T838: MODIFY ALARM SETTINGS

PURPOSE

This Recipe, based upon use of the CyOTE methodology[1] (Figure 1), provides asset owners and operators (AOO) with general guidance for confirming suspicion of the Modify Alarm Settings attack technique for the Inhibit Response Function tactic as defined by the MITRE ATT&CK® for Industrial Control Systems (ICS) framework[2,3] allowing them to be able to make informed business decisions based on collaborative analysis of the nature and context of the attack. This document also includes supplemental material with suggestions and recommendations for securing assets and improving detection capabilities. Additional information on this technique can be found in the *Modify Alarm Settings (T838) Technique Detection Capability Sheet* for the Inhibit Response Function tactic.[4]

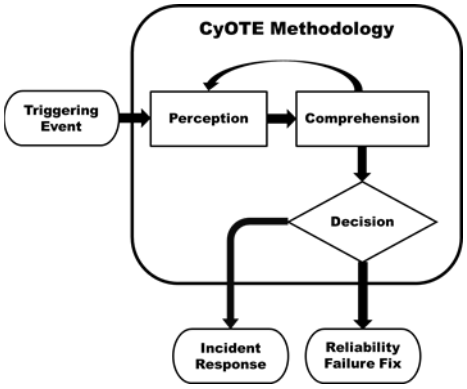

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, adversaries may modify alarm settings to change the threshold of alarms to either flood operators as a distraction or to hide the presence of an alarm condition.[5] Operator flooding might distract the response of personnel to a red herring event while an attacker performs actions in another portion of the environment. Alarm setting modification attacks that suppress alarms might cover the signs of a process-related attack within the environment.

PERCEPTION: IDENTIFYING ANOMALIES

Perception (Figure 2) is the first active step in employing CyOTE's methodology. CyOTE uses the terms "perception" and "comprehension" as opposed to terms like "detection" and "understanding." This nomenclature follows the North American Electric Reliability Corporation (NERC) nomenclature, which was adapted from Dr. Mica Endsley's model of situation awareness[6] – these terms cause the reader to think of the necessary individual and organizational human cognition as opposed to merely automated

[1] CESER, Methodology for Cybersecurity in Operational Technology Environments, CyOTE Program. Department of Energy, FY21, https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf.
[2] MITRE, Modify Alarm Settings, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0838.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Modify Alarm Settings (T838) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Modify Alarm Settings, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0838.
[6] Mica R. Endsley, "Situation Awareness Misconceptions and Misunderstandings," Journal of Cognitive Engineering and Decision Making 9, no. 1 (March 2015):4, https://doi.org/10.1177%2F1555343415572631.

data processing. Perception is defined as a signature capable of being detected by a human; perception does not mean opinion or subjective interpretation. It provides the starting point—detection of a triggering event in the organization—for investigation during the comprehension step. This stage involves the identification of observables, anomalies, and triggering events of a potential malicious event; please consult the CyOTE methodology for more information on these terms.[7]

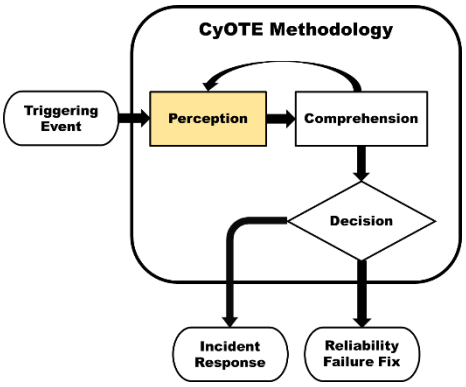

Figure 2: CyOTE Methodology – Perception Step

EXAMPLE OBSERVABLES AND ANOMALIES OF THE MODIFY ALARM SETTINGS TECHNIQUE

Differences between operational environments require AOOs to understand the generic and unique attributes of the environment under analysis. The anomalies and observables in Table 1 serve as a generic starting point to adapt to the realities of the specific environment. Each potential anomaly includes data sources where it may be observed, as well as what the observables may be.

