

Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping

Roger Kwon, Travis Ashley, Jerry Castleberry, Penny Mckenzie, Sri Nikhil Gupta Gouriseti
Pacific Northwest National Laboratory
{roger.kwon, travis.ashley, jerry.castleberry, penny.mckenzie, sri}@pnnl.gov

Abstract—Cyber-attack and defense frameworks offer numerous ways to protect systems and networks from threats. However, only a few of these numerous attack and defense frameworks provide countermeasures by linking multiple frameworks. Due to the lack of attack-defense mapped frameworks, a number of cyber security practitioners are often puzzled how to cope with cyber-attacks when it occurs. The objective of this paper is to present a tool called the “Cyber Threat Dictionary” to solve the problem. Cyber Threat Dictionary offers approaches and practical solutions to the threats by mapping MITRE ATT&CK Matrix to the NIST Cybersecurity Framework. By providing immediate solutions to cyber security practitioners, Cyber Threat Dictionary enables effective responses against cyber-attacks.

Keywords—MITRE ATT&CK MATRIX, NIST Cybersecurity Framework, CSF, cyber threat landscape, facilities, buildings

I. INTRODUCTION

The operational technology (OT) cyber threat landscape is constantly changing with non-linearly evolving threats. This challenge is further amplified by the increased penetration of connected smart systems in the traditionally isolated OT space. What Intel refers to as the “big data bang,” the number of Internet of Things (IoT) devices is expected to reach 200 billion in 2020 [1] (there were only 15 billion IoT devices connected in 2015). Research-based evidence shows that often the IoT systems have unattended security vulnerabilities. According to the 2020 Unit 42 IoT Threat Report [2], a study was conducted on 1.2 million IoT devices to better understand today’s threat landscape and 57% of IoT devices were found to be vulnerable to medium or high severity attacks. Despite the gaps and challenges, deployments of smart connected systems are happening at alarming rates in facilities (around 80% [3]) because they contribute to increased sustainability, efficiency of facility operations, enhanced data collection, and optimization¹. As evidence, the smart building market is forecasted to grow at a Compound Annual Growth Rate of 11.7% from 2019 to 2024, reaching nearly 106 billion USD by 2024 [4]. To secure the facilities and networks, it is critical to understand the threats, vulnerabilities, and the relevance of those threats to the facility related control systems (FRCS). These vulnerable devices are being deployed across various critical infrastructure systems such as connected buildings, the power grid, industrial facilities, etc. With no end in sight, the facilities are steadily and exponentially augmenting the cyber threat landscape through increased connectivity. Threat actors are constantly engineering innovative methods to

exploit connected devices, such as recent threat actors taking advantage of the COVID-19 pandemic by pursuing organizations and individuals under work-from-home policies [5]. While many cyber-attacks have been extensively analyzed post-mortem and have offered many insightful findings, the steps taken by threat actors during attacks typically deviate greatly due to the threat actor personal preferences. A variety of cyber-attack and defense mechanisms exist and are used by critical infrastructure facility operators, but few provide defense tactics in response to specific attack tactics issued by the threat actors. To solve this problem, a Cyber Threat Dictionary (CTD) was created to map systematic defensive mechanisms suitable for each step of the attack—not against the attack itself. This paper presents a new cybersecurity framework by mapping MITRE ATT&CK ICS MatrixTM (hereby referred to as ATT&CK ICS in the paper) to the facility cybersecurity framework (FCF: <https://facilitycyber.labworks.org/>). FCF is designed strictly based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) but tailored to FRCS/OT networks. The CTD can be used by facility operators in addition, and as a supplement, to their current cybersecurity policies to better align their incident response plans with the NIST CSF. Critical infrastructure owners can use CTD to do the following:

1. Determine the gaps and discover significant and relevant ATT&CK ICS techniques to the facility.
2. Develop efficient mitigation and detection methods to monitor the networks and mitigate the vulnerabilities.
3. Enumerate a correlation matrix between the critical cyber-attack techniques relevant to the facility and the FCF controls that need to be addressed to mitigate the attacks.
4. Perform vulnerability prioritization based on the FCF assessment and the correlation matrix.
5. Design practical solutions to potentially prevent the threats against the facility.

