE has several other projects dealing with mobile device security and management that can be used in conjunction with this ITAM project. For more information, please visit the NCCoE's Mobile Device Security project page: https://nccoe.nist.gov/projects/building_blocks/mobile_device_security.

4.4.4 Network Devices

The ITAM lab is almost totally composed of virtual machines. Some of the virtual machines are performing the duties of network devices, such as routers, firewalls, and switches. Where possible, the configurations and data collected by these devices are used by the ITAM system.

4.4.5 Limited Replication of Enterprise Network

The NCCoE was able to replicate the physical asset, physical security, IT systems, and network security silos in a limited manner. The goal was to demonstrate both logically and physically that functions could be performed from a centralized ITAM system regardless of where it is located in the enterprise. In a real-world environment, the interconnections between the silos are fully dependent on the business needs and compliance requirements of the individual enterprise. We did not attempt to replicate these interconnections. Rather, we acknowledge that implementing the project build or its components would create new interfaces across silos. We focused on providing general information on how to remain within the bounds of compliance should the build be adopted.

4.5 Risk Assessment and Mitigation

NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments* [6], states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* [7]—material that is available to the public. The risk management framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

We performed two types of risk assessment: the initial analysis of the risk posed to the financial sector, which led to the creation of the use case and the desired security characteristics, and an analysis to show users how to manage the cybersecurity risk to the components introduced by adoption of the solution.

In order to effectively enforce and audit security policy, an organization must first know what equipment and software are present. For example, knowing what hardware and software are present is the first step to enabling application whitelisting or blacklisting, and network access controls. The ability to view the status and configuration of everything in an organization from one centralized location is a very powerful tool that could result in disaster if it were to fall into the wrong hands. Therefore, the ITAM system must be extremely well protected and monitored. In response, we implemented access controls, network access restrictions, network monitoring, secure data transmission, configuration

management, and user activity monitoring. Section 4.5.2 provides a security evaluation of the architecture and a list of the security characteristics.

4.5.1 Assessing Risk Posture

Using the guidance in NIST's series of publications concerning the RMF, the NCCoE performed two key activities to identify the most compelling risks encountered by organizations within the financial sector. The first was a face-to-face meeting with members of the financial sector community to define the main security risks to business operations. This meeting identified a primary risk concern: the lack of a converged view and reporting capability for IT assets. We then identified the core risk area, ITAM, and established the core operational risks encountered daily in this area. The following associated tactical risks were identified:

- lack of knowledge of the IT asset locations
- lack of configuration controls for IT assets
- ineffective patch management
- lack of software vulnerability management
- lack of a common operating picture of the enterprise's IT assets
- lack of a converged repository of IT assets

The phone interviews with members of the financial sector gave us a better understanding of the business risks as they relate to the potential cost and business value. NIST SP 800-39, Managing Information Security Risk [8], focuses particularly on the business aspect of risk, namely at the enterprise level. This foundation is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. The following is a summary of the strategic risks:

- impact on service delivery – ensuring people have access to systems needed to perform their job functions in the security operations organization
- cost of implementation – implementing ITAM once and using it across all systems may reduce both system management and operational costs. Reuse of existing systems where possible
- budget expenditure as it relates to investment in security technologies
- projected cost savings and operational efficiencies to be gained as a result of new investment in security
- compliance with existing industry standards – FFIEC CAT requires deliberate and timely control of IT assets.
- high-quality reputation or public image
- risk of alternative or no action

Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary operational and strategic risk information, which was subsequently translated to security characteristics. Table 4-1 illustrates the mapping of these characteristics to NIST's SP 800-53 Rev. 4 [3] controls, along with the Cybersecurity Assessment Tool (CAT) and other security controls and best practices.

Implementing these security controls will substantially lower overall cyber-risk by providing mitigations against known cyber threats. Having a comprehensive ITAM system in place, like the one in this document, enables the effective implementation of other mitigations such as application whitelisting/blacklisting, and network access controls. A full list of the security technologies used to implement this reference architecture can be found in Table 4-2.

4.5.2 Security Characteristics and Controls Mapping

Table 4-1 maps the project's security characteristics to the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF), relevant NIST standards, Federal Financial Institution Examination Council Cybersecurity Assessment Tool (FFIEC CAT), and best practices. The mapping in Table 4-1 comes from the white paper we drafted when we initially defined this challenge [9].

Table 4-1 Security Characteristics and Controls Mapping

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
complement existing asset management, security, and network systems	Identify	Business Environment	ID.BE-4 Dependencies and critical functions for delivery of critical services are established	SA-14		D1.G.IT.B.2

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
	Protect	Access Control	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, AC-16	A.13.1.1, A.13.1.3, A.13.2.1	D3.DC.Im.B.1, D3.DC.Im.Int.1

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
provide APIs for communicating with other security devices and systems such as firewalls and intrusion detection and identity and access management (IDAM) systems	Detect	Anomalies and Events	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-5, SI-4		D3.DC.Ev.E.1

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
	Detect	Detection Processes	DE.DP-4: Event detection information is communicated to appropriate parties	AU-6, CA-7, RA-5, SI-4	A.16.1.2	D3.DC.Ev.B.2, D5.ER.Is.B.1, D5.ER.Is.E.1
know and control which assets, both virtual and physical, are connected	Identify	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	CA-7	A.8.1.1	D1.G.IT.B.1
	Identify	Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, SA-14, CA-7, CM-8, PE-20, SI-4	A.8.1.1	D1.G.IT.B.1

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
to the enterprise network	Identify	Asset Management	ID.AM-5: Resources are prioritized based on their classification, criticality and business value	IA-3	A.8.2.1	D1.G.IT.B.2
	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	PE-6, SC-7, SC-30, SC-32		D3.DC.Ev.B.3
detect and alert when unauthorized devices attempt to access the network	Detect	Anomalies and Events	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-2, AU-6, CA-7, IR-4, IR-5, SI-4		D3.DC.Ev.E.1
	Detect	Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	AU-12, CA-7, SC-7, SI-4		D3.DC.An.B.2

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	CM-8, PE-6, PE-20, SI-4, AU-12		D3.DC.Ev.B.3
	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented and reviewed in accordance with policy	IA-3, IR-6	A.12.4.1, A.12.4.3	D1.G.SP.B.3, D2.MA.Ma.B.1, D2.MA.Ma.B.2
integrate with ways to validate a trusted network connection	Identify	Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried	AU-2	A.8.1.1	D1.G.IT.B.1
	Identify	Asset Management	ID.AM-5: Resources are prioritized based on their classification, criticality and business value	CM-8, CA-7	A.8.1.1	D1.G.IT.B.1

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
	Identify	Asset Management	ID.AM-5: Resources are prioritized based on their classification, criticality and business value	SA-14, IA-3	A.8.2.1	D1.G.IT.B.2
	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-6, IR-5, IR-6	A.12.4.1, A.12.4.3	D1.G.SP.B.3
	Protect	Data Security	PR.DS-2: Data-in-transit is protected	SC-8	A.13.1.1, A.13.2.1, A.14.1.2	D3.PC.Am.B.13, D3.PC.Am.E.5, D3.PC.Am.Int.7
	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	AU-12, CA-7, CM-8, PE-3, PE-6, PE-20, SI-4		D3.DC.Ev.B.3

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
	Respond	Communications	RS.CO-2: Events are reported consistent with established criteria	AU-6, IR-6	A.16.1.2	D5.IR.Pl.B.2, D5.DR.Re.B.4, D5.DR.Re.E.6, D5.ER.Es.B.4
enable administrators to define and control the hardware and software that can be connected to the corporate environment	Identify	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8, IA-3	A.8.1.1	D1.G.IT.B.1
	Identify	Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1	D1.G.IT.B.1
	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	AU-12, CA-7, CM-8, PE-3, PE-6, PE-20, SI-4		D3.DC.Ev.B.3
enforce software restriction policies relating to what software is	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices, users (and software)	CM-2, IA-3		D3.PC.Im.B.7, D3.PC.Am.B.6

