PRECURSOR ANALYSIS REPORT: REMOTE ACCESS ATTACK ON OLDSMAR WATER TREATMENT FACILITY 2021

Cybersecurity for the Operational Technology Environment (CyOTE)

31 DECEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

INL/RPT-22-70551

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: REMOTE ACCESS ATTACK ON OLDSMAR WATER TREATMENT FACILITY 2021

1. EXECUTIVE SUMMARY

The Remote Access Attack on Oldsmar Water Treatment Facility 2021 Precursor Analysis Report leverages publicly available information about the Oldsmar cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

On 5 February 2021, an adversary gained unauthorized remote access to Bruce T. Haddock Water Treatment Plant in Oldsmar, Florida, which provides treated water to 15,000 customers.[1] The adversary accessed the facility's Supervisory Control and Data Acquisition (SCADA) workstation and human machine interface (HMI) to change the chemical concentration of sodium hydroxide, commonly referred to as lye and used to regulate acidity levels, from 100 parts per million (PPM) to 11,100 PPM.[2] The chemical was raised to lethal levels that if ingested could lead to serious soft tissue damage, burns, or even death.[3]

The facility, however, had redundancies and alarms in place to alert personnel of dangerous chemical levels,[4] and facility officials stated it would have taken 24 to 36 hours for the chemical changes to affect the water supply.[5]

Researchers and analysts identified six unique techniques utilized during the attack with a total of 23 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Four of the identified techniques used during the Oldsmar cyber attack were precursors to the triggering event. Analysis identified 21 observables associated with these precursor techniques, 20 of which were assessed to have an increased likelihood of being perceived in the minutes preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

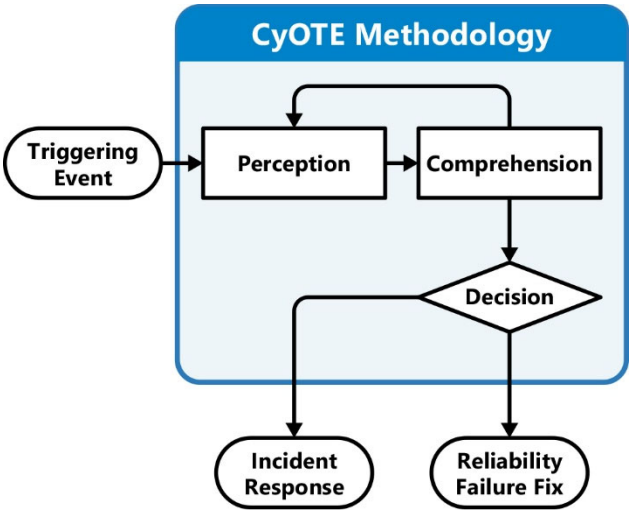


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

On 5 February 2021, an adversary gained unauthorized access to the Bruce T. Haddock Water Treatment Plant in Oldsmar, Florida via remote access and changed the chemical concentration of sodium hydroxide entering the water supply from 100 parts per million (PPM) to 11,100 PPM.[6] The Oldsmar plant provides treated water to 15,000 customers in Oldsmar, Florida.

The adversary very likely was able to remotely access the plant's human-machine interface (HMI) by exploiting cybersecurity weaknesses, including poor password procedures and an outdated operating system, Windows 7.[7] The initial intrusion took place at 8:00 AM EST (H-5), when the adversary remotely accessed the system and an operator noticed a small movement of the mouse cursor. This was not unusual, as supervisors and other personnel often monitor systems remotely. There was no immediate cause for concern.

