WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Incident Response for Operational Technology (OT)

Preparing for and Responding to OT Security Incidents in Industrial Environments

TIM ENNIS | SENIOR INDUSTRIAL INCIDENT RESPONDER
DANA-MEGAN ROSSI | SENIOR DIRECTOR OF GLOBAL SERVICES
KAI THOMSEN | DIRECTOR OF GLOBAL INCIDENT RESPONSE SERVICES
JACOB BENJAMIN | DIRECTOR OF PROFESSIONAL SERVICES
JAN HOFF | PRINCIPAL INDUSTRIAL INCIDENT RESPONDER
SETH ENOKA | PRINCIPAL INDUSTRIAL RESPONDER II
FAHAD ALQAHTANI | PRINCIPAL INDUSTRIAL RESPONDER

MARCH 2023

TABLE OF CONTENTS

Executive Summary 3

Introduction 4

The Convergence of Incident Response and Incident Management Principles 5

- What is Incident Response and Incident Management? 5
- Incident Command across the Globe – Communication & Coordination for IM 6
- OT Incident Response 7

Why is OT Incident Response Different than IT Response? 8

- Scope and Context 8
- Organizational Capability 11
- Priorities and Data Loss 12
- Different Data Sets for IT and OT 13
- Forensic Data Collection 15

How the Phases of Incident Response are Different Within Industrial Environments 16

- Preparation 16
- Identification 17
- Containment 18
- Eradication 18
- Recovery 19
- Lessons Learned 19
- Ownership of the PICERL Phases 20

How to Prepare for Effective Incident Response for OT 20

- Facilities 21
- Equipment 22
- Personnel 24
- Procedures 25
- Communications 32

Putting the Actions Into a Plan, and the Plan Into Action 34

Conclusion 34

Appendix A – Acronyms Table 35

Appendix B – Incident Response Preparedness Key Actions Checklist 36

Appendix C – Methodology for Creating and Developing a CMF 37

Appendix D – Incident Dashboard and Reporting Example 41

Executive Summary

Incident Response (IR) teams tasked with preparing for and responding to incidents in industrial environments face a unique set of challenges associated with Operational Technology (OT), largely focused on Automation, Industrial Control Systems (ICS) and SCADA systems. Some traditional IT (Information Technology) Computer Incident Response Team (CIRT) principles and actions can be applicable in industrial environments with some careful adjustments, while other traditional IT response actions and tools may be ineffective, inefficient, or even dangerous. That is why implementing an ICS-specific response plan is a critical step for incident response preparedness in OT environments.[1]

Dragos has distilled guidance and best practices for performing effective incident response for ICS based on years of collective experience, supporting OT defenders in both their cybersecurity incident preparedness and response efforts.

The recommendations are provided in detail within the **"How to Prepare for Effective Incident Response for OT"** section of this document, providing OT defenders with actionable items to implement in order to improve incident preparedness and allow effective response.

1 https://hub.dragos.com/guide/5-critical-controls

Introduction

OT defenders may be experienced in the preparation for and response to industrial incidents such as fire, loss of containment, and other hazardous situations that can arise in industrial facilities. However, few OT defenders have the same level of training and experience in cybersecurity incident response in industrial environments.

This whitepaper provides recommendations which OT defenders can implement relatively easily to improve their IR capability, regardless of whether the organization seeks to perform all IR activities internally, or with the assistance of external support such as a company like Dragos that can provide OT incident response specialists.

This whitepaper is divided into two main sections. It first provides an overview of Incident Response (IR) and Incident Management (IM) as well as the distinction between IT and OT IR concepts. Each phase of the Incident Response process is analyzed, and key differences highlighted. The second part of this whitepaper focuses on specific preparations operators and OT Incident Responders should perform to be effective when a response case is triggered. Appendices to this whitepaper provide material practitioners and managers can use to support the build-up and validation of IR procedures and effective foundations for IR activities.

The Convergence of Incident Response and Incident Management Principles

The terms Incident Response (IR) and Incident Management (IM) interchangeably when performing professional services for customers across different regions. It is also common for forensic analysis to be considered as the only component of Incident Response, or the only action that an Incident Responder takes. Forensic analysis can be part of incident response, although in OT environments a swift restoration of processes and mitigating dangers to life and environment often take precedence. Forensics usually is performed during root cause analysis later in the Incident Response process. However, reacting to and managing the incident requires much more, such as containing and eradicating an adversary from the environment and recovering to normal operations. Forensics may be part of those processes but is not always performed or necessary.

In OT environments, the term Incident Management predates cybersecurity and the unique challenges it poses. Conversely, the established practices for responding to hazardous situations may not be easily applied wholesale to tackle an OT cybersecurity incident.

What is Incident Response and Incident Management?

The National Fire Protection Association[1] provides a definition of Incident Management (IM):

> The combination of facilities, equipment, personnel, procedures and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

Breaking down each of the items in the list, it is easier to imagine the constituent parts of an Incident Management system and how it would be applied to different scenarios:

COMPONENT / SITUATION	FIRE	ON SITE CHEMICAL SPILL	CYBERSECURITY
Facilities	• Control center	• Spill kits • Eye wash stations • Control center	• Help desk • SOC • Forensics Lab
Equipment	• Fire extinguishers • Fire blankets • Risers	• PPE • Absorbent materials	• Security tools • Hard drive write-blockers • Evidence bags
Personnel	• Fire crews • Duty officer	• First aid team	• Analysts • DFIR specialists
Procedures	• Evacuation, muster	• Containment • Clean-up • Reporting	• IR plan • BCP
Communications	• Fire alarm • All clear • Call to fire brigade	• Emergency contact number	• Report an event • Comms to employees • Press releases

Table 1: Incident Management components for different scenarios

One distinguishing characteristic of OT incident response is the convergence of all the capabilities of IM with the ability to respond to a cybersecurity event. IM encompasses all parts required for operators, analysts, fire fighters and other stakeholders (i.e., the people), to perform incident response actions. Whether that means using a fire extinguisher, performing roll call at a muster point, donning Personal Protective Equipment (PPE) and laying oil spill socks, or analyzing Windows Event Logs on an Engineering Workstation. Therefore, it is important to consider all aspects of incident response, not just forensic analysis or tactical actions when building or improving an incident response function.

2 https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

Incident Command Across the Globe – Communication & Coordination for IM

Another key concept common to IM is the tiered approach for Incident Command. There are multiple examples of levels of command:

Incident Command System (part of U.S. National Incident Management System or "NIMS")	*The National Incident Management System (NIMS)*[3] is an approach to Incident Management communication and coordination used in the United States, applicable across government and private sectors with the intention of providing a common standard for incident management. Within NIMS, the Incident Command System (ICS) is an element of the command and management component, consisting of procedures for controlling personnel, facilities, equipment, and communications. It provides for coordinated decision-making and planning in the event of a national disaster or emergency.
Gold-Silver-Bronze	Predominantly used in the United Kingdom (UK), the Gold-Silver-Bronze command structure[4] is an incident command hierarchy for emergency services during major operations, with alignment to "Strategic-Tactical-Operational" command structures. The concept of roles within the command structure is for each role to be allocated according to skill, expertise, location, and competency.
GRIP	*Gecoördineerde Regionale Incidentbestrijdings Procedure* (GRIP), loosely translates to Coordinated Regional Incident-Management Procedure, and is the incident management system used across the Netherlands to measure the scale of an emergency and is used as a way of coordinating emergency services across the country.[5]
ICS4ICS	The ISA Global Cybersecurity Alliance and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) are leading an initiative to update the ICS (NIMS) framework to create the Incident Command System for Industrial Control Systems (ICS4ICS)[6] in order to develop an approach to guide companies, organizations, and municipalities for responding to cyber incidents affecting Industrial Control Systems.
Führungsstab[7]	An organizational setup for command in German firefighting, emergency/disaster response and military operation. Structurally like the other Incident Command Structure frameworks with multilevel, subject-specific sub-commanders. Can be deployed federated in case of major emergency situations or multi-site incidents.

Emergency services and OT operators are well versed in applying this concept and often have Incident Management setups that align with the concepts described earlier.

Examples include responding to storms, floods and other natural disasters, terrorist attacks, or an explosion or loss of containment event at an industrial facility. In these examples, there will likely be response efforts at local, regional, and state/government levels, requiring coordination of the IM components (facilities, equipment, etc.) with regular and clear communication up and down the levels of command.

3 https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013914/national-critical-incident-management-guidance-v13.0-ext.pdf

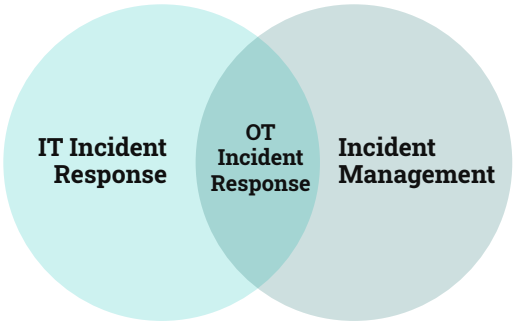
5 https://www.in-prep.eu/2019/04/10/getting-to-grips-with-grip-gecoordneerde-regionale-incidentbestrijding-procedure/

6 https://gca.isa.org/ics4ics

7 https://www.bbk.bund.de/SharedDocs/Glossareintraege/DE/F/fuehrungsstab.html

OT Incident Response

Situated within the IM frameworks described above exists the intersection of traditional IT incident response and industrial incident management.



IT cybersecurity specialists from a variety ofbackgrounds (financial, law enforcement, military, etc.) have extensive experience in responding to computer security incidents. Plant Operators and incident management specialists have extensive experience in preparing for, and in some cases are called to respond to, industrial incidents and realization of hazards. Where these two domains of specialization intersect is Industrial Incident Response, or OT incident response.

A key difference to contend with compared to pure physical events such as fire, flooding, or an explosion, is that in most of those situations the event is not actively fighting against or reacting to the responders' actions. Acting on experienced judgment developed from emergency planning and response requires some adjustments within OT incident response to make the right decisions and be able to get in front of the situation. This is especially relevant if an adversary is present and active in an industrial environment. Determining and understanding the root cause is the only means for responders to get in front of the situation, as described in the Dragos whitepaper, *Preparing for Incident Handling and Response in ICS*.[8]

There are many aspects of traditional incident management that are transferable and beneficial to effective OT incident response; notably the training and mindset for crisis management and the understanding of key concepts to scale-up and scale-down the resources required to manage an incident to conclusion. However, there are many aspects of industrial incident management which tend to require complementary skills such as digital forensics, analytical problem solving, and an in-depth knowledge of Industrial Control Systems and processes. OT operators may be required to utilize third parties during planning or incident response to fully maintain control over an incident.

8 https://www.dragos.com/resource/preparing-for-incident-handling-and-response-in-ics/

Why is OT Incident Response Different than IT Response?

