T856: SPOOF REPORTING MESSAGE

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 Spoof Reporting Message 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 *Spoof Reporting Message (T856) Technique Detection Capability Sheet* for the Evasion and Impair Process Control tactics.[4]

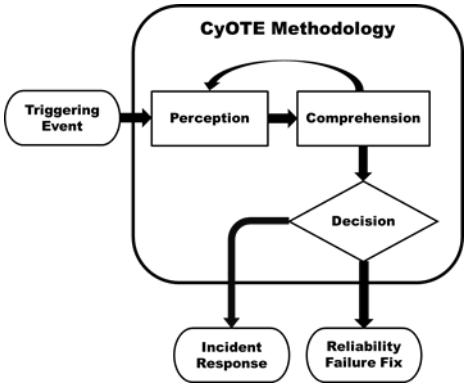

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

Spoofing reporting messages involves the creation of false report messages to deceive both operators and systems about the industrial environment's true operational state. As defined by the MITRE ATT&CK® for ICS framework, adversaries may use the Spoof Reporting Message technique to evade and/or impair process control in control system environments by sending false information concerning the process state or to divert defensive resources away from the actual problem source.[5] Fraudulent report messages might result in an operator or autonomous system incorrectly making or not making a decision due to the lack of situational awareness about the true state of the process. This may result in damage to OT process interdependencies and equipment, as well as potential harm to personnel. Report message spoofing can occur if an application's receiving network stack is modified to accept malicious injected packets at a point in the network or at a host. Under most circumstances, this technique would be secondary to others and may be used for potential incident correlation.

[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, Spoof Reporting Message, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0856.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Spoof Reporting Message (T856) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Spoof Reporting Message, 2021. Available online https://collaborate.mitre.org/attackics/index.php/Technique/T0856.

PERCEPTION: IDENTIFYING ANOMALIES

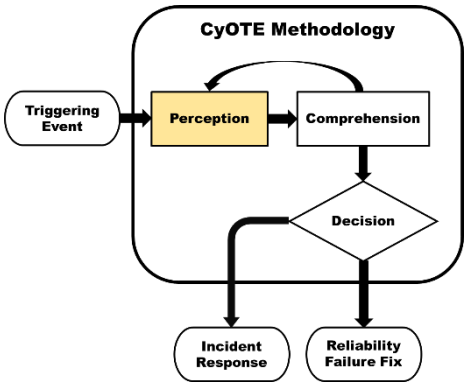

Figure 2: CyOTE Methodology - Perception Step

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 SPOOF REPORTING MESSAGE 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 Spoof Reporting Message technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
For observable protocols, network traffic analysis might provide visibility into a network-based attack.	Reporting message from unauthorized/unexpected source asset	• Raw Network Data (Captured) • Raw Network Data (Live)
Stuxnet renamed the legitimate communication dynamic link library (DLL) and added a second DLL to hook	Unexpected change in host communication driver	• 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
communications. Host-based monitoring or manual integrity checks of application integrity might note changes to communication drivers on a host.		
A single device or small number of devices showing a wider clock drift	Process time issue (wrong timestamp, sequence number, or other metadata) observed in communication or logged on an endpoint	• Raw Network Data (Captured) • Raw Network Data (Live)
• An increase in industrial protocol communication errors due to the destination asset not accepting the packet • An increase in transmission control protocol (TCP) resets or other core protocol errors	Increase in error messages associated with rejected packets	• Raw Network Data (Captured) • Raw Network Data (Live)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL SPOOFED REPORTING MESSAGES

Asset owners and operators aiming to monitor for use of the Spoof Reporting Message 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 critical and secondary process systems and data points to monitor for spoofed reporting messages
    a. Identify critical components
    b. Identify potentially susceptible components or communication paths (e.g., protective relays and remote terminal units [RTU]/automation controllers)
2. Identify the capability location and when it will operate
    a. Example capability locations: from firewall, integrated host, server, IDS/IPS, other
    b. Example operating timeframes: at startup, real-time, daily, weekly
3. Identify tap points (sensors) for observing device traffic for identified devices and systems

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

a. This may include servers, switches, security appliances, and logging locations (hosts)
    i. Plan sensor placement based on locations within the architecture that provide context related to the anomaly and prioritize systems at greater risk
b. Identify the existing network connections (e.g., ethernet, fiber, serial, Wi-Fi, RF, broadcast domains)
    i. Depending on the environment, serial device servers may be needed to convert between multiple different protocols
c. Establish passive network taps
    i. Monitoring and traffic aggregation may necessitate tap placement on both sides of the identified devices (e.g., MAC addresses may change as information traverses networking infrastructure like protocol converters)
d. Recommend establishing capture requirements for monitoring OT traffic and their locations[9, 10]
    i. Storage (how much and for how long)
    ii. Line rate (e.g., 1/10/40/100 Gb)
    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.