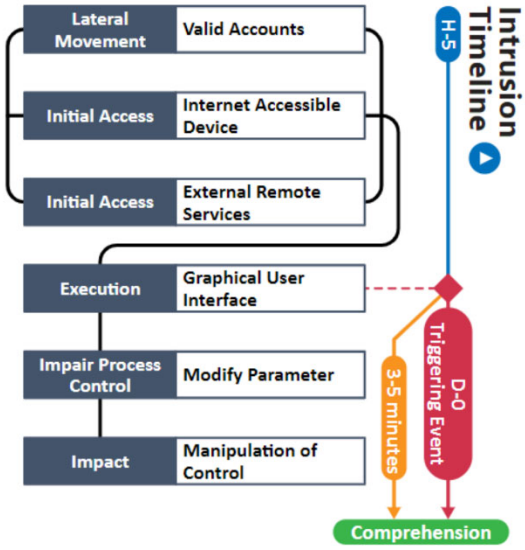


Figure 2. Intrusion Timeline

At 1:30 PM EST (D-0), a second mouse cursor movement occurred. The operator witnessed the remote user move the cursor to increase the amount of sodium hydroxide entering the water supply. The Oldsmar Water Treatment Facility contains brackish ground water, so levels of sodium hydroxide depend on the chemical makeup of the water at any given time. A wide range of sodium hydroxide levels are available for modification for that reason.[8]

Water treatment plant personnel immediately noticed the change and corrected the issue before the system software detected the manipulation.

A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of hours prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

Due to the immediate change back to normal levels, the water supply was not affected and operations continued as normal.[9] Initial investigation revealed the adversary remotely accessed the system for a total of 3 to 5 minutes.[10] Oldsmar facility officials stated it would have taken 24 to 36 hours for the chemical change to affect the drinking supply.[11] Oldsmar personnel disabled their remote access application and notified authorities of the incident.[12] This attack exemplifies potential risks of password sharing and remote access within critical infrastructure.

Analysis identified six unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Oldsmar Water Treatment Facility Cyber Attack

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**6**
Technique Observables	**23**
Precursor Techniques	**4**
Precursor Technique Observables	**21**
Highly Perceivable Precursor Technique Observable	**20**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

3.1. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The adversary used valid accounts to gain remote access into the Oldsmar water treatment facility's OT environment. It is unknown how these credentials were obtained, but the adversary very likely exploited cybersecurity weaknesses, such as shared usernames and passwords across OT staff, and vulnerabilities of an outdated operating system (OS), Windows 7.[13]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous user logins. However, this would not have prompted a security response as the adversary used valid accounts and supervisors used remote access regularly to monitor the systems from home.

One observable was identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it allows the adversary to use compromised credentials to bypass access controls, pivot across accounts and systems, including directly to the HMI, and reach a high level of access within the enterprise and OT environments. This technique appears early in the attack and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from accessing any system, eliminating the intrusion.

The observable associated with this technique is not assessed to be highly perceivable and is listed in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers[a]	IT Staff, IT Cybersecurity, OT Cybersecurity

[a] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

3.2. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

The adversary likely used valid credentials to access internet-exposed devices within Oldsmar's OT environment. The Supervisory Control and Data Acquisition (SCADA) system likely was running on the same domain controller as the desktop sharing software TeamViewer.[14]

IT Staff and IT Cybersecurity personnel may have been able to observe internet-accessible devices on the network and may have been able to observe the anomalous logons and network traffic originating from the adversary.

A total of nine observables were identified with the use of the Internet Accessible Device technique (T0883). This technique is important for investigation as it establishes the initial access vector and allows the adversary to gain access into the control system network. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from accessing assets in the OT environment.

All nine observables associated with this technique are assessed to be highly perceivable and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Internet Accessible Device technique
Technique Observers	IT Staff, IT Cybersecurity

3.3. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

Once TeamViewer authenticated the credentials, the adversary was able to interfere directly with the facility's SCADA system twice over a span of six and a half hours.[15] Without proper multi-factor authentication, the credentials allowed the adversary access to OT systems without raising suspicion.[16] Only when the adversary adjusted the sodium hydroxide levels did the operator perceive the activity as malicious.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, and Management personnel may have been able to observe remote access to the systems, mouse cursor movement, and adjustments of the system's parameters.

A total of nine observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it provides a point of initial access into the system from an external location. This technique appears relatively early and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit operational damage.

All nine observables associated with this technique are assessed to be highly perceivable and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, and Management

3.4. GRAPHICAL USER INTERFACE TECHNIQUE (T0823) FOR EXECUTION

Once the adversary was in Oldsmar's SCADA system, they were able to interact with the Graphical User Interface (GUI) to enhance their execution capabilities and interaction with the OT HMI system (Figure 3).[17] Utilizing TeamViewer remote desktop protocol (RDP), the adversary was able to move the mouse cursor across the HMI screen to adjust the chemical levels and composition in a matter of seconds.