There are many challenges, and potentially dangers, to applying standard IT response practices to an OT environment. The following paragraphs help to understand differences and how they must be considered when planning for and implementing Incident Response.

Scope and Context

Modern industrial control systems contain many components and services that are like enterprise IT environments such as Windows and Linux based workstations and servers, firewalls and switches. Often the environmental conditions for industrial devices require that the equipment is a ruggedized version, and the underlying functionality may appear to be the same as the IT equivalent. However, the key difference in the OT networks is the physical process that the equipment is controlling.

The functionality required from the equipment can be associated with key timing and scheduling of a machinery and valves, or part of a safety integrity loop. In fact, a common phrase used to describe the scope of OT is "all of the things in IT, plus physics." For this reason, different organizational requirements exist from a purely IT-focused incident, and the potential consequences of a compromise of an OT system are much more severe. Specifically, the difference between an OT compromise compared to an IT system compromise are the potential (real world) consequences,

Table 2: Potential consequences of OT system compromise

POTENTIAL CONSEQUENCE	EXAMPLES	CYBER INCIDENT EXAMPLE
Plant damage	• Damage to control system equipment • Excessive wear on final elements (such as actuators) • Over-pressurization of vessels and pipework • Fire or explosion	• TRISIS[9] • CrashOverride[10]
Loss of production	• Plant trips (opening of circuit breakers, activation of shutdown measures). • Manual shutdown of plant as a conservative decision. • Manual shutdown of plant due to loss of billing, production, shipping data from ERP systems.	• CrashOverride[10] • TRISIS[9] • Colonial Pipeline[11] • Norsk Hydro[12] • Honda[13] • Mariposa Botnet at Electric Utility (2012)[14]

9 https://www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/

10 https://www.dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/

11 https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

12 https://www.hydro.com/en-GB/media/on-the-agenda/cyber-attack/

13 https://www.bbc.co.uk/news/technology-52982427

14 https://www.cisa.gov/uscert/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

Table 2: Potential consequences of OT system compromise – continued

POTENTIAL CONSEQUENCE	EXAMPLES	CYBER INCIDENT EXAMPLE
Impact on product quality	• Contamination of product. • Changes to logic sequences. • Delay in sealing/packaging/chilling product.	• Oldsmar Water treatment facility attack[15]
Industrial safety event	• Loss of limb, livelihood, life to an onsite worker or member of the public • Exposure to hazardous substances	• No known public record of cyber-attack leading to injury or death of onsite worker or member of the public.
Environmental safety event	• Uncontrolled release to the environment • Discharge of untreated effluent • Loss of containment	• Maroochy Shire Sewage Spill[16]
Loss of system certification or assurance cases	• Uncontrolled changes to plant configuration baseline resulting in the requirement for recertification to • Company or regulatory standards such as current Good Manufacturing Practice (CGMP)	• No known public record of cyber-attack leading to direct suspension of a manufacturing license

The examples provided in Table 2 highlight the importance for incident responders to be experienced and familiar with the physical processes within an OT environment. Being able to understand, at least at a conceptual level, the physical process being controlled and monitored is imperative to being able to determine if an event observed from a digital asset could cause impacts on industrial equipment and thus the physical process.

A Note on Destructive OT Malware Analysis

TRISIS caused a trip of the plant's safety system, causing it to fail-safe to a shutdown state.

CrashOverride interrupted the flow of electricity in an electrical transmission network, and delayed recovery operations resulting in prolonged impact. The malware caused de-energization of transmission-level substations by continuously sending commands to open circuit breakers, and de-energizing electric lines and prevented system operators from managing the circuit breakers to re-energize the lines from control centers. This resulted in deployment of operators to local control points to perform manual operations.

The malware analysis performed by Dragos revealed that the intent of both pieces of malware, if implemented/executed as intended, was to cause damage to the station and its protective capabilities and therefore posed potential risk to the life of the operators.

15 https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/

16 https://web.mit.edu/smadnick/www/wp/2017-09.pdf

As described in the Dragos whitepaper, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*,[17] further analysis of the CrashOverride malware and other available artifacts determined that the malware included attempts to cause a functional Denial of Service (DoS) attack that would disable protective relay devices, coinciding with operators suffering a loss of view and loss of control on the electrical circuits and substations. The result would be protective systems being inhibited such that when services were restored, the restored electrical circuit would not be protected by protective relays, and therefore would not be in a safe condition, potentially resulting in physical damage.

Further analysis on TRISIS performed by Dragos[18] involving the understanding of Safety Instrumented System (SIS) operations and the specific implementation of vendor SIS at the targeted plant deduced that the malware sought to not just disable the SIS functionality, but to enable arbitrary modifications to the SIS operations while being undetected by plant operators.

The capability to modify SIS parameters to inhibit or reduce SIS responses to unsafe conditions without the operators being aware results in many potentially dangerous scenarios. This could include the adversary compromising the SIS and simultaneously manipulating the control system to produce an unsafe event that would place a demand on the SIS to act when its functionality is degraded or inhibited.

Anatomy of Disruptive Attacks on Physical Processes (An Impact Case Study)

As described in the SANS whitepaper, *The Industrial Control System Cyber Kill Chain*,[19] provides a model for describing and illustrating what happens when an attack occurs on an industrial control system, which helps to articulate how disruptive cyber attacks can cause physical process impacts.

Using this model, the Dragos whitepaper on CrashOverride[20] provides the anatomy of the attack from initial intrusion, to pivoting to the OT, to movement within the OT, and then to the deployment of OT specific malware and its execution on the controllers that resulted in the opening of circuit breakers in a transmission level substation. Additionally, the paper also details other elements of the attack that hampered restoration efforts such as wiper modules to clear registry keys, removing key OT project and configuration files, and finally killing processes resulting in system instability of the hosts.

The physical impact of the attack in 2016 resulted in an electrical outage to approximately 230,000 customers, before manual operations restored power within 30 to 60 minutes.

From an OT incident response perspective, a key learning outcome from this event is to focus on how to detect and respond to proceeding events as early as possible in the kill chain to prevent, or at least mitigate, the potential for physical impacts.

17 https://www.dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

18 https://www.dragos.com/resource/stuxnet-to-crashoverride-to-trisis-evaluating-the-history-and-future-of-integrity-based-attacks-on-industrial-environments/

19 https://www.sans.org/white-papers/36297/?msc=blog-ics-library

20 https://www.dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/

Organizational Capability

Organizations have often implemented an IT incident response capability within the organization – often driven by IT operational or information security (ISMS) considerations. This can result in the industrial domain either not being covered by the IR capability, or that is delegated to other functions within the organization. With an increasing focus on OT by attackers and defenders, existing IT concepts are copied into the OT aspect – often without success. An OT incident response function should be embedded into the overall organization, but not considered equivalent to IT incident response.

If the organization has realized the need for OT-specific incident response capability, there is often the desire to build a dedicated team with the following ingredients:

- OT incident response skills, with the requirements derived from a steadily maturing cybersecurity program and numerous iterations of an OT cybersecurity strategy
- Development of the response capability after significant resources have been assigned to policy and governance development, discovery, and assessment activities.

This often results in the aspiration to build an internal OT incident response capability remaining exactly that: an aspiration. For example, organizations may plan to implement OT incident response (IR) capability, but only once earlier phases of a security program are complete, resulting IR planning being delayed and/or deemed too costly to pursue.

Personnel, resourcing, and training in the IT domain has improved in the past. If an organization wants to establish an IT incident response function, the market for skilled workforce is still difficult but continuously improving. If internal resourcing is difficult, IT incident responders may be realized as managed security service providers (MSSP) and embedded into the IT organization.

When hiring, training, and retaining security personnel with OT knowledge and capability, the market for a skilled workforce is one of the greatest challenges for organizations that want to establish their own OT incident response function. If that is combined with insufficient funding and missing procedures in the OT domain, an effective OT incident response organization cannot be established. Industrial defenders should plan for and train either IT personnel to respond and understand OT-specific operations, or OT personnel to perform incident response functions. Depending on the organization, hybrid teams can be very effective – the industrial process and the impact on such by incident response should be part of every organizational capability. If internal capabilities are not available in case of an incident, a trusted partner-like Dragos should be utilized to maintain capabilities to respond to incidents in an appropriate manner.

Outsourcing OT security monitoring and response to an internal corporate Security Operations Center (SOC) or external SOC provider can be difficult to achieve as OT operators must retain ownership of the process operations and are hesitant to allow remote teams (often from within the IT organization) to lead on response efforts and on configuration of the equipment used within plant operations. When utilizing third parties like Dragos, organizations should ensure that the individual challenges in the industrial domain and the specifics in monitoring and responding in industrial are considered in such a service. Dragos has specifically designed OT Watch to be such a service that allows appropriate external support.

Priorities and Data Loss

When performing IT incident response, the focus is on the information assets and their availability, integrity, and confidentiality. In the OT domain, additional and specific considerations are required, since loss of data can also be damaging due to the impact it can cause to the organization's reputation and the loss of data can lead indirectly to ICS Cyber Kill Chain[21] Stage 2 attacks.

Table 3: Examples of high importance data loss in OT systems

OT DATA TYPE	EXAMPLES
Production trade secrets	• Automotive manufacturing sequencing steps and timing. • High tensile light weight steel manufacturing.
Data that moves from the OT environment to the business networks	• Data required for billing. • Data required for ERP systems.
Manufacturing data stored for regulatory reasons	• Automobile manufacturers are required to store torque tool data. • Pharmaceutical manufacturers storing batch data.

Even though it is worth considering, loss of data is seldom the main incentive regarding OT cybersecurity incident response. For example, the response activities related to the destructive attacks in Ukraine and Saudi Arabia were not driven from a loss of data situation. For many OT systems and their operations, the driver is more likely to be based on maintaining the availability of the systems or ensuring the integrity of the systems to maintain safety and reliability of OT operations and limiting any potential impact to the business.

Different Data Sets for IT and OT

There are generally four distinct datasets that are available in an OT environment: network, physical process data, host (memory), and host (disk artifacts) data, as shown in Figure 1.

Process data is unique to OT. It is vital to provide root cause and effective impact assessment during an incident response operation.

Each dataset provides an opportunity to inform an analyst's overall understanding of the OT operations for incident response investigation.