II. BACKGROUND

A. MITRE ATT&CK ICS Matrix

The ATT&CK ICS framework was selected because its criteria align with Lockheed Martin’s Cyber Kill Chain (CKC) and it addresses most contemporary global cyber threats [6]. ATT&CK ICS has 300 attack tactics that are organized in the

¹ In this paper, the term facilities refer to DHS’s 16 critical infrastructure facilities including but not limited to federal facilities, buildings, and energy utilities.

This study was conducted at the Pacific Northwest National Laboratory, which is operated for the U. S. Department of Energy by Battelle Memorial Institute under Contract DE-AC05-75RL01830.

knowledge base and categorized by threat actors' attack processes by technique (from Initial Access to Impact, in chronological order) [7]. ATT&CK ICS covers not only cyber-attacks that threaten information technology networks, but also those in operational technology (OT) networks in the MITRE ATT&CK for Industrial Control Systems Matrix™ (ATT&CK ICS) [8] that is suitable for reference by facilities' network personnel.

B. NIST Cybersecurity Framework

NIST CSF was published in February 2014 in response to the 2013 presidential EO 13636, "Improving Critical Infrastructure Cybersecurity," which called for critical infrastructure owners and operators to bolster cybersecurity defenses and resiliency [9]. The 2017 EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," [10] then mandated that all critical infrastructures comply with CSF.

CSF provides a wide range of defense mechanisms using 100+ cyber defense controls in five domains (i.e., Identify, Protect, Detect, Respond, and Recover), and each domain is split into various categories that have a narrower scope. The domains and categories that compose the CSF are updated based on trends of new cyber threats that occur each year.

C. Facility Cybersecurity Framework

The facility cybersecurity framework (FCF) is a web-based cybersecurity assessment tool developed using the NIST CSF. This free-to-use FCF tool can be accessed at www.facilitycyber.labworks.org [11]. FCF can be used by critical infrastructure owners and OT operators to (1) discover their current cybersecurity posture, (2) identify tailored security gaps, (3) describe their target cybersecurity state, (4) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, (5) assess progress toward the target state, and (6) communicate among internal and external stakeholders about cybersecurity risk. Despite FCF's efficacy, in its original state, FCF was only able to determine the gaps but did not provide threat information. To evaluate the risk associated with a facility and the overall impact of a security event, acquiring threat intelligence is as important as discovering system vulnerabilities. To address this limitation, the FCF security controls (OT-tailored version of NIST CSF) were mapped to the ATT&CK ICS Matrix. Using this novel mapping, cybersecurity practitioners can use the vulnerabilities and associated threats to effectively prepare for potential cyber-attacks and respond in a timely fashion to mitigate an attack if it occurs.

Using the vulnerability to threat mapping, facility owners can develop prioritized risk-driven timeboxed mitigation plans and processes. In addition, they can evaluate risk mitigation, acceptance, and transfer options. To effectively respond and recover when a facility is subjected to a cyber-attack, it is crucial to prioritize the assets to be defended and to understand the attack process. No matter how much knowledge cybersecurity practitioner(s) have about cyber vulnerabilities, if they lack the experience to respond to and recover from cyber threats, it will be difficult to deal with the attack. To address this problem, FCF provides facility cybersecurity training programs to defend against cyber-attacks in stages, using scenarios based on real cyber-attack cases.

III. METHODOLOGY

ATT&CK ICS catalogs about 300 cyber-attack tactics and 1200 strategies for detecting and mitigating the listed attacks. Mapping all attack and defense tactics to each of the FCF controls is a non-trivial process. This section presents the methodology and process followed to classify the mitigation and detection subcategories and map them to FCF controls. Figure 1 presents the overall development process.