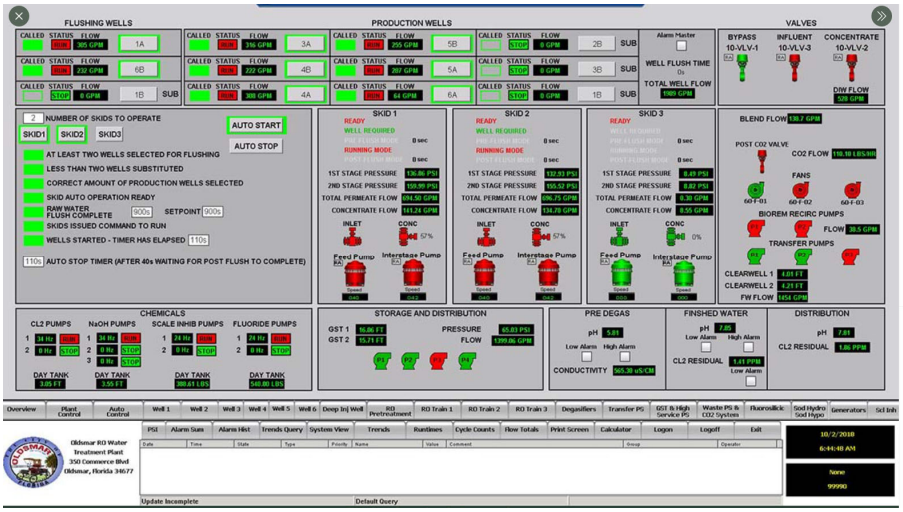


Figure 3. Oldsmar HMI

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering staff may have been able to observe remote access into the systems, anomalous mouse cursor movement, and adjustments of the systems parameters.

A total of two observables were identified with the use of the Graphical User Interface technique (T0823). This technique is important for investigation because adversaries may gain access to a machine and enhance their execution capabilities. This technique appears in the middle of the attack. Responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit operational damage as the adversary would not have direct access to equipment that controls the chemical components of the treatment facility.

Both observables associated with this technique are assessed to be highly perceivable and are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 60 artifacts could be generated by the Graphical User Interface technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering

3.5. MODIFY PARAMETERS TECHNIQUE (T0836) FOR IMPAIR PROCESS CONTROL

The adversary was able to modify the parameters of the sodium hydroxide levels by moving the mouse cursor across the HMI screen, changing the value from 100 PPM to 11,100 PPM, over 100 times the normal level.[18]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe mouse cursor movement and adjustments of the systems parameters.

One observable was identified with the use of the Modify Parameters technique (T0836). This technique is important for investigation because modified critical parameters may not only impact systems but create dangerous conditions. This technique appears later in the attack and represents the triggering event, as it is the point at which the victim noticed the mouse cursor change the sodium hydroxide level to well outside of normal levels. Responding to this technique will prevent the adversary from changing the chemical composition of the drinking water supply. Terminating the chain of techniques at this point would prevent damage and impact.

The observable associated with this technique is assessed to be highly perceivable and is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 18 artifacts could be generated by the Modify Parameters technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering

3.6. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

The adversary was able to manipulate the physical process control within the OT environment by moving the mouse cursor to change the composition of the water being treated. The duration of the adversary's manipulation of the controls was brief; however, this short window allowed the adversary time to make changes to the chemical composition of the water supply. The operator's immediate response to the adversary's manipulation prevented the water supply from being adversely affected.[19]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe mouse cursor movement and adjustments of the systems parameters.

One observable was identified with the use of the Manipulation of Control technique (T0831). This technique is important for investigation because adversaries can manipulate physical process controls within the OT environment, potentially causing safety concerns. They can use the HMI to manipulate process control setpoint values well beyond normal levels. This technique appears later in the timeline, after the triggering event and typically beyond the point at which the victim could limit the impact of the attack. However, with redundancies, alarms, and rapid operator response as demonstrated in this case, terminating the chain of techniques at this point can limit operational damage.