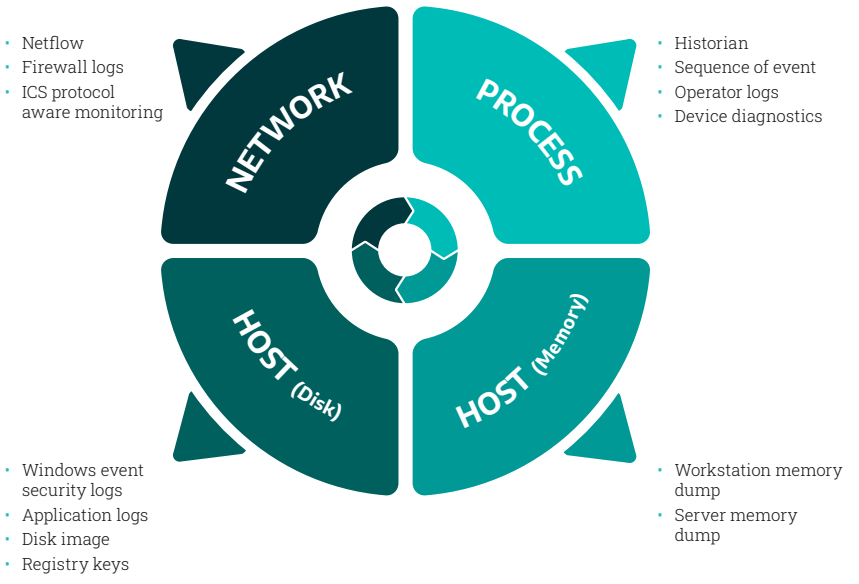


Figure 1: The 4 categories of Data Sets in OT environments

21 https://www.sans.org/white-papers/36297/?msc=blog-ics-library

Not all datasets are equal, and some require specialist tools and capability to interpret them to the level of detail required for root cause analysis and forensic investigation.

OT environments contain several log sources which are similar to IT environments: Windows Event Logs, authentication logs, NetFlow, etc. Applying operational knowledge and context to these log sources can provide incident responders which a large number of high-quality logs for analysis, thereby enabling root cause analysis. While this data provides a good starting place for an incident response team to investigate, it will not provide the OT visibility required to understand which control commands have been issued or any other communications between engineering workstations, HMIs and the controllers performing control and protection of the systems. Obtaining the capability to observe these key communications usually requires the monitoring of East-West traffic (i.e., traffic on the same Purdue level or within the same datacenter) using tools with the capability to interpret OT protocols.

In addition to the typical IT type log sources, OT environments also contain a significant number of OT-specific data sets, including sequence of event logs, historian data, alarm and plant trip records, and vendor specific communications to control equipment. Understanding the sources of these data types and how to access them can provide incident response teams with insights required to understand how the OT is operating and provide opportunities to identify notable events on the incident timeline to pivot into forensic analysis of other artifacts.

Often this will require manual collection and analysis to obtain the data from individual devices, historian applications, and potentially even from interviews with plant operators and engineers.

Many OT devices that do not have security logging capability may still be able to provide artifacts of interest to a responder performing investigation, such as diagnostic logging. However, it is common for these diagnostic logs to be unique to each vendor and are likely to require vendor support to obtain and interpret the data.

Forensic Data Collection

Collection and forwarding of forensic data from enterprise products is demonstrably easier year on year. Deployment of tools, training of personnel to use them, and the processes followed during an incident can enable the collection and analysis of multiple data sources from across an enterprise within minutes.

Endpoint Detection and Response (EDR) solutions can provide some value to OT network defenders, particularly in the upper levels of the Purdue model such as an OT DMZ or supervisory level. Note, these solutions cannot be relied upon in OT environments in the same manner as they would for enterprise incident response due to their lack of analysis of OT protocols and controller configuration software packages. Even if EDR solutions were deployed across an industrial environment, they lack the capability to bridge the gap between IT network activity and manipulation of industrial processes. Domain-wide deployment of EDR solutions in industrial environments remains rare for multiple reasons:

- EDR solutions are designed for enterprise operations and many OT applications, processes, trend, and database files are commonly required to be on exclusion lists
- EDR solutions may not be available for legacy systems, or may require additional support purchases to remain covered
- EDR deployment may not be applicable for OT devices due to memory and processor constraints

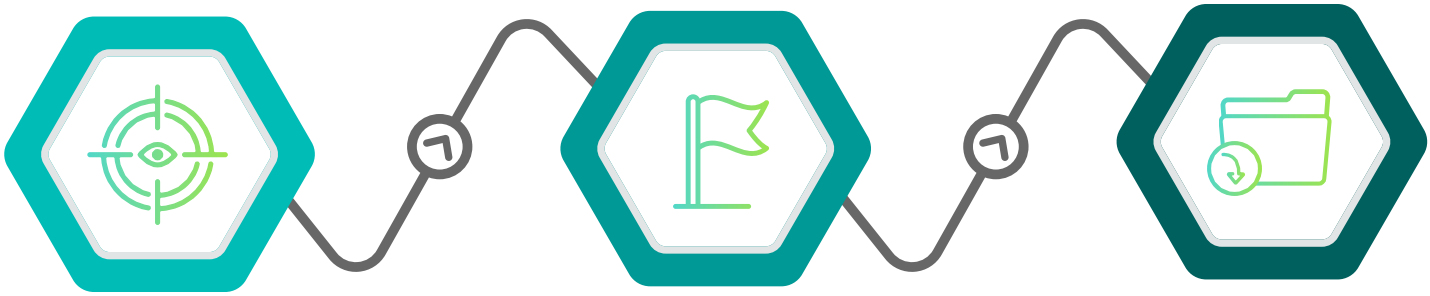
- The models used to determine likelihood of a process being malicious tend to lead to a higher number of false positives in an OT environment
- EDR solutions configured to terminate processes or isolate endpoints may cause negative impact on safety or reliability of operations

Security Information and Event Monitoring (SIEM) tools allow analysts to query large amounts of logs and identify anomalies. Effective use of SIEM technology requires appropriate logging capability of devices and services as well as the ability to parse the logs. In OT environments which contain legacy devices and non-standard components, IT-based approaches to log management and onboarding of sources often fall short.

For these reasons, Dragos recommends the Collection Management Framework (CMF) approach. The CMF provided by Dragos uses a scalable and repeatable method to determine the log sources available from an OT environment, how they can be accessed, how long they are stored, and what type of incident response questions can be answered from those log sources. The benefits stated to clients during those engagements are that developing a CMF identifies:

- Collaborative approach to preparedness for tactical requirements of an OT incident response
- Coverage gaps and shortfalls in similar configurations across and an OT estate; and
- All relevant data sources for incident response investigation and how to access them.

During incident response, the ability for an IR team to quickly identify the available log sources greatly assists in scoping the collection, transfer, and analysis of forensic artifacts. Knowing what is available and what answers the logs may be able to provide help to identify potential adversary activity and speed up the analysis required to identify the root cause. Considering the level of effort vs. the value it provides within an industrial environment is a crucial aspect of industrial incident response. This provides the incident response team (IRT) with a significant advantage when it comes to identifying what to collect and from where. Using the prepopulated CMF helps the IRT focus, prioritize, and collect from the OT environment for investigation.



Focus

on the most valuable hosts and datasets

Prioritize

collection of volatile, time-sensitive or time-consuming datasets

Collect

from individual systems via removable media

Figure 2: Dragos recommended methodology for OT forensic collection

PLC Challenges

Logging capabilities of OT devices such as PLCs are continuing to increase after introduction of syslog capability for PLCs in 2015.[22] More PLCs are also moving to standard real-time operating systems -that have built-in syslog capabilities. Collecting forensic data from firmware on PLCs remains challenging and is yet to be demonstrated as a reliable option for industrial incident response teams. To date, the acquisition of PLC firmware has been performed in lab and training environments. The process may slowly become an easier task to complete but applying it in an immediate incident response situation still remains impracticable. For most OT operations conventional acquisition will require a significant amount of planning and justification to be able to remove the device, extensive co-ordination with vendors to be able to forensically examine the device, and large amounts of highly specialized and vendor-specific analysis to determine a potential root cause. Being able to articulate and justify the resources to perform those actions is a significant challenge.

The incident response efforts to determine root cause will require timely analysis. Waiting for the collection, abstraction, and analysis directly from a PLC will likely not be timely enough for most industrial incident response cases. Therefore, the IRT will need to be agile in determining what other actions could be performed -- either instead specialized forensic analysis of OT devices such as a controller, or in parallel efforts if the value of controller analysis is warranted, bearing in mind that one industrial plant may contain hundreds of controller devices.

Network monitoring can save a significant amount of time and effort in these situations by providing visibility to the interactions with devices such as PLCs before and during an incident. Being able to determine if controller logic changes have been pushed to a device, or if communication with configuration suites from engineering workstations took place will help to quickly narrow down the scope of an investigation.

OT Network Security Management (NSM) During Incidents, Case Studies from the Field

During two separate cases over the last two years, Dragos has responded to industrial cybersecurity incidents where OT NSM could have significantly reduced the amount of analysis required to determine root cause and return to normal operations.

Case 1:

As described in the Dragos 2021 Year In Review,[23] “The Ghost in the Power Generator”, Dragos responded to a power generation utility that had experienced an unexpected gas-powered turbine automatic start-up. Due to the lack of OT NSM, Dragos responders had to rely on logs and host data and were able to determine root cause following the collection and analysis of the logs, interviews with site personnel, and testing of hypotheses on human-machine interfaces (HMI). Had OT network monitoring been in place at the site, malicious activity could have been ruled out as a root cause much faster by confirming or ruling out any remote access (i.e., network traffic) to the HMI, potentially enabling the local operations team to identify the actual cause without having to call in external responders. Further, the commands from the HMI would have been immediately observed by the operations staff leading to less lost time and quicker root cause analysis on an operations issue.

22 Schneider Electric M580 https://media.distributordatasolutions.com/schneider/2016q2/d5b1c8dc2ba82c76bce73d1ef060d2c2e5421eb4

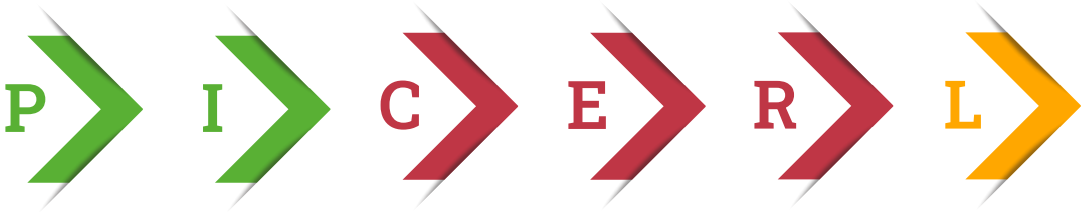
23 https://www.dragos.com/year-in-review/

Case 2:

In 2022, Dragos responded to an industrial operator after they had observed multiple events at separate facilities including configuration changes to a historian, programming mode change of a PLC, and loss of operator visibility to process values coinciding with failure of primary and secondary controllers. Following extensive scoping, collection, analysis, and coordinated discussions with operators, vendors, and analysts, it was determined that the events were caused by hardware failures on 20+ year old controllers, and configuration errors caused by Windows SCCM or Windows Installer reconfiguration. A significant amount of effort was required by the operator's OT team and Dragos analysts to enumerate the networks at both sites involving packet capture and replay, collection, correlation, and analysis of incomplete network diagrams and asset inventories.

