WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Cyber Threat Scenarios and Protection Steps for Manufacturing

Preventing, Detecting, and Responding to Relevant Threat Scenarios

GLORIA CEDILLO | SENIOR INDUSTRIAL CONSULTANT
MIKE HOFFMAN | CONSULTANT TECHNICAL LEAD
SHAUNNA HARGRAVE | INDUSTRIAL CONSULTANT
DRAGOS, INC.
AUGUST 2023

TABLE OF CONTENTS

Executive Summary 3
Cyber Risk Overview for Manufacturing 5
Scenario 1: Ransomware 6
Scenario 2: Trusted Vendor Compromise 7
Scenario 3: Shared IT/OT Dependencies 8
Scenario 4: PIPEDREAM 8
Potential Impacts in a Manufacturing Environment 11
Recommendations Summary 12
Prevention Recommendations 14
Detection Recommendations 16
Response Recommendations 18
The Destination, the Journey, and What You Need to Get There 21
References 22

Executive Summary

Cybersecurity Risks to Manufacturing Operations

Manufacturing systems are tightly integrated. An attack on one system can cause cascading impacts through an entire plant, leading to a complete loss of revenue. Downstream effects to any dependent operations increase the impact.

Threat scenarios are essential components of cybersecurity planning for operational technology (OT) environments, offering a range of key benefits. They facilitate risk assessment by pinpointing vulnerabilities and prioritizing resource allocation. Preparedness planning is enhanced through simulated threat scenarios, helping manufacturers evaluate their readiness and identify security control gaps. Proactive defense measures are informed by threat scenario analysis, enabling the implementation of security controls to mitigate risks. Incident response planning benefits from scenario simulations, allowing organizations to devise effective strategies, define roles, and outline containment and recovery procedures. Regular training based on threat scenarios educates employees, aligning with compliance requirements and fostering continuous improvement. Ultimately, leveraging threat scenarios empowers manufacturing organizations to enhance security, readiness, and resilience in OT environments, thereby minimizing the potential impacts of cyber threats like the scenarios discussed in this paper: ransomware; trusted vendor compromise; shared IT/OT dependencies; and PIPEDREAM.

Industrial ransomware targets manufacturing over 70 percent of the time, and ransomware attacks can be carried out by traditional IT ransomware gangs that cross over into OT environments due to linkages between OT and IT assets. Additionally, there are 22 Threat Groups that specialize in industrial cyber attacks; five of those target manufacturing, including two new groups in 2022 - CHERNOVITE and BENTONITE.

Attackers are working hard to create new purpose-built modular malware for ICS/OT at high scale. PIPEDREAM, discovered in 2022, is the seventh known ICS-specific malware that targets core software functions impacting millions of devices across thousands of equipment types and numerous vendors. The scale of reach and potential impact is unprecedented.

Dependency on third parties is increasing – remote access into OT systems – and cross-over between OT and IT systems create additional risk factors that accelerate with digital transformation, smart factories, and related initiatives.

THREAT SCENARIO	DESCRIPTION
Ransomware	Ransomware's initial access can come from different paths, such as remote connections or leveraging IT/OT dependencies. The attack starts with exfiltrating information, encrypting files, and finally locking the compromised computing systems with requests for ransom payment to unlock systems, recover stolen data, and not sell to prospective buyers. Most ransomware targets the IT environment. However, IT/OT dependency is very high in many environments, so continuing operations after an attack depends on how well OT can be isolated and operated independently from IT.
Trusted Vendor Compromise	As an example, software used for updating end users' assets becomes compromised at the vendor before even being distributed. These compromises can be exploited in ways that affect the supply chain.

THREAT SCENARIO	DESCRIPTION
Shared IT/OT Dependencies	OT dependencies on IT resident systems, shared IT/OT domains, or insecure remote access into OT all create an environment where IT compromise can cross into OT and cause disruption.
PIPEDREAM	A highly scalable and capable family of industrial malware that includes attack methodology and compromises with embedded OPC-UA and CODESYS software components embedded in thousands of systems, impacting millions of assets.

Implications of Attack

Depending on the malware functions and attack intentions, attacks can target manufacturing operations by affecting:

1) **Manufacturing Execution Systems (MES):** The MES comprises different subsystems, but it is highly critical in manufacturing as it interchanges the data between business and operations.
2) **Plant floor assets such as Human Machine Interfaces (HMIs) and controllers:** The HMIs and the controllers are the plant's brains and eyes; without these systems, the equipment, rooms, and labs cannot be operated or controlled, which halts manufacturing production.
3) **Enterprise Resource Management (ERP):** Like the MES, this system is comprised of several subsystems that are normally part of the manufacturing industry's corporate side. The system concentrates the plant data downtimes, and production constraints.

Summary of Recommendations to Defend OT

The threats and impacts mentioned above can be prevented and mitigated by following general steps that, according to the capabilities and environment, should be detailed with specific procedures and detections. Dragos believes that framing those protections with the *SANS 5 Critical Controls for OT Security* provides helpful guidance and an achievable approach. The detailed guidelines that aid manufacturing in implementing security controls to defend against the threats mentioned in the sections below should be paired with specific procedures and detection technologies, tailored to your organization's capabilities.

STAGE	RELEVANT CRITICAL CONTROL	RELATED ACTIONS
PREVENT	#2 Defensible Architecture	Network segmentation: domain, credential, and privilege segmentation that limits the ability for threats to enter and traverse OT environment.
	#3 ICS Network Monitoring & Visibility	Enables asset inventory that is the basis of tracking vulnerabilities, identifying critical systems, understanding traffic flows, and monitoring/validating controls.
	#4 Secure Remote Access	Core technology and deployment architecture that minimizes the risk of access into OT environments. Requires proper technology and architecture implementation.
	#5 Risk Based Vuln Management	Awareness of vulnerabilities tied to assets in the environment, with a risk analysis of impact and likelihood plus alternative mitigation to minimize risk until the maintenance window/patch.

