FY21 TECHNIQUE PRIORITIZATION REPORT

OCTOBER 21, 2021

CyOTE Cybersecurity for the Operational Technology Environment

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

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

Idaho National Laboratory

Table of Contents

1 EXECUTIVE SUMMARY

The Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) program, is working with energy sector Asset Owners and Operators (AOO) and Idaho National Laboratory (INL) to develop threat detection capabilities for partners to independently identify adversarial tactics, techniques, and procedures (TTP) within their operational technology (OT) environments. An objective of the CYOTE program is to assist AOOs in identifying evidence of anomalous activity within their OT environments through the use of the CyOTE methodology and application of developed capabilities.

The CyOTE methodology applies fundamental concepts of perception and comprehension to the universe of knowns and unknowns, increasingly disaggregated into observables, anomalies, and triggering events. CyOTE capabilities correlate Use Cases developed by industry working group members to individual techniques. The three industry-affirmed Use Cases: Human Machine Interface (HMI), Remote Login, and Alarm Logs, were mapped to the updated (April 2021) MITRE ATT&CK® for Industrial Control System (ICS) Framework.[1]

This paper outlines the updated process for the prioritization of techniques identified in the MITRE ATT&CK® for ICS Framework (April 2021) to be addressed by the CyOTE program and supersedes the previous document dated 31 July 2019. The prioritization criteria include:

- Deprecation of detection capabilities previously developed by the CyOTE program
- Identification of techniques used by adversaries in cyberattacks based on the MITRE ATT&CK ICS framework with a focus on frequency of use
- Application of techniques to the three industry Use Cases
- Moving AOO's threat detection capabilities earlier into an attack campaign

The output from the subsequent analysis and refinement has resulted in a list of prioritized techniques for which the CyOTE program will develop capabilities.

2 INTRODUCTION

In 2019, the CyOTE Pilot leveraged a pre-release version of the MITRE ATT&CK for ICS framework (2019) to analyze adversary TTPs. These previous efforts analyzed the techniques used and applied the three industry Use Cases – HMI, Remote Login, and Alarm Logs – affirmed by the CyOTE Industry Working Group and validated through INL analysis. This analysis evaluated historical cyber case studies where OT log data may have had a high likelihood of containing attack indicators as an adversary traverses OT networks during an attack. Taken together, the three Use Cases identified data sources and fields which covered 87 percent of all techniques described in the ATT&CK for ICS framework.[2] The CyOTE team mapped the

Use Cases to applicable adversary techniques, identifying available data sources and potential limitations (Figure 1).

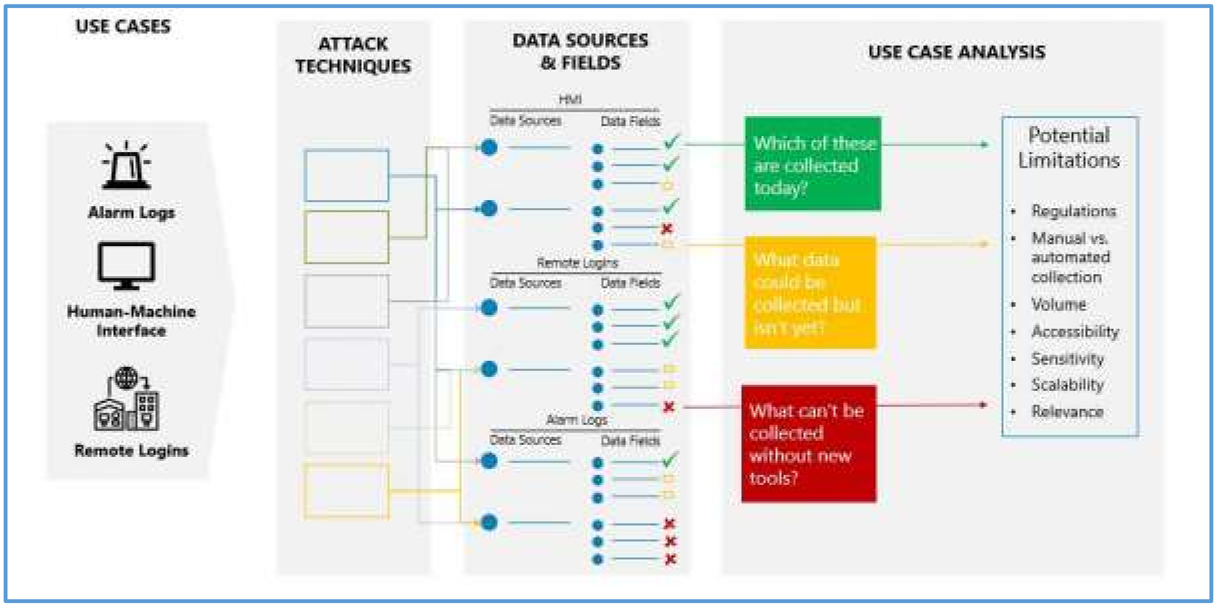


Figure 1 Mapping Adversary Techniques to Data Availability

The Industry Working Group Use Case analysis identified three observable types: 1) observables associated to tactics and techniques with implemented collection pathways and validated signatures; 2) observables associated to tactics and techniques with available collection pathways and workable signatures; and 3) observables without known collection tools or techniques. Regarding observables listed within item 2, the CyOTE program noted the existence of numerous commercially available detection capabilities which identify the use of techniques associated with the Initial Access tactic.[3] As a result, many of the Initial Access techniques were not considered for development. To identify malicious anomalies earlier in the adversary kill chain[a], CyOTE focused on adversarial use of techniques identified in the MITRE ATT&CK for ICS framework, which are located left of the Impact tactic. As a result, techniques associated with the Impact tactic were not considered in the prioritization effort. CyOTE used the remaining TTPs, as seen in the MITRE ATT&CK for ICS framework, to define malicious behaviors or techniques, indicative of a potential attack.

This led to further refinement of the remaining techniques. The analysis identified techniques that an adversary could use in one or more of the Industry Use Cases within OT environments. This analysis resulted in a prioritized list of techniques based upon their applicability to two or more Use Cases as outlined in the prioritization criteria above.

The purpose of this paper is to update the CyOTE program's prioritization of techniques based on updates to the MITRE ATT&CK for ICS framework.

[a] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

2.1 MITRE ATT&CK FOR INDUSTRIAL CONTROL SYSTEMS (ICS) FRAMEWORK (2021)

This paper incorporates changes to the updated MITRE ATT&CK for ICS framework from 29 April 2021 (Figure 2). The updated framework is broadly categorized, takes consideration for the heterogeneous nature of ICS/OT network environments and, *"… focuses on adversaries who have a primary goal of disrupting an industrial control process, destroying property, or causing temporary or permanent harm or death to humans by attacking industrial control systems*."[4]

The updated ICS framework (2021) visually aligns 79 individual techniques, 10 of which align to more than one tactic. MITRE added the Inhibit Response Function and Impact tactics to the framework to reflect adversary goals. This resulted in the identification of 12 applicable tactics for use in characterizing and describing post-compromise adversary behaviors of OT environments.[5, 6] Additionally, the current version of the ATT&CK for ICS framework maintains its arrangement of tactics from left to right: the early stages of an attack focus on initial access, execution, and persistence, evading detection, and exploring the environment. The later stages of the attack focus on inhibiting response functions, impairing process controls, and in some cases realizing a physical impact.

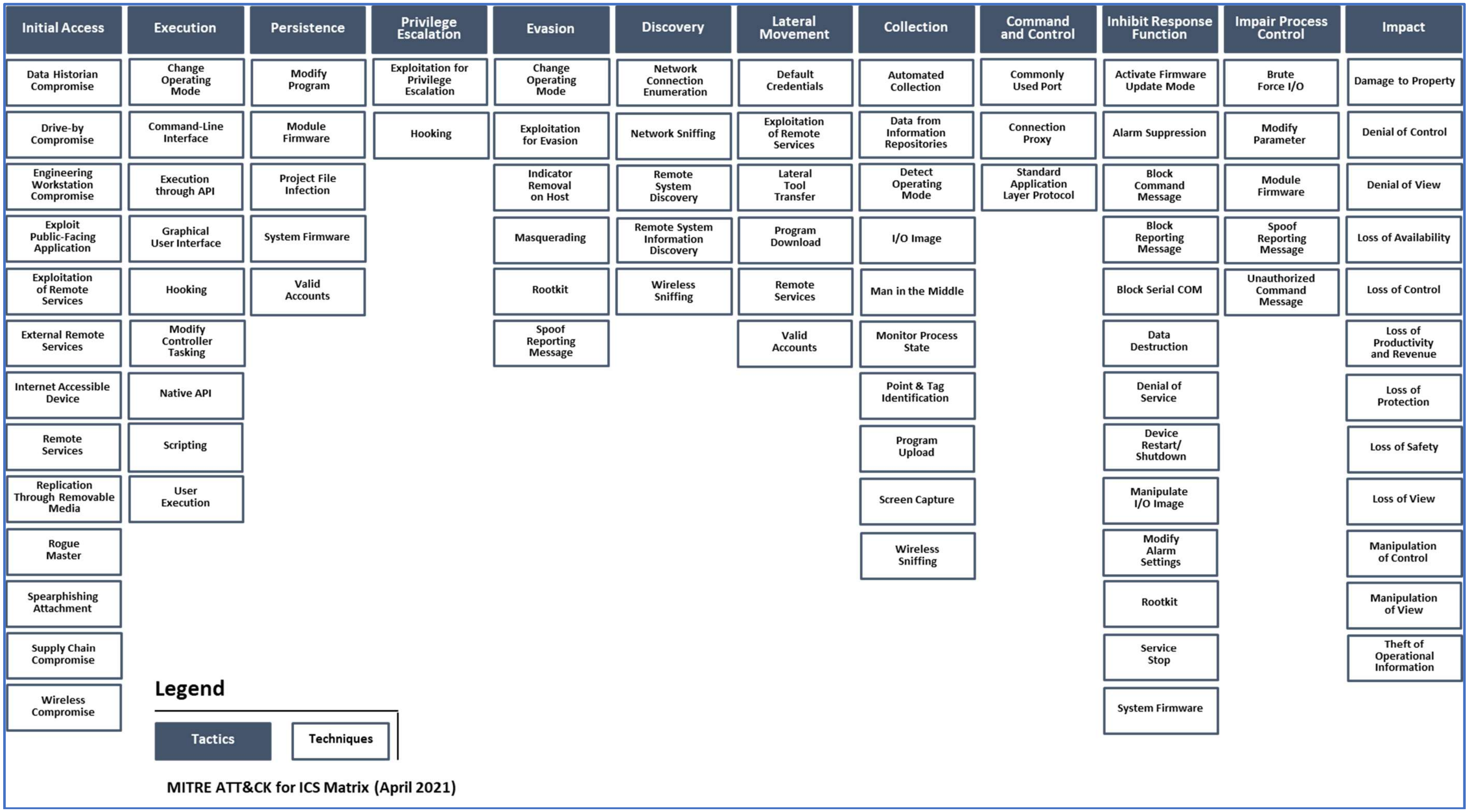
Just like in previous iterations of the ATT&CK for ICS framework, techniques are presented in alphabetical order under each tactic in the framework. Definitions for each technique can be found within the framework from MITRE.[7] The updated MITRE ATT&CK frameworks (2021) have expanded development of their three public frameworks – Enterprise, Mobile, and ICS – to include Cloud.[8] The Enterprise, Mobile, and Cloud frameworks primarily focus on IT communications. As a result, the techniques associated with those frameworks are presently excluded from current prioritization consideration. The CyOTE program's primary focus is on increasing security for OT environments. As Enterprise, Mobile, and Cloud frameworks become more integrated within OT environments, consideration for expanding prioritization to include the associated techniques will be made.

