INDUSTRIAL CONTROL SYSTEMS SECURITY

SANS

A Simple Framework for OT Ransomware Preparation

Author: Lesley Carhart

Contents

Abstract

Ransomware remains a pervasive threat across all industries, with industrial networks being particularly vulnerable due to their unique characteristics and challenges. The impact of ransomware in operational technology (OT) environments is especially critical, often disrupting systems essential for control and visibility of safe and reliable operations. This vulnerability is exacerbated by the relative security and architectural immaturity common in process networks. To address this challenge, it is essential to develop actionable ransomware response playbooks tailored to critical infrastructure, with a focus on life safety and operational continuity. This white paper presents a structured framework for creating, testing, and refining ransomware response playbooks, emphasizing preparedness and resilience in OT environments.

Introduction

Ransomware continues to pose a serious threat in 2025, showing no signs of slowing down despite persistent efforts to disrupt its operations. Cybercrime, heavily driven by ransomware initial access brokers, malware development, and ransomware affiliate activities, has evolved into a thriving trillion-dollar industry[1]. No organization or industry vertical is immune to this pervasive threat.

While cybersecurity defenses have improved across many organizations, attackers have adapted their strategies, targeting less defended networks and organizations, particularly those with immature cybersecurity programs. This shift is particularly concerning for industrial control systems (ICS)/OT networks, which often underpin critical and highly visible operations but tend to lack the security maturity found in other sectors.

Industrial networks present an increasingly attractive target for ransomware actors due to their operational importance and their potential to cause significant real-world impacts that facilitate extortion. Although ransomware attacks rarely compromise lower-level process systems such as programmable logic controllers (PLCs), they often disrupt higher-level systems essential for process visibility, control, management, and telemetry. Such disruptions can force operators to shut down or limit operations until the affected systems are restored, leading to operational and financial losses.

Despite the growing threat, many organizations remain underprepared for ransomware incidents targeting industrial networks. Immature planning and incomplete incident response strategies often result in errors and inefficiencies across the incident response lifecycle. This gap underscores the urgent need for comprehensive, functional, and tested playbooks for responding to ransomware incidents in OT environments.

This paper aims to address this need by proposing a simple framework for developing essential ransomware response playbooks tailored to OT environments. These playbooks are designed as foundational tools to guide organizations in managing ransomware incidents effectively. Once established, the playbooks should be treated as living documents, evolving alongside changes in organizational environments, threat landscapes, and defensive capabilities. By adopting and refining these playbooks, organizations can significantly enhance their resilience against ransomware threats and mitigate their impact on critical operations.

[1] Cybercrime Magazine. (2023, July). Global ransomware damage costs predicted to reach $250 billion USD by 2031. Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Related Work

The Five ICS Cybersecurity Critical Controls[2] white paper by Tim Conway and Robert M. Lee describes essential functional areas of developing cybersecurity maturity and essential defensive capabilities in industrial environments. These capabilities are:

1. ICS Incident Response
2. Defensible Architecture
3. ICS Network Visibility Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Analysis

Each of these areas requires development and awareness to build a holistic and effective OT cybersecurity program and defensible environment.

This paper focuses on a single Critical Control, Incident Response planning – specifically for ransomware incidents.

ICS Incident Response

Operations-informed incident response plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

Defensible Architecture

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

ICS Network Visibility Monitoring

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control

Secure Remote Access

Identification and inventory of all remote access points and allowed destination environments, on-demand access and multi-factor authentication (MFA) where possible, jump host environments to provide control and monitor points within secure segment

Risk-Based Vulnerability Management

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Figure 1: Five Critical Controls for Industrial Cybersecurity

[2] Lee, R. M., & Conway, T. (2022b, April 2, 2025). The Five ICS Cybersecurity Critical Controls. https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

The State of Ransomware in ICS

It is important to remember that ransomware actors operate with the primary objective of maximizing financial gain as efficiently as possible. Consequently, their tactics have evolved over time to adapt to defender strategies and law enforcement efforts, resulting in increasingly specialized and compartmentalized roles within their operations. Modern ransomware campaigns are typically executed by affiliate groups that purchase malware and pre-established network access from initial access brokers—threat actors who specialize in gaining initial intrusions and establishing footholds within target environments. There can be months between a network being compromised by the initial access broker and it being ransomed.

From an efficiency standpoint, these actors now prioritize targeting networks that are less defended and minimally monitored, often characterized by older computer systems and outdated security tools. Additionally, they prefer victims that are likely to pay ransom demands, particularly those where the encrypted systems are critical to operations or highly visible. This unfortunate combination of factors makes industrial networks particularly attractive to ransomware operators, regardless of size or sector. There is rarely a substantial effort made to impact lower-level systems directly, because that is currently not necessary or efficient for achieving their financial goals (though that will likely change with the attacker and defender maturity landscape).

