T863: USER EXECUTION

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 User Execution attack technique for the Execution 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 *User Execution (T863) Technique Detection Capability Sheet* for the Execution tactic.[4]

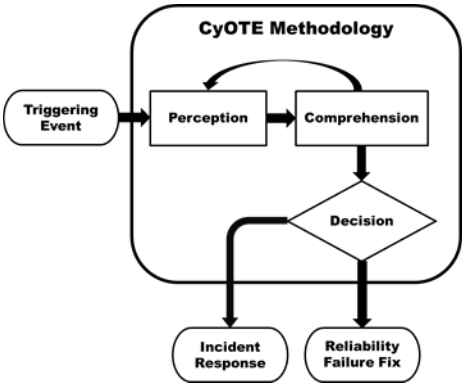

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, the User Execution technique includes all techniques that rely on user interaction to perform a given operation (e.g., opening attachments, installing software, granting permissions). User execution may involve a spearphishing attachment, for example, which can be used by an attacker to gain initial access into a network. User execution to allow heightened permissions might also be leveraged to move from one network subnet to another or to breach from the corporate network into the plant.[5]

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 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

[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, User Execution, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0863.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, User Execution (T863) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, User Execution, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0863.
[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.

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]

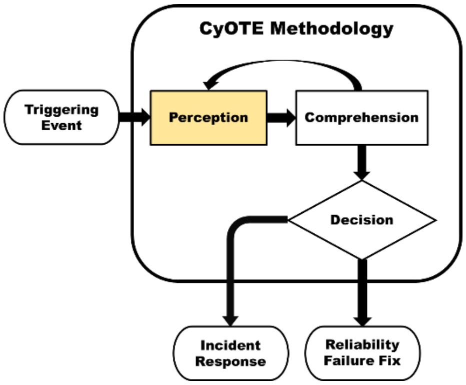

Figure 2: CyOTE Methodology – Perception Step

EXAMPLE OBSERVABLES AND ANOMALIES OF THE USER EXECUTION 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 User Execution technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
● Operators might notice signs of application usage outside of expected shift scheduled or operating procedure ● User execution occurs across various stages of the attack campaign and leverages different applications. ● Initial access via spear phishing will leave signs of user execution based on the attachment a user opened and executed. User execution at later stages might include metadata changes associated with plant applications.	Unusual or unexpected signs of access might be observed by plant personnel in application or event logs	● Operator or Plant Personnel ● Windows Event Logs (Standard) ● Application Logs
● Attackers might leverage arbitrary execution options in existing applications to run malicious code. These actions might be visible in application debug logs or in windows	Unusual or unexpected command line arguments to scripts and/or applications	● Windows Event Logs (Standard) ● Application Logs

[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
event logs. - Endpoint protection applications might also contain signs of malicious user execution.		
- As seen with Stuxnet, an attacker might leverage loading of a malicious application library to achieve malicious user execution. - Malicious modifications to existing applications might be visible in file metadata on disk or in memory or new malicious application libraries might be observed on disk or in memory.	Modified or copycat application binaries or application libraries observed on disk or executing	- File Metadata - Windows Event Logs (Standard)

STEPS FOR IDENTIFYING HIGH-CONSEQUENCE SYSTEMS, PATHWAYS, AND POTENTIAL ANOMALOUS USER EXECUTION

Asset owners and operators aiming to develop potential capabilities to monitor for use of the User Execution 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 User Execution
   a. E.g., remote terminal units (RTU)/automation controllers, programmable logic controllers (PLC)
   b. Identify the hardware and software configuration on assets to assist with identification of data sources available to support analysis.
   c. Identify protocols in the environment, e.g., Ethernet/IP, S7Comm, Profibus, SERCOS III, Modbus, DNP3, host access protocol (HAP). Ensure identification includes both open source and vendor proprietary protocols.
2. Identify the capability location and when it will operate

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

   a. Example capability locations: from firewall, integrated host, server, Intrusion detection systems (IDS), intrusion prevention systems (IPS)
   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 User Execution.
   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

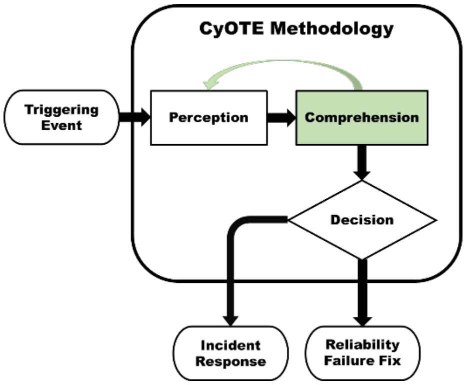

Figure 3: CyOTE Methodology - Comprehension Step

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

purposes of CyOTE is an organizational ability, not an individual one.

