

TLP:CLEAR



2023 CYBER TRENDS AND INSIGHTS IN THE MARINE ENVIRONMENT

Coast Guard Cyber Command



United States Coast Guard

TLP:CLEAR

Disclosure: The information in this report is provided “as is” for informational purposes only. The U.S. Coast Guard does not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis.

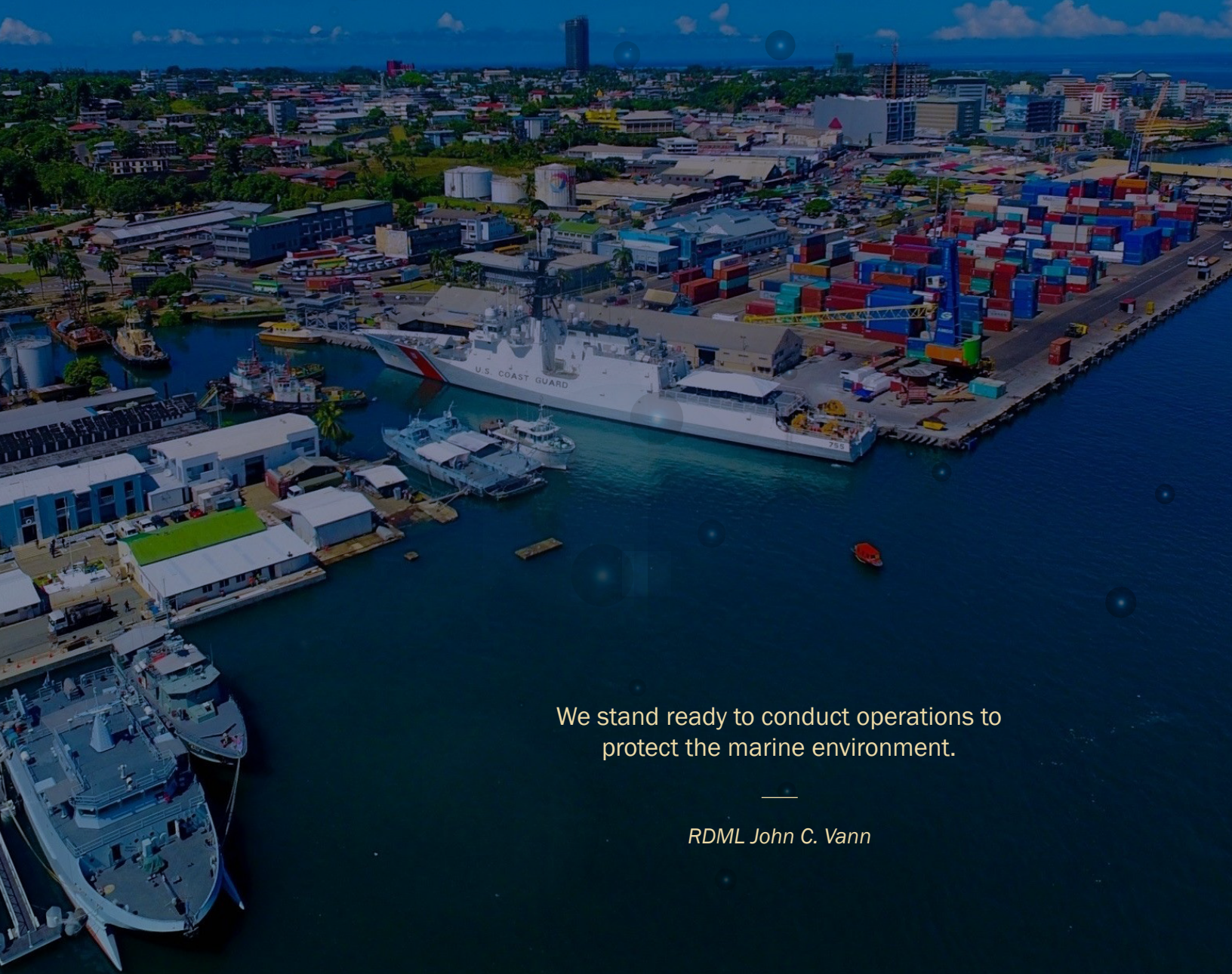
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, by applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see <https://www.cisa.gov/tlp/>.