Over two decades of consistent IT/OT convergence has exacerbated this problem. Modern OT networks typically contain many higher-level Windows and Linux computers which are vulnerable to ransomware. Additionally, these computers are increasingly connected to remote access, the enterprise, and the cloud for the sake of process efficiency, reduced staffing, and telemetry. Virtualization is also becoming prevalent in and essential to some OT environments, and hypervisors are a typical target for ransomware affiliates. Today, ransomware is a 'when,' not an 'if' for OT networks. Planning and preparing for an attack are essential.

Playbook Development Methodology

Prerequisites

Developing incident response plans for any environment necessitates a foundational understanding of the environment's architecture, asset inventory, key personnel, security controls, and operational functions. Before drafting response playbooks, it is essential for stakeholders from OT, infrastructure, and cybersecurity teams to collaborate and engage in discussions to establish a shared understanding of the facility. This process also helps identify key subject matter experts who will play critical roles during an incident. While this mutual understanding does not need to be exhaustive at the outset, it should encompass fundamental aspects of the environment to ensure the development of an effective ransomware-specific or general OT incident response playbook.

Key questions to ask include:

If a cybersecurity issue such as ransomware was detected by an operator today, who would they report it to, and how?

Cybersecurity detection in OT environments often relies heavily on OT operators and engineers noting an abnormality in a system or process. This necessitates a healthy and prompt communication flow between OT personnel and cybersecurity. It is important to understand how and when a report of a lockscreen or abnormality on an operator system would be escalated to the cybersecurity team.

What network and process communication topology is utilized in the environment?

Understand the layout of the environment. Are there multiple segments? Is the network flat? How does the network connect to the enterprise or internet? Are there vendor or engineer remote access provisions? The topology of an OT environment will heavily influence how far and fast ransomware can be spread, potential intrusion vectors, and potential scale of future incidents and recovery efforts.

What are the vendors, versions, and operating systems of the higher-level process components (human machine interfaces (HMIs), engineering workstations, virtual servers, supervisory control and data acquisition (SCADA), etc.)? Are there any exceptions to this?

Performing response and detection in legacy environments will be significantly different than performing response and detection for modern operating systems. Additionally, vendor-owned and managed systems pose unique challenges in both forensic analysis and restoration.

What security detection, prevention, and monitoring tools are currently in place?

A strong awareness of what logging and forensic data is available will assist with making key decisions during an incident. If no Collection Management Framework[3] exists for the environment, it is advisable to generate one.

Who, if anyone, currently performs security detection and response functions for this facility or network?

Detection technologies, staffing, and methods indicate how ransomware may be identified in the environment, and how early in the attack lifecycle it may be detected.

Is there a Business Continuity Plan (BCP) and/or Disaster Recovery Plan (DRP) in place?

Existing BCPs and DRPs in OT environments frequently contain essential details on system restoration, backups, and capability to restore operations within established and required timeframes. This information is crucial to the Recovery phase of incident response and weighing the criticality of incidents based on process consequences.

[3] Lee, R. M., Miller, B, & Stacey M, (2018, December 7). The Community Defense Model for Industrial Control Systems (ICS). Retrieved from https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf

Fostering a Collaborative IT/OT Environment

Unhealthy or outright hostile relationships between cybersecurity and OT teams are a common issue in many organizations globally. Miscommunication and a lack of shared mission and common vocabulary have caused issues in conducting critical incident response planning activities in many organizations. To be successful in planning activities, it is essential to begin mending relations between teams and increasing collaboration and communication. Some suggestions for improving relationships and fostering a culture of cooperation include:

- **Focus discussions on safety and process impact:** Frame all discussions with a focus on safety and process consequences. Malware and hacker techniques alone are not a primary concern to most industrial engineers, however, risk to process, personnel, and equipment certainly are. All discussions related to cybersecurity must focus on the potential realistic consequences of attacks on the process, considering mitigating safety controls in the environment. Start all discussions regarding incident response with a clear and mutual understanding of what a "worst day" in the process environment would look like and realistic consideration of what digital devices could impact.
- **Create and maintain a shared glossary of terms:** There is frequent term and acronym overlap between engineering and cybersecurity personnel, and it can lead to dangerous and frustrating miscommunication.
- **Implement a job shadowing program:** Provide new cybersecurity personnel with opportunities to learn about process environments and operations through structured job shadowing programs—with a focus on mission and safety.
- **Establish routine communication channels:** Maintain regular communication between facility and cybersecurity teams. These could take the form of monthly calls, routine emails, or available site cybersecurity champions. These outlets decrease the temptation to evade cybersecurity controls or conduct shadow IT activities when cybersecurity policies impact industrial operations. They also enable faster and healthier incident response planning and execution.