Note that this table is not intended to be an exhaustive list of anomalies, data sources, or observables tied to the Modify Alarm Settings technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
• Unexpected change in file modification, access, or creation time • Creation of unexpected file metadata or application logs associated with file access	File metadata change (e.g., access time, user) by unauthorized user	File Metadata
• Plant personnel might notice device operating outside of normal parameters when monitoring device activity	Alarms failing to trigger when device operates outside of normal parameters	• Operator or Plant Personnel • Application Logs
• Plant personnel might notice a deviation in the amount and times alarms trigger	Change in alarm volume or frequency	• Application Logs • Sequential event recorder • Operator or Plant Personnel • Alarm history

[7] CESER, Methodology for Cybersecurity in Operational Technology Environments, CyOTE Program. Department of Energy, FY21, https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf.

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS MODIFIED ALARM SETTINGS

Asset owners and operators aiming to develop potential capabilities to monitor for use of the Modify Alarm Settings technique should consider a phased approach to development of the monitoring capability, to include continuous testing and evaluation throughout capability's life cycle. To complement this, it is highly encouraged to use the following steps to map out existing OT infrastructure both logically and physically. This supports capability development and the analysis of potential alerts, enabling the quick identification of control devices communicating within the infrastructure.

Continual testing and evaluation will ensure the newly introduced software does not negatively impact, adversely affect, or introduce vulnerabilities into the existing OT environment. As a guideline, during the development phase, secure coding practices should be employed.[8]

1. Identify critical and secondary process systems and data points to monitor for modified alarm settings
    a. Identify critical components
    b. Identify potentially susceptible components or communication paths (e.g., protective relays and remote terminal units [RTU]/automation controllers)
2. Identify applicable protocols and parsers utilized by these processes
    a. E.g., Common Industrial Protocol (CIP) (ControlNet, DeviceNet, Ethernet/IP), S7Comm, Profibus, SERCOS III, Modbus, DNP3, Host HAP, Koyo DirectNET
3. Identify logs and log types (such as .pcapng) that need to be forwarded to this capability from fielded devices
4. Identify tap points (sensors) for observing device traffic for identified devices and systems
    a. This may include servers, switches, security appliances, and logging locations (hosts)
        i. Plan sensor placement based on locations within the architecture that provide context related to the anomaly and prioritize systems at greater risk
    b. Identify the existing network connections (e.g., ethernet, fiber, serial, Wi-Fi, RF, broadcast domains)
        i. Depending on the environment, serial device servers may be needed to convert between multiple different protocols
    c. Establish passive network taps
        i. Monitoring and traffic aggregation may necessitate tap placement on both sides of the identified devices (e.g., media access control [MAC] addresses may change as information traverses networking infrastructure like protocol converters)
    d. Recommend establishing capture requirements for monitoring OT traffic and their locations[9, 10]
        i. Storage (how much and for how long)
        ii. Line rate (e.g., 1/10/40/100 Gb)

[8] Microsoft, "Security engineering SDL practices," Blog, available online at https://www.microsoft.com/en-us/securityengineering/sdl/practices.
[9] CESER, Security Monitoring Best Practices, CyOTE, 2021.
[10] CESER, Lessons Learned, CyOTE Program, Department of Energy, 2021.

iii. Live stream data or full Packet Capture (PCAP) offline
iv. Central versus distributed collection/analysis/alerting

5. Identify business processes that support identification of Modify Alarm Settings
   a. Identify opportunities where plant personnel or other network and device users would identify signs of technique occurrence
   b. Identify operational data stores that might assist with confirmation of technique identification
      i. Help desk tickets related to technique
      ii. Plant maintenance tickets related to technique
      iii. Unusual behaviors or actions that plant personnel or a network user would observe related to the technique

COMPREHENSION: ANALYZING TRIGGERS AND THEIR CONTEXT

The second step of employing the CyOTE methodology is Comprehension (Figure 3). Comprehension is the ability to understand an anomaly in all its relevant context across the operations, OT, information technology (IT), business, and cybersecurity domains. Comprehension involves understanding the nature and possible origins of the anomaly and developing broader awareness of the overall context in which the triggering event came to be. Because of the multidisciplinary approach used for a sufficient investigation, comprehension for the purposes of CyOTE is an organizational ability, not an individual one.