STAGE	RELEVANT CRITICAL CONTROL	RELATED ACTIONS
DETECT	#3: ICS Network Visibility & Monitoring	Continuously monitoring the environment to identify potential threat behaviors, validate security controls; providing an event dashboard and information to investigate events.
RESPOND	#1: ICS Incident Response Plan	Plan that proactively defines people, roles, and procedures to effectively respond to potential security events; considers the unique character of investigating events in industrial settings. A tested IRP is increasingly required by government regulations.
	#3: ICS Network Visibility & Monitoring	Provides logging and forensic records that enable simpler investigation and root cause analysis.

Cyber Risk Overview for Manufacturing

New Threat Groups Contribute to Increase in Manufacturing Attacks

The cyber risk to industrial sectors has grown and accelerated dramatically in recent years. Operational Technology (OT) and Industrial Control Systems (ICS) cyber threat activity continues to rise in terms of the number of distinct threat groups and the industries and regions these threat groups are targeting. Manufacturing systems are often tightly integrated and are highly dependent on multiple product lines and cells working in unison to create a part, assembly, or product. Therefore, an attack on one system can cascade impacts onto an entire plant or even affect other industries, as one plant can be the supply chain for another.

Because of the similarities between some OT and IT assets, a cyber adversary with minimal process understanding can connect to the operational networks and perform non-targeted actions, potentionally causing disruption or system damage, against those systems without requiring complex offensive tools. With high IT/OT interconnectivity and reliance on vendor remote support and maintenance, the manufacturing sector is vulnerable to cyber attacks that can disrupt operations, put individual and community safety at risk, and impact the supply chain.

Ransomware attacks on industrial infrastructure organizations nearly doubled in 2022, with over 70 percent of all ransomware attacks targeting manufacturing. Risks are especially increased in OT networks with poor segmentation and lack of remote access security. The Dragos 2022 Year in Review research shows that attacks on manufacturing have accelerated, with increased attacks in the food and beverage and pharmaceutical industries.

The Year in Review also highlights five Threat Groups that can actively target manufacturing sectors. Two of these Threat Groups, CHERNOVITE and BENTONITE, are newly active in manufacturing. Furthermore, PIPEDREAM, the seventh known ICS-specific malware, was identified, demonstrating significant ongoing investment into weaponizing OT cyber capabilities. These capabilities discovered could be easily deployed against manufacturing assets, as software and hardware are highly used in manufacturing.

Manufacturers struggle to obtain the necessary funding to procure cybersecurity technology, let alone the human resources to implement, maintain, and monitor the technology. Without these resources, they will be unable to quickly detect and respond to a cybersecurity incident before significant operational impacts occur, costing time, money, and supply chain disruption. Only with an approach that combines IT-centric visibility with OT-relevant

analysis and awareness can we adequately understand the nature of cyber intrusions in operational environments and justify the importance of comprehensive programs to mitigate the risk.

Scenario 1: Ransomware

Manufacturing is Targeted in 72% of Industrial Ransomware Cases

Ransomware is one of the main threats to manufacturing because disrupting the IT environment can also impact production operations. Even though the main achievement of ransomware attacks is within Stage 1 of the ICS Cyber Kill Chain, manufacturing operations are often highly impacted due to the interdependency between IT and ICS/OT systems to maintain the performance of the plant, logistics, operations data, and quality control. Adversaries look to exploit trusted data pathways, crossing between IT/OT systems where poor network segmentation practices, and security controls are prevalent.

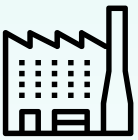
The Dragos Year in Review reports that ransomware attacks targeted 437 manufacturing entities in 104 unique manufacturing sub-sectors. Of these attacks, 9 percent targeted food and beverage, and 4 percent targeted pharmaceuticals. Ten percent of victims were in metal products manufacturing, 9 percent were in automotive, six percent were in electronic and semiconductor, 5.7 percent were in building materials, 5.5 percent were in industrial equipment and supplies manufacturing, and 5 percent were in plastics.

87%

Ransomware attacks against industrial organizations **increased 87 percent** over last year.

+35%

Dragos tracked **35% more ransomware groups** impacting ICS/OT in 2022.



72%

of all ransomware attacks targeted **437 manufacturing entities** in **104 unique manufacturing subsectors**.

2017 NotPetya Attacks

A well-known ransomware attack is the series of NotPetya attacks on June 27, 2017, which affected pharmaceutical companies and several industrial organizations. Merck, one of the affected companies, announced that the cyber attack impacted global operations, including manufacturing. SEC filings revealed that production outages resulted in the inability to fulfill orders for certain products, with the supply of the Gardasil vaccine being particularly affected. Since 2006, nations worldwide have increasingly incorporated the HPV vaccine into their national immunization schedules, and Merck was a major supplier of this vaccine. Therefore, the impact on the supply chain was not limited to a specific region but had worldwide and unpredictable consequences. Merck arranged to borrow supply from the US CDC strategic stockpile to address the disruption until production could catch up.

According to IBM's 2022 Cost of a Data Breach report, the pharmaceutical industry ranked third in terms of the average cost impact, only trailing behind healthcare and the financial industry. The report also highlighted that highly regulated industries, including pharmaceuticals, experience ongoing financial impacts for longer periods following a security breach compared to other sectors. This aligns with anecdotal evidence seen in the case of Merck, where cost estimates for the NotPetya incident continued to emerge over the years, ultimately resulting in a $1.4 billion insurance settlement nearly five years after the incident occurred, as evidenced by court documents.

This attack started as a supply chain attack where a vendor's software was compromised, and the attack targeted IT networks and affected manufacturing, sales, and research and development. NotPetya does not encrypt files but the hard drive Master File Table (MFT), which renders the Windows Operating system reboot impossible. The MFT is the database that has the directory of every file on a computer hard drive.

Scenario 2: Trusted Vendor Compromise

In trusted vendor compromise attacks, software for updating end users' assets becomes compromised at the vendor before even being distributed. These compromises can be exploited in ways that affect the supply chain. As an illustration, consider the well-documented SolarWinds incident of 2020. During this event, the Orion software developed by SolarWinds was infiltrated by the Sunburst malicious code, which had the malicious intent of surreptitiously extracting data and sensitive information. A number of users fell victim to compromise after innocently updating their software from Orion SolarWinds. These impacted users spanned across various industries such as manufacturing, pharmaceuticals, and the food and beverage sector. This incident is commonly referred to as a supply chain attack. Microsoft Threat Intelligence Center (MSTIC) attributes the 2020 SolarWinds compromise to the threat group NOBELIUM, the moniker provided by MSTIC for APT29.