Playbook Framework

The development of a ransomware response playbook should remain a collaborative effort involving IT, cybersecurity, and OT teams. Each stakeholder group brings critical insights and expertise that contribute to the playbook's structure and effectiveness. An effective ransomware playbook should be organized into distinct sections aligned with the phases of the incident response lifecycle. For the purposes of this paper, the SANS PICERL lifecycle[4], —encompassing *Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned*—will be used as a reference. However, the principles and strategies outlined are applicable to any widely recognized incident response lifecycle framework.

Metadata and Purpose

Like all incident response documentation, ransomware playbooks for OT should be properly owned, maintained on a set cycle, and revision controlled. It is also important to clearly state the scope and purpose of the ransomware playbook to ensure that it supports a specific mission function **– the timely detection, analysis, response, and recovery from ransomware attacks.** The playbook should also clearly state its dependencies and linkages to organizational OT and enterprise Incident Response Plans, existing IT focused ransomware response plans, Emergency Operations Center Plans, BCPs, and DRPs.

Preparation

Preparing for a ransomware incident in a critical process environment requires careful consideration of factors unique to minimizing risks to life, safety, and operational continuity. The primary objective during a major process-impacting incident is the safe and timely restoration of operations. Achieving this goal often involves significant capital expenditures, including investments in replacement computer equipment, supplemental IT and OT personnel (through contracts or retainers), industrial vendor services, and the procurement of specialized or legacy equipment. In cases where an organization decides to pay a ransom, additional costs must also be considered, including the ransom itself and associated legal and negotiation services.

A vital element of the preparation phase is establishing clear executive ownership or delegation for approving emergency purchases and contracts. These decisions may need to be made within hours of a crisis, emphasizing the importance of predefined authority and processes to prevent delays.

Another critical aspect of preparation is drilling the ransomware response playbook. If tabletop exercises and drill cycles are not explicitly outlined in a parent OT incident response plan, these should be clearly defined within the ransomware playbook. Tabletop exercises involving OT personnel should be conducted at least annually, though more frequent exercises are preferable. Additionally, all critical technical procedures described in the playbook should be regularly drilled. These drills should be scheduled to align with maintenance windows or performed in controlled environments, such as laboratories or digital twin systems, to ensure readiness and reduce potential disruptions to live operations.

[4] SANS Institute. (2016, November 5). Incident response cycle cheat sheet. Retrieved from https://www.sans.org/media/score/504-incident-response-cycle.pdf

Identification

Identification encapsulates the activities of detection, activation, and response through forensic analysis. While these activities are often summarized broadly, breaking them out more clearly highlights the real-world steps required to handle ransomware in OT environments.

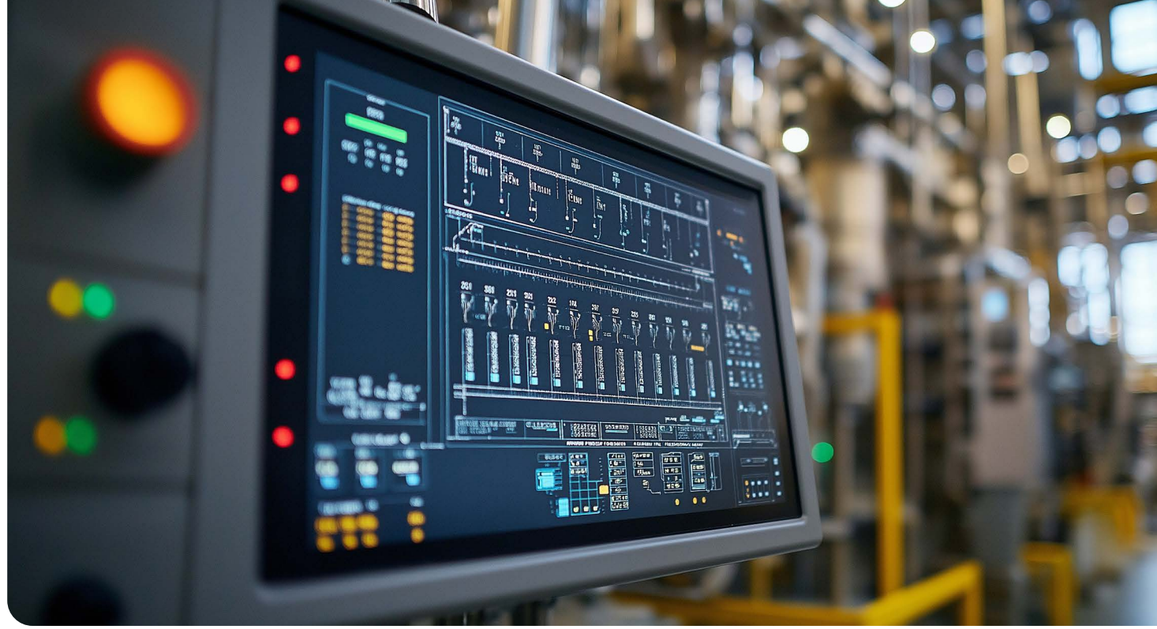
To begin, it is important to establish the substantial differences between detection of ransomware in OT environments versus traditional IT environments. Most OT process networks are less mature in detection due to numerous technology, vendor, and process restrictions. While there are several well-established commercial OT network detection products available, (and it is highly recommended that your organization deploy a product of this type), host tooling such as endpoint detection and response (EDR), extended detection and response (XDR), and next-generation antimalware products are rarely available or widely deployed. Detection methods for ransomware must adapt to these limitations.