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
allowed to run in the corporate environment	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-6, IR-5, IR-6	A.12.4.1, A.12.4.3	D1.G.SP.B.3, D2.MA.Ma.B.1, D2.MA.Ma.B.2
	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	AU-12, CA-7, CM-8, PE-3, PE-6, PE-20, SI-4		D3.DC.Ev.B.3
	Identify	Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-7, CA-8, RA-5, SI-2, SI-4, SI-5	A.12.6.1, A.18.2.3	D2.TI.Ti.B.2, D1.RM.RA.E.2
	Identify	Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	PM-15, SI-5	A.6.1.4	D2.TI.Ti.B.1
	Respond	Mitigate Vulnerabilities	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	CA-7, RA-5	A.12.6.1	D1.RM.RA.E.1

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	**Cybersecurity Framework Function [2]**	**Cybersecurity Framework Category [2]**	**Cybersecurity Framework Subcategory [2]**	**NIST 800-53 [3]**	**IEC/ISO27001 [10]**	**FFIEC CAT**
record and track the prescribed attributes of assets	Detect	Security Continuous Monitoring	DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-8, PE-20, SI-4		D3.DC.Ev.B.3
audit and monitor changes in the asset's state and connection	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	AU-12, CA-7, CM-8, PE-20, SI-4		D3.DC.Ev.B.3
	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-6, IR-5, IR-6, SI-4	A.12.4.1, A.12.4.3	D1.G.SP.B.3, D2.MA.Ma.B.1, D2.MA.Ma.B.2
integrate with log analysis tools to collect and store audited information	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-6, IR-5, IR-6, SI-4	A.12.4.1, A.12.4.3	D1.G.SP.B.3, D2.MA.Ma.B.1, D2.MA.Ma.B.2

	Cybersecurity Standards and Best Practices					Financial Sector Best Practices
Security Characteristics	Cybersecurity Framework Function [2]	Cybersecurity Framework Category [2]	Cybersecurity Framework Subcategory [2]	NIST 800-53 [3]	IEC/ISO27001 [10]	FFIEC CAT
does not introduce new attack vectors into existing systems	Detect	Security Continuous Monitoring	DE.CM-8: Vulnerability scans are performed	RA-5	12.6.1	D3.DC.Th.E.5

4.6 Technologies

Table 4-2 lists all of the technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. The Architecture Location column refers to Figure 5-4, ITAM Build.

Table 4-2 Products and Technologies

Company	Product	Version	Architecture Location	Use	CSF Subcategory	NIST 800-53 rev4 Controls
AlphaPoint Technology	AssetCentral	2.1.1 Build 1157	Physical Asset Mgmt.	Stores and displays information on all physical assets in a data center.	ID.AM-1	CM-8
RedJack	Fathom	1.8.0	DMZ	Collects and analyzes NetFlow data and unencrypted banner information from network traffic to detect machines and anomalies.	DE.CM-1	AU-12, CA7, SC-7, SI-4

Company	Product	Version	Architecture Location	Use	CSF Subcategory	NIST 800-53 rev4 Controls
N/A (open source)	Bro	2.3.2	DMZ	Monitors the network and reports on all connections. Also analyzes known bad IP addresses and misconfigured network settings.	DE.CM-1	AU-12, CA-7, SC-7, SI-4
N/A (open source)	Snort	2.9.6.0	DMZ	Examines network traffic and generates alerts based on signatures of known security issues.	DE.CM-1	AU-12, CA-7, SC-7, SI-4
Belarc	BelManage	8.1.31	Network Security	Collects information on the operating system and installed software.	ID.AM-1	CM-8
					ID.AM-2	CM-8
					DE.CM-7	AU-12, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
Belarc	BelManage Analytics	N/A	Network Security	Provides query capability and automated analytics for BelManage data.	DE.CM-7	AU-12, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
PuppetLabs	Puppet	8.3	IT Systems	Provides configuration management, enforcement and validation.	RS.MI-2	IR-4
					ID.AM-2	CM-8

Company	Product	Version	Architecture Location	Use	CSF Subcategory	NIST 800-53 rev4 Controls
N/A (open source)	OpenVAS	4.0.1	Network Security	Scans machines for known vulnerabilities.	DE.CM-8	RA-5
					ID.RA-1	CA-7, CA-8, RA-5, SI-2, SI-4, SI-5
					ID.RA-2	PM-15, PM-16, SI-5
Splunk	Splunk Enterprise	6.2	ITAM	Collects, stores and analyzes the IT asset data.	ID.AM-1	CM-8
					ID.AM-2	CM-8
					DE.AE-3	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
Microsoft	WSUS	6.3.9600.17477	DMZ	Provides patches and updates to Microsoft Windows machines.	RS.MI-2	IR-4
Ubuntu	Apt-Cache	Apt 1.0.1ubuntu2	DMZ	Provides patches and updates to Ubuntu Linux machines.	RS:MI-2	IR-4
CA Technologies	ITAM		Physical Asset Mgmt.	Provides physical asset management.	ID.AM-1	CM-8
Tyco	iStar Edge		Physical Security	Provides physical access management.	PR.AC-1	AC-2, IA Family
N/A (open source)	Openswan	U2.6.38	DMZ	Provides secure access and transport to the off-site mainframe computer.	PR.DS-2	SC-3

Company	Product	Version	Architecture Location	Use	CSF Subcategory	NIST 800-53 rev4 Controls
N/A (open source)	pfSense	2.2.2	All (6 instances)	Provides routing and network segregation between all network segments.	PR.AC-5	AC-4, SC-7
Vanguard Integrity Professionals	Security Manager	N/A	External	Provides security alert information from mainframe assets	ID.AM-1, ID.AM-2	CM-8
Microsoft	Server 2012R2 Certificate Authority	Server2012R2	IT Systems	Provide certificates and PKI management.	PR.AC-1: Identities and credentials are managed.	AC-2, IA Family

5 Architecture

5.1 Reference Architecture Description

ITAM refers to a set of policies and procedures that an organization uses to track, audit, and monitor the state of its IT assets, and maintain system configurations. These assets include "… computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards)" [11]. The cybersecurity value of ITAM is derived from some key aspects of the Risk Management Framework [12] and the NIST Framework for Improving Critical Infrastructure Cybersecurity [2], including:

- selection and application of baseline security controls
- continuous monitoring and reporting of asset status to a data store
- implementation of anomaly detection mechanisms. Examples include deviations from normal network traffic or deviations from established configuration baselines
- provision of context to detected anomalies and cybersecurity events within the reporting and analytic engine

Implementing the first two elements above addresses the Select, Implement, and Monitor aspects of the Risk Management Framework by providing a method to select a baseline, implement it (both configuration and enforcement), and detect changes in the baseline. ITAM addresses the Identify, Protect, Detect, and Respond aspects of the NIST Framework for Improving Critical Infrastructure Cybersecurity [2] by implementing the last two bullets, which identify anomalies and add context to events, aiding in remediation.

The ITAM processes supported by our reference architecture include data collection, data storage, configuration management, policy enforcement, data analytics, and reporting/visualization. The reference architecture is depicted in Figure 5-1.