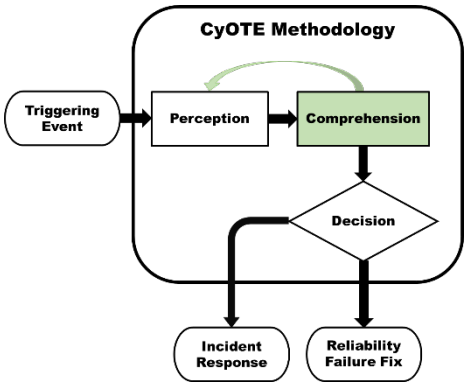

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO SPOOF REPORTING MESSAGE

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, 2021.
[10] CESER, Lessons Learned, CyOTE Program, Department of Energy, 2021.

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 Spoof Reporting Message

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 IDENTIFYING AND EXTRACTING INFORMATION FROM OT NETWORK TRAFFIC FOR ANALYSIS OF SPOOF REPORTING MESSAGE

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, with timelines established for capturing and holding information for analysis and review.

Suggested data fields to collect include:

- Timestamp

- Device Identifier (will vary based on environment)
  - Source and destination IP addresses
  - Source and destination ports
  - MAC addresses
- Message type
- Message frame (e.g., bytes)

STEPS FOR ANALYZING EXTRACTED FIELDS AND IDENTIFYING OBSERVABLES WITHIN MESSAGES THAT INDICATE SPOOFED REPORTING MESSAGES

The suggested fields above are applied to data analysis and assist in establishing triggers. 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 potential triggers to identify potentially anomalous/malicious messages.

1. Compare data points from independent and main communication channels for message manipulation
2. Analyze data captures
   a. Correlate data from sensors to monitor communicating devices
3. Establish protocol stack element validation
   a. E.g., digital signatures, allowed MAC addresses, IP addresses
   b. Latency in solicited or unsolicited message responses (e.g., man in the middle [MITM], proxy connections)
4. Identify baseline for average latency of transmitted/received packets
   a. Establish alerts for increase/decrease outside of parameters
5. Establish triggers
   a. Incorporate the analytical findings provided by observation and identification and establish alert parameters

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 Spoof Reporting Message

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Unexpected change in host communication driver on mission-critical system	Internal or external team responsible for process or network resource	1 hour	Collaborative troubleshooting should occur to identify and remediate the root cause
Unexpected service stop command sent from external IT asset to OT asset	IT security team responsible for originating asset	1 hour	• Collaborative troubleshooting should occur to identify and remediate the root cause • Identify if IT asset is compromised
Time-critical device transmitting incorrect timestamp	IT or OT team responsible for originating asset	1 business hour	• Collaborative troubleshooting should occur to identify and remediate the root cause • Resolve time issue to minimize operational impact
Non-time-critical device transmitting incorrect timestamp	IT or OT team responsible for originating asset	48 business hours	• Collaborative troubleshooting should occur to identify and remediate the root cause • Resolve time issue to minimize operational impact

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 that is the result of a spoofed reporting message might produce digital footprints like logs and errors. It might correspond to data loss, unauthorized configuration changes, elevated user permissions, or account activity at unusual hours.

Technical Analysis

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

The use of reporting messages will vary depending on the devices in an environment, including vendor make and model and device configuration. In some environments, industrial protocol analysis might provide one analytic lens to understand host and network behavior. Other environments might use proprietary or encrypted traffic, limiting the ability to perform protocol analysis. Analyzing host data can be another method to analyze spoofed reporting messages. Understanding the application components that transmit report messages and developing the capability to validate integrity of communication components enable technical analysis to prove or disprove message manipulation.

Context-Building Questions

A root cause analysis for suspected report message spoofing should begin with analysis of the hosts suspected to be involved in the message spoofing. Due to the variety of services in industrial environments, analysis might need to first identify applications and systems that produce and consume report messages. Consider the following questions:

- Did the spoofed report message originate from an asset within an internal network segment? Was any packet spoofing used and/or does the source host information seem valid? The spoofed reporting message might be spoofed with a low-level socket or packet-crafting library (e.g., Python's Scapy library), and it is important to rule this situation out to understand potential data sources of interest.