Each framework identifies tactics and techniques which have been used by adversaries against the various environments.

The updated ATT&CK for ICS framework (Figure 2) better identifies adversary tactics and techniques specifically employed in attacks targeting OT/ICS environments.[9] Example techniques include:

- Native Application Programming Interface (API)
- Remote Services
- Remote Systems Information Discovery

Finally, the April 2021 version of the ATT&CK for ICS framework establishes an updated common taxonomy which combines many similar techniques to increase clarity in highlighting observed and reported TTPs used by adversaries during attacks targeting OT environments. The April 2021 version of the MITRE ATT&CK ICS framework will be used throughout the remainder of the paper as a common lexicon to discuss recent threat activity.



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Legend

Tactics | Techniques

MITRE ATT&CK for ICS Matrix (April 2021)

Figure 2 MITRE ATT&CK ICS Framework[10]

2.2 DEVELOPED CAPABILITIES

Prioritization of TTPs for analysis and capabilities development was derived from examination of the CyOTE Use Cases and consultations with the CyOTE participating AOOs for validating operational context. This prioritization led to the development of the following capabilities in FY20 and FY21:

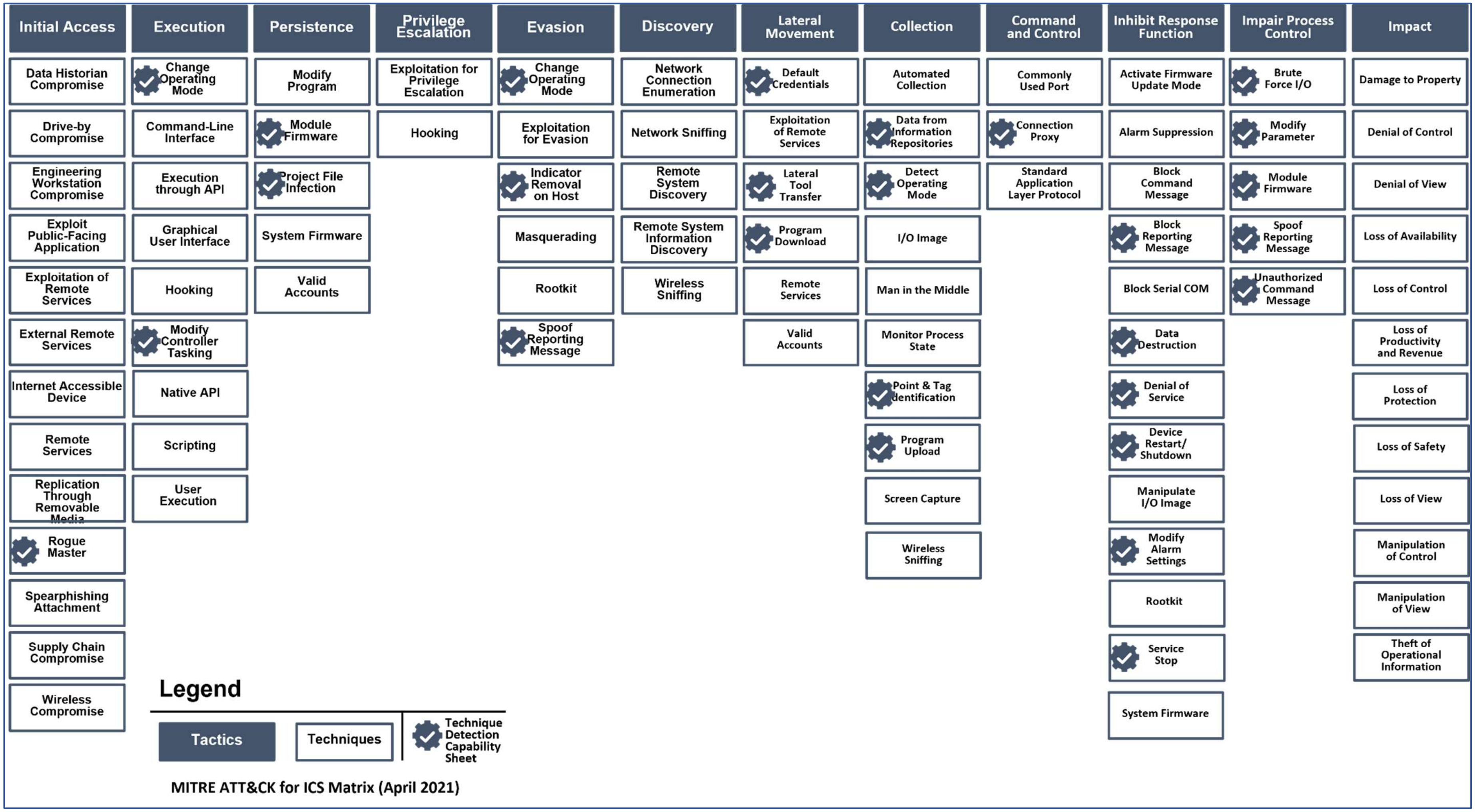
- *T804 Block Reporting Message*
- *T806 Brute Force I/O*
- *T858 Change Operating Mode*
- *Change Program State**
- *T884 Connection Proxy*
- *Control Device Identification**
- *T809 Data Destruction*
- *T811 Data from Information Repositories*
- *T812 Default Credentials*
- *T814 Denial of Service*
- *T868 Detect Operating Mode*
- *T816 Device Restart/Shutdown*
- *I/O Module Discovery**
- *T872 Indicator Removal on Host*
- *T867 Lateral Tool Transfer*
- *T838 Modify Alarm Settings*
- *Modify Control Logic**
- *T836 Modify Parameter*
- *T839 Module Firmware*
- *T861 Point & Tag Identification*
- *T843 Program Download*
- *T845 Program Upload*
- *T873 Project File Infection*
- *T848 Rogue Master*
- *T881 Service Stop*
- *T856 Spoof Reporting Message*
- *T855 Unauthorized Command Message*

Table 1. Developed Capabilities

Note: Items followed by "*" represent capabilities developed prior to the August 29, 2021 update to the MITRE framework which have either been deprecated or merged.

The capabilities listed above currently have Technique Capability Detection sheets that are available to AOOs to improve detection of anomalous activity when implemented within their OT environment. Capabilities developed and shown in Figure 3 are documented and available in the "CyOTE Technique Detection Capabilities Report."[b]

[b] Contact CyOTE.Program@hq.doe.gov for more information regarding the "CyOTE Technique Detection Capabilities Report."



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	✓ Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	✓ Change Operating Mode	Network Connection Enumeration	✓ Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	✓ Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	✓ Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	✓ Data from Information Repositories	✓ Connection Proxy	Alarm Suppression	✓ Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	✓ Project File Infection		✓ Indicator Removal on Host	Remote System Discovery	✓ Lateral Tool Transfer	✓ Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	✓ Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	✓ Program Download	I/O Image		✓ Block Reporting Message	✓ Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	✓ Unauthorized Command Message	Loss of Control
External Remote Services	✓ Modify Controller Tasking			✓ Spoof Reporting Message		Valid Accounts	Monitor Process State		✓ Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						✓ Point & Tag Identification		✓ Denial of Service		Loss of Protection
Remote Services	Scripting						✓ Program Upload		✓ Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
✓ Rogue Master							Wireless Sniffing		✓ Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									✓ Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Legend

Tactics | Techniques | ✓ Technique Detection Capability Sheet

MITRE ATT&CK for ICS Matrix (April 2021)

Figure 3 Developed Capabilities (as of August, 2021)

3 ANALYTICAL FRAMEWORK

This paper supersedes the documented analytical framework located in the 2019, "*Threat-Informed Tactic, Technique, and Procedure Prioritization Report,*" used in the prioritization of techniques in FY20. The following analytical framework makes use of cyberattacks outlined in the MITRE ATT&CK for ICS framework and case studies of adversarial targeting of OT networks to identify frequently used techniques during threat events. The analysis of the techniques employed are then supported through the findings and observation by both Department of Homeland Security incident responders and CyOTE subject matter experts (SME) to identify and remove any potential disqualifiers[c]. Further refinements of techniques are accomplished through the application of industry Use Cases (HMI, Remote Login, and Alarm Logs) in which the techniques with the greatest applicability to the three Use Cases receive highest priority. The analytical results generated a list of prioritized techniques which the CyOTE program will use to evaluate future research. The method by which the CyOTE program prioritizes techniques is detailed below in the following schema.

The CyOTE team employs a differential weighting strategy to assign each technique a value between 0-10 based on the following contributing factors:[11]

- Deprecation of detection capabilities previously developed by the CyOTE program
- Identification of techniques used by adversaries in cyber-attacks based on the MITRE ATT&CK ICS framework with a focus on frequency of use
- Application of techniques to the three industry Use Cases
- Moving AOO's threat detection capabilities earlier into an attack campaign

3.1 IDENTIFICATION OF TECHNIQUES USED BY ADVERSARIES IN CYBERATTACKS BASED ON MITRE ATT&CK FOR ICS FRAMEWORK AND USE

The past decade has witnessed a litany of attacks targeting OT environments from Stuxnet in Iran, Industroyer in Ukraine, to Triton in Saudi Arabia. The evolution of these ICS cyberattacks have been documented by the CyOTE team in the 2019 "Threat-Informed Tactic, Technique, and Procedure Prioritization Report."[12] More recently, industry has witnessed a rise in the number of adversaries and attacks specifically targeting industrial control systems across multiple sectors from CryptoLocker and WannaCry, to Ryuk, EKANS, and DarkSide. As a result, cyberattacks against physical equipment is now a globally available action that can be leveraged for commercial, strategic, and financial gains.[13]

In February 2019, Joseph Slowik wrote of growing threats to ICS based on earlier attacks. Except for Stuxnet, "*[ICS cyber] events have progressed from mere enumeration and data gathering (HAVEX campaigns) to active disruption of operations (Ukraine events) to potentially seeking physical destruction (TRISIS).*"[d][14] The report identified increases in adversary sophistication, abilities, and how techniques were employed. This signaled a maturing adversarial approach towards offensive cyber operations.

