T872: INDICATOR REMOVAL ON HOST

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 Indicator Removal on Host attack technique for the Evasion and Impair Process Control 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 *Indicator Removal on Host (T872) Technique Detection Capability Sheet* for the Evasion and Impair Process Control tactics.[4]

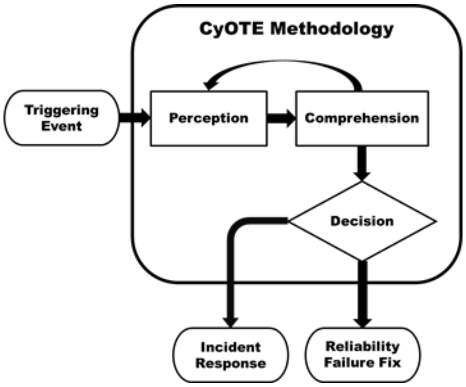

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

The Indicator Removal on Host technique masks the footprint of an attacker or an attacker's malware. As defined by the MITRE ATT&CK® for ICS framework, adversaries may attempt to remove indicators of their presence on a host to obfuscate movement and intentions using the Indicator Removal on Host technique. This technique allows adversaries to evade detection by covering their tracks. Indicator removal might include modifications to or deletion of system logs and changes to file system metadata (e.g., access times).

In cases where an adversary may perceive detection is imminent, they may attempt to overwrite, delete, or cover up changes to the host device using native functionality and/or additional open-source software. These changes may affect control system devices (e.g., human-machine interfaces [HMI], Protection Relays, and Safety Instrumented Systems [SIS]). This may result in an adversary removing critical process files as they cover their tracks, which could possibly impact operations and ongoing critical processes.[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, Indicator Removal on Host, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0872.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Indicator Removal on Host (T872) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Indicator Removal on Host, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0872.

PERCEPTION: IDENTIFYING ANOMALIES

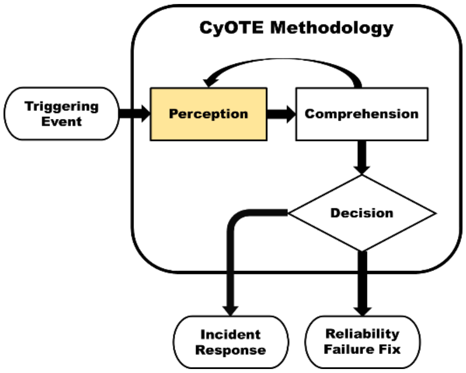

Figure 2: CyOTE Methodology – Perception Step

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 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 INDICATOR REMOVAL ON HOST 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 Indicator Removal on Host technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
● Log-cleared messages in event or system logs (e.g., Windows Event ID 1102) ● Results from automated malware analysis (Cuckoo Sandbox, Palo Alto WildFire, CrowdStrike Falcon Sandbox, VirusTotal, etc.) showing	Unexpected file deletion noticed by an operator or by other plant personnel	● File Metadata ● Application Logs ● Windows Event Logs (Standard) ● Windows Event Logs (Enhanced)

[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
removal or editing of logs		
• System and application logs often contain logs or watchdog monitors for critical files. Changelogs might contain signs of indicator removal actions. • Unexpected changes to log file size, or a checksum value indicates file and configuration changes. This metadata might also contain user metadata to assist with further analysis.	Unexpected file and configuration changes noticed by an operator or by other plant personnel	• File Metadata • Application Logs • Windows Event Logs (Standard) • Windows Event Logs (Enhanced)
• Operating system logs might contain events associated with reads or writes to log files and include the user who initiated the event. • File and system metadata might also contain unusual or unexpected user information	Attempts to read, write log files from an unprivileged account(s)	• File Metadata • Application Logs • Windows Event Logs (Standard) • Windows Event Logs (Enhanced)
Some devices report the number of programs written in industrial applications or via industrial protocols. A controller's program counter increasing then decreasing might be one sign of indicator removal.	Increment then decrement of PLC program counter	• Application Logs • Raw Network Data (Captured) • Raw Network Data (Live)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS INDICATOR REMOVAL ON HOST

Asset owners and operators desiring to develop and implement the Indicator Removal on Host technique capability should consider a phased approach to development to include continuous testing and evaluation of the capability throughout its lifecycle. 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 capability development phase, secure coding practices should be employed.[8]

