T858: CHANGE OPERATING MODE

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 Change Operating Mode attack technique for the Evasion and Execution tactics 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 *Change Operating Mode (T858) Technique Detection Capability Sheet* for the Evasion and Execution tactics.[4]

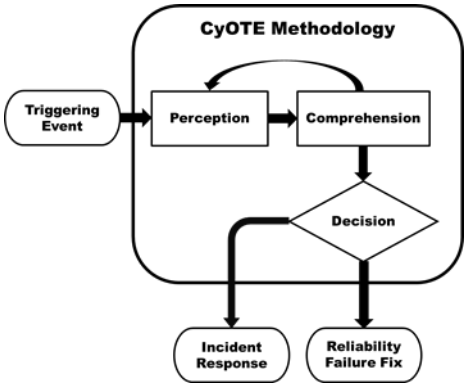

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, adversaries may use the Change Operating Mode technique to place controllers into an operating mode, or run state, that enables the adversary to change configuration settings to execute evasive code, inhibit device response functionality, or load potentially malicious program(s) on a device. This can be done either physically, through a switch on the device, or virtually, through commands sent over an industrial protocol. Depending on how a particular device implements the run state, a physical switch has the potential to be overridden with a change to the run state in the software.

Devices that can be impacted by the Change Operating Mode technique include field controllers, Intelligent Electronic Devices (IED), programmable logical controllers (PLC), remote terminal units (RTU), or other devices with a physical key switch to lock out programming that malware could override. Run states commonly implemented by controllers include program, run, remote, stop, reset, and test/monitor mode. This may force the device into an unsafe state or open the device to future vulnerability, resulting in damage to personnel, OT process interdependencies, and equipment.[5]

---

[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, Change Operating Mode, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0858.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Change Operating Mode (T858) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Change Operating Mode, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0858.

PERCEPTION: IDENTIFYING ANOMALIES

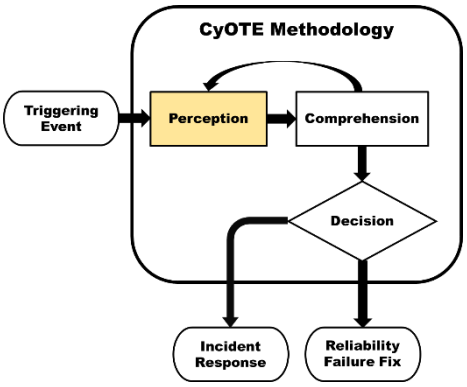

Figure 2: CyOTE Methodology – Perception Step

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" for the same reasons that the North American Electric Reliability Corporation (NERC) uses those terms, which were adapted from Dr. Mica Endsley's model of situation awareness[6] – because they cause the reader to think of the necessary individual and organizational human cognition as opposed to merely automated data processing. Perception is defined as a signature capable of being detected by a human that was actually detected; 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]

EXAMPLE OBSERVABLES AND ANOMALIES OF THE CHANGE OPERATING MODE 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 Change Operating Mode technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
• A change in run state based on device status might be passively observed when sent out over the network • A change in run state when using an industrial application such as a human machine interface (HMI) or engineering workstation (EWS)	An unexpected change in device run state or operating mode observed by an operator or other plant personnel	• Raw Network Data (Captured) • Raw Network Data (Live • Asset Identification Inventory (Active) • Asset Identification Inventory (Passive)

[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.
[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.

Observables	Anomalies	Data Sources
• A device that does not physically match the reported operating mode • This observable requires at least two visibility points in order to observe the disagreement about the current state	An inexplicable difference between a device's actual operating state with the state it is reporting	• Raw Network Data (Captured) • Raw Network Data (Live) • Asset Identification Inventory (Active) • Asset Identification Inventory (Passive)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALIES IN OPERATING MODES

Asset owners and operators aiming to detect potential capabilities to monitor for use of the Change Operating Mode technique should consider a phased approach to development to include continuous testing and evaluation throughout its 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 devices to be monitored for process state changes
    a. E.g., PLCs or relays that have key switch lockout features
2. Identify applicable protocols and parsers for those used protocols
    a. E.g., 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 to observe device traffic
    a. Consider the environment being monitored; a protocol converter such as a serial device server may be needed to convert between multiple different protocols (e.g., Modbus to Profibus); not every connection will be wired through ethernet (e.g., RF, serial, Wi-Fi)
    b. This includes servers, networking 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
    c. Monitoring and traffic aggregation may necessitate tap placement on both sides of the identified devices (e.g., a host's MAC address, changes for each new local network a packet traverses as it is being sent between each pair of routers on its way to the final destination)

[8] Microsoft, "Security engineering SDL practices," Blog, available online at https://www.microsoft.com/en-us/securityengineering/sdl/practices.

d. Recommend establishing capture requirements for monitoring OT traffic[9, 10]
   i. Storage (how much and for how long)
   ii. Line rate (e.g., 1/10/40/100 Gb)
   iii. Live stream data or full Packet Capture (PCAP) offline
   iv. Central versus distributed collection/analysis/alerting

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.