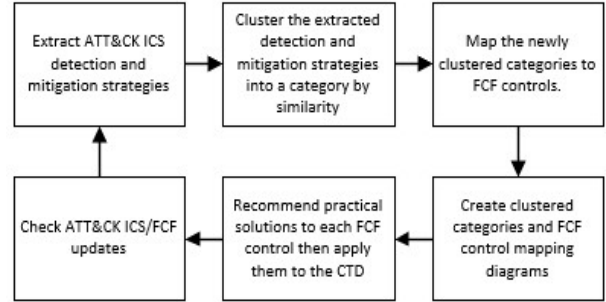


Fig. 1. Cyber Threat Dictionary Development Process

A. Extract ATT&CK ICS detection and mitigation strategies

For the first step, detection and mitigation mechanisms for all cyber-attack tactics presented in ATT&CK ICS were extracted. The extraction derived 468 detection skills and 770 mitigation skills for all attack tactics specified in the matrix. In this context, a skill is a way to mitigate and detect cyber-attacks. Table I shows part of the Initial Access remediation strategies in the matrix.

TABLE I. PART OF MITRE ATT&CK MATRIX DETECTION AND MITIGATION

Initial Access		
Drive-by Compromise	Detection	Firewalls
		Proxies
		Network IDS
	Mitigation	Up-to-date browsers and plug-ins with security features on
		Adblockers, Script blocking extensions
		Virtualization and application micro-segmentation
Exploit Public-Facing Application	Detection	Security applications
		Monitor logs
	Mitigation	Deep packet inspection
		Application isolation
External Remote Services	Detection	Least privilege
		Web Application Firewalls
	Mitigation	Collect authentication logs
		Limit access to remote services
		Strong two-factor or multi-factor authentication

B. Clustering detection and mitigation tactics by similarity

The next step is to recategorize all of the listed detection and mitigation tactics that have similar attributes into categories. For example, in Table II *Disable Autorun* from the row *Replication Through Removable Media*; *Ensure that unnecessary ports and services are closed* from the row *Network Sniffing*; and *Minimize available services* from the row *Exploitation of Remote Services* are all re-categorized under *Close Unnecessary Ports/Services* shown in Table III. A total of 1238 detection and mitigation tactics were grouped

according to their similarities, forming 50 new detection categories and 62 new mitigation categories. The main categories of detection are Log/data analysis, Collect logs, Audit policy, Monitoring, Software comparison, among others. The mitigation categories mainly include Access control, Audit accounts, Authentication, Firewall, Intrusion Detection System, Network segmentation, User training, and Whitelisting.

TABLE II. PART OF MITRE ATT&CK MATRIX DETECTION AND MITIGATION

Replication Through Removable Media	Detection	Monitor file access on removable data
	Mitigation	Disable Autorun Whitelisting
Network Sniffing	Detection	Monitor for ARP spoofing Auditing admin logins
	Mitigation	Ensure that unnecessary ports and services are closed
		Monitor switches and network Whitelisting
Exploitation of Remote Services	Detection	Look for behavior on the endpoint system that might indicate successful compromise
	Mitigation	Minimize available services
		Regularly scan the internal network
		Update software regularly Control flow integrity checking

TABLE III. PART OF RE-CATEGORIZED DETECTION AND MITIGATION STRATEGIES

Detection and Mitigation Category	Sub-category
Close Unnecessary Ports/Services	Ensure that unnecessary ports and services are closed
	Disable autorun
	Minimize available services
Whitelisting	Application Whitelisting
	Whitelisting
System Monitoring	File system monitoring
	Monitor file access on removable data
	File access monitoring
	Monitoring API calls
	Monitoring for the creation of suspicious files

C. Mapping categories to FCF controls

Controls in FCF provide a checklist and an approach to problem solving related to cybersecurity incidents. Furthermore, FCF suggests how to apply the control itself to the practical defense mechanisms. A single FCF control may be insufficient to provide solutions to a category by itself; therefore, multiple FCF control combinations are essential to addressing this problem. For example, a combination of FCF control PR.PT-3 (the principle of least functionality is incorporated by configuring systems to provide only essential capabilities) and PR.DS-5 (protections against data leaks are implemented) produces a more effective guideline for mitigating potential data exfiltration through unnecessarily opened ports or services, in contrast to using each control individually. Table IV shows an example of mapping ATT&CK ICS detection and mitigation categories to FCF controls.