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

1. Identify devices and protocols to monitor which can implement access control policies
2. Identify existing host-based access controls
3. Implement host-based access controls, limiting the number of authorized change users
    a. E.g., execute applications, write to application .exe files and dependencies, write to log files, write changes to system memory, start/stop services
    b. Recommend enforcing least privilege
4. Identify tap points (sensors) for observing identified devices
    a. This may include engineering workstations, servers, switches, security appliances, and logging locations (hosts)
    b. Plan sensor placement based on locations within the architecture that provide context related to the anomaly and prioritize systems at greater risk
    c. Recommend establishing capture requirements for monitoring OT locations[9,10]
        i. Storage (how much and for how long)
        ii. Data size (e.g., 1 Kb/10 Mb/40 Gb)
        iii. Central vs. 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.

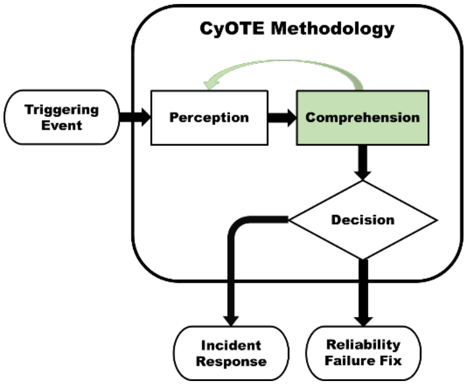

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATED TO INDICATOR REMOVAL ON HOST

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

[9] CESER, Security Monitoring Best Practices, CyOTE Program, Department of Energy, 2021
[10] CESER, Lessons Learned, CyOTE Program, Department of Energy, 2021, available online, https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf.

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 Indicator Removal on Host

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.
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 ENABLING REMOTE LOG COLLECTION AND REMOTE SYSTEM PROCESS MONITORING FOR ANALYSIS OF INDICATOR REMOVAL ON HOSTS

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

Enable logging on devices, including:

- Security logs
- Access logs with timestamps on endpoints
- Error logs
- Syslog message logs (if supported)
- Host logs
- Firewall logs
- Device identifier (will vary based on environment)
    - Host name
    - Source and destination IP addresses
    - MAC addresses

If required by SIEM, install remote agents on endpoints and enable remote system process monitoring with timestamps on endpoints for the following:

- System logging
- Metric logging
- Service logging

Install additional remote agents as necessary.

STEPS FOR ANALYZING EXTRACTED FIELDS FROM LOGS AND IDENTIFYING FIELD-LEVEL ANOMALIES FOR INDICATOR REMOVAL ON HOST

The suggested fields above are applied to data analysis and assist in establishing 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 are given greater precedence for analysis and correlation with other observables to identify potentially anomalous/malicious messages.

1. Identify host devices to alert on
    a. Document indicator 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
            1. E.g., whether the modification is from an authorized user
2. Identify 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 anomalies

   a. E.g., changes to access/security logs, log file deletion, timeout value between log collections, process start/stop/restart, file creation/modification, event logs
   b. Incorporate the analysis findings provided in the remote log collection and remote system process monitoring and implement to refine alert parameters
      i. Use this analysis to focus on useful information and minimize the number of non-useful alerts

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 Indicator Removal on Host

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
An unexpected change to log content associated with a system or application	The team responsible for process or network resource	1 day	● Identify if this trigger event occurred due to a known and expected change ● Identify the presence of malicious behavior on the host
The disappearance of individual debug data sources or a loss of aggregate analytic output related to security events or overall environment events	Team or teams responsible for managing assets associated with data sources	1 day	● Work with other teams to identify the source of the data loss ● Assess further actions needed to compensate for the loss of situational awareness

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 might produce digital footprints like logs and errors – if those are not present, this could indicate that an adversary is removing these indicators. This might also 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 in the comprehension stage, depends on the situation; typically, it will inform many of the context-building questions outlined in the following section.

Technical analysis should begin with identification of the root cause for the disappearance of the indicator. Understanding the logging architecture and any associated safeguards assists with identification of potential log sources. The analysis should then validate the integrity of the safeguards and identify any deviations from expected behavior.

Context-Building Questions

A root cause analysis for suspected indicator removal on a host should focus on expected retention and granularity of indicators on a host. Understanding the baseline behaviors as well as the impact of any configuration changes assists with identification of unexpected or malicious events. Consider the following questions:

- What circumstances generate an indicator?
- Where does the indicator log to and what are the storage limitations?

