T846: REMOTE SYSTEM DISCOVERY

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 Remote System Discovery attack technique for the Discovery 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 *Remote System Discovery (T846) Technique Detection Capability Sheet* for the Discovery tactic.[4]

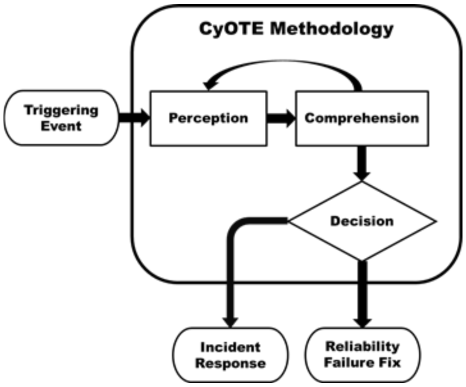

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, the Remote System Discovery technique includes all network and host techniques used by adversaries for identification of other systems. This data might be present on the host in event logs, process command lines, utilities (netstat), or determined via network polls. Remote system discovery might not be visible on the network if the attacker uses a host-based technique or if network monitoring does not cover the communication path between source and destination hosts.[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, Remote System Discovery, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0846.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Remote System Discovery (T846) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Remote System Discovery, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0846.

PERCEPTION: IDENTIFYING ANOMALIES

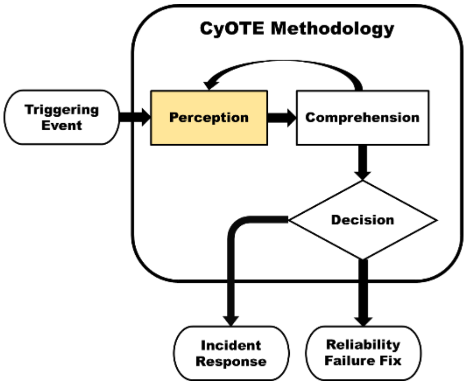

Figure 2: CyOTE Methodology – Perception Step

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." This nomenclature follows the North American Electric Reliability Corporation (NERC) nomenclature, which was adapted from Dr. Mica Endsley's model of situation awareness[6] – these terms cause the reader to think of the necessary individual and organizational human cognition as opposed to merely automated data processing. Perception is defined as a signature capable of being detected by a human; perception does not mean opinion or subjective interpretation. It provides the starting point—detection of a triggering event in the organization—for investigation during the comprehension step. This stage involves the identification of observables, anomalies, and triggering events of a potential malicious event; please consult the CyOTE methodology for more information on these terms.[7]

EXAMPLE OBSERVABLES AND ANOMALIES OF THE REMOTE SYSTEM DISCOVERY 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 Remote System Discovery technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
● TCP half open and simple TCP or UDP connections to industrial ports may indicate remote system discovery of industrial applications ● System discovery traffic patterns might also increment ports on a given host or increment host IPs or addresses in the network	An increase in handshake or partial handshake network connections if TCP or an increase in small or empty packets if UDP or not TCP	● Raw Network Data (Captured) ● Raw Network Data (Live) ● Network Flow Data (Captured) ● Network Flow Data (Live) ● Windows Event Logs (Standard)

[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
• Operators might notice an increase in the number of alarms or error codes from devices if an attacker floods the network with remote system discovery requests • Some industrial protocols, such as DNP3, have specific error messages devices may generate when they are overwhelmed with traffic	Network flooded with reconnaissance data that degrades the performance of industrial devices and applications	Operator or Plant Personnel
• The windows firewall or other endpoint protection software might log rejected remote system discovery requests • The quantity of logs might depend on the enabled ruleset and on the alert and log retention settings enabled on the device	Operating system and other application logs might include a significant increase in logged or rejected connections	• Operator or Plant Personnel • Windows Event Logs (Standard) • Application Logs
• Devices might be observed communicating from new subnets or from new hosts in existing subnets that communicate with industrial systems. • Windows or other operating system event logs or other application logs might contain connection metadata associated with the discovery campaign	An increase in traffic across network boundaries or for new hosts might be observed during remote system discovery	• Network Flow Data (Captured) • Network Flow Data (Live) • Windows Event Logs (Standard)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS REMOTE SYSTEM DISCOVERY

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

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

1. Identify what devices and protocols to monitor for Remote System Discovery

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

   a. E.g., remote terminal units (RTU)/automation controllers, programmable logic controllers (PLC)
   b. Identify parsers for the applicable protocols of each potential trigger
2. Identify the capability location and when it will operate
   a. Example capability locations: from firewall, integrated host, server, intrusion detection systems (IDS) and intrusion prevention systems (IPS), other
   b. Example operating timeframes: at startup, real-time, daily, weekly
3. Identify tap points (sensors) for observing device traffic for identified devices
   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. Monitoring and traffic aggregation may necessitate tap placement on both sides of the identified devices
      i. E.g., media access control (MAC) addresses may change as information traverses networking infrastructure like protocol converters
   c. 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
4. Identify business processes that support identification of Remote System Discovery
   a. Identify opportunities where plant personnel or other network and device users would identify signs of technique occurrence
   b. Identify operational data stores that might assist with confirmation of technique identification
      i. Help desk tickets related to technique
      ii. Plant maintenance tickets related to technique
      iii. Unusual behaviors or actions that plant personnel or a network user would observe related to the technique

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

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.

