NISTIR 8428

Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)

Eran Salfati
Michael Pease

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8428

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NISTIR 8428

Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)

Eran Salfati
Michael Pease
Smart Connected Systems Division
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8428

June 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8428
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8428, 61 pages (June 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8428

Abstract

This document provides a new Digital Forensics and Incident Response (DFIR) framework dedicated to Operational Technology. This framework expands the traditional technical steps of IT Incident Response by giving an Incident Response procedure based on event escalation and provides techniques for OT Digital Forensics. The document begins with an overview of OT DFIR while discussing DFIR terms in general and explaining the unique properties of DFIR in OT. Later, the document describes the needed preparations for OT DFIR, such as an IRT establishment and Digital Forensics lab tools. Finally, the document provides the suggested OT DFIR framework with a detailed explanation of its phases and steps.

Keywords

Incident Handling; Digital Forensics; Incident Response; Industrial Control Systems; Operational Technology.

Acknowledgments

The author gratefully acknowledges and appreciates the significant contributions of Timothy Zimmerman, and CheeYee Tang from the NIST Communications Technology Laboratory, and Barbara Guttman from the NIST Software and Systems Division. The author would particularly like to acknowledge Keith Stouffer for hosting and supervising this research and contributing to the content of this document.

Table of Contents

List of Figures

1. Introduction

1.1. Preface

Digital Forensics and Incident Response (DFIR) are two common terms in cybersecurity initially developed for Information Technology (IT) systems, based on technical steps including preparation, detection, containment, eradication, recovery, and post-incident activity [1]. Each step can be detailed to many technical actions which require high skills to perform.

Operational Technology (OT) describes a family of systems used to manage, monitor, and control industrial operations focusing on the physical devices and processes they use (e.g., electricity, water, pharmaceutical). Implementing DFIR methods for these systems requires a series of dedicated extensions of procedures and techniques due to some unique aspects of OT.

1.1.1. Main Incident Response challenge in OT

Traditional Incident Response steps mainly focus on the technical aspects of the process and not on the procedure that leads the process. This issue is not a problem while dealing with an event in IT environments because, in most cases, the IT system is under the full responsibility and control of one department, the IT department. However, this is not the case in OT [2]. A primary aspect that affects incident handling in OT is the number of stakeholders (e.g., operators, maintenance teams, engineers, cyber analysts) doing some level of analysis in the system. As a result, a lack of clear procedures, lack of coordination, and lack of clear definitions of responsibility and authority can lead to failures when managing a real-time cyber incident.

Moreover, although OT systems are considered reliable, non-cyber incidents such as technical malfunctions or process anomalies are not rare. Therefore, there is always a challenge to balance between edge approaches: On one hand, addressing every technical issue as a standard technical event and providing technical support that can take a long period of time while getting the risk of missing actual cyber events. On the other hand, addressing every technical issue as a potential cyber incident while getting the risk of having many false positives, which will erode the Incident Response Team.

1.1.2. Main Digital Forensic challenge in OT

At a very fundamental meaning, Digital Forensics is about analyzing data with tools and techniques to answer questions such as what happened in the system, how it occurred, and what the impact was. The levels of analysis differ in the types of data and tools, the level of needed skill, and the time invested.

Unique devices and data types in OT require unique knowledge and skills to accomplish Digital Forensics. In addition, OT is a type of system that has a strong connection to the physical world. There is great importance in understanding the possible implications for safety and operation resulting from any forensic-related action performed in the system. Therefore, there must be a strong connection between technical OT personnel and Digital Forensics analysts.

1.2. Purpose and Scope

The purpose of this document is to provide an OT Digital Forensics and Incident Response (DFIR) framework. This framework expands the traditional technical steps by giving an Incident Response procedure based on the event escalation and provides additional techniques for OT Digital Forensics.

The scope of this document includes an overview of DFIR and its implementation within OT environments. Its goal is to provide the whole picture as a starting point for the organizations to establish their own OT DFIR capabilities.

This document will not dive deeply into the bits and bytes or describe specific protocols, logs, or tools instructions. This level of technical details depends on each organization's particular equipment, vendors, and systems. Each organization should use the methods proposed in this document to build its dedicated technical procedures.

1.3. Audience

This document's audience includes OT Incident Handlers, who should be familiar with three main fields: Cybersecurity, OT/Industrial Control System (ICS) engineering, and Digital Forensics. Practically, engineers of this type rarely exist in organizations. That is why OT Incident Handlers must work as part of a team, which may include: Cyber OT Engineers (Engineers who are familiar with both fields: OT/ICS Systems and OT Cybersecurity), Industrial Control Engineers, IT professionals, researchers, analysts, Process Engineers, Safety Engineers, and Managers who are responsible for OT.

1.4. Document Structure

The remainder of this guide is divided into the following major sections:

- Section 2 provides an overview of OT DFIR. It includes an explanation of the general term and a list of unique properties divided into two main categories: properties that affect OT Incident Response and Properties that affect OT Digital Forensic.
- Section 3 discusses the preparation that should be done to establish an OT Incident Response Team. One aspect of this section deals with the Incident Response Team itself, and the other aspect deals with the resources for Digital Forensics.
- Section 4 describes the OT DFIR framework. It starts with a general overview of the process and continues with every step in extended detail.
- Appendix A lists acronyms and abbreviations used in this document.
- Appendix B provides a suggested small-scale organization implementation of the OT DFIR framework.

2. Overview of OT DFIR

The first part of this section will describe three main terms which will be used in this document: Active Defense (AD), Incident Response (IR), and Digital Forensics (DF). The second part of this section will discuss some of the unique properties of OT systems, which base the motivation for the suggested OT DFIR framework in this document. Each paragraph in this section presents the different challenges and opportunities with any unique property and an essential strategy to deal with them.

2.1. DFIR in general

2.1.1. Active Defense

According to the Sliding Scale of Cyber Security, a cybersecurity program is built on five levels [3][4]. The first two levels are *Architecture* and *Passive Defense*. These two levels include all the fundamental design considerations and security controls needed to eliminate most of the low-level and traditional cyber attacks. In comparison to physical defense, these levels are the walls and gates around the property. But walls and gates are not enough. To achieve a satisfactory level of protection against sophisticated adversaries, guardians (or analysts in cybersecurity) must constantly walk around (or analyze the environment) looking for the next attack. In addition, they need to collect intelligence and use their monitoring systems to hunt the adversary before they can gain a foothold. Accordingly, the following two levels in the cybersecurity program are *Active Defense* and *Threat Intelligence*. The last level deals with *Offensive* activity to subdue the adversary while still in his environment. As shown in Fig. 1, the foremost part of the active defense approach related to this document is the *Incident Response*.

Fig. 1. The Sliding Scale of Cyber Security: Active Defense

2.1.2. Incident Response

OT Incident Response is an organized approach to handling and managing the aftereffects of an incident with the primary goal of gathering enough information to contain and recover the system to operate safely. This is sometimes contrary to IT Incident Response which may focus on recovering the system to its pre-incident state immediately rather than examining every piece of forensic data.

NIST SP 800-61 [1] provides guidance for establishing and operating an IT Incident Response process in organizations. Although initially designed for IT environments, it can be adopted for OT systems with some adjustments. The general process includes preparation activities needed to be done before an incident occurs, a set of activities during an incident handling (detection & analysis, containment, eradication & recovery), and post-incident activities.

2.1.3. Digital Forensics

Digital Forensics is a subset of forensic science. It is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data [5]. Digital forensic techniques can be used for many purposes, such as investigating crimes and internal policy violations, reconstructing security incidents, troubleshooting operational problems, and recovering from accidental system damage. This guide presents Digital Forensics from a system point of view, not a law enforcement view.

Digital Forensics is both a field of science and a field of art. It has no deterministic technical procedure to provide a step-by-step guide that will lead the analyst directly to the answer. A lot of training and practice are needed to reach a proficient skill level. Therefore, the goal of this document is to provide the fundamental tools and techniques that will help to build specific OT Digital Forensics capabilities, while a high level of skill can be achieved after continued practice and training.

NIST SP 800-86 [6] is a guide for integrating Forensic Techniques into an Incident Response process. It includes four main phases:

- **Collection** – Relevant data is identified, labeled, recorded, and collected.
- **Examination** – Forensic tools and techniques are applied to identify and extract the relevant information from the collected data.
- **Analysis** – Information is analyzed to achieve the proof that will explain the incident's root cause.
- **Reporting** – Summarize the results and further recommendations.

2.2. OT DFIR Unique Properties

2.2.1. Properties that affect OT Incident Response

2.2.1.1. Analysis levels during Incident Response

The primary property that affects the Incident Response process in OT is the number of stakeholders performing some level of analysis in the system. During normal operations, operators use sensors and actuators to perform process measurement and control. In addition, Security Operation Center (SOC) analysts are examining alerts and anomalies in the network and other IT components.

During a technical event, the maintenance teams perform a technical inspection to identify and solve mechanical (such as valve mechanism or pump transmission failure) and electrical malfunctions (such as valve actuator or pump motor failure). In addition, the control system engineers perform software analysis to provide technical support.

During a cyber incident, the Incident Response Team uses response methods and Digital Forensics to understand and resolve the incident. An after-event team can perform deep forensics (such as malware reverse engineering) to understand the incident.

The basic principles of these teams are similar. They all use data, tools, and skills to understand an issue in the system and respond correspondingly. The main differences are how much resources and attention each team invests during the Incident Response.

This property raises a major challenge in OT Incident Response. Any lack of clear procedure, lack of coordination, and clear definitions of responsibility and authority can lead to failures when managing a real-time cyber incident. One of the primary goals of the OT DFIR framework in this document is to address that challenge.

It should be mentioned that in small-scale organizations, that may not be a major problem. Usually, the problem of small organizations is the opposite. Lack of manpower and staff having multiple roles (i.e., being both on the engineering team and the Incident Response Team). Appendix B suggested a small-scale organization implementation for the framework.

2.2.1.2. Is it a Malfunction or an Attack?

Technical malfunctions and process anomalies may occur more frequently than cyber incidents in OT systems. While cyber incidents are rare, they will usually start with similar symptoms. There are two edge strategies to deal with these malfunctions. One option is to address any technical issue as a potential cyber incident. On the one hand, this approach will ensure that no case is missed, but on the other hand, the Response Team may be desensitized due to many false positives and alert fatigue.

Another option is to provide regular technical support with zero cyber considerations. In this way, the Response Team will only be activated during complex events, but on the other hand, the initial stages of actual cyber events may be missed due to false negatives. The challenge is to balance these two edge strategies. The OT DFIR Framework in this guide suggests a balanced approach.

2.2.1.3. Availability Versus Understanding the Incident

Another challenge during the Incident Response process is the time required to perform an event analysis. While the Incident Response Team would like to have as much time as possible to analyze the data deeply, the system stakeholder's target is to bring the system back to operation as soon as possible. The primary approach to address this challenge involves collecting as much data as possible before the incident occurs, using fast automation capabilities during the event, and then using an offline forensic lab for the investigation.

2.2.2. Properties that affect OT Digital Forensic

2.2.2.1. Knowledge and Skills Needed for the Incident Response Team

Cybersecurity in general and Digital Forensics are large fields of knowledge that require a unique set of skills and tools. The same can also be said for OT and ICS. Therefore, an Incident Response Team member must have the ability to understand both Digital Cyber Forensic techniques together with OT technologies. Additionally, they must understand the impact and consequences on the process and its safety, such as loss of localized or remote control over the process, loss of production, compromise of safety, cascading failures that affect critical infrastructure, environmental damage, injury, loss of human life, and financial loss.

A Digital Forensic team in OT may not get frequent practice due to the limited number of real-world events compared to IT environments. A best practice to address that issue is to incorporate these team members to solve technical events and malfunctions in the OT system and participate in the IT Incident Response Team. Another best practice is to train OT Incident Response members with courses and simulations of cyber incidents periodically.

2.2.2.2. Legacy Versus New Systems

Traditionally, OT systems evolve slowly while using legacy technologies with limited or no adequate forensic data or auditing capability. Moreover, many OT systems are based on undocumented proprietary operating systems and protocols, which are difficult to analyze.

Legacy systems upgrade projects and new systems establishments are good opportunities to introduce technologies, protocols, and architectures that support forensic capability. These forensic capabilities should be included as part of the system design basic requirements. Of course, it is not enough to deploy new components with forensic features solely. The engineers must also configure the system components correctly and design a collection mechanism for the forensic data that does not impact the OT processes.

2.2.2.3. Offline Versus Online Digital Forensic

Offline forensics in a separate lab can decrease time pressure and prevent safety risks to the facility while performing the investigation. But offline forensics also has one significant disadvantage: static data. One primary uniqueness of OT systems versus IT is their strong connection to the real world. Forensics in OT systems is not only about analyzing the network data and the PC's processes. It also requires a good understanding of the industrial control system's components and their relations to the process. It can be hard to understand the behavior of a Programmable Logic Controller (PLC) program and the input/output (IO) signals without examining them in real-time. In that case, if the system is still running, online forensics may be an opportunity to provide significant value under the appropriate safety supervision and risk management.

2.2.2.4. Integrating Forensic data Collection into System Routine

In addition to integrating forensic capabilities into the system design, forensic data collection should be a part of the system routine for two main reasons. First, forensic data that was not collected during routine operations would not be available when an event occurs. Second, some sophisticated malwares may be aware that forensic data is being collected and can reduce their activity.