Detection

Plans and playbooks must account for detections from non-standard means, including:

- Human Reporting: Facility human awareness and reporting mechanisms must be well-established and monitored by cybersecurity during all operational periods. Awareness campaigns for OT facilities should include indicators of both ransomware deployment (such as account lockouts, abnormal input device activity such as phantom mouse movement, and antimalware pop-ups), and where to report clear indicators of ransomware such as lockscreens. This is a vital detection source in less mature environments.
- Passive Network Detection for OT: Cybersecurity personnel responsible for OT detection should ensure the deployment, tuning, and monitoring of modern OT-focused network detection appliances which do not interfere with process or infrastructure. These network-based detections will not be the same as modern EDR/XDR alerts – ransomware network activity detections will more frequently encapsulate invalid administrator account usage, suspicious or malicious file transfers from system to system using unencrypted protocols, and network scanning activity.
- Proper Identification and Monitoring of OT Security Tools: Due to the relative immaturity of cybersecurity practices and the common disconnect between OT and cybersecurity teams in typical OT environments, there may be standalone, vendor-specific, or legacy security tools in place that are not effectively maintained or monitored by cybersecurity personnel. During initial collaborative discussions, it is essential to identify existing security measures—such as antivirus software, firewalls, and intrusion detection systems—within the industrial environment.

Policies should be established to ensure that logs from these tools are periodically reviewed or integrated into broader security monitoring processes. Even legacy or end-of-life tools can provide valuable insights by detecting certain stages of the ransomware lifecycle. Additionally, fostering communication between OT subject matter experts and cybersecurity teams is crucial, as OT experts can help interpret unusual detections within the environment. This collaborative approach ensures that critical alerts are not overlooked due to a lack of contextual understanding.



Activation

Once ransomware (or suspected ransomware) is detected in a process environment, it is essential to escalate and begin incident response activities as rapidly as possible. Modern ransomware affiliates move quickly (hours, not days) to damage and encrypt devices, and quick analysis and containment is crucial to preventing increasingly negative outcomes. This means it is essential to include or reference clear, process-focused escalation processes and severity matrices in the ransomware playbook.

It is not possible to utilize traditional cybersecurity measures of incident severity in OT environments. A critical severity incident in OT almost always involves risk to life or safety, loss of production, damage to equipment, contamination or loss of quality of a product, contamination of the environment, loss of consumer confidence, or regulatory violations. Therefore, establishing the severity of ransomware in an OT environment requires those clear initial discussions of applicable consequences, and what the ransom and subsequent disablement of high-level OT systems would realistically cause. This necessitates discussion of the feasibility of safe manual operations, ability to function on secondary (segmented) operations centers, and reliance on computers for dispatch, efficiency, and billing. With those criteria in mind, the realistic severity of a ransomware infection in some or all OT network segments can be quantified appropriately for the organization.

Ransomware attacks can impact an organization in multiple ways, particularly through double extortion tactics. During activation processes, ensure that standard corporate incident communications are conducted and that all necessary communications to OT personnel are also planned. Controlling social media and news media communications about a ransomware attack is important, especially since ransomware actors often post their victims' information publicly to apply pressure for payment.

Ensure that all appropriate stakeholders in OT are notified through an established communication flow and included appropriately during incident activation, as they will be vital to every following stage of response, particularly restoration of services and containment decision-making. Additionally, there may be sector specific voluntary or required information sharing regulatory and reporting requirements in critical infrastructure environments, which should also be noted or cross-referenced in the ransomware playbook.