A watering hole attack is another attack type wherein adversaries compromise vendor websites where end users trust the site to download software updates, applications, functions, or tools. In June 2014, a new variant of the Dragonfly trojan targeted pharmaceutical industries by compromising a trusted vendor for ICS/OT that OEMs in manufacturing normally use to download the controllers' software. Although these trojans did not initially risk the plant's equipment or operation, they put the plant's production at risk, as the main goal of the attack was to steal information, including recipes and batch productions. The attack also included collecting network information that could later be used for further and more studied attacks.

> Microsoft has observed NOBELIUM targeting privileged accounts of service providers to move laterally in cloud environments, leveraging the trusted relationships to gain access to downstream customers and enable further attacks or access targeted systems. These attacks are not the result of a product security vulnerability but rather a continuation of NOBELIUM's use of a diverse and dynamic toolkit that includes sophisticated malware, password sprays, supply chain attacks, token theft, API abuse, and spear phishing to compromise user accounts and leverage the access of those accounts.
>
> **— MICROSOFT SECURITY BLOG —**
> NOBELIUM targeting delegated administrative privileges to facilitate broader attacks: https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

Initially discovered in 2013, Dragonfly was a malware campaign targeting ICS industries, mainly the energy sector. The malware does not intend to disrupt operations but instead gathers information from plant control systems. The campaign started with spear-phishing and then moved to waterhole techniques to redirect to a Dragonfly-operated website, and finally leveraged trojanized ICS software on vendor websites. These three techniques all focused on getting HAVEX malware installed on ICS/OT systems. Once installed, the HAVEX malware communicates back to a command-and-control server and leverages an OPC-DA payload, which begins to scan the ICS/OT environment looking for OPC-DA servers and exfiltrate data back to the advisory for reconnaissance.

Scenario 3: Shared IT/OT Dependencies

The data interchange between business and plant operations is essential in manufacturing, as both systems are interdependent in calculating resource usage, forecasting, and handling operations data. These interconnected systems often require the use of remote connections. In many cases, manufacturers will leverage shared credentials across the environment for ease of use. However, these shared credentials are one of the main targets that adversaries look to steal, as they can use them as entry points into manufacturing systems. The Dragos Year in Review highlights that 73 percent of manufacturers assessed still have shared IT/OT user management, such as Active Directory domains where user management and assets belong to the same domain as ICS/OT assets, allowing adversaries to pivot from one system to another.

One of the main risks of unsecured IT/OT interconnections is the spread of ransomware and malware to OT systems. For example, the EKANS malware leverages the trust between IT and OT networks by looking for ICS-related Windows processes such as SQL databases, historians, or HMI web services. Although this malware does not manipulate or command the ICS/OT assets, it primarily seeks to provoke loss-of-view or denial-of-service to the compromised assets. This can disturb the plant due to the performance reduction on the network and limited access to certain assets.

As it relates to pharmaceuticals, APT threat groups have historically been observed targeting intellectual property, as discussed in the scenario. This theft of information may be used to accelerate national interests by providing companies a shortcut into a dynamic market with current techniques, technology, and previously tested solutions. The ability to control the supply of pharmaceuticals has already been established through the various government proclamations valuing the industry as critical, and accordingly, other nations may have a strategic interest in gaining or advancing their country's capabilities in this area.

Scenario 4: PIPEDREAM

In early 2022, Dragos discovered and analyzed the PIPEDREAM malware, which specifically targets industrial control systems. Fortunately, this malware was detected before it could impact any industrial systems. However, it is important to note that it may still be part of the adversary's toolkit or undergoing further development. This situation presents an opportunity to learn and prepare for potential attacks on our infrastructure before PIPEDREAM or similar malware is deployed.

PIPEDREAM possesses capabilities that can affect various technologies commonly found in manufacturing environments. This malware represents an ongoing evolution of industrial malware and highlights that adversaries actively invest resources to attack industrial infrastructure by developing malicious toolkits like PIPEDREAM.

PIPEDREAM: CHERNOVITE'S Emerging Malware Targeting Industrial Control Systems whitepaper highlights that this malware is a highly capable offensive ICS attack framework. It can execute 36 known ICS attack techniques (which is 46 percent of known ICS attack tactics) as measured against the MITRE ATT&CK for ICS behavior matrix.

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify Formware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Blockk Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication via Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

As shown in the figure above, the malware impacts different levels of the Purdue Model through five distinct modules. Two of them leverage Windows capabilities to deploy the malware, while the other three modules are designed to interact and directly scan ICS/OT assets, including servers running OPC-UA, and PLCs utilizing CODESYS or Omron Software.

The following list describes examples of how the malware acts through the four levels of the Purdue Model:

- **DUSTTUNNEL,** distinguished for a remote operational implant to perform host reconnaissance and command and control, can be exploited at Level 4 of the Purdue Model (IT and Corporate Network) combined with a phishing attack to facilitate access to adversaries.
- **LAZYCARGO** enables persistence or privilege escalation on an engineering station by exploiting a vulnerable Windows driver (CVE-2020-15368).
- **MOUSEHOLE** interacts with OPC-UA servers and can read and write node attribute data, enumerate OPC-UA Servers namespace and associated Nodelds, and brute force credentials. This module can be leveraged on assets such as OPC and HMI servers, SCADA, and Historians as implemented.

- **BADOMEN** is designed to scan, identify and interact with Omron's NX/NJ controllers series. Dragos found that this module can crash the controllers disturbing their operation. BADOMEN also has a module that to affects Servo drives series R88D-1S by allowing modifications on their parameters. It can modify certain drive parameters to affect the motors' operations, such as speed and rotation direction. Furthermore, this module allows logic modifications to manipulate more complex automation processes.
- **EVILSCHOLAR** is another module dedicated to affecting PLC functionality and targeting the operations at a plant. This module is designed to discover, access, manipulate and disable Schneider Electric PLCs. The module can also target additional hardware through the CODESYSv3 library. The attacks include directly modifying the controller's logic and slowing their operation performances. PLCs and Servo drives are critical on the industry as they directly interact with the plant's physical equipment.