TABLE IV. EXAMPLE OF MITRE ATT&CK MATRIX – FCF CONTROL MAPPING

Detection and Mitigation Category	Facility Cybersecurity Framework Control
Close Unnecessary Ports/Services	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. AND PR.DS-5: Protections against data leaks are implemented.
Whitelisting	DE.CM-1: The network is monitored to detect potential cybersecurity events. AND DE.DP-4: Event detection information is communicated.
System Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events. AND DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
Account Monitoring	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. OR DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed. AND DE.CM-1: The network is monitored to detect potential cybersecurity events.

D. MITRE ATT&CK Matrix and FCF Maps

In addition to listing FCF controls related to detection and mitigation categories, maps with AND/OR logic gates are used to present step-by-step solutions to cyber-attacks over time. Figure 2 shows the FCF controls for account monitoring. For account monitoring, if the monitoring activity of authorized (DE.CM-3) OR unauthorized personnel (DE.CM-7) is primarily performed, then potential cybersecurity events will be more likely to be detected; however, if the personnel monitoring process fails to detect a cyber event, then network monitoring (DE.CM-1) would be the next mechanism to detect it. Each control is progressively harder to get past, which makes it more difficult for the threat actor to break into the targeted network.

TABLE V. AND/OR LOGIC GATES IN THE CTD

	All inputs getting through the 'AND' gate needs to be fully or largely implemented.
	At least one of the inputs getting through the 'OR' gate needs to be fully or large implemented.

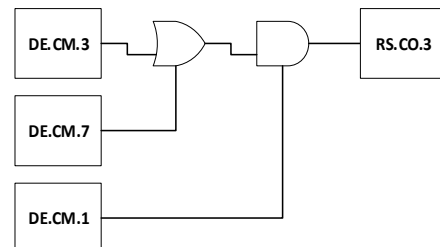


Fig. 2. Control diagram for Account Monitoring

E. Practical solution suggestion

The CTD not only provides FCF controls for cyber-attack mapping but also facilitates practical solutions pertaining to applicable policies or security applications to remediate related threats. Table VI shows FCF controls and practical solution mappings. Each control has a detailed description and suggested candidate solutions to satisfy the corresponding elements. Cybersecurity practitioners can refer to the dictionary and deploy the necessary equipment or mechanisms to remediate threats against the network.

TABLE VI. EXAMPLE OF FCF DESCRIPTION AND SOLUTION

FCF Control	Description	Solution/Example
ID.RA-1: Are asset vulnerabilities identified and documented?	All vulnerabilities should be documented so that the entire cybersecurity team will have direct access to this information, and so that a history of patches or fixes can be established for subsequent security administrators.	The Common Vulnerabilities and Exposure (CVE) List contains records of identified vulnerabilities and publishes them with a unique identifier.
ID.RA-2: Is threat and vulnerability information received from information sharing forums and sources?	Subscribing to information sharing sources is a great way to stay informed about vulnerabilities by learning when new vulnerabilities are found or when known vulnerabilities are updated.	Information sharing sources include ISACs, US-CERT, NIST National Vulnerability Database (NVD), MITRE Common Vulnerabilities and Exposures (CVE), FBI InfraGard program, etc.
ID.RA-3: Are both internal and external threats identified and documented?	Threats should be identified and documented so that the facility knows what the current environment is like and can better defend the network against exploitation.	Some example of internal threats includes disgruntled employees, user errors, or victims of social engineering. National Insider Threat Task Force (NITTF) identifies 5 categories of insider threats.

The mapping is done by manually matching all FCF controls and ATT&CK ICS tactics. Whenever the ATT&CK ICS or NIST CSF controls are updated due to the advent of new cyber-attack techniques, we apply the updates to CTD. The ATT&CK ICS updates from time to time when a new attack type appears. In the case of NIST CSF, CSF version 1.1 was released in 2018, four years after the release of CSF 1.0, and detailed control revisions and updates are being made from time to time. Appendix A is an excerpt from the first part of the mitigation category of the CTD as of September 2020. Currently the research team is experimenting methods to semi-automate the process.

IV. HOW TO USE THE DICTIONARY

This section uses examples to show how cybersecurity practitioners can use CTD. A scenario is provided that demonstrates the two components of CTD, including the search, which provides details and solutions to deal with the attack, and the solution suggestion, which offers diagrams and tables.