Forensics and Scoping

Finally, identification also includes scoping and forensic analysis of the ransomware incident. Lack of OT cybersecurity maturity means that ransomware affiliates may have made substantial headway in the environment by the time cybersecurity team members are notified of the attack. Given the reduced cybersecurity tooling in most OT environments, it is essential to clearly define how cybersecurity team members will evaluate the intrusion vector and the spread of ransomware across the environment. Some prime considerations to address in the playbook include:

- Who will collect initial, key metadata about the ransomware variant and group in play? This information is essential to request third-party help and to evaluate recovery options. Metadata may include lock screen information, malicious file hashes, detection signatures, and encrypted file extensions. It is recommended to write a clear set of instructions for gathering all these details when available.
- How often will incident status updates occur, who is performing documentation duty, and whose responsibility is organizing those calls?
- Who will perform detailed forensic analysis of logs, network data, and hosts? If this will be carried out by a third-party incident response provider, how will their team be promptly activated and granted access to facility data? Note: If a third-party provider is utilized for analysis, it is still important to include basic considerations for evidence and log preservation in the OT environment during the Identification phase. For instance, disconnecting impacted systems from the network—rather than powering them off—can help preserve volatile memory. Another example is saving and replacing physical hard drives from impacted computers scheduled for reimaging.
- Is there an Active Directory (AD) domain in place in the OT environment, and if so, who can perform queries of its logs, policies, and accounts?
- Who in the OT environment is the network engineer responsible for checking the status of switches, physically and wirelessly connected devices, wireless networks, or firewall activity?
- What security, infrastructure, and logging data is available for the environment, and how long is it retained? (A cross-referenced Collection Management Framework[5] document is incredibly useful, here).
- How will analysts scope the spread of human-deployed ransomware files and system modifications (using living-off-the-land tactics) to OT hosts, where modern security tooling may not be in place or complete?
- How will analysts scope the spread of wormable ransomware files and system modifications to OT hosts?
- How will analysts identify the potential ransomware intrusion vector? In OT environments, these frequently include exploited and vulnerable perimeter devices, compromised remote access credentials, external USB media, transient assets, and bridged or dual-homed systems. Consider how each of these potential methods might be eliminated as a hypothesis.

[5] Lee, R. M., Miller, B, & Stacey M, (2018, December 7). The Community Defense Model for Industrial Control Systems (ICS). Retrieved from https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf

Containment

Containment is a challenging decision in enterprise environments on the best of days, and it can be a paralyzing decision point in process environments, where it may substantially impact operations and restoration. However, containment is an essential tool in preventing spread and damage from ransomware during an incident. Containment in OT is typically performed in very different ways than in IT. In IT, modern endpoint tools often allow isolation of individual hosts or groups of hosts, remotely and rapidly. In OT environments, containment typically means physical or logical whole-network isolation at a firewall, router, or switch.

Obviously, this type of mass disconnection has notable side effects. Therefore, it's vital during time-critical ransomware incidents that decision makers for containment are clearly identified and given all the tools possible to make good decisions as rapidly as possible. Containment final decision makers in OT are typically not cybersecurity personnel. They may be facility or safety managers, advised by the cybersecurity team. Vital guidance to provide those decisionmakers include:

- **Securing the System:** Where applicable, utilize the engineered capabilities of the process to place the system in manual or control-inhibit modes of operation.
- **Pre-Established Risk Criteria or Scenarios:** Define criteria or scenarios for considering containment.
- **Technical Options and Procedures:** Clearly outline available technical options and defined procedures for disconnecting all or part of the OT network. Identify who will perform these activities.
- **Understanding the Side-Effects:** Detail the impacts of network isolation on process operations and on incident response and recovery activities.
- **Validation and Isolation:** Define how isolation will be effectively validated.
- **Impact Analysis:** Assess the effects of containment actions on system-to-system communications and the broader process under control.
- **Protecting Interconnected Networks:** Include considerations for containment actions to safeguard interconnected customer or provider networks.