OT systems, especially ICS, are built on three main types of components: PLCs and industrial equipment, workstations and servers, and network components. All of these components can hold valuable digital data that can be used for baseline snapshots and Digital Forensics. Workstations, servers, and network components are similar to the same elements in the IT environment. The difference is more about the data content. The OT protocols, applications, and logs can be very different from the IT and less suitable for data collection. Much more challenging is collecting data from the core ICS components like PLCs and industrial equipment.

Ideally, the baseline should include periodic snapshots of data from all the system sources. However, this can raise many dilemmas. For example, what data can be collected remotely from an external monitoring center, and what must be collected locally at the device? What can be collected automatically, and what must be collected manually? How much data should be saved, and how much storage is required? How often should baseline snapshots be taken, and for how long should they be kept? How can the data be secured while flowing from the device to the monitoring center and verify its integrity? How can the data be used during an Incident Response? The organization needs a strategy and capability to address all these questions and more. Answers and strategies for these questions are provided in Section 4.

3. OT DFIR Preparation

This section will discuss some of the preparation that should be done before an incident occurs. The section is focused on three main topics. First is the Incident Response Team's structure, tools, facilities, and training. The second is the Digital Forensic hardware and software tools and resources. And the third is the OT field systems preparations for forensics.

3.1. Incident Response Team

3.1.1. Roles and Responsibilities

An Incident Response Team (IRT) can be a dedicated team that handles incidents as a full-time job. In most cases, this team is based on existing personnel defined and overseen by the management to be IRT members when needed, in addition to their day-to-day job.

As described above, many groups should be involved in the Incident Response process in OT systems. Here are some of the prominent roles that should be included in the team. Notice that it is a Role-Based list and not a Human Resource one. In a small organization, part of these roles could be applied by the same personnel or outsourcing.

- **Cyber OT Engineers** – Engineers familiar with both fields: OT/ICS Systems and OT Cybersecurity. This group should consist of three types of roles in a hierarchical order:
    - **Team Leader** – Responsible for establishing and maintaining the team and interfaces with management and POCs at other organizations.
    - **Incident Leader** – Coordinates all handlers, guides personnel, focuses the efforts, timeline the evens, maintains situational awareness, etc.
    - **Data Handler** – Responsible for digital data collection, performing timely analysis, containing and cleaning the infected systems, inform the leader. These members should have strong communication skills, work well in a team and under high stress, have patience, work by the plan, and ask for help when needed.
- **SOC Analysts** – Security Operation Center Analysts routinely monitor the IT and OT environments. This group is familiar with the system's baseline and should analyze the data and alerts from the monitoring systems.
- **Control System Engineers** – Experts in control systems development who also serve as a Technical Support Team. This group is most familiar with the PLC and HMI codes of the specific systems and should help with explaining the expected system behavior.
- **Process Operators** – The Facility Control Room operators are most familiar with the process behavior. Together with the Control System Engineers, the control system can be well understood.
- **Facility Maintenance Team** – This local Facility Maintenance Team daily deals with mechanical and electrical malfunctions in the system and can be beneficial during an investigation.

- **IT Security** – Technology personnel within the IT security department should help with the event investigation and interpret regulatory requirements.
- **Physical Security** – Physical security staff can assist in gaining access to locations and physically securing forensic data and the area.
- **IT Professional** – Usually, this group is not in charge of the OT systems but can help with their networking and operation systems knowledge.
- **Management** – During an OT Digital Forensics process, it is essential to have management representatives be involved and informed.
- **Other Internal or External third-parties** – There might be a need to rely on Internal or External third parties to help with unique activities such as data recovery from damaged media, Legal advisors, Policy, Private aspects, etc.

3.1.2. Tool Kit

Here are some recommendations for additional tools (not a list of software collection and analysis tools) to include in an IR jump kit:

- **Safety –**
  - Personal protection equipment such as hard hats.
  - Out-of-band communication methods.
- **IR Workstations –**
  - A laptop with imaging/data collection tools.
  - Approved scripts and software for timely analysis.
- **Network tools** –
  - Hub or tap that can support the expected bandwidth.
  - Physical-layer converters.
- **Storage –**
  - A few high-volume Hard Drives to store digital images and network traffic.
  - Blank CDs and USB Drives.
- **Auxiliaries –**
  - Cables/Connectors (USB, Serial, SATA, etc.)
  - Digital camera for scene photography.
  - Screwdrivers, power strips, flashlights.
  - Notebooks and labels.
  - Procedure checklists.
- **Digital Forensic Data list –**
  - Fundamental data types (Section 4.2.1, Step A.2).
  - Supplementary data types (Section 4.2.4, Step D.4).

3.1.3. Situation Room

- One of the uniqueness of dealing with the OT system is the number of stakeholders in the system. For example, Operators, local support teams, control systems engineers, Incident Response Teams, management, etc. During the incident handling, there is a risk that someone will do some action in the system without informing all the team members. Therefore, everyone must be in sync and up to date throughout the process.

- The Situation Room should be used for situation assessments and should serve only the directly related personnel to the incident. The Situation Room is the place for managing the incident, answering questions from the management, contacting POCs, updating timelines, etc. This is not the place for technical analysis to get done; that would occur in the Digital Forensics Lab.

3.1.4. Training and practice

- **Training** – The OT Incident Response Team must have an education roadmap to earn knowledge and skills in various fields of profession. These fields include network architecture, industrial protocols, control systems development, industrial plants and processes, operating systems, virtual machines, forensic tools and methods, cybersecurity components, data analysis, scripting, incident handling, malware analysis, etc. This knowledge can be achieved through commercial and academic courses and self-research. An educational framework, for example, could be the NIST National Initiative for Cybersecurity Education (NICE) which provides training for various specialty areas such as Exploitation Analysis, Threat Analysis, and more.

- **Practice** – Theoretical knowledge in Digital Forensic fields is crucial but not enough. While actual OT Cyber incidents are fortunately not daily, the Forensic teams must practice their skills through exercises and incident simulations. These simulations can vary from practicing forensic methods while dealing with regular technical malfunctions to comprehensive organizational Cyber exercises.

- **Testing Lab** – The IRT members need a lab to test their tools and training. They must have experience with the tools they are using and understand each tool's capability and limitation. This lab should include Workstations and Hardware with an identical configuration as those in the OT systems, virtual environments for practice and running malware samples, IR off-network workstations, and of course, IR tools.

3.2. Digital Forensic Lab

3.2.1. Hardware

The Digital Forensic Lab is a facility that should allow examination and analysis of the data after it has been collected. Digital labs require specialized hardware to support forensic analysis, including:

- **Gateway Workstation** – This workstation has two main roles. First, allowing a safe and secure gate for entering digital data into the Digital Forensic servers. That should include a mechanism for copying the data and ensuring its integrity without damaging the original files. For example, some utilities can copy CDs and Hard Drives without

influencing the original media. Second, because of the high potential of malware presence in the data source, the Digital Forensic Lab must allow data only to enter inside and prevent data from going back out. That can be achieved with a unidirectional component like a data diode or one-time media to copy the original data.

- **PCs and Servers** – This equipment need to host all the Digital Forensic tools. The only requirement for these computers is that they have enough resources and peripheral inputs to meet all the analyst's needs. It can be considered to install these workstations as stateless machines (with tools like Live CD), so each Digital Forensics process will start up with a clean operating system. A similar result can be achieved with a Virtual Machine platform.

- **Industrial Components** – This part is crucial for an OT Digital Forensic lab. As part of the OT Digital Forensic process, it is necessary to examine the forensic data as close as possible to the actual operating environment. Since, for many reasons, it can be impossible to perform a local Digital Forensic on the infected OT system, the Digital Forensic lab must include some physical industrial components like PLCs and industrial equipment to allow emulation of the real environment.

3.2.2. Software

This layer of the Digital Forensic Lab should include software tools from a few groups:

- **Virtual Machine** – There are many good reasons to work on a virtual machine platform instead of the local operating system of the workstation; their goal is to provide a safe working environment to analyze and run malicious code. Virtual Machine allows the creation of different setups that can suit different OT systems specifications in the organizations (e,g. the exact OS version and ICS programs). Another advantage is the ability to startup any Digital Forensic process from a known clean point. That can be achieved by using the VM snapshot feature. This is very useful because Digital Forensic data potentially includes digital malwares.

- **IT-Based Forensic tools** – This category includes Forensic tools generally used for IT environments and can be applied to OT systems. That should include tools to analyze Network data, Logs, Memory, Files, Processes, etc. It also should include configuration tools for Network devices, Operating systems, Servers, and PCs.

- **OT-Based Forensic tools** – This category includes dedicated tools and applications for OT devices Configuration, Development, and Maintenance. These tools should allow access to the PLCs and Industrial equipment's software, firmware, and diagnostics.

- **Emulating Control Systems** – Expanding the Digital Forensics Lab with physical hardware such as PLC can significantly improve the analysis process. However, it is not always possible to do it, especially while simulating an extensive OT system. Software-based emulation can be applied by installing HMI, OPC Client, PLC emulator, Honeypots, etc.

3.3. Preparations in the field OT systems

Although what is presented in this section is not a direct role of the OT DFIR team but the engineering teams, and although most of the issues are mentioned throughout the document, it is worth concentrating on some preparations required in the OT systems themselves to bring them to a position that will allow forensics when necessary.

- **System Clock** – The forensics analyst must be able to establish a context of the time when evaluating collected data. Some organizations use Global Positioning System (GPS) or other authoritative clocks (e.g., time.nist.gov) to ensure ubiquitous time across the domain. However, it is not uncommon that network latency can introduce considerable time differences amongst devices. Network Time Protocol (NTP) can be used to estimate and account for this latency, and some organizations incorporate both methods.

- **Install Collection methods** – In order to enable the collection of forensic data during the routine and an event, a suitable architecture must be planned. Moreover, the collection points, as well as the collection mechanisms, must also be prepared. Such technical adjustments should not be made while handling the incident.

- **Allowing Forensic data** – The system components must be configured to create forensic data and transfer it to the collection center. The required settings in the communication switch to collect network traffic must be made. It is also necessary to allow log creation in each endpoint and ensure that any needed data for the investigation is produced initially.

- **Integrating Forensic data Collection into System Routine** – As mentioned above, forensic data collection should be a part of the system routine. Fundamental forensic data such as project files backups, security logs, network traffic, and even configuration files and memory dump from time to time must be collected to accustom the system to forensic data collection.

4. OT DFIR Framework

This section will introduce the OT DFIR Framework. It will describe the framework in general and then dive deep into every step of the process. The motivation for this framework is based on the unique properties of OT systems which are widely discussed in Sections 1 and 2.

4.1. The Framework

Fig. 2 below describes the main **Phases** of the framework, while **Fig. 3,** on the next page, describes the detailed activities during each **Step** of each phase.

Fig. 2. The OT DFIR Framework

A. **Routine** – This phase includes the activities needed before an event occurs. The framework will describe only the essential activities related directly to the following phases. Therefore, the main activity during the routine is Asset Identification and Data Collection. The strong connection between the operational side and the cyber team is emphasized already at this phase. While the SOC is doing Cyber Monitoring and recording fundamental data, the Facility Control Room (FCR) is doing process monitoring and managing an operational Events Log.

   This data is critical to enable anomaly detection and allow incident investigation when it occurs. Another benefit of this phase is integrating data collection into the system routine so that it would not be a new operation in the presence of malware. While collecting digital and operational data, it is essential to verify that all data sources are synchronized to a unified timeline. Moreover, periodic snapshots of collected data should be used as the system baseline for later comparison.

B. **Initial Identification and Reporting** – This phase starts when something comes up in the system. It can be an operational alert or malfunction observed at the FCR, and it can be some anomaly or an alert at the SOC. Although most of the time, it may be a typical operational malfunction, at this point, the relevant center needs to initiate a fundamental analysis while updating the other center and trying to keep the forensic data intact. Mutual updating is crucial in case this local event escalates to a cyber incident. After a short analysis, if both centers agree that this is a typical operational malfunction, they will solve it and go back to routine. If not, the initiator center should report and open a ticket for technical support.

C. **Technical Event Handling** – This phase starts when a more significant event is involved, and more in-depth technical support is needed. At this point, the Technical Support Team (TST) engineers need to collaborate with the SOC for the chance of an escalation. If both teams agree that this is a typical technical issue, the TST will perform technical support and close the ticket. Otherwise, the TST will summarize the chain of

custody in a short draft report to enable a situation assessment by the management. The situation assessment decision can either go back to more technical inspection and support or move forward to the next phase.

In case the event looks very unusual from the beginning of this phase, the TST can immediately gather a situation assessment to save time and reduce risks while moving forward to the next phase and treat the event as a Suspicion of a Cyber Incident.

D. **Cyber Incident Analysis and Response** – This phase begins after the management agrees to move from a usual event handling process to a cyber Incident Response. That decision can be accepted due to odd symptoms in the system or due to a clear observation of a cyber-attack. The first step is to declare the incident status and report it to all the system stakeholders. The most significant impact of this act is raising awareness. It can be expected that this announcement will increase the stress and focus on all the involved teams.

   Simultaneously, the IRT needs to be activated by the management. The first step of the IRT will be to collect data for the investigation. Part of this data will be based on the data already collected during the routine phase. Supplementary data will be collected as fast as possible before things will change in the system. As mentioned before, the IRT needs to consider collecting supplemental data locally at the system or from a long-distance security center.

