T881: SERVICE STOP

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 Service Stop 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 *Service Stop (T881) Technique Detection Capability Sheet* for the Inhibit Response Function tactic.[4]

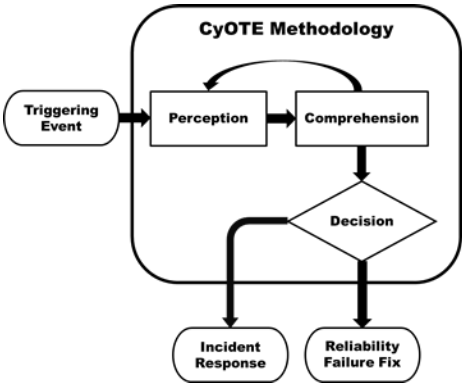

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, adversaries may use the Service Stop technique to “disable or stop services on a system, rendering them unavailable to legitimate users. Stopping critical services can inhibit or stop response to an incident or aid the adversary in achieving their overall objectives.”[5] This technique allows adversaries to target any system or server running daemons or processes to disrupt a service or obfuscate malicious actions. Critical services might be related to operating system services or services resident in industrial protocols. Services resident to an industrial protocol include services within the Common Industrial Protocol (CIP), such as the connection manager.

[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, Service Stop, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0881.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Service Stop (T881) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Service Stop, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0881.

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" 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]

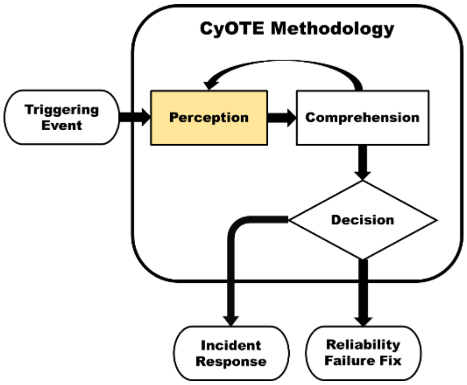

Figure 2: CyOTE Methodology – Perception Step

EXAMPLE OBSERVABLES AND ANOMALIES OF THE SERVICE STOP 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 Service Stop technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
If enabled, Microsoft Sysinternals's sysmon utility event IDs 5, 7, and 8 indicate process crash and exit events	A process associated with a critical service crashed unexpectedly	• Windows Event Logs (Enhanced) • Application Logs
• If enabled, Microsoft Sysinternals's Sysmon utility event IDs 12, 13, and 14 track changes to registry keys	A process associated with a critical service is disabled or deleted	• Windows Event Logs (Enhanced) • Application Logs

[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
• Operating system or application logs that include changes to service statuses • File deletion metadata • Usernames and time of action		
• Required resource availability • An unexpected or unexplained increase in TCP resets on the application server	A process crashes due to changes in the availability of local or remote external application dependencies	• Raw Network Data (Captured) • Raw Network Data (Live)
• Service stop commands from unexpected sources or different trust boundaries • Service stop commands at atypical times	A service stops due to valid service stop command issuance over the network	• Raw Network Data (Captured) • Raw Network Data (Live)
• Service stop commands in network traffic to nonexistent or non-supported devices from compromised hosts • Operators might also observe an increase in exceptions reported by industrial assets due to industrial devise rejecting the communication	Service stop commands issued to unusual devices	• Raw Network Data (Captured) • Raw Network Data (Live)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS SERVICE STOPS

Asset owners and operators aiming to detect potential capabilities to monitor for use of the Service Stop 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 what devices and services to monitor for service stop
   a. Devices running Linux kernel 4.4 and newer
   b. E.g., protective relays, RTUs/automation controllers, HMIs, computers
2. Identify potential triggers

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

a. Software service stops
b. Unexpected crashes
c. Zombie services
d. Unresponsive services
e. Watchdog fails to restart service

COMPREHENSION: ANALYZING TRIGGERS AND THEIR CONTEXT

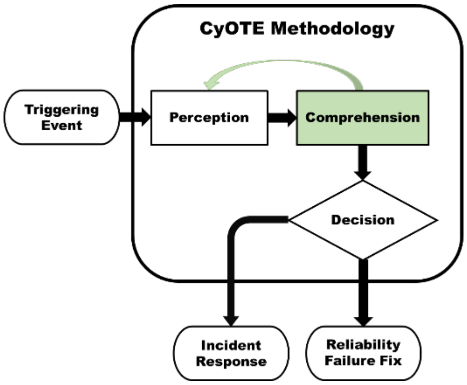

Figure 3: CyOTE Methodology - Comprehension Step

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.