The graphic below illustrates how each PIPEDREAM module interacts across the different levels of the Purdue Model and traverses from the IT to ICS/OT network.

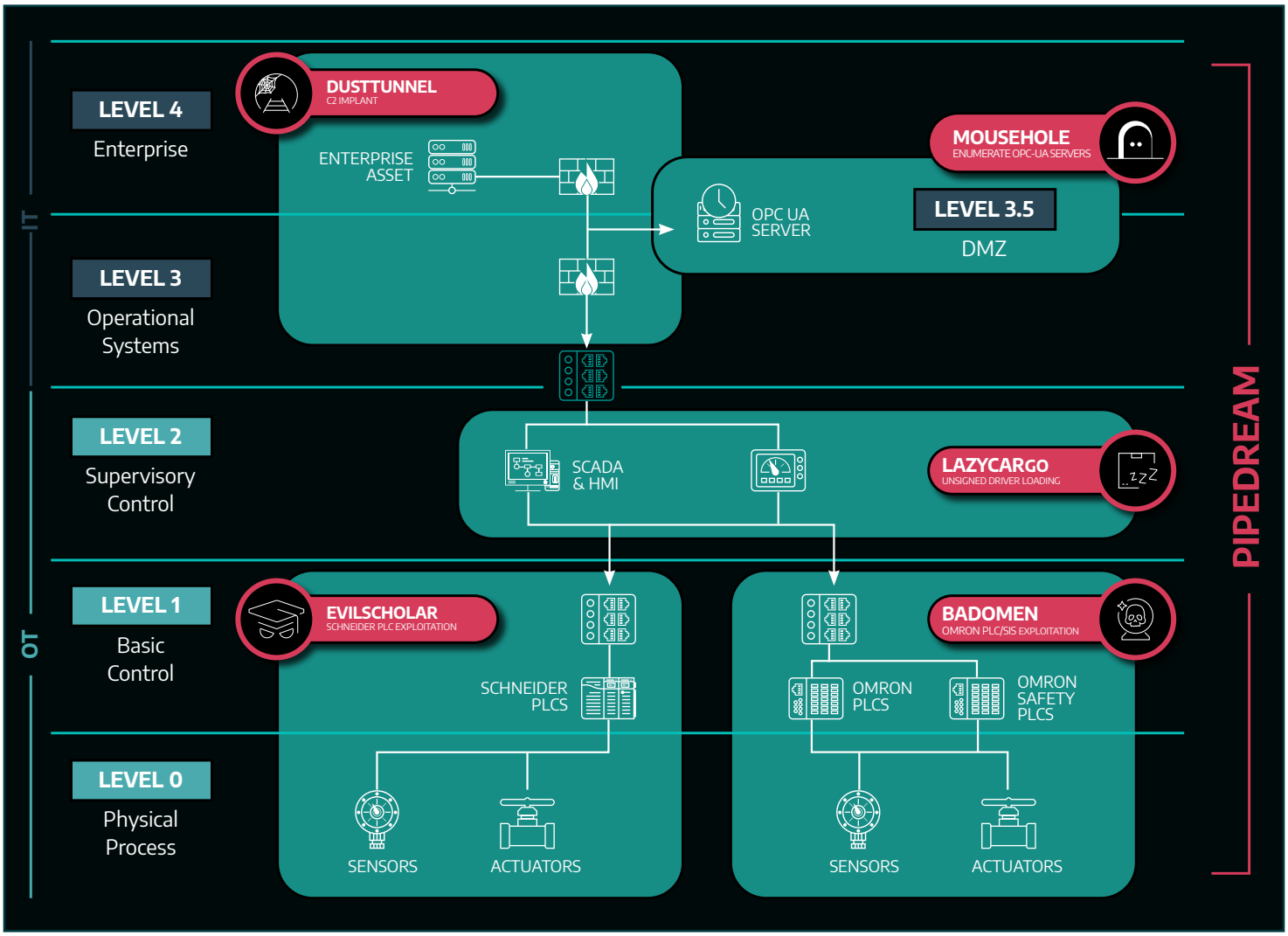


Fig 1: Example of the deployment scenario across the Purdue Model, using the different modules

As malware evolves to interact with industrial controllers through modular capabilities, the potential for such attacks increases. Considering the ongoing advancement of industrial malware, as evidenced by the discovery of PIPEDREAM in early 2022, this threat remains a concern for all manufacturing sub-sectors.

Potential Impacts in a Manufacturing Environment

Depending on the malware functions and attack intentions, attacks can target manufacturing operations by affecting any of the three main systems of a plant.

Manufacturing Execution Systems (MES):

The MES comprises different subsystems, but it is highly critical in manufacturing as it interchanges the data between business and operations. Manipulating its data can impact plant operations or production forecasts and outage plans. Some of the functions that can be impacted in this system are tracking systems, recipes, inventory management, and quality control. Although injecting strategically incorrect data into tracking, materials, or batch records may not impact the functionality or operation at the plant, it can have tangent production and quality impacts. These can lead to missing compliance requirements, ultimately affecting production as systems are shut down for investigations. The information that the MES system handles is also valuable for external actors. For example, if information from a recipe is stolen, this can affect marketability as a competitor can use it by making slight changes without violating any laws.

Plant Floor Assets Such as Human Machine Interfaces (HMIs) and Controllers:

HMIs and controllers are the plant's brains and eyes; without these systems, the equipment, rooms, and labs cannot be operated or controlled, which halts manufacturing production.

Safety and equipment damage is another significant concern; affecting set points, alarms, controller functions, and interfaces can cause worse problems than just stopping a machine. Manufacturing is such a diverse industry – for example, even though a plant may not manufacture chemicals, it can handle them, including toxic and explosive substances. If set points or controllers' functions do not work properly, it can cause an accident at the plant. Tanks can spill or mix incorrect substances, leading to chemical poisoning or explosions. The food industry, for example, gives special attention to Cleaning-In-Place (CIP) systems that utilize chemicals to maintain clean containers to avoid food contamination. If this system is affected, it can greatly impact the enterprise and even create legal issues.

Safety also applies to equipment where mechanical forces, safety gate access protections, and emergency stops are handled through different controllers. If any of those fail, it can provoke accidents that could harm people, such as flying steel sheets or crush injuries due to pressing machines or robots.