- Did the spoofed reporting message originate from a host typically associated with the protocol used, and were the specific operations or function codes within the protocol expected between the source and destination hosts? You might also model the frequency of communication to check for unexplainable statistical anomalies.

- Do you have access to the source host responsible for sending the spoofed reporting messages? Are any artifacts present to assess the integrity of the application associated with the generation of the report message? In the case of Stuxnet, a second Windows dynamic linked library (DLL) was

added to modify report messages on the host. An attacker might conduct a similar attack to "hook" report message generation.

Context building for spoofed report messages should uncover the reason(s) a spoofed message was transmitted. Because there are multiple places a spoofed message can originate from, it is important to use network and host data to isolate the portion of the network and specific host responsible for the traffic. This context might also assist in uncovering a wider intrusion into the environment.

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.

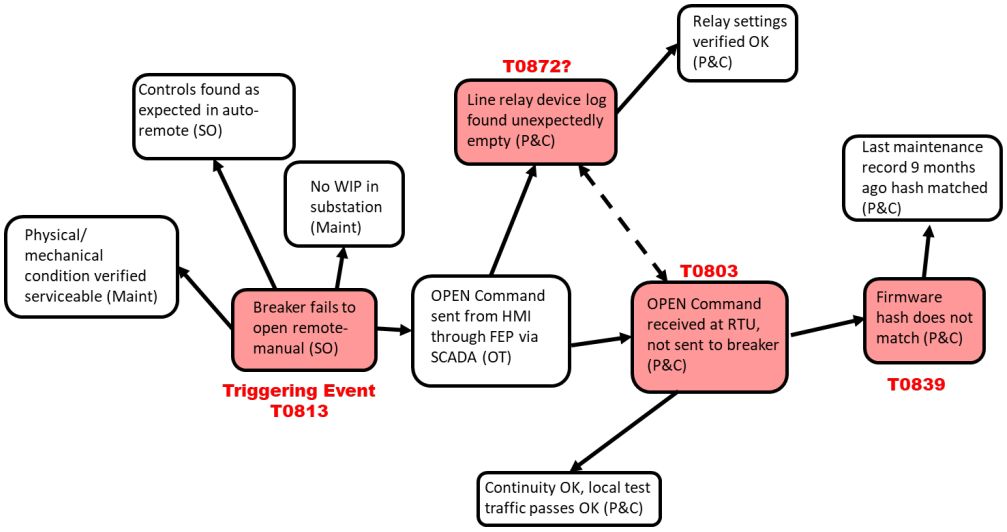

Figure 4: Example CyOTE Observables Link Diagram

INVESTIGATE POTENTIALLY RELATED ANOMALIES

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

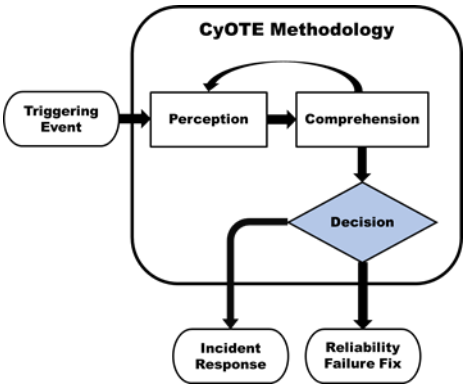

Figure 5: CyOTE Methodology - Decision Step

INCIDENT RESPONSE

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

CORRECTIVE MAINTENANCE

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

IMPROVING SECURITY CAPABILITIES

Prevention and preparation include proactive measures to reduce the risk or likelihood of an attack or enable an organization to respond more rapidly 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 potentially anomalous triggers.