   Next will begin the Digital Forensics and Response steps in parallel with continuous situation assessments. At the Digital Forensics step, the IRT will do a Timely Analysis of the data in order to achieve a good understanding of the incident. Following the decisions of the management situation assessments, the IRT will apply actions like Containment, Eradication, and Recovery operations in the system.

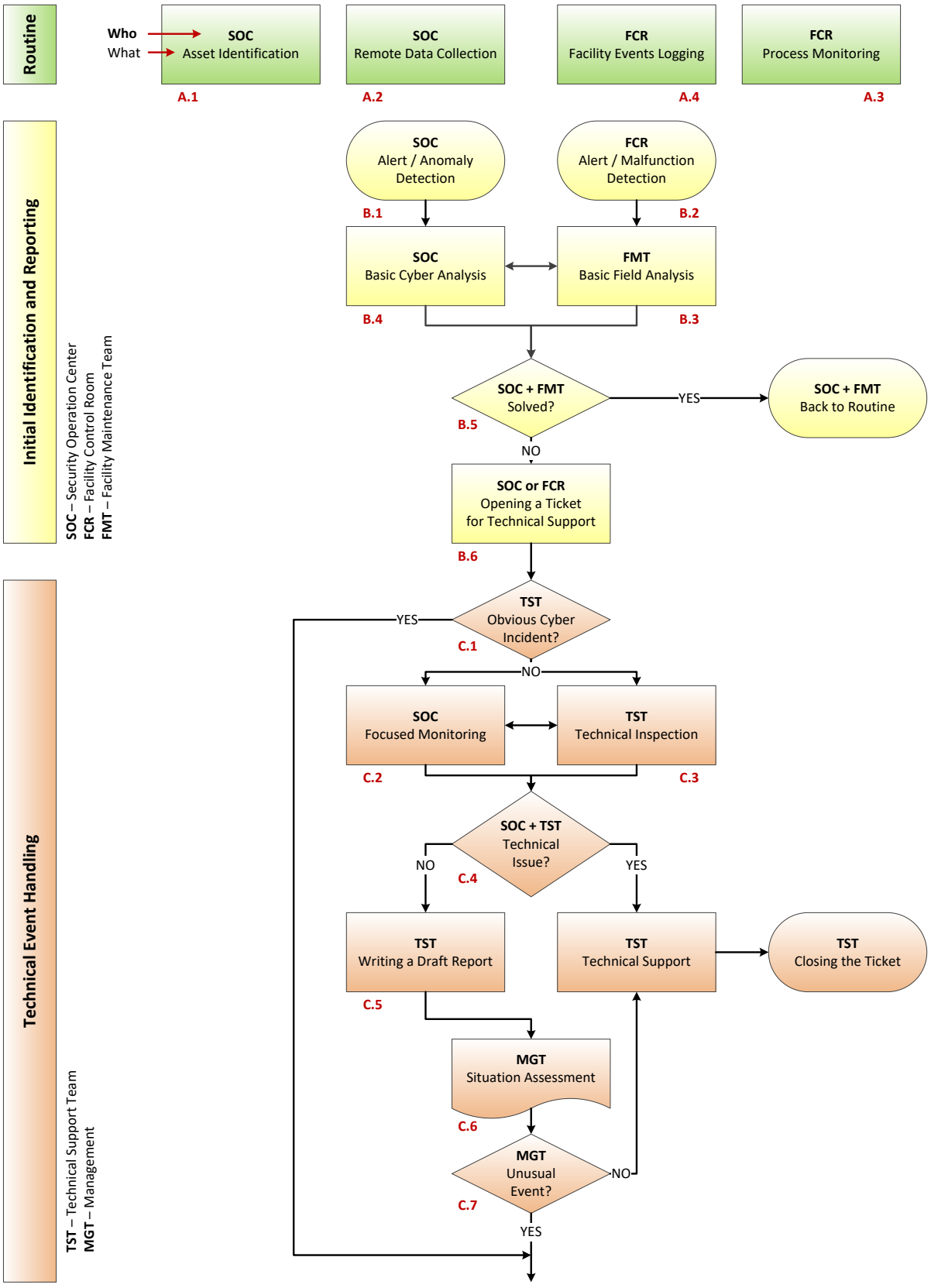
E. **End of Cyber Incident** – This phase deals with the activities needed to be done to end the incident. Sometimes, announcing the end of the incident is simply a management decision, even though not all the issues have been resolved. But this announcement will allow the facility to plan how to move forward and go back to some form of routine.

   Next, The IRT will conclude some lessons learned to improve the security level and their next time activities and publish a final report while closing the ticket.

F. **Post-Incident** – The primary activity at this phase is to back to a system operating under a Supervised Routine. Therefore, the SOC and the FCR need to increase monitoring and focus on the system behavior for a well-defined period.

   The IRT should publish the lessons learned from the incident to raise awareness in the organization and implement the recommendations from the final report to strengthen the security level. Another activity that the IRT can make is advanced forensics to gain an in-depth understanding of the malware behavior.

4.2. The Detailed Process



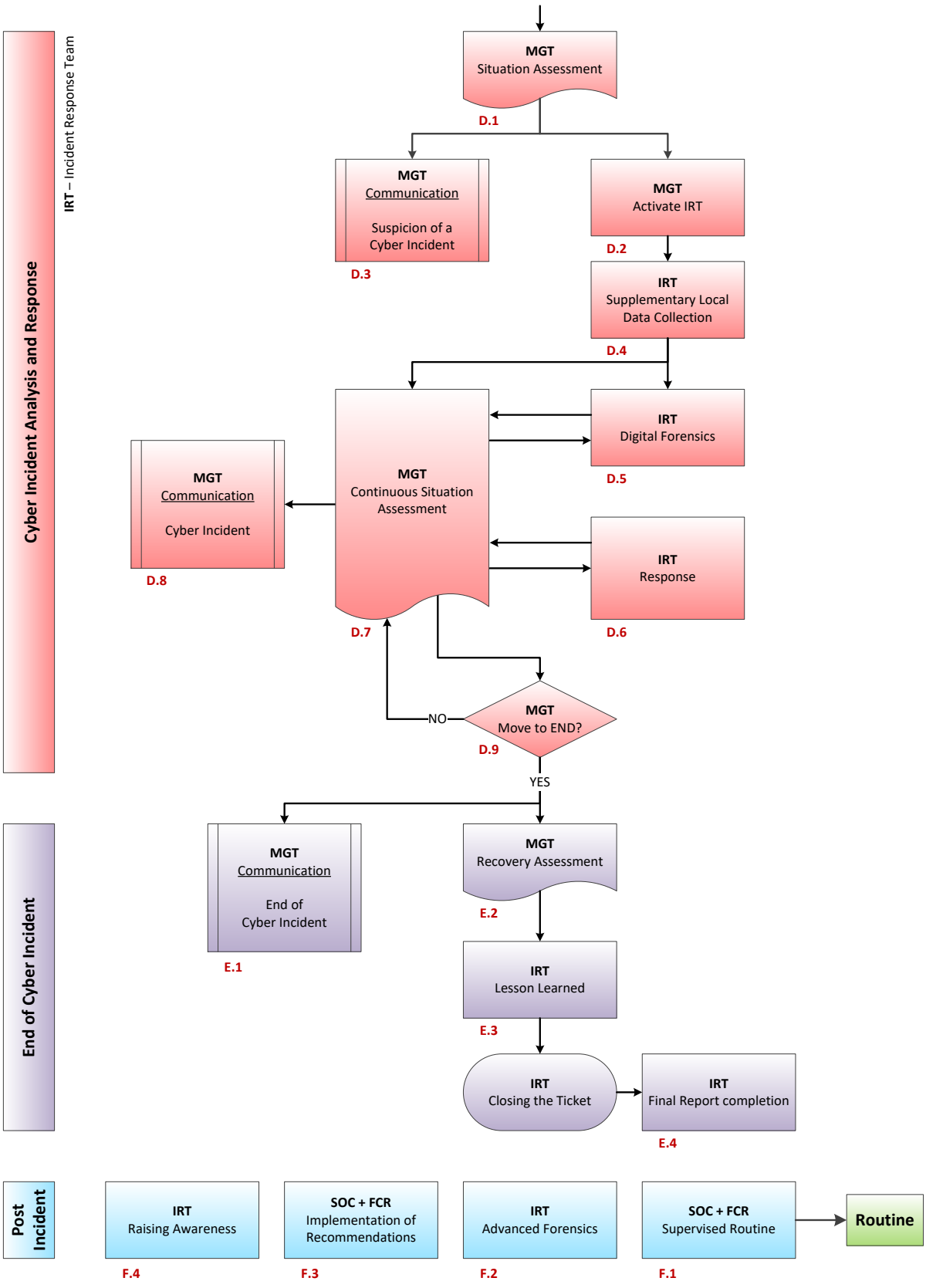


Fig. 3. The OT DFIR Detailed Process

From this point of the document, every subsection will expand each **Step** of the framework, structured as follows:

- **Background** – An explanation of the motivation for the activities in the step.
- **Goal(s)** – A definition of the required target.
- **Who** – A definition of the person or team who should lead the step activities.
- **How** – An explanation of tools, techniques, and strategies to achieve the step goal. These explanations will not be detailed to the level of step-by-step technical operations, as these depend on the equipment, vendors, and systems specific to each organization. Every organization should use the methods proposed in this chapter to build its dedicated technical procedures.

4.2.1. Routine

The SOC and the FCR do many activities during the routine phase. This OT DFIR framework is focused only on the steps and actions that relate to and serve the future phases in the process. Therefore, this phase will describe the main activities in the SOC (Asset Identification and Remote Data Collection) and at the FCR (Process Monitoring and Event Logging) during the routine, that is, before an event.

A.1	SOC	Asset Identification

- **Background** – This Step describes the initial data that needs to be available to investigate a Cyber Incident. It is essential to identify all the assets and connections in the system and have an up-to-date network architecture diagram, including interfaces to the IT/corporate network or any other networks. Moreover, this is not a one-time activity; the map must be updated periodically with any change in the network. Finally, the map should be detailed as possible, including all asset identifications, addresses, ports, protocols, etc.
- **Goal(s)** – Having an up-to-date network architecture map.
- **Who** – SOC analysts together with the OT engineers.
- **How** –
    - **Validate existing info** – A good starting point for this step is to look for existing maps and diagrams and validate their accuracy. There can be assets on the maps that no longer exist and vice-versa. The validation should be done by looking at how detailed the information is and when it was created and updated. It can also be done by visually inspecting assets and connections inside the facility.
    - **Collect information** – New information can be collected in a few ways, with pros and cons to each. In order to not affect the operation and the safety, it is always preferred to collect information with the least intrusive method. Another note to mention is that most of the collection methods are built to reveal IP-Based assets, while OT systems can also include non-IP-Based components.

- **Passive Traffic Analysis** – This is the safest and least time-consuming method of performing asset identification. This method can be applied by collecting raw data from selected chokepoints at the network and analyzing it with a network analyzer tool. The raw data can be collected continuously using an online communication link to the network **(covered in the next step – Remote data collection)** or by manually taking a sample of the data using a network tap.

  It can take a while to discover all the assets in the network. An asset is discovered only when it transmits data into the network. If the raw data capturing is done for a limited period, and not all the assets communicate during this time, they will not be identified. Moreover, if the collection point (or chokepoint) has not been placed correctly, it is possible to miss assets that are connected through a different path.

- **Configuration File Analysis** – Configuration files can add additional information to the asset identification. For example, ARP tables from network devices can reveal MAC and IP address pairing. In addition, firewall configurations can show what paths are opened and what ports are currently being blocked or allowed.

- **Active Scanning** – Active scanning can be a quick way to identify assets on the network, but it is also risky to the OT system. Active scanning tools can use a lot of network bandwidth while sending requests to devices to discover them. It can also query network ports that devices might not support correctly and cause unexpected behavior in the OT devices. However, it is possible to safely perform active scanning in an OT system after testing the tools on an external testbed and performing the scanning during system downtimes, such as maintenance periods.

- **Documenting** –

  - **Configuration management** – The collected information should be documented in an accessible and easy-to-use platform. If possible, the best way is to use a dedicated configuration management tool or any engineering drawing platform. In addition, it is recommended that the documentation include technical details such as hardware, software, and firmware versions.

A.2	SOC	Remote Data Collection

- **Background** – There are two main reasons for performing a good remote routine collection mechanism. First, the essential data that will help understand a cyber incident is usually the data that runs in the system before and during an incident. If not collected all the time automatically, that data probably would not be available after the incident has already begun. Second, the better and more comprehensive the data gathering mechanism will be, the more time and effort saved during an incident. In that case, only

supplementary data will be needed to collect manually. Collecting data for monitoring is especially useful in an OT environment due to rarely patched equipment.

This step is focused on the fundamental data that should be collected continuously. Supplementary data collected during incident handling will be detailed in step D.4.