More recently in 2020 and 2021, adversaries have shifted from immediate process disruption, undermining integrity of physical processes and undermining reliability of underlying process(es), toward the simplification of initial access operations through the use of native system tools and common IT-centric TTPs, "living-off-the-land" instead of using customized malware to gain an initial foothold in an ICS

[d] Stuxnet represents an outlier to this trend, as it caused physical damage as early as 2010.

network.[15] This change in strategy allows an adversary to avoid detection in the early phases of their attack by “blending in” with normal user behavior. This increases the chances of adversary actions being overlooked by cyber defenders and operators searching for malicious activity. Increasingly, the introduction of custom malware intended to disrupt ICS processes or cause physical impact is reserved for operations, post compromise.[16]

In contrast, the recent events from 2020 and 2021 illustrate the relative success of less sophisticated adversaries and techniques (ex. Ransomware) used in targeting ICS environments, highlighting a relative decrease in adversary sophistication. In its 2020 *ICS Threat Landscape Report for H2*, cybersecurity firm Kaspersky noted that while ransomware attacks targeting ICS computers dropped globally, the number of attacks targeting ICS computers increased in developed countries (ex. United States +0.25%). …” *these curious dynamics could indicate the response of threat actors to the economic consequences of the pandemic*...” Put simply, cybercriminals understand that economically stable organizations (AOOs) in developed countries, like the United States of America, can pay ransom.[17]

To identify tactics and techniques historically used by adversaries during cyberattacks targeting ICS, the CyOTE program leveraged events listed by MITRE on their website. Using MITRE’s analysis for mapping techniques to adversary actions, the CyOTE team analyzed seven historical events targeting ICS. Further analysis identified 19 malwares and 13 adversary groups that have or are actively targeting ICS. The below example highlights results from a Case Study analyzed and prepared by the CyOTE team.

Note: For scoring relating to specific attacks and techniques used by adversaries to target OT environments, see the scoring spreadsheets located in APPENDIX B

3.1.1 Sunburst Case Study Example Results

3.1.1.1 Overview

In December 2020, FireEye revealed details of a sophisticated threat actor (UNC2452)[e] which conducted a supply-chain compromise of a Dynamic Link Library (DLL) associated with a variety of SolarWinds Orion products designed to monitor and manage on-premise and hosted infrastructures.[18] The initial compromise of the supply-chain is assessed to have occurred in March 2020 and facilitated the abuse of legitimate accounts and the deployment of a backdoor called SUNBURST, affecting the U.S. Government, critical infrastructure, industrial organizations, utilities, and private sector organizations.[19] Additional actions allowed the threat actor to bypass multi-factor authentication, compromising Outlook Web Application (OWA), Azure, and M365. Persistence was maintained via the applications of a malicious binary which had a legitimate code signing certificate associated. The attack continues to impact organizations worldwide.[f20]

3.1.1.2 Techniques Used

T878 Alarm Suppression

T802 Automated Collection

T807 Command Line Interface

T885 Commonly Used Port

T884 Connection Proxy

T809 Data Destruction

T812 Default Credentials

T816 Device Restart/Shutdown

T820 Exploitation for Evasion

[e] The U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR).

[f] Additional information is available from the CISA website.

T866 External Remote Services

T872 Indicator Removal on Host

T849 Masquerading

T886 Remote Services

T846 Remote System Discovery

T853 Scripting

T869 Standard Application Layer Protocol

T862 Supply Chain Compromise

T863 User Execution

T859 Valid Accounts

3.1.2 Oldsmar Water Treatment Plant 2021

3.1.2.1 Overview

On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at the Oldsmar Water Treatment plant located in the U.S. The unidentified event(s) modified the SCADA system's software to increase the amount of sodium hydroxide (lye) used in the water treatment process. According to CISA, "*…plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change.*"[21]

3.1.2.2 Oldsmar Techniques Observed

T822 External Remote Services

T823 Graphical User Interface

T836 Modify Parameter

T859 Valid Accounts

3.1.3 DarkSide/Colonial 2021

3.1.3.1 Overview

On April 29, 2021 ransomware group Darkside gained access to Colonial Pipeline Company using legitimate credentials for an orphaned virtual private network (VPN) account. This provided attackers remote access to the company's computer network. In the early morning of May 7, 2021, a Colonial employee working in the control room observed a ransom note appear on a computer and reported to the operations supervisor who initiated the shut-down processes of the pipeline. The implications resulted in a loss of fuel across 18 states, negatively impacting countless people and industries on the East Coast of the United States, and the loss of 100 gigabits of data from Colonial networks. Presently, there is no indication that the attackers were able to access the OT network.[22]

3.1.3.2 Darkside/Colonial Techniques Observed

T878 Alarm Suppression

T807 Command-Line Interface

T885 Commonly Used Port

T884 Connection Proxy

T809 Data Destruction

T810 Data Historian Compromise

T811 Data from Information Repositories

T812 Default Credentials

T813 Denial of Control

T814 Denial of Service

T817 Drive-by Compromise

T818 Engineering Workstation Compromise

T871 Execution through API

T819 Exploit Public Facing Application

T866 Exploitation of Remote Services

T823 Graphical User Interface

T872 Indicator Removal on Host

T827 Loss of Control

T828 Loss of Productivity and Revenue

T829 Loss of View

T849 Masquerading

T838 Modify Alarm Settings

T834 Native API

T846 Remote System Discovery

T888 Remote System Information Discovery

T847 Replication Through Removable Media

T853 Scripting

T881 Service Stop

T856 Spearphishing Attachment

T869 Standard Application Layer Protocol

T882 Theft of Operational Information

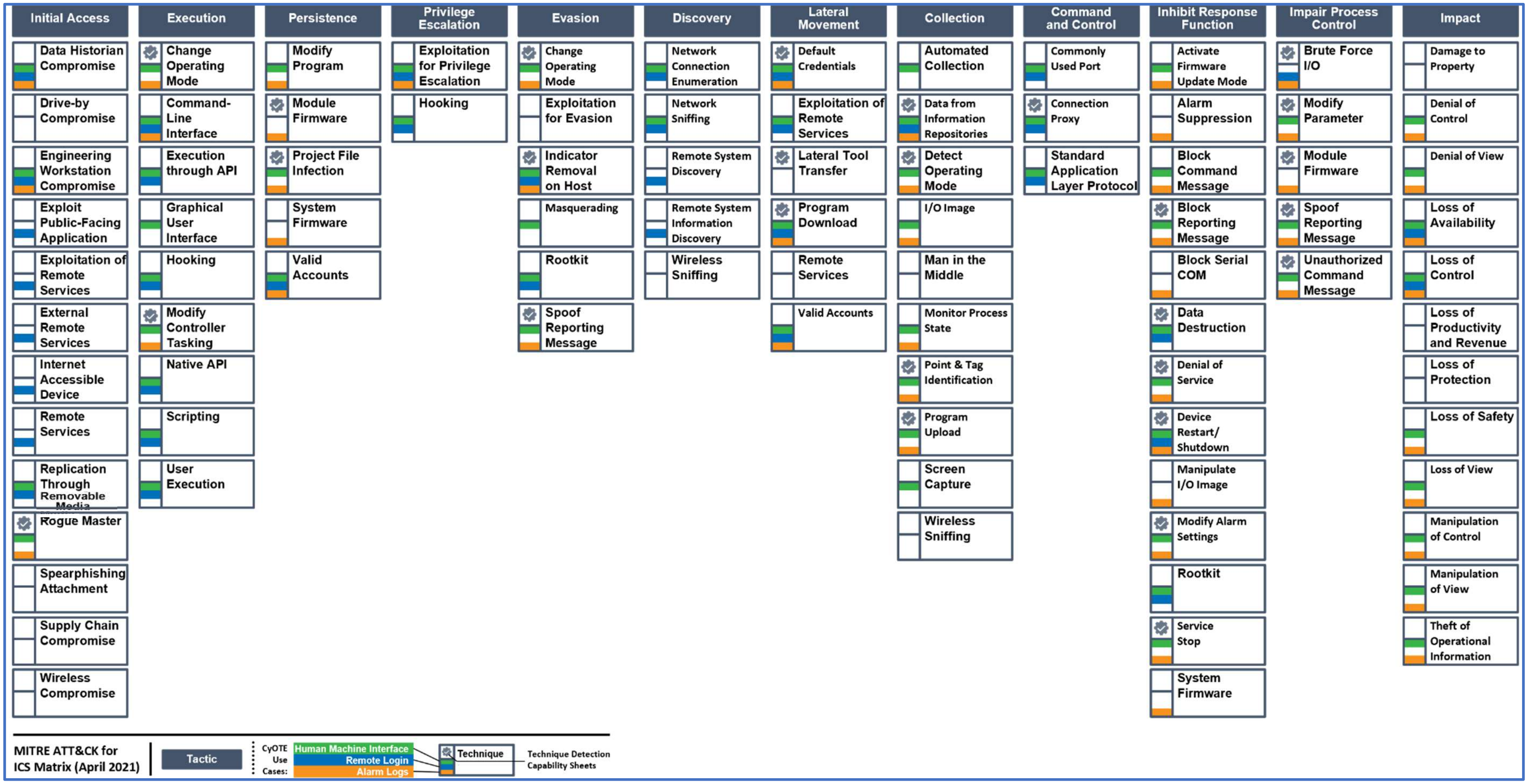
T863 User Execution

T859 Valid Accounts

3.2 APPLICATION OF TECHNIQUES TO INDUSTRY USE CASES

With regard to the application of Industry Use Cases, prioritization is based upon the applicability of the technique to one or more of the three industry Use Cases – HMI, Remote Login, and Alarm Logs. Increased priority is given to techniques that apply to all three Use Cases and reduced reflective to the application to fewer cases. Figure 4 highlights which of the 79 total techniques can potentially be observed by each of the three industry Use Cases. The results (APPENDIX B, Table 3) are 11 techniques can potentially be observed by all three Use Cases; 41 techniques can potentially be observed by two Use Cases; 16 techniques can potentially be observed by a single Use Case; and 11 techniques cannot be observed by any of the currently identified Industry Use Cases.

Note: The MITRE ATT&CK for ICS framework contains 89 techniques across 12 Tactics, 10 of the techniques are redundant and found in more than one tactic. This results in a total number of 79 unique techniques.