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO USER EXECUTION

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 User Execution

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 DATA FOR ANALYSIS OF USER EXECUTION

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
- Program payload
- Payload size (e.g., bytes)
- Service / Process name
- Account executing process / service
- Parameters associated with service / process

STEPS FOR ANALYZING ANOMALIES FROM PARSED DATA FOR USER EXECUTION

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 process / application execution events of interest to alert on
    a. Document anomalies based on host
        i. Identify the existing process executions
        ii. Include the frequency and type of process / application execution events
    b. Identify and match process / application execution events to high-risk devices with criticality to the physical process
        i. Determine if the alert is valid or invalid based on analysis of the application / process executed as well as associated parameters
2. Identify anomalous program / application execution events occurring on hosts
    a. Analyze process logs for anomalous process and application execution events
    b. Conduct a comparative analysis to identify new process and application execution events and alerts versus older ones
    c. Determine whether process / application execution events are occurring at an abnormal frequency or with anomalous parameters
        i. E.g., frequency, order, type, timing
        ii. Track execution events 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., new or abnormal process / application, high risk device execution, anomalous 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 User Execution

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Unexpected changes to industrial application binaries, libraries, and supporting files	Operator or Plant Personnel	48 business hours	Determine if the change to the application occurred in conjunction with a maintenance activity

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 User Execution technique needs to identify the applications executed and various means by which an attacker might benefit. For spearphishing, technical analysis might involve email clients and common attachment formats that attackers leverage; scripts in PDFs and word documents are common attack mediums. Within industrial networks, the attacker might leverage authentic or modified industrial applications to conduct a user execution-based attack.

Context Building Questions

Because the User Execution technique covers a wide range of activities, it is important to consider the scope of each particular investigation to ensure completeness and to understand the defender techniques and tools required to respond successfully. Context building should begin by narrowing the scope of the investigation to a particular starting point. This initial focus should leave room for later investigation as the chain of events unfolds, however it is important to start at a focused and coordinated point.

- What is the attack surface of your organization and at what points can an attacker leverage the User Execution ATT&CK for ICS technique?
- What network and/or host artifacts and evidence are available at each attack point?
- Would investigation require a single data source or multiple data sources?
- What tools and analysis techniques are available to analyze data sources?
- What is the complexity to collect and analyze the data for the different attack scenarios?
- What other groups and organizations might need to be involved to successfully analyze an attack leveraging the User Execution technique?

The context building questions above assist with the isolation of data required, tools required, analysis techniques used, and possible coordination with external teams.

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[11] of this diagram for an investigation in progress is shown in Figure 4.

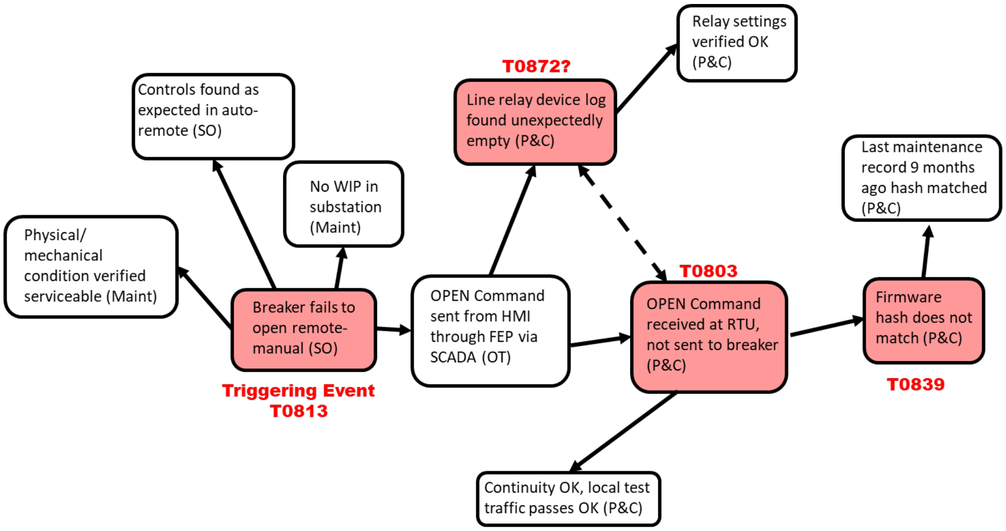
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
Last maintenance record 9 months ago hash matched (P&C)
No WIP in substation (Maint)
Physical/ mechanical condition verified serviceable (Maint)
T0803
Breaker fails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

Figure 4: Example CyOTE Observables Link Diagram

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO USER EXECUTION

After an anomaly has been comprehended sufficiently and mapped to a technique, repeat the steps above, starting from each questioning line resulting from the initial anomaly analysis. The importance of recording and organizing the information discovered in the comprehension process and visualizing it through a node and link diagram becomes exponentially more important as the first perceived anomaly expands into a web of postulated, confirmed, and denied relationships.

[11] Current CyOTE Case Studies do not include an analysis on the use of this technique in a historical attack; thus, there is no link diagram specific to this technique at this time.

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.