If an entity wishes to create and distribute derivatives of this report they should: (1) provide notice to Coast Guard Cyber Command before distributing such derivatives and (2) refrain from affixing the Coast Guard Cyber logo or DHS seal to the derivatives, unless they have obtained written permission to do so from the Coast Guard Office of External Affairs.

The unauthorized use of any Federal agency’s seal is governed by the U.S. Code, Title 18, sections 506, 701, 709, and 1017. Further, U.S. Code, Title 14, section 934 prohibits individuals, corporations, and other businesses from using the words “Coast Guard” or “United States Coast Guard” for trade or business purposes.

TABLE OF CONTENTS

Table of Contents	3
Foreword	5
Executive Summary	6
Introduction	7
Scorecard	8
Understanding the Marine Environment	9
Cyber Protection Team Missions	10
Maritime Cyber Trends	12
Attack Paths Used on Assessments	16
Top 5 Findings from Assessments	17
Hunt & Incident Response Recap	22
Securing Operational Technology	24
Port Security Grant Program	28
Look Ahead To 2024	29
Appendix A	
Maritime Cyber Alerts	31
Appendix B	
Observed Cyber Criminal Organizations	32
Appendix C	
Known Exploitable Vulnerabilities Detected on CPT Missions	33
Appendix D	
Summary of CPT Attack Paths	38
Appendix E	
Summarized Findings of 2023 CPT Assess Missions	39
Appendix F	
Mitigations	40
Appendix G	
Coast Guard Cyber Command Overview	53
Appendix H	
List of Acronyms	55
Appendix I	
List of Figures	57
Appendix J	
List of Tables	58



We stand ready to conduct operations to
protect the marine environment.

RDML John C. Vann

FOREWORD



I am pleased to present the 2023 Cyber Trends and Insights in the Marine Environment (CTIME) report. This report summarizes U.S. Coast Guard Cyber Command's (CGCYBER) findings from calendar year 2023 and the associated mitigation recommendations. CGCYBER continues to expand its presence and navigate an increasingly interconnected marine environment. As we witness a surge in technological advancements, the organizations that facilitate the exchange of goods face evolving cyber threats, demanding our unwavering attention and concerted action.

The maritime sector's advancement into the digital realm demands a paradigm shift in our approach to cybersecurity. Physical barriers alone can no longer shield our ports from external threats. Today, cyber defense and resilience are as crucial as the structural integrity of piers, terminals, fences and gates. Collaborative efforts between governments, private entities, and international organizations are imperative to create a unified front against cyber threats. As discussed in this report, maritime infrastructure and the connected supply chains have become attractive targets for cyber adversaries seeking financial rewards, economic disruption, or geopolitical leverage. The consequences of a cyberattack on port infrastructure extend far beyond financial losses. Disruptions to the supply chain can have cascading effects on global economies, impacting industries and livelihoods. As stewards of maritime trade, it is our collective responsibility to safeguard our ports and maritime infrastructure.

This report offers a comprehensive analysis of the current state of cybersecurity in the marine environment, identifying vulnerabilities, assessing risks, and presenting strategic recommendations to fortify our defenses. Our goal is not just to secure individual ports, but to elevate the resilience of the entire marine environment. In pursuit of this goal, we outline the urgency of implementing basic cyber hygiene measures and investing in cybersecurity professionals who can foster a culture of awareness within maritime organizations. These steps are pivotal to build a robust defense against evolving cyber threats. This report serves as a call to arms, urging stakeholders to prioritize cybersecurity in their strategic agendas. By doing so, we not only secure the arteries of global trade but also fortify the foundation of our interconnected world. If you would like the assistance of CGCYBER, please reach out to us at MaritimeCyber@uscg.mil. We stand ready to conduct operations to protect the marine environment. Together, we will navigate the digital seas with vigilance, toward resilience, ensuring the prosperity and security of maritime trade for generations to come.

Semper Paratus,

A handwritten signature in blue ink, appearing to read 'John C. Vann'. The signature is fluid and cursive, with a large loop at the beginning.