Figure 5-1 Reference Architecture

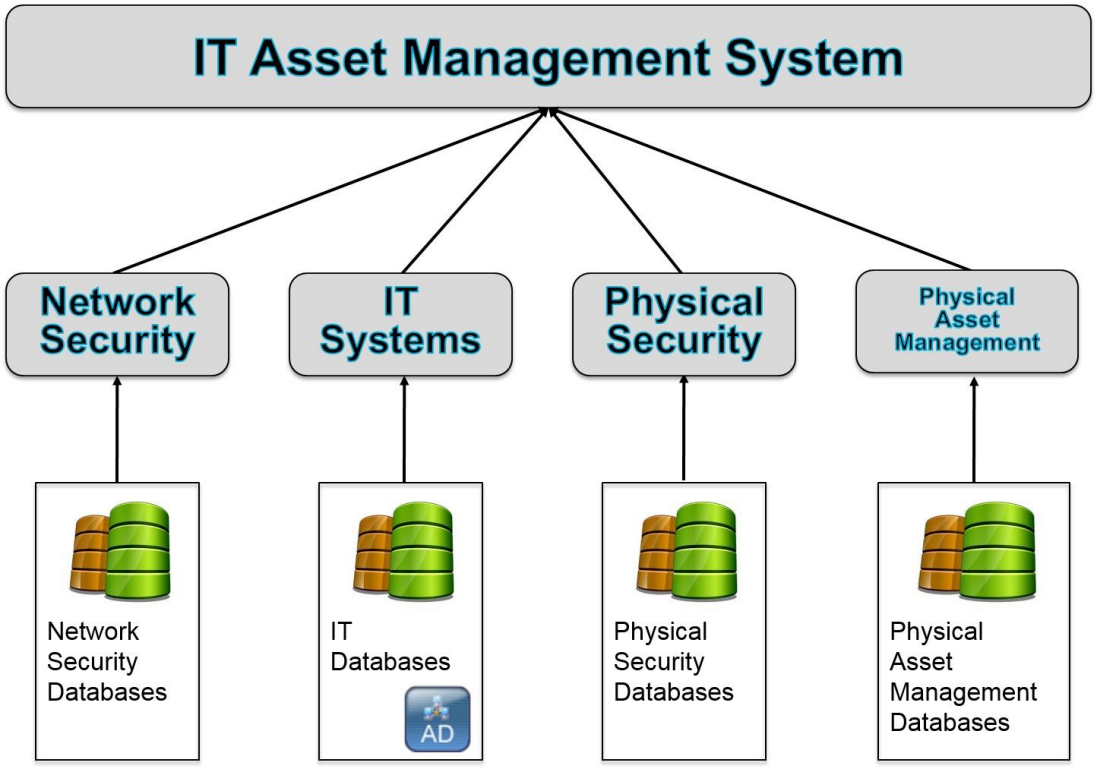
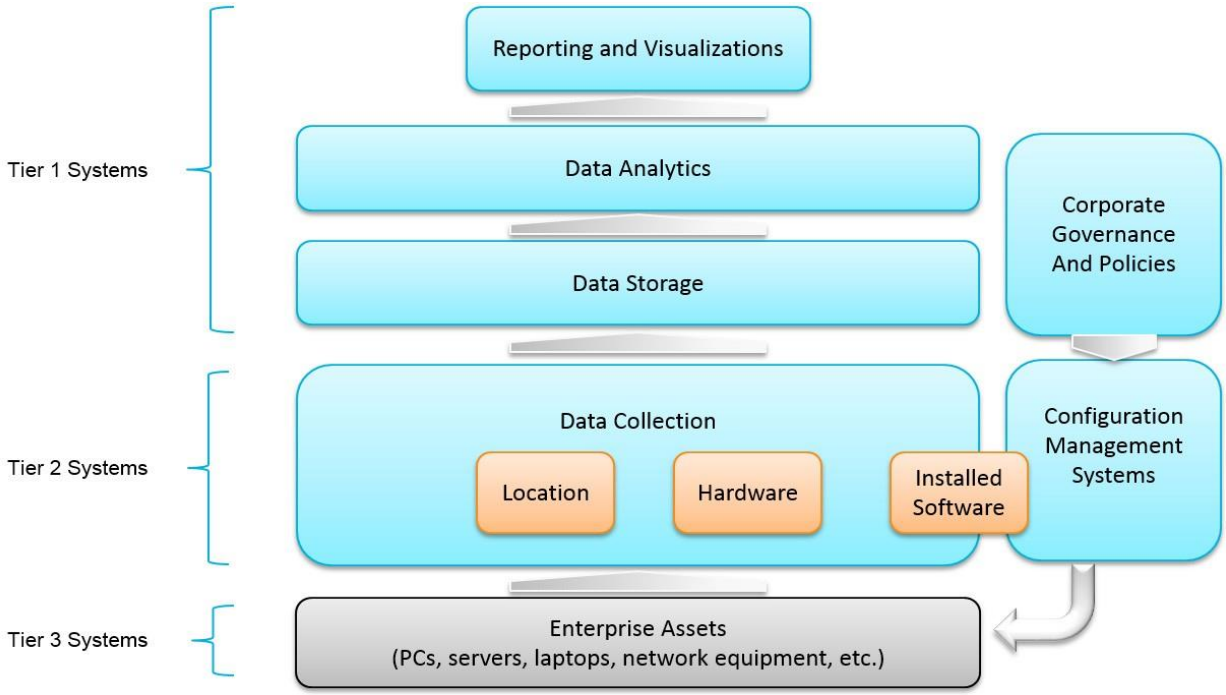


Figure 5-2, ITAM Reference Functionality, shows how data flows through the ITAM system. Tier 3 is composed of enterprise assets themselves. Tier 3 is made up of all of the assets being tracked including hardware, software, and virtual machines. Tier 2 includes the sensors and independent systems that feed data into the enterprise ITAM system. Tier 2 systems include passive and active collection sensor and agents. Tier 1 is the enterprise ITAM system that provides the aggregation of data from all Tier 2 systems into business and security intelligence.

Figure 5-2 ITAM Reference Functionality



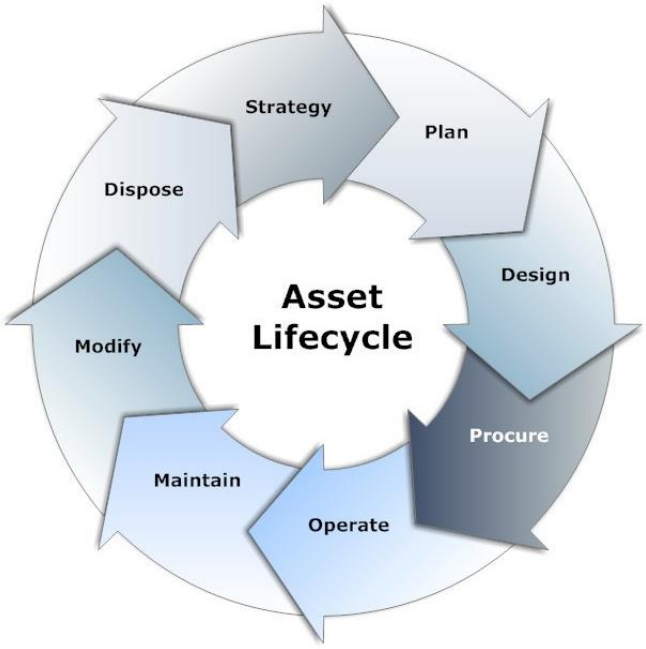
The following capabilities are demonstrated in the ITAM build (see Figure 5-2, ITAM Reference Functionality):

- **Data Collection** is the capability to enumerate and report the unique software and system configuration of each asset and transfer that information to the Data Storage capability.
- **Data Storage** is the capability that receives data from the data collection capability, re-formats as needed, and stores the data in a storage system.
- **Data Analytics** is the capability that performs analytic functions on the data made available by the Data Storage capability.
- **Corporate Governance and Policies** are all of the rules that are placed upon the IT assets. These rules can include the network/web sites that employees can visit, what software can be installed, and what network services are allowed.
- **Configuration Management Systems** enforce Corporate Governance and Policies through actions such as applying software patches and updates, removing blacklisted software, and automatically updating configurations.
- **Reporting and Visualizations** is the capability that generates human-readable graphical and numerical tables of information provided by the Data Analytics capability.