Enterprise Resource Management (ERP):

Similar to the MES, this system is composed of several subsystems that are normally part of the manufacturing industry's corporate side. The system concentrates plant data, downtimes, and production constraints. It is also used to manage resources and plan business strategies. This system can also have relevant information for materials

production, recipes, and external customer information. The information handled in this system is critical for the industry's product strategies and manufacturing production.

MES and ERP systems are the most exposed to ransomware attacks due to the ERP (and even sometimes the MES) sitting on the corporate network. They share similarities with the IT software, the information they maintain, and the frequent data interchange between business and operations systems. The ransomware impact on the ICS/OT systems partly depends on the overall architecture segmentation and underlying sub zones and conduits further down at the plant floor. For example, how well the network can be isolated from a compromised MES system and maintain operations. Just as important, however, is how well the compromised asset(s) can be recovered due to the immutability of the backup, their Recovery Point Objective (RPO), and backup quality. This means that even if a manufacturing facility is targeted by ransomware, it can be less impacted due to the proper security controls around recovery and segmentation to maintain safe and reliable operations.

Besides these three main systems, manufacturing has quality control labs and research and development departments. The relationship of these systems to production will depend on an organization's structure but compromising them also highly impacts manufacturing production. Additionally, if research data is stolen, it can also impact brand trust as the information can be manipulated or published with political or activist motivations. For example, several nation-states attempted to steal vaccine-related intellectual property in the wake of the COVID-19 pandemic.[1]

These systems, including the MES and ERP and in certain cases SCADA applications, are migrating to cloud infrastructure to reduce the capital expenditure of on-premises technologies. This adds an extra layer of risk if the perimeter, interfaces, and accesses are not well-defined, segmented, and maintained.

Recommendations Summary

SANS 5 Critical Controls

There are many frameworks that companies use to provide a system of controls and maturity levels to reduce risk. The SANS Institute has distilled much of this work into the more approachable *SANS 5 ICS Cybersecurity Critical Controls*.

ICS Incident Response Plan 1

"Response" may seem strange as the first critical control, but it highlights the imperative to proactively plan how to respond to cyber events in highly complex Industrial environments. Organizations need to thoughtfully plan how to navigate employee and public safety, environmental, and revenue impacts in advance.

Defensible Architecture 2

Focuses on architecting and engineering the environment to proactively: a) limit the ability for adversaries to enter, traverse systems, and propagate; b) limit ability for mistakes by employees and contractors to introduce risk and vulnerabilities.

1. https://www.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html

ICS Network Visibility & Monitoring 3

Monitoring is about understanding the assets/devices in the environment and analyzing system communications and network traffic. Asset inventory is a core starting point, but this tooling also automates the ability to detect threats, map vulnerabilities, alert to key events, and provide data sets for rapid investigation.

Secure Remote Access 4

Remote access is the primary way that threats enter OT. Remote access is increasing – engineers from the asset owner, operations and management firms, system OEM technicians, and, increasingly, analytics and optimization software access industrial systems from offsite locations and add to cyber risk.

Risk-Based Vulnerability Management 5

Vulnerabilities are weaknesses exploited in cyber attacks. OT vulnerabilities represent a unique challenge, as patching devices requires downtime and interruption of operations. Taking a risk-based approach translates IT-based severity to an OT perspective, and provides alternative mitigation to limit risk prior to patch.

Using 5 Critical Controls to Prevent, Detect, and Respond

We can cast the SANS Five Critical Controls into a more traditional cybersecurity thought process: how to take PREVENTATIVE steps, how to DETECT threat behaviors, and how to RESPOND to events. A summary is presented below.

STAGE	RELEVANT CRITICAL CONTROL	RELATED ACTIONS
PREVENT	#2 Defensible Architecture	Network segmentation: domain, credential, and privilege segmentation; all to limit ability for threats to enter and traverse OT environment.
	#3 ICS Network Monitoring & Visibility	Enables asset inventory that is basis of tracking vulnerabilities, identifying critical systems, understanding traffic flows, monitoring/ validating controls.
	#4 Secure Remote Access	Core technology and deployment architecture that minimizes risk of access into OT environments.
	#5 Risk Based Vuln Management	Awareness of vulnerabilities tied to assets in the environment, with risk analysis of impact and likelihood plus alternative mitigation to minimize risk until maintenance window/patch.
DETECT	#3: ICS Network Visibility & Monitoring	Continuously monitoring the environment to identify potential threat behaviors, validate security controls, providing a event dashboard and information to investigate events.

RESPOND	#1: ICS Incident Response Plan	Preparation, communication, and practiced response to reduce the impacts of an incident as well as the cost associated with root cause analysis (RCA).
	#3: ICS Network Visibility & Monitoring	Provides logging and forensic records that enables simpler investigation and root cause analysis.

Prevention Recommendations

This is about architecting your defenses to limit exposure to employee mistakes, as minimizing the ability for adversaries to enter and propagate through your OT system environment. Taking the scenario approach helps narrow the scope of all that is possible. Here we reference the SANS 5 Critical Controls, and specific aspects of each control.

ICS Network Visibility And Monitoring (SANS Critical Control #3)

- Asset Inventory – A listing of the devices/assets and their profiles becomes the basis of numerous other controls. It enables the ability to:
  - Identify assets and maintain an asset inventory.
  - Conduct a Crown Jewel Analysis to identify the critical systems in a plant and prioritize security controls around these systems avoiding high impacts should the ICS/OT environment suffer an incident.
- Monitoring and validation of security controls –As policies are implemented, you want to make sure that changes to the environment don't undermine the policy put in place. Monitoring helps evaluate system and network traffic to validate the effectiveness of those controls.
- Visibility also helps operations to maintain an asset inventory of the equipment they have in the OT network and understand how those assets communicate. This asset inventory also allows the plant to link this list to their inventory and backup images to recover systems with software backups or spare parts.
- The detection also allows operations to avoid disruption by alarming the system with abnormal behaviors such as non-common communications. Additionally, logging and monitoring helps to investigate and provide information for root cause analysis when an incident happens.