A. Search in the Cyber Threat Dictionary

Assume a facility's cybersecurity practitioner has been affected by a replication through a removable media exploit and wants to remediate it. If the cybersecurity practitioner searches through the CTD, he/she can find the kind of attack that is affecting the system. The dictionary entry includes the mitigation/detection tactics corresponding to the attack, which are *Disable Autorun*, *Whitelisting*, and *Monitor file access on removable data*. Table VII shows an example of detection and mitigation tactics to remediate "Replication through removable media" attack.

TABLE VII. DETECTION AND MITIGATION TACTICS FOR REPLICATION THROUGH REMOVABLE MEDIA

Replication Through Removable Media	Mitigation	Disable Autorun Whitelisting
	Detection	Monitor file access on removable data

B. Cyber Threat Dictionary suggests solutions by providing FCF controls and diagrams

In the following section, the dictionary presents FCF controls (Table VIII) that correspond to the defense strategies, along with diagrams that enable practitioners to develop a defense strategy over time. For example, referring to Table VIII, *Disable Autorun* belongs to *Close Unnecessary Ports/Services* and solutions are presented in the 3rd column, FCF Control. Figure 3 is the whole diagram that provides defense tactics suitable for the attack stage by referring to the diagram's AND/OR gates in chronological order.

TABLE VIII. MITRE ATT&CK MATRIX/FCF CONTROL MAP FOR REPLICATION THROUGH REMOVABLE MEDIA

Category	Sub-category	FCF Control
Close Unnecessary Ports/Services	Ensure that unnecessary ports and services are closed.	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
	Disable Autorun. Minimize available services.	AND PR.DS-5: Protections against data leaks are implemented.
Whitelisting	Application whitelisting	DE.CM-1: The network is monitored to detect potential cybersecurity events.
	Whitelisting (Email, Network, Firewall)	AND DE.DP-4: Event detection information is communicated.
System Monitoring	Monitor file access on removable data	DE.CM-1: The network is monitored to detect potential cybersecurity events.
	Monitoring API calls	AND
	Monitor for the creation of suspicious files.	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.

Based on Figure 3, the first step to defend against “Replication Through Removable Media” is to detect it by monitoring potential events, personnel, devices, and software. The second step is whitelisting suspicious processes, and the last step is closing unnecessary services to protect data exfiltration.

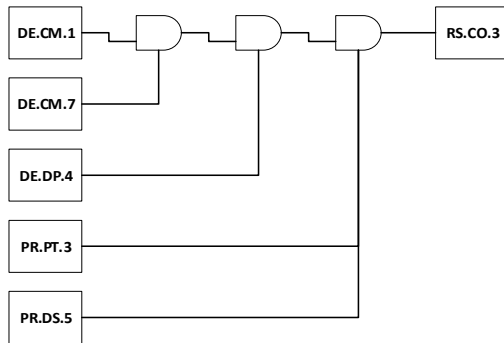


Fig. 3. Control diagram for Replication Through Removable Media

As a final step, the dictionary suggests practical tools or ways to apply defense mechanisms to the network, as seen in Table IX. To successfully implement the FCF controls, it is important to determine the dependencies among the controls to proceed in a sequential fashion. Figure 3 and Table IX shows an illustration of such hierarchy or dependency. In summary, once the mitigation and detection sub-categories from Table VII are mapped to the FCF controls (Table VIII), the FCF control maps with dependencies are developed (Fig. 3 and Table IX) to effectively implement all mapped FCF controls shown in Table VIII.