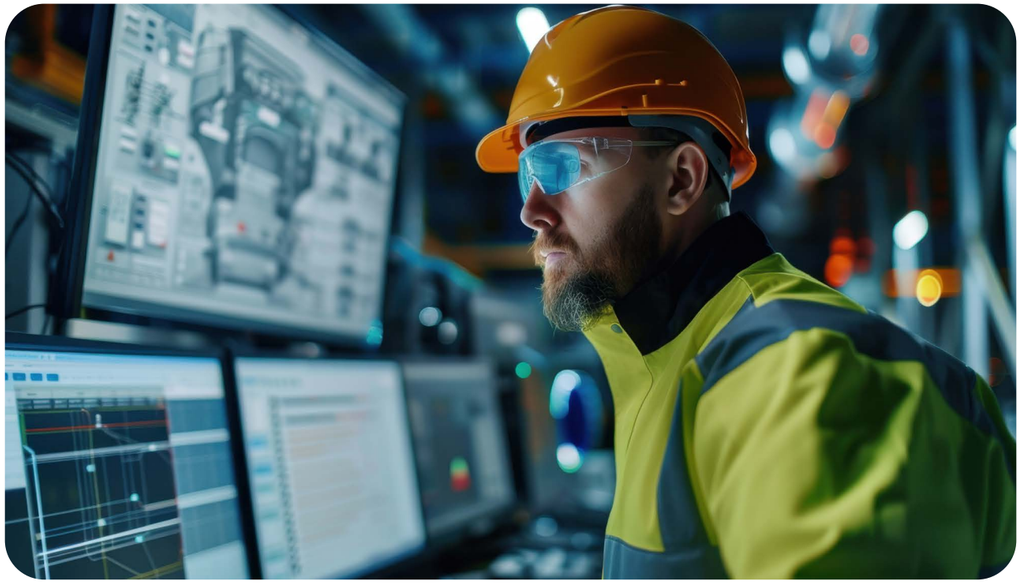
The more detailed the containment portion of the playbook, and the more clearly it identifies the people responsible while providing them with clear instructions and resources, the more comfortable they will be in making timely and effective decisions to slow or stop the spread of ransomware.

Eradication

Eradication involves removing ransomware components, affiliate tools, and unauthorized access from the OT environment. This process includes many components, including rogue accounts, stolen passwords, firewall rule changes, hacking tools, reconfigured remote access devices, altered host services, and persistent malware. These types of changes must be removed from devices that will not be fully rebuilt or replaced before restoring operations. This task becomes even more challenging in legacy or less-mature OT environments.

At a minimum, the eradication section of an OT ransomware playbook should include guidance or cross-references to the following considerations:

- **Impact on Operations:** What impact could modifications to the process environment have on operations, and who is responsible for approving eradication actions?
- **AD Domain:** If an AD domain is present in the OT environment, who is responsible for rebuilding tampered or deleted Domain services, and do they have the necessary processes and backups to do so?
- **Credential Reset:** How are large-scale account credential resets performed, and who is responsible for executing them?
- **Specialized Credentials:** If vendor credentials, shared credentials, hard-coded credentials in industrial applications, or service accounts need to be changed, who is the primary stakeholder?
- **Domain-Joined Systems:** For domain-joined OT systems, how will processes, services, and files be removed from multiple computers, and who is responsible for these tasks?
- **Standalone Systems:** For standalone OT systems, how will processes, services, and files be removed, and who will perform these changes?
- **Network Infrastructure Devices:** Who will revert changes to network infrastructure devices in the OT environment, and do they have access to the appropriate configuration backups?
- **Local File Servers:** Who maintains and manages any local file servers in the OT environment, and what are their procedures for cleaning and restoring critical shared files if they are encrypted or tampered with?



Recovery

The recovery phase of the Incident Response process involves returning systems to production and restoring services. In OT environments affected by modern ransomware, the challenges and deviations from standard enterprise recovery procedures mirror those encountered during the eradication phase. However, an additional consideration in OT environments is the potential for a ransomware payment to be factored into the recovery strategy.

Ransom Payment Consideration

As previously emphasized, the primary concern in any OT environment is ensuring the safe operation of critical processes. Processes vary significantly in their capacity to continue operating manually, the duration they can safely function without digital systems, and the complexity and cost associated with rebuilding large numbers of compromised systems. Ultimately, decisions regarding the approach to recovery—whether through traditional incident response and system restoration or by opting to pay a ransom—are risk-based determinations made by facility and executive management.

To guide these decisions effectively, a ransomware playbook should include or cross-reference specific criteria tailored to the organization and its unique operational environment. These criteria serve as a foundation for informed decision-making during a ransomware incident and should be considered in the playbook:

- **Decryptor Availability:** Given the metadata collected in the Identification phase, are decryptor tools for the ransomware variant available from third-party security firms? If so, when tested on an isolated impacted system, do they function reliably?
- **Tolerable Outage:** What are tolerable outage durations for the process as documented in the BCP?
- **System Disablement Impact:** How will disabling some or all high-level computers in the OT environment impact normal and safe operations?
- **Fallback Operations:** Are there safe reliable fallbacks to manual operations without those systems, and how long can they be sustained at a reasonable cost?
- **Recovery Versus Ransom:** After evaluating recovery methods (discussed later in this section), what will the cost be to investigate and restore the environment versus paying the ransom and subsequently removing the attacker? Note: Obtaining an accurate ransom quote may require engaging a negotiation service to contact the ransomware affiliate, which carries its own risks.
- **Geopolitical and Policy Concerns:** Are there specific geopolitical or organizational policies that prohibit paying a ransom to the criminal group or state involved?