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO SERVICE STOP

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 Service Stops

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.

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 IDENTIFYING AND EXTRACTING INFORMATION FROM OT NETWORK TRAFFIC FOR ANALYSIS OF SERVICE STOPS

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.

1. Prioritize extracted information based on importance
    a. Establish timelines for capturing and holding information for analysis and review
2. Define information reporting from the host
    a. Define reporting location and process
    b. Define reporting message content
    c. Define reporting alert criteria
3. Suggested data fields to collect include:
    a. Timestamp
    b. Username for process initiation
    c. Device identifier
        i. Hostname
    d. Process identification
    e. Command(s) used to start process
    f. Process tree

   g. Process exit value (code)
   h. Process run time

STEPS FOR ANALYZING EXTRACTED FIELDS AND IDENTIFYING FIELD-LEVEL ANOMALIES FOR SERVICE STOPS

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 downloads.

1. Identify service logs of interest to alert on
   a. Document triggers based on host
      i. Identify the service stop exit code
      ii. Include the frequency and type of service(s) operating
   b. Identify the magnitude of the physical process controlled by the service
      i. Determine if the alert is valid or invalid based on analysis of host system
      ii. E.g., legitimate reasons for service stopping or reset
2. Identify process stopping or restarting from new or abnormal hosts
   a. Analyze host lists for commands issued to end device(s)
   b. Conduct a comparative analysis to identify new connections and alerts vs. older ones
   c. Messages executing commands at an abnormal frequency
      i. Track messages and perform statistical and/or procedural tests
      ii. E.g., frequency, order, type, messaging timing

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 Service Stops

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Unexpected service stop on asset managed by another IT/OT team related to an application	Team responsible for process or network resource	• 1 hour (critical application) • 48 business hours (non-critical application)	Collaborative troubleshooting should occur to identify and remediate the root cause
Incompatible change to vendor-supported baseline	• Support vendors • Network security team	• 1 hour (critical application) • 48 business hours (non-critical application)	• Validate if the change or account access correlates with known activity or scheduled vendor service events • Validate vendor access controls like time limits on interactive sessions
Service stop command issued across network trust boundary	• Network security team • Team responsible for network resource	48 business hours (non-critical application)	Identify source host

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, a service that is stopped unexpectedly 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). Attacks using the Service Stop technique might cover a variety of scenarios. In one situation, an attacker might leverage valid network protocols to stop or disable a service on a remote host. In other scenarios, a service might stop due to the deliberate or unintentional actions of a user or external system. Technical analysis will depend on the situation that caused the service to stop.

Technical analysis should focus on the log sources particular to your situation. For suspected user-driven action in a windows domain, the windows event logs might hold diagnostic information for determining the root cause of the event. If a safety system or other network device issued valid service stop commands, passive network analysis might show the network transmissions responsible for the service state change. For service stop commands issued across network boundaries monitored by network traffic summarization, the technical analysis might also include network communication metadata to identify external systems and assets talking to industrial devices.

Context Building Questions

Root cause analysis for an unexpected service stop should begin with the application associated with the stopped service itself and secondary applications that interact with a given application. Due to the variety of services in industrial environments, the analysis might need first to identify applications and systems that directly interact with the stopped service. Consider the following questions to assist with the identification of related applications:

- Do you have the ability to access the endpoint or device with the service that stopped? If so, can you log in to triage logs and other application data related to the event in question?
- What other applications on the same host interact with the service that crashed? What other hosts and endpoints on the network interact with the service that stopped? Do any of those applications contain logs that might indicate the timeline or reasons for the crash? What service or user accounts may be involved, and can they access other systems?

The existence of a service stop itself isn’t suspicious; however, unusual or unexpected service stops might indicate nefarious activity. Further context development questions should focus on splitting known good behavior from any deviations from this known good.

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.