TABLE IX. SOLUTIONS AND DEFENSE CONTROL DESCRIPTIONS FOR REPLICATION THROUGH REMOVABLE MEDIA

FCF Control	Description	Solution/Example
DE.CM-1	ICS/OT network monitoring refers to the practice of overseeing the operation of a computer network using specialized management software tools to ensure the availability and overall performance of network components and network services.	Opensource monitoring tool suggestion: Wireshark, Nagios Core, Icinga, Zabbix
DE.CM-7	Your facility should be monitored to identify any cybersecurity events and to verify that the protective measures that you have in place are effective.	Opensource monitoring tool suggestion: Wireshark [12], Nagios Core [13], Icinga [14], Zabbix [15]
DE.DP-4	Having established communication channels will help you find the problem and resolve it in a timely manner, whether it is within the organization or with a third-party provider.	Refer to NIST SP 800-63B [16]
PR.PT-3	In information security, the principle of least functionality requires that in an abstract layer of a computing environment, every module must be able to access only the information and resources	Blacklisting, verifying the integrity of whitelisted software. Organizations can use network scanning tools, intrusion detection and prevention systems, and

	that are necessary for its legitimate purpose.	end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
PR.DS-5	There are many security measures to keep in mind to ensure that data leaks do not happen within your organization. Strong passwords, encryption, authentication, and more.	Refer to NIST 800-53 [17]

V. CONCLUSION

The ever-changing state of the cyber threat landscape makes cyber-attacks a difficult problem for cyber security professionals to address. The buildings sector is a large contributor to this challenge because most smart facilities contain internet-connected devices that are likely vulnerable to attacks. Once systems are compromised, the impacts of cyber-attacks are critical and difficult to recover from; therefore, the most important defense is to implement strong cybersecurity policies to protect the network from cyber threats. If security is compromised, the next priority is identifying the current attack stage of ATT&CK ICS to respond immediately and mitigate the attack before further malicious action is taken. CTD can be used in both reactive and proactive ways. In terms of reactive usage, by using CTD cybersecurity practitioners can identify actions to take once an attack is detected. For proactive use, CTD can be used to identify how controls will defend the users against possible attacks by identifying gaps before being exploited. The CTD is a tool that can be used by critical infrastructure facility operators to supplement their cybersecurity policies to better align their incident response plan with the FCF controls. In addition to the CTD, more attack-defense mapping tools must be developed to help cybersecurity personnel, and both a web version and client application are needed for ease of access by cybersecurity practitioners.

REFERENCES

- [1] A guide to the Internet of Things. [Online]. Available: <https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>
- [2] 2020 Unit 42 IoT Threat Report. March 10, 2020 [Online]. Available: <https://unit42.paloaltonetworks.com/iot-threat-report-2020/>
- [3] IoT in Smart Buildings Market Outlook and Forecasts 2018 – 2023. [Online]. Available: https://www.researchandmarkets.com/research/xbg8kv/iot_in_smart?w=5
- [4] Smart building market by component (solution, services), solution (security and emergency management, energy management), services, building type (commercial, industrial), region (North America, Europe, APAC, MEA, Latin America) – Global forecast to 2024. [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/smart-building-market-1169.html>
- [5] Hacking against corporations surges as workers take computers home, April 17, 2020. [Online]. Available: <https://www.reuters.com/article/us-health-coronavirus-cyber-corporations/hacking-against-corporations-surges-as-workers-take-computers-home-idUSKBN21Z0Y6>
- [6] Proactively Detect Persistent Threats, Cyber Kill Chain. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

- [7] MITRE ATT&CK Matrix. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [8] ATT&CK for Industrial Control Systems. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page
- [9] Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013. [Online]. Available: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- [10] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. [Online]. Available: <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>
- [11] Facility Cybersecurity, Self-assessment tools for hardening your facilities against cyber attacks [Online]. Available: <https://facilitycyber.labworks.org/>
- [12] Wireshark. [Online]. Available: <https://www.wireshark.org/>
- [13] Nagios Core. [Online]. Available: <https://www.nagios.org/projects/nagios-core/>
- [14] Inspect your Entire Infrastructure, Icinga. [Online]. Available: <https://icinga.com/>
- [15] Freedom and Integrity of Monitoring, Zabbix. [Online]. Available: <https://www.zabbix.com/>
- [16] NIST Special Publication 800-63B. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>
- [17] NIST National Vulnerability Database. [Online]. Available: <https://nvd.nist.gov/800-53>

APPENDIX A

Mapping MITRE ATT&CK For Industrial Control Systems Matrix™ (ATT&CK ICS) Mitigation Strategies to FCF Controls