Network security monitoring at these locations could have provided the operators OT team with the insights required to determine the network configuration and the identification of legacy OT assets with aging hardware. Additionally, the network monitoring could have assisted with scoping the investigation by being able to confirm that no interaction with the primary and secondary controllers had taken place prior to their failure.

How the Phases of Incident Response are Different within Industrial Environments



P = Preparation, I = Identification, C = Containment, E= Eradication, R= Recovery, L = Lessons Learned
PICERL: green = IRT, red = OT, yellow = combined effort

PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) is a framework developed by SANS that provides the structure for dealing with the various phases of incident response. It is applicable to IT and OT environments, however the implementation for OT is significantly different.

Preparation

In all Incident Management (IM) models, preparation is the most important phase in incident response regardless of IT, OT, or other domains. One of the most significant differences for OT is that an incident responder may need to complete specific health and safety briefings, helicopter crash training, use of PPE, etc. before being able to physically access the facility where the OT equipment resides. Preparing for an incident may also mean pre-certifying responders (internal and external) and maintaining the permission to go onsite.

Additionally, due to plant operating requirements or jurisdictions, it is likely that even the most qualified and experienced incident responder will not have the authority to touch or interact with an OT system or device. Being prepared for these situations is vastly different than for IT incident response. For these reasons, there is a smaller pool of resources available to help, and organizations must prepare for this.

Preparing for OT incident response also means to be aware and train emergency cases, where access to parts of a plant or the infrastructure is not possible or prohibited. Equipment and procedures should consider alternative means of responding in case of an incident.

Identification

The most important aspect of the identification phase is understanding if an alert, notification, event, or other suspicious activity warrants the declaration of an incident, that may require a rapid understanding of scope and context.

In many OT organizations, the decision-making process and incident command structure is relatively new and may be inexperienced with handling the types of cybersecurity alerts, notifications, and events from the OT systems and networks. Forensic data is often destroyed, intentionally or accidentally, since operator training will likely prompt for system restarts when investigating plant issues or problems with computer systems. Conversely, being able to collect information from a machine to assist in the process of identification may require access to the hazardous environment at a time when the integrity of the system responsible for ensuring safety of workers is in question. This occurred during the response to Trisis,[24] where responders were investigating a part of the sulfur recovery unit which is responsible for shutting the plant down if unsafe levels of hydrogen sulphide were detected.

It is also common for cybersecurity to be a later consideration of cause. Operations and maintenance teams may have been working to determine and fix a problem for weeks or months prior to considering any investigation into malicious activity. Volatile forensic evidence is more likely to have been lost, and the event horizon is more likely to have expired in these situations making the identification phase a different challenge than within an IT environment. It is important to raise cybersecurity awareness with operations personnel to better inform them of when the involvement of the OT incident response team would be required.

It is very difficult to compare the current state of an OT environment during an incident when there is a lack of visibility, asset inventory or a known baselines of how the system and networks normally behave. Non-existent or incomplete network diagrams and asset inventories are more prevalent in OT environments. This is particularly true where active scanning and network discovery tools can cause serious adverse effects on operations. The lack of visibility makes the incident response teams task more challenging when trying to determine the scope of an intrusion. For example, identifying the number of assets, processes, or sites that are affected or potentially affected by a threat can take significant time and effort, even when a relatively simple indicator of compromise is available. This was observed across many organizations in the response efforts to the SolarWinds compromise in late 2020, where many organizations were not able to quickly identify which sites contained SolarWinds Orion servers directly or embedded within (vendor specific) OT packages and were not able to effectively scope down which networks required attention.

24 https://darknetdiaries.com/episode/68/

Containment

Traditional OT networks tend have a significant advantage over corporate environments in terms of their relative static nature; it is uncommon for widespread use of transient assets, mobile devices, and temporary networks in OT environments. However, this advantage can be nullified if the IRT are not able to act swiftly and thoroughly in response to threats in terms of containment (and ultimately eradication) actions. The importance of being able to act swiftly will become even more challenging with an increase in converged IT/OT and use of cloud.

Defensible architectures mean that containment must be possible by design. A long standing and widely recognized systemic issue for many OT environments is lack of visibility. This includes the visibility into the dependencies and interdependencies between systems, and between the OT environment and IT systems. Many OT defenders have overcome this challenge and have a good understanding of traffic that crosses the IT and OT divide and have measures in place to remove this connectivity as one method of containment. However, many networks do not yet have this control in place yet, making containment difficult to achieve, or increasing the risk that a response action will cause further disruption to the business by removing the connectivity required for the business to operate.

The use of containment methodologies such as network isolation can inhibit the incident response efforts by removing the access to any monitoring solution that was present or removing the visibility from the remote and/or outsourced incident response teams performing analysis. Additionally, as described in the Forensic Data Collection section, EDR solutions are not usually available to assist with the scoping and containment efforts. SIEM systems often have limited coverage when it comes to the field devices and non-standard equipment.

Eradication

Most eradication methodologies are described as being the longer term or permanent implementation of measures to remove an adversary from an environment. Whether methods are short term, temporary, or permanent, they require confirmation/validation that they were effective. For many OT networks using legacy systems and lacking in visibility, the validation of effective eradication measures is much more challenging.

Many eradication methodologies will involve restoration of systems from backup images, rather than relying on malware removal using security tools. Many businesses will have business continuity planning and disaster recovery plans. Restoration from backups in an IT environment can often be performed in a relatively quick manner. Restoring an industrial control system from backup is likely never performed in its entirety; some parts of the system may be tested on a regular basis, but even in these cases it is likely that the testing period is determined by planned facility outages which may be months, if not years, apart.

Full eradication of an environment including rebuilding Active Directory and reimaging of relevant systems is a significant task to complete for any network. For OT environments this task is likely to be considerably more challenging than in an IT environment due to the support required from OT vendors and operations staff to rebuild and recommission the systems.

An important difference to IT incident response is the need to validate process functionality during and after eradication. Where the removal or reinstall of a system in the IT domain usually does not have hidden process dependencies, a change in the OT environment may require extensive validation and potentially recertification of operating equipment and/or industrial processes.

Recovery

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are usually determined through business continuity and resilience planning. The RTO and RPO essentially define how quickly the business unit or organization needs to recover, and how far back the team needs to be able to recover the systems to.

Recovery Point Objectives (RPOs) are historical recovery points that are required, e.g., how much operational data loss can be tolerated and the determination of the frequency of backups.

With some industrial verticals, long RPOs are common in environments that operate batch processes, such as pharmaceutical and automotive manufacturing, where records of production are required for long durations for regulatory and quality assurance purposes.

Recovery Time Objectives (RTOs) are the time required to recover and return to normal operations.

In relation to responding to cybersecurity incidents in OT, the RTO is essentially how long a business can survive in emergency mode. For example:

- how long can operations be performed in manual mode
- how long can production on a line be disrupted before knock-on effects occur

RTO and RPO are a key part of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), and are applicable to an entire organization, not just OT or IT. However, a key difference for OT environments is that a physical impact on the plant may be involved in addition to business impacts caused by loss of production or degradation of services. Additionally, the physical equipment required to perform recovery of an OT system is more specialized than within an IT environment. For example, the make and model of an HMI, ruggedized distribution switch or remote terminal unit may be more difficult to source, install, configure, and commission when compared to same activities required to re-deploy a Windows Server for use in an enterprise environment.

Lessons Learned

As a concept, there is no difference here between IT and OT. Many industrial organizations will have governance in place to perform lessons learned activities following an industrial accident or a near miss, or the completion of a project.

Many OT defenders likely have not yet experienced a cybersecurity incident and will therefore not have well established lessons learned workflows to capture learning points. Tabletop exercises are therefore even more important to identify quick wins and shortfalls in their cybersecurity response capabilities prior to a real incident.

Ownership of the PICERL Phases

A final key difference between IT and OT in terms of Incident Response is the ownership of each of the PICERL phases. It is common within IT environments for the IRT to be responsible for each of the phases, including taking the ownership to perform the actions within containment, eradication, and recovery phases. For many employees, the swift and decisive action taken by the IRT may not even by noticed during day-to-day work.

Within OT environments the actions required to contain, eradicate and recovery from an incident must be owned and enacted by OT operations and those with ultimate responsibility for the facility. The advice and guidance from the IRT to the OT team should be clear and timely, but the IRT will not and should not have the full authority to implement the actions in the OT environment.

How to Prepare for Effective Incident Response for OT

Now that we have established the key differences between IT and OT in terms of Incident Response, we can now focus on how to prepare for IR in OT, using the incident management system that was introduced earlier as a framework.

For each of the incident management system components (facilities, equipment, personnel, procedures, and communications) Dragos recommends the following, as a minimum, be developed as part of an OT operator's incident response readiness. This is based on Dragos' experience in responding to dozens of cybersecurity incidents across multiple verticals and regions over the last five years, and from performing proactive services such as Tabletop Exercises and Threat Hunts. Each of the items listed in **Table 4** is described in detail throughout the remainder of this document.

Table 4: Component | Dragos Recommendation: Dragos' recommendations for IR readiness, aligned to the Incident Command System categories

Facilities	• Collaboration space for Incident Response providers and support teams • Incident response line and out-of-band communications • IR room with whiteboards • Virtual war rooms as required for multinational organizations
Equipment	• Network Security monitoring tools • Grab bag including copy of an up-to-date CMF • Forensic collection tools
Personnel	• Defined Incident Response team size and structure • Incident Command structure (Dedicated Incident Commander appointed, site champions) • Relevant training, site, and professional certifications

Table 4: Component | Dragos Recommendation – continued

Procedures	• Forensic Collection procedure • OT network containment procedure • Host isolation procedure • Predefined eradication strategies • Predefined recovery processes and procedures
Communications	• Severity matrix incorporated into an OT specific incident response plan • Established IR battle rhythm meeting agenda and reporting board • Documented IR battle rhythm template with the required information, contact details and timing requirements

Facilities

Collaboration Space for IR Support Teams

Dragos recommends OT defenders **prepare processes and authorizations for how information would be made available to support teams.** For some jurisdictions, this could be in the form a dedicated external SharePoint or similar collaboration platform being established with IR providers authorized to access it. For other scenarios, such as those with restrictions on data sovereignty, more complex arrangements may be required. In any case, being able to share the required incident information with support teams is imperative.

Alternatively, an operator may choose to prepare and maintain a dedicated out-of-band infrastructure that allows for collaboration and communication. Such an infrastructure needs proper planning and testing. Building such an infrastructure during an active incident is too late and will likely result in mistakes and delays during incident handling and information sharing.