- **Goal(s)** – Having the fundamental forensics data for baseline and event analysis.
- **Who** – SOC analysts while supported by OT Engineers.
- **How** –
    - **Data Types** – At this step, the target is to collect the most valuable data that make sense to deal with, not all the data.
        - **Network Full content traffic** – A complete packet capture of network traffic, whether it is Serial-based or Ethernet-based data. Usually, this type of data generates a PCAP (Packet CAPture) file format. This data can be used to create network maps and statistics, conversation summaries, deep packet inspection, and much more. However, The amount of data generated by this type of collection can be overwhelming, especially if collected continuously; therefore, accumulating and storing is not suitable for every organization.
        - **Network Flow Data** – A summary of the network traffic, usually in an IPFIX format like Cisco NetFlow, which provides visibility on traffic flow and volume, and tracks where traffic is coming from, where it is going, and how much traffic is being generated any time.
        - **Logs** – Logs are event records generated by network and endpoint components in the system. This includes various file formats like Syslog, Windows event logs, etc. The logs are easy to modify, so they must be saved in a read-only repository while taken.
        - **Files** – This category refers to the most important files that should be collected as part of the system baseline. That may include configuration files, firmware, PLC codes, etc.
    - **Collection methods** – Network full content traffic should be collected through chokepoints. These are essentially intended bottlenecks on the network that do not limit bandwidth or cause latency, usually applied by using a network Tap or a mirror port while sending the traffic to a capture system. Several naturally forming chokepoints will be created when a network is segmented correctly.

      Network flow data should be aggregated via an exporter server toward one or more flow collectors. Similarly, dedicated endpoint agents should collect logs and files and forward them to a collection server.
        - **Mirror Port** – A physical port in a managed network switch that duplicates traffic from one or more ports or VLANs, directing the

copied stream to a designated destination port. The most significant benefit of port mirroring is that the platform already exists in most managed switches. It is merely a software configuration setting to activate the feature. The major downside is the limited throughput of the mirror port, which can lead to excess traffic being dropped.

- **Network TAP** – A dedicated device that duplicates network traffic to a capturing destination. The main benefit of a TAP is that it is designed to do its job exceedingly well. A high-quality TAP can assure not to lose traffic, provide multiple monitoring ports and redundant power supplies, allow traffic to pass across the monitoring link even without power to the device, and more. The main drawbacks of network TAP include the high price and downtime required to be installed.

- **Reducing impact on the system** – Collecting data might affect the system in two significant ways. First, it can affect the system's performance because more data needs to be generated and forwarded. Second, the tunnels that deliver the data to a centralized center can be abused to attack the system remotely. The data collection mechanism should address these two issues. Logs and files should be collected with lite software agents that do not consume many computing resources. Network data should be collected through a network Tap or Mirror port and without using the operational network bandwidth (out-of-band). Moreover, it is recommended to use a unidirectional tunnel to the data center, so this tunnel can not be used to intrude malware into the network.

- **Reducing impact on the data** – Data through the collection tunnel might be exposed for manipulation if this tunnel is not secured enough. A physical hardening or an encryption method must be applied to prevent unauthorized access to the data. In addition, a database of hash signatures should be maintained separately from the forensics data to ensure the integrity of the data.

A.3	FCR	Process Monitoring

- **Background** – This step probably describes the most traditional action in OT systems. In this step, the process is monitored continuously by the facility's operators through sensors, indicators, and HMI systems, to achieve business goals and safety. The added value of including this step into the OT DFIR framework is to strengthen the connections between the operational and the cyber security teams. These teams should collaborate during an incident handling process as well as the routine.

  The process data collected by the operators could be precious to support a digital forensic process in the future. As mentioned above, technical malfunctions and process anomalies may occur more frequently than cyber incidents in OT systems. While cyber incidents are rarer, they will usually start with similar symptoms. Therefore, every organization must find the balance between treating any event only as a technical malfunction and getting risk in false-negative to treating any event as a cyber incident and getting risk in false-positive. This balance can be achieved only by continuous cooperation between the teams.

- **Goal(s)** – Monitoring the physical process's parameters with the awareness of the risk of a cyber incident in the back of mind.
- **Who** – Operators in the Facility Control Room.
- **How** –
    - **Process Historian** – Data historians contain valuable historical and statistical data for collection. Detection of deviations and anomalies can be used to understand the threat and the scope of the incident. For example, if the data historian values and setpoints have recently changed after a cyber incident, it is a good indication that the system might have been impacted.

      Data historians can differ in various ways, but essentially, they are all databases. A good practice is to store the data securely and sync it with a collection tool such as a SIEM to give a more holistic view of the incident.
    - **Screen Recorder** – Another piece of critical operational data is a log of all the actions made in the system. Any operation in the HMI should be recorded either by some internal logging mechanism or simply by recording the whole screen continuously. The last option has the added value of showing the full picture of the HMI during the incident period in a simple way, like in video file format.

A.4	FCR	Facility Events Logging

- **Background** – Not every action or event in the OT environment occurs in the digital space as the HMI or any other server. Many activities and routines are taking place in the physical space of the operational environment. These actions and events are also crucial to investigating a future cyber incident. For example, the investigators must well understand if the system's pressure is raised because of a valve that has been closed manually by the operators or because a value in the PLC has been changed by malware.
- **Goal(s)** – Managing a log to document events in the system.
- **Who** – Operators in the Facility Control Room.
- **How** –
    - **Logbook** – The events documentation can be made manually in a hardcopy logbook or digitally in a software tool platform. Obviously, managing a digital platform will make it easier to search for information when needed. The logbook should contain any significant event that happed in the system. For example, shift change, recipe change for production, maintenance operations, intentional downtimes, changes in the raw materials, decisions made by the operators or facility managers, etc. High-quality event documentation will save valuable time and many questions from the response team.

4.2.2. Initial Identification and Reporting

The entrance to this phase can be by any anomaly or malfunction in the system; most of the time, this phase will be completely technical. The main goal of this phase is to allow the operational teams to initiate a collaboration with the cyber SOC team. The better this collaboration is, the better the teams will be prepared to deal with an actual cyber event. On the one hand, their target is to consider the possibility of a cyber-attack from the beginning of the event to allow a later investigation. While on the other hand, not to burden the Incident Response Teams with false positives. The key to a successful collaboration is communication and mutual updates.

B.1	SOC	Alert / Anomaly Detection

- **Background** – In this step, all the collected data should be used to detect threats. Detection is not about diving deep into all the network traffic, logs, files, and so on. Instead, the detection requires using indicators, warnings, and alerts to realize that something is happening in the system.
- **Goal(s)** – Detect an anomaly in the digital space of the system.
- **Who** – SOC Analysts.
- **How** –
    - **Types of Threat Detection** – The detection approach should help analysts understand the context of the threat and what they should do with the information. Any detection approach has pros and cons, so they should be used smartly together. An Intrusion Detection System (IDS) is a system that can alert on anomalies in the system, from policy violations to malicious activity. Its mechanism can be based on signature and well-defined indicators or on a heuristic algorithm that looks for odd behavior or deviation from baseline activity created by the tool. The following types of threat detection are the principle of operation of many IDSs on the market.
        - **Configuration-based** – This is an allowlist-style approach. The SOC analysts should look for system configuration or architecture changes in this type of threat detection. This approach might cause false positives because it catches almost everything, such as new processes, threads, files, folders, and valid network activity.
        - **Model-based** – This is a more sophisticated way to apply configuration-based threat detection. In this approach, a learning mechanism continuously creates a system model to represent the nominal state of the system as well as acceptable minor changes. The downsides of this approach are that the model should be trained constantly, and it does not provide any context to the detected threat.
        - **Indicators-based** – This approach looks for a specific description of the threat, such as a digital hash of malware. This approach can provide the most context information about the threat from that perspective.

However, it requires a daily updated database, and it is usually useless for tailored threats for a specific system.

- **Behavior-based** – This is a more sophisticated way to apply indicator-based threat detection. This approach focuses on tradecraft instead of the specific threat indicator. For example, it can alert anytime someone uses a VPN to access an HMI, drop a new file, and send commands to the RTU. This holistic approach can provide a context for the threat and deal with various threats.

- **Threat Hunting** – This is a much more active approach to detecting threats and usually demands a dedicated specialized team to have the expertise to hunt for advanced threats. This detection approach is the process of searching through the network environment for adversaries that have the intent, opportunity, and capability to harm the system. The advantage of threat hunting is that it helps discover unknown threats that other detection approaches may not detect.

- **Recommended starting points for detection** – Identify the highest and the lowest talker in the network; most significant bandwidth users; encrypted communication; critical assets and normalized traffic; look for known tradecraft before looking for anomalies; identify files being passed to hosts; understand when an event should be or should not be occurring on the network, such as firmware updates and patching.

B.2	FCR	Alert / Malfunction Detection

- **Background** – Previous ICS/OT cyber incidents show that one of the primary triggers for the cyber investigation was the physical symptoms observed by the FCR's operators.

  In this step, the operators use the operational data collected about the process to detect physical anomalies and technical malfunctions. While, in most cases, this kind of detection will lead to regular technical support, the OT DFIR framework must give some level of attention to these kinds of events for the possibility of turning into cyber incidents.

- **Goal(s)** – Detect an anomaly in the physical space of the system.

- **Who** – FCR's Operators.

- **How** –

  - **Types of Threat Detection** – Because of serious concern for safety events in an OT system, detecting a physical anomaly in most cases is based on strict threshold rules. However, a large gray area of warnings under the thresholds can indicate that something bad is about to happen to the production process or the safety.

    - **Rule-based** – This method is based on well-defined rules in the PLC program or the safety equipment. These rules must be simple and

meaningful to allow the operators to understand the anomaly and respond quickly.

- **Model-based** – A more sophisticated detection method uses a logical process model that can help predict the system's expected behavior. The advantage of this approach is to have a warning before something bad happens. The downside is that these warnings provide less meaningful context, making it harder to understand the root cause and take action.
- **Physical inspection** – Sometimes, the traditional and straightforward inspection of the physical system is necessary and can be very helpful in following the process. For example, experienced operators can detect nonregular trends in the system only by following the sound of the machines and mechanical equipment.

B.3	FMT	Basic Field Analysis

- **Background** – An operational alert or a technical malfunction should lead to basic technical analysis. That will allow the operators to take action in the system, such as turning off an actuator and changing a parameter's value or allowing the local technical support team to replace or fix a damaged part of the system.

  The second action that should be done in this step is to contact the SOC and inform them about the event in a very simple way. This little piece of information can allow the SOC to keep an eye on the specific assets of the system and see if there is any supportive information that can help explain the event. Moreover, it will allow the SOC to acknowledge alerts that will raise according to technical support actions.

  It is vital to emphasize that the working assumption is that the event is technical-based and not a cyber-attack at this step. However, if needed, the goal is to allow future escalation without regret for losing time and data. Therefore, there must be a balance between the need for connection with the SOC and that it can cause some overload to the technical process.

- **Goal(s)** – Initiate a basic technical analysis while being in touch with the SOC.
- **Who** – The FMT, while supported by the operators.
- **How** –
  - **Basic Field Analysis** – The local FMT can address many alerts and malfunctions without external support. The local team is trained to change process parameters, replace mechanical parts, and repair issues with the electrical boards. Sometimes, they are trained to perform simple actions in computing and networking systems, such as restarting and replacing peripheral devices. A critical thought to keep in mind is that essential data can be lost during these activities. For example, any simple reset for a workstation can delete its volatile memory. Again it is all about the balance; no rules can replace common sense in these cases.

- **Inform the SOC** – The communication link for the mutual update must be secure and straightforward. Any short email or phone call within the internal business network can address that need. It is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.

B.4	SOC	Basic Cyber Analysis

- **Background** – After alert raising or anomaly detection, it is up to the cyber analysis step to check whether the threat seems real or can be mitigated quickly without impacting the operation. There will always be alerts on the detection systems; most will be between false-positive and policy violations or configuration issues. But fundamental analysis is needed to decide whether to escalate the event or not.

  This step is not intended to perform a deep analysis of threats as it should be during the Incident Response steps. Instead, the goal is to gain a basic understanding of the event to help decision-makers determine if and how the threat should be elevated for handling. It is also not the analyst's role to decide what to do with the system or the production process. Such a decision will be made after assessing the situation with the facility managers.

  Another target at this step is to make sure that analysts in the SOC contact operators in the FCR and let them know about the alerts related to their system. Otherwise, there is no way that the operator could know that something could get wrong with their system. The FCR should keep an eye on the system and support the SOC with the analysis.

- **Goal(s)** – Initiate a basic cyber analysis while being in touch with the FCR.

- **Who** – SOC Analysts while supported by the operators.

- **How** –

  - **Packet Analysis** – This is a process of extracting information from the raw packet capture of the network to explain the abnormal behavior. This process is not about understanding the big picture; the focus should be on individual sessions of packets related to the alert. A proper packet analysis should rely on the technical knowledge of protocols and packets and the baseline behavior of the network. Following the TCP/UDP stream, looking for the 5-Tuple (Source/Destination IP, Source/Destination Port, and Protocol) can be a good starting point.

  - **Traffic Analysis** – This is a process of examining the network traffic to determine patterns and behaviors beyond individual sessions. Traffic analysis is used to explore the larger context of the network. It should be used when a quick look is needed at a network segment, or a large amount of data needs to be evaluated. For example, it should look at the most active workstations, queries across the network, flow data, file movement, and more.

  - **File Analysis** – In this step, a file analysis aims to determine its origin, nature, and context. It is not intended to verify if a file is malicious and how it works.

Instead, a simple check should be performed, such as comparing to baseline, checking the file signature, and extracting the file from the network traffic to examine it in an isolated workstation.