All six are “run-time” capabilities in that they happen periodically in an automated fashion. After performing the initial configuration and manually entering the asset into the asset database, most tasks are performed automatically. Analysts are required to perform a periodic review of the reports stored in the analytic engine to determine anomalies and perform remediation.

The architecture for this project correlates asset management information with security and event management information in order to provide context to events, intrusions, attacks, and anomalies on the network. It consists of processes and technologies that enable the enrollment, tracking and monitoring of assets throughout the enterprise. Furthermore, it provides processes to detect unenrolled or untrusted assets within the enterprise.

Figure 5-3 Typical Asset Lifecycle [13]



In a typical lifecycle, an asset goes through the enrollment, operation, and end-of-life phases. Enrollment usually involves manual activities performed by IT staff such as assigning and tagging the asset with a serial number and barcode, loading a baseline IT image, assigning the asset to an owner, and, finally, recording the serial number as well as other attributes into a database. The attributes might also include primary location, hardware model, baseline IT image, and owner.

As the asset goes through the operations phase, changes can occur. Such changes could include introduction of new or unauthorized software, the removal of certain critical software, or the removal of the physical asset itself from the enterprise. These changes need to be tracked and recorded. As a

consequence, asset monitoring, anomaly detection, reporting, and policy enforcement are the primary activities in this phase.

The assets within the enterprise are monitored using installed agents that reside on the asset, as well as network-based monitoring systems that scan and capture network traffic. These monitoring systems collect data from and about the assets and send periodic reports to the analytics engine. Each monitoring system sends reports with slightly differing emphasis on aspects of these enterprise assets. Reports are collected regarding installed and licensed software, vulnerabilities, anomalous traffic (i.e. traffic to new sites or drastic changes in the volume of traffic), and policy enforcement status.

As an asset reaches the end of its operational life, it goes through activities within the end-of-life phase that include returning the asset to IT support for data removal and removing the serial number from the registration database and other associated databases. Finally, the asset is prepared for physical removal from the enterprise facility.

The ITAM workflow calls for enrolling the asset once it is received, assigning and recording a serial number, loading a base IT image with a list of approved software, including configuration management agents and asset management agents that start monitoring, and reporting on the assets once enrolled. These software agents collect information previously defined by administrators.

A security and configuration baseline is enforced by configuration management agents, installed software is captured by software asset management agents, and both categories of agents forward reports to their respective servers, which serve as data storage facilities. The servers format the data in a suitable form prior to forwarding these periodic reports to the analytics engine. With the visualization capability of the analytics engine, an analyst or manager can retrieve a visual report with the appropriate level of specificity. Changes that affect the asset attributes are captured in these reports sent to the analytics engine. While the ITAM system does provide some automated anomaly detection, analysts should periodically review reports to determine anomalies or relevant changes that may have occurred. Views with specific information about the assets are defined within the analytics engine, enabling analysts to detect policy violations or anomalies that could warrant further investigation. Alerts from other security information sources are also triggers for more detailed investigations by an analyst.

Detection of policy violations triggers policy enforcement or remediation if a relevant and negative alert was detected. These alerts could include, but are not limited to, newly discovered vulnerabilities or the discovery of blacklisted software. The configuration management facility would be used to enforce the removal of such software or the patching of the vulnerability on any number of hosts, bringing the enterprise into a more compliant state as defined by enterprise policy.

5.2 Reference Architecture Relationship

This ITAM project presents the following four scenarios:

1. A new laptop is purchased: the ITAM system will track the laptop from arrival, through configuration, and to its new owner. The laptop will continue to be monitored during its lifecycle.
2. A server is transferred from one department to another. The ITAM system is used to update the physical asset system and the server itself.
3. A virtual machine migrates between physical servers. The ITAM system is notified of all migrations and can alert if a policy violation occurs.
4. Incident detection, response, and prevention: If a sensor, such as an intrusion detection system, triggers an alert, the ITAM system should provide additional information on that asset such as configuration, location, and ownership, if possible.

The ITAM system ties into the existing silos of physical assets, physical security, IT systems, and network security to provide a comprehensive view of all assets in the enterprise. This view allows for queries, dashboards, and process automation supporting the four scenarios listed above.

Scenario 1: New devices are entered into the existing physical asset database, which sends a message to the ITAM system, which triggers other messages to be sent (IT support for configuration). When IT support configures the new laptop, that triggers numerous ITAM database updates related to hardware and software configuration. When the configured laptop is delivered to the new owner, a database update is performed recording the new ownership information.

Scenario 2: Scenario 2 is very similar to the first scenario. A machine changes ownership and is reconfigured. In this scenario, a work order is entered to transfer a server from one department to another. This work order finds its way into the ITAM system, which triggers a series of events, messages, and reconfigurations that result in updates to the databases and changes to the software on the server.

Scenario 3: The ITAM system receives a message for each virtual machine migration. These messages are checked against policy to determine if the move is valid or not. If the move is not valid, an alert is raised. These migration messages can also be used to improve performance by detecting machine or configuration issues that cause excess migrations.

Scenario 4: The ITAM system adds context to security alerts from various sensors that are already on the network. For example, if an intrusion detection system triggers an alert such as “Illegal connection 192.168.1.102 -> 8.8.8.8 TCP”, the ITAM system provides all of the system information pertaining to 192.168.1.102 (the internal machine) such as machine name, operating system, configuration, location and owner. This saves the analyst valuable time and allows for more detailed event filters.