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
🟩🟦🟧 Data Historian Compromise	⚙ 🟩🟧 Change Operating Mode	🟩🟧 Modify Program	🟩🟦🟧 Exploitation for Privilege Escalation	⚙ 🟩🟧 Change Operating Mode	🟩🟦 Network Connection Enumeration	⚙ 🟩🟦🟧 Default Credentials	🟩 Automated Collection	🟩🟦 Commonly Used Port	🟩🟧 Activate Firmware Update Mode	⚙ 🟦🟧 Brute Force I/O	Damage to Property
Drive-by Compromise	🟩🟦🟧 Command-Line Interface	⚙ 🟧 Module Firmware	🟩🟦 Hooking	Exploitation for Evasion	🟩🟦 Network Sniffing	🟩🟦 Exploitation of Remote Services	⚙ 🟩🟦🟧 Data from Information Repositories	⚙ 🟩🟦 Connection Proxy	🟧 Alarm Suppression	⚙ 🟩🟧 Modify Parameter	🟩🟧 Denial of Control
🟩🟦🟧 Engineering Workstation Compromise	🟩🟦 Execution through API	⚙ 🟩🟧 Project File Infection		⚙ 🟩🟦🟧 Indicator Removal on Host	🟦 Remote System Discovery	⚙ Lateral Tool Transfer	⚙ 🟩🟧 Detect Operating Mode	🟩🟦 Standard Application Layer Protocol	🟩🟧 Block Command Message	⚙ 🟧 Module Firmware	🟩🟧 Denial of View
🟦 Exploit Public-Facing Application	🟩 Graphical User Interface	🟧 System Firmware		🟩 Masquerading	🟦 Remote System Information Discovery	⚙ 🟩🟦🟧 Program Download	🟩🟧 I/O Image		⚙ 🟩🟧 Block Reporting Message	⚙ 🟩🟧 Spoof Reporting Message	🟩🟦🟧 Loss of Availability
🟦 Exploitation of Remote Services	🟩🟦 Hooking	🟩🟦🟧 Valid Accounts		🟩🟦 Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		🟧 Block Serial COM	⚙ 🟩🟧 Unauthorized Command Message	🟩🟦🟧 Loss of Control
🟦 External Remote Services	⚙ 🟩🟧 Modify Controller Tasking			⚙ 🟩🟧 Spoof Reporting Message		🟩🟦🟧 Valid Accounts	🟩🟧 Monitor Process State		⚙ 🟩🟦 Data Destruction		Loss of Productivity and Revenue
🟦 Internet Accessible Device	🟩🟦 Native API						⚙ 🟩🟧 Point & Tag Identification		⚙ 🟩🟧 Denial of Service		Loss of Protection
🟦 Remote Services	🟩🟦 Scripting						⚙ 🟩🟧 Program Upload		⚙ 🟩🟦🟧 Device Restart/ Shutdown		🟩🟧 Loss of Safety
🟩🟦 Replication Through Removable Media	🟩🟦 User Execution						🟩 Screen Capture		🟧 Manipulate I/O Image		🟩🟧 Loss of View
⚙ 🟩🟧 Rogue Master							Wireless Sniffing		⚙ 🟩🟧 Modify Alarm Settings		🟩🟧 Manipulation of Control
Spearphishing Attachment									🟩🟦 Rootkit		🟩🟧 Manipulation of View
Supply Chain Compromise									⚙ 🟩🟧 Service Stop		🟩🟧 Theft of Operational Information
Wireless Compromise									🟧 System Firmware		

MITRE ATT&CK for ICS Matrix (April 2021) | Tactic | CyOTE Use Cases: 🟩 Human Machine Interface 🟦 Remote Login 🟧 Alarm Logs | ⚙ Technique — Technique Detection Capability Sheets

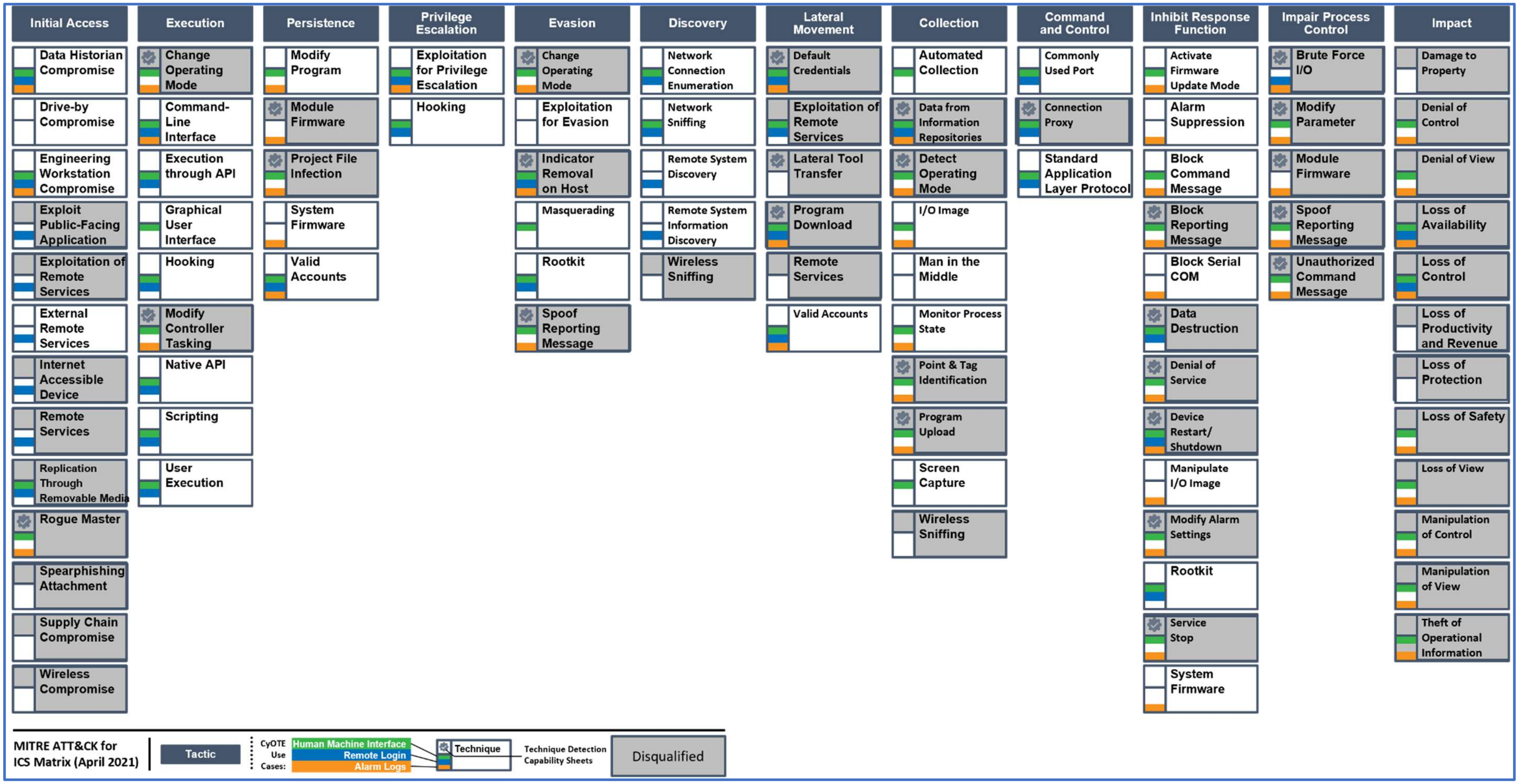
Figure 4 Application of Techniques to Industry Use Cases

3.3 MOVING AOO'S THREAT DETECTION CAPABILITIES EARLIER INTO AN ATTACK CAMPAIGN

The CyOTE program is focused on providing AOO's capabilities that support their ability to develop threat identification capability to independently identify indicators of attack within their OT networks. In prioritizing the techniques listed in the MITRE ATT&CK ICS Framework the following evaluation criteria was also applied:

- Techniques which have been realized as achieved in FY21 via Technique Detection Capability Sheet [27]
- Techniques which do not support the AOO's understanding of OT data to make better risk-informed decisions to secure their OT environments (i.e. the Impact tactic) [12]
- Techniques which do not have dependencies for OT infrastructure components, functions, or systems (Ex. Supply chain compromise) [9]

This analysis resulted in the removal of 45 techniques from current consideration out of a total 79 techniques shown in Figure 5 of the MITRE ATT&CK for ICS framework.



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Figure 5 Application of Techniques to CyOTE Program Requirements

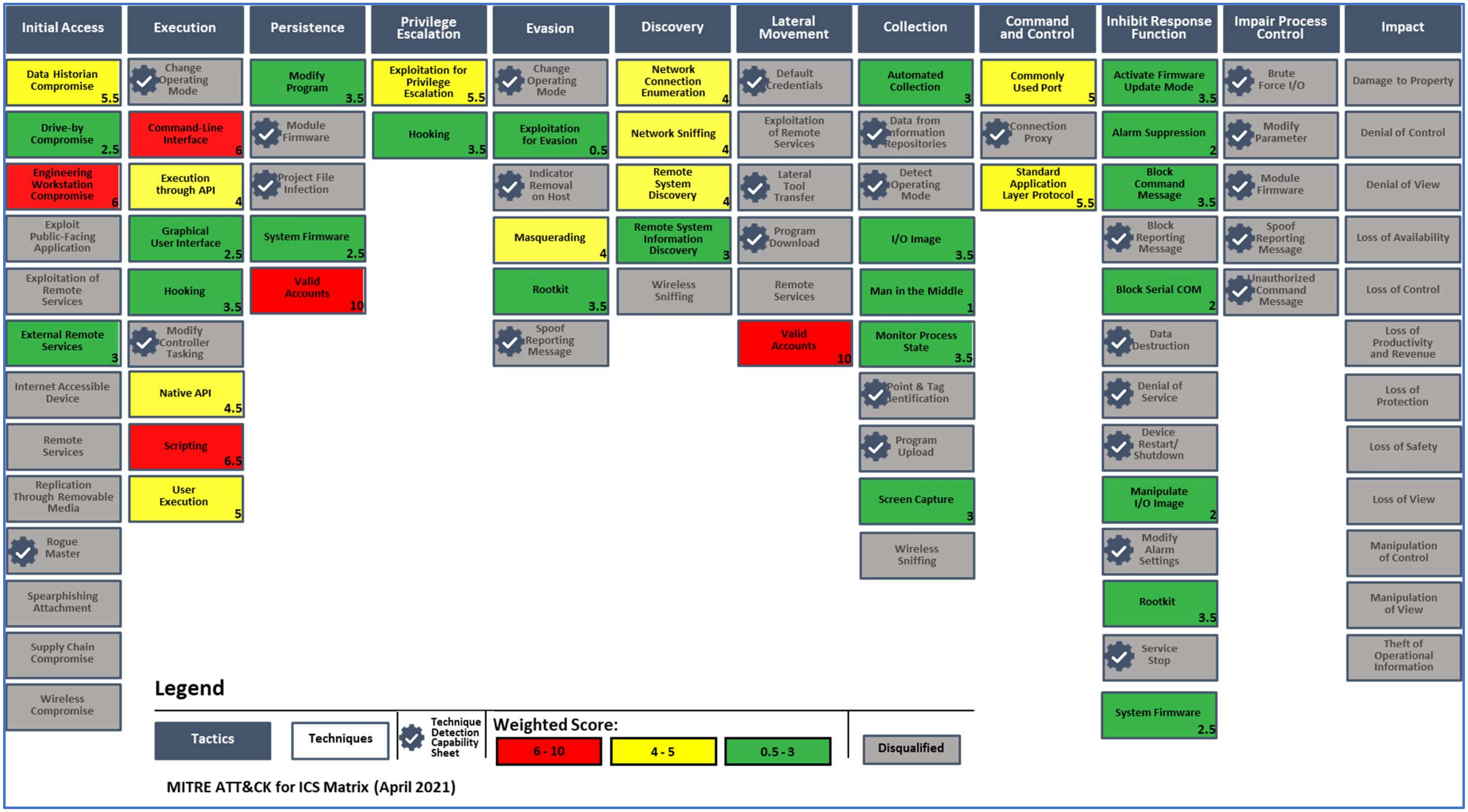
4 ANALYSIS

An analysis of the data and constraints identified in Sections 2 and 3 resulted in the creation of an excel document (APPENDIX B) where the CyOTE team calculated weighted scores using the analytic framework referenced in Section 3 to refine the techniques. Then, the CyOTE team applied the techniques to the industry Use Cases in Section 1.1, which identified technique applicability to individual Use Cases and prioritized those techniques based on a decreasing scale. Next, the techniques were applied to the CyOTE program requirements from section 3.3. This enabled the identification of techniques to be removed from current consideration based on the criteria.