- **Timeline Analysis** – This method can add context to individual actions in the network by examining them in the order they occurred. For example, a series of detected events or alerts are analyzed to discover trends and adversary progression in the network. Visualization of data is also important for timeline analysis as it allows the analyst to notice patterns that may not be inherent to computer systems.

- **Inform the FMT** – The communication link for the mutual update must be secure and straightforward. Any email or phone call within the internal business network can address this need. It is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.

B.5	SOC + FMT	Solved?

- **Background** – Seemingly, this sounds like a simple question, but the challenge is that both teams should agree on the answer TOGETHER. The reason for that is, again, the need for balance. Naturally, the operational side is motivated to go back to routine as soon as possible. On the other hand, the cyber side is motivated to analyze every event to deny future cyber incidents.

  The need for agreement on the event status forces each side to see the whole picture and consider all options. It is important to note that the way to reach an agreement should be as short and effective as possible.

- **Goal(s)** – Decide whether to escalate the event or go back to routine.

- **Who** – SOC analysts together with FMT technicians.

- **How** –

  - **Quick Assessment** – Both sides should make a short conversation via phone call or email and discuss the event. Example Considerations:

    - Has an operational risk arisen that requires special attention?
    - Is this a known technical malfunction?
    - Is a clear technical explanation found?
    - Is there an effect on software or hardware in the system?
    - Is it possible to answer without the need for outside support?
    - Is there a clear connection between the symptoms in the system and the alert data in the SOC?
    - Has support and maintenance activity been performed on the system recently?

  - **Decision** – If both sides have agreed event's meanings and the ability to respond independently, the problem can be addressed, and they can be returned to

routine. Otherwise, the side where the incident was discovered should open a ticket for a more in-depth inspection by the engineering staff.

B.6	SOC or FCR	Opening a Ticket for Technical Support

- **Background** – In case both sides do not reach an agreement or the problem is not resolved through the internal staff of the facility, a ticket opening is required for an in-depth technical inspection from the engineering team.

  From this point on, the potential for a cyber incident does increase somewhat, but most of the incidents will still be closed as technical events that require intervention in changing hardware or software.

- **Goal(s)** – Documenting and tracking the development of the event.
- **Who** – SOC analyst or FCR operator depends on where the event was initially detected.
- **How** –
  - **Opening a ticket** – The best way to open a ticket is to use an organizational ticketing system. These systems are designed to contain all the relevant information about the event, the technical data about the specific assets, the ability to contact the engineering team, and much more.
  - **Sharing information** – The communication link for contacting the engineering team beyond the information inside the ticket must be secure and straightforward. Any short email or phone call within the internal business network can address that need. It is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.

4.2.3. Technical Event Handling

The entrance to this phase will be after both the local facility maintenance team and the SOC analysts agree that the anomaly or malfunction they detected could not be addressed solely by the local group or that it seems to be more suspicious. In this phase also, most cases will probably end as a technical issue. However, this phase's importance is again the collaboration between the technical engineers and the cyber analysts. Two main characteristics set this phase apart from the previous one. First, the technical inspection in this phase will be done by external teams that are less involved in the operational process, which may allow for additional perspectives for viewing the information. Second, the technical inspection in this phase will be much deeper than in the previous phase, which may impact the forensic data.

C.1	TST	Obvious Cyber Incident?

- **Background** – The first step in this phase is a type of bypass to the next steps. The goal is to allow skipping the engineer's technical inspection in cases where the probability of a cyber incident is very high. For example, when some workstations have been locked by ransomware. Since the support engineers have a deeper understanding of the system and since they are less involved in the internal considerations of the

facility, they are the ones who should recommend skipping steps in the phase. In such a case, it is not that the technical inspection will not be carried out; it will be carried out as part of the Incident Response Team activity, which the support engineers are part of it.

- **Goal(s)** – Providing the opportunity to save time and damage to forensic data if the likelihood of a cyber incident seems high.
- **Who** – Technical Support Team.
- **How** –
    - **Decision** – Based on the engineer's experience, they only need to consider if the event symptoms look similar to previous events and if giving time for a technical inspection is worth the try. In any other cases, they should forward the decision to consider a cyber incident announcement to a management team assessment. Of course, there is always a possibility of mistake judgment, but again, it is all about finding the balance.

C.2	SOC	Focused Monitoring

- **Background** – The importance of this step is, again, the collaboration between the cyber team with the supporting engineers. The SOC analysts can continue with a similar analysis as they did in the previous phase, but this time they should focus their efforts on supporting the engineers and providing them the information they would not be able to have locally in the system.

  The engineers' actions in the system will probably be pretty noisy on the network. Any interaction with the PLC program, the HMI workstation, the engineer workstation, and the network will exceed the baseline. The SOC analysts must be aware of that and acknowledge alerts that would come up. But they also should look if something is getting wrong beyond these actions. It will also be an excellent action to filter and record that network data related to the event so it can be used if any further investigation starts later.
- **Goal(s)** – Follow the engineers' actions with the collection and detection systems and support their actions from the SOC.
- **Who** – SOC analysts while informing the TST.
- **How** –
    - **Monitoring and Analysis** – Performing actions as described in step B.4 (Packet Analysis, Traffic Analysis, File Analysis, Timeline Analysis) while focusing on the artifacts related to the examined event.
    - **Inform the TST** – The communication link for the mutual update must be secure and straightforward. Any email or phone call within the internal business network can address that need. It is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.

C.3	TST	Technical Inspection

- **Background** – If the progress of the framework is currently on this step, it means that the assumption is that the event seems to be a technical issue. The TST will initiate a technical inspection that will include examining the PLC program, the system hardware, the network, the logic, etc. The technical inspection should be in cooperation and coordination with the SOC. It is clear that if the cooperation with the SOC takes too much effort, it will not last for long. But this cooperation will gain value if the events escalate to a cyber incident.
- **Goal(s)** – Performing a technical inspection in cooperation with the SOC.
- **Who** – OT Engineers supported by the facility teams and the SOC.
- **How** –
    - **Monitoring and Analysis** – Performing Similar actions as the analysis actions in the previous phase.
    - **Inform the SOC** – The communication link for the mutual update must be secure and straightforward. Any email or phone call within the internal business network can address that need. It is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.

C.4	SOC + TST	Technical Issue?

- **Background** – The OT engineers and the SOC should estimate together if the event seems to be a technical issue or they need a much more in-depth situation assessment. Even if they were wrong, they already collected so much data, understanding, and collaboration that will allow them to turn the event into an Incident Response quickly.
- **Goal(s)** – Decide if the event is based on a technical issue or not.
- **Who** – The OT engineers together with SOC analysts.
- **How** –
    - **Quick Assessment** – Example considerations:
        - Has an operational risk arisen that requires special attention?
        - Is this a known technical malfunction?
        - Is a clear technical explanation found?
        - Is there an effect on software or hardware in the system?
        - Is there a clear connection between the symptoms in the system and the alert data in the SOC?
    - **Decision** – If both sides have agreed event's meanings and the ability to respond, technical support can address the problem. Otherwise, they should write an initial draft report to summarize all the findings to this point. This report will be the basis for the situation assessment later.

C.5	TST	Writing a Draft Report

- **Background** – After the technical inspection did not discover an apparent technical issue, a situation assessment led by management representatives from all stakeholders is needed. To allow a practical discussion, the technical support team must write and provide a draft report of the event to summarize all the artifacts and findings known to this point. That would be the activity of this step.
- **Goal(s)** – Providing a starting point for the situation assessment.
- **Who** – Technical support team.
- **How** –
    - **Report Content** – The report should be written clearly, concisely, and fact-focused. It should include at least the following topics: The chain of events, technical inspection results, basic cyber analysis results, and current risks.

C.6	MGT	Situation Assessment

- **Background** – This is the first situation assessment in the OT DFIR framework. Its purpose is to stop for a moment a decide how to treat the event. Deciding to declare the event as a cyber incident can have many implications: managerial focus and increased pressure, human resources and money to be invested in handling the incident, impact on production and business process, etc. This is the main reason the management representatives should lead this situational assessment. Another benefit can be their professional experience; they may have seen this event in the past and may have a technical explanation.
- **Goal(s)** – Consider if to escalate the event into a cyber incident or not.
- **Who** – Management as the leader, facility representative, cyber analyst, OT engineer.
- **How** –
    - **Situation Assessment** – Example considerations:
        - Has an operational risk arisen that requires special attention?
        - Is this a known technical malfunction?
        - Have there been such incidents in the past?
        - Have any maintenance operations been performed on the system recently?

C.7	MGT	Unusual Event?

- **Background** – This step is the decision point of step C.6.
- **Goal(s)** – Decide if to escalate the event into a cyber incident or not.
- **Who** – MGT.

- **How** –
    - **Decision** – The decision at this step will either recommend escalating the event into a cyber incident or keep going as a technical event.

4.2.4. Cyber Incident Analysis and Response

This phase is the main phase of treating the event as a cyber incident or a suspicion of a cyber incident. The entrance to this phase will be after a technical inspector ruled out the possibility of a common technical issue at some probability level. It may look like the path to this phase is very long, but it depends on the specific case. For example, in case of an event that looks like a cyber incident with a high likelihood, the entrance to this phase will be very fast. The main activities during this phase will be the Incident Response Team's activities and a recurrent situation assessment that will help decide each step of the handling process.

D.1	MGT	Situation Assessment

- **Background** – The last step of the previous phase was also a situation assessment, which seems like a duplication. This separation is relevant **only** for large organizations with several levels of management hierarchy related to the OT system. This separation will allow junior management to verify that all technical actions have been exhausted before announcing a cyber event, and the event begins to receive focus and pressure from senior management. Of course, this is not relevant for a small organization, and both assessments will occur together in such a case.
- **Goal(s)** – Decide if to declare a cyber incident and activate the IRT.
- **Who** – Management as the leader, facility representative, cyber analyst, OT engineer, and any other stakeholder.
- **How** –
    - **Situation Assessment** – Example considerations:
        - Are such events known in similar organizations?
        - What interfaces does the system have with other systems?
        - What are the safety, operational, and business implications in the event of a facility shutdown?
        - What external influences can the organization have?
        - What are the resources required to deal with the incident?
        - What is the accepted schedule for dealing with the event?
        - Is outside help needed?
    - **Decision** – The decision in this step is whether to declare the event a cyber incident and activate the Incident Response Team according to various considerations such as described above.

- **Severity Level** – From the first assessment of the situation, the severity level of the incident should be determined and updated from time to time. A few parameters can affect the severity level, such as the alert type, the affected assets type and amount, the industrial process type, the spread potential, etc. In addition, the severity level will determine the list of people who will be reported, the initial containment actions, the impact on operation, etc.

D.2	MGT	Activate IRT

- **Background** – Once the decision to treat the event as a cyber incident was made, the first step that should be done is to activate the Incident Response Team. The IRT in most organizations is not a full-time job team dedicated only to Incident Response. Instead, it is a group of personnel who serve as IRT in addition to their day-to-day duty. The important thing is they should always be ready to be activated and gather to the mission. The process of activating the team must be simple, efficient, fast, and secure.
- **Goal(s)** – Send the Incident Response Team to handle the incident.
- **Who** – Management representative.
- **How** –
  - **During working hours** – The communication link to activate the IRT must be secure and straightforward. Any short email or phone call within the internal business network can address that need.
  - **After working hours** – While using an external network such as the internet or cell phones, it is crucial to deliver as minimum information as possible while using external networks that the adversary can monitor.
  - **The activating procedure** – The very initial procedure of activating the IRT should be strictly clear to everyone. Each member should know the code word for the process, their role, when and where they should go, and what they should take with them. Ideally, the gathering location should be in the situation room.

D.3	MGT	Communication: Suspicion of a Cyber Incident

- **Background** – Simultaneously with the activation of the response team, an official announcement of the event as a cyber incident is required. Such an announcement puts the whole organization at a certain level of alertness. As a result, managers and staff will begin to monitor the incident's development closely. Some of them will be required to carry out certain preventive actions, and production facilities will be prepared for a state of production stoppage, etc. Therefore, the event's announcement should also include its severity level.
- **Goal(s)** – Declare the event's status as a Suspicion of Cyber Incident.
- **Who** – Management representative.

- **How** –
    - **Report** – Each organization should have a preprepared list of stakeholders who need to be informed about the incident state for each severity level. These stakeholders could be internal and/or external to the organization.

      The report should include at least the following details: The incident state, severity level, chain of events, current risks, and actions to follow.

D.4	IRT	Supplementary Local Data Collection

- **Background** – This step's primary importance is to freeze the system's state and allow the response team to collect data as quickly as possible before anything changes in the forensic data or in the system and enable a forensic analysis to take place later. Scenarios likely exist in which it is preferable to clean systems and restore them quickly than to preserve them for forensic analysis; it is thus crucial to collect digital data.

  Ideally, all the fundamental data should be collected continuously during the routine, so only supplementary data will be collected in this step. If no data was collected initially, all the required data should be collected during this step. The collection strategy should define the collection order according to each data type's attributes like its value, volatility, and effort required.

- **Goal(s)** – Having all the required forensics data for the incident investigation.

- **Who** – IRT while supported by OT Engineers.