John C. Vann

Rear Admiral, United States Coast Guard
Commander, Coast Guard Cyber Command

EXECUTIVE SUMMARY

Continuing the United States Coast Guard's tradition of stewardship and collaboration with owners, operators, and industry partners in the Marine Environment (ME), CGCYBER has published the third annual CTIME report. This report provides relevant information and lessons learned about cybersecurity risks as well as best practices to drive hardening actions and secure critical systems. The observations and findings in this report also provide Coast Guard units, their partners, and all stakeholders with key insights to identify and address current and emerging cyber risks. Coast Guard Cyber Protection Teams (CPTs) and CGCYBER's Maritime Cyber Readiness Branch (MCRB) developed these findings through ongoing operations, technical exchanges, and industry engagements in 2023.

The area where we've seen the most evolution is around cyber and cyber risk in the marine transportation system.¹

– ADM Linda Fagan,
April 2023

Key Takeaways

- 1. Significant uptick of reported Advanced Persistent Threats targeting the ME.** Announced in the Joint Cyber Security Advisory released in May of 2023 ([AA23-144A](#)),² Volt Typhoon, a state-sponsored actor associated with the People's Republic of China (PRC), is believed to have targeted networks across U.S. critical infrastructure sectors, including within the ME.
- 2. Ransomware incidents continue to surge in 2023.** Reports of ransomware incidents increased 80% from 2022 to 2023 and the average requested ransom more than tripled. Types of organizations targeted include:
 - Maritime shipping companies;
 - Liquid natural gas processors/distributors and petrochemical companies; and
 - Maritime logistics and technology service providers.
- 3. CGCYBER identified similar cybersecurity deficiencies that were in the two previous CTIME reports.** In 2023, CPT missions reinforced many of the same recommendations to partners as provided to other organizations in past years. This

confirms the presence of persistent vulnerabilities within the ME. Recommendations focused on improving basic cyber hygiene, including implementing a **Patch Management Policy**, enforcing the principle of **Least Privilege**, and implementing **Multi-Factor Authentication (MFA)**.

- 4. Network-connected Operational Technology (OT) introduces attack vectors to the ME.** Across the ME, organizations continue to expand the use of internet connected OT systems. In 2023, CPTs found that OT network segments often contained an organization's most critical and most vulnerable systems. In most cases, CPTs observed OT systems running End-of-Life software with known exploitable vulnerabilities (KEV). Additionally, OT systems often utilized vulnerable network protocols allowing for further exploitation and privilege escalation. These risks are further exacerbated when OT networks lack sufficient access controls, allowing adversaries to jump from the information technology (IT) networks to the OT networks. This could allow adversaries to deliver effects in the physical domain.

¹ Source: <https://www.csis.org/analysis/beyond-americas-coastline-conversation-admiral-linda-l-fagan-27th-commandant-united-states>

² Source: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

INTRODUCTION

The contents of this report are intended to inform stakeholders and increase their ability to identify and address cybersecurity risks within their purview.

This report provides a high-level analysis of observed cybersecurity practices and adversary activities within the ME from January 1, 2023 to December 31, 2023. Across the calendar year, CGCYBER has recorded metrics to identify trends that will aid Coast Guard and maritime industry decision makers. These decision makers include: Coast Guard Area/District/Sector Commanders, their staff; and maritime facility leadership and management teams; including Facility Security Officers (FSOs), IT Directors, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Cybersecurity Officers (CySOs) and other executives.

The Coast Guard has been designated as the Co-Sector Risk Management Agency (SRMA) for the maritime portion of the Transportation Sector, making the Coast Guard responsible for identifying and managing risks to maritime critical infrastructure. To meet these responsibilities, the Coast Guard has been given authority to prevent, detect, and respond to threats endangering maritime critical infrastructure. As highlighted in recent Coast Guard publications, protection and defense of the Marine Transportation System (MTS) in the cyber domain remains a strategic objective of the Coast Guard. As such, the Service continues to invest in cybersecurity capabilities and capacities. The Coast Guard has established three Active Duty CPTs and each Area, District, and Sector Commander has a Marine Transportation Systems Specialist – Cyber (MTSS-C) to advise their command on cyber risks in the ME.

What's New in 2023?

In 2023, the ME saw an increase in industry reporting of Nation-State actors targeting U.S. Critical Infrastructure. In response, CGCYBER focused CPT resources towards finding these actors and focused on incorporating OT in CPT missions. 2023's CTIME report reflects the change in priority with the added sections for *Hunt & Incident Response RECAP* and *Securing OT*.