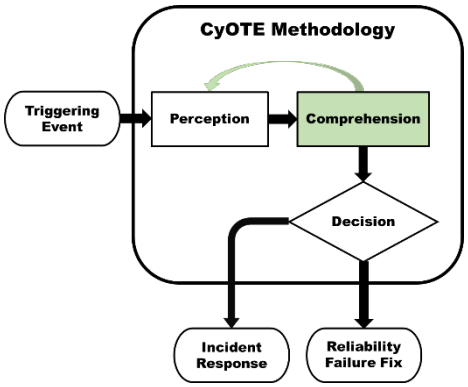

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO OPERATING MODE CHANGES

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 Change Operating Mode

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

[9] CESER, Security Monitoring Best Practices, CyOTE, 2021.
[10] CESER, Lessons Learned, CyOTE Program, Department of Energy, 2021.

Organization	Capacity
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 PARSING AND EXTRACTING INFORMATION FROM OT NETWORK TRAFFIC FOR ANALYSIS OF OPERATING MODE CHANGES

The information on high-consequence systems, pathways, and potential anomalies collected 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 protocol elements to collect include:

- Timestamp
- Device identifier(s) (will vary based on environment)
    - Source and destination IP addresses
    - Source and destination ports
    - MAC addresses
    - Operation to be watched
- Message types
- Message frame

Suggested logs to collect include:

- PLC logs identifying the filename with the operation performed or observed
- Security logs

- Syslogs
- Windows Management Instrumentation (WMI) logs

STEPS FOR ANALYZING PARSED TRAFFIC ANOMALIES FOR OPERATING MODE CHANGES

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 potentially anomalous/malicious modifications.

The Evasion tactic detection technique will monitor device logs for state-change entries. The Inhibit Response Function tactic detection technique will focus on monitoring OT network traffic for anomalies and state-change messages.

1. Identify traffic coming from new or abnormal hosts
    a. E.g., a new device or sensor communicating with controller
    b. E.g., an engineering laptop being used outside of business hours or operational maintenance windows
2. Analyze traffic for messages
    a. Start, stop, reset, load processes in various key switch states
    b. Moving between states by means of manual commands from operators or engineers
    c. Moving between states through automated means, such as sensor or other input
    d. New program downloaded to controller in various key switch states
    e. Program is uploaded from controller in various key switch states
3. Identify other TTPs to use for correlation of potential incidents
    a. Unauthorized command message
    b. Spoof reporting message
    c. Download new program

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 Change Operating Mode

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Incorrect operating mode on safety critical or operational critical system	• OT engineering team responsible for process or network resource • Safety organization(s)	Immediate	Immediate awareness of potential life safety risk to initiate immediate resolution
Incorrect operating mode on non-safety-critical or operational critical system	OT engineering team responsible for process or network resource	1 hour	Engineering break/fix ticket to troubleshoot and resolve issue

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 change to a device's operating mode 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 end goal for technical analysis should validate or disprove the hypotheses associated with the triggering condition(s). Technical analysis for changes to operating mode of a device should focus on the circumstances of the mode change and any associated human or system actions that might have

originated the operating mode change. A change to operating mode might be initiated by a hardware switch or through software. Because of the existence of both hardware and software switches, it is important to validate both sources as a potential origination source.

Context Building Questions

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 questions intend to assist with initial analysis:

- Does the device support both hardware and software changes to operating modes?
- What operating mode changes are possible with hardware and software switches?
- Does the hardware operating mode switch match the reported mode of the device?
- Is the hardware operating mode switch or key implemented in software or firmware and has that underlying software or firmware recently been modified?
- For software-implemented operating mode switches, have there been any attempts to write to memory locations associated with operating mode functionality?
- For protocols that send operating mode information over the network, can the time of the operating mode change be identified? What other control system traffic occurred in the same timeframe?

Once the scope of possible hosts associated with the potential root cause are identified and data is collected, analysis should focus on proving the original hypotheses developed through the original anomalous event. Proving or disproving the anomalous event hypotheses will support the decision-making process by validating initial perceptions and reducing initial cognitive bias.

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 of this diagram for an investigation in progress is shown in Figure 4.