CONTROL MATRIX FOR SPOOF REPORTING MESSAGE

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 Traffic Community Deviation	MITRE D3FEND: D3-NTCD[11]	Network traffic community deviation and protocol metadata anomaly detection consider the metadata and contents of traffic transiting the network. Spoofed reporting messages might contain anomalous metadata when compared to good traffic or other traffic features that can be detected. • Understand the statistical baseline for network traffic within your environment. • Deviations might be calculated on the high-level communications summary or the specific function code or operation within a given protocol. • Protocol metadata anomalies might include a spite in error messages due to applications rejecting the spoofed messages.
Protocol Metadata Anomaly Detection	MITRE D3FEND: D3-PMAD[12]	
Audit	MITRE ICS ATT&CK: M0947[13]	Audits, privileged account management, and local account monitoring assist with endpoint-based detection and prevention of spoofed reporting messages. Organizations should employ the principles of least privilege to limit who can reconfigure a given system or gain the level of authentication needed to generate spoofed traffic. • Conduct system audits on a regular basis to validate existing controls and identify opportunities to implement new controls. • Limit user, service and system account access to only essential systems and resources.
Privileged Account Management	MITRE ICS ATT&CK: M0926[14]	
Local Account Monitoring	MITRE D3FEND: D3-LAM[15]	

[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, Audit, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0947.
[14] MITRE, Privileged Account Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0926.
[15] MITRE, Local Account Monitoring, 2021. Available online: https://d3fend.mitre.org/technique/d3f:LocalAccountMonitoring.

Control	Matrix	Relevance
Operating System Monitoring	MITRE D3FEND: D3-OSM[16]	Operating system monitoring, system file analysis, and service binary verification all validate the integrity of the application level and operating system level code responsible for message generation. Previous attacks leveraged changes to dynamically linked libraries to spoof reporting messages. • Operating system and file analysis should focus on integrity of critical system services as well as application files associated with core functionality. • For spoofed reporting message prevention, binaries and libraries associated with report message spoofing and the network stack of the OS should be secured and monitored for signs of tampering.
System File Analysis	MITRE D3FEND: D3-SFA[17]	
Service Binary Verification	MITRE D3FEND: D3-SBV[18]	
Software Process and Device Authentication	MITRE ICS ATT&CK: M0813[19]	
Inbound Traffic Filtering	MITRE D3FEND: D3-ITF[20]	Network segmentation divides your network into sections based on manufacturer specification, role, or by the design of your organization. Network traffic filtering and inbound traffic filtering apply sets of rules at different points in the network or on a host to stop the communication of packets that meet a given signature. Network allowlists can also be used to block traffic based on traffic metadata such as IP address, ports, time, or other fields within a given communication stream. • Limit the source traffic subnets allowed to communicate with critical assets. • Where connection is needed, employ stateful firewalls that can filter protocol traffic based on content.
Network Segmentation	MITRE ICS ATT&CK: M0930[21]	
Filter Network Traffic	MITRE ICS ATT&CK: M0937[22]	
Network Allowlists	MITRE ICS ATT&CK: M0931[23]	

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR SPOOF REPORTING MESSAGE

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

1. Validate triggers and alerts
    a. Ensure the capability does not conflict with existing monitoring functionality
    b. Ensure the capability does not adversely impact the existing environment

[16] MITRE, Operating System Monitoring, 2021. Available online: https://d3fend.mitre.org/technique/d3f:OperatingSystemMonitoring.
[17] MITRE, System File Analysis, 2021. Available online: https://d3fend.mitre.org/technique/d3f:SystemFileAnalysis.
[18] MITRE, Service Binary Verification, 2021. Available online: https://d3fend.mitre.org/technique/d3f:ServiceBinaryVerification.
[19] MITRE, Software Process and Device Authentication, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0813.
[20] MITRE, Inbound Traffic Filtering, 2021. Available online: https://d3fend.mitre.org/technique/d3f:InboundTrafficFiltering.
[21] MITRE, Network Segmentation, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0930.
[22] MITRE, Filter Network Traffic, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0937.
[23] MITRE, Network Allowlists, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0807.

c. Test alerting functions
    i. Use synthetic data (e.g., PCAPs)
    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 Spoof Reporting Message 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 Spoof Reporting Message technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Spoof Reporting Message 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 Spoof Reporting Message technique came to be. Renamed libraries; changes to communication drivers on a host; wider clock drifts; and increases in industrial protocol errors and resets are all potential observables that could indicate the use of Spoof Reporting Message technique. Anomalies tied to these observables could be reporting messages sent from unauthorized/unexpected source assets, unexpected changes in host communication driver, process time issues, or increases in error messages associated with rejected packets.

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 Spoof Reporting Message technique. This will allow them to more quickly identify triggering events using the Spoof Reporting Message 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 reporting message is indicative of an adversary's presence in the network spoofing these messages (thus initiating incident response procedures) or if there is no evidence of malicious activity associated with the anomalous reporting messages (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 T856: SPOOF REPORTING MESSAGE

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