Figure 6 shows an overlay of technique prioritization results discussed in this paper. This overlay is designed to highlight commonalities in each of the aspects of the analysis performed. Based on this synthesis, the analysis team recommends the highlighted techniques, as shown in in Figure 6, be considered for future CyOTE analysis. This resulted in the creation of a prioritized list containing 34 techniques for the CyOTE Program*

- Valid Accounts
- Scripting
- Command-Line Interface
- Engineering Workstation Compromise
- Data Historian Compromise
- Exploitation for Privilege Escalation
- Standard Application Layer Protocol
- Commonly Used Port
- User Execution
- Native API
- Network Connection Enumeration
- Network Sniffing
- Masquerading
- Execution through API
- Remote System Discovery
- Monitor Process State
- Block Command Message
- Hooking
- Activate Firmware Update Mode
- I/O Image
- Modify Program
- Rootkit
- Remote System Information Discovery
- Automated Collection
- Screen Capture
- External Remote Services
- Drive-by Compromise
- Graphical User Interface
- System Firmware
- Alarm Suppression
- Manipulate I/O Image
- Block Serial COM
- Man in the Middle
- Exploitation for Evasion

*See APPENDIX B, Table 5 for detailed prioritization information



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise 5.5	✓ Change Operating Mode	Modify Program 3.5	Exploitation for Privilege Escalation 5.5	✓ Change Operating Mode	Network Connection Enumeration 4	✓ Default Credentials	Automated Collection 3	Commonly Used Port 5	Activate Firmware Update Mode 3.5	✓ Brute Force I/O	Damage to Property
Drive-by Compromise 2.5	Command-Line Interface 6	✓ Module Firmware	Hooking 3.5	Exploitation for Evasion 0.5	Network Sniffing 4	Exploitation of Remote Services	✓ Data from Information Repositories	✓ Connection Proxy	Alarm Suppression 2	✓ Modify Parameter	Denial of Control
Engineering Workstation Compromise 6	Execution through API 4	✓ Project File Infection		✓ Indicator Removal on Host	Remote System Discovery 4	✓ Lateral Tool Transfer	✓ Detect Operating Mode	Standard Application Layer Protocol 5.5	Block Command Message 3.5	✓ Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface 2.5	System Firmware 2.5		Masquerading 4	Remote System Information Discovery 3	✓ Program Download	I/O Image 3.5		✓ Block Reporting Message	✓ Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking 3.5	Valid Accounts 10		Rootkit 3.5	Wireless Sniffing	Remote Services	Man in the Middle 1		Block Serial COM 2	✓ Unauthorized Command Message	Loss of Control
External Remote Services 3	✓ Modify Controller Tasking			✓ Spoof Reporting Message		Valid Accounts 10	Monitor Process State 3.5		✓ Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API 4.5						✓ Point & Tag Identification		✓ Denial of Service		Loss of Protection
Remote Services	Scripting 6.5						✓ Program Upload		✓ Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution 5						Screen Capture 3		Manipulate I/O Image 2		Loss of View
✓ Rogue Master							Wireless Sniffing		✓ Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit 3.5		Manipulation of View
Supply Chain Compromise									✓ Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware 2.5		

Legend

Tactics | Techniques | ✓ Technique Detection Capability Sheet | Weighted Score: 🟥 6 - 10 🟨 4 - 5 🟩 0.5 - 3 | Disqualified

MITRE ATT&CK for ICS Matrix (April 2021)

Figure 6 Final Scoring of Techniques

5 CONCLUSION

From the information contained in Sections 2-3.3 and the resulting analysis in Section 4, the CyOTE program prioritized and identified 34 techniques that would assist AOO's to improve their understanding of OT data to make better risk-informed decisions. This paper supports this endeavor by prioritizing identified techniques used by adversaries during cyberattacks, applying the three industry Use Cases, and evaluating these techniques based on improving the AOO's risk decision making by moving AOO's threat detection capabilities earlier into an attack campaign. Through synthesizing these sources, this paper outlined the process for prioritizing techniques for development consideration supporting ongoing and future CyOTE efforts.

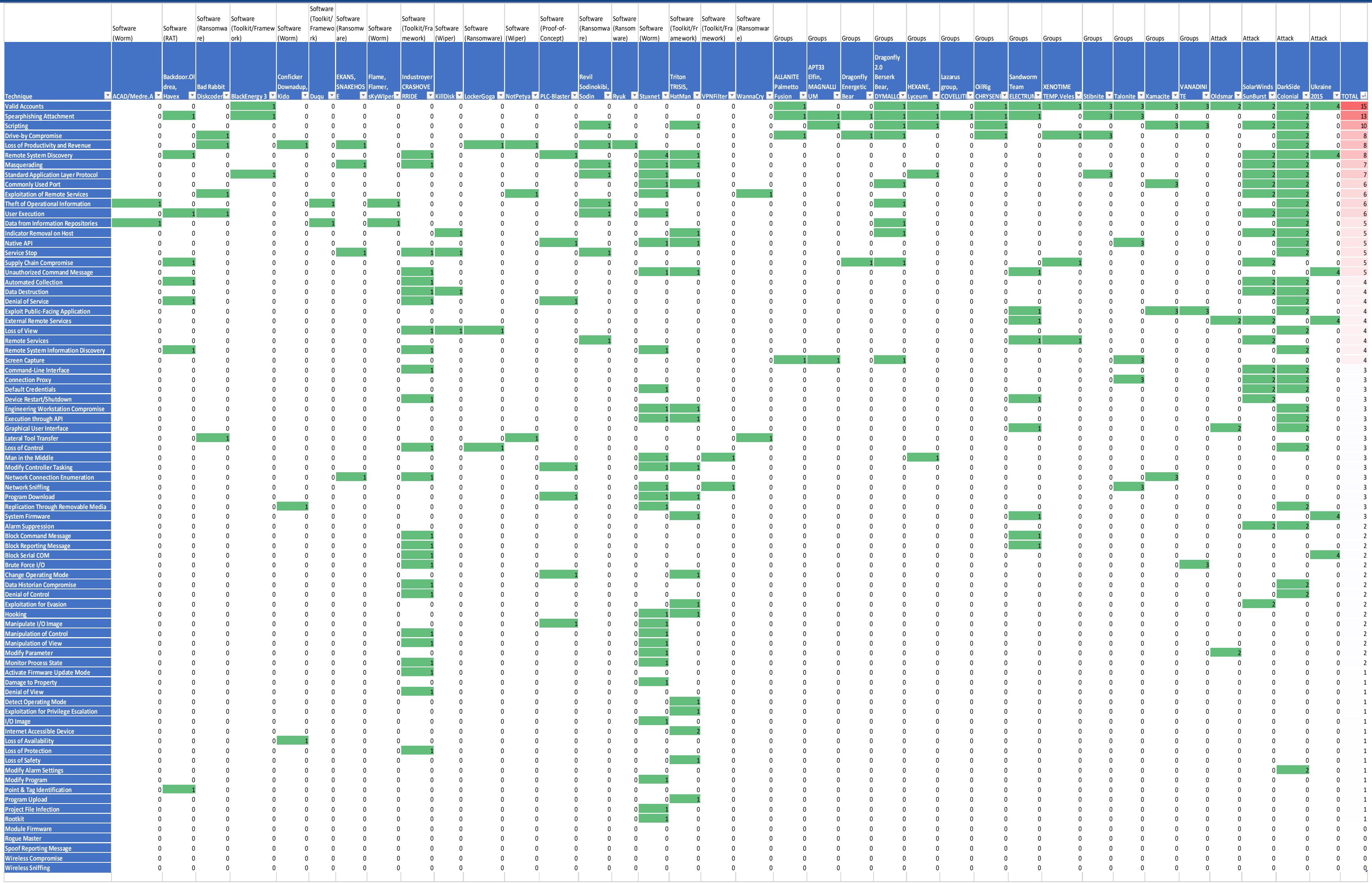
6 APPENDIX A: CYOTE SUBJECT MATTER EXPERT KEY FINDINGS

CyOTE researchers engaged with participating AOOs via interviews and Working Group sessions to identify techniques of industry concern. This process resulted in the following summary of findings:

- IT/OT networks contain similar operating systems and present similar vulnerabilities
- The abuse of native system functionality obfuscates detection requiring increased detection and identification of anomalous observables and technique specific detection capabilities
- Selection is impacted by existing available tools to detect specific techniques in OT environments
- Selection of techniques is dependent upon the availability of resources
- Identification of supply chain compromise of hardware is outside of the CyOTE scope and current capabilities
- Visibility gaps based on AOO criticality and technique correlation is essential to prioritization and selection of capability development efforts
- Identification and monitoring of “choke points” reduces risk and likely vectors of compromise
- Development of common techniques used across attacks increase likelihood of detection
- Focus should be within the borders of the OT environment, between Initial Access and Impact
- Application of detection capabilities in concert with the CyOTE methodology enables faster perception and comprehension of anomalies resulting in more agile risk decisions and risk reduction