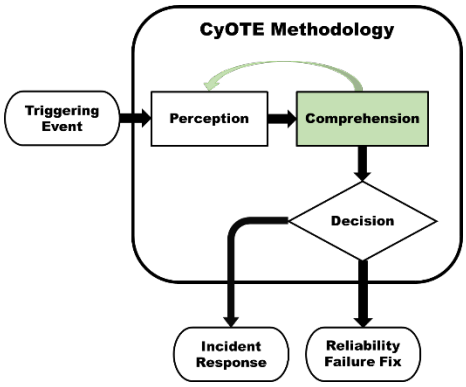

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO MODIFY ALARM SETTINGS

Developing comprehension around an anomaly is most effective and efficient when small core teams of full-time system operators, OT technicians, and cybersecurity analysts from different departments and external resources come together to purposefully focus on the problem in the context of their shared organization. Table 2 includes a list of different organizations that could be leveraged to collect information on an anomaly. Depending on the size and resources of your organization, some of these resources might not be applicable.

Table 2: Business Organizations that Support Information Collection for Modify Alarm Settings

Organization	Capacity
• System Operations Departments	Control center field operators and real-time engineers should be one of the first sources consulted. Information

Organization	Capacity
• Engineering Departments	collected might include manual logs, notes from field personnel investigations, or other records if the anomaly involved a disruption in the system above some established threshold.
Cybersecurity Departments	Includes those responsible for the confidentiality, integrity, and availability of the organization's digital assets provide the threat-informed perspective and bring experience and capabilities to analyze situations and data for security issues.
Original Equipment Manufacturers (OEM)	Includes those who produce and support the hardware and software present within the industrial environment. OEMs might or might not be under support contracts but might provide technical documentation and expert advice on expected device behavior.
Third-Party Support Vendors	Cybersecurity, threat intel, and other vendors that provide subject matter expertise might be able to provide insight into anomalies surrounding the trigger conditions.

Since access to raw data typically requires coordination with human organizational oversight, it generally is better to pursue information and context from different departments within the organization. When needed, have them provide the identified data under their control for shared analysis. Appendix A provides specific datasets and information that could be helpful depending on the situation.

STEPS FOR IDENTIFYING AND EXTRACTING INFORMATION FROM OT DATA FOR ANALYSIS OF MODIFY ALARM SETTINGS

The information on high-consequence systems, pathways, and potential anomalies identified previously becomes more refined for collection in this process. Extracted information should be prioritized based on importance, with timelines established for capturing and holding information for analysis and review.

Suggested data fields to collect include:

- Timestamp
- Device Identifier (will vary based on environment)
    - Source and destination IP addresses
    - MAC addresses
- Message
- Program payload
- Alarm setting parameters

- Payload size (e.g., bytes)

STEPS FOR ANALYZING ANOMALIES FROM PARSED DATA FOR MODIFY ALARM SETTTINGS

The suggested fields above are applied to data analysis and used to help establish anomalies. The list below includes suggested ways to use the extracted fields to help identify anomalies that could be alerted on. Any message revealing two or more parameters is given greater precedence for analysis and correlation with other observables to identify potential anomalies.