The observable associated with this technique is assessed to be highly perceivable and is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Manipulation of Control technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Internal Credentials Posted on Public Site

Observables Associated with Internet Accessible Device Technique (T0883)	
Observable 1 †	*Anomalous DNS Traffic*
Observable 2 †	*Anomalous Domain Name System (DNS) Request: from Internal Domain Controller: to *.teamviewer.com: Over TCP/UDP Port 53*
Observable 3 †	*Anomalous Usage of Remote Support Software: Remote Desktop Protocol (RDP): From external IP to internal domain controller: over TCP 5938*
Observable 4†	*Anomalous Successful Logon to Domain Controller: Windows Event ID 4624 Type 10: At 8:00 AM EST on 5 February 2021.*
Observable 5 †	*Anomalous Successful Logon to Domain Controller: Windows Event ID 4624 Type 10: At 1:30 PM EST on 5 February 2021.*
Observable 6 †	*Anomalous Successful Logon to Domain Controller: Special Privileges Assigned to New Logon Windows Event ID 4672*
Observable 7 †	*Anomalous Successful Logon to Domain Controller: The Domain Controller Attempted to Validate the Credentials for an Account Windows Event ID 4776*
Observable 8 †	*Anomalous Remote Support Software Application Logs: TeamViewer: File Path C:\Program Files (x86)\TeamViewer\TeamViewerXX_Logfile.log*
Observable 9 †	*Anomalous access log entries on webapp service account: TeamViewer.com*

Observables Associated with External Remote Services Technique (T0822)	
Observable 1 †	*Anomalous DNS Traffic*
Observable 2 †	*Anomalous Domain Name System (DNS) Request: from Internal Domain Controller: to support.teamviewer.com: Over TCP/UDP Port 53*
Observable 3 †	*Anomalous Usage of Remote Support Software: Remote Desktop Protocol (RDP): From external IP to internal domain controller: over TCP 5938*
Observable 4 †	*Anomalous Successful Logon to Domain Controller: Windows Event ID 4624 Type 10: At 8:00 AM EST on 5 February 2021.*
Observable 5 †	*Anomalous Successful Logon to Domain Controller: Windows Event ID 4624 Type 10: At 1:30 PM EST on 5 February 2021.*
Observable 6 †	*Anomalous Successful Logon to Domain Controller: Special Privileges Assigned to New Logon Windows Event ID 4672*
Observable 7 †	*Anomalous Successful Logon to Domain Controller: The Domain Controller Attempted to Validate the Credentials for an Account Windows Event ID 4776*
Observable 8 †	*Anomalous Remote Support Software Application Logs: TeamViewer: File Path C:\Program Files (x86)\TeamViewer\TeamViewerXX_Logfile.log*

Observables Associated with External Remote Services Technique (T0822)	
Observable 9 †	*Anomalous access log entries on webapp service account*

Observables Associated with Graphical User Interface Technique (T0823)	
Observable 1 †	*Anomalous mouse cursor movement on HMI: At 8:00 AM EST on 5 February 2021.*
Observable 2 †	*Anomalous mouse cursor movement on HMI: At 1:30 PM EST on 5 February 2021.*

Observables Associated with Modify Parameters Technique (T0836)	
Observable 1 †	*Anomalous manipulation of industrial process: Manipulation of water treatment chemicals: Increase in levels of sodium hydroxide: from 100 PPM to 11,000 PPM*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1 †	*Anomalous manipulation of industrial process: Manipulation of water treatment chemicals: Increase in levels of sodium hydroxide: from 100 PPM to 11,000 PPM*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 1	Host Registry Entries
Artifact 2	HTTPS Traffic
Artifact 3	Suspicious Connections in Proxy Logs
Artifact 4	Timestamps
Artifact 5	VPN Log Off Events
Artifact 6	Suspicious Connections in Firewall Logs
Artifact 7	VPN Log On Events
Artifact 8	SAP Traffic
Artifact 9	Host Registry Entries HKEY_LOCAL_MACHINE\SYSTEM
Artifact 10	SQL Traffic
Artifact 11	Host Information in External Data Store or Website (SHODAN)
Artifact 12	HTTP 80
Artifact 13	VNC Traffic Port 5800 or
Artifact 14	Dialog Boxes Opened on HMI or
Artifact 15	Application Authentication Events