- **How** –
    - **Data Types** – Below listed the supplementary data, which should be added to the data detailed in step A.2.
        - **System's Memory** – High value and highly volatile as things enter and exit memory constantly. Malwares, executables, crypto keys, etc., all get passed into and through memory.
        - **Supplementary network traffic data** – Network traffic is volatile, but malware often communicates regularly, making network traffic less volatile but extremely valuable. While the majority of the network traffic should be collected routinely, there is a possibility that additional collection will be needed, especially for non-IP-based traffic.
        - **VPNs** – These network tunnels are heavily used in OT environments to communicate between businesses to the control network and from the vendor to the OT. Most VPN services can provide logs, including connection attempts, session lengths, and data transfer sizes. Adversaries are well aware of tracks they leave, and VPNs tend to be a prime point and lateral movement strategy for them. Therefore, they are more likely to delete or manipulate the logs for VPNs in OT. Consequently, it is vital to collect VPN logs early in an investigation.

- **Registries** – These are groups of registry keys and subkeys that contain data such as login attempts, passwords, browser settings, and any changes on the system, such as new USBs. Some malwares use the registry hives for persistent access.
- **HMI** – Although consideration must be given to some vendor-specific software applications that are tied uniquely to the control process, it is often the case that the underlying functions of the core operating system will allow for forensics analysis. The systems that run HMIs are often windows-based, similar to any other windows system. However, these are the systems that adversaries would probably look for. Therefore, these systems should enable logging such Windows events and Security logs. The HMI will also often have records of what commands and buttons were clicked, which alarms were dismissed, etc.
- **Engineering Workstation** – These workstations usually have the highest privilege in the OT system. They hold the development platform, the source codes, and access to all the devices. If an adversary wants to understand the process, a key approach is to search the engineering workstation and find the project files and engineering documents.
- **Controllers** – PLCs and RTUs are usually proprietary devices, making them challenging to analyze. Logging and network interactions with these devices are vital for the investigation. Although this type of information may not be available on all of these types of devices, the OT vendor community is producing field systems with such capabilities at a rapid rate. In the same way that an attacker may be able to leverage both the network functionality and device capability of the elements within an OT environment, the forensics investigator should be able to use those same types of technologies to aid in an investigation. The analysts should also have the capability to pull project files and logic information from the field devices, hash it and compare it against known and validated files.

- **Order of Volatility** – This is an approach to collect data based on what valuable data is most likely to be changed or deleted first. However, the order should be flexible. For example, system memory is much more volatile than the hard drive, but it should be prioritized first if valuable data is about to be changed on the hard drive. A general order of volatility can be cache and register content; network data; memory; system processes; temporary filesystem; data on a hard drive; remotely logged data; and archived media data.
- **Collection methods** – The collection process should be documented. Automation scripts can be beneficial in saving valuable time and decision-making throughout the process. The data must be hashed and secure to ensure its integrity and existence.

- **Local Versus Remote collection** – The remote approach for collecting data is mainly reserved for continuous and routine collection, as described in step A.2. Although it can also be used during the Incident Response, a local approach is preferred in this step unless there is no other option. In this step, the IRT needs to collect a large amount of data like hard-drive images, demanding a lot of bandwidth for remote collection. Moreover, some valuable data exists only on-site, like standalone computers and visual observations.

  Some key elements are critical to the OT operation, and it is assumed that they cannot be taken offline for forensics analysis. However, although the ad-hoc interaction with the system can cause some risks, sometimes this would be a recommended approach to analyze them locally. Because if these technologies are involved in the actual attack, the current state, process, and connection status can greatly empower the forensics investigator. Due to the real-time requirements for OT operations, acquiring real-time information about the incident activity is critical. In these cases, the proactive incorporation of real-time forensics aids may prove very useful to the investigator [9].

  All the collecting tools should be tested on an emulation system in a lab environment before use in the OT environment. The collection must be coordinated with the local engineers or operators, and it is better to have someone present to witness the actions. If time permits, all possible data should be collected. It is recommended to take pictures of valuable spots in the system, such as the PLC cards status. Specifically, anything on the screen, such as command prompts or files, should be photographed, as it could benefit later analysis.

- **Capture kit** – The DFIR Team should have a well-defined list of Forensic data sources and a detailed procedure to collect them during an incident. The necessary collection resources should be prepared [7][8], such as workstations, backup devices, blank media, notebooks, a chain of custody forms, storage bags, digital cameras, etc.

  Because installing digital forensic tools on the local OT workstations is complicated and sometimes not allowable, it is advised to consider using clean, approved, and tested bootable USBs. USBs allow digital imaging software to be run directly from the USB instead of installing software on the victim machine. However, it is a USB and thus may not be allowed in an OT environment. In addition, USBs on a system create new registry key values and can spread infection. If using a USB drive, it should be a one-time device.

- **Technical aspects** – The workstation should match the expected load, and the necessary storage should be calculated. According to the permissions, the access should be direct or securely remote such as SSH. Furthermore, the operating system should be hardened. And last, the

capture platform's clock should be accurate and synchronized to a trusted source.

- **Best practices for Forensic data handling** –
  - Define a workflow to allow forensic data of different types to be looked at by those with relative skill sets.
  - Document all forensic data with a digital hash and a short description.
  - Have a central database to "check out" forensic data to ensure that multiple people do not work on the same piece.
  - Have the central database the capability to upload notes and detection signatures/IOCs to go with the forensic data.
  - Never work from the original data file; always use a copy.
  - Have a plan and database to store previous analyses securely.
  - Describe the chain of custody – A process that tracks the movement of artifacts through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the artifacts, the date/time it was collected or transferred, and the purpose for the transfer.

D.5	IRT	Digital Forensics

- **Background** – After the supplementary data collection step, the IRT should be focused on Digital Forensics by using 'timely analysis' methods. Their purpose is to empower the situation assessment team to understand the scope of the incident so they can make decisions about the safety and operation of the OT system.

  The analysis at this point should be thorough enough to answer the situation assessment team's questions, such as how did the system become infected? What systems are affected by the malware? Does the spread of the malware continue? What is the malware's interaction with the system and the operators? How the malware affects the operation? Has data been leaked out? And so on.

  The analysis is not intended to understand exactly how the malware works, how its code is written, and who the adversary is. These questions can be addressed later in the advanced forensics step at the post-incident phase.

  The Incident Response Team should cooperate with the SOC analysts and use them as their scouts. This team supposes to hold valuable fundamental data such as asset identification, network map, traffic PCAP, security logs, etc. Identifying differences in current network traffic and flow data compared to the known baseline is an effective way to identify threats quickly. The IRT conclusions can be passed back to the SOC to establish IDS rules and focus on identifying new and reoccurring infections.

- **Goal(s)** – Detect the incident's root cause and its effects on the system.
- **Who** – The Incident Response Team.

- **How** – Below are some Digital Forensics methods that can be used during the Incident Analysis and Response phase in the OT environment. This is not a step-by-step process but a list of tools and techniques to use as needed in a 'Timely Analysis' form.
    - **Basic 'Timely Analysis' methods** –
        - **Baseline Comparison** – The baseline of a system is a database that contains asset and software inventory, network flow data, logs, files, hashes, etc., which represent the system operation at standard conditions. Such a database can drastically reduce the effort and time needed for Incident Response to figure out the event. Of course, these databases must be taken and prepared long before an incident occurs.
        - **Whitelists** – This approach is based on a list of digital signatures representing the system's valid files and processes. These lists enable analysts to ignore known-good files and software quickly. Pre-incident create and maintain a whitelist of digital hashes to make Incident Response faster and spot threats.
        - **Indicator Of Compromise** – IOCs are great tools to identify known threats. These are lists of rules that describe various parameters and behaviors about a threat. IOCs should be developed according to information from threat intelligence and previous incidents. SOC analysts can use IOCs to design and implement IDS signatures. After creating the IOC, it is important to test it against known-bad and known-good samples to ensure it works as anticipated.
        - **Initial Attack Vectors** – The starting point for analyzing and understanding a threat is generally its initial attack vector. Initial attack vectors could include spear-phishing emails, exploitation of external websites, direct internet connections to control systems, and abused trusted networks and connections between other networks, such as a vendor or corporate networks. Analyzing how a threat initially infected the ICS can drive remediation recommendations and can help identify and eliminate the vulnerability to reduce the chances of reinfection.
    - **OT Components**
        - **Project files validation** – Any adversary who wants to manipulate a system's process or cause damage may have to manipulate the system logic or project files. Project files may contain the running firmware, the control application (commonly called Control-logic), the physical process state information measured through the input from sensors and output to actuators, operational configuration data, and event logs. The most basic analysis includes the ability to pull the files from the various system components, hash them and compare their signature to a separate and secure repository that has been prepared ahead of time. This capability requires familiarity with the software tool that the

equipment's vendor provides with the hardware. Typically, these tools can compare project files and detect differences within the logic.

- **Logic-Field Interactions** – After validating the project files integrity, the next level is to in-dept analyze the interactions between the PLC logic, the HMI indications, and the physical facility itself. That level of analysis requires a very good understanding of the physical process and the program that runs this process, and it must be done by OT engineers while supported by the facility operators. The best way to analyze this interaction is to do it locally while connecting to the system in real-time. That, of course, can only be done if the system is running and under strict safety supervision. Alternatively, the analysis can be done offline in the forensic lab, but a real value will be achieved if the lab is equipped with a simulator or emulator of the system and the process.

- **Network Traffic Analysis** –

  - **Full Network Traffic Analysis** – Manual Analysis of the full network traffic PCAPs can be very challenging due to the amount of data. A basic analysis could be done by several open-source tools, but in order to get a details analysis, a deep packet inspection tool such as IDS will be required.

  - **Using NetFlow for network traffic forensics** – A NetFlow is a statistical summary of traffic observed at a point in the environment with common attributes, including source/destination IP addresses, protocols, source/destination ports, start and stop times, data volume, and the ingress network interface.

    - NetFlow allows an analyst to investigate network traffic of interest at a rate many orders of magnitude faster than possible when parsing PCAP files. NetFlow also provides a single means of searching all network traffic, regardless of protocol. Another excellent use case for NetFlow analysis is encrypted communications. In this case, NetFlow is invaluable since it is a record of the connection without its respective content.

    - An efficient analysis can quickly identify many conditions worth further attention, such as highest-volume IP addresses, subnets, or protocols; Most common or heavily trafficked network communications; Communications with known-bad IP addresses identified by threat intelligence sources; Erratic traffic spikes in terms of packet count or volume.

  - **OT Protocols** –

    - **TCP/IP-Based Protocols** – Network communication protocols in OT systems are characterized by unique structures that are sometimes based on standard protocols and sometimes on

proprietary protocols. Many vendors use a known public protocol such as Modbus TCP for communication between the PLC and the HMI. But above that, they have created a proprietary protocol for communication between the software development tool and the PLC to edit the PLC logic and configuration. Some of these protocols have not been developed based on security considerations and do not require identification and permissions to send commands to the PLC. Although many monitoring tools today allow for a good level of automated analysis of these protocols, an in-depth understanding of these protocols by the IRT is critical for Digital Forensics and incident investigation.

- **Serial communication** – Legacy system components and sometimes even new components may use serial communication protocols. The analysis approach to investigating what is happening in these communication methods can be complicated. One way to investigate serial communication is by using communication adapters capable of converting serial communication to TCP/IP-based communication. This will allow the analyst to use all the other methodologies that this section deals with. Another approach is to use a serial tap to allow monitoring serial communications between two devices that do not have an OS like Windows or Linux.

- **Field-Level anomaly analysis** – Another approach to dealing with systems based on serial communication or even IP-based communication but based on proprietary protocols is analyzing the system's physical input/output behavior. Some tools can measure the electrical signals of these I/O ports to build a system profile and detect anomalies in the system behavior regardless of the network communication above. Like many other forensic capabilities, these tools should be installed in the system long before an incident occurs. The system profile creation quality is related to the time period the device learns the system.

- **Logging Protocols** –

  - **Challenges** – There are a few challenges with logging aggregation and analysis which emphasize the need for a well-defined strategy to deal with all the data:

    - There are several standard logging protocols, such as Syslog. The difficulty is that every application/system component may send different messages that require parsing and analysis to interpret.

- Many devices do not have any form of persistent storage available. Therefore, log data is stored in memory. When the allocated memory is filled, old log entries will be purged from the buffer, lost forever. Also, log data will be lost if the device is powered down/rebooted.
- When thousands of systems in an environment maintain their log storage, the investigator's job becomes incredibly difficult.
- Most attackers are aware that the systems they compromise are logging some or all of their activities and actively seeking to scrub logs or remove them entirely. However, a log aggregation solution simultaneously records those log entries to multiple locations. Unless the attacker knows this and also compromises the log aggregators, there will be duplicate records of their activity. This becomes especially useful when an investigator discovers a disparity in the on-system and the aggregated logs- it can indicate what an attacker wanted to hide.

- **Syslog** – Syslog is a log aggregation mechanism for UNIX/Linux-based machines. The protocol receives log event messages and delivers them to one or more destinations according to its configuration file. Those destinations could be files, other applications, or other systems on the network. The protocol defines how the data is structured and delivered on the wire. Maintaining durable log data is a critical component of a proper security investigation as it serves as a partial transcript of past events.

  Most core OT networking equipment such as PLCs, routers, switches, intrusion detection systems, firewalls, and wireless access points can send log events to another host using the Syslog protocol. Moreover, many hardware devices provide options to use the Syslog protocol for off-system monitoring. This group includes storage devices, video surveillance cameras, alarm systems, motion detectors, and more.