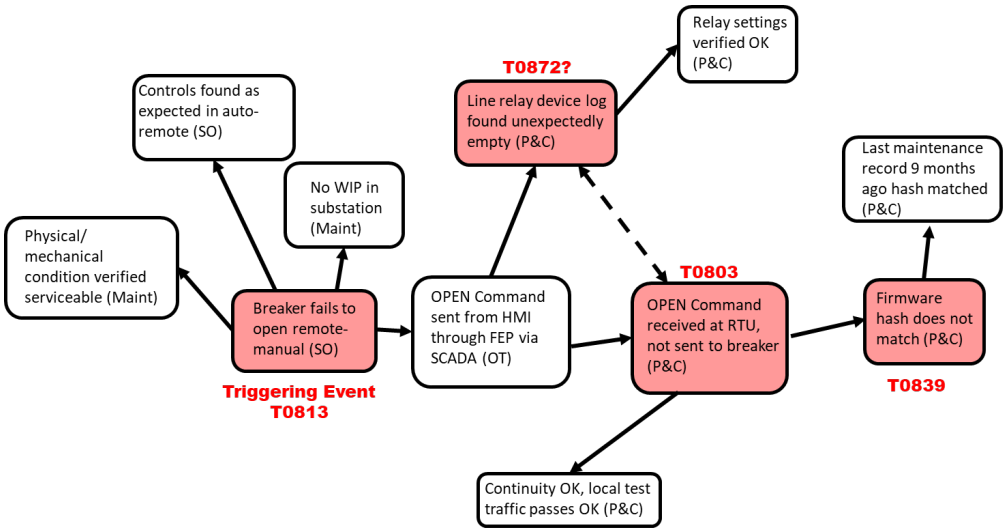

Figure 4: Example CyOTE Observables Link Diagram

A worm diagram showing the use of the Change Operating Mode technique in the 2017 Triton attack on the Petro Rabigh refinery complex in Rabigh, Saudi Arabia is shown in Figure 5.[11]

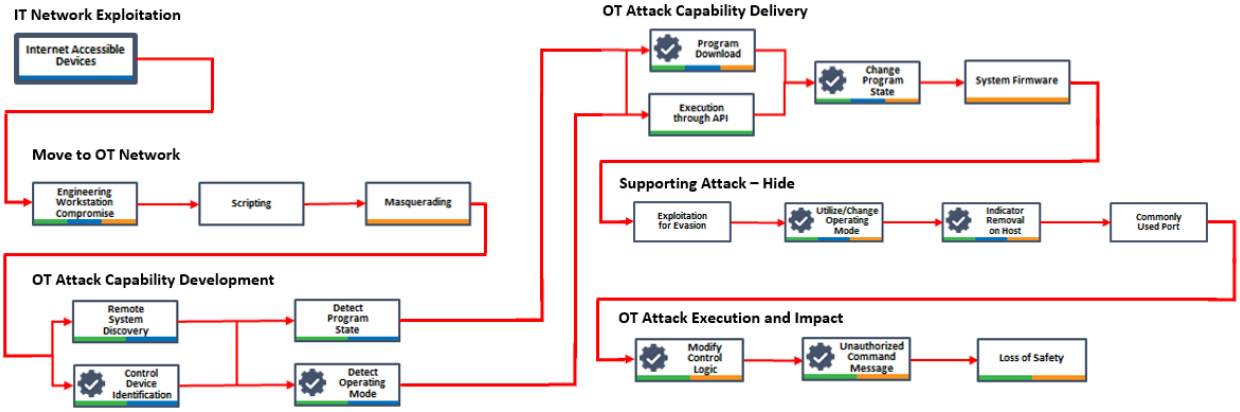

Figure 5: CyOTE Observables Link Diagram in Triton Case Study

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO OPERATING MODE CHANGES

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

[11] Refer to the CyOTE Case Study for full link diagram: CyOTE Case Study: Triton in Petro Rabigh, https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf

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.

DECISION: REMEDIATING THE CAUSE AND EFFECTS OF A TRIGGERING EVENT

The last step of the CyOTE methodology is the Decision step (Figure 6). 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.