5.3 Building an Instance of the Reference Architecture

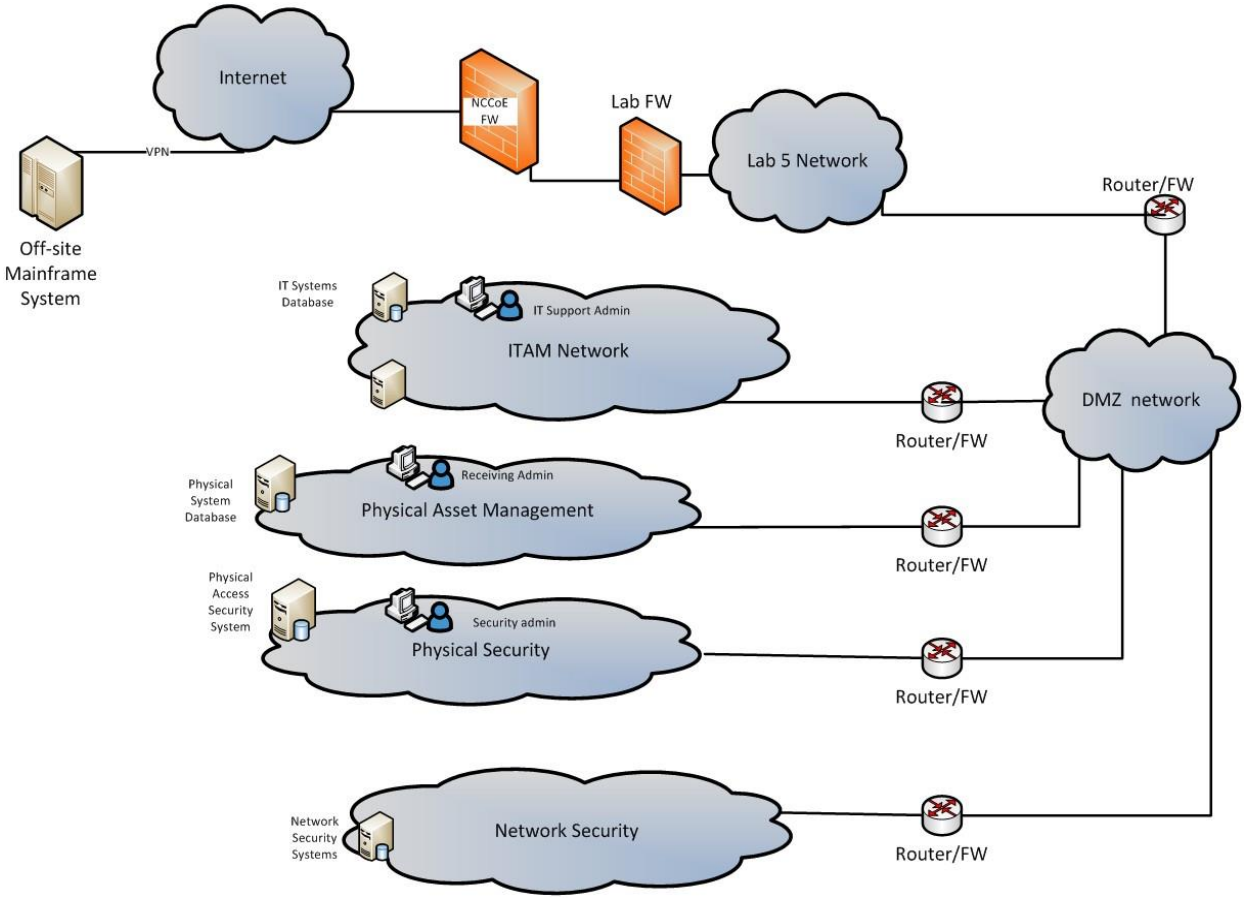
We built one instance of the centralized ITAM capability. This build consists of a DMZ along with network security, IT systems, physical security, and physical asset management silos to implement the workflow and the ITAM system. Each silo has its own router, private subnet, and functionality. Each silo supports aspects of the Risk Management Framework and the NIST Framework for Improving Critical Infrastructure Cybersecurity. Each silo performs data collection, data storage, data analytics, and visualization specific to each silo's purpose. Additionally, each silo integrates into the ITAM system to provide comprehensive reporting and visualizations for the end user.

A detailed list of the components used in the ITAM build can be found in Table 4-2.

5.3.1 ITAM Build

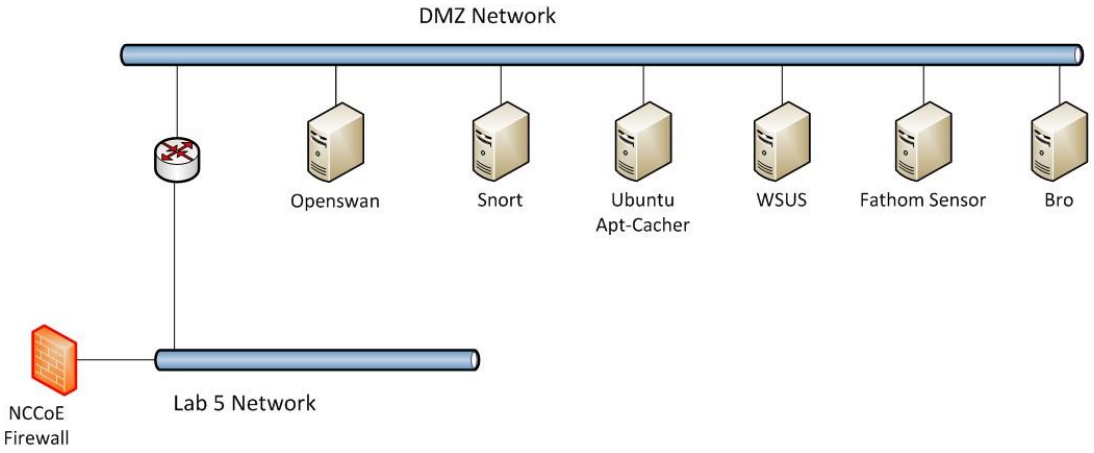
The NCCoE constructed the ITAM build infrastructure using off-the-shelf hardware and software, along with open source tools. While the reference solution was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with existing tools and infrastructure.

Figure 5-4 ITAM Build



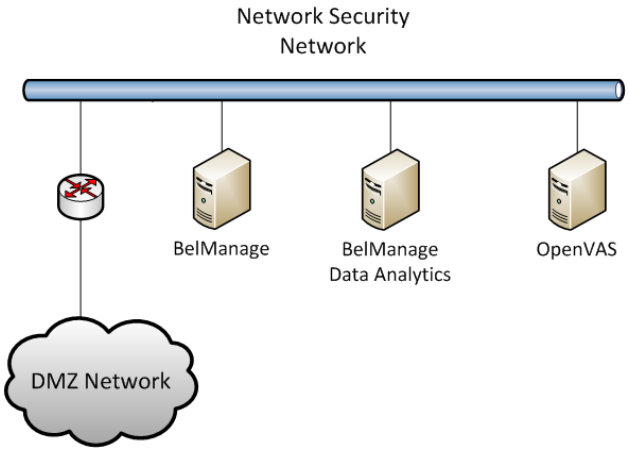
The build architecture consists of multiple networks implemented to mirror the infrastructure of a typical financial services sector corporation. Figure 5-4 illustrates the ITAM build. The build is made up of five subnets that are all connected to a sixth DMZ network. The DMZ network (Figure 5-5) provides technologies that monitor and detect cybersecurity events, conduct patch management, and provide secure access to the mainframe computer. The Physical Asset Management Network (Figure 5-9) provides management of data such as system barcodes, room numbers, and ownership information. Network Security (Figure 5-6) provides vulnerability scanning along with a database for collection and analysis of data from hardware and software components. The IT Systems Network (Figure 5-7) includes systems that provide typical IT services such as email, public key infrastructure (PKI), and directory services. Physical Security (Figure 5-8) consists of management consoles for devices that operate and manage physical security. Such devices consist of badge readers and cameras. Firewalls between each subnet are configured to limit access to and from the networks, blocking all traffic except required inter-network communications.

Figure 5-5 DMZ Network



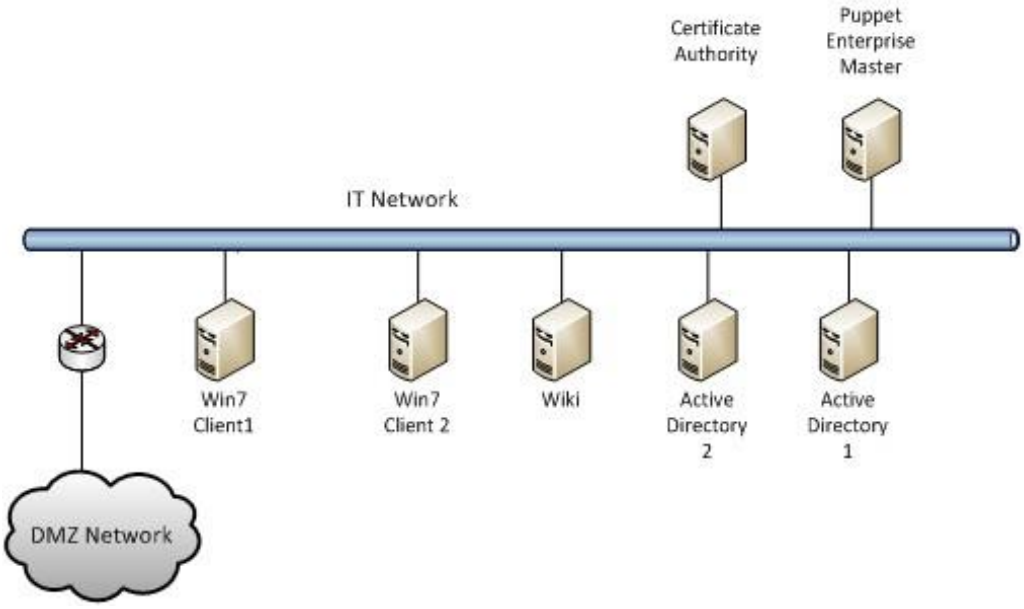
Demilitarized Zone – The DMZ in Figure 5-5 provides a protected neutral network space that the other networks of the production network can use to route traffic to and from the Internet or each other. There is an external and internal facing subnet. The DMZ also provides technologies that monitor and detect cybersecurity events, conduct patch management, and issue secure access to the mainframe computer. DMZ devices consist of Router0, Apt-Cacher, Bro, Fathom Sensor, Snort, and WSUS, as shown in Figure 5-6. Due to network configuration constraints, the network sensors were placed inside of the DMZ instead of in the Network Security subnet (Figure 5-6).