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 16	Internet Address in Memory Socket Data
Artifact 17	Remote Logins in OS Logs (Windows Event)
Artifact 18	Operational Database Connection to External Addresses
Artifact 19	Industrial Traffic from Internet Address
Artifact 20	Standard Traffic from Internet Address
Artifact 21	Internet Address in Application Logs
Artifact 22	Internet Address in OS Logs
Artifact 23	Internet Address in Command Line Record Data (netstat)

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 1	Remote Session Key
Artifact 2	User Account Creation
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logon s Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Services Protocols
Artifact 9	Logon Event Type
Artifact 10	VPN Connections
Artifact 11	System Registry Network Interfaces
Artifact 12	Remote Services Logon
Artifact 13	TLS Certificate
Artifact 14	Session Logoff Event
Artifact 15	Blocked Incoming Connections Event
Artifact 16	Logon Event Type
Artifact 17	User Privileges Change
Artifact 18	Encrypted Network Traffic
Artifact 19	Blocked Incoming Packet Event
Artifact 20	External IP Address
Artifact 21	Security Account Manager Registry Password Hashes
Artifact 22	Command Prompt Window Opened
Artifact 23	Dialog Box Pop-Up
Artifact 24	Security Account Manager Registry Entries

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 25	User Client Address
Artifact 26	User Account Name
Artifact 27	Domain Controller Log
Artifact 28	Mouse Movement

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 1	Cursor Movement
Artifact 2	SSH Connections
Artifact 3	Host-Screen Adjustments
Artifact 4	Code Injections
Artifact 5	Program Executions
Artifact 6	RDP Connections
Artifact 7	VNC Connections
Artifact 8	Prefetch Files Created
Artifact 9	SSH Port
Artifact 10	Keyboard Entries
Artifact 11	Mouse Movement
Artifact 12	RDP Port
Artifact 13	SMB Port
Artifact 14	Application Execution via Input Devices
Artifact 15	Service Creation
Artifact 16	Service Modification
Artifact 17	Process Input Changes
Artifact 18	JUMPLIST Creation
Artifact 19	SHELLBAG Creation
Artifact 20	System Resource Use Management Changes
Artifact 21	Network Connection Durations
Artifact 22	Changes In Bytes Sent and Received
Artifact 23	Increase CPU Cycles
Artifact 24	Host System Crash
Artifact 25	Application Usage Increase
Artifact 26	Remote Client Execution
Artifact 27	Logon Event
Artifact 28	Screen Resolution Changes

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 29	Network Bandwidth Changes
Artifact 30	Remote Vendor Connections
Artifact 31	Event Log Creation
Artifact 32	VPN Connections
Artifact 33	Session Authentication
Artifact 34	Failed Logons Event
Artifact 35	Session Timestamp
Artifact 36	Logon Event Type 3
Artifact 37	Logon Event Type 10
Artifact 38	Logon Event Type 11
Artifact 39	Remote Session Key
Artifact 40	System Registry Network Interfaces
Artifact 41	Remote Services Logon
Artifact 42	TLS Certificate
Artifact 43	Session Logoff Event
Artifact 44	Domain Controller Log
Artifact 45	External IP Address
Artifact 46	Process Creations
Artifact 47	External MAC Address
Artifact 48	Encrypted Network Traffic
Artifact 49	Remote Services Protocols
Artifact 50	Blocked Incoming Packet Event
Artifact 51	Blocked Incoming Connections Event
Artifact 52	User Account Creation
Artifact 53	Security Account Manager Registry Password Hashes
Artifact 54	Command Prompt Window Opened
Artifact 55	Mouse Movement
Artifact 56	Dialog Box Pop-Up
Artifact 57	Security Account Manager Registry Entries
Artifact 58	User Client Address
Artifact 59	User Account Name
Artifact 60	User Privileges Change