CGCYBER continued to build capacity to support the growing demand from partners in the ME seeking CPT assistance. The 2003 CPT reached Initial Operating Capability in August of 2023 and is expected to reach Full Operating Capability in 2024. Additionally, CGCYBER established a Reserve Component CPT, 1941 CPT, which will supplement the Active Duty CPTs and provide specialized expertise to support and augment operations.

We have stood up a cyber special rating within the Coast Guard to ensure our own expertise, and then are hiring individuals who know cyber, but also understand the marine transportation system.³

– ADM Linda Fagan, April 2023

³ Source: <https://www.csis.org/analysis/beyond-americas-coastline-conversation-admiral-hinda-l-fagan-27th-commandant-united-states>

2023 TRENDS & INSIGHTS

SCORECARD



Average cost of breach for critical infrastructure:

■ **CY23 4.5%↑**
\$5.04M⁴



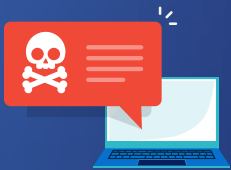
Average cost of all breaches:

■ **CY23 2.2%↑**
\$4.45M



■ **60.1%**

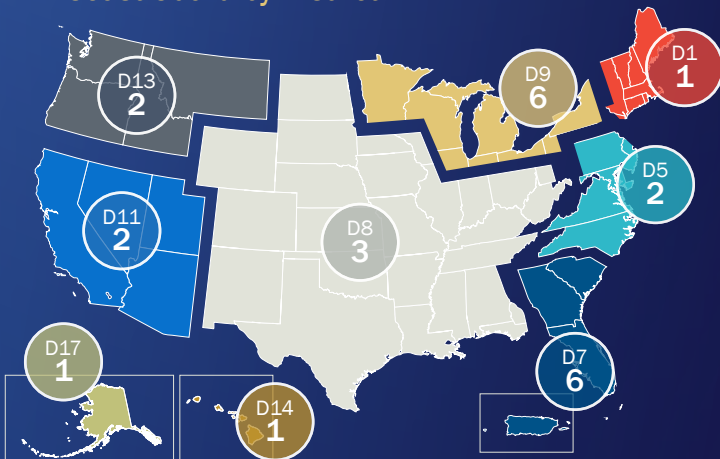
success rate when **Brute Force Cracking Passwords** during 2023 CPT missions



■ **80%**

increase in reported **Ransomware** incidents

■ Cyber Events Reported to Coast Guard by District



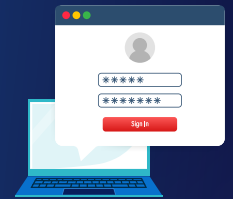
■ **66%**

of CPT missions gained initial access through **Phishing for Information**

Default Credentials were in use at

■ **94.4%**

of organizations



■ **304**

Known Exploitable Vulnerabilities (KEVs) detected across assessments

5 Most Commonly Detected KEVs:

- **CVE-2013-3900 (CVSS: 7.6)**
27.7% organizations
- **CVE-2021-40438 (CVSS: 9.0)**
27.7% organizations
- **CVE-2019-0708 (CVSS: 9.8)**
22.2% organizations
- **CVE-2019-11043 (CVSS: 9.8)**
22.2% organizations
- **CVE-2020-1938 (CVSS: 9.8)**
22.2% organizations

⁴ Source: https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077724063994&p5=e&gad_source=1&gclid=CjwKCAiAopuvBhBCEi-wAm8jaMZuiX6_-CWpKol8QNKd-xukOkpnXpTpzrFSTYP3DshAayQFHw0GyxCpngQAvD_BwE&gclid=aw.ds

UNDERSTANDING THE MARINE ENVIRONMENT

The ME is made up of more than just the maritime components: ships, ports, shipyards, aids to navigation, etc. Of the more than 3,500 waterfront facilities, more than half overlap with at least one other critical infrastructure sector.