1. Identify host devices to alert on
    a. Document alarm modifications based on host
        i. Include the frequency and type of modification(s)
    b. Identify and match high-risk medication type(s) or magnitude for the physical process
        i. Determine if the alert is valid or invalid based on analysis of the message parameters and source
2. Identify alarm modifications coming from new or abnormal hosts
    a. Analyze host lists for modifications to host files and log files
    b. Conduct a comparative analysis of old logs vs. new logs
        i. Unauthorized start/stop/restart of a process or service
        ii. Perform statistical and/or analytical review
            1. E.g., frequency, order, type, messaging timing
3. Establish triggers
    a. Incorporate the analysis findings provided previously and implement to refine alert parameters to focus on useful information and minimize the number of non-useful alerts
        i. E.g., new or abnormal messages, high-risk program modification messages, out-of-bound readings without alarms

REPORTING TRIGGERING EVENTS

Security needs to consider the operational and business aspects of the organization. Timely reporting of anomalous activity reduces the time needed to comprehend triggering events and make a decision, leading to reduced process outage times. The following guidance aims to enhance your organization's existing reporting procedures, although these guidelines might also vary based on the composition of your organization. If your industry or organization requires stricter timeframes or processes, you should default to the more stringent timeframe and procedures.

Programmatic alarms should already be logging information, but organizations should document any contextual information for further analysis and reporting. Organizations should also report unusual operating conditions not based on programmatic alarms. Examples of essential details to record include the usual and intended conditions and how the observed operating condition deviates from expected. Table 3 below provides reporting guidelines for a sample of triggering events but is by no means an exhaustive list.

Table 3: Triggering Event Reporting Suggestions for Modify Alarm Settings

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Device operating outside of normal parameters	• Owner of the account that made the modification • Team responsible for network resource • Network security team	1 hour (operational impact)	• Identify if the change in alarm setting is related to planned business activity • Identify user or process responsible for command issuance • Identify other potential observables associated with nefarious actions on the system • Validate if the change or account access correlates to know activity or vendor service window

ANALYZE INFORMATION AND CONTEXT COLLABORATIVELY

Documentation and Knowledge Management Process

Begin a documentation and knowledge management process in support of the investigation. Start with a determination of perceived actions in the triggering event. Did the change occur within:

- The physical domain (something involving telemetered quantities such as noise, voltage, current, frequency, or temperature, or the physical configuration of a piece of infrastructure); or
- The OT domain (something involving traffic or signals transiting a communication medium, or the logical configuration of a piece of infrastructure, or something involving memory/storage metrics); or
- Both the physical and the OT domains?

Given the determination of a physical or OT starting point, identify what expected corresponding, perceptible observables would exist in the other domain and search for their presence or absence. For example, an unplanned file server reboot initiated by a program that was downloaded might produce digital footprints like logs and errors. It might correspond to data loss, unauthorized configuration changes, elevated user permissions, or account activity at unusual hours.

Technical Analysis

The order for which technical analysis should occur, or whether it is even necessary for the comprehension stage, depends on the situation, but typically it will inform many of the context-building questions outlined in the following section.

Attacks using the Modify Alarm Settings technique will likely require network traffic, host log, and file system analysis reports to properly comprehend the context and nature of the attack and determine how/if the triggering event is connected to other attack techniques. Network analysis may include flow analysis and packet inspection, depending on the circumstance. Technical analysis should first identify the scope of impacted devices and all peripheral systems, applications, and/or accounts that have been compromised.

Configuration files should be compared to a copy of a baseline configuration file to determine if improper or malicious configuration changes have occurred. If no baseline exists, suspect configuration files should be analyzed.

Context Building

Network data, if available, can provide the initial cluster of devices to focus on for initial context analysis. The viability of network analysis might vary depending on enabled protocols and the ability to parse communications from the protocols. The following considerations intend to assist with initial analysis:

- Context building should originate with either the system directly observed as being under attack or with the system reporting the highest severity of operational errors. The initial origin point of analysis might require an operator or analyst to leverage their knowledge and experience within the environment and intuition to determine the ideal starting point.
- Determination of significant operational impact might involve discussions with operators. While operators might not be security experts, they do understand the physics of the environment and might also have a level of intuition as to what “normal” is within the environment.
- Determination of systems under attack might involve a review of host data or network data. Comparing alarm settings to previous backups can provide insight into attacker motivation and/or desired impact.