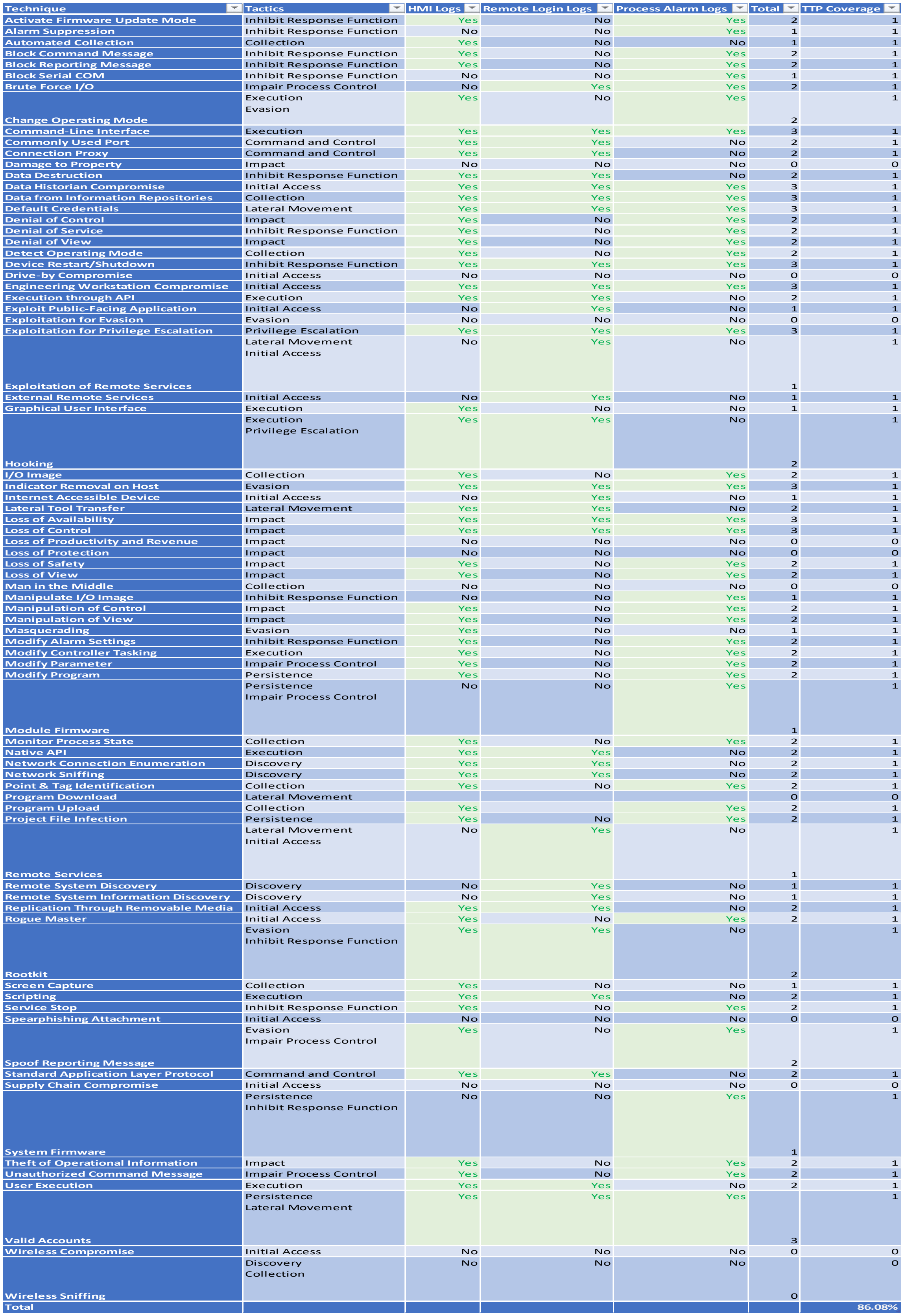
7 APPENDIX B

The following are scoring spreadsheets, which are used during the technique prioritization process to 1) identify MITRE ATT&CK for ICS techniques used by adversaries during cyberattacks and the frequency of use; 2) apply techniques to industry Use Cases; 3) apply remaining techniques to current disqualifiers. The resulting output is a list of prioritized techniques for the CyOTE program (Table 5).



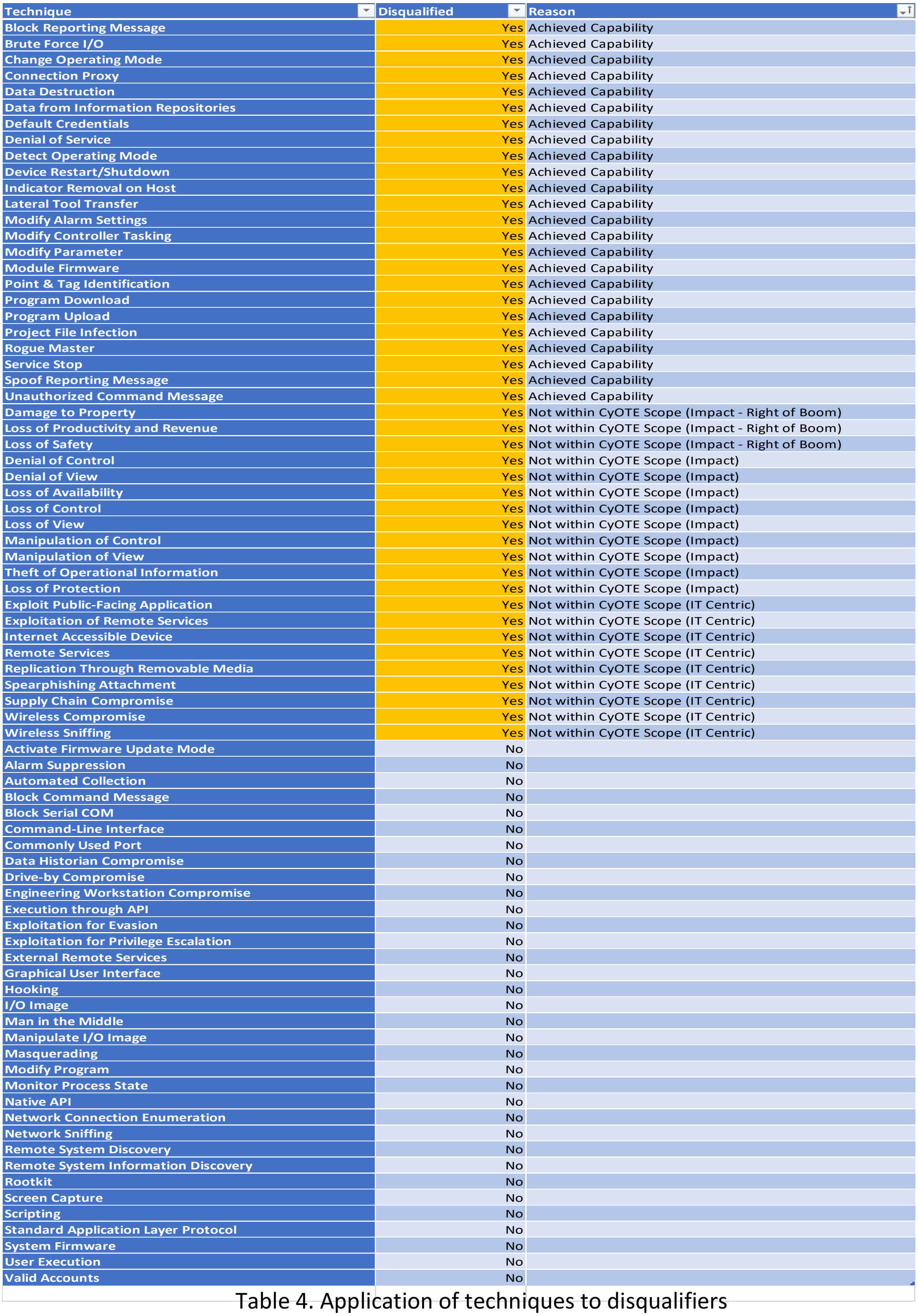
	Software (Worm)	Software (RAT)	Software (Ransomware)	Software (Toolkit/Framework)	Software (Worm)	Software (Toolkit/Framework)	Software (Ransomware)	Software (Worm)	Software (Toolkit/Framework)	Software (Wiper)	Software (Ransomware)	Software (Wiper)	Software (Proof-of-Concept)	Software (Ransomware)	Software (Ransomware)	Software (Worm)	Software (Toolkit/Framework)	Software (Toolkit/Framework)	Software (Ransomware)	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Groups	Attack	Attack	Attack	Attack	
Technique	ACAD/Medre.A	Backdoor.Oldrea, Havex	Bad Rabbit Diskcoder	BlackEnergy 3	Conficker Downadup, Kido	Duqu	EKANS, SNAKEHOSE	Flame, Flamer, sKyWIper	Industroyer CRASHOVERRIDE	KillDisk	LockerGoga	NotPetya	PLC-Blaster	Revil Sodinokibi, Sodin	Ryuk	Stuxnet	Triton TRISIS, HatMan	VPNFilter	WannaCry	ALLANITE Palmetto Fusion	APT33 Elfin, MAGNALLIUM	Dragonfly Energetic Bear	Dragonfly 2.0 Berserk Bear, DYMALLC	HEXANE, Lyceum	Lazarus group, COVELLITE	OilRig CHRYSENE	Sandworm Team ELECTRUM	XENOTIME TEMP.Veles	Stibnite	Talonite	Kamacite	VANADINITE	Oldsmar	SolarWinds SunBurst	DarkSide Colonial	Ukraine 2015	TOTAL
Valid Accounts	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	3	3	3	3	2	2	2	4	15
Spearphishing Attachment	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	3	3	0	0	0	0	2	0	13
Scripting	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	1	1	0	1	0	0	0	0	3	3	0	2	2	0	10
Drive-by Compromise	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	1	3	0	0	0	0	0	2	0	8
Loss of Productivity and Revenue	0	0	1	0	1	0	1	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	8
Remote System Discovery	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	4	8
Masquerading	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	7
Standard Application Layer Protocol	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	3	0	0	0	0	2	2	0	7
Commonly Used Port	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	3	0	0	2	2	0	6
Exploitation of Remote Services	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	6
Theft of Operational Information	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	0	6
User Execution	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	6
Data from Information Repositories	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	0	5
Indicator Removal on Host	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	2	0	5
Native API	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	2	0	5
Service Stop	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	5
Supply Chain Compromise	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	2	0	0	5
Unauthorized Command Message	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	4	5
Automated Collection	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	4
Data Destruction	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	4
Denial of Service	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	4
Exploit Public-Facing Application	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	3	0	0	2	0	4
External Remote Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	2	0	4	4
Loss of View	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	4
Remote Services	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	2	0	0	4
Remote System Information Discovery	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	4
Screen Capture	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	3	0	0	0	0	0	0	4
Command-Line Interface	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	3
Connection Proxy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	2	2	0	3
Default Credentials	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	3
Device Restart/Shutdown	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	2	0	0	3
Engineering Workstation Compromise	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	3
Execution through API	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	3
Graphical User Interface	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	0	2	0	3
Lateral Tool Transfer	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
Loss of Control	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	3
Man in the Middle	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3
Modify Controller Tasking	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
Network Connection Enumeration	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	3
Network Sniffing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	3
Program Download	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
Replication Through Removable Media	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	3
System Firmware	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	4	3
Alarm Suppression	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	2
Block Command Message	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2
Block Reporting Message	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2
Block Serial COM	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2
Brute Force I/O	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	2
Change Operating Mode	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Data Historian Compromise	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	2
Denial of Control	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	2
Exploitation for Evasion	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
Hooking	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Manipulate I/O Image	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Manipulation of Control	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Manipulation of View	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Modify Parameter	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
Monitor Process State	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Activate Firmware Update Mode	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Damage to Property	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Denial of View	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Detect Operating Mode	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Exploitation for Privilege Escalation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I/O Image	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Internet Accessible Device	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Loss of Availability	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Loss of Protection	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Loss of Safety	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Modify Alarm Settings	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1
Modify Program	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Point & Tag Identification	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Program Upload	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Project File Infection	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Rootkit	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Module Firmware	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rogue Master	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Spoof Reporting Message	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wireless Compromise	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wireless Sniffing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 2. MITRE-identified techniques used by adversaries during cyberattacks and frequency of use.