- Does the indicator use a rollover buffer or another first-in-first-out data structure where rollover is expected?
- What access or change restrictions might be associated with a given indicator?
- Did a system or application change recently occur that might account for indicator changes on a system?
- What other indicators exist that might serve as a canary for unexpected or unauthorized changes?
- How might an attacker modify an indicator, and what associated detection opportunities exist for each attack path?

Once the 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 trigger event. Proving or disproving the trigger event hypotheses will support the decision-making process by validating initial perceptions and reducing initial cognitive biases.

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.

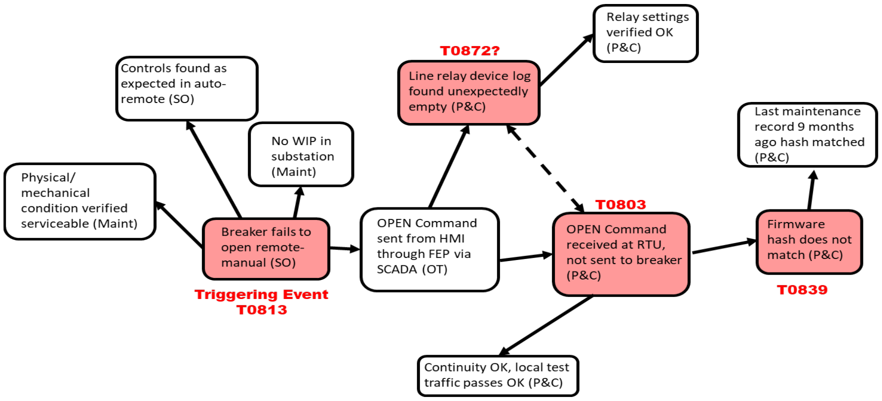
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
No WIP in substation (Maint)
Last maintenance record 9 months ago hash matched (P&C)
Physical/ mechanical condition verified serviceable (Maint)
Breaker fails to open remote-manual (SO)
Triggering Event T0813
OPEN Command sent from HMI through FEP via SCADA (OT)
T0803
OPEN Command received at RTU, not sent to breaker (P&C)
Firmware hash does not match (P&C)
T0839
Continuity OK, local test traffic passes OK (P&C)

Figure 4: Example CyOTE Observables Link Diagram

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

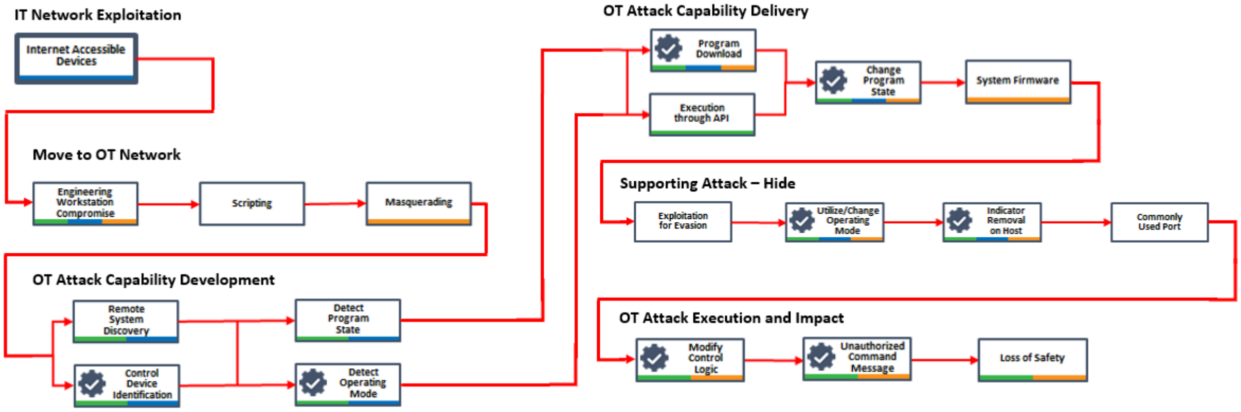

Figure 5: CyOTE Observables Link Diagram in Triton Case Study

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO INDICATOR REMOVAL ON HOST

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] 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

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.