  Even though Syslog was initially designed for UNIX-based devices, Windows systems can also push proprietary log messages to a Syslog destination through third-party service software. That provides a common logging platform for such a wide variety of source devices.

  Log aggregation platforms such as Security Information and Event Management (SIEM) can receive Syslog messages from the network. These platforms also can parse and digest Syslog messages and run a wide range of queries to analyze them.

- **Windows Logs** – Since the first release of Windows NT in 1993, Windows shipped with a core logging capability that remained in use until 2007. Even though the platforms using this framework are past Microsoft's end-of-life, they still can be found in OT environments.

Windows Logging platforms include three main log files. First, the System log contains details about system components such as drivers and services. Second, the Application log includes items from programs running on the system. And third, the Security log contains entries regarding login attempts, file accesses, deletions, etc.

New frameworks also added two new core log files. The Setup log contains events related to software installation processes, and the Forwarded Events log includes items that have been collected from other Event Logging sources. Individual applications and services also can create log files within the logging framework.

- In the OT environment, many of the workstations in the system are Windows-based machines. Therefore, these logs can be beneficial for analyzing data from PC workstations, such as HMI, Historians, Engineering, etc. Because the Syslog protocol is so deeply entrenched in the IT sector and OT, sometimes the easiest solution is to implement a bridge that converts Windows Logs to Syslog messages.

- **Firewall Logs** – A firewall may be the single most useful tool for both defensive posturing and Incident Response. They are deployed widely and almost universally support robust logging. In addition, their typical placement at strategic points on the network provides excellent vantage points for traffic monitoring and eventual blocking. In most cases, adversaries tend to get into firewalls before finding the service or vulnerability they need to start attempting access. Even the most skilled attackers must conduct a proper reconnaissance on their targets before launching an exploit that commences the more tangible phases of an attack. By identifying what ports and protocols were targeted during reconnaissance, it is possible to establish a clearer picture of the attacker's intent and capabilities. When this reconnaissance is performed through automated tools, an investigator can establish a profile for the attacker, possibly correlating such activity to other events that have been logged throughout the environment or broader security community.

  - **During the incident** – Investigators can create rules that log traffic but still allow it to pass through unimpeded. This allows critical forensic data gathering without compromising the operational security of the investigation.

  - **After the incident** – Firewalls can transition to log and block known malicious traffic. This configuration will help minimize an attacker's access to the victim's network and provide useful intelligence about their actions. At this stage, it is often useful to combine these block actions with a wider log-and-allow net to try and identify whether the attacker still has access to the network using previously unknown mechanisms.

- **Malware Analysis** – The purpose of malware analysis is to manipulate the threat to gain as much information as possible about it in a 'timely' manner. It helps to identify valuable information to protecting systems, such as the

discovery of vulnerabilities, and it allows analysts to understand the tactics, techniques, and procedures of the adversary.

- **Antivirus scans** – After suspect files have been extracted, it is useful to examine them with antivirus on isolated machines. The importance of doing this is to keep the forensic analysis secret. OT attacks are more likely to be new, advanced, and impactful, submitting online alerts to the adversary. Running copies on isolated systems ensures that the forensic data is not destroyed and can return valuable information. It is also better to use more than one AV machine, which is known as having an antivirus farm.
- **Static Analysis** – These types of information can be gathered without executing the malware. It is the quickest way to get useful information, but it does not reveal as much as the other forms of analysis. For example, a digital hash is a static property of a file, detecting if the file is packed. In addition, Portable Executable (PE) file formats can give information on data and compilation time and information about functions imported or exported by the file to the system. This method can be useful for quickly creating IOCs or establishing blacklists.
- **Dynamic Analysis** – Interactive behavior analysis is the process of executing malicious files and observing their interactions on the system, including processes recognition; files modified, created, or accessed; registry keys manipulated; network traffic; and so on. Tools such as those that examine running processes and services, automate data collection through pre-compiled scripts or programs, bit copy processes, or generate checksums for complete and total image verification can be helpful for this type of analysis.

D.6	IRT	Response

- **Background** – In this step, maintaining and restoring operations activities should be done. These activities are based on three common categories: containment, eradication, and recovery. The order of activities in these categories does not have to be serial and will be determined by the incident managers according to its specific details.
- **Goal(s)** – Contain the incident, eradicate the threat, and recover the system.
- **Who** – The Incident Response Team.
- **How** –
  - **Containment** – It may be necessary to make changes in the system as part of the response actions. It is critical to prepare for any environmental manipulations well before an incident; nothing should occur to the environment without proper planning and testing ahead of time.

- **Physical changes** – Hardware type changes may include architecture changes, device, part replacement, etc. Almost any hardware change may also require configuration and software adjustments.
- **Logical changes** – Logical network changes can be made at switches, routers, and firewalls to enable MAC or IP filtering, port security, or other policy enforcements. Another type of logical change includes program changes in PLCs or HMIs and workstations updates/patches. These changes must be done in coordination with the operators and after a risk assessment.

- **Eradication** – Eradication occurs when the threat and all its traces are removed: Delete rootkits, remove viruses, clean manipulated Registry keys, and so on. It is more likely that to eradicate threats, personnel should reimage systems, reinstall programs, and reconfigure them. It is also a good practice to perform vulnerability scans and assessments as a complementary action.
- **Recovery** – Restoration occurs in traditional Incident Response when the systems that were contained or removed from the network are brought back online and into production. There are a few key things to note: testing is a requirement for restoring systems; ensure that system architects and engineers are doing the restoration/testing and that personnel expects a chance for the system to fail or not restore properly. It may be best to keep certain systems that were contained or segmented from the network in that status if it still supports normal operations.

D.7	MGT	Continuous Situation Assessment

- **Background** – This step is about a continuous situation assessment which goes hand in hand with the digital forensic and response team's actions. The reason for that goes back to the motivation for this framework. As mentioned above, the technical steps of the traditional Incident Response method cannot always take place one by one in a serial process as they may occur in IT systems.

  In the case of OT systems, there is a need to reassess the next step with every action done in the system. Every system has its risks, constraints, acceptable downtime, etc. There may be enough time to detect the threat before performing response actions in some cases. In other cases, containment and eradication will occur before the detection is done completely. Therefore, the activities of the IRT must feed the situation assessment meetings, and the MGT should make decisions for the following actions to come.

  Another decision to make by the situation assessment team is when and how to end the incident. Ending the incident doesn't necessarily mean answers to all the questions. However, it does mean that the situation is under control; there is enough knowledge to estimate whether it was a cyber incident, and the next steps can be calculated. Sometimes, moving forward into a supervised routine is just a managerial decision and not a result of solving the incident. That allows the facility and the people to go back to some level of operation.

- **Goal(s)** – Guide the response team, declare the type of incident and severity level, and decide on actions to follow.
- **Who** – Management as the leader, facility representative, cyber analyst, OT engineer, and any other stakeholder.
- **How** –
    - **Situation Assessment** – Example considerations:
        - Have all the required forensic data been collected?
        - Is there stability in the level of control over the facility?
        - Has the spread of the incident been identified to additional facilities?
        - Are there any backups available that can be put to work?
        - Is it possible to stop the production processes in the facility?
        - What is the business impact of the event?
        - Is there a public impact that requires coping?
        - Does an understanding of the causes of the event become clear?
        - Is it possible to return the facility to production in parallel with the forensic analysis?
    - **Decision** – The decision in this step is when and how to end the incident.

D.8	MGT	Communication: Cyber Incident

- **Background** – A cyber incident is characterized by uncertainty, frustration, and stress for many people. One of the teams' goals in the incident management is to deliver updates and provide simple answers to outside officials who are not necessarily proficient in the professional technical meanings.

  This announcement comes to complete the previous statement. After the last report declared a situation of suspicion of a cyber incident, in that case, this statement should give a slightly more accurate description and explain whether it was indeed a cyber incident, the known details, and the actions to follow.
- **Goal(s)** – Declare the status as a Cyber Incident.
- **Who** – Management representative.
- **How** –
    - **Report** – Each organization should have a preprepared list of stakeholders who need to be informed about the incident state for each severity level. These stakeholders could be internal and/or external to the organization.

      The report should include at least the following details: The incident state, severity level, chain of events, current risks, and actions to follow.

D.9	MGT	Move to END?

- **Background** – This step is the decision point of step D.7.
- **Goal(s)** – Decide when to end the Incident Response process and move forward.
- **Who** – MGT.
- **How** –
    - **Decision** – The decision at this step will either recommend ending the incident or keep going with the Incident Response process.

4.2.5. End of Cyber Incident

This phase includes steps to perform during the end of the incident. The main actions include drawing lessons, summarizing the events, and deciding how to operate the facility for the coming period.

E.1	MGT	Communication: End of Cyber Incident

- **Background** – If the incident management team has decided that it is time to end the incident, even if there are no answers to all the questions yet, this statement should be stated clearly. This announcement will allow facility managers to prepare for a return to production in the form of a supervised routine.
- **Goal(s)** – Declare the status as an end of Cyber Incident.
- **Who** – Management representative.
- **How** –
    - **Report** – This announcement will be made similar to previous statements. The report should include at least the following details: The incident state, severity level, chain of events, current risks, and actions to follow.

E.2	MGT	Recovery Assessment

- **Background** – At the end of the incident, the management team must decide how to return to production and what actions to take during the supervised routine. For example, this assessment can decide to delay the recovery actions from the 'Cyber Incident Analysis and Response' phase to the 'End of Cyber Incident' phase within this framework.
- **Goal(s)** – A decision on how to return the facility to a production state and actions for the supervised routine.
- **Who** – Management as the leader, facility representative, cyber analyst, OT engineer, and any other stakeholder.

- **How** –
    - **Situation Assessment** – Example considerations:
        - Is the system in safe mode and under control?
        - What changes have been or will be made to the system?
        - What level of supervision is required, and for how long?
        - Are any necessary operations in other systems as a result of the event?
        - What changes need to be made in the layers of security?
        - What will be the conditions for returning to a full routine?
    - **Decision** – The decision in this step will be the following action to perform at the end of the incident and later on.

E.3	IRT	Lesson Learned

- **Background** – From any such incident, one can learn something which will help strengthen the layers of protection for the next time. This step is when the response team should summarize the conclusions raised during the incident and draw lessons as a basis for further decisions.
- **Goal(s)** – Summary of the conclusions and lessons learned from the incident.
- **Who** – The Incident Response Team.
- **How** –
    - Lessons learned are more specific than information sharing. Information sharing is everything relevant that might be useful to people inside or outside the organization. Instead, lessons learned are meant to highlight best practices and things that did not go according to plan and can be used internally in the organization. The IRT should document findings and pass information to the SOC and engineers to watch for reinfection and strengthen the defense.

E.4	IRT	Final Report completion

- **Background** – Upon completion of this step, the IRT should summarize all the incident details and complete the draft report, which started to be written in its early stages.
- **Goal(s)** – Providing a final report to summarize the incident.
- **Who** – The Incident Response Team.
- **How** –
    - **Report Content** – The report should be written clearly, concisely, and fact-focused. It should include at least the following topics: The chain of events, technical inspection results, basic cyber analysis results, current risks, the forensic action made during the incident, the results, conclusions, and decisions to follow.

4.2.6. Post-Incident

The last phase of the framework includes activities that should be done after the incident. Since there is never a 100% certainty that the incident was over in the cyber field, there must be a period to run the system under a supervised routine. During this period, the conclusions from the incident must be applied, the lessons learned should be published, and an optional advanced forensic can be made.

F.1	SOC + FCR	Supervised Routine

- **Background** – This is when the system needs to operate under closer supervision than usual. The supervision of the system should come from both the operating and the cyber monitoring center. This period is necessary because the assumption is that not all the components have been cleared. The summary report should clearly define the actions required during this period, the person responsible for each task, and the performance schedule. After this period, the system will resume operation in a completely routine.
- **Goal(s)** – Implement the decisions regarding operating the system during the supervised routine period.
- **Who** – The SOC analysts and the FCR operators.
- **How** –
    - **Implementation** – Each decision should be clearly defined, along with the person's name in charge and a timetable for execution. The network should be monitored for reinfections. The incident responder's ability to pass off appropriate information to the advanced forensic team and back through threat intelligence consumption and into the hands of the SOC personnel ensures that follow-on analysis is accurately done.
    - **Supervision** – Periodic work meetings are required to monitor the task's progress. At the end of the period, a report must be issued summarizing the status of the actions performed to confirm completion formally.

F.2	IRT	Advanced Forensics

- **Background** – The digital forensic actions performed during the Incident Response are based on the 'timely analysis' principle. In the post-incident phase, there is room to perform advanced forensic procedures. Of course, these actions will be taken if necessary and if the organizational capabilities exist to support them. These operations may include an in-depth investigation of files, processes, and even reverse engineering operations.

  Advanced forensics can lead to gaining information such as IOCs for SOC monitoring and Incident Response. Malware should be understood and manipulated to identify routines, deactivation commands, or weaknesses. For example, identify weaknesses such as automated scanning or hardcoded IP addresses/passwords. This information can also be shared with others in the form of threat intelligence.