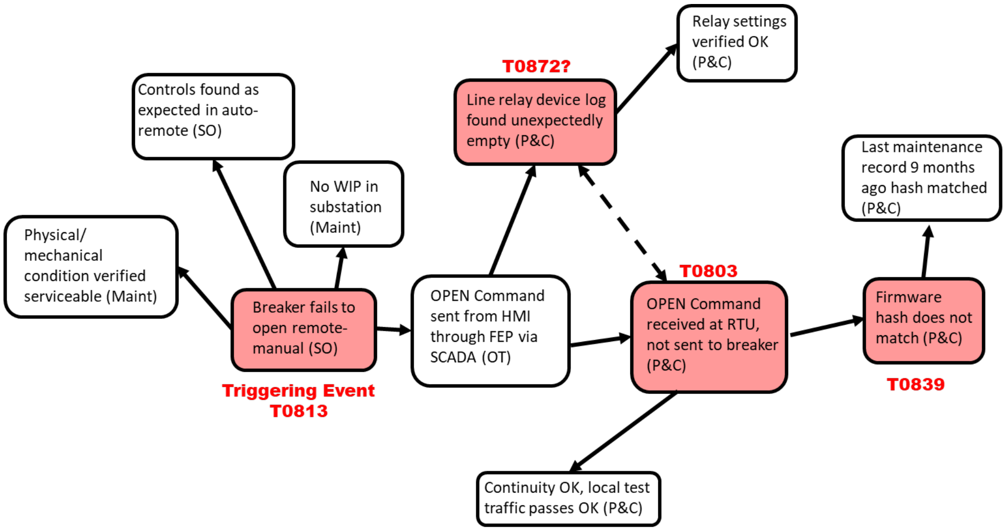
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
Last maintenance record 9 months ago hash matched (P&C)
No WIP in substation (Maint)
Physical/ mechanical condition verified serviceable (Maint)
T0803
Breaker fails to open remote-manual (SO)
OPEN Command sent from HMI through FEP via SCADA (OT)
OPEN Command received at RTU, not sent to breaker (P&C)
Firmware hash does not match (P&C)
Triggering Event
T0813
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 Service Stop technique in the 2017 Triton attack on the Petro Rabigh refinery complex in Rabigh, Saudi Arabia is shown in Figure 5.[9]

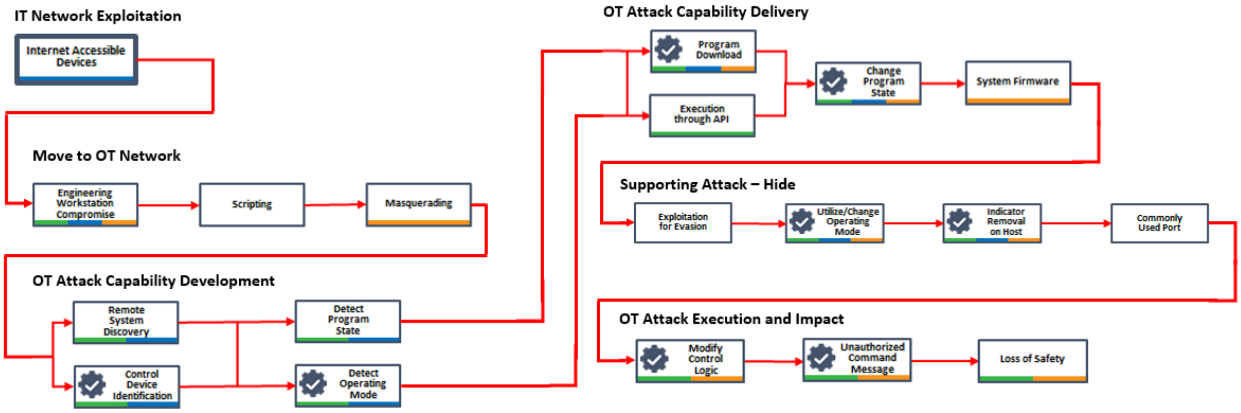

Figure 5: CyOTE Observables Link Diagram in Triton Case Study

[9] 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

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO SERVICE STOPS

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.

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.

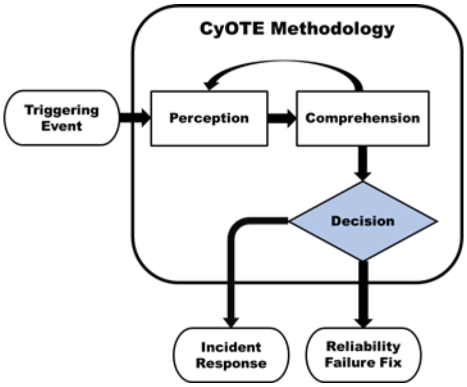

Figure 6: CyOTE Methodology - Decision Step

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 SERVICE STOPS

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[10]	Used in conjunction, network segmentation, network traffic community deviation, protocol metadata anomaly detection, and client-server payload profiling provide a detailed 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 have host-based application and operating system logs related to the network traffic. • Understand the statistical baseline for network traffic within your environment might provide the opportunity to detect report message spoofing. • Possible deviation calculation points include the high-level communications summary or the specific function code or operation within a given protocol.
Network Traffic Community Deviation	MITRE D3FEND™: D3-NTCD[11]	
Protocol Metadata Anomaly Detection	MITRE D3FEND: D3-PMAD[12]	
Client-server Payload Profiling	MITRE D3FEND: D3-CSPP[13]	
Strong Password Policy	MITRE D3FEND: D3-SPP[14]	Strong passwords provide a line of defense against both insider threats and external threats. • Without a strong password policy, an attacker might use weak credentials to stop a service manually. • Attackers might also use weak passwords to leverage industrial control system applications that natively issue stop commands to issue the stop command.