Defensible Architecture (SANS Critical Control #2)

- Network Segmentation & Access Control Policies
  - Implement segmentation of the ICS/OT networks from the IT (corporate) networks and the internet, including a demilitarized zone (DMZ) for limiting and breaking network connections using proxies. This facilitates network handling, monitoring, and containment procedures in case network isolations are necessary.
  - Deny externally routable connections from within the ICS/OT network and designate dedicated authorized devices from the ICS/OT network to initiate these connections.
  - Limit the ingress and egress between ICS/OT, IT, and other zones to as few pathways as possible, ultimately creating "choke points." These natural choke points can be leveraged for Network Security Monitoring (NSM).
  - Implement robust firewall rules, which should be tested, refined, and annually reviewed.

- Introduce more granularity to improve security at the plant floor and network performance for "East-West" traffic.
  - This granular separation, by different processes, is known as "micro-segmentation." Micro-segmentation is a cybersecurity technique that segments the internal networks based on a diverse set of variables describing network zones.

- Segmentation of Domains, Credentials, & Privileges
  - Separate Active Directory domains to avoid having the same management system on IT and ICS/OT networks. This enables better credential handling and reduces the use of the shared credentials between IT/OT. Having assets managed by separate Active Directory domains makes isolating the ICS/OT environment easier if IT becomes compromised.
  - Organizations should create specific Domain Administrator accounts that are separate from standard everyday user accounts. Usage of these accounts should be monitored, require multi-factor authentication, and only be used to administer the domain(s).
  - Reduce or limit the use of service accounts; these accounts usually have admin or system-level privileges.
  - Reduce the use of share credentials and implement role-based access control (RBAC) in ICS/OT assets.
  - Put admin/system users in a Protected Users group in Active Directory. Additionally, consider disabling interactive login capabilities for service accounts. This is often an unnecessary and unused privilege that is left on by default and grants user access to both local and domain resources.

Secure Remote Access (SANS Critical Control #4)

Remote connection security is another method to prevent intruders from the ICS/OT environment. Vulnerabilities in remote connections have been leveraged by adversaries to access the ICS/OT environments and propagate ransomware. According to Dragos's 2022 Year in Review, adversaries commonly leverage SMB and RDP protocols to do lateral movements and ransomware propagation.

Remote connections are also leveraged to access assets such as engineering stations, historians, and MES servers to obtain information regarding plant operations or directly disturb those systems. The following are essential steps to prevent unauthorized remote access control of the ICS/OT environment.

- Use a secure method to connect to the corporate network, such as a VPN.
- Use multi-factor authentication (MFA) in addition to the VPN to establish the corporate network connection.
- Ensure each connection terminates in the DMZ.
- In the DMZ, allow only known IP addresses to communicate in or out of the network.
- Limit remote access to systems connected using a jump server placed in the DMZ. Enforce the use of separate jump boxes to have better control over vendors and internal remote accesses. Ensure all remote connections are logged locally and forwarded to an enterprise SIEM. If possible, consider solutions that implement session recording to capture detailed aspects of interactions during the remote session.
- Ensure connections time out and require the user to re-authenticate when a time out occurs, or the user reconnects.
- Require vendors to follow the same or enhanced security policies and procedures established for corporate users.

- As previously explained in the shared IT/OT dependencies threat section, insecure credentials are another weakness adversaries look to leverage, granting them access to the ICS/OT environment.

Risk-Based Vulnerability Management (SANS Control #5)

Managing vulnerabilities is an important strategy to prevent exposures, but must be managed properly in OT context. ICS/OT systems are not always available to patch and functionality after patching should be highly monitored. If not well tested, the patch can cause malfunctions on the asset operation and lead to productions delays.

Following are some best practices for vulnerability management in manufacturing.

- Prioritize the analysis of alerts and advisories linked to the manufacturing threat scenario.
- Establish a risk-centric approach to identifying and managing vulnerabilities in ICS/OT assets, including: applications, security devices, databases, and vendor propriety products in use in the environment.
- Establish regular reviews of the asset inventory to identify outdated or end-of-life products/equipment.
- Prioritize vulnerability mitigations for:
  - Systems that bridge IT/OT, such as firewalls, historians, etc.
  - Vulnerabilities that are network exploitable.
  - Vulnerabilities that have been actively exploited in the wild.
  - Vulnerabilities for which a public exploit is available online.
- Establish a mechanism to track vulnerabilities, implement compensating controls for assets that cannot be modified, and ensure an acceptable risk tolerance level is maintained.
- Prioritize crown jewel and boundary/perimeter assets.
- Communication to assets identified as crown jewels should be limited to only assets that need to communicate with them.
  - This reduces the need to patch asset vulnerabilities deep within the architecture that are well-segmented from other assets.
- Consider mitigations techniques other than applying patches, such as:
  - Network segmentation (firewall rules, etc.)
  - Focused network monitoring and alerts
  - Physical switches on controllers preventing unplanned logic changes

Detection Recommendations

The detection method is divided into three phases: implementation of ICS network monitoring, analysis of key host logs, and analysis data to detect threat behaviors.

Implementing effective ICS/OT network monitoring is an easier and more effective method for detection of cyber threats. You can create manual processes leveraging centralized log sources (covered in PREVENT) that can start to approximate an ICS-specific network monitoring system; but if you evaluate the cost, time, and effectiveness to build those process at scale, ICS Network Monitoring will prove to be simpler, cheaper, and more effective. Centralized log sources are still used for evaluation of host specific threat behaviors, but are not required for all the other monitoring work.

Once effective monitoring is in place, detection based on analysis of traffic and logs to find threats needs mechanisms to trigger and prioritize alarms and to integrate into triage and investigation queues.

Defensible Architecture (SANS Critical Control #2)

- Centralization of Logs
  - The implementation consists of strategically collecting and centralizing logs and data from the hosts and network. This can be used to augment ICS Network Security Visibility & Monitoring systems during investigations or used as the basis for manual analysis of network traffic and data to continuously monitor the system to look for any abnormality, such as new connections or unauthorized accesses.
  - Begin by identifying critical data sources. Include those essential to advancing your business but also those which could harm your business, aid competition, or enable further attacks on the organization.
  - Implement log centralization as it is essential to detect and identify threats and assist in forensics analysis during incident response. Centralized logging is preferred over manual collection and analysis.
  - Enable logging on the edge and network-level assets.