Incident Response Communications Line and Out-of-Band Communications

A key requirement of an incident response plan, and the company's use of it, relies on having a clear line of communication for operators and personnel to contact and report a cybersecurity event or incident. Ideally, this should be a telephone line that on-call members of an IRT can answer, alongside a ticketing system and email alias for reporting.

For inter-team communications, Dragos recommends **establishing and testing the use of out-of-band communication** methods to avoid situations where an adversary may have compromised or disrupted the normal communication channels of an organization. All relevant internal and external stakeholders should be aware and trained in case out-of-band communications is required. Depending on the organization or industry vertical multiple means of communication (e.g., in case of internet/network outage) may be required. Especially when realizing an incident command organization, the individual teams might want to detach detailed communications from the overall incident management communication.

IR Room with at Least One Whiteboard

Emergency control rooms are commonly found on industrial sites, such as a dedicated facility as part of nuclear site license emergency preparedness procedures. These rooms are usually equipped with Public Address (site-wide PA) systems, PPE, key site documentation including procedures, plant diagrams, and local area maps. Additionally, it is common for these rooms to contain multiple whiteboards, sometimes with specific layouts for incident and emergency response. Incident Response Work and Resources (WAR) rooms are also commonly equipped with at least one whiteboard. Other required communication and documentation equipment should be prepared and kept ready. This might include flipchart paper, functioning pens, magnets, etc.

For OT Incident Response, Dragos recommends OT defenders **locate a suitable room for the incident response team to use,** bearing in mind that IT facilities are often equipped with restricted access to non-IT personnel, and may be located some distance away from where plant operators and engineering teams reside. The incident response team room should contain at least one whiteboard for recording key information about an incident, recording assigned actions and results, and a rudimentary timeline of events and actions. Collaboration tools such as Confluence or OneNote can be useful for sharing information within the Incident Response Team, particularly for teams which are geographically dispersed.

Equipment

Network Security Monitoring

For adequate coverage of threat detection and anomalous events, passive network security monitoring is ideal for providing monitoring coverage with the requirement to deploy agents or make configuration changes to OT assets.

Dedicated network security monitoring for OT environments that is deployed correctly to monitor for East-West traffic in addition to North-South traffic provides insights required to understand if controller configuration is being performed, if any commands are being sent to controllers, and if lateral movement is potentially occurred within the OT environment.

For incident response, this is crucial in determining the scope of an incident, the severity, and helping to inform where to perform actions such as forensic collection and containment.

Grab Bag

There are many items which would be useful to keep ready in a Grab Bag. Ultimately the contents should be determined by the local teams that will maintain the contents and use the equipment in the event of an incident, therefore it is important that Grab Bag is owned by the IRT. Dragos has previously provided some suggestions for Grab Bag contents in the *"Preparing for Industrial Cyber Response: What to have in your IR toolkit"* **blog.**[25]

Part of the incident preparation activities should also be a process for regular updating and validation of the Grab Bag, to ensure it remains fit-for-purpose in case of an incident. This includes charging of batteries, updating documentation, diagrams and plans as well as keeping tools and licenses up to date.

25 https://www.dragos.com/blog/industry-news/preparing-for-industrial-cyber-response-what-to-have-in-your-incident-response-toolkit/

Collection Management Framework (CMF) for IR

Creating and maintaining a Collection Management Framework (CMF) for an OT environment[26] is recognized as best practice, either from direct or indirect inference from standards and guidance, or from the recommendations of practitioners such as Dragos. A CMF is recognized best practice for improving both the proactive and reactive aspects of an OT operator's security posture.

In the context of incident response, a Collection Management Framework for logging and monitoring is a powerful tool for the IRTs to refer to during an incident, and a relatively easy step to update post-incident as part of the lessons learned phase of incident response. Dragos strongly recommends **OT defenders prepare CMFs in advance to determine which log sources are available, their retention period and location, and who within the organization has authority to access them.** This saves valuable time during incident response and reduces the frustration of response efforts which might be hampered by being unable to analyze forensic artifacts. The CMF approach is described in detail in a Dragos **blog**.[27] To assist OT defenders further with the creation of a CMF for IR preparation a step-by-step methodology is provided within Appendix B – Simplified methodology for creating and developing a CMF.

Dragos also recommends that the IRT **use the CMF to practice situational awareness**, using the data within the CMF during tabletop exercises and rehearsal of concept drills to discuss and assess what adversary activity could be present in the environment, and identifying which data sources in the CMF could be used to validate assumptions or answer other questions related to adversary TTPs.

Dragos often observes a tendency within TTX engagements where defenders are not able to describe what activity is being detected in a consistent manner, i.e., what TTPs are observed or where in the ICS Cyber Kill Chain an intrusion may be. Being able to articulate findings during the response to an incident helps to communicate the *"so what?"* to other stakeholders in terms of potential impact and consequence. Additionally, awareness and use of ICS Cyber Kill Chain and MITRE ATT&CK can also help to focus the IRT on what actions to take next as part of an OODA (Observe-Orient-Decide-Act) loop.

Forensic Collection Tools

Regardless of whether OT specific monitoring is deployed across a network, OT defenders should be prepared for performing forensic collection of artifacts from hosts and networks. For collection from hosts, for example engineering workstations, domain controllers, and SCADA application servers, Dragos recommends that OT defenders **have a prepared forensic collection tool(s) that have been tested,** and a procedure for authorized personnel to use the tools on the assets. OT operators usually have a strict set of criteria for who can interact with equipment and when, usually using criteria of authorized personnel and work order card systems. For these reasons it is vitally important **to ensure that the tools are pre-qualified for use**, and the site personnel required to perform collection are trained and comfortable running the tools and using dedicated removable media. Forensic tools should be regularly checked for functionality. An updated to existing collection methods may be required following changes to the OT environments infrastructure, hardware, and software.

26 https://www.dragos.com/blog/industry-news/preparing-for-industrial-cyber-response-what-to-have-in-your-incident-response-toolkit/

27 https://www.dragos.com/blog/industry-news/building-a-collection-management-framework-for-industrial-control-systems/

Personnel

Incident Response Team Size and Structure

In an ideal situation, an OT Incident Response Team's size would be determined by an assessment of required capability, the available resources, and would be aligned to a strategic OT security program with traceable links to the BCP. The required capability of the team would match the required response for the business, meeting productivity and resilience requirements, while also satisfying regulatory requirements.

This ideal situation may not be realized in many organizations. Even for well-resourced OT defenders, there may be a need to factor in external support, either to perform some key IRT functions, or to supplement the well-resourced team with specialist skills when they are required. Regardless of where an organization is in their cybersecurity maturity, Dragos recommends that OT defenders assess and document the types of IR external support that would be required. This helps the organization in their self-assessment (as-is -> to-be), but also helps scope out the right IR support organizations whether it is specialist forensics, breach coaching, malware reverse engineering, provision of Threat Intelligence, or a combination of all the above.

How to Define Requirements for Response Team Size and Structure

RPO and RTO helps define what the organizations requirements are for recovering from an incident. These requirements should help define the capability required, and therefore shape the size and structure of the team. Being able to provide a compelling justification for the resources required, linking back to clearly defined business objectives can help with the creation and presentation of the business case to the board or leadership team.

Inevitably, there will likely be a need for the IRT to be able to scale to be prepared to deal with a large-scale incident, while also maintaining the required skills and overall control of the incident and operations. In situations **where external IR support is required, it is highly recommended to assign a single point of contact to coordinate** the external resources. This role should also including provide context to IR providers. Being able to pull in external resources quickly and providing them with situational update as they join the incident team will help those responders get up to speed as quickly as possible and be able to assign the right skills where required. For example, dead box forensic image analysis could take a significant amount of time, especially if the analyst is lacking any context as to what type of malicious activity was detected or suspected, or during what timeframe the activity took place. If third parties need to be involved Dragos strongly recommends that defenders test activation procedures and establish relationships with external support personnel. This can be done with tabletop exercises, drills or similar.

Incident Command Structure

Dragos recommends that organizations **appoint a dedicated Incident Commander.** The purpose of an Incident Commander is to maintain an order and flow to the management of an incident. The Incident Commander should have delegated authority within the organization to make decisions, assign actions to IRT members and approve their completion.

Additionally, for organizations that operate across multiple sites, it is recommended to **assign site champions** that fulfill the role of providing site specific understanding and expertise to the Incident Commander and the rest of the IRT. This is to ensure that the intricacies and nuance of individual sites is taken into consideration with the IRT analysis and actions. These roles can also alleviate common concerns that site managers and operations teams can have when decisions are made from central teams, third parties or "head office".

Relevant Training, Site Authorization, and Professional Certifications

Many OT operators will enforce site staff and contractors to demonstrate competence to a defined set of criteria, often resulting in a designation such as a "Responsible Person", "Responsible Engineer", "Suitably Qualified and Experienced Person" for example.

Dragos recommends that OT defenders **define and document the requirements for on-site personnel with responsibilities for incident response activities**, including the required training and certifications. The requirements will differ from organization to organization, and may even differ from site to site, but should enable a basic set of activities to be performed such as those described in the Procedures section. Should external support require certification in a target environment, it should be either considered in the activation procedure or third-party support arrangements to ensure that pre-certification is considered as part of the onboarding.

Procedures

OT Dataset Analysis Procedures

Having a comprehensive understanding of the four categories of data sets from an OT environment helps the IRT scope the incident and pivot the investigation in order to remain agile and avoid lengthy and time-consuming analysis of data. Taking the outputs from the CMF, the IRT can quickly assess which tools and skillsets are available to them to collect and analyze from each of the four categories, and where additional support would be required or provide benefit. **IRT are recommended to assess their coverage of tools and skillsets required to perform analysis across the four categories of data sets from an OT environment.**

Table 5: Examples of 4 categories of OT data sets [27]

CATEGORY	EXAMPLES	EFFECTIVENESS IN UNDERSTANDING OT SECURITY EVENTS	RATIONALE	TOOLS AVAILABLE*[28]	ADDITIONAL SUPPORT OPTIONS
Network	NetFlow	Low	Provides an understanding of communicating assets on the network, flow and volume	• SolarWinds • WhatsUP Gold	
	Packet capture	Medium	Provides a basic understanding of communicating assets on the network and some coverage of OT protocols	• Wireshark • Tshark • CyberLens • Dragos Platform	
	Firewall Logs	Medium	Dependent upon configuration and deployment	• SolarWinds • Event Manager • SIEM	
	Network Security Monitoring	High	Continuous visibility and characterization of adversary TTPs.	• Dragos Platform	OT Watch Dragos IR services
Host (memory)	Memory Dump	Medium	Large amount of forensic evidence available with analysis, more challenging to obtain from OT assets.	• SANS SIFT • Volatility • CyberTriage	

28 Please consider tools mentioned as examples, there are often more tools available for each category. Mentions of commercial tools should not be regarded as endorsements for specific products.