Visual Information Modeling

Enumerate all the lines of questioning identified through this stage of the analysis of the anomaly. At this point, it is beneficial to begin a node and link diagram from the information documented in the knowledge management processes to help visualize relationships between observables; the CyOTE program colloquially refers to this observable linking diagram as a “worm diagram.”

The triggering event is the first node, with all its related observables radially connected to it; include both confirmed observables and observables that were expected but not found, with some sort of visual

discriminator between presence and absence (e.g., solid or dashed lines). Highlight the triggering event if the event relates to the implementation of a specific adversary technique. Include links emanating from the triggering event representing the as-yet-unanswered questions considered, as well as links and additional nodes for answered questions that confidently satisfy the extent of a particular line of inquiry. A notional example[11] of this diagram for an investigation in progress is shown in Figure 4.

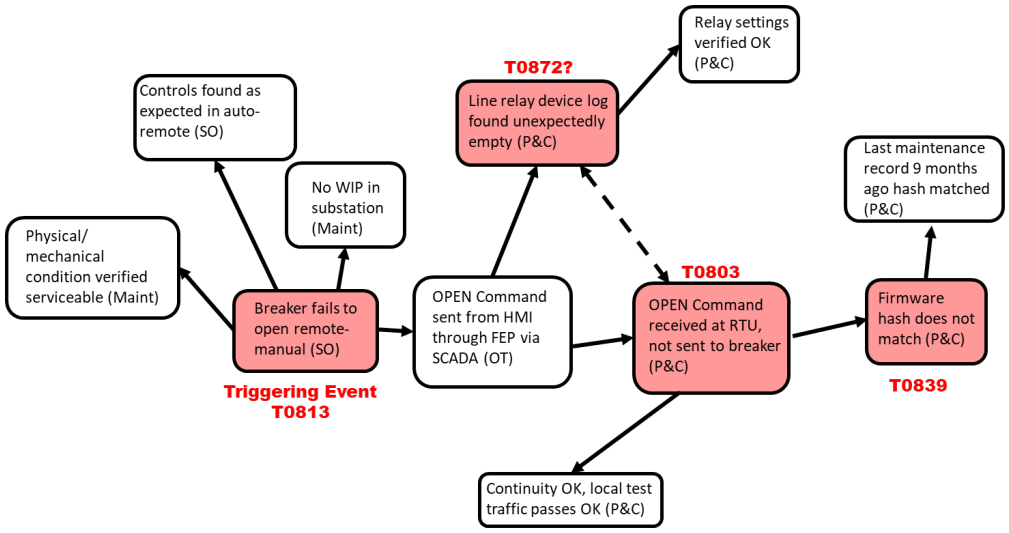

Figure 4: Example CyOTE Observables Link Diagram

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO MODIFY ALARM SETTINGS

After an anomaly has been comprehended sufficiently and mapped to a technique, repeat the steps above, starting from each questioning line resulting from the initial anomaly analysis. The importance of recording and organizing the information discovered in the comprehension process and visualizing it through a node and link diagram becomes exponentially more important as the first perceived anomaly expands into a web of postulated, confirmed, and denied relationships.

[11] Current CyOTE Case Studies do not include an analysis on the use of this technique in a historical attack; thus, there is no link diagram specific to this technique at this time.

DECISION: REMEDIATING THE CAUSE AND EFFECTS OF A TRIGGERING EVENT

The last step of the CyOTE methodology is the Decision step (Figure 5). In this step, the AOO makes a risk-informed business decision on how to proceed based on the information gathered in the previous steps. The level of comprehension and detail needed to make the decision will vary from company to company and may be related to resource availability. The length and consistency of a discovered and comprehended "worm diagram" representing a prospective kill chain fragment needed to decide to proceed with incident response will also vary based on a company's risk tolerance.