Figure 5-6 Network Security Network



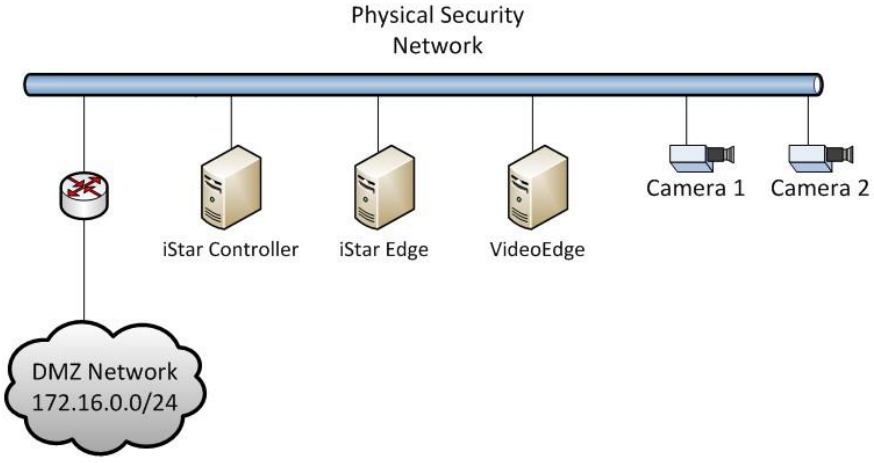
Network Security – The network security architecture is represented in Figure 5-6. Network Security is where all devices pertaining to network security reside. These types of devices include IDS/IPS, SIEM/logging systems and vulnerability scanners. Devices within this network consist of Router2, OpenVAS, BelManage, and BelManage Data Analytics servers.

Figure 5-7 IT Systems Network



IT Systems – The IT Systems network, shown in Figure 5-7, is dedicated to traditional IT systems. Devices included in this particular subnet are Router1, two Windows 7 clients, a wiki, certificate authority, email server, and two Windows 2012 Active Directory servers. One serves as primary while the other serves as a backup. Active Directory1 and Active Directory2 also provide domain name services (DNS).

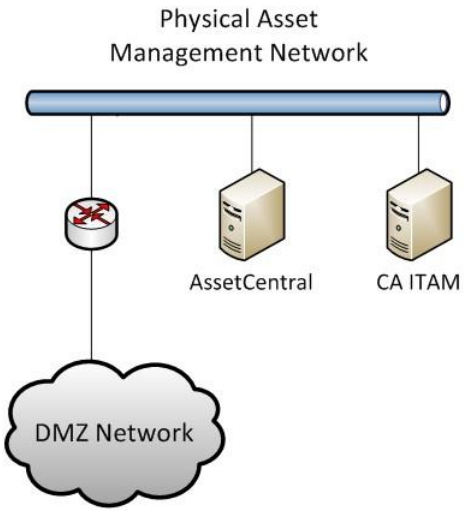
Figure 5-8 Physical Security Network



Physical Security – The Physical Security Network (Figure 5-8) houses the devices that operate and manage physical security such as badge reader and cameras, along with their management consoles. Video Edge is a digital video recorder that records video from Camera1 and Camera2. Both cameras are

in the server room recording anyone who physically accesses the ITAM hardware. iStar Edge is an embedded system that contains two radio frequency identification (RFID) badge readers. The iStar Controller communicates with both the Video Edge and iStar Edge systems. The iStar Controller determines if a valid badge was presented and if that badge should grant access into the server room.