ICS Network Visibility & Monitoring (SANS Critical Control #3)

Here is a list of monitoring and analysis steps that should be reviewed, either through building a of manual process or, in a more automated way, by implementing ICS Network Monitoring:

- Create baselines and analyze changes to:
  - Asset inventories
  - Normal range of set points,
  - Communications protocols, top talkers, and sources of approved logic changes
- Log forensic data for use in investigations and root cause analysis:
  - Traffic and key commands
  - Provide a mechanism for data capture
- Analyze data flows between network segments:
  - Scan for indicators of compromise (IOCs) – requires up to date intelligence on industrial focused IOCs.
  - Identify threat behaviors activities that traverse the local network and can be identified before an encryption event or ransomware staging activity such as reconnaissance and positioning, malware distribution prior to detonation, and targeting of critical management servers.
  - Monitor and validate policy rules in firewalls, jump hosts, segmentation architectures, etc.
  - Monitor remote connections and sessions continuously by reviewing user access and logs on a regular basis.
  - Identify new connections and established communications.
  - Review external communications and make sure that ICS/OT assets are not trying to communicate externally.
  - Identify new PLC-to-PLC communications or communications from ICS/OT systems outbound to internet addresses.

- Identify if there are any clear text passwords in use.
- Investigate unusual IP addresses and ports in command lines.
- Provide prioritized alerts of events taking place in the environment.

In addition to Analyze host records and logs for abnormal threat behaviors:

- Identify any new accounts or abnormal account activity, software, and new driver installations on PLC engineering workstations, HMIs, and servers that may have trusted path access.
- Monitor files for file manipulation.
- Monitor newly created scheduled jobs and any changes made to scheduled jobs. Changes made to services may attempt to manipulate features of their artifacts to make them appear legitimate.
- Monitor changes made to the Windows registry that may stop or disable services.

The type of technology is important. Effective technology solutions provide: a) deep knowledge of the operational technology systems/assets and related network protocols; and, b) the ability to identify threat behaviors related to those unique systems. A key mistake is to avoid applying IT-focused detection technology to OT. While IT-focused tools may be able to accomplish the base use case of asset inventory, they lack the understanding of the OEM system network protocols key to ongoing monitoring. Further, tools that use general "anomaly" engines – baselines of normalcy and flagging of abnormal traffic – lead to very high alarm rates where true threats can hide.

The design implementation of ICS network monitoring can be a complex exercise dependent on several variables. It is best done with experienced solution architects and implementation engineers. Some of the considerations include:

- Prioritize IT/OT perimeter monitoring. This is a critical point of monitoring remote access and traffic transiting from IT systems.
- Distribute monitoring across conventional computing hosts such as engineering stations.
- Implement adequate network security monitoring across the plant through critical and identified choke points.

Response Recommendations

As discussed earlier, effective response requires planning, preparation, and practice. Even though this is the last stage of an attack, and one you hope never to encounter, the following actions should be implemented to prepare and reduce the impacts of an incident as well as the cost associated with root cause analysis (RCA).

An ICS-specific Incident Response Plan (IRP) should:

- Require the application of Crown Jewel Analysis or a similar methodology to determine the organization's priority systems and crown jewels. For example, a CJA conducted for an automotive manufacturing plant might identify the plant floor VIN management system as the critical system and database server with build recipes, the associated backup server, SCADA Server, and connected PLCs and HMIs, to be the crown jewels.
- Be regularly tested, reviewed, and enhanced to maintain proper methodologies and documentation that will allow the manufacturing organization to act accordingly, timely and preserve forensics data. This documentation and data are critical to understanding the TTPs and applying proper security controls to avoid the same threat accessing the ICS/OT environment.

A Tabletop Exercise (TTX) is an excellent way to test those procedures. TTXs should be developed based on real scenarios and focused on the manufacturing industry. The threat scenarios presented in this paper, ransomware, shared IT/OT dependencies, trusted vendor compromise, and PIPEDREAM's individual modules, are excellent examples that manufacturing organizations can utilize to test their incident response plan and procedures. The threats highlighted in this paper are the most common within manufacturing.

An incident response consists of a lifecycle of seven phases that defines different activities and their prioritization depending on each cycle phase. This cycle is well-known as PICERL due to its initials at each phase: Prepare, Identify, Contain, Eradicate, Restore, Learn, and Repeat.

Besides the PICERL phases, documentation and communication practices should always be considered during an incident. The following are some recommendations that manufacturers should focus on at each cycle phase.

Preparation

- Identify actual scenarios where manufacturing industries were targeted.
- Perform a risk assessment identifying impacts that those scenarios can provoke within your industry.
- Analyze and identify critical systems, functions, and assets. Conducting a Crown Jewel Analysis aids organizations in identifying those critical systems.
- Enhance or develop incident response plans, playbooks, and procedures to run an incident response effectively.
- Identify roles and responsibilities.
- Define communication channels and pertinent permissions, including incident response teams' credentials, to avoid delaying IR activities due to the lack of access permissions to the incident response team.
- The incident response team should also have an incident response kit handy with the tools and necessary software to cover an incident.
- Maintain an incident response plan that includes at least:
  - A call tree with established roles and responsibilities, including backup personnel in case key staff members are unavailable.
  - Strategies and criteria to escalate an incident.
  - Identification of possible events and their severities.
  - Defined communications channels to utilize internally and externally. Indicate the procedures and defined roles to handle both communications.
  - Response methodologies with procedures or playbooks linked to each required phase of the PICERL method.

Identification or Detection

- Maintain a centralized system that allows one to monitor and investigate events associated with an incident.
- Follow the detection section for further information on network monitoring and visibility implementation and analysis.
- Maintain a Collection Management Framework (CMF), which serves as a roadmap for incident responders to locate the existing logs and their storage time.

- Make sure that the detections tool has correlation capabilities across multiple data sets to avoid delaying the detection of cybersecurity incidents.
- Train the plant's engineers, operators, and maintenance personnel to identify and consider cybersecurity behaviors against regular equipment and process troubleshooting.