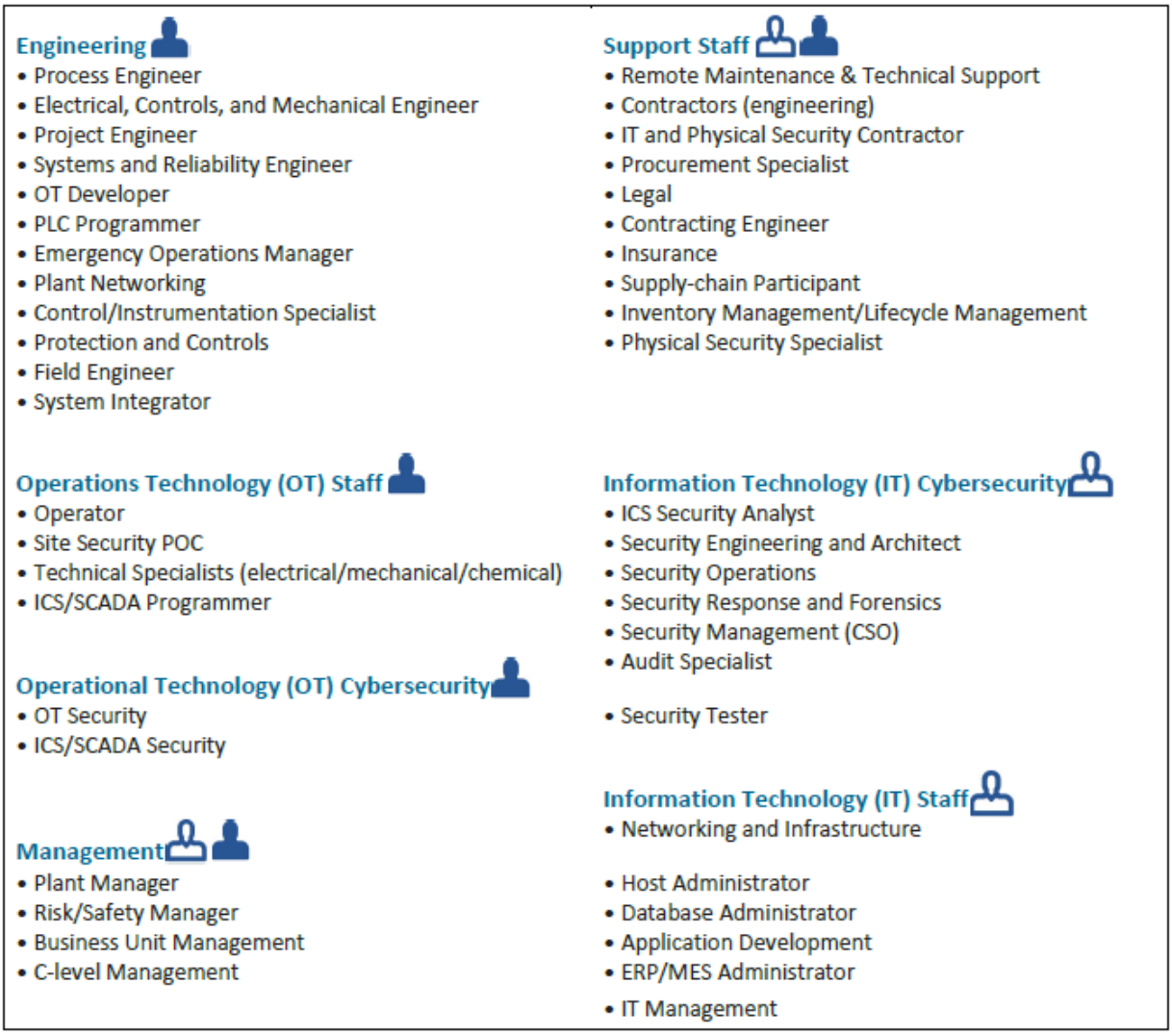
Artifacts Associated with Modify Parameter Technique (T0836)	
Artifact 1	Device Set Points Changed
Artifact 2	Device Alert
Artifact 3	Device Failure
Artifact 4	Process Performance Degradation
Artifact 5	Application Log Events
Artifact 6	Machine State Change
Artifact 7	Industrial Protocol Packets
Artifact 8	Project File Changes
Artifact 9	Configuration Changes
Artifact 10	Non-Standard Application Calls
Artifact 11	New Software Installed
Artifact 12	Nonstandard Service Creation
Artifact 13	Process Creation
Artifact 14	.dll Changes
Artifact 15	Driver Modifications
Artifact 16	Alert Failure
Artifact 17	Network Traffic
Artifact 18	Remote GUI Manipulation