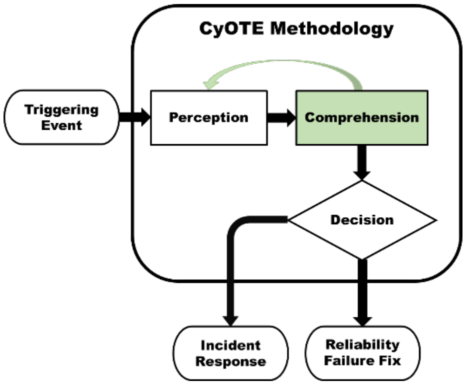

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO REMOTE SYSTEM DISCOVERY

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 Remote System Discovery

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

Organization	Capacity
	provide technical documentation and expert advice on expected device behavior.
Third-Party Support Vendors	Cybersecurity, threat intel, and other vendors that provide subject matter expertise might be able to provide insight into anomalies surrounding the trigger conditions.

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

STEPS FOR IDENTIFYING AND EXTRACTING INFORMATION FROM OT DATA FOR ANALYSIS OF REMOTE SYSTEM DISCOVERY

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

Suggested data fields to collect include:

- Timestamp
- Device Identifier (will vary based on environment)
  - Source and destination IP addresses
  - MAC addresses
- Remote System Discovery message
- Network captures (PCAPs)
- NetFlow records
- Firewall logs

STEPS FOR ANALYZING ANOMALIES FROM PARSED DATA FOR REMOTE SYSTEM DISCOVERY

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

1. Identify system discovery packets of interest to alert on
   a. Document anomalies based on host
      i. Identify the existing traffic origination points

            ii. Include the frequency and type of packets
    b. Identify and match system discovery packets to high-risk devices with criticality to the physical process
        i. Determine if the alert is valid or invalid based on analysis of the message parameters and source(s)
2. Identify system discovery packets coming from new or abnormal hosts
    a. Conduct a comparative analysis to identify new connections and alerts versus older ones
    b. Determine whether system discovery packets are occurring at an abnormal frequency
        i. E.g., frequency, order, type, messaging timing
        ii. Track system discovery packets and perform statistical and/or procedural tests
3. Establish anomalies
    a. Incorporate the analysis findings provided in Step 3 and implement to refine alert parameters to focus on the useful information and minimize the number of non-useful alerts
        i. E.g., abnormal system discovery packets received, high-risk devices being probed from external sources

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 Remote System Discovery

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
An increase in alarms or device error codes associated with production systems	Operator or Plant Personnel	1 hour	Awareness of potential impact to operation in case plant personnel aren’t already aware of device degradation

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
An originating device or endpoint managed by another team	Team responsible for endpoint resource	48 business hours	● Awareness of potential compromised system ● Discontinuation of traffic from the originating 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, an unplanned file server reboot initiated by a program that was downloaded might produce digital footprints like logs and errors. It might correspond to data loss, unauthorized configuration changes, elevated user permissions, or account activity at unusual hours.

Technical Analysis

Technical analysis for the Remote System Discovery technique should start with identification of system behaviors in scope for the type of discovery suspected. A wide range of possible actions might be classified as system discovery depending on the context of the behavior observed. System discovery might also take place on the network, on a single host, or on both network and host. Analysts performing technical analysis should focus on isolation of specific Remote System Discovery techniques in order to identify necessary date and specific analysis techniques.

Context Building

System discovery might consist of very obvious and overt behaviors by unsophisticated attackers or attackers that select high visibility discovery techniques. Likewise, sophisticated attackers, or attackers that closely mimic expected traffic patterns, might not be as overt.

- Leverage subnet to subnet traffic patterns observed in network and host data to understand the frequency of host-to-host communications. Understand the context associated with connections and the ports and protocols that hosts should connect to between subnets.
- Analyze host and network connection logs for an increase in rejected communications. Identify if rejected communications might be associated with remote system discovery requests.
- Analyze the applications on an endpoint that should be communicating with industrial ports and protocols. Alert on and investigate significant unexpected changes to industrial port and protocol associated traffic.