Contain

Include playbooks with the procedures to isolate critical areas, such as crown jewels and related systems. As described in the prevention section, having a segmented network facilitates isolating and containing different networks in the ICS/OT environment.

- Ensure that the playbooks include thresholds, impacts, and prioritization to perform containment procedures. The procedures should also include the time and tempo to initiate containment actions.
- Initiate the roles and responsibilities of the staff performing the containment on the IRP.
- Identify and document existing choke points where isolation can be performed. For example, restrict traffic on the perimeter firewalls.
- Consider first containing networks from the "North-South" traffic to separate ICS/OT and stop any traffic from the DMZ and corporate networks. This includes remote connections. Then, if necessary, isolate the "East-West" traffic to disable any lateral movement from spreading malware to further zones at the plant.
- Train plant engineers to locate the key points for isolation and containment.
- Consider logical containment procedures over physical ones as a priority, as they can easily be identified and reverted if needed.
- Non-local connections should be funneled through chokepoints, like a firewall, that can quickly and easily be disconnected in the event of a security incident. Someone with access and authority to this choke point should always be available. Consider having trained staff on-site that can help with the containment phases.
- Maintain emergency firewall ruleset templates for different rapid isolation scenarios. These templates serve to logically collapse network segments, allowing for rapid quarantining and resuming of normal operations after recovery from an incident.

Once an incident is declared and moves forward to the containment phase, preserving data from the compromised assets is crucial. This information serves as legal evidence and allows incident responders to understand the attack process better and generate IOCs to avoid this same attack in the future. Depending on the attack's consequences or regulatory impacts, it is also necessary to maintain the chain of custody of evidence in case the incident must be escalated to law enforcement.

The CMF is essential during forensics as it includes the type of information the responders have access to and its location.

Eradicate

This phase is a step before recovery, where the identified compromised assets are cleaned up and malware should be removed.

- Include playbooks and procedures to eliminate malware, procedures to patch systems, define the strategies to eliminate or replace equipment, and criteria to disable accounts.
- Define the tools to eradicate malware, such as antivirus software, spyware detection, removal utilities, and patch management software. However, keep in mind that with ICS-dedicated malware, the restoration and complete clean-up (e.g. factory restore) of the system might be required as some eradication and detection software might be limited to detecting just IT infections.
- Define criteria to rebuild systems in cases where the adversary escalates to administrator privileges, which could be an indication of the systems files modifications and malfunctions on a system even when standard eradication procedures were considered.
- Test and analyze that the system is free of all malware and corrupted data.

Restore and Recover

At this phase, the compromised systems return to their regular operation state. To achieve this, organizations should consider the following steps:

- Define restoration prioritizations (e.g., which systems should be restored first), based on criticality and interdependency between assets or systems.
- Include policies and procedures for 3rd parties involved in restoring the systems, including the downtimes expectancies.
- Maintain templates and gold images for systems to ensure a reliable and faster recovery.
- Establish test procedures for backups after an incident and test those backups to make sure the system is operating as it should be.
- Enforce the 3-2-1 backup strategy, which means having three copies of the backups, where two copies can be stored on servers or cloud systems, and at least one copy should be kept off-site.

Lessons Learned Documentation

The preparation phase indicates the procedures and playbooks that an incident response plan should consider within each PICERL stage. Documentation should also include the practices for tracking the evidence, responses, and results once an incident has been declared. It is understood that not all information can be tracked, but having tools and a defined role for documenting helps to maintain a consistent timeline at each stage of the incident. The strategies to track this information should be defined in the IRP. Tracking information during the incident allows responders and stakeholders to better understand the attack's paths and nature. This information is then used to implement new IDS and SIEM systems detection rules. Additionally, this information is helpful to document lessons learned and enhance the procedures, playbooks, and overall incident response plan.

The Destination, the Journey, and What You Need To Get There

Here is a short summary of the information presented in this paper:

- You are trying to protect against defined Threat Scenarios (in this case, Ransomware, Trusted Third Parties, IT/OT Interface, and PIPEDREAM).
- Your simplified path to effective protection is distilled in the SANS 5 Critical Controls (ICS Incident Response Plan, Defensible Architecture, ICS Network Visibility and Monitoring, Secure Remote Access, and Risk-Based Vulnerability Management).
- Every organization has its own cybersecurity journey along that path – different characteristics, starting points, and needs. Varying levels of resources and expertise in OT cyber are a major variable for which you need to solve.

Dragos has developed a three-step OT Cybersecurity Journey that identifies key steps in implementing the SANS 5 Critical Controls, including how to start with benchmarking your starting point – a Baseline. The visual below shows the core steps in that journey.

To determine where your organization sits today, and learn how to take the next steps, book an appointment with one of our experienced OT professionals.

Building An Effective OT Security Program

Establish Baseline (Leverage Dragos Platform)

- Conduct Architecture Assessment
- Create an Incident Response Plan
- Organize your assets inventory & collection management

Operate Dragos Platform

- Monitor OT assets & network traffic in Crown Jewel sites
- Identify & manage key OT vulnerabilities
- Detect & respond to OT incidents

Expand & Mature

- Expand deployment to medium & low impact OT sites
- Integrate OT incidents & intelligence with IT SOC
- Validate defensive controls

REFERENCES

- IBM X-Force and Dragos Data: **https://securityintelligence.com/posts/attacks-operational-technology-ibm-dragos-data/**
- PIPEDREAM Malware and the CHERNOVITE Threat Group: **https://hub.dragos.com/on-demand/pipedream-malware-chernovite-activity-group**
- Analyzing PIPEDREAM: Results from Runtime Testing: **https://www.dragos.com/blog/analyzing-PIPEDREAM-results-from-runtime-testing/**
- CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS): **https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/**
- KOSTOVITE: **https://www.dragos.com/threat/kostovite/**
- ICS/OT Cybersecurity Year in Review 2022: **https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en**
- EKANS Ransomware and ICS operations: **https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/**
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability: **https://www.cisa.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf**
- The Five ICS Cybersecurity Critical Controls: **https://sansorg.egnyte.com/dl/4hgxqaIF7N**
- Network segmentation challenges and Solutions: **https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_WP_Manufacturing_Segmentation_June23_FINAL.pdf?hsLang=en**
- Petya Malware Variant and recommendations: **https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-181-01c**