In certain scenarios, paying the ransom in an OT environment may be the only viable option to ensure safe operations and maintain business continuity. However, it is critical to recognize that ransom payment does not eliminate the presence of the initial access broker or ransomware affiliate within the process environment. A comprehensive investigation and subsequent containment efforts are essential to fully remove their access after system restoration.

While paying the ransom may facilitate the restoration of individual system functionality, it does not guarantee the reliability or integrity of those systems to a level sufficient for safe industrial operations. Therefore, organizations must approach ransom payment as a temporary and incomplete solution, emphasizing the necessity of a thorough post-incident forensic investigation to secure the environment.

If an organization foresees any scenario where ransom payment may be a desired option, their ransomware playbook should clearly reference the chosen negotiation firm (or one selected by their insurer) to streamline the process.

System and Process Restoration

The preferred response to a ransomware incident is to rebuild and restore systems and infrastructure without resorting to ransom payment. The effectiveness and resilience of this process are significantly enhanced by having well-defined and thoroughly tested playbooks that are regularly practiced.

Modern ransomware actors often target numerous systems rapidly, including both physical hosts and virtual machines. Organizations generally face two options for restoring ransomed systems:

1. **Decryptor Tools:** Leveraging tools developed by security researchers to decrypt affected systems without paying a ransom.
2. **Manual Restoration:** Rebuilding affected systems or restoring them from backups.

Both approaches require careful planning and execution to ensure the timely and secure restoration of operations.

The key to successfully restoring ransomed systems is having high-quality, tested backups of all impacted OT systems. This poses a challenge in environments with standalone, legacy, and vendor-provided systems.

The ransomware playbook should include or cross-reference backup restoration and DRPs and emphasize the importance of regular testing and validating backups and the restoration process. Restoration of virtualized systems is also a key concern, as modern ransomware actors frequently destroy hypervisors early in their attack playbook. While individual virtual machines might be easy to restore, many organizations do not have full offline backups of their hypervisor servers.

At a minimum, the recovery section of an OT ransomware playbook should address the following considerations:

- **Restoration Process:** What is the process for restoring each class of OT high-level computer from backups, and who performs those tasks? Would they require additional support during a large-scale incident impacting many computers?
- **Backup Components:** Are backups maintained for device configurations, logic, displays, installers, licenses, necessary firmware, and updates?
- **Backup Storage and Testing:** Are backups maintained off the local network? How often are they tested? How long are they retained?
- **AD Domains:** If an AD domain is present, who is responsible for fully rebuilding the Domain Controller(s), and do they have a defined process to do so?
- **Vendor-Managed Systems:** For vendor-managed and operated systems, who is responsible for restoration, and what is the service-level agreement (SLA) for completion?
- **File Servers and Cloud Services:** Who maintains local file servers or cloud services in the OT environment, and what are their procedures for full restoration or recovery if they are encrypted or tampered with?
- **Lower-Level System Validation:** Who is responsible for validating that lower-level systems and their project files have not been purposefully or accidentally modified or corrupted during the ransomware event? Do they have processes and tools verify this?

Lessons Learned

After a stressful ransomware incident, it's easy to want to stop and rest. However, there are important after-action activities which should be considered in an OT incident.

The first step in the post-incident review process is to convene key stakeholders to evaluate the effectiveness of the incident response effort. In OT environments, the metrics used to assess performance—key performance indicators (KPIs)—may differ from those typically employed in enterprise IT contexts. Due to the primary focus on safety and operational continuity, metrics such as time to recovery and the impact on process operations are often prioritized over the depth of forensic analysis.

The ransomware response playbook should explicitly mandate a post-incident meeting to review the incident response. This meeting should focus on identifying successful strategies, areas requiring improvement, and urgent issues requiring immediate remediation. These evaluations are critical for refining the playbook and enhancing the organization's preparedness for future incidents.

Additionally, the ransomware playbook should recommend evaluating potential updates to various documents relevant to the impacted environment, including:

- OT Incident Response Plan
- Ransomware Playbook
- Business Continuity Plan
- Disaster Recovery Plan
- Network Topology Diagrams
- Asset Inventory/configuration management database (CMDB)
- Detection and Monitoring Program Playbooks

Finally, it is important to securely maintain detailed notes about the incident, including information on the ransomware affiliate, variant, and intrusion timelines, for future reference and preparedness.