Table 5: Examples of 4 categories of OT data sets [27] – continued

CATEGORY	EXAMPLES	EFFECTIVENESS IN UNDERSTANDING OT SECURITY EVENTS	RATIONALE	TOOLS AVAILABLE*[28]	ADDITIONAL SUPPORT OPTIONS
Host (disk artifacts)	Windows Event Logs	Medium	Dependent upon configuration and ability to forward and/or collect.	• SIEM • Event Log • Explorer	
	Application Logs	Medium	Dependent upon configuration and ability to forward and/or collect. Examples Include project changes within FactoryTalk Audit Log.	• SIEM • FactoryTalk • AssetCentre	Rockwell Automation
	Sysmon	Medium	Dependent upon deployment status, configuration and ability to forward and/or collect.	• SIEM	
	Authentication logs	Medium	Dependent upon configuration of logging, and the au-thentication strategy deployed across the environment.	• SIEM	
	Registry	Medium	Various information can be obtained including USB drive usage, user operations, and adversary persistence techniques.	• SANS SIFT • Registry • Explorer	
	Shimcache, prefetch, jump lists	Medium	Windows process execution	• EZTools	
	Full disk image	Medium/High	Large amount of forensic evi-dence available with analysis such as Process execution, file creation etc..	• SANS SIFT • CyberTriage • EZTools	

28 Please consider tools mentioned as examples, there are often more tools available for each category. Mentions of commercial tools should not be regarded as endorsements for specific products.

Table 5: Examples of 4 categories of OT data sets [27] – continued

CATEGORY	EXAMPLES	EFFECTIVENESS IN UNDERSTANDING OT SECURITY EVENTS	RATIONALE	TOOLS AVAILABLE*[28]	ADDITIONAL SUPPORT OPTIONS
Process Data	Historian & SOE	Medium/High	Useful to help scope incident, and useful for determining timeframe.	• Historian software • Dragos Platform (OSIsoft PI integration[29]) • FactoryTalk • Alarms and Events	Vendor
	Device diagnostics	Varies	Wide range of device types, diagnostic coverage and solutions available	• HART communicator • Manual review of alarm schedules review • Vendor solutions such as Simatic Assessment Suite • Data Collector [30] (SAS-DC) or FactoryTalk Diagnostics service.	Vendor
	Operator Logs	Medium	Useful to help scope incident, and useful for determining timeframe.	• Manual review of written logs Operator interviews	• Operator • Supervisors • Engineers
	Engineering change control records	Medium	Provides a record of authorized changes made to OT devices, including timeframe of change.	Manual review of change control records	Vendor (if O&M support is provided)

28 Please consider tools mentioned as examples, there are often more tools available for each category. Mentions of commercial tools should not be regarded as endorsements for specific products.

29 https://www.dragos.com/wp-content/uploads/Dragos-PI.pdf

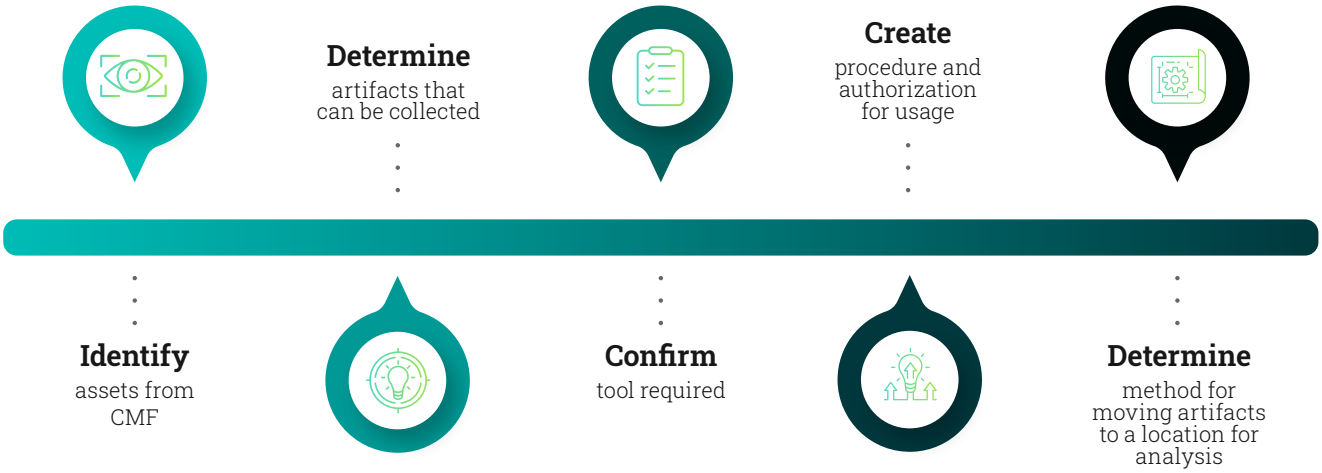
30 https://support.industry.siemens.com/cs/document/65976201/how-do-you-efficiently-collect-diagnostics-and-system-information-with-the-simatic-assessment-suite-data-collector-(sas-dc)-?dti=0&lc=en-WW

Forensic Collection Procedure

As described in the Equipment section, OT defenders should be prepared with tools that can be used to perform forensic collection from OT networks, informed and scoped from network monitoring. Forensic collection tools should be complemented with site specific forensic collection procedures and playbooks that the IRT can practice and drill to ensure familiarization with the process and minimize any potential impact to operations. Forensic collection tools must be checked regularly so they can be kept current remain fit-for-purpose. Changes in OT network processes, architecture, hardware, and software may trigger the need for validation.

Dragos recommends IRTs use a Focus, Prioritize, Collect methodology within forensic collection procedures, making use of CMFs to focus on collection from most valuable hosts and datasets, prioritizing those that are volatile, time-sensitive or time-consuming.

Dragos recommends that the forensic collection processes should include the use of portable media to obtain the collected artifact. Additionally, the processes should describe how the collected artifacts are moved from the OT environment to a platform for forensic analysis. This could be a forensic analysis lab located on the same site as the OT network itself, corporate network, IR providers network, or a combination of all.



Containment & Eradication Strategies Defined and Tested

Once the IRT has obtained enough information and analysis within the Identification phase, and an incident has been declared, the response team shifts into the containment and eradication phases. The success of the incident response depends on the execution of containment and eradication strategies and the monitoring their efficacy. IRT's should make the conscious and recorded decision to enact predefined containment and eradication strategies, coupled with the understanding of the consequences of actions in relation to plant operation, forensic artifact retention, and the possibility of indicating known presence to an active adversary. Change control is a fundamental aspect of maintaining safe and reliable operations. Therefore, the network and host isolation procedures network cut points and procedures) must be pre-defined and approved through the change control process in order to save the IRT significant amounts of time and stress that would occur if the procedures were required to be processed through

emergency plant modification analysis and justification. Of key importance here is that ultimately it is the decision of the OT operations team responsible for a plant or site to enact containment and eradication, not the IRT's. The IRT should be providing advice and guidance to those responsible for operation and configuration of the facility.

The planning of the network disconnection and individual host isolation should include analysis and documentation of the consequences of taking the actions:

- What is the impact on operations, if any?
- What information will no longer be available from the enterprise side?
- What security visibility and monitoring will be temporarily lost?
- What is known about the adversary and what their next actions may be?
- What will be asked of operators and plant personnel in terms of additional monitoring, manual inspection, etc.?
- Is the potential loss of host-based forensic artifacts known and accepted?

Regardless of the containment and eradication actions taken, the IRT should understand their own capability to test and validate the effectiveness of their actions.

Eradication strategies for OT environments tend to require the network defenders to work from a defensible cyber position, in other words from an isolated and islanded network position. At a high level, the eradication strategy should include the capability to scope the extent of an incident, perform isolation of hosts, re-image from known good backups, and implement account resets across the environment. Ideally for each action taken, the IRT should have the capability and visibility to monitor the effectiveness of their actions, providing a feedback mechanism to ensure that the incident remains well scoped. A conceptual model for this is provided in Figure 2. Documented procedures of these actions can include guidance, such as which accounts can be reset, how they are to be rest, and in which order they should be reset.

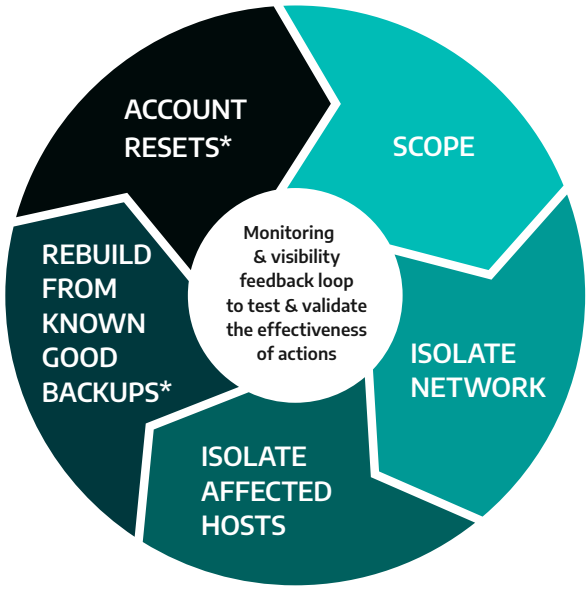


Figure 3: Eradication strategy for OT environments

Re-Image Vs. Malware Removal in OT Environments

Many malware removal software tools are available for assets such as Windows workstations and servers and provide useful functionality for personal computers to remove, quarantine or “clean up” commodity malware. Usually operating on the principle of scanning to identify known malware based on signatures, and removing the malicious files and processes, malware removal tools allow for the computer to remain in use, which is convenient and often appropriate for enterprise environments to enable the workforce to remain productive.

Within OT environments, Windows workstations and servers perform different and specific roles compared with those in enterprise environments. The assets can be either directly or indirectly performing functionality that requires assurance due to the importance of the process being controlled or monitored. While removal of malware may limit or prevent the adverse effects associated with the malicious software, it may cause enough changes to impact the operation of the OT specific function being performed or result in changes which degrade the assurance of the system’s operation. In these situations, a system re-build and re-image is required. Malware removal tools are also liable to leave remnants of malware behind, which can lead to re-infection or alerts in the future when fragments are detected again.

Account Resets in OT Environments

Full account resets across a domain, including all service accounts can be a challenging task to complete. It is common within OT environments, particularly legacy systems, for user and accounts to be assigned permission roles within groups by default. Conversely, it is not common for Group Managed Service Account (gMSA) capability to be present and utilized for service account management.

Even in situations where account management utilities and vendor documentation may provide all the required information and capability to perform full account resets, for example across a DCS, it is not likely to be a well-practiced action for operators to take.