Figure 5-9 Physical Asset Management

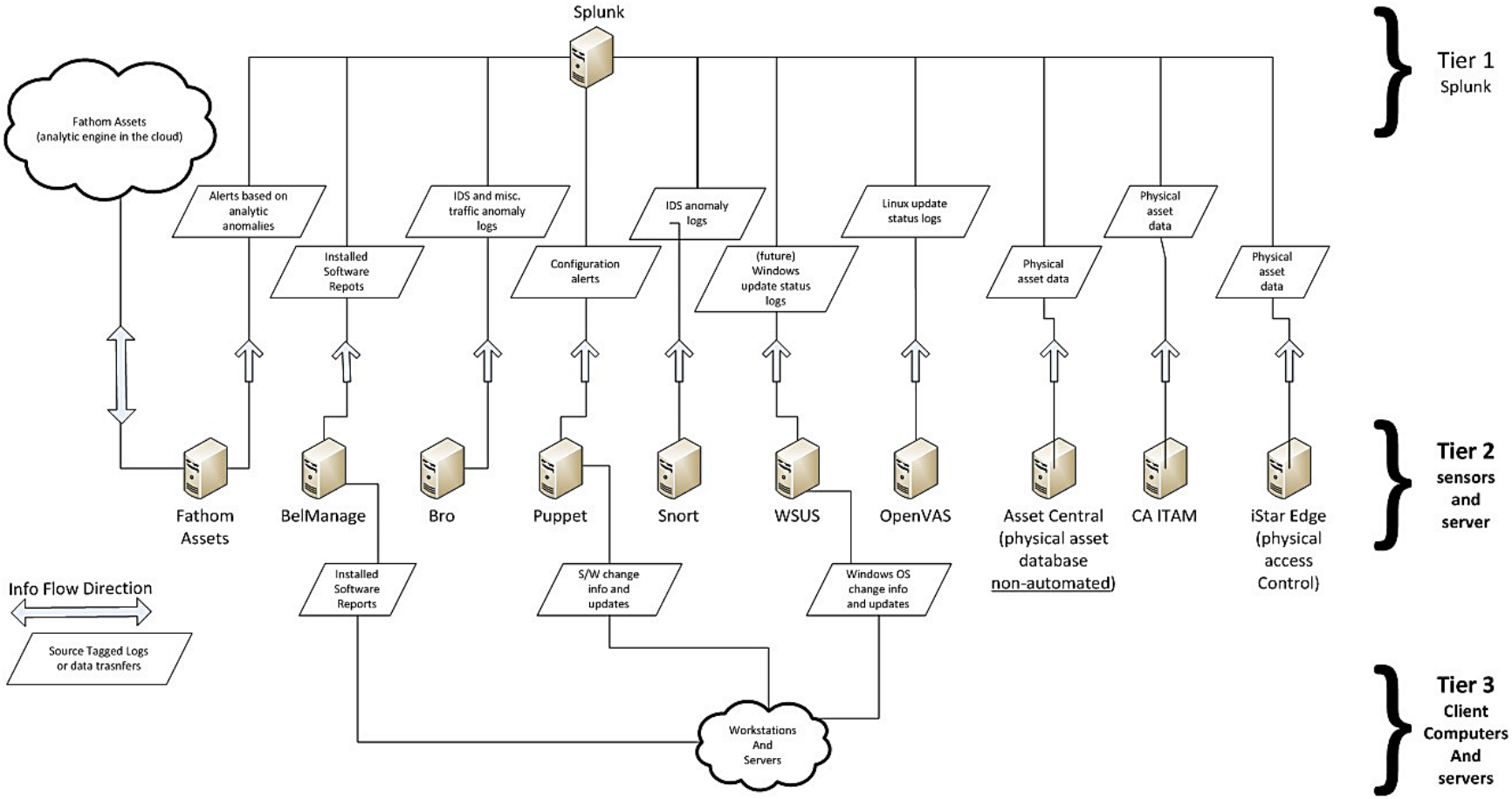


Physical Asset Management – The Physical Asset Management Network (Figure 5-9) contains devices that provide and collect information regarding physical assets. The devices include Router 3 and the data center asset management system, or AssetCentral. AssetCentral is a physical asset inventory and analysis system from AlphaPoint Technology. This tool allows users to view assets from multiple viewpoints including building, room, floor, rack, project, collection, or owner. CA ITAM is running IT Asset Management software from CA Technologies. The CA ITAM system records both new IT assets and ownership changes to IT assets.

5.3.2 Access Authorization Information Flow and Control Points

The ITAM solution deploys sensors throughout the enterprise that collect data from, or about, enterprise assets. The sensors can be installed on the assets, collecting data about installed software, or they can be remote devices that monitor and scan the network, reporting on vulnerabilities, anomalies, and intrusions. These sensors forward collected data to middle tier services that are responsible for storing, formatting, filtering, and forwarding the data to the analysis engine. Further analysis of the data is performed on the analysis engine and involves running select queries to retrieve defined data using a visualization tool also installed on the analysis engine.

Figure 5-10 ITAM Data Flow



5.3.3 Tier 1 Systems

Tier 1 systems collect, store, and analyze the data that they receive from the Tier 2 systems. They allow users to analyze the data and to visualize it for further analysis.

5.3.3.1 Splunk Enterprise

Splunk Enterprise serves as an operational intelligence platform that collects, stores, and analyzes the data from IT assets. The Splunk Enterprise services are responsible for the indexing, analysis, and visualization of the data. All filtered and formatted data makes its way, eventually, to the Splunk Enterprise system. Additional information can be found at http://www.splunk.com/.

5.3.4 Tier 2 Systems

Tier 2 is composed of systems that each perform a unique task. Each Tier 2 system is fully capable of collecting, storing, and analyzing data pertaining to its unique task. The middle tier systems filter relevant and desired data from the raw data collected and forward this data to the analysis engine and visualization tool for further analysis.

5.3.4.1 Fathom

Fathom Sensor passively monitors, captures, and optionally forwards summarized network traffic to its service running on the Amazon AWScloud. The Fathom service periodically compares the network traffic in the ITAM build to an aggregate of the network traffic from several other organizations to determine if abnormal activity has occurred. If abnormal activity is detected, Fathom Sensor will capture the type of activity and forward this information to Splunk Enterprise for further analysis. Additional information can be found at http://www.redjack.com/.

5.3.4.2 Bro

Bro monitors all network traffic in the enterprise and is configured to detect policy violations. It uses AlienVault, Mandiant and TOR threat intelligence data feeds to detect traffic to or from known bad sites. Alerts and messages from Bro are forwarded to the analysis engine and visualization tool. Network traffic information such as connections, DNS traffic, HTTP traffic, and SSL certificates are also forwarded to Splunk Enterprise. Bro messages are, by default, ASCII and tab delimited. Additional information can be found at https://www.bro.org/.

5.3.4.3 Snort

Snort is used to detect intrusions by capturing network traffic and comparing it to known signatures. If intrusions are detected, Snort creates alerts and forwards such alerts via CSV format to Splunk Enterprise. Information such as source and destination IP and port addresses, as well as type of

signature match, are included in the updates. Additional information can be found at https://www.snort.org/.

5.3.4.4 OpenVAS

OpenVAS periodically scans enterprise hosts for known vulnerabilities, generates reports based on its findings, and forwards these reports in XML format to Splunk Enterprise. These reports indicate vulnerable systems, applications, and services. Additional information can be found at http://www.openvas.org/.

5.3.4.5 WSUS

Enterprise hosts with Microsoft Windows operating systems are configured to receive updates from WSUS. WSUS detects whether or not the hosts have the latest updates and sends updates to those hosts that are not in compliance. WSUS forwards reports in CSV format with details of compliance to Splunk Enterprise. Additional information can be found at https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx.

5.3.4.6 BelManage

The BelManage server has agents installed on all clients. BelManage agents collect information about the installed software and forward it to the BelManage server, which stores it in its local database. The CSV-formatted reports are retrieved from the database and are sent periodically to Splunk Enterprise. Additional information can be found at http://www.belarc.com/belmanage.html.

5.3.4.7 BelManage Data Analytics

BelManage Data Analytics (BDA) provides an easy way for users to access, query, and create reports based on the data collected and analyzed by BelManage. The ITAM project gathers data from some of the queries for incorporation in overall dashboards. Additional information can be found at http://www.belarc.com/data_analytics.html. The information in BelManage is gathered directly by Splunk Enterprise using an SQL database query.

5.3.4.8 Puppet Enterprise

Puppet Enterprise enforces a configuration baseline on servers and workstations. Puppet agents run periodically, downloading a compiled configuration catalog from the Master and executing it on the hosts. A successful Puppet Enterprise agent run can make configuration changes, install new software or remove unwanted software, and sends success status updates to the Master. The ITAM solution configured the Puppet Enterprise Master to forward an absent or present status for enterprise hosts indicating whether or not they have had successful agent runs. These status messages are forwarded to Splunk Enterprise using the syslog facility. Additional information can be found at https://puppetlabs.com/puppet/puppet-enterprise.

5.3.4.9 Openswan

Openswan is an open-source virtual private network (VPN) for Linux operating systems. Openswan is used in the ITAM project for connecting the lab at the NCCoE to a facility in Nevada run by Vanguard Integrity Professionals, where the mainframe computer is located. Openswan is configured to provide a site-to-site VPN using IPsec. Additional information can be found at https://www.openswan.org/.

5.3.4.10 Ubuntu Apt-Cacher0

Ubuntu Apt-Cacher0 is an Ubuntu Linux server that provides package caching services for the ITAM lab. All of the Ubuntu devices on the network receive their software, patches, and updates from Ubuntu Apt-Cacher0. This centralizes update management, reduces the number of machines accessing the Internet, and reduces Internet bandwidth usage. Additional information can be found at https://help.ubuntu.com/community/Apt-Cacher-Server.

5.3.4.11 AssetCentral

AssetCentral is a Web-based IT asset management and data center management solution. Information on all physical IT assets used in the ITAM project was entered into AssetCentral. This information includes make, model, serial number, barcode, room, rack, and owner. This information is then used to provide a complete picture of the state of an asset. Splunk Enterprise utilizes a direct SQL database query to gather information from AssetCentral.

5.3.4.12 CA Technologies IT Asset Manager

CA Technologies IT Asset Manager provides asset management lifecycle support. This project uses CA ITAM for asset-based workflow management. For example, when a new asset arrives, it is entered into the CA ITAM product, which then tracks its provisioning and delivery. Splunk Enterprise utilizes a direct SQL database query to gather information from CA ITAM. Additional information can be found at http://www.ca.com/us/intellicenter/ca-it-asset-manager.aspx.