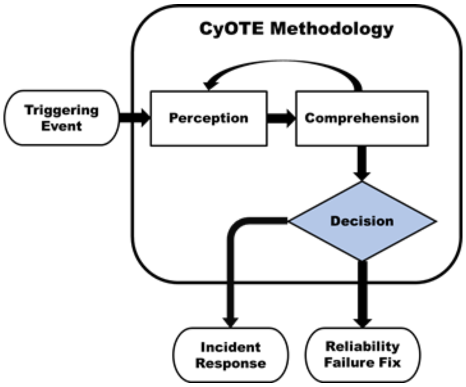

Figure 5: CyOTE Methodology - Decision Step

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. 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 USER EXECUTION

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
Sender MTA Reputation Analysis	MITRE D3FEND: D3-SMRA[12]	Sender MTA reputation analysis and sender reputation analysis look at the reputation of the mail sending infrastructure and data within the individual message. The combination of these two controls aims to make spear phishing more difficult. ● Use sender reputation analysis to make user execution attacks that leverage spear phishing more difficult. These controls will make an attacker invest in better infrastructure and adapt other attack techniques. ● Sender reputation analysis can be implemented algorithmically or through indicator feeds of known good and malicious senders.
Sender Reputation Analysis	MITRE D3FEND: D3-SRA[13]	
File Carving	MITRE D3FEND: D3-FC[14]	File content rules and file hashing provide two static methods for analysis of files on disk or going over the network. File carving enables extraction of a file from a network stream in order to apply file content rules and file hashing. ● File content rules written in open-source frameworks like Yara or Suricata might be used to detect known file signatures associated with user execution attack techniques. ● To analyze a file sent over the network, file carving might be needed before file content rules can be applied. ● File carving might also be used to extract a file embedded in another file on disk.
File Content Rules	MITRE D3FEND: D3-FCR[15]	
File Hashing	MITRE D3FEND: D3-FH[16]	
Process Spawn Analysis	MITRE D3FEND: D3-PSA[17]	Process spawn analysis, process lineage analysis, and script execution analysis all look at the origin of and metadata around program and script execution. This includes parent

[12] MITRE, D3-SMRA: Sender MTA Reputation Analysis, 2021. Available from: https://d3fend.mitre.org/technique/d3f:SenderMTAReputationAnalysis/.
[13] MITRE, D3-SRA: Sender Reputation Analysis, 2021. Available from: https://d3fend.mitre.org/technique/d3f:SenderReputationAnalysis/.
[14] MITRE, D3-FC: File Carving, 2021. Available from: https://d3fend.mitre.org/technique/d3f:FileCarving/.
[15] MITRE, D3-FCR: File Content Rules. 2021. Available from: https://d3fend.mitre.org/technique/d3f:FileContentRules/.
[16] MITRE, D3-FH: File Hashing, 2021. Available from: https://d3fend.mitre.org/technique/d3f:FileHashing/.
[17] MITRE, D3-PSA: Process Spawn Analysis, 2021. Available from: https://d3fend.mitre.org/technique/d3f:ProcessSpawnAnalysis/.

Control	Matrix	Relevance
Process Lineage Analysis	MITRE D3FEND: D3-PLA[18]	processes, parameters on the command line, and path and image information. ● Ensure host log analysis and dynamic analysis tools are capable of extracting process information. ● Process information might be compared against an atomic indicator of compromise or included in statistical analysis or anomaly detection to look for atypical or suspicious patterns. ● Metadata newness analytics might also discover malicious process patterns such as Microsoft Word launching a command prompt or calling out to adversary attack infrastructure.
Script Execution Analysis	MITRE D3FEND: D3-SEA[19]	

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR USER EXECUTION

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., log files containing application / process execution)
        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

[18] MITRE, D3-PLA: Process Lineage Analysis, 2021. Available from: https://d3fend.mitre.org/technique/d3f:ProcessLineageAnalysis/.
[19] MITRE, D3-SEA: Script Execution Analysis, 2021. Available from: https://d3fend.mitre.org/technique/d3f:ScriptExecutionAnalysis/.

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 User Execution 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 User Execution technique is being used as part of a malicious cyber-attack.

Through the Perception step, the AOO identifies observables and anomalies indicative of the User Execution 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 User Execution technique came to be. Signs of application usage outside of expected times or procedures, the use of arbitrary execution options noted in application logs, and modifications to existing applications as seen in file metadata or application libraries are all potential observables that could indicate the use of the User Execution technique. Anomalies tied to these observables could be unusual or unexpected signs of access, unexpected command line arguments to scripts and/or applications, or modified or copycat application binaries or libraries noticed on disk or when executing.

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 User Execution technique. This will allow them to more quickly identify triggering events using the User Execution 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 anomaly as a result of a user's action 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 anomaly (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 T863: USER EXECUTION

Table 5: Datasets to Assist with Analyzing Triggering Events

Dataset	Example Tools	Who Can Assist	Relevance
Device and System Logs	SysInternals SysMon SysInternals PsLogList EvtxToElk Python-evtx OSQuery	Network Security Team IT or OT System Admins	Device and system logs contain application and process execution data. The information contained in device and system logs enables an analyst to observe the effects caused by a user executing malicious programs or scripts. This might involve outbound connections to adversary infrastructure or suspicious child processes.

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