For OT environments it is important to stress here that account resets are for those that are in use across an entire domain. There may be many passwords in use for local machines or OT devices which are not used across a domain, and some may even be vendor default passwords or PIN numbers, some of which may be written down locally or etched into instrument panels. In these situations, the passwords and storage will clearly be in violation of any enterprise password policy, however with adequate compensating controls such as physical security controls these situations may be acceptable for OT defenders and therefore not require resetting or changing during the incident. The intention of performing domain wide account resets in this phase of incident response is to reduce the ability of a remote attacker. Additional consideration would be required if the incident involves an insider threat.

Communications

Common Understanding of Terminology

From Dragos' recent observations during incident response and tabletop exercise engagements, the importance of having a common understanding of terminology across the response team is imperative. For a team-of-teams approach to be successful, it is important for aspects such as severity, impact, and consequence to be clearly understood and relevant to the OT environment in question.

For example, loss of view is a well-known term in cybersecurity and documented as an impact within the MITRE ATT&CK framework. For some plant operations, loss of view to an operator workstation may have already been assessed in terms of hazard identification and operability studies, resulting in a plant design and operational procedures that allows for the operator to relocate to a separate operating environment that is suitable for a defined period of operations. Loss of view affecting an operator workstation without redundant and separate capability would likely result in a different impact with higher incident severity.

Conversely, being able to use language and terminology that plant operators are familiar with will help communicate cybersecurity concerns more effectively. For example, being able to communicate that loss of view is occurring across an entire domain due to ransomware or KillDisk operations rendering any operator terminal potential unavailable, will enable the operations team to quickly identify and action the required operating procedures. **Dragos recommends using existing resources to incorporate a severity matrix into an OT incident response plan**, and ideally expanding on the generic examples to ensure that those used in the IRP are as relevant as possible to the OT environment in question.

NIST Computer Security Incident Handling Guide

		NIST SP 800-61 REV. 2: COMPUTER SECURITY INCIDENT HANDLING GUIDE*[31]			NCSC[32]
		FUNCTIONAL IMPACT	INFORMATION IMPACT	RECOVERABILITY IMPACT	
Severity	Very High / Critical	N/A	N/A	Not Recoverable	Critical systems offline with no known resolution.
	High	Lost ability to provide critical service to any user	Integrity loss	Extended	Non-critical systems affected, or critical systems affected with known resolution
	Medium	Lost ability to provide a critical service to a sub-set of users	Proprietary breach	Supplemented	Small number of non-critical systems affected with known resolutions
	Low	Minimal	Privacy breach	Regular	One or two non-sensitive / non-critical machines affected

31 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

32 https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes#category

Incident Dashboards & Reporting Templates

Dragos has observed excellent **use of reporting templates and IRT orientation boards** during incidents and tabletop exercises. The use of a predefined set of criteria put on an IRT's meeting room whiteboard helps the IRT to regularly orient themselves to the situation at hand, ensuring a "battle rhythm" is established to capture key information, allow for the assignment and tracking of actions to closure, and to ensure that communications with stakeholders is timely and informative. The use of these boards is also useful in terms of recording the key information required to summarize the incident via internal reporting and to facilitate lessons learned. Kanban boards and software tools such as Jira can be utilized to good effect for these purposes.

Using predefined templates with checklists and response boxes to capture the information required by various stakeholders makes it easier to delegate actions and ensure that complete information capture occurs during stressful situations.

Dragos recommends that these **battle rhythm meetings and reporting boards include the following agenda items:**

- Review and update of events timeline
- Tracking of actions assigned, completed and their result
- Status review of the potential impact to plant operations and revisit to incident severity matrices
- Orientation of events and information in relation to *ICS Kill Chain and/or MITRE ATT&CK*

These dashboards also serve as prompts and reminders to the IRT to regularly orient themselves to the situation, making use of available resources and techniques such as OODA loops[33] or Active Cyber Defense Cycle.[34]

An example of an Incident Dashboard table is provided in Appendix C - Incident Dashboard and Reporting Example.

Dedicated incident response or project management tools such as TheHive[35] are recommended. However, this information could simply be recorded on a whiteboard within an IR incident room, or captured electronically using Excel, which is achievable for any level of IR capability or maturity of an OT operator.

As cybersecurity regulations have evolved, the requirement for reporting cybersecurity incidents to regulatory bodies has become well-established for many OT defenders, particularly those under the jurisdiction of NERC regulations or NIS Directive derivatives. Reporting requirements under NERC CIP are clearly defined for electric sector operators in North America. For operators of essential services across Europe, reporting to regulators of the NIS Directives derivatives is now established. For these regulatory reporting requirements, it's prudent to **create a template with the required information, contact details and timing requirements** and reference it within an OT incident response plan, reducing the possibility of failing to collect key required information during the stress of a genuine incident.
It may also be beneficial to test reporting with the regulatory body as part of the regular incident exercises to ensure effectivity or templates and processes.

33 https://csrc.nist.gov/CSRC/media/Presentations/The-Cyber-OODA-Loop-How-Your-Attacker-Should-Help/images-media/day3_security-automation_930-1020.pdf

34 https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/

35 https://thehive-project.org/

Putting the Actions into a Plan and the Plan into Action

Critical Control #1 from the SANS Whitepaper *"The Five ICS Cybersecurity Critical Controls"*[36] states that OT defenders should have an ICS-specific Incident Response Plan (IRP). Ideally, all recommendations provided in this paper should be addressed within that ICS-specific IRP. This may not be attainable for all OT teams today, however all the recommendations can be placed onto a roadmap for implementation as the organization matures in capability. Regardless of the approach OT defenders take to develop their cybersecurity maturity and incident response preparation, two overarching requirements exist:

- Document an OT specific Incident Response Plan
- Exercise the OT Incident Response Plan

An ICS-specific IRP doesn't need to be perfect before it is documented, but it does need to be documented. The IRP should also be considered an evolving document that needs to be maintained and updated regularly. With an increase of cybersecurity maturity in an industrial environment, additional capabilities or requirements might develop.

Exercising doesn't need to be full scale adversary simulation across multiple days or teams. Exercising can start by being as simple as an informal walkthrough of a procedure, or an hour-long generic tabletop exercise using a scenario from the SANS resource on OT IR Tabletops.[37] The procedures required during incident response can also be walked through as drills to further refine them and increase the team's familiarity with them during less stressful situations. Organizations can then work up to perform evaluation and continuous improvement of their capability through facilitated tabletop exercises, either generic in nature or customized to their environment and goals.

Conclusion

Effective Incident Response requires a solid foundation of preparation and planning. Effective Incident Response within an OT environment requires adaptation of emergency planning, incident management and digital forensics to cater for differences of OT compared to IT systems.

OT defenders should make use of existing resources and capabilities, and tailor them to be effective for their OT environments by following the recommendations established in this whitepaper and the references provided within. In doing so, OT defenders can quickly establish a solid foundation of preparedness that will prove valuable if a genuine incident occurs.

36 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

37 https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/

Appendix A – Acronyms Table

BCP	Business Continuity Plan
CIRT	Computer Incident Response Team
CMF	Collection Management Framework
DCS	Distributed Control System
DFIR	Digital Forensics and Incident Response
DRP	Disaster Recovery Plan
EDR	Endpoint Detection and Response system
ERP	Enterprise Resource Planning systems
HMI	Human Machine Interface
ICS	Industrial Control System
ICS (NIMS)	Incident Command System (National Incident Management System)
IM	Incident Management
IR	Incident Response
IRT	Incident Response Team
IT	Information Technology
OODA	Observe, Orient, Decide, Act
OT	Operational Technology
PA	Public Address system
PICERL	Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned
PLC	Programmable Logic Controller
PPE	Personal Protective Equipment
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SOC	Security Operations Centre
TTP	Tactics, Techniques and Procedures
TTX	Tabletop Exercise
WAR	Work and Resources Room

Appendix B – Incident Response Preparedness Key Actions Checklist

COMPONENT	DRAGOS RECOMMENDATION	COMPLETED
Facilities	Documented processes and authorizations obtained for information sharing and data transfer to IR support teams	☐
	Established and tested out-of-band communication	☐
	Suitable room for the incident response team to use located	☐
Equipment	CMF(s) prepared that document which log sources are available, their retention period and location, and who within the organization has authority to access them	☐
	Exercise the IRP and practice situational awareness referring to the CMF(s)	☐
	Forensic collection tool(s) tested and are pre-qualified for use	☐
Personnel	Documented assessment of IR external support that would be required, and assign a single point of contact to coordinate it	☐
	Dedicated Incident Commander appointed	☐
	Site champion(s) assigned to help communicate site specific information to the IRT	☐
	Documented competence requirements for on-site personnel with responsibilities for incident response activities	☐
Procedures	Assess coverage of procedures (tools and skillsets) required to perform analysis across the four categories of data sets from an OT environment	☐
	Forensic collection tools complemented with site specific forensic collection procedures and playbooks	☐
	Use a Focus, Prioritize, Collect methodology within forensic collection procedures	☐
	Documented procedures for transfer of collected artifacts from the OT environment to a platform for forensic analysis	☐
	IRT's should make the conscious and recorded decision to enact predefined containment and eradication strategies	☐
	Documented procedures for OT network disconnection and individual host isolation	☐
	Capability confirmed to test and validate the effectiveness of IRT team actions for containment and eradication	☐
	Documented assessment of the organization/site/facility RPO and RTO	☐
Communications	Severity matrix incorporated into an OT specific incident response plan	☐
	Established IR battle rhythm meeting agenda and reporting board	☐
	Documented IR battle rhythm template with the required information, contact details and timing requirements	☐