5.3.4.13 iStar/C-Cure Controller

The C-Cure controller from Software House provides badging and access controls for the physical security silo of this project. The C-Cure controller is part of the physical security system from Tyco Security Products that we used. The C-Cure Controller interacts with the iStar Edge and VideoEdge systems to provide an overall physical security solution. Access request information is exported from the iStar/C-Cure controller in .CSV format for use by Splunk Enterprise. Additional information can be found at http://www.swhouse.com/products/CCURE_ID_Badging.aspx.

5.3.4.14 VideoEdge

VideoEdge is a network video recorder that records video from Camera1 and Camera2. VideoEdge is part of the physical security system from Tyco Security Products used in this project. Additional information can be found at http://www.americandynamics.net/products/videoedge_nvr.aspx.

5.3.5 Tier 3 Systems

Tier 3 systems are the assets (end points) on the enterprise network that are owned by the enterprise, such as workstations, switches, servers, users' laptops, virtual machines, and other devices. All enterprise assets are monitored from the start of their lifecycle until disposal by the systems in the Tier 2. Device location, owner, installed software catalog, current security vulnerabilities, and abnormal traffic activity are captured to allow for better visibility by administrators.

5.3.5.1 AD1

Active Directory (AD) is a special-purpose database that holds objects and attributes related to users, contacts, groups, computers, and organizational units. AD is used for authentication, authorization, and auditing of users and computers. Additionally, AD1 provides domain name services (DNS) to the entire lab network. The AD machines used for this project are run on top of the Microsoft Windows 2012R2 64-bit operating system. Additional information can be found at https://msdn.microsoft.com/en-us/library/Aa746492%28v=VS.85%29.aspx.

5.3.5.2 AD2

AD2 is a replica of AD1. The two systems provide redundancy and fault tolerance.

5.3.5.3 Certificate Authority

The Certificate Authority (CA) provides PKI capabilities to the lab. The CA creates and signs X.509 cryptographic certificates for users and computers that are used throughout the lab. This project utilizes the CA that is part of the Microsoft Windows 2012R2 64-bit operating system. Additional information can be found at https://technet.microsoft.com/en-us/library/cc770357%28v=ws.10%29.aspx.

5.3.5.4 Email Server

The ITAM project utilizes the Postfix email server. The email server is used to collect messages, both status and informational, as well as for workflow management. Additional information can be found at http://www.postfix.org/.

5.3.5.5 Ubuntu-Client1

Ubuntu-Client1 functions as a representative Linux client for the ITAM lab. Ubuntu-Client1 is configured as a full desktop load with a graphical operating system. The purpose of Ubuntu-Client1 is to show that the various ITAM functions, such as hardware and software monitoring, function correctly on a Linux system. Additional information can be found at http://www.ubuntu.com/.

5.3.5.6 Win7-Client1

Win7-Client1 functions as a representative Microsoft Windows client for the ITAM lab. Win7-Client1 includes the full Microsoft Windows 7 desktop installation along with additional software such as Firefox, Google Chrome, and WinSCP. Win7-Client1 is a member of the lab5.nccoe.gov domain. The purpose of Win7-Client1 is to show that the various ITAM functions, such as hardware and software monitoring, function correctly on a Windows system.

5.3.5.7 Win7-Client2

Win7-Client2 performs the same functions as Win7-Client1. The purpose of Win7-Client2 is to provide additional data points for the ITAM system.

5.3.5.8 Mainframe

The mainframe computer provided by Vanguard Integrity Professionals and running their security, compliance, and configuration management software provides the ITAM system with information regarding the state of the mainframe. State information includes configuration, usage, and compliance information. The mainframe computer is physically located at Vanguard and accessed via VPN. You can find additional information at https://www.go2vanguard.com/.

5.3.5.9 iStar Edge

The iStar Edge is a door controller that is accessed over Internet Protocol (IP)-based networks. iStar controls access to two doors by using its RFID badge readers. The iStar Edge is controlled via the iStar Controller. The iStar system provides the ITAM system with information on human assets that are entering sensitive server rooms. The iStar Edge controller is part of the physical security system from Tyco Security Products used in this project. The iStar Edge is part of the physical security silo of the ITAM system. Additional information can be found at http://www.swhouse.com/products/hardware_iSTAR_Edge.aspx.

5.3.5.10 Camera1

Camera1 is an Illustra 600 compact mini-dome IP camera that is part of the physical security silo of the ITAM system. Camera1 is part of the physical security system from Tyco Security Products. Camera1 sends its images to the VideoEdge network video recorder. Additional information can be found at http://www.americandynamics.net/products/illustra-minidomes.aspx.

5.3.5.11 Camera2

Camera2 is same as Camera1 but is pointed in a different direction to capture different images.

5.3.5.12 Routers/Firewalls

The ITAM lab uses six routers/firewalls to route, segment, and filter traffic inside of the ITAM network. All of the routers/firewalls are virtual machines running the community version of pfSense. Each network segment has its own router/firewall and each router/firewall has its own unique configuration. Alerts and messages are forwarded to the analysis and visualization system. Additional information can be found at https://www.pfsense.org.

Appendix A List of Acronyms

AD	Active Directory
CA	CA Technologies
CA	Certificate Authority
COTS	Commercial Off-The-Shelf
CRADA	Collaborative Research and Development Agreement
CSF	NIST Framework for Improving Critical Infrastructure Cybersecurity
.csv	Comma-Separated Value
DMZ	Demilitarized Zone
FS	Financial Sector
HR	Human Resources
ID	Identity
ITAM	Information Technology Asset Management
IDS	Intrusion Detection System
IP	Internet Protocol
NAS	Network Attached Storage
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PKI	Public Key Infrastructure
SME	Subject Matter Expert
SQL	Structured Query Language
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guideline
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Appendix B References

[1] *CIS Critical Security Controls*, SANS Institute [Website], https://www.sans.org/critical-security-controls/ [accessed 08/07/18].

[2] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, Gaithersburg, Maryland, April 16, 2018. http://www.nist.gov/cyberframework/ [accessed 08/07/18].

[3] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 08/07/18].

[4] *Security Technical Implementation Guides (STIGs)*, Defense Information Systems Agency [Website], http://iase.disa.mil/stigs/Pages/index.aspx [accessed 08/07/18].

[5] International Organization for Standardization/International Electrotechnical Commission, *Information Technology – Security techniques – Code of practice for information security controls*, ISO/IEC 27002, 2013. http://www.iso.org/iso/catalogue_detail?csnumber=54533 [accessed 08/07/18].

[6] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 08/07/18].

[7] *Risk Management Framework: Quick Start Guides*, National Institute of Standards and Technology [Website], http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/ [accessed 08/07/18].

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf [accessed 08/07/18].

[9] *IT Asset Management: Securing Assets for the Financial Services Sector*, Version 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 1, 2014, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/fs-itam-project-description-final.pdf [accessed 08/07/18].

[10] International Organization for Standardization/International Electrotechnical Commission, *Information technology — Security techniques — Information security management systems — Requirements*, IEC/ISO 27001, 2013. http://www.iso.org/iso/iso27001. [accessed 08/07/18].

[11] J. Wunder, A. Halbardier, and D. Waltermire, *Specification for Asset Identification*, NISTIR 7693 Version 1.1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7693.pdf [accessed 08/07/18].

[12] *Risk Management Framework (RMF) Overview*, National Institute of Standards and Technology [Website], http://csrc.nist.gov/groups/SMA/fisma/framework.html [accessed 08/07/18].

[13] http://wc1.smartdraw.com/cmsstorage/exampleimages/44b341d1-a502-465f-854a-4e68b8e4bf75.png [accessed 08/07/18].