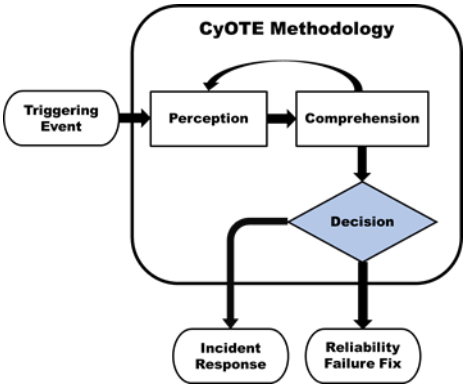

Figure 6: CyOTE Methodology - Decision Step

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 OPERATING MODE CHANGES

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
Network Segmentation	MITRE ATT&CK for ICS: M0930[12]	Used in conjunction, network segmentation, network traffic community deviation, and protocol metadata anomaly detection provide an exhaustive view into the network behaviors associated with the analysis of service stop commands. This group of controls does not exclusively include network data but can also include host-based application and operating system logs associated with the network traffic. • Leverage knowledge of the network environment to understand where industrial protocol messages should originate from to a given controller • Proper network segmentation provides functional boundaries where monitor and block actions can be implemented to prevent unauthorized changes to operation mode from unauthorized subnets • Understanding of program metadata for all protocols supported and enabled in your environment is critical for proper observation of changes to operating modes
Network Traffic Community Deviation	MITRE D3FEND™: D3-NTCD[13]	
Protocol Metadata Anomaly Detection	MITRE D3FEND: D3-PMAD[14]	
Network Allowlists	MITRE ATT&CK for ICS: M0807[15]	
Strong Password Policy	MITRE D3FEND: D3-SPP[16]	Strong passwords provide a line of defense against both insider threat and external threats. Strong passwords should be used on all endpoints in order to protect misuse of the applications capable of conducting operating mode changes. • Without a strong password policy, an attacker might use weak credentials to compromise an account and change the operating mode of a device remotely.

[12] MITRE, Network Segmentation, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0930.
[13] MITRE, Network Traffic Community Deviation, 2021. Available online: https://d3fend.mitre.org/technique/d3f:NetworkTrafficCommunityDeviation.
[14] MITRE, Protocol Metadata Anomaly Detection, 2021. Available online: https://d3fend.mitre.org/technique/d3f:ProtocolMetadataAnomalyDetection.
[15] MITRE, Network Allowlists, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0807.
[16] MITRE, Strong Password Policy, 2021. Available online: https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy.

Control	Matrix	Relevance
Audit	MITRE ATT&CK for ICS: M0947[17]	Account auditing validates the permissions of existing accounts and review of access logs. Proper account auditing provides a host-based baseline monitoring opportunity. • Identify and limit what roles are required for users on endpoints that regularly make operating mode changes • Ensure proper logging exists for attempts to act outside of a user's expected roles.
Privileged Account Management	MITRE ATT&CK for ICS: M0926[18]	
Local Account Monitoring	MITRE D3FEND: D3-LAM[19]	
Access Management	• MITRE ATT&CK for ICS: M0801[20] • NIST 800-53: SI-7(8)[21] • NIST 800-53: AC-2[22] • NIST-800-82: 6.2.3[23] • NIST-800-82: 6.2.17[24]	

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR OPERATING MODE CHANGES

The parameters and established triggers 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 using synthetic data (e.g., synthetic PCAPs)
        i. If the test fails, re-evaluate the steps taken iteratively (line by line)
        ii. If successful, enact a graduated deployment schedule and retest for each iteration
2. Consider communication criteria for multiple locations and information consolidation during graduated deployment
    a. Identify output destination(s) (SIEM, Splunk, Gravwell, Elk)
    b. Identify output format(s) (STIX, Syslog, JSON, CSV)
    c. Define actionable data requirements, processes, and responses
        i. Logging

[17] MITRE, Audit, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0947.
[18] MITRE, Privileged Account Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0926.
[19] MITRE, Local Account Monitoring, 2021. Available online: https://d3fend.mitre.org/technique/d3f:LocalAccountMonitoring.
[20] MITRE, Access Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0801.
[21] NIST, NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations,"2020, available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[22] Ibid.
[23] NIST, NIST Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security," 2015, available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
[24] Ibid.

ii. Alert content
iii. Alert response(s) (local or SOC)

3. Identify what information to log (long-term/short-term)
    a. Aggregating different log types may assist in identifying potentially anomalous behaviors within OT environments

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 Change Operating Mode 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 Change Operating Mode technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Change Operating Mode 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 Change Operating Mode technique came to be. A change in run state and a device that does not physically match the reported operating mode are both potential observables that could indicate the use of Change Operating Mode technique.

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 Change Operating Mode technique. This will allow them to more quickly identify triggering events using the Change Operating Mode 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 the information gathered, the AOO will be able to determine whether an anomalous operating mode change 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 change in operating mode (thus initiating corrective maintenance procedures).

Additional assistance regarding general sensor placement and capability development is available through DOE; contact CyOTE.Program@hq.doe.gov for more information. 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 T858: CHANGE OPERATING MODE

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 assists with identification of systems communicating operating mode changes and possibly detailed communication details
Device & System Configuration Files and Change History	• Sysinternals Suite • Engineering Workstation or HMI Software	• Network Security Team • IT or OT System Admins	Device & system configuration files and change history assist with root cause identification and timeline generation
Physical access logs and security monitoring data like CCTV output	Application Specific	Physical Security Team	Physical security logs and CCTV adds another factor of logging to identify hardware-based operating mode changes

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557