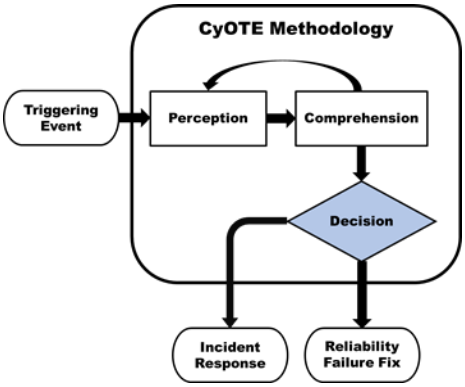

Figure 5: CyOTE Methodology - Decision Step

INCIDENT RESPONSE

In situations where there is sufficient belief that the anomalies perceived and comprehended indicate possible malicious cyber activity, the appropriate organizational action is to initiate a cybersecurity incident response process according to established policy and procedures. The information and context developed through the application of the CyOTE methodology will be helpful to incident handlers for developing and implementing appropriate mitigating actions. Consult with your organization's incident response procedures for the next steps.

CORRECTIVE MAINTENANCE

When analysis fails to establish a reasonable indication of malicious cyber activity, the next step is to determine if the anomalies indicate that a non-malicious failure is occurring. One appropriate action involves resolving any deficiencies discovered through corrective maintenance and work management processes according to organizational policy and procedures. It is worthwhile to maintain records of these situations for future reference and comparison to subsequent anomalies. Consult with your organization's engineers, operators, and other parties responsible for maintenance in your environment. For vendor-supported devices, coordinate with external parties when necessary.

IMPROVING SECURITY CAPABILITIES

Prevention and preparation include proactive measures to reduce the risk or likelihood of an attack or enable an organization to respond more rapidly. Preventive actions may raise the cost of an attack, which could deter the attacker from an act or eliminate the possibility that specific attack paths would be used altogether. AOOs should develop and deploy data collection management strategies to prepare for the collection of data needed to detect this technique and properly analyze potentially anomalous triggers.

CONTROL MATRIX FOR MODIFY ALARM SETTINGS

The control matrix (Table 4) is a technical capability or system designed to prevent or sabotage specific attack techniques used by malicious actors. The control matrix assists with the identification of detection capability improvement areas.

Table 4: Control Matrix

Control	Matrix	Relevance
Application Hardening	MITRE D3FEND: D3-AH[12]	Application Hardening helps prevent certain applications from being exploited and, in turn, prevents an adversary from leveraging existing code or introducing their own. This is a common method used because it can allow an adversary to modify alarm settings by modifying in memory code to fixed values or tampering with assembly level instruction code. • Be sure to properly vet third party products and software before integrating them into your network. Discuss with the vendor what Application Hardening techniques they use for their products.
Authorization Enforcement	MITRE M0800[13] NIST SP 800-53 Rev. 4[14]	Authorization Enforcement restricts certain rights and privileges, such as read and write, to only those necessary. Always abide by the Principle of Least Privilege which states to only grant users with the minimum level of access needed to perform their job function. • Role Based Access Control schemes can be useful when for managing privileges at scale • Track privileged user activity
Software Process and Device Authentication	MITRE ATT&CK for ICS: M0813[15]	Software process and device authentication require certain processes and devices to be authenticated where appropriate. Level of authentication can vary depending on the criticality of the system that is being accessed or the process that is trying to execute. • Heavy authentication should be used for devices using remote connections to prevent unauthorized access. • Software processes that control or impact device functionality should also be authenticated prior to execution to prevent unauthorized access to any protected functions. • Validate that the authentication methods implemented do

[12] MITRE, Application Hardening, 2021. Available from: https://d3fend.mitre.org/technique/d3f:ApplicationHardening/.
[13] MITRE, M0800: Authorization Enforcement, 2020. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0800.
[14] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, 2020. Available from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22. This publication was withdrawn on 09/03/2021, one year after the publication of revision 5.
[15] MITRE, Software Process and Device Authentication, 2020. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0813.