- **Goal(s)** – Gaining in-depth information about the threat will help straighten the defense and detection capabilities:
    - Determine the nature of the threat.
    - Extract valuable information for SOC analysts.
    - Identify the IOCs of the malware to help Incident Response.
    - Understand the malware's tactics to identify weaknesses in the current architecture of the OT.
    - Identify valuable information in contributing to community knowledge.
- **Who** – The Incident Response Team or a dedicated Forensic Team.
- **How** –
    - **Pre considerations** – In this step, the interaction would probably be with a real threat, which means that at some point, an actual malware will be run in an environment. Therefore, the threat must not be manipulated in the production environment, even if it is possible to neutralize it. Also, malwares can have safeguards to active unknown routines such as self-destruction, data-destruction, or sending back data to the adversary. Therefore, as described in Section 3.2, a safe working environment is essential for this process.
    - **Memory Forensics** – Because everything has to go through memory, it is an extremely viable source of forensics data. Instead of hunting the entirety of the physical disk looking for malware, it is possible to analyze memory and see the malware running. Memory decays quickly and loses its value when not powered; if a system is shut down or restarted, the memory value is destroyed. Because memory is so volatile, it displays only recent information about a system. Obtaining information from multiple weeks ago is not often practical.
        - **Memory-Only Malwares** – One of the advances in malware is to create memory-only malware. The malware does not install files, manipulate Registry keys, or otherwise interact directly with the physical system; it lives entirely in the virtual memory of a system. One of the most significant weaknesses in memory-only malware is the inability to survive a reboot. It is not useful in IT environments; however, OT environments do not usually have frequent reboots of systems, making memory-only malware worthwhile.
        - **PLC memory forensics** – Memory analysis of PLCs can help answer important forensic questions about the attack, such as the presence of malicious firmware, injection of modified control logic, and manipulation of I/O devices. However, PLCs have heterogeneous hardware architecture, proprietary firmware, and control software, making it challenging to employ a unified framework for their memory forensics. Recent studies, such as [10], are trying to find a generic framework to analyze PLCs memory regardless of type and vendor by following a methodology that focuses on the functional layer of PLCs

instead of reverse-engineering the firmware applicable to all PLCs. By employing a sequence of planned test cases and analyzing the resultant memory variations, a memory profile can be generated comprising a set of rules to extract artifacts from a memory dump. The profile generation task includes identifying data structure definitions, searching data structure instances in a memory dump, and formulating the rules.

- **Advanced Malware Analysis** – Malware analysis involves interacting with and understanding malware and is often identified as Reverse Engineering Malware (REM). The ability to perform malware analysis drives the development of threat information, such as IOCs and context key to internal threat intelligence and actionable information for network security monitoring and Incident Response.
  - **Manual Code Reversing** – Manual code reversing is the manual examination of the code through decoding it, deconstructing it, and analyzing the functions and capabilities of the malware. Lots of useful information can be gained this way; this is the only way to consistently understand all the capabilities of a piece of malware, but it is time-consuming. Manual code reversing requires a debugger and a disassembler. The Disassembler takes the binary files and translates them into "human-readable" assembly code. The Debugger helps step through that disassembled code to understand what is inside it.

F.3	SOC + FCR	Implementation of Recommendations

- **Background** – This step deals with implementing decisions that must be made immediately after the incident and which are not necessarily related to the period of supervised routine. These decisions may include installing updates, changing security settings, changing procedures, and more. Of course, these decisions are also required to appear in the incident summary report.
- **Goal(s)** – Implementing decisions for hardening cyber defense.
- **Who** – The SOC analysts and the FCR operators.
- **How** –
  - **Implementation** – Each decision should be clearly defined, along with the person's name in charge and a timetable for execution.
  - **Supervision** – At the end of the implementation, a report must be issued summarizing the status of the actions performed to confirm completion formally.

F.4	IRT	Raising Awareness

- **Background** – The last but not the least important step is to increase organizational awareness of cyber issues. Conclusions and insights that emerged from the incident, which are not very technical in nature, should be shared with the employees in the

organization. Conclusions that can affect procedures and work processes, procurement processes, and external relations can significantly help prevent and deal with the next incident.

- **Goal(s)** – Sharing knowledge and conclusions that emerged from the incident.
- **Who** – The Incident Response Team.
- **How** –
    - **Sharing** – Knowledge sharing can be done in any way that suits the organization. Platforms, for example, can include a corporate website, newsletter, refinement of procedures, seminars, courses and training, and more. The important thing is that the information is accessible, usable, and straightforward.
    - **Type of Audience** – Although most of the information should be shared with all employees in the organization, some can be shared with more limited groups. Understanding these audience types and what they need helps drive the goals of the shared information.
    - **Type of Information** –
        - **Strategic Information** – This information can be used to brief executives and decision-makers at the strategic level. This can include organization-wide decisions, changes in goals, resource investments, etc.
        - **Operational Information** – This can serve as a decision on staffing and training requirements for the security team, refinement of procedures, etc.
        - **Tactical Information** – This type of information can be useful for external members of the OT, who are also doing day-to-day security defense. Identifying adversary TTPs, IOCs, and other types of information that can be quickly used for security purposes.

References

[1] Paul Cichonski, et al., NIST SP 800-61r2, Computer Security Incident Handling Guide, August 2012, https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

[2] Keith Stouffer, et al., NIST SP 800-82r3, Guide to Operational Technology (OT) Security, July 2022, https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final.

[3] Robert M. Lee, The Sliding Scale of Cyber Security, August 2015, https://www.sans.org/white-papers/36240/.

[4] Robert M. Lee, ICS Active Defense and Incident Response, 2018, SANS Technology Institute.

[5] Lewes Technology Consulting, LLC and Mat Oldham, Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, 2019, SANS Technology Institute.

[6] Kent Karen, et al., NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, August 2006, https://csrc.nist.gov/publications/detail/sp/800-86/final.

[7] Derek Banks, Custom Full Packet Capture System, February 2013, https://www.sans.org/white-papers/34177/

[8] Gordon Fraser, Building a Home Network Configured to Collect Artifacts for Supporting Network Forensic Incident Response, September 2016, https://www.sans.org/white-papers/37302/

[9] Mark Fabro, Eric Cornelius, Recommended Practice: Creating Cyber Forensics Plans for Control Systems, August 2008.

[10] Muhammad Haris Rais, et al., Memory forensic analysis of a programmable logic controller in industrial control systems, Forensic Science International: Digital Investigation, April 2022.

Appendix A: Acronyms and Abbreviations

AD Active Defense

ARP Address Resolution Protocol

AV Antivirus

CD Compact Disk

DFIR Digital Forensics and Incident Response

FCR Facility Control Room

FMT Facility Maintenance Team

GPS Global Positioning System

HMI Human Machine Interface

ICS Industrial Control System

IDS Intrusion Detection System

IO Input Output

IOC Indicators of Compromise

IP Internet Protocol

IRT Incident Response Team

IT Information Technology

MAC Media Access Control

MGT Management

NTP Network Time Protocol

OEM Original Equipment Manufacturer

OPC Open Platform Communications

OS Operating System

OT Operational Technology

PC Personal Computer

PCAP Packet CAPture

PE Portable Executable

PLC Programmable Logic Controller

POC Point Of Contact

REM Reverse Engineering Malware

RTU Remote Terminal Unit

SATA Serial Advanced Technology Attachment

SIEM Security Information and Event Management

SOC Security Operation Center

SSH Secure Shell

TAP Test Access Point

TCP Transmission Control Protocol

TST Technical Support Team

TTP Tactics, Techniques, and Procedures

UDP User Datagram Protocol

USB Universal Serial Bus

VLAN Virtual Local Area Networks

VM Virtual Machine

VPN Virtual Pritave Network

Appendix B: OT DFIR Framework – A suggested small-scale organization implementation

The OT DFIR framework described in section 4 is primarily suitable for large-scale organizations. These organizations are often characterized by a volume of resources that allow them to possess dedicated professionals for a wide range of roles related to the OT systems. However, this relative advantage brings a challenge in managing the interfaces between all stakeholders during cyber incident handling, one of the challenges that the framework described in this document attempts to solve. Obviously, not all OT organizations are large-scale organizations, and the complete OT DFIR framework might be too detailed for them. For that reason, this appendix suggests a small-scale organization implementation for the framework.

As shown in **Fig. 4**, there are three main differences between the two frameworks. First, small-scale organizations are characterized by a relative lack of resources, which means that one staff member may perform various roles. For example, the OT engineer may also serve as the cyber OT engineer and cyber analyst. In addition, the facility itself may not have dedicated maintenance personnel. And, there may not be a dedicated cyber monitoring center or control rooms. Therefore, the short framework does not include each step responsible (Who) but only the action performed at that step (What). The definition of responsibility was left to each organization to determine for itself.

Second, since it can be assumed that the same persons will perform the initial technical response, phase number two and phase number three of the complete framework were consolidated into one phase. The main emphasis at this stage is to preserve the principle of examining technical events from some level of cyber perspective. This extended analysis can be done by looking at the IDS or keeping and collecting artifacts for further investigation.

And third, to simplify the framework, some of the steps were omitted under the assumption that they would be a part of other main steps. For example, the opening and closing of a ticket should be part of the first technical inspection and the ending of the incident phase. In addition, a situation assessment should be part of each decision point. For that reason, the index pointers of each step have not been included in the short framework.

Finally, this appendix is not replacing the need to read the entire document. The reader should be familiar with the complete framework and all the detailed actions in each phase and step. Moreover, as the title emphasizes, this is only a suggested framework implementation. Different organizations may find other framework customizations for their unique needs, characteristics, and constraints.

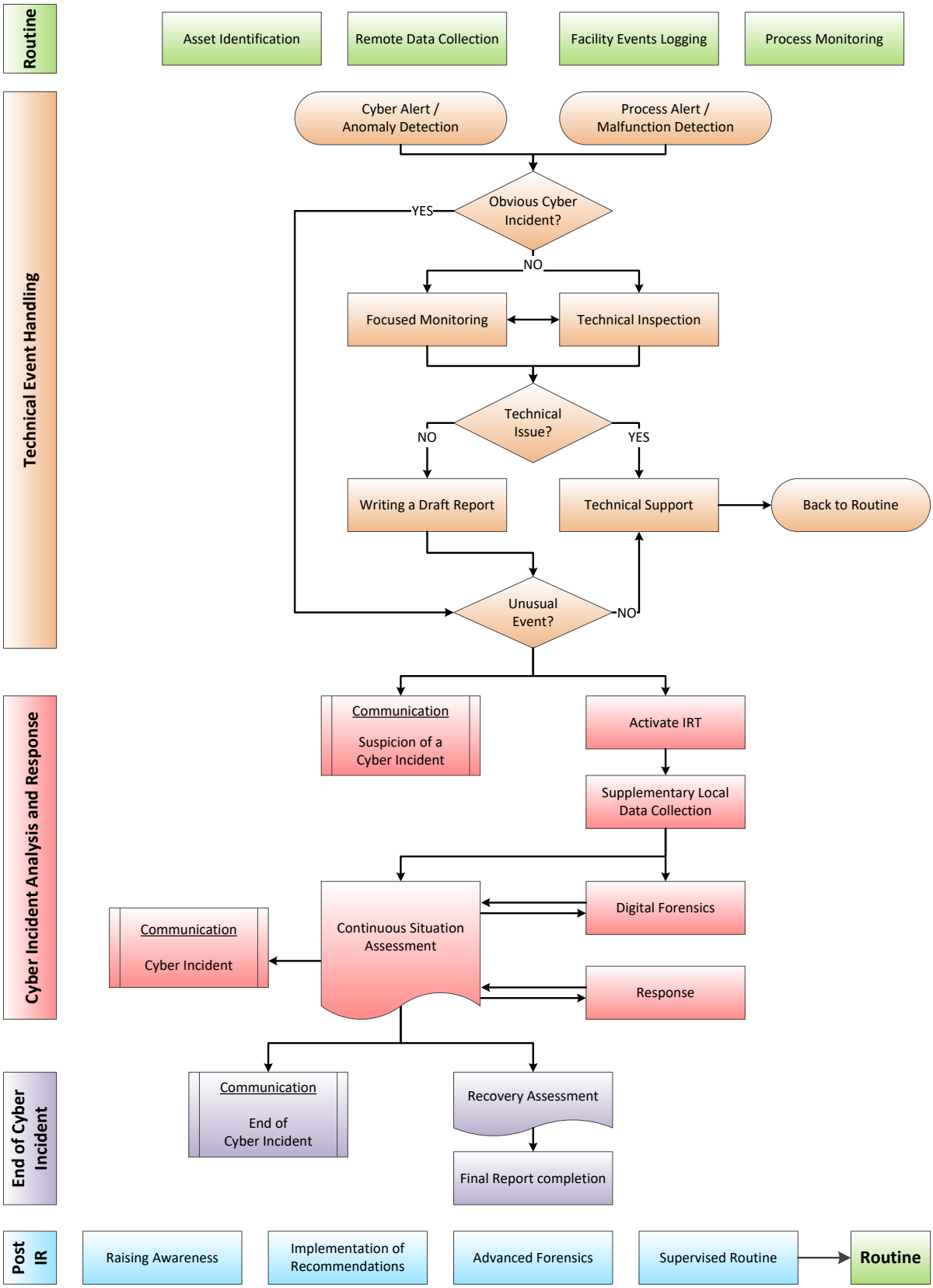


Fig. 4. A suggested small-scale organization framework implementation