The ME consists of 25,000 miles of coastal and inland waterways, serving 361 ports, 124 shipyards, over 3,500 maritime facilities, 20,000 bridges, 50,000 Federal aids to navigation, and 95,000 miles of shoreline that interconnects with critical highways, railways, airports, pipelines, countless shipping vessels, as well as undersea cables carrying 99% of U.S. communications abroad. This integrated ecosystem supports the flow of approximately \$5.4 Trillion in goods and services, constituting 25% of the United States gross domestic product. The ME is one of the most crucial elements of the global supply chain, with 90% of U.S. imports and exports entering or exiting by ship. To support this level of economic activity, the ME fosters employment for over 23 million Americans.⁵ In early 2023, congestion and turnaround times within ports showed signs of returning to their pre Covid-19 pandemic levels. Most notably, as countries further adopt and increase automation within their ports, several show port performances outperforming previous best levels from prior to the pandemic.⁶



Figure 1. Critical Infrastructure Sectors with ME Organizations

Figure 1: Critical Infrastructure Sectors with ME Organizations provides a breakdown of critical infrastructure sectors that overlap with the ME.

⁵ Source: <https://media.defense.gov/2018/Oct/05/2002049100/-1/-1/1/USCG%20MARITIME%20COMMERCE%20STRATEGIC%20OUTLOOK-RELEASABLE.PDF>

⁶ Source: <https://unctad.org/publication/review-maritime-transport-2023>

CYBER PROTECTION TEAM MISSIONS

CPTs are the Coast Guard’s deployable forces delivering capabilities to prevent, detect, and respond to cyber threats impacting U.S. Critical Infrastructure in the ME. Coast Guard CPTs deploy in support of Coast Guard Operational Commanders and organizations in the ME across the world.

Many of the insights in this report are informed by data and analysis collected during Coast Guard CPT missions, as well as from incidents reported to the CGCYBER MCRB. [Figures 2, 3, and 4](#) provide visual representations of the CPT across geographic regions and critical infrastructure sectors. As shown in [Figure 3](#) (next page), CPTs have conducted missions on eight different critical infrastructure sectors that overlap with the ME.

For more information on the structure and capabilities of Coast Guard CPTs and MCRB, see [Appendix H: Coast Guard Cyber Command Overview](#).