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	Controller Set Point Change
Artifact 2	Event Log Creation
Artifact 3	Process Restart
Artifact 4	Process Shutdown
Artifact 5	Process State Change
Artifact 6	Process Initiated
Artifact 7	Controller Tag Change
Artifact 8	Controller Parameter Change
Artifact 9	I/O Modification
Artifact 10	Operational Data Modification
Artifact 11	Application File Modification
Artifact 12	Application Log Event
Artifact 13	Command Execution
Artifact 14	HMI Input Manipulation

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 15	Altered Command Sequences
Artifact 16	Engineering Workstation Mouse Movement

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



REFERENCES

[1] [U.S. Department of Homeland Security | “Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant” | https://www.mi-wea.org/docs/1._DHS_ST-Chemical_Considerations_for_the_Incident_at_Oldsmar_FL-10_FEB_2021.pdf | 5 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[2] [U.S. Department of Homeland Security | “Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant” | https://www.mi-wea.org/docs/1._DHS_ST-Chemical_Considerations_for_the_Incident_at_Oldsmar_FL-10_FEB_2021.pdf | 5 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[3] [U.S. Department of Homeland Security | “Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant” | https://www.mi-wea.org/docs/1._DHS_ST-Chemical_Considerations_for_the_Incident_at_Oldsmar_FL-10_FEB_2021.pdf | 5 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[4] [LSIE Logical Systems | Patrick Honeycutt | “Security Incident at Oldsmar Water Treatment Plant Lessons Learned” | https://www.logicalsysinc.com/wp-content/uploads/2021/03/SecurityIncident_OldsmarWaterTreatmentPlant_LessonsLearned.pdf | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[5] [LSIE Logical Systems | Patrick Honeycutt | “Security Incident at Oldsmar Water Treatment Plant Lessons Learned” | https://www.logicalsysinc.com/wp-content/uploads/2021/03/SecurityIncident_OldsmarWaterTreatmentPlant_LessonsLearned.pdf | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[6] [U.S. Department of Homeland Security | “Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant” | https://www.mi-wea.org/docs/1._DHS_ST-Chemical_Considerations_for_the_Incident_at_Oldsmar_FL-10_FEB_2021.pdf | 5 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [Joint Cybersecurity Advisory | Kent Backman | “Compromise of U.S. Water Treatment Facility” | https://www.ic3.gov/Media/News/2021/210212.pdf |11 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[8] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[9] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[10] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[11] [LSIE Logical Systems | Patrick Honeycutt | “Security Incident at Oldsmar Water Treatment Plant Lessons Learned” | https://www.logicalsysinc.com/wp-content/uploads/2021/03/SecurityIncident_OldsmarWaterTreatmentPlant_LessonsLearned.pdf | 4

November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[12] [LSIE Logical Systems | Patrick Honeycutt | “Security Incident at Oldsmar Water Treatment Plant Lessons Learned” | https://www.logicalsysinc.com/wp-content/uploads/2021/03/SecurityIncident_OldsmarWaterTreatmentPlant_LessonsLearned.pdf | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[13] [Federal Bureau of Investigation, Cyber Division | Private Industry Notification | 9 February 2021 | Accessed on 1 September 2022 | The source is publicly available information and does not contain classification markings]

[14] [U.S. Department of Homeland Security | “Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant” | https://www.mi-wea.org/docs/1._DHS_ST-Chemical_Considerations_for_the_Incident_at_Oldsmar_FL-10_FEB_2021.pdf | 5 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[15] [Joint Cybersecurity Advisory | Kent Backman | “Compromise of U.S. Water Treatment Facility” | https://www.ic3.gov/Media/News/2021/210212.pdf |11 February 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[16] [Cybersecurity and Infrastructure Security Agency | “Alert (AA21-287A) Ongoing Cyber Threats to U.S. Water and Wastewater Systems” | https://www.cisa.gov/uscert/ncas/alerts/aa21-287a |14 October 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[17] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[18] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[19] [Pinellas County Sheriff’s Office | “21-015 Detectives Investigate Computer Software Intrusion at Oldsmar’s Water Treatment Plant” | https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant | 4 November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]