System discovery might require the correlation of several events in order to recognize malicious intent. Some system discovery techniques might blend with normal traffic patterns or between expected systems. Asset owners should continually understand how system discovery might be identified in the traffic patterns of their own environments and also practice correlation with other event sources and techniques.

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.

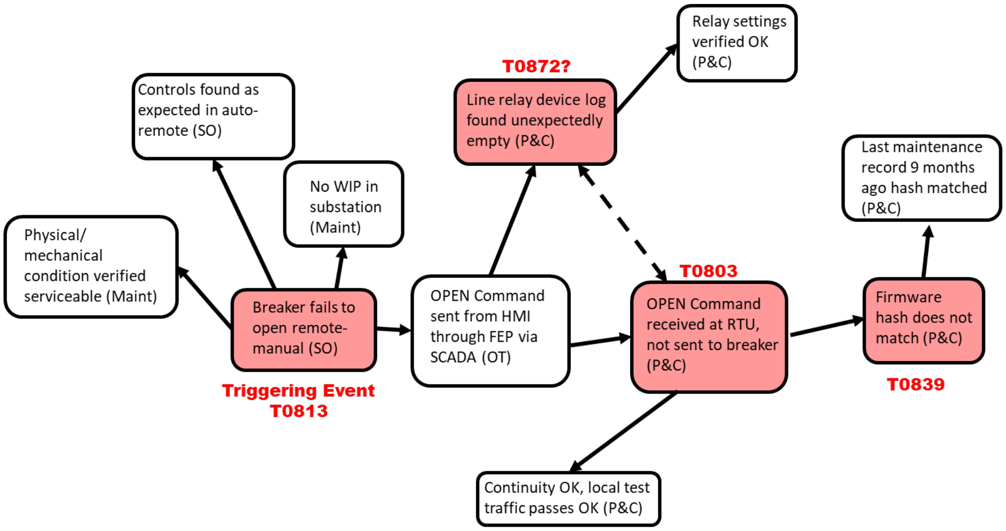
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
No WIP in substation (Maint)
Last maintenance record 9 months ago hash matched (P&C)
Physical/ mechanical condition verified serviceable (Maint)
Breaker fails to open remote-manual (SO)
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)
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 Remote System Discovery technique in the 2017 Triton attack on the Petro Rabigh refinery complex in Rabigh, Saudi Arabia is shown in Figure 5.[11]

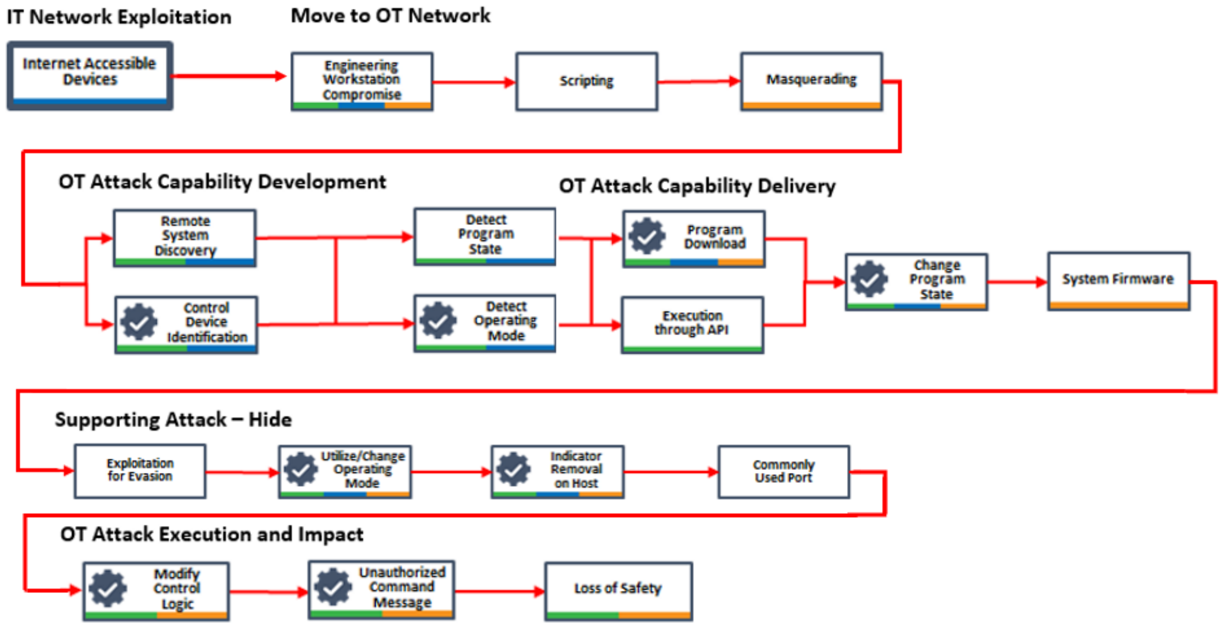

Figure 5: CyOTE Observables Link Diagram in Triton Case Study

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO REMOTE SYSTEM DISCOVERY

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

[11] CyOTE Case Study: Triton in Petro Rabigh, https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf
A legend for this diagram is included in the CyOTE Case Study: Trion in Petro Rabigh

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.

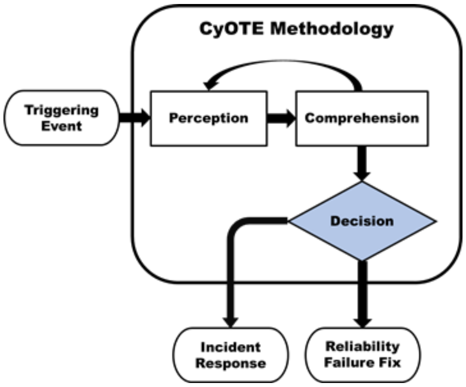

Figure 6: CyOTE Methodology - Decision Step

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 REMOTE SYSTEM DISCOVERIES

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
Inbound Traffic Filtering	MITRE D3FEND: D3-ITF[12]	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 applies a set of rules at different points in the network or on a host to stop the communication of packets that meet a given signature. Network allowlists can also be used to block traffic based on traffic metadata such as IP address, ports, time, or other fields within a given communication stream. ● Limit hosts communication to only essential traffic required between different subnets. While remote system discovery might still be possible with some protocols, protecting the scope of possible discovery requires an attacker to take additional actions that might be detected. ● Filter industrial ports and protocols to only operational subnets
Network Segmentation	MITRE ATT&CK for ICS: M0930[13]	
Filter Network Traffic	MITRE ATT&CK for ICS: M0937[14]	
Network Allowlists	MITRE ATT&CK for ICS: M0807[15]	
Network Traffic Community Deviation	MITRE D3FEND: D3-NTCD[16]	Network traffic community deviation and protocol metadata anomaly detection consider the metadata and contents of traffic transiting the network. Malicious point and tag identification requests might deviate significantly from expected traffic patterns and protocol metadata patterns. ● Protocol metadata anomalies might be focused on connection attempts or on protocol queries associated with device identification function codes. Certain protocols implement device identification functions an attacker can use for remote system discovery. ● System discovery might also leverage operating system functionality to perform network and device identification
Protocol Metadata Anomaly Detection	MITRE D3FEND: D3-PMAD[17]	

[12] MITRE, D3-ITF: Inbound Traffic Filtering, 2021. Available from: https://d3fend.mitre.org/technique/d3f:InboundTrafficFiltering/.

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

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

[15] MITRE, M087: Network Allowlists, 2021. Available from: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0807.

[16] MITRE, D3-NTCD: Network Traffic Community Deviation, 2021. Available from: https://d3fend.mitre.org/technique/d3f:NetworkTrafficCommunityDeviation/.

[17] MITRE, d3-PMAD: Protocol Metadata Anomaly Detection, 2021. Available from: https://d3fend.mitre.org/technique/d3f:ProtocolMetadataAnomalyDetection/.

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR REMOTE SYSTEM DISCOVERIES

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

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

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 Remote System Discovery 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 Remote System Discovery technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Remote System Discovery 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 Remote System Discovery technique came to be. TCP or UDP connections to industrial port, an increase in alarms or error messages, logs indicating rejected remote system discovery requests, and devices communicating from new subnets or from new hosts in existing subnets are all potential observables that could indicate the use of the Remote System Discovery technique. Anomalies tied to these observables could be increases in handshake or partial handshake network connections, networks being flooded with reconnaissance data, or significant increases in logged or rejected connections.

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 Remote System Discovery technique. This will allow them to more quickly identify triggering events using the Remote System Discovery 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 remote system discovery 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 remote system discovery (thus initiating corrective maintenance procedures).

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

APPENDIX A: DATASETS TO SUPPORT TRIGGERING EVENT ANALYSIS FOR T846: REMOTE SYSTEM DISCOVERY

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 provides a network-based perspective into potential remote system discovery behaviors and attacker actions
Device and System Logs	SysInternals SysMon SysInternals PsLogList EvtxToElk Python-evtx OSQuery	Network Security Team IT or OT System Admins	Data from the device and system logs might contain connection records associated with remote system discovery. If the system discovery is conducted by a rogue application, device and system logs might be used to trace the origin of remote system discovery queries from a given host. This is useful to identify a rogue application on a given host.
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

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