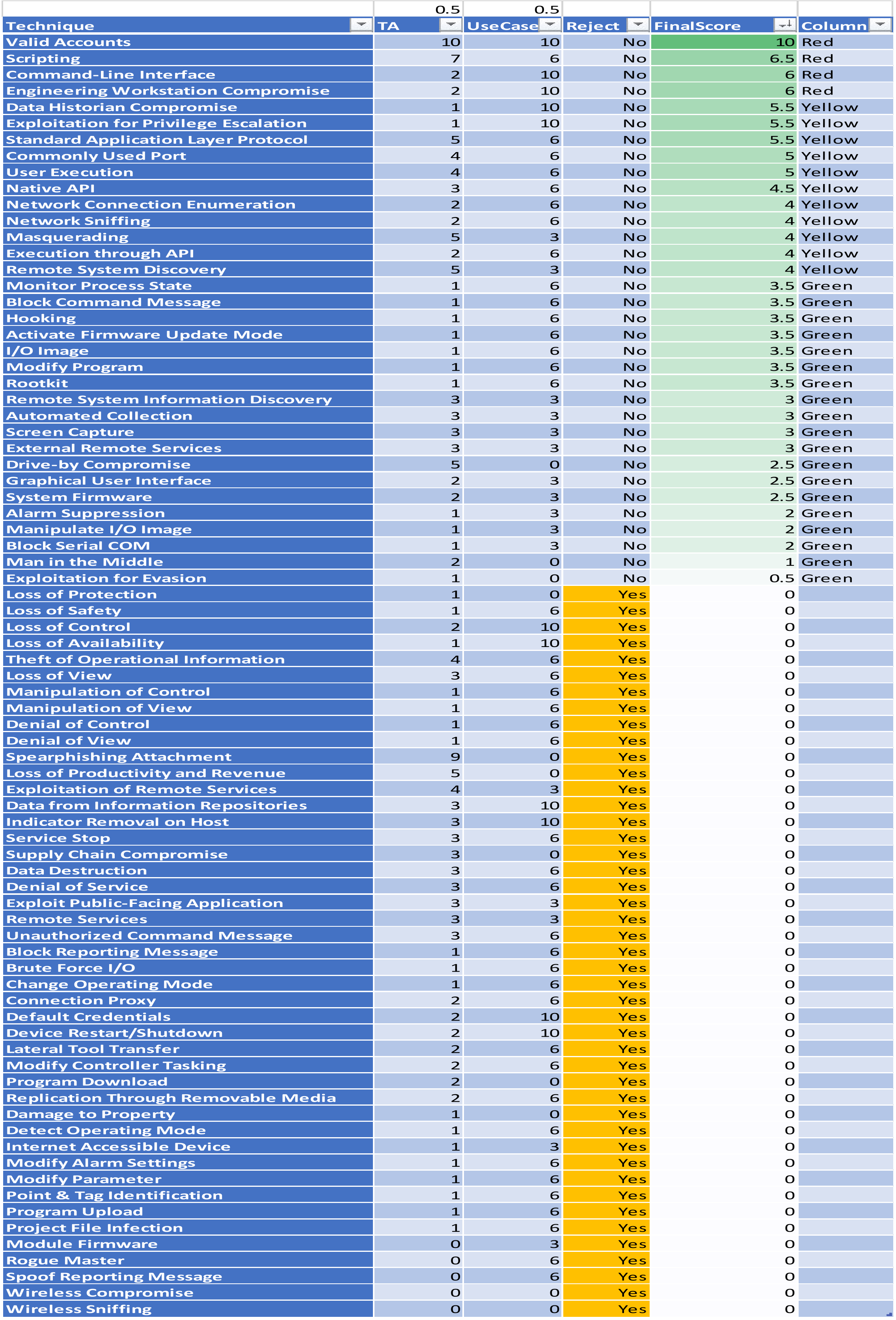
Technique	Tactics	HMI Logs	Remote Login Logs	Process Alarm Logs	Total	TTP Coverage
Activate Firmware Update Mode	Inhibit Response Function	Yes	No	Yes	2	1
Alarm Suppression	Inhibit Response Function	No	No	Yes	1	1
Automated Collection	Collection	Yes	No	No	1	1
Block Command Message	Inhibit Response Function	Yes	No	Yes	2	1
Block Reporting Message	Inhibit Response Function	Yes	No	Yes	2	1
Block Serial COM	Inhibit Response Function	No	No	Yes	1	1
Brute Force I/O	Impair Process Control	No	Yes	Yes	2	1
Change Operating Mode	Execution Evasion	Yes	No	Yes	2	1
Command-Line Interface	Execution	Yes	Yes	Yes	3	1
Commonly Used Port	Command and Control	Yes	Yes	No	2	1
Connection Proxy	Command and Control	Yes	Yes	No	2	1
Damage to Property	Impact	No	No	No	0	0
Data Destruction	Inhibit Response Function	Yes	Yes	No	2	1
Data Historian Compromise	Initial Access	Yes	Yes	Yes	3	1
Data from Information Repositories	Collection	Yes	Yes	Yes	3	1
Default Credentials	Lateral Movement	Yes	Yes	Yes	3	1
Denial of Control	Impact	Yes	No	Yes	2	1
Denial of Service	Inhibit Response Function	Yes	No	Yes	2	1
Denial of View	Impact	Yes	No	Yes	2	1
Detect Operating Mode	Collection	Yes	No	Yes	2	1
Device Restart/Shutdown	Inhibit Response Function	Yes	Yes	Yes	3	1
Drive-by Compromise	Initial Access	No	No	No	0	0
Engineering Workstation Compromise	Initial Access	Yes	Yes	Yes	3	1
Execution through API	Execution	Yes	Yes	No	2	1
Exploit Public-Facing Application	Initial Access	No	Yes	No	1	1
Exploitation for Evasion	Evasion	No	No	No	0	0
Exploitation for Privilege Escalation	Privilege Escalation	Yes	Yes	Yes	3	1
Exploitation of Remote Services	Lateral Movement Initial Access	No	Yes	No	1	1
External Remote Services	Initial Access	No	Yes	No	1	1
Graphical User Interface	Execution	Yes	No	No	1	1
Hooking	Execution Privilege Escalation	Yes	Yes	No	2	1
I/O Image	Collection	Yes	No	Yes	2	1
Indicator Removal on Host	Evasion	Yes	Yes	Yes	3	1
Internet Accessible Device	Initial Access	No	Yes	No	1	1
Lateral Tool Transfer	Lateral Movement	Yes	Yes	No	2	1
Loss of Availability	Impact	Yes	Yes	Yes	3	1
Loss of Control	Impact	Yes	Yes	Yes	3	1
Loss of Productivity and Revenue	Impact	No	No	No	0	0
Loss of Protection	Impact	No	No	No	0	0
Loss of Safety	Impact	Yes	No	Yes	2	1
Loss of View	Impact	Yes	No	Yes	2	1
Man in the Middle	Collection	No	No	No	0	0
Manipulate I/O Image	Inhibit Response Function	No	No	Yes	1	1
Manipulation of Control	Impact	Yes	No	Yes	2	1
Manipulation of View	Impact	Yes	No	Yes	2	1
Masquerading	Evasion	Yes	No	No	1	1
Modify Alarm Settings	Inhibit Response Function	Yes	No	Yes	2	1
Modify Controller Tasking	Execution	Yes	No	Yes	2	1
Modify Parameter	Impair Process Control	Yes	No	Yes	2	1
Modify Program	Persistence	Yes	No	Yes	2	1
Module Firmware	Persistence Impair Process Control	No	No	Yes	1	1
Monitor Process State	Collection	Yes	No	Yes	2	1
Native API	Execution	Yes	Yes	No	2	1
Network Connection Enumeration	Discovery	Yes	Yes	No	2	1
Network Sniffing	Discovery	Yes	Yes	No	2	1
Point & Tag Identification	Collection	Yes	No	Yes	2	1
Program Download	Lateral Movement				0	0
Program Upload	Collection	Yes		Yes	2	1
Project File Infection	Persistence	Yes	No	Yes	2	1
Remote Services	Lateral Movement Initial Access	No	Yes	No	1	1
Remote System Discovery	Discovery	No	Yes	No	1	1
Remote System Information Discovery	Discovery	No	Yes	No	1	1
Replication Through Removable Media	Initial Access	Yes	Yes	No	2	1
Rogue Master	Initial Access	Yes	No	Yes	2	1
Rootkit	Evasion Inhibit Response Function	Yes	Yes	No	2	1
Screen Capture	Collection	Yes	No	No	1	1
Scripting	Execution	Yes	Yes	No	2	1
Service Stop	Inhibit Response Function	Yes	No	Yes	2	1
Spearphishing Attachment	Initial Access	No	No	No	0	0
Spoof Reporting Message	Evasion Impair Process Control	Yes	No	Yes	2	1
Standard Application Layer Protocol	Command and Control	Yes	Yes	No	2	1
Supply Chain Compromise	Initial Access	No	No	No	0	0
System Firmware	Persistence Inhibit Response Function	No	No	Yes	1	1
Theft of Operational Information	Impact	Yes	No	Yes	2	1
Unauthorized Command Message	Impair Process Control	Yes	No	Yes	2	1
User Execution	Execution	Yes	Yes	No	2	1
Valid Accounts	Persistence Lateral Movement	Yes	Yes	Yes	3	1
Wireless Compromise	Initial Access	No	No	No	0	0
Wireless Sniffing	Discovery Collection	No	No	No	0	0
Total						86.08%

Table 3. Application of techniques to industry Use Cases.