Control	Matrix	Relevance
		not send credentials over the network.
Mandatory Access Control	MITRE D3FEND: D3-MAC[16]	Mandatory Access Control by file path level controls is a kernel-level execution isolation security control used to control access to information repositories by pathname level access policies • Access policy must be implemented before developing or acquiring a capability for this security control. • Some implementations can be complex and difficult to maintain over time.
Software Update	MITRE D3FEND: D3-SU[17]	Software Update is a platform hardening security control used to reduce the attack surface of OT software. For T838, it is necessary to update any software or application which authenticates or facilitates user access to information repositories. • Identify and document all software, applications, and their versions. Additionally, keep an updated log/history for documented software. • Implement systems to alert relevant personnel to newly available software versions. • Implement systems to alert relevant personnel to any CVEs, vulnerabilities, or recent exploits to current or previous software versions used to authenticate or facilitate access to information repositories. • Consider that a newly exploited vulnerability in an older software version may not yet be patched in an up-to-date version. • Develop a policy regarding software update standards and requirements. Consider employees, contractors, remote access applications, and software acquisition. • Develop guidelines to employ authentication mechanisms (like hashing) for software update sources.
Network Segmentation	MITRE ATT&CK for ICS: M0930[18]	Network segmentation divides your network into sections based on manufacturer specification, role, or by the design of your organization. Network traffic filtering applies a set of rules at different points in the network or on a host to stop the communication of packets that meet a given signature. Network allowlists can also be used to block traffic based on

[16] MITRE, Mandatory Access Control, D3-MAC, 2021. Available from: https://d3fend.mitre.org/technique/d3f:MandatoryAccessControl/.
[17] MITRE, Software Update, 2021. Available from: https://d3fend.mitre.org/technique/d3f:SoftwareUpdate/.
[18] MITRE, M0930: Network Segmentation, 2021. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0930.

Control	Matrix	Relevance
Filter Network Traffic	MITRE ATT&CK for ICS: M0937[19]	traffic metadata such as IP address, ports, time, or other fields within a given communication stream. • Network segmentation enables additional choke points to filter network traffic at or implement other network allowlist based techniques • Consider what network services should be accessed between network segments and apply rules at the host and network level to enforce the segmentation • Traffic filters and allowlists provide two means of protection by actively limiting what functions can be performed at different points across the network. This prevents unauthorized command messages from certain network segments.
Network Allowlists	MITRE ATT&CK for ICS: M0807[20]	

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR MODIFY ALARM SETTINGS

The parameters and established anomalies from previous analysis lead to the continual testing and gradual deployment of the capability and evaluation of alerts. The resulting output functions and considerations are realized during this process, the products of which are sent to output destination(s) in selected format(s).

1. Validate triggers and alerts
    a. Ensure the capability does not conflict with existing monitoring functionality
    b. Ensure the capability does not adversely impact the existing environment
    c. Test alerting functions
        i. Use synthetic data (e.g., PCAPs containing program downloads)
        ii. If the test fails, re-evaluate the steps taken iteratively (line by line)
        iii. If successful, enact a graduated deployment schedule and retest for each iteration
    d. Consider communication criteria for multiple locations and information consolidation during graduated deployment
2. Identify output destination(s) (e.g., SIEM, Splunk, Gravwell, Elk)
    a. Identify output format(s) (e.g., STIX, Syslog, JSON, CSV)
    b. Define actionable data requirements, processes, and responses
        i. Logging
        ii. Alert content
        iii. Alert response(s) (local or SOC)
3. Identify what information to log (long-term/short-term)
    a. The aggregation of different log types may assist in identifying potentially anomalous behaviors within OT environments

[19] MITRE, M0937: Filter Network Traffic, 2021. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0937.
[20] MITRE: M0807: Network Allowlists, 2021. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0807.

The overall output of this process may result in one of the following: script, application, YARA rule, SIEM plugin, or another tool capable of identifying and alerting on the use of the Program Download technique within OT environments.