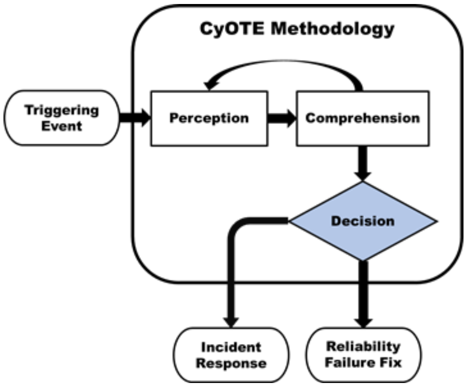

Figure 6: CyOTE Methodology - Decision Step

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 to a situation. 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 potential anomalies.

CONTROL MATRIX

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
Strong Password Policy	MITRE D3FEND: D3-SPP[12]	Strong passwords provide a line of defense against both insider threat and external threats. Without a strong password policy, an attacker might use weak credentials to compromise an account and remove indicators. ● If identification of a weak password occurs, audit the history of actions associated with the account to determine if the weak password was used to remove indicators.
File Access Pattern Analysis	MITRE D3FEND: D3-FAPA[13]	File access pattern analysis allows detection of anomalies associated with an attacker covering their tracks. This might include file deletions or modifications to erase indicators or file additions to manipulate system configurations. ● Building user patterns for file creation, access, and modification might provide an opportunity for a host data baseline. ● While an attacker might outright delete a file, make sure to also look for file creation or modification that changes the logging configuration of a device.
Emulated File Analysis	MITRE D3FEND: D3-EFA[14]	Emulated file analysis allows AOOs to detect indicator deletion on non-production systems. This security control might provide early warning of an attack going on or assist with an active investigation after the event occurs. ● Deploy honeypots that emulate similar file structures to production systems. Monitor for attempts to overwrite or remove indicators on the honeypot.
System File Analysis	MITRE D3FEND: D3-SFA[15]	Analysis of system files might yield proof of malicious tampering that caused or was associated with indicator removal from a host. System file analysis includes monitoring of databases, registry keys, logs, and executables. ● Monitor for file system metadata changes as well as changes to data within files. ● Reconfiguration or unexpected changes of Windows registry keys might also indicate a change to application or

[12] MITRE, Strong Password Policy, 2021. Available online: https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy.
[13] MITRE, File Access Pattern Analysis, 2021. Available online: https://d3fend.mitre.org/technique/d3f:FileAccessPatternAnalysis.
[14] MITRE, Emulated File Analysis, 2021. Available online: https://d3fend.mitre.org/technique/d3f:EmulatedFileAnalysis.
[15] MITRE, System File Analysis, 2021. Available online: https://d3fend.mitre.org/technique/d3f:SystemFileAnalysis.

Control	Matrix	Relevance
		file system logging or metadata.

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR INDICATOR REMOVAL ON HOST

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 anomalies 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., logs, WMI)
      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) (SIEM, Splunk, Gravwell, Elk)
   a. Identify output format(s) (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

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 Indicator Removal on Host 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 Indicator Removal on Host technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Indicator Removal on Host 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 Indicator Removal on Host technique came to be. Edited or removed application logs (and indications of this action in changelogs), unexpected changes in log file size, unrecognized or unauthorized users changing log information, and program counters increasing then decreasing are all potential observables that could indicate the use of the Indicator Removal on Host technique. Anomalies tied to these observables could be unexpected file deletion or changes or attempts to read or write log files from unauthorized accounts.

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 Indicator Removal on Host technique. This will allow them to more quickly identify triggering events using the Indicator Removal on Host 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 indicator removal 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 indicator removal (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 T872: INDICATOR REMOVAL ON HOST

Table 5: Datasets to Assist with Analyzing Triggering Events

Dataset	Example Tools	Who Can Assist	Relevance
Device & System Logs	● SysInternals SysMon ● SysInternals PsLogList ● EvtxToElk ● Python-evtx ● OSQuery	● Network Security Team ● IT or OT System Admins	Some device and system logs include events
Device & System Configuration Files and Change History	SysInternals Suite	● Network Security Team ● IT or OT System Admins	Device & system configuration files and change history assists with identification of systems communicating and possibly detailed communication details
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 document and logs assists with identification of systems communicating and possibly detailed communication details
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 identification of other log sources to assist in indicator removal investigations
Any other data relevant to the investigation	Various	● Network Security Team ● IT or OT System Admins ● OEMs/Third-Party Vendors	Other data sources associated with service stop commands might contain

Dataset	Example Tools	Who Can Assist	Relevance
			information specific to a given trigger event

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