[10] MITRE, Network Segmentation, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0930.

[11] MITRE, Network Traffic Community Deviation, 2021. Available online: https://d3fend.mitre.org/technique/d3f:NetworkTrafficCommunityDeviation.

[12] MITRE, Protocol Metadata Anomaly Detection, 2021. Available online: https://d3fend.mitre.org/technique/d3f:ProtocolMetadataAnomalyDetection.

[13] MITRE, Client-server Payload Profiling, 2021. Available online: https://d3fend.mitre.org/technique/d3f:Client-serverPayloadProfiling.

[14] MITRE, Strong Password Policy, 2021. Available online: https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy.

Control	Matrix	Relevance
Multi-Factor Authentication	- MITRE D3FEND: D3-MFA[15] - NIST 800-53: IA-5[16] - NIST 800-82: 6.2.7.3[17] - NIST 800-82: 6.2.7.4[18] - NIST 800-82: 6.2.7.5[19]	Multi-factor authentication can protect an endpoint against host-originated attacks by further limiting access by non-sophisticated attackers. - Employ multi-factor authentication on boundary hosts (jump boxes) and any other supporting endpoints. - Multi-factor authentication provides another layer of defense to prevent unauthorized users from issuing service stop commands.
- Audit - Privileged Account Management - Local Account Monitoring	- MITRE ATT&CK for ICS: M0947[20] - MITRE ATT&CK for ICS: M0926[21] - MITRE D3FEND: D3-LAM[22] - NIST 800-53: SI-7(8)[23] - NIST 800-53: AC-2[24] - NIST 800-82: 6.2.3[25] - NIST 800-82: 6.2.17[26]	Account auditing validates the permissions of existing accounts and reviews access logs. Proper account auditing provides a host-based baseline monitoring opportunity. - Conduct system audits regularly to validate existing controls and identify opportunities to implement new controls. - Limit user, service, and system account access to only essential systems and resources.
Decoy Network Resource	MITRE D3FEND: D3-DNR[27]	Decoy network resources provide early warning for suspicious actions. Unlike production systems, the average baseline on decoy systems contains a lower noise volume than production systems. - Decoy network resources serve as a honeypot that might receive service stop requests from attackers with low situational awareness of the environment.

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR SERVICE STOPS

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).

[15] MITRE, Multi-Factor Authentication, 2021. Available online: https://d3fend.mitre.org/technique/d3f:Multi-factorAuthentication.

[16] 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.

[17] 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.

[18] Ibid.

[19] Ibid.

[20] MITRE, Audit, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0947.

[21] MITRE, Privileged Account Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0926.

[22] MITRE, Local Account Monitoring, 2021. Available online: https://d3fend.mitre.org/technique/d3f:LocalAccountMonitoring.

[23] 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.

[24] Ibid.

[25] 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.

[26] Ibid.

[27] MITRE, Decoy Network Resource, 2021. Available online: https://d3fend.mitre.org/technique/d3f:DecoyNetworkResource.

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 a test host to perform validation
        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 Service Stop 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 Service Stop technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Service Stop 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 Service Stop technique came to be. Processes associated with critical services crashing unexpectedly or being disabled or deleted are all potential observables that could indicate the use of Service Stop technique. Anomalies tied to these observables could be changes to system or application logs, file deletion, or process crash IDs.

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 Service Stop technique. This will allow them to more quickly identify triggering events using the Service Stop 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 service stop 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 service stop (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 T881: SERVICE STOP

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 and possibly detailed communication details
Device & System Logs	• SysInternals SysMon • SysInternals PsLogList • EvtxToElk • Python-evtx • OSQuery	• Network Security Team • IT or OT System Admins	Device & system log data assists with identification of systems communicating and possibly detailed communication details
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

Dataset	Example Tools	Who Can Assist	Relevance
Physical access logs and security monitoring data like CCTV output	Application Specific	Physical Security Team	Physical security logs and CCTV adds another factor of validation to assist with validation of true source
System engineering documents like network layouts and other schematics or diagrams	Diagram Specific	• Network Security Team • IT or OT System Admins • OEMs/Third-Party Vendors	Environment documentation assists with 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 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/Third-Party Vendors	Other data sources might contain 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