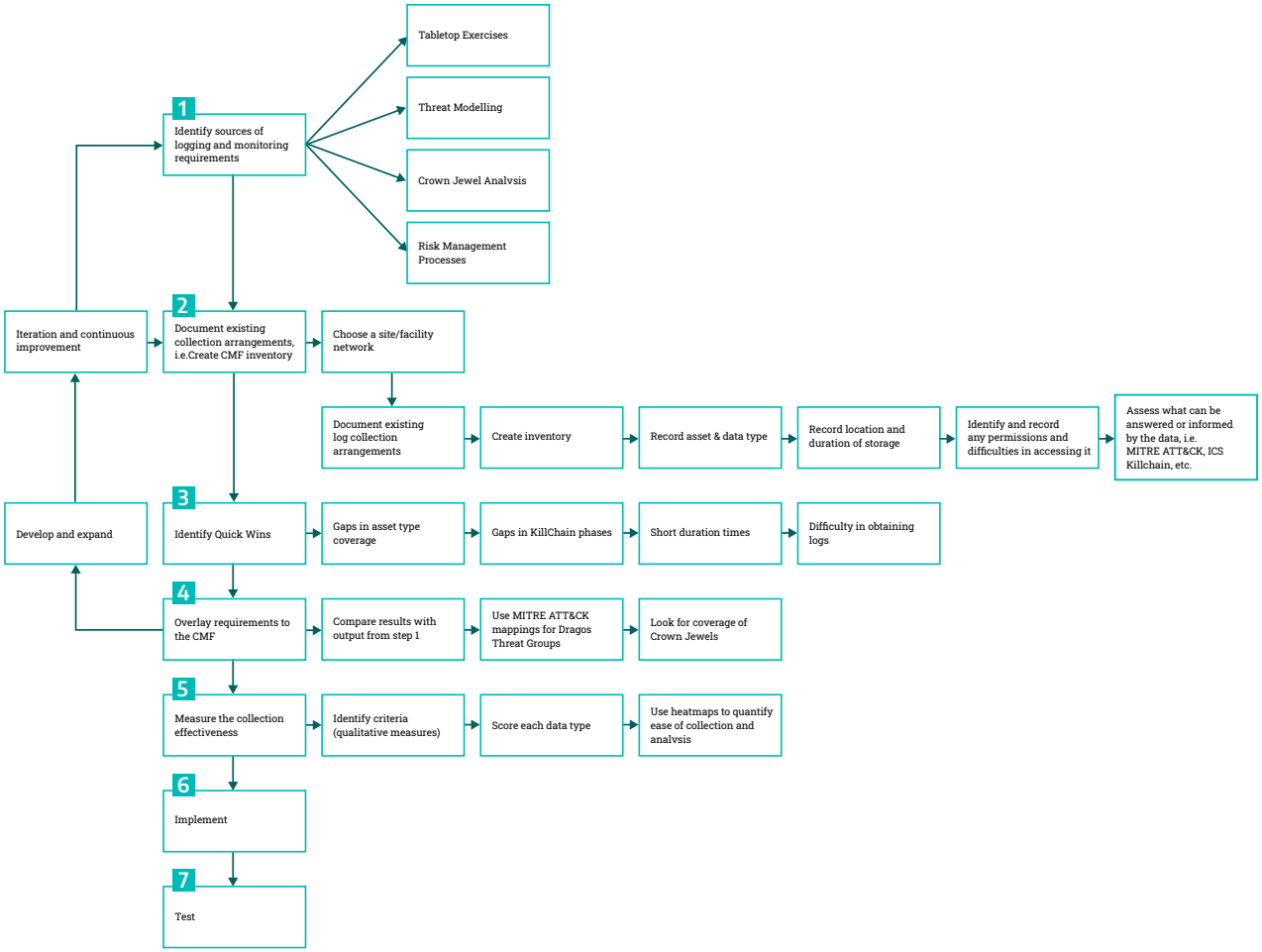
Appendix C – Methodology for Creating and Developing a CMF

Introduction to CMF

The Collection Management Framework for OT is a *"a structured approach to identifying data sources and what information can be obtained from each source"*.[38] The methodology is tailored for OT environments and provides a model for identifying, implementing, and testing requirements using a range of techniques. The approach considers which events would trigger the identification of new logging and monitoring requirements. For example, following the response to an incident and the lessons learned phase some new monitoring and logging scope may be identified.

Additionally, the approach also considers follow-on sources of logging and monitoring collection to aid the response team in identification, triage, and incident response analysis. This proactive approach also provides the asset owner/operator with an understanding of the tasks required to obtain the information. For example:

- is the collection a manual or automatic process?
- how difficult is it to obtain the data?
- what support required to obtain the data?
- which tools and procedures are required to obtain and analyze the data?



38 https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/

Step 1. Identify Sources Logging and Monitoring Requirements

As described above, the CMF for OT approach considers how to form requirements from different activities and initiatives. A key principle to consider in this approach is that the CMF should be dynamic in its formation and maintenance; it can be created relatively quickly and updated regularly. This is particularly useful for legacy environments where a detailed risk assessment can take a significant amount of time and resources to complete.

Four activities that can be used to identify requirements are:

Tabletop Exercises

OT specific tabletop exercises (TTX) are used to test the response capabilities of an asset owner/operator. Ideally, the exercises will prompt the response team to consider how to use their incident response plan to identify, contain, eradicate, and recover from the cyber incident. During these exercises and the lessons learned activities within their conclusion, the incident response team will likely determine improvements that could have been made in their response in terms of their ability to investigate and validate assumptions related to the incident. These exercises can therefore be useful in identifying additional logging requirements or identifying improvements to existing log forwarding or collection arrangements.

Threat Modeling

Obtaining and using threat intelligence can provide a source of requirements for monitoring and logging, aligned, and mapped to frameworks such as MITRE ATT&CK. For example, threat briefings associated with specific incidents, which can be mapped to MITRE ATT&CK for ICS, provide detail of threat actor tactics, techniques, and procedures. Known threat tradecraft used to gain access to, and cause impacts within, OT environments can be used to create requirements for logging and monitoring to detect and respond to those same TTPs.

Another example is from threat intelligence feeds provided by dedicated OT security threat intelligence research teams, that cover threat actor groups in general. This information can be used to determine which threats are relevant to a particular industry vertical and region to increase the applicability to an organization and provide a means to validate assumptions on threat behavior and an organization's ability to detect and respond to applicable threats.

Crown Jewel Analysis (CJA)

A Crown Jewel Analysis (CJA) is a structured and repeatable method for understanding the assets which can have the highest consequence to a business or operation. This also enables the organization to understand and prioritize what logging and monitoring is in place to protect those assets, and to understand the most likely kill chains and threat TTPs which are applicable to them. A CJA focused approach equips OT defenders with a plan of where to start and how to prioritize the logging and monitoring of a legacy system. This is especially useful if the OT network is large and relatively unknown, where it can be daunting to develop a logging strategy in its entirety.

Risk Management Processes

Risk assessments often result in the recommendation to "perform monitoring", but most will not identify in enough detail what to monitor. However, if risk assessments have been performed for a system or zone, such as a completed risk assessment of a System under Consideration (SuC) following the IEC 62443-3-2 methodology, the output from that assessment can be used a source of requirements for the CMF. In other words, the Security Level (Target) that is being set for the system may include derived requirements for logging and monitoring. For example, consider a system with an SL-T of 2, requiring "unique authentication and identification of human users". This may derive requirements for logging of authentication logs, and monitoring in place to detect failed authentication attempts.

Step 2. Document Existing Collection Arrangements

Using one or more of the above techniques to identify requirements, the results can be documented into a simple table using a whiteboard, spreadsheet or other simple tool. The table headings can be adjusted to suit the asset owner or OT network. An example is provided below:

Step 3. Identify Quick Wins

The value in the simplified CMF process is being able to quickly identify the existing logging and monitoring coverage and determine quick wins to address shortfalls and gaps. For example, easily identifying where coverage is lacking from key assets and crown jewels, identifying where log retention is short, or identifying log sources which are difficult to access.

Step 4. Overlay Requirements to the CMF

The next step involves the addition of TTPs which are required to be monitored, and analysis to determine if the existing arrangement allows for monitoring of those TTPs. A good example of this is using the MITRE ATT&CK framework to map out threats which are of particular interest to an operator, or simply using examples from recent OT cyber-attacks mapped to TTPs to determine coverage against specific threats or to benchmark using OT incidents and known events.

LOCATION/ ZONE	ASSET TYPE	DATA TYPE	ICS KILL CHAIN PHASES	DATA STORAGE DURATION	EASE OF ACCESS	FOLLOW ON COLLECTION
Follow on Collection	Workstation	Event Logs	Exploitation, Installation, Actions on Objectives	60 days	Difficult	Memory
Plant Control Network (PCN)	Network Intrusion Detection System	Alerts	Lateral Movement	12 months	Easy	Ruleset, packet captures

Develop and Expand

Repeat the process across other sites to identify any systemic gaps and to increase the coverage across the wider estate of OT networks. For example, when completing multiple CMFs across other facilities, using the approach to identify if there are commonalities in how logs are collected (or not) or how devices are configured.

Iteration and Continuous Improvement

Once the CMF document is established, it should be protected, maintained, and periodically audited for completeness. Routine reviews can be performed to look for changes made to frameworks the CMF is mapped to (such as MITRE ATT&CK for ICS), or following any changes made to asset and network configurations that the CMF represents.

Identification of new requirements when opportunities are presented can be included. For example, following an incident response investigation, or upon the discovery of a new threat or vulnerability.

Step 5. Measure the Effectiveness

Measuring the effectiveness of the CMF is performed by firstly identifying some criteria (qualitative measures) to score the current version. Examples of criteria could be maturity of the log source, authority to collect, ease of access to the log source. Using the criteria, each data type identified in the CMF can be scored across a scale. For example, for maturity of log source the scale could range from the collection of a log source having never been performed before, up to the collection being performed routinely. Using a simple color scheme, the CMF can then be updated to create a heatmap that highlights areas of improvement.

Step 6. Implement

Using the outputs from the previous steps (i.e., the first revision of the CMF document) an implementation plan can be formed to address gaps and shortfalls based on the logging and monitoring source. For example, an implementation plan may be required to change the configuration of logging settings of applications across an environment, or network monitoring solutions may need to be specified with associated network taps or span/mirror port configurations. The implementation phase may also consist of establishing procedures for manual log collection from OT assets, or analysis procedures for performing IOC sweeps of collected artifacts.

Step 7. Test

The testing phase may include a range of tests and procedures, dependent on the implementation phase. For example, the testing of procedures for collection from the identified log sources, or the testing and commissioning of a network monitoring solution and integration to a SIEM solution or managed services provider.

Appendix D - Incident Dashboard and Reporting Example

At a minimum, the following can be used to track incident response team actions and the summary of information received from IRT members.

RESPONSE TRACKING								
INFORMATION RECEIVED			ACTIONS ASSIGNED				ACTIONS COMPLETED	
INFORMATION	SOURCE	DATE - TIME RECEIVED	ACTION	ASSIGNED TO	PRIORITY	DATE-TIME ASSIGNED	ACTION & RESULT	DATE-TIME COMPLETED
Notification of suspected organizational breach	Government Agency	2022-04-22 1400 UTC	Assemble Incident Response Team	Incident Commander	High	2022-04-22 1530 UTC	IRT comms stood up, incident status report logged in dedicated comms channel	2022-04-22 1730 UTC
n/a	n/a	n/a	Investigate network traffic for new or suspicious connections	OT Security Analyst	High	2022-004-22 1730 UTC	Updated incident status report - no new connections identified from initial analysis. Continuing to analysis available logs	2022-04-22 2000 UTC
Plant operating status reported as normal.	Ops manager	2022-04-23 0800 UTC	Update incident status report	Duty incident information handler	Low	2022-04-23 0830 UTC	Incident status report updated	2022-04-23 0900 UTC
Threat intelligence report states that vendor X devices are being targeted	Threat Intelligence provider & Information sharing portal	2022-04-23 0900 UTC	Contact vendor and establish communications	System Owner	Medium	2022-04-23 0930 UTC	Vendor contacted and agent assigned to provide support as per SLA.	2022-04-23 1430 UTC

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.