Technique	Disqualified	Reason
Block Reporting Message	Yes	Achieved Capability
Brute Force I/O	Yes	Achieved Capability
Change Operating Mode	Yes	Achieved Capability
Connection Proxy	Yes	Achieved Capability
Data Destruction	Yes	Achieved Capability
Data from Information Repositories	Yes	Achieved Capability
Default Credentials	Yes	Achieved Capability
Denial of Service	Yes	Achieved Capability
Detect Operating Mode	Yes	Achieved Capability
Device Restart/Shutdown	Yes	Achieved Capability
Indicator Removal on Host	Yes	Achieved Capability
Lateral Tool Transfer	Yes	Achieved Capability
Modify Alarm Settings	Yes	Achieved Capability
Modify Controller Tasking	Yes	Achieved Capability
Modify Parameter	Yes	Achieved Capability
Module Firmware	Yes	Achieved Capability
Point & Tag Identification	Yes	Achieved Capability
Program Download	Yes	Achieved Capability
Program Upload	Yes	Achieved Capability
Project File Infection	Yes	Achieved Capability
Rogue Master	Yes	Achieved Capability
Service Stop	Yes	Achieved Capability
Spoof Reporting Message	Yes	Achieved Capability
Unauthorized Command Message	Yes	Achieved Capability
Damage to Property	Yes	Not within CyOTE Scope (Impact - Right of Boom)
Loss of Productivity and Revenue	Yes	Not within CyOTE Scope (Impact - Right of Boom)
Loss of Safety	Yes	Not within CyOTE Scope (Impact - Right of Boom)
Denial of Control	Yes	Not within CyOTE Scope (Impact)
Denial of View	Yes	Not within CyOTE Scope (Impact)
Loss of Availability	Yes	Not within CyOTE Scope (Impact)
Loss of Control	Yes	Not within CyOTE Scope (Impact)
Loss of View	Yes	Not within CyOTE Scope (Impact)
Manipulation of Control	Yes	Not within CyOTE Scope (Impact)
Manipulation of View	Yes	Not within CyOTE Scope (Impact)
Theft of Operational Information	Yes	Not within CyOTE Scope (Impact)
Loss of Protection	Yes	Not within CyOTE Scope (Impact)
Exploit Public-Facing Application	Yes	Not within CyOTE Scope (IT Centric)
Exploitation of Remote Services	Yes	Not within CyOTE Scope (IT Centric)
Internet Accessible Device	Yes	Not within CyOTE Scope (IT Centric)
Remote Services	Yes	Not within CyOTE Scope (IT Centric)
Replication Through Removable Media	Yes	Not within CyOTE Scope (IT Centric)
Spearphishing Attachment	Yes	Not within CyOTE Scope (IT Centric)
Supply Chain Compromise	Yes	Not within CyOTE Scope (IT Centric)
Wireless Compromise	Yes	Not within CyOTE Scope (IT Centric)
Wireless Sniffing	Yes	Not within CyOTE Scope (IT Centric)
Activate Firmware Update Mode	No	
Alarm Suppression	No	
Automated Collection	No	
Block Command Message	No	
Block Serial COM	No	
Command-Line Interface	No	
Commonly Used Port	No	
Data Historian Compromise	No	
Drive-by Compromise	No	
Engineering Workstation Compromise	No	
Execution through API	No	
Exploitation for Evasion	No	
Exploitation for Privilege Escalation	No	
External Remote Services	No	
Graphical User Interface	No	
Hooking	No	
I/O Image	No	
Man in the Middle	No	
Manipulate I/O Image	No	
Masquerading	No	
Modify Program	No	
Monitor Process State	No	
Native API	No	
Network Connection Enumeration	No	
Network Sniffing	No	
Remote System Discovery	No	
Remote System Information Discovery	No	
Rootkit	No	
Screen Capture	No	
Scripting	No	
Standard Application Layer Protocol	No	
System Firmware	No	
User Execution	No	
Valid Accounts	No	

Table 4. Application of techniques to disqualifiers



	0.5	0.5			
Technique	TA	UseCase	Reject	FinalScore	Column
Valid Accounts	10	10	No	10	Red
Scripting	7	6	No	6.5	Red
Command-Line Interface	2	10	No	6	Red
Engineering Workstation Compromise	2	10	No	6	Red
Data Historian Compromise	1	10	No	5.5	Yellow
Exploitation for Privilege Escalation	1	10	No	5.5	Yellow
Standard Application Layer Protocol	5	6	No	5.5	Yellow
Commonly Used Port	4	6	No	5	Yellow
User Execution	4	6	No	5	Yellow
Native API	3	6	No	4.5	Yellow
Network Connection Enumeration	2	6	No	4	Yellow
Network Sniffing	2	6	No	4	Yellow
Masquerading	5	3	No	4	Yellow
Execution through API	2	6	No	4	Yellow
Remote System Discovery	5	3	No	4	Yellow
Monitor Process State	1	6	No	3.5	Green
Block Command Message	1	6	No	3.5	Green
Hooking	1	6	No	3.5	Green
Activate Firmware Update Mode	1	6	No	3.5	Green
I/O Image	1	6	No	3.5	Green
Modify Program	1	6	No	3.5	Green
Rootkit	1	6	No	3.5	Green
Remote System Information Discovery	3	3	No	3	Green
Automated Collection	3	3	No	3	Green
Screen Capture	3	3	No	3	Green
External Remote Services	3	3	No	3	Green
Drive-by Compromise	5	0	No	2.5	Green
Graphical User Interface	2	3	No	2.5	Green
System Firmware	2	3	No	2.5	Green
Alarm Suppression	1	3	No	2	Green
Manipulate I/O Image	1	3	No	2	Green
Block Serial COM	1	3	No	2	Green
Man in the Middle	2	0	No	1	Green
Exploitation for Evasion	1	0	No	0.5	Green
Loss of Protection	1	0	Yes	0	
Loss of Safety	1	6	Yes	0	
Loss of Control	2	10	Yes	0	
Loss of Availability	1	10	Yes	0	
Theft of Operational Information	4	6	Yes	0	
Loss of View	3	6	Yes	0	
Manipulation of Control	1	6	Yes	0	
Manipulation of View	1	6	Yes	0	
Denial of Control	1	6	Yes	0	
Denial of View	1	6	Yes	0	
Spearphishing Attachment	9	0	Yes	0	
Loss of Productivity and Revenue	5	0	Yes	0	
Exploitation of Remote Services	4	3	Yes	0	
Data from Information Repositories	3	10	Yes	0	
Indicator Removal on Host	3	10	Yes	0	
Service Stop	3	6	Yes	0	
Supply Chain Compromise	3	0	Yes	0	
Data Destruction	3	6	Yes	0	
Denial of Service	3	6	Yes	0	
Exploit Public-Facing Application	3	3	Yes	0	
Remote Services	3	3	Yes	0	
Unauthorized Command Message	3	6	Yes	0	
Block Reporting Message	1	6	Yes	0	
Brute Force I/O	1	6	Yes	0	
Change Operating Mode	1	6	Yes	0	
Connection Proxy	2	6	Yes	0	
Default Credentials	2	10	Yes	0	
Device Restart/Shutdown	2	10	Yes	0	
Lateral Tool Transfer	2	6	Yes	0	
Modify Controller Tasking	2	6	Yes	0	
Program Download	2	0	Yes	0	
Replication Through Removable Media	2	6	Yes	0	
Damage to Property	1	0	Yes	0	
Detect Operating Mode	1	6	Yes	0	
Internet Accessible Device	1	3	Yes	0	
Modify Alarm Settings	1	6	Yes	0	
Modify Parameter	1	6	Yes	0	
Point & Tag Identification	1	6	Yes	0	
Program Upload	1	6	Yes	0	
Project File Infection	1	6	Yes	0	
Module Firmware	0	3	Yes	0	
Rogue Master	0	6	Yes	0	
Spoof Reporting Message	0	6	Yes	0	
Wireless Compromise	0	0	Yes	0	
Wireless Sniffing	0	0	Yes	0	

Table 5. Prioritized list of Techniques

8 REFERENCES

[1]MITRE. "ATT&CK for Industrial Control Systems (ICS)." Online. June 11, 2021. https://collaborate.mitre.org/attackics/index.php/Main_Page.

[2] CYOTE. "Methodology for Cybersecurity in Operational Technology Environments." 25 June 2021. https://inl.gov/wp-content/uploads/2021/07/CyOTE-Methodology-20210625-final.pdf

[3] INL. "Intrusion Detection Systems and Sensors for Operational Technology Environments." MSC. March 2017.

[4] MITRE. "Overview." MITRE Partnership Network. 16 June 2021. https://collaborate.mitre.org/attackics/index.php/Overview.

[5] Ibid

[6] MITRE. "Techniques." MITRE Partnership Network. Accessed 22 June 2021. https://collaborate.mitre.org/attackics/index.php/All_Techniques.

[7] Ibid.

[8] MITRE. "ATT&CK for Industrial Control Systems (ICS)." Online. June 11, 2021. https://collaborate.mitre.org/attackics/index.php/Main_Page.

[9] MITRE. "Techniques." MITRE. Online. June 11, 2021. https://collaborate.mitre.org/attackics/index.php/All_Techniques.

[10] MITRE, "Technique Matrix." MITRE Partnership Network. 16 June 2021. https://collaborate.mitre.org/attackics/index.php/Technique_Matrix

[11] Maggino, Filomena and Elena Ruviglioni. "*Obtaining Weights: F*rom objective to subjective approaches in view of more participative methods in the construction of composite indicators." European Union. Online. July 18, 2021. https://ec.europa.eu/eurostat/documents/1001617/4398464/POSTER-1A-OBTAINING-WEIGHTS-MAGGINO-RUVIGLIONI.pdf.

[12] DOE. "Threat-Informed Tactic, Technique, and Procedure Prioritization Report." CYOTE. July 31, 2019.

[13] Derek R. Harp and Bengt Gregory-Brown. "IT/OT Convergence: Bridging the Divide." SANS Institute. Online. Accessed July 28, 2019. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

[14] Joseph Slowik. "Evolution of ICS Attacks and the Prospects for Future Disruptive Events." Dragos Inc. Online. February 25, 2019. Accessed July 28, 2019. https://dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

[15] Michael J. Assante and Robert M. Lee. "The Industrial Control System Cyber Kill Chain." SANS Institute. Online. Accessed July 28, 2019. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

[16] Joseph Slowik. "Evolution of ICS Attacks and the Prospects for Future Disruptive Events."

[17] Security Affairs. Pierluigi Paganini. "33.4% of ICS Computers Hit by a Cyberattack in H2 2020." April 5, 2021. https://securityaffairs.co/wordpress/116360/ics-scada/ics-statistics-data.html. August 16, 2021.

[18] CISA. "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." April 15, 2021. Alert AA20-352A. https://www.us-cert.cisa.gov/ncas/alerts/aa20-352a. July 17, 2021.

[19] Security week. Eduard Kovacs. "Hundreds of Industrial Organizations Received Sunburst Malware in SolarWinds Attack." January 27, 2021. https://www.securityweek.com/hundreds-industrial-organizations-received-sunburst-malware-solarwinds-attack.

[20] FireEye. Bromiley, M., Rector, A., and Robert Wallace. "Light in the Dark: Hunting for SUNBURST." February 16, 2021. https://www.fireeye.com/blog/products-and-services/2021/02/light-in-the-dark-hunting-for-sunburst.html.

[21] CISA. "Compromise of U.S. Water Treatment Facility." Alert AA21-042A. February 11, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-042a.

[22] William Turton and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password+&cd=1&hl=en&ct=clnk&gl=us.