CONCLUSION

By employing the strategies in each step of the CyOTE methodology outlined in this Recipe, AOOs will be able to develop a capability to read and analyze their OT traffic and determine whether the Modify Alarm Settings technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Modify Alarm Settings technique. Determining the associated observables and potential data sources for these anomalies will give the AOO the basis they need to begin comprehending the context in which a triggering event involving the Modify Alarm Settings technique came to be. Unexpected file metadata changes, devices operating outside of normal parameters, and deviations in the timing and amount of alarms triggering are all potential observables that could indicate the use of the Modify Alarm Settings technique. Anomalies tied to these observables could be file metadata changes made by unauthorized users, alarms failing to trigger when expected, or unexpected changes to alarm volume or frequency.

The Comprehension step is used to collect information around observables and anomalies via the data sources identified in the previous step. AOOs should leverage various business organizations and areas of the OT environment for information for identifying and analyzing anomalies related to the Modify Alarm Settings technique. This will allow them to more quickly identify triggering events using the Modify Alarm Settings technique, enabling the decision making in the Decision step.

AOOs use the Decision step to determine a course of action based on an event that has occurred. With on the information gathered, the AOO will be able to determine whether an anomalous alarm setting modification is indicative of an adversary's presence in the network (thus initiating incident response procedures) or if there is no evidence of malicious activity associated with the anomalous alarm setting modification (thus initiating corrective maintenance procedures).

Additional assistance regarding general sensor placement and capability development is available through DOE. AOOs can refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

APPENDIX A: DATASETS TO SUPPORT TRIGGERING EVENT ANALYSIS FOR T838: MODIFY ALARM SETTINGS

Table 5: Datasets to Assist with Analyzing Triggering Events

Dataset	Example Tools	Who Can Assist	Relevance
NetFlow and Packet Data	• Wireshark/Tshark • Commercial Passive Network Monitoring Tools (Claroty, Dragos, Nozomi, SilentDefense) • Zeek • NetworkMiner • Snort • Suricata • Security Onion	• Network Security Team • IT or OT System Admins	NetFlow and packet data assist with the identification of systems communicating with an information repository and possibly detailed communication details.
Device and System Logs	• SysInternals SysMon • SysInternals PsLogList • EvtxToElk • Python-evtx • OSQuery	• Network Security Team • IT or OT System Admins	Data from the device and system logs assist with the identification of behaviors associated with information repository access.
Device and System Configuration Files and Change History	SysInternals Suite	• Network Security Team • IT or OT System Admins	Device and system configuration files and change history assists with the identification of other data sources to pivot off of
Account administration data like permission settings, account logs, onboarding information	SysInternals Suite	• Network Security Team • IT or OT System Admins	Permission settings, account logs, and onboarding information for accounts can assist with discovering other associated behaviors with the trigger event in question.
Device or System Maintenance Documentation/Logs	SysInternals Suite	• Network Security Team • IT or OT System Admins	Device or system maintenance documents and logs assist with the identification of systems communicating with an information repository and possibly detailed communication details.

Dataset	Example Tools	Who Can Assist	Relevance
Physical access logs and security monitoring data like CCTV output	Application Logs	Physical Security Team	Physical security logs and CCTV adds another factor of validation to assist with the validation of the true source.
System engineering documents like network layouts and other schematics or diagrams	Internal Organization Diagrams and Documentation	• Network Security Team • IT or OT System Admins • OEMs/Vendors	Environment documentation assists with the identification of other logging sources or impacted systems.
Lists of software, apps, hardware, devices, or other relevant systems and their respective manufacturers	Asset Inventory Tools (Claroty, Dragos, Nozomi, SilentDefense)	• Network Security Team • IT or OT System Admins	Software and hardware lists assist with the identification of other impacted systems as well as other potential log resources to validate a trigger event.
Any other data relevant to the investigation	Various	• Network Security Team • IT or OT System Admins • OEMs/Vendors	Other data sources associated with information repositories might contain information specific to a given trigger event.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov