T840: NETWORK CONNECTION ENUMERATION

PURPOSE

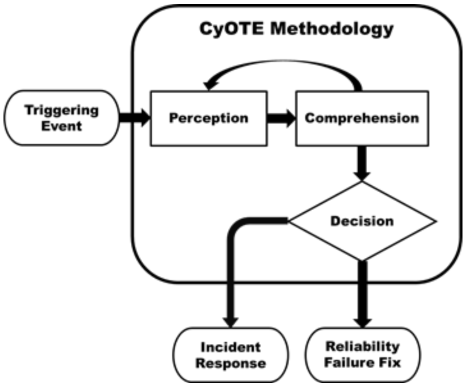

Figure 1: CyOTE Methodology Diagram

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 Network Connection Enumeration attack technique for the Discovery tactic as defined by the MITRE ATT&CK® for Industrial Control Systems (ICS) framework.[2,3] This allows 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 *Network Connection Enumeration (T840) Technique Detection Capability Sheet* for the *Discovery* tactic.[4]

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, adversaries may use the Network Connection Enumeration technique to learn about device communication patterns and determine the role of certain devices on the network.[5] Adversaries may also use the Network Sniffing technique (T842) to gather information about the traffic source, destination, protocol, and content.[6] Any networked device on the compromised network can be impacted by the Network Connection Enumeration technique, such as programmable logic controllers (PLC), human-machine interfaces (HMI), operator workstations, or any other additional supporting on premise or cloud infrastructure.

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." This nomenclature follows the North American Electric Reliability Corporation (NERC) nomenclature, which

[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, Network Connection Enumeration, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0840.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Network Connection Enumeration (T840) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Network Connection Enumeration, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0840.
[6] MITRE, Network Sniffing, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0842.

was adapted from Dr. Mica Endsley's model of situation awareness[7] – 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.[8]

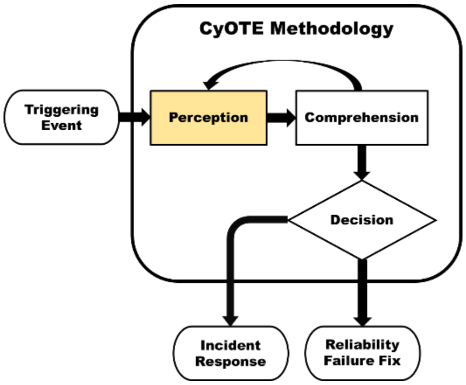

Figure 2: CyOTE Methodology – Perception Step

EXAMPLE OBSERVABLES AND ANOMALIES OF THE NETWORK CONNECTION ENUMERATION 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 Network Connection Enumeration technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
• Alert in security information and event management (SIEM), if applicable • Alert in endpoint detection/response software (EDR), if applicable • New networking/network scanning software present on endpoint	Use of network administration/discovery tools	• Endpoint command execution logs ○ Windows Event logs ○ Sysmon logs ○ EDR logs ○ PowerShell logs • Endpoint application execution logs ○ Windows event logs ○ Sysmon logs ○ EDR logs
• Alert in SIEM, if applicable • Alert in EDR software, if applicable	NXDOMAIN domain name system (DNS) query response	• Endpoint DNS query logs ○ Windows event logs ○ Sysmon logs

[7] 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.
[8] 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
• Alert in network detection/response software (NDR), if applicable • Network traffic live and collected	(Query for a domain that does not exist) • QueryResults field of Windows event logs and sysmon • dns.flags.rcode == 3 filter in Wireshark	○ EDR logs • DNS Server query logs ○ Windows event logs ○ Sysmon logs ○ EDR logs • NetFlow records • Zeek/bro logs • Firewall records • Packet captures (PCAP)
• Alert in SIEM, if applicable • Alert in EDR software, if applicable • Alert in NDR software, if applicable • Network traffic live and collected	Excessive network connection attempts from a single endpoint to either numerous ports or hosts, in succession	• Endpoint network logs • DNS Server network logs • NetFlow records • Firewall records • PCAP (feed SIEM alerting) • NetFlow records • bro/zeek logs
• Alert in SIEM, if applicable • Alert in EDR software, if applicable	Use of native system APIs	• Endpoint command execution logs ○ Windows event logs ○ Sysmon logs ○ EDR logs • Endpoint application logs ○ Windows event logs ○ Sysmon logs ○ EDR logs
• Industrial or standard network protocol enumeration[9]	Unusual usage of network protocols to determine network information	• PCAP • Network traffic anomaly detection • Host application logs

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS ACTIVITY IN OT ENVIRONMENTS

Asset owners and operators aiming to develop potential capabilities to monitor for use of the Network Connection Enumeration 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 operational technology (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.

As guidelines, the following best practices are recommended at a minimum:

[9] MITRE, Network Connection Enumeration, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0840.

1. Identify and compile a list of assets that are capable of performing or being targeted by Network Connection Enumeration
    a. Identify the hardware and software configuration on assets to assist with identification of data sources available to support analysis. This may include logging functionality, enabled industrial and/or IT protocols, and polling frequencies, among other configurations.
    b. Identify protocols in the environment, e.g., Ethernet/IP, S7Comm, Profibus, SERCOS III, Modbus, DNP3, Host HAP. Ensure identification includes both open source and vendor proprietary protocols.
2. Identify devices to be monitored for process state changes (e.g., PLCs, intelligent electronic devices [IED])
3. Identify data, logs, and log types needed to support identification of Network Connection Enumeration from these key devices, including field devices
    a. Identify tap points to observe device network traffic
    b. Identify log stores on endpoints that contain important data relevant to the technique
    c. Include servers, networking switches, security appliances, and logging devices (hosts)
    d. Include logs that can be manually connected or sent to central log collection data stores
    e. Identify log retention timelines for each data source. Some devices might have rolling logs, so it is necessary to understand the capacity limit for when log sources roll over and how frequently that limit is reached in your environment. This might impact central log collection data stores and/or raw network data collection sources.
4. Identify business processes that support identification of Network Connection Enumeration
    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

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.

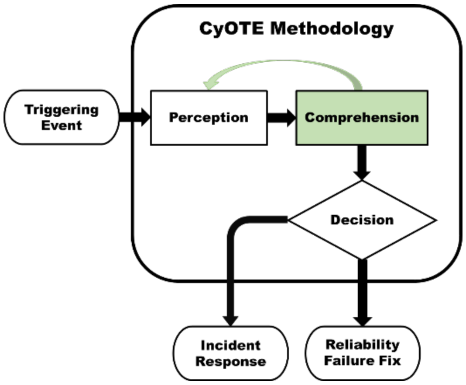

Figure 3: CyOTE Methodology - Comprehension Step

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO NETWORK CONNECTION ENUMERATION

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 organizational roles 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 Network Connection Enumeration

Organization	Capacity
System Operations and Engineering Roles	Includes control center field operators and real-time engineers responsible for the safe and reliable operation of OT systems. These individuals should be one of the first sources consulted. Information they may provide regarding an anomalous event includes institutional knowledge, manual logs, notes from field personnel investigations, and relevant established thresholds related to the anomaly.
Cybersecurity Roles	Includes those responsible for the confidentiality, integrity, and availability of the organization's digital assets. These individuals provide a threat-informed perspective and bring experience and capabilities to analyze situations and data for cybersecurity issues.

Organization	Capacity
IT Roles	Includes those responsible for the ownership, support, and administration of an organization's information technology assets.
OT Cybersecurity Roles	Includes those responsible for the support, administration, confidentiality, integrity, and availability of an organization's operational technology assets.

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

STEPS FOR PARSING AND EXTRACTING INFORMATION FROM OT DATA FOR ANALYSIS OF NETWORK CONNECTION ENUMERATION

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.

Data collected here can be used for further analysis, outlined in the next section of this recipe. It is unlikely that any single AOO will have all of the data sources mentioned, this is a compilation of all possible data sources that would contain valuable data to identify the technique. Each individual AOO should collect what is available in their environment

Suggested OT data elements to collect include:

- Network data, including both the collection of data at tap and span ports as well as analysis of network logs from appliances with relevant metadata

Suggested Logs elements to collect:

- Timestamp
- Device identifier(s) (will vary based on environment)
  - Hostnames
  - Source and destination IP addresses
  - Source and destination ports
  - Media access control (MAC) addresses
- Session size and duration
- DNS protocol packets
- Network captures (PCAPs)
- NetFlow records

- Firewall logs

Host data includes data stored on individual endpoints as well as data forwarded to central log collection storage locations. Host data might also include embedded devices, printers, and other non-traditional endpoints. Consider the following host data sources for data parsing and extraction:

- Endpoint DNS logs
- Endpoint network logs
- Endpoint command execution logs
- Endpoint application logs
- DNS server logs

STEPS FOR ANALYZING OT DATA ANOMALIES FOR NETWORK CONNECTION ENUMERATION

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 Network Connection Enumeration.

1. Identify the procedure being used. How is the enumeration performed? what method/methods were performed to enumerate the network connections?
    a. Are any tools being executed?
    b. Are files being read?
    c. Does the enumeration generate network traffic, or only endpoint logs?
    d. Which program(s) are generating the anomaly?
    e. Is there a pattern to the anomalous activity?
2. Identify the process that performed the procedure. What is the process/parent process and why is it here?
    a. Is this anomalous activity a result of an unknown binary executing?
    b. Is this anomalous activity the result of newly deployed software or process to the OT environment?
    c. Is this anomalous activity the result of an update or change to existing software?
    d. Ask software vendors or technicians: are these new binaries/software or changes to existing software/binaries expected?
3. Identify surrounding/related activity to the procedure. What other things is the process performing?
    a. Is the application that triggered the anomalous activity performing any other tactics, techniques, and procedures that look anomalous?
4. Verify no other endpoints in the environment have performed the procedure in the past/present
    a. Check current and historical logs for signs of other hosts performing this activity

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 Network Connection Enumeration

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Unknown software or file discovered on endpoint	• Engineering Department • Systems Operations Department • IT Department • Cybersecurity Department	Immediately	Understand what the software is used for, who/what installed it and why
Unknown use of network administration tools	Cybersecurity Department	Immediately	• Understand what the usage was for • What information was obtained by the execution which performed it?
NXDOMAIN Queries (Query for a domain that does not exist)	Cybersecurity Department	Immediately	• What domain is being queried? • Is this domain knowingly associated with malware? • Are there additional queries associated with this query? • Does this query appear to be a part of network enumeration?
Excessive network connection attempts from a single endpoint to either	Cybersecurity Department	Immediately	• What addresses, ports, or protocols are being queried/used? • Does this appear to be a port scan?

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
numerous ports or hosts, in succession			• Does this appear to be a Denial-of-Service (DOS)? • Does the endpoint usually make excessive connections across the network?
Unknown use of native system APIs	Cybersecurity Department	Immediately	• Which application or process is performing these calls? • Why are these new calls being made? • What information would be obtained from the call? • Could this information be used to enumerate the network?

ANALYZE INFORMATION AND CONTEXT COLLABORATIVELY

Documentation and Knowledge Management Process

Begin a documentation and knowledge management process in support of the investigation. Start with a determination of perceived actions in the triggering event. Did the change occur within:

- The physical domain (something involving telemetered quantities such as noise, voltage, current, frequency, or temperature, or the physical configuration of a piece of infrastructure); or
- The OT domain (something involving traffic or signals transiting a communication medium, or the logical configuration of a piece of infrastructure, or something involving memory/storage metrics); or
- Both the physical and the OT domains?

Given the determination of a physical or OT starting point, identify what expected corresponding, perceptible observables would exist in the other domain and search for their presence or absence. For example, an unplanned change to a device's operating mode might produce digital footprints like logs and errors. It might correspond to data loss, unauthorized configuration changes, elevated user permissions, or account activity at unusual hours.

Technical Analysis

The end goal for technical analysis should validate or disprove the hypotheses associated with the triggering condition(s). Technical analysis for network connection enumeration of a device should focus on the circumstances of the enumeration activity and any technical or human actions that might have instantiated the activity. Network connection enumeration might be initiated by a new physical link, or by software, so it is important to understand the origin of the activity.

Context Building Questions

Network data, if available, can provide the initial cluster of devices to focus on for initial context analysis. The viability of network analysis might vary depending on enabled protocols and the ability to parse communications from the protocols. The following questions intend to assist with initial analysis:

- Was the enumeration host-based, or did it generate network traffic?
- What information was gathered during the enumeration?
- Are any follow-up communications to any of the enumerated devices observed?
- Which process(es) instantiated the enumeration activity?
- Why did the process(es) perform this enumeration?
- What actions were taken with the enumerated data?

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

Visual Information Modeling

Enumerate all the lines of questioning identified through this stage of the analysis of the anomaly. At this point, it is beneficial to begin a node and link diagram from the information documented in the knowledge management processes to help visualize relationships between observables; the CyOTE program colloquially refers to this observable linking diagram as a “worm diagram.”

The triggering event is the first node, with all its related observables radially connected to it; include both confirmed observables and observables that were expected but not found, with some sort of visual discriminator between presence and absence (e.g., solid or dashed lines). Highlight the triggering event if the event relates to the implementation of a specific adversary technique. Include links emanating from the triggering event representing the as-yet-unanswered questions considered, as well as links and additional nodes for answered questions that confidently satisfy the extent of a particular line of inquiry. A notional example of this diagram for an investigation in progress is shown in Figure 4.

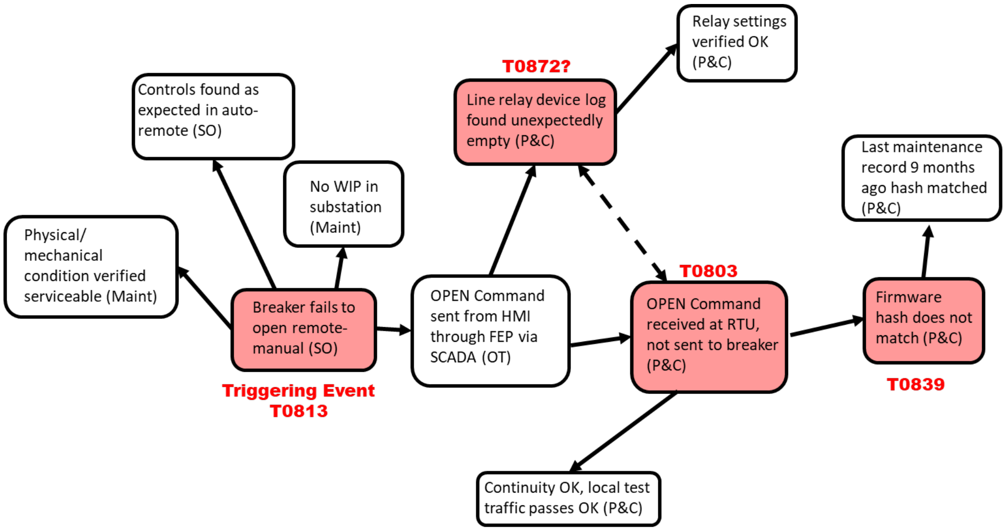
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
No WIP in substation (Maint)
Last maintenance record 9 months ago hash matched (P&C)
Physical/ mechanical condition verified serviceable (Maint)
Breaker fails to 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)
T0839
Triggering Event
T0813
Continuity OK, local test traffic passes OK (P&C)

Figure 4: Example CyOTE Observables Link Diagram

A worm diagram showing the use of the Network Connection Enumeration technique in the 2016 Industroyer/CRASHOVERRIDE attack on the Ukrainian power grid is shown in Figure 5.[10]

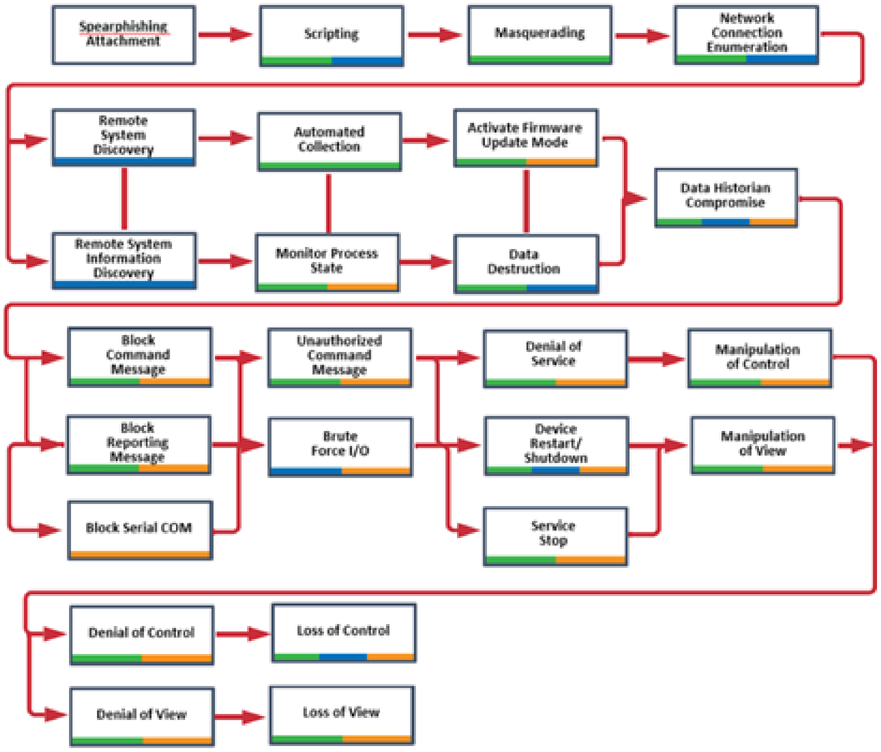

Figure 5: CyOTE Observables Link Diagram in Industroyer/CRASHOVERRIDE Case Study

[10] Case Study: CRASHOVERRIDE/Industroyer, https://inl.gov/wp-content/uploads/2021/12/CRASHOVERRIDE-CyOTE-Case-Study.pdf
A legend for this diagram is included in the CyOTE Case Study: CRASHOVERRIDE/Industroyer

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO NETWORK CONNECTION ENUMERATION

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.

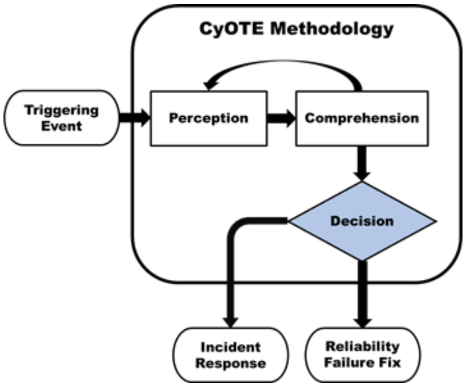

Figure 6: CyOTE Methodology - Decision Step

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 NETWORK CONNECTION ENUMERATION

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
Process Spawn Analysis	MITRE D3FEND™: D3-PSA[11]	• Monitoring and analyzing process spawns and arguments can help you detect various tools performing enumeration. • Additional analysis of process spawns and scripts can help identify parent process of the enumeration, as well as establish the context in which it was performed.
Script Execution Analysis	MITRE D3FEND: D3-SEA[12]	
DNS Traffic Analysis	MITRE D3FEND: D3-DNSTA[13]	• Monitoring DNS requests, their responses and metadata can help identify hosts performing queries to domains that do not exist on the network. • In addition, monitoring for new domains can help identify new activity in the network that could be a part of initial enumeration.
Connected Honeynet	MITRE D3FEND: D3-CHN[14]	• The deployment of honeypots, honeynets, or decoy resources can help aid in detection of network connection enumeration on the network. • Since no normal processes should interact with either host-side or network-deployed honeypots, and a large portion of malware is indiscriminate in its enumeration, interaction with these resources may be a good indicator of compromise.
Integrated Honeynet	MITRE D3FEND: D3-IHN[15]	
Standalone Honeynet	MITRE D3FEND: D3-SHN[16]	
Decoy Network Resource	MITRE D3FEND: D3-DNR[17]	

[11] MITRE, D3-PSA, Process Spawn Analysis. Available from: https://d3fend.mitre.org/technique/d3f:ProcessSpawnAnalysis/.
[12] MITRE, D3-SEA, Script Execution Analysis. Available from: https://d3fend.mitre.org/technique/d3f:ScriptExecutionAnalysis/.
[13] MITRE, D3-DNSTA, DNS Traffic Analysis. Available from: https://d3fend.mitre.org/technique/d3f:DNSTrafficAnalysis/.
[14] MITRE, D3-CHN, Connected Honeynet. Available from: https://d3fend.mitre.org/technique/d3f:ConnectedHoneynet/.
[15] MITRE, D3-IHN, Integrated Honeynet. Available from: https://d3fend.mitre.org/technique/d3f:IntegratedHoneynet/.
[16] MITRE, D3-SHN, Standalone Honeynet. Available from: https://d3fend.mitre.org/technique/d3f:StandaloneHoneynet/.
[17] MITRE, D3-DNR, Decoy Network Resource. Available from: https://d3fend.mitre.org/technique/d3f:DecoyNetworkResource/.

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR NETWORK CONNECTION ENUMERATION

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

1. Identify logging data required to perform alerting
    a. DNS query and response logs
    b. Network traffic captures
    c. Endpoint command execution logs
    d. Endpoint network connection logs
    e. Endpoint process execution logs
2. Where feasible, identify opportunities to ingest logging data into an alerting platform (e.g., SIEM, EDR/NDR, Datalake). Ensure collection balances collection of data that supports remote service alerting and analysis with operational network stability limitations and constraints. Some industrial OEMs have preferred products to accomplish this designed for different industrial control systems.
    a. Network tapping and data
    b. Endpoint native or third-party log forwarders to SIEM
3. Where feasible, implement logging and data collection equipment and configurations. If not feasible, identify opportunities to supplement logging and data collection with processes and technologies that accomplish similar outcomes.
    a. SIEM
    b. EDR
    c. NDR
    d. Windows Event Forwarding (WEF)/Syslog Forwarding
4. Create alert(s) to monitor for activity
5. Implement protection/prevention capability/configurations
    a. Reference the Control Matrix in Table 4 of this Recipe for different protection and prevention opportunities
    b. Ensure that selected protection and prevention controls fit the parameters of your environment and don't degrade or interfere with operations

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 Network Connection Enumeration technique within OT environments. Continual testing and evaluation will ensure that any defensive measures introduced do not negatively impact, adversely affect, or introduce vulnerabilities into the existing OT environment.

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 Network Connection Enumeration technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the Network Connection Enumeration 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 Network Connection Enumeration technique came to be. Invalid or new DNS queries, or unexpected use of endpoint network administration tools are both observables that could indicate the use of Network Connection Enumeration technique. Anomalies tied to these observables could be the use of network administration/discovery tools, queries to domains that do not exist, excessive network connection attempts from a single endpoint to numerous points or hosts, and the use of native system APIs.

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 Network Connection Enumeration technique. This will allow them to more quickly identify triggering events using the Network Connection Enumeration 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 Network connection enumeration 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 network connection enumeration (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 T840: NETWORK CONNECTION ENUMERATION

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 performing active network connection enumeration
Device & System Endpoint Activity Logs	• EDR Logs • Syslogs • Windows Event Logs	• Information Security Team • IT or OT System Admins	Endpoint logs contain host-side activity such as process start logs or command line execution. This detail can be useful in knowing if passive enumeration was performed.

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