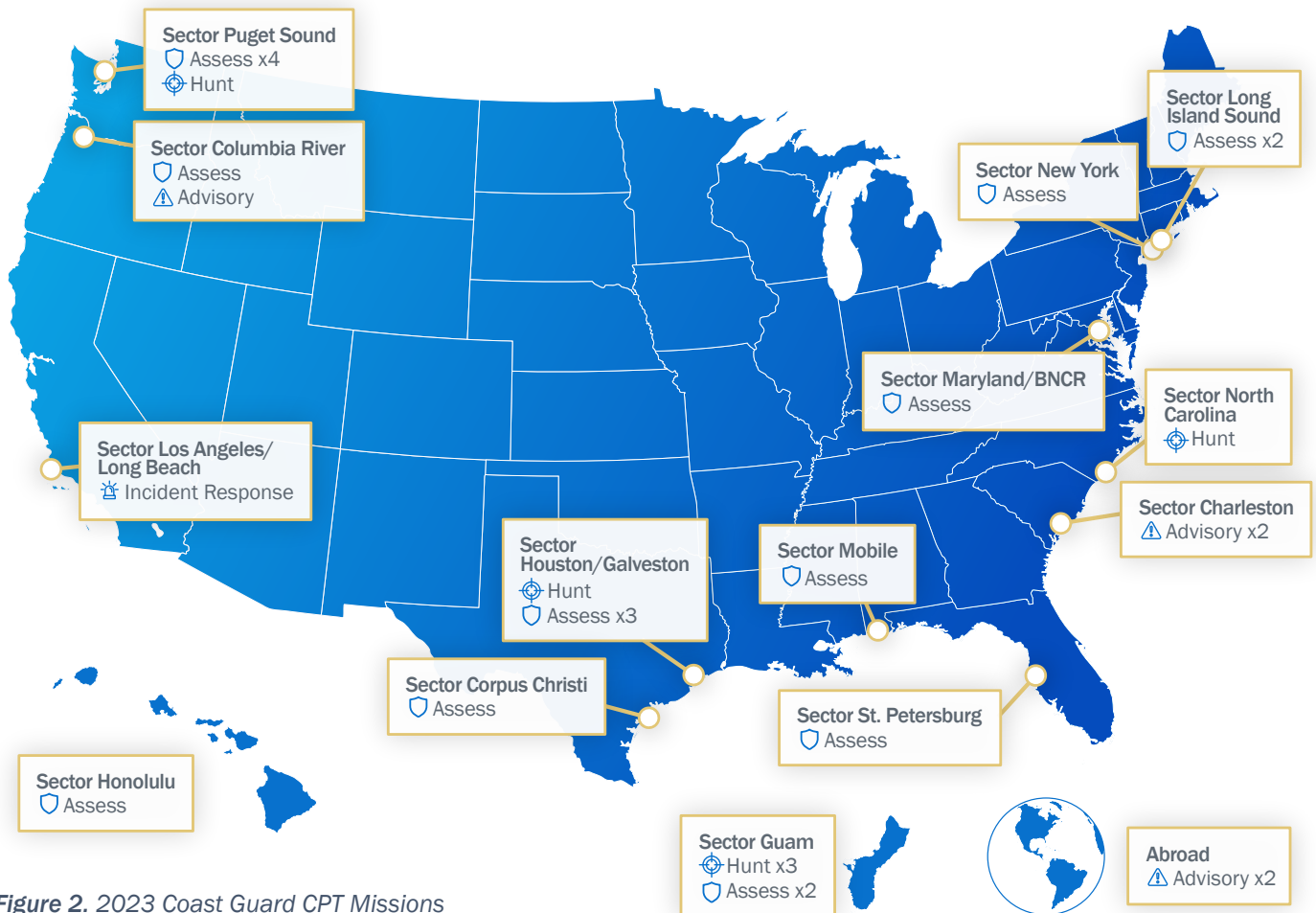


Figure 2. 2023 Coast Guard CPT Missions

CPT Missions per Critical Infrastructure Sector

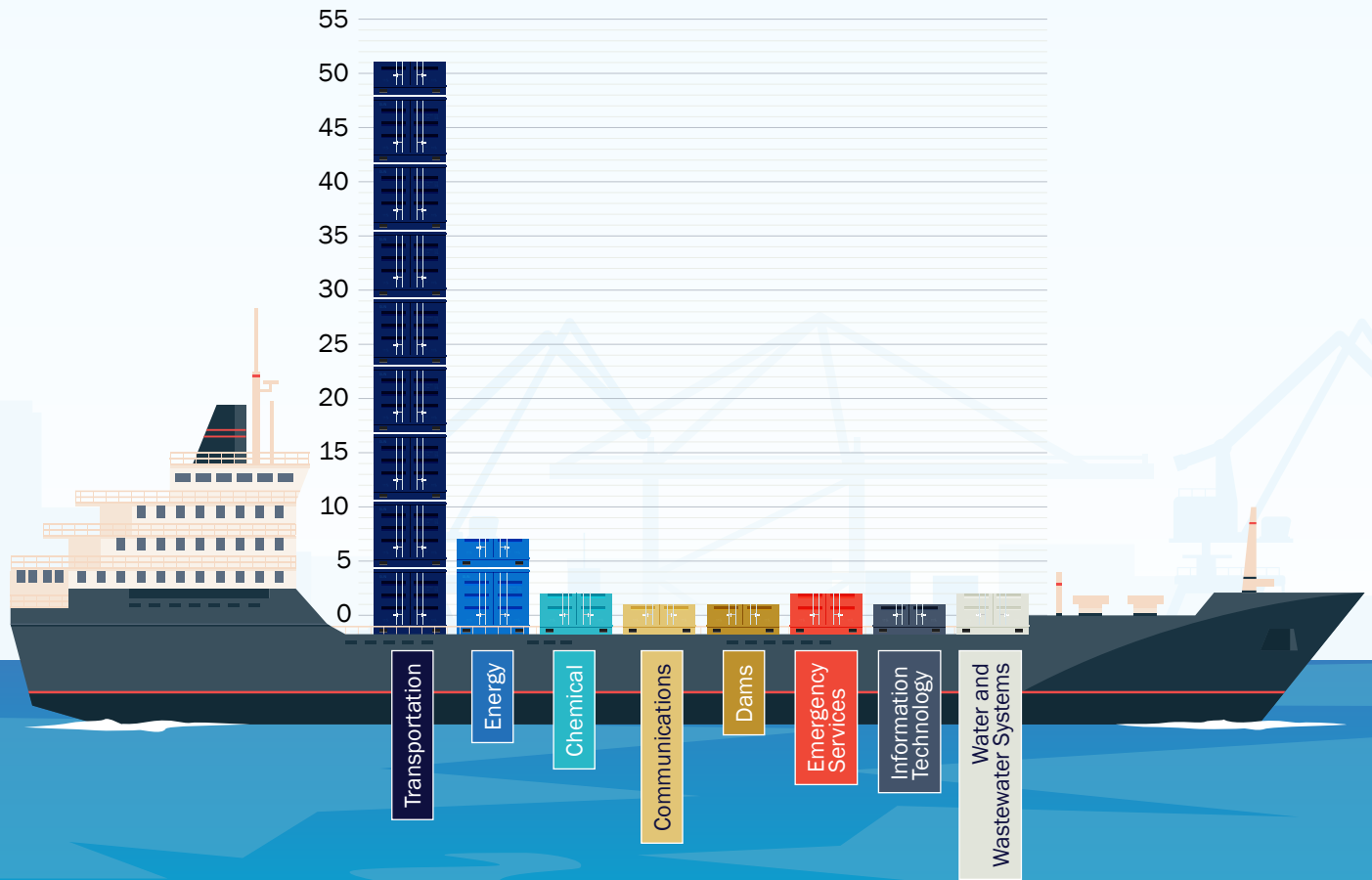


Figure 3. CPT Missions per Critical Infrastructure Sector

Coast Guard CPT Missions Year over Year

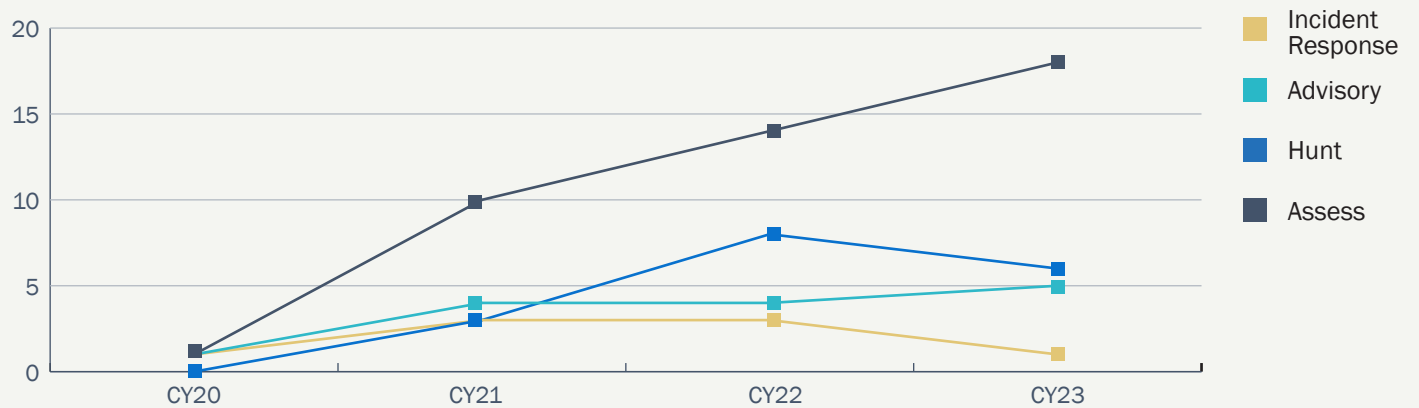


Figure 4. CPT Missions by Type Year over Year

MARITIME CYBER TRENDS

CGCYBER’s MCRB is uniquely qualified, with expertise in marine safety and cybersecurity, to translate cybersecurity details into measurable operational risk. MCRB’s risk analysis supports Coast Guard decision-makers and guides response actions. When a security incident is cybersecurity-related, the MCRB plays a crucial role in helping operational field units stay informed and accurately assess risk.

In 2023, MCRB and local Coast Guard units conducted 46 investigations on reports of cyber incidents. This included several incidents which significantly affected large-scale international organizations. Though the overall number of reported incidents has decreased since 2022, MCRB believes many incidents go undetected or unreported by organizations who are fearful of the public’s perception as a result of a cyber incident. Nation-State actors and opportunistic cybercriminals consistently target the ME, given more than 90% of U.S. imports and exports flow through U.S. maritime ports annually. [Figure 5: 2023 Cyber Events Investigated by MCRB and Local Coast Guard Units](#) provides a visual of cybersecurity reports in 2023.