Mitigation Category	Sub-category	FCF Control
Access Control	Prevent adversary access to privileged accounts	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
	Do not put user or admin domain accounts in the local administrator groups across systems	
	Appropriate implementation of access control mechanisms	
	Mitigate access to Valid Accounts	
	Limit privileges of user accounts and groups	
	Ensure proper process, registry, and file permissions are in place to inhibit adversaries from disabling or interfering with critical services	
Access Control (Least Privilege)	Least privilege	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties OR PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
	Minimize permissions and access for service accounts	
Access Control (Remote)	Limit access to remote services	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties AND {PR.AC-3: () Remote access is managed OR PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access}
Analysis	Operate analysis system	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) AND RS.AN-1: Notifications from detection systems are investigated
Audit Accounts	Audit domain and local accounts	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes AND PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Authentication	Strong two-factor or multi-factor authentication	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes OR PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties OR PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions OR PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	Credential Access	
	Proper permissions and authentication	
	Use multifactor authentication	
Backup	Ensure backups are stored off system	PR.IP-4: Backups of information are conducted, maintained, and tested AND PR.DS-1: Data-at-rest is protected
Blacklisting	Block unknown or unused files in transit by default	{DE.CM-1: The network is monitored to detect potential cybersecurity events OR DE.CM-4: Malicious code is detected OR DE.CM-5: Unauthorized mobile code is detected} AND {DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events OR DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed}
	Preventing adversary tools from running earlier in the chain	

Close Unnecessary Ports/Services	Ensure that unnecessary ports and services are closed	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities AND PR.DS-5: Protections against data leaks are implemented
	Disable Autotun	
	Minimize available services	
Code Security	Use secure coding best practices	PR.DS-5: Protections against data leaks are implemented
Data Isolation	Off-system storage of sensitive information	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value AND {PR.DS-1: Data-at-rest is protected OR PR.DS-5: () Protections against data leaks are implemented}
Database Policy	Develop and publish policies that define acceptable information to be stored	ID.AM-3: Organizational communication and data flows are mapped AND ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value AND PR.DS-5: Protections against data leaks are implemented
Encryption	Obfuscate/encrypt event files locally and in transit	PR.DS-1: Data-at-rest is protected AND PR.DS-2: Data-in-transit is protected
	Ensure that all wireless traffic is encrypted appropriately	
	Encryption	
Firewall	Web Application Firewalls	PR.DS-5: Protections against data leaks are implemented AND PR.IP-7: Protection processes are improved AND PR.PT-4: Communications and control networks are protected AND PR.IP-8: Effectiveness of protection technologies is shared
IDS/IPS	Network IDS	PR.DS-5: Protections against data leaks are implemented AND PR.IP-7: Protection processes are improved AND PR.PT-4: Communications and control networks are protected AND PR.IP-8: Effectiveness of protection technologies is shared
Information Policy	Information policy	ID.GV-1: Organizational cybersecurity policy is established and communicated AND PR.IP-6: Data is destroyed according to policy AND PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy AND PR.PT-2: Removable media is protected and its use restricted according to policy
Integrity Check	Control flow integrity checking	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity AND PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity AND PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
	Check the integrity of the existing BIOS or EFI	
Intelligence Capability	Develop a robust cyber threat intelligence capability	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
Isolation	Application Isolation	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
Limitation	Limit credential overlap across systems to prevent access	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Logging	Automatically forward events to a log server or data repository	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools AND PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access AND PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Minimize Time Delay	Minimize time delay on event reporting to avoid prolonged storage on the local system	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value AND RS.CO-2: Incidents are reported consistent with established criteria
Monitoring	Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events AND {DE.CM-2: The physical environment is monitored to detect potential cybersecurity events AND DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed}
	Monitor switches and network	
Network Segmentation	Network segmentation	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
Password	Ensure that local administrator accounts have complex, unique passwords across all systems on the network	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes OR PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions AND PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	Strong passwords	
	Refer to NIST guidelines when creating passwords	
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	
Patch	Up-to-date browsers and plug-ins with security features on	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks AND RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
	Patch systems	
	Patch management	
	Patch the BIOS and EFI	
	whitelisting	