Playbook Appendices

A ransomware playbook should be concise to ensure it remains manageable during a crisis or by a junior team member. Detailed tactical workflows developed in the main sections should be placed in the appendices and cross-referenced accordingly. Common appendices for successful OT ransomware playbooks include procedures for:

- Collection of ransomware metadata
- Preservation of evidence
- Scoping ransomware spread within the OT environment
- Containment strategies for rapidly spreading ransomware
- Eradication of common ransomware artifacts across the network
- Decision trees for manual restoration versus ransomware payment

Additional playbooks addressing broader incident types may also be developed. However, it is often more practical to include these within the overarching OT Incident Response Plan and reference them in the ransomware-specific playbook as needed. This approach ensures coherence, avoids unnecessary duplication, and maintains a comprehensive response framework.

Conclusion

Ransomware remains a critical threat to OT environments, where its impact can disrupt essential processes, compromise safety, and challenge organizational resilience. This paper presents a structured framework for developing ransomware response playbooks specifically tailored to OT environments, emphasizing preparedness, collaboration, and process-centric response strategies.

By focusing on the unique challenges of OT networks, such as their architectural immaturity and the criticality of safe operations, the framework provides actionable guidance to enhance incident response capabilities. From fostering collaboration between IT and OT to defining playbook phases aligned with the SANS PICERL lifecycle, the approach equips organizations to effectively detect, contain, eradicate, and recover from ransomware incidents while minimizing risks to safety and operations.

The proposed ransomware playbooks are not static documents but living frameworks that require regular testing, refinement, and updates as technologies, threats, and organizational environments evolve. Integrating these playbooks into broader incident response plans and embedding them into routine drills will help organizations build resilience against the growing ransomware threat.

Ultimately, proactive preparation and cross-disciplinary collaboration remain the most effective strategies for protecting critical infrastructure and ensuring operational continuity in the face of growing ransomware challenges.

About the Author

Lesley Carhart is the Director of Incident Response for North America at Dragos and a SANS Instructor. A long-time member of the SANS community, Lesley has earned multiple certifications—including GCFA, GCFE, GREM, GPEN, GCIH, and GRID—and has been taking SANS courses since 2008. She also serves as a faculty member at the SANS Technology Institute, a designated NSA Center of Academic Excellence in Cyber Defense and multi-time winner of the National Cyber League competition.

Recognized as a leader in cybersecurity, Lesley has been honored as DEF CON's Hacker of the Year, a SANS Difference Maker, an SC Magazine "Power Player," and one of GlobalData's "Top 10 Influencers in Cybersecurity." With a strong foundation in digital forensics and incident response, she specializes in protecting critical infrastructure and industrial control systems. Her deep expertise in ICS security keeps her on the cutting edge of industry trends—insight she brings directly into the classroom.

A veteran of the U.S. Air Force Reserves, Lesley combines leadership experience with hands-on technical skill. She is also known for her contributions to the cybersecurity community through public speaking, mentorship, and education—including founding PancakesCon, a free online hacking and cybersecurity conference that emphasizes community-building and support for students and early-career professionals.

Learn more about Lesley

Resources

Still feeling lost? Need to see some great examples of general cybersecurity playbooks? Check out these phenomenal examples:

WA Cyber Security Unit (DGOV Technical)'s Cybersecurity Playbooks: https://soc.cyber.wa.gov.au/guidelines/playbooks/

Canadian Centre for Cyber Security's Ransomware Playbooks: https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

References

Christopher, J. (2024, October 9). SANS 2024 State of ICS/OT Cybersecurity. Retrieved from https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

Cybercrime Magazine. (2023, July). Global ransomware damage costs predicted to reach $250 billion USD by 2031. Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Industrial Cyber. (2024, May). Growing threat of malware and ransomware attacks continues to put industrial environments at risk. Retrieved from https://industrialcyber.co/features/growing-threat-of-malware-and-ransomware-attacks-continues-to-put-industrial-environments-at-risk/

Lee, R. M., & Conway, T. (2022b, November 7). The Five ICS Cybersecurity Critical Controls. Retrieved from https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Lee, R. M., Miller, B., & Stacey, M. (2018, December 7). The Community Defense Model for Industrial Control Systems (ICS). Retrieved from https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf

SANS Institute. (2016, November 5). Incident response cycle cheat sheet. Retrieved from https://www.sans.org/media/score/504-incident-response-cycle.pdf

SANS Institute. (2024). SANS 2024 Top Attacks and Threats Report. Retrieved from https://www.sans.org/white-papers/sans-2024-top-attacks-threats-report/

SANS Institute. (2024, November). SANS Threat Analysis Rundown in Review: Breaking Down November 2024's Top Threats. Retrieved from https://www.sans.org/blog/sans-threat-analysis-rundown-in-review-breaking-down-november-2024-s-top-threats/

INDUSTRIAL CONTROL SYSTEMS SECURITY

SANS