T886: REMOTE SERVICES

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 Services attack technique for the Initial Access & Lateral Movement tactics 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 *Remote Services (T886) Technique Detection Capability Sheet* for the Initial Access & Lateral Movement tactics.[4]

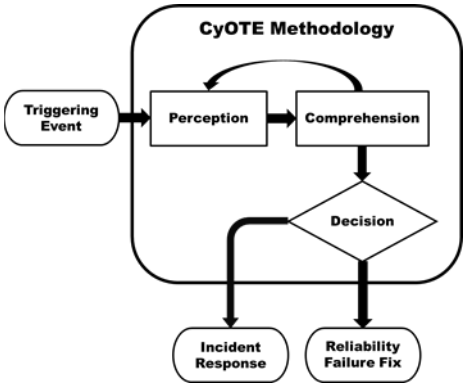

Figure 1: CyOTE Methodology Diagram

POTENTIAL ATTACK TARGETS

As defined by the MITRE ATT&CK® for ICS framework, adversaries may use the Remote Services technique to gain initial access to a system via protocols such as remote desktop protocol (RDP) and Secure Shell (SSH), among others. Upon gaining access, adversaries often move laterally between network assets/segments wherein further action is taken including but not limited to remote code execution, data exfiltration/transmission, and authentication.

Devices that can be impacted by the Remote Services technique include engineering workstations, human-machine interfaces (HMI), and control servers.[5] While those in traditional IT spaces might suggest eliminating the attack surface entirely by disabling remote services, owners and operators of industrial networks understand that remote access is more often enabled out of necessity rather than convenience. That said, AOOs should consider any asset with remote access (e.g., programmable logic controllers [PLC], remote terminal units [RTU], various field controllers) a possible attack vector.

---

[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 Services, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0886.
[3] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
[4] CESER, Remote Services (T886) Technique Detection Capability Sheet, CyOTE Program. Department of Energy, FY21.
[5] MITRE, Remote Services, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0886.

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 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]

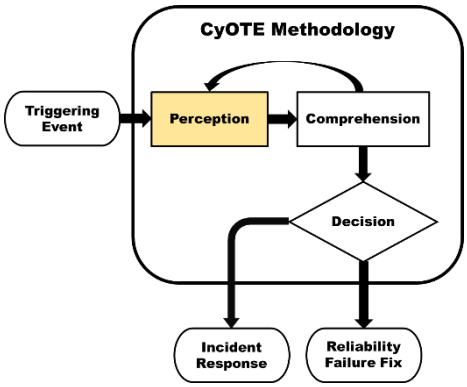

Figure 2: CyOTE Methodology – Perception Step

EXAMPLE OBSERVABLES AND ANOMALIES OF THE REMOTE SERVICES 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 Services technique.

Table 1: Notional Events

Observables	Anomalies	Data Sources
• Alert in security information and event management (SIEM) • Momentary opening of terminal/console windows, mouse-pointer movement not directed by operator	Command execution associated with an unusual remote service connection	• Endpoint OS command execution logs (e.g., Windows PowerShell logs, Sysinternals Sysmon logs) • Endpoint application execution logs • NetFlow data

[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
• Network traffic observed to remote service	New or unusual connection observed in network traffic, host traffic, or firewall data	Live or captured packet capture (PCAP) data
• Alert in SIEM	User login or logout at unusual time/frequency/geolocation or successful logon after high number of failed attempts	• Endpoint new user logon session logs • Logon session metadata in windows event logs or other authentication logs
• Alert in SIEM	Missing or improper network share access for endpoints/users	Endpoint network share logs (e.g., Windows Server Message Block [SMB] Client or Server event logs)
• Alert in SIEM • Potential change in network performance	• Anomalously high in/outbound network traffic related to remote service protocols (e.g., SMB, SSH) • Network captures showing unfamiliar protocol utilization	• Endpoint network connection creation logs • NetFlow records • Firewall records • PCAPs
• Alert in SIEM • Potential change in system performance/functionality • Slow or unexpected/abnormal system behavior	• Unusual change in system resource usage such as CPU/memory • OS API Execution	• Endpoint system/process monitors • Endpoint process creation, change, access, and exit logs • Endpoint application logs • Task Manager, likely indicating high system resource utilization

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 Remote Services 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.

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

1. Identify and compile a list of assets that are capable of performing or being targeted by Remote Services
    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, polling frequencies, etc.
    b. Identify protocols in the environment, e.g., Ethernet/IP, S7Comm, Profibus, SERCOS III, Modbus, Distributed Network Protocol 3 (DNP3), host access protocol (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 Remote Services 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 Remote Services
    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

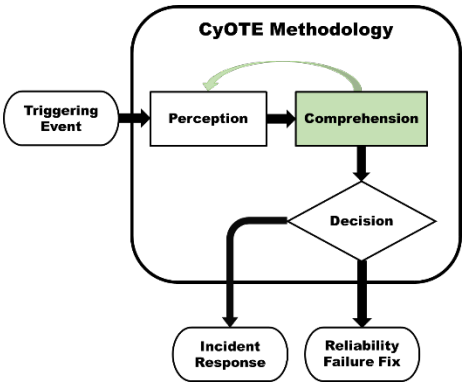

Figure 3: CyOTE Methodology - Comprehension Step

broader awareness of the overall context in which the triggering event came to be. Because of the multidisciplinary approach used for a sufficient investigation, comprehension for the purposes of CyOTE is an organizational ability, not an individual one.

IDENTIFY AND COLLECT AVAILABLE INFORMATION RELATING TO REMOTE SERVICES

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 Remote Services

Organization	Capacity
System Operations and Engineering Roles	Includes control center field operators and 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.
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 REMOTE SERVICES

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 elements to collect include:

- Network data
    - Network share access lists
    - Network access control lists (ACL)
    - Valid user accounts and logins
    - Trusted IP addresses
    - Network topology and segmentation (physical/logical)
    - Firewall states
- Host data
    - Suspicious/unknown binaries
    - IP/MAC Addresses
    - Asset-specific ACLs (e.g., if static address tables are configured)
    - Acceptable protocol use and process execution for devices or device groups

Suggested logs to collect include:

- Field controller logs
- Data Historian logs
- Windows Event Viewer Logs
    - Application/Security/System
    - Key Management Service
    - Hardware Events
    - PowerShell
    - SSH

STEPS FOR ANALYZING ANOMALIES FOR REMOTE SERVICES

The suggestions above are applied to data analysis and used to help establish anomalies. The list below includes suggested ways to use the extracted data 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 Remote Services.

The **Initial Access** tactic detection technique will monitor application logs, command execution, logon sessions, and network traffic while the **Lateral Movement** tactic detection technique will focus on network traffic, logon sessions, process handling, and command execution.

1. Assess network traffic for anomalous patterns
    a. Transfer of unknown binaries between network segments or OT levels
    b. New or unusually timed user logons
    c. New or unusually timed virtual private network (VPN) connections
    d. Suspicious or higher-than-normal outbound communication
2. Audit host access & communications for suspicious activity
    a. Unsigned/self-signed binaries
    b. Command-line executions
    c. Previously unseen executables from unusual sources
    d. Spawn of new process
    e. Termination of single or multiple running processes
    f. Process making API or system calls
3. Identify other tactics, techniques, and procedures (TTP) to use for correlation of potential incidents
    a. Anomalous activity on dual-homed hosts
    b. Privileged account creation
    c. Multiple systems accessed remotely over short period of time
    d. Domain privilege alteration
    e. Contextual logon metadata
    f. Process modified or accessed by another process

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 time frame 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 Services

What To Report	Whom To Report To	Recommended Timeframe	Desired Outcome
Suspicious remote access patterns on valid account	• IT Department • Cybersecurity Department • Possibly others, depending on nature of remote asset	Immediate	Inform user of possible breach, termination of remote session, password reset of compromised account, log analysis of account activity
Network share access granted to unauthorized user	• IT Department • Cybersecurity Department • Possibly others, depending on nature of network share	Immediate	Sysadmin/user notified, audit of user account, password reset, event log analysis of account and domain 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 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 Remote Services of a device should focus on the circumstances of the suspicious remote logon activity and any technical or human actions that might have instantiated the activity. In the OT space, remote services logons can occur during unusual hours (i.e., 24/7 plant operation begets 24/7 asset access), so it is important to understand/verify activity origins. This holistic perspective on anomalous user activity requires analysts to have a baseline familiarity with what would be considered "normal" user behavior. In most cases, lateral communication between departments is the simplest way to avoid confusion or false alarms.

Context Building Questions

Network and host 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. Host data might also observe session information not visible on the network. The windows event logs can help piece together the context of an encrypted RDP or SMB session. The following questions intend to assist with initial analysis:

- Who is authorized to remotely access the affected systems?
- What other remote assets do potentially compromised accounts have direct or indirect access to?
- Are the endpoints windows or other machines with authentication logs (Windows Event Log Security EVTX) that can assist with developing context behind a remote session?
- What sort of anomalous traffic patterns or alerts could be observed during the incident? Was a user's account used to authenticate to a service while they were on vacation or not working? Does the user have a valid need for that service?

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

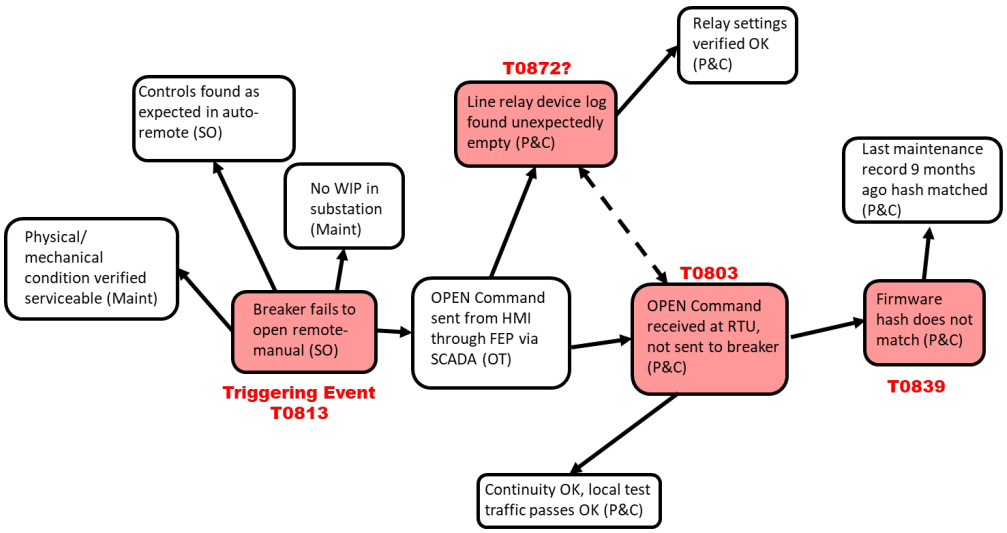

Figure 4: Example CyOTE Observables Link Diagram

INVESTIGATE POTENTIALLY RELATED ANOMALIES TO REMOTE SERVICES

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.

[8] 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.

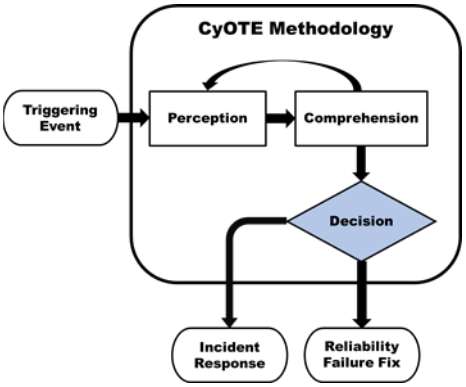

Figure 5: CyOTE Methodology - Decision Step

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 REMOTE SERVICES

The control matrix (Table 4) is a technical capability or system designed to prevent or sabotage specific attack techniques used by malicious actors. The control matrix assists with the identification of detection capability improvement areas.

Table 4: Control Matrix

Control	Matrix	Relevance
Network Segmentation	MITRE ATT&CK for ICS: M0930[9]	Used in conjunction, network segmentation, network traffic community deviation, and protocol metadata anomaly detection provide an exhaustive view into the network behaviors associated with the analysis of service stop commands. This group of controls does not exclusively include network data but can also include host-based application and operating system logs associated with the network traffic. • Leverage knowledge of the network environment to understand where industrial protocol messages should originate from to a given controller • Proper network segmentation provides functional boundaries where monitor and block actions can be implemented to prevent unauthorized changes to operation mode from unauthorized subnets • Understanding of program metadata for all protocols supported and enabled in your environment is critical for proper observation of remote services
Network Traffic Community Deviation	MITRE D3FEND™: D3-NTCD[10]	
Filter Network Traffic	MITRE ATT&CK for ICS: M0937[11]	
Network Allow Lists	MITRE ATT&CK for ICS: M0807[12]	
Password Policies	MITRE ATT&CK for ICS: M0927[13]	Strong passwords provide a line of defense against both insider threat and external threats. Strong passwords should be enforced on all endpoints in order to prevent misuse of the applications capable of conducting remote access. • Without a strong password policy, an attacker might use weak credentials to compromise an account, attain unauthorized remote access, and/or move laterally between systems • Password policies targeting frequent password changes reduces the probability harvested credentials will be valid, preventing unauthorized access to remote services
Strong Password Policy	MITRE D3FEND: D3-SPP[14]	

[9] MITRE, Network Segmentation, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0930.
[10] MITRE, Network Traffic Community Deviation, 2021. Available online: https://d3fend.mitre.org/technique/d3f:NetworkTrafficCommunityDeviation.
[11] MITRE, Filter Network Traffic, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0937.
[12] MITRE, Network Allowlists, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0807.
[13] MITRE, Password Policies, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0927.
[14] MITRE, Strong Password Policy, 2021. Available online: https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy.

Control	Matrix	Relevance
Human User Authentication	MITRE ATT&CK for ICS: M0804[15]	Strong authentication methods should always be utilized for users as well as device/process communications and API calls. • Multi-factor authentication, when operationally feasible and practical, is preferred • Authentication of inter-device communications is an effective control against message spoofing between master and outstation assets
Software Process and Device Authentication	MITRE ATT&CK for ICS: M0813[16]	
Authorization Enforcement	MITRE ATT&CK for ICS: M0800[17]	Account auditing validates the permissions of existing accounts and review of access logs. Proper account auditing provides a host-based baseline monitoring opportunity. • Identify and limit what roles are required for users on endpoints that regularly make operating mode changes • Ensure proper logging exists for attempts to act outside of a user's expected roles • Utilize least privilege models to ensure each user only has the access they need
User Account Management	MITRE ATT&CK for ICS: M0918[18]	
Access Management	• MITRE ATT&CK for ICS: M0801[19] • NIST 800-53: SI-7(8)[20] • NIST 800-53: AC-2[21] • NIST-800-82: 6.2.3[22] • NIST-800-82: 6.2.17[23]	

TESTING, DEPLOYING, AND REFINING ALERTING PARAMETERS FOR REMOTE SERVICES

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. Domain name system (DNS) query and response logs
    b. Network traffic captures
    c. Endpoint command execution logs

[15] MITRE, Human User Authentication, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0804.
[16] MITRE, Software Process and Device Authentication, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0813.
[17] MITRE, Authorization Enforcement, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0800.
[18] MITRE, User Account Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0918.
[19] MITRE, Access Management, 2021. Available online: https://collaborate.mitre.org/attackics/index.php/Mitigation/M0801.
[20] NIST, NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations,"2020, available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[21] Ibid.
[22] NIST, NIST Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security," 2015, available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
[23] Ibid.

   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, endpoint detection and response [EDR]/network detection and response [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 Remote Services 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 Services 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 Services 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 Services technique came to be. Unusual logon behavior and/or unauthorized process terminations are observables that could indicate the use of Remote Services technique. Anomalies tied to these observables could include missing or improper network share access for

endpoints/users, high in/outbound network traffic related to remote service protocols, and unusual changes in system resource usage.

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 Services technique. This will allow them to more quickly identify triggering events using the Remote Services 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 anomalous remote access patterns are 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 access patterns (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 T886: REMOTE SERVICES

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) • Zeek • NetworkMiner • Snort • Suricata • Security Onion	• Information Security Team • IT or OT System Admins	NetFlow and packet data assists with identification of systems with remote connections and possibly communication details
Device & System Configuration Files and Change History	• Sysinternals Suite • Engineering Workstation or HMI Software • Event Viewer	• Network Security Team • IT or OT System Admins	Device & system configuration files, event logs, and change history assist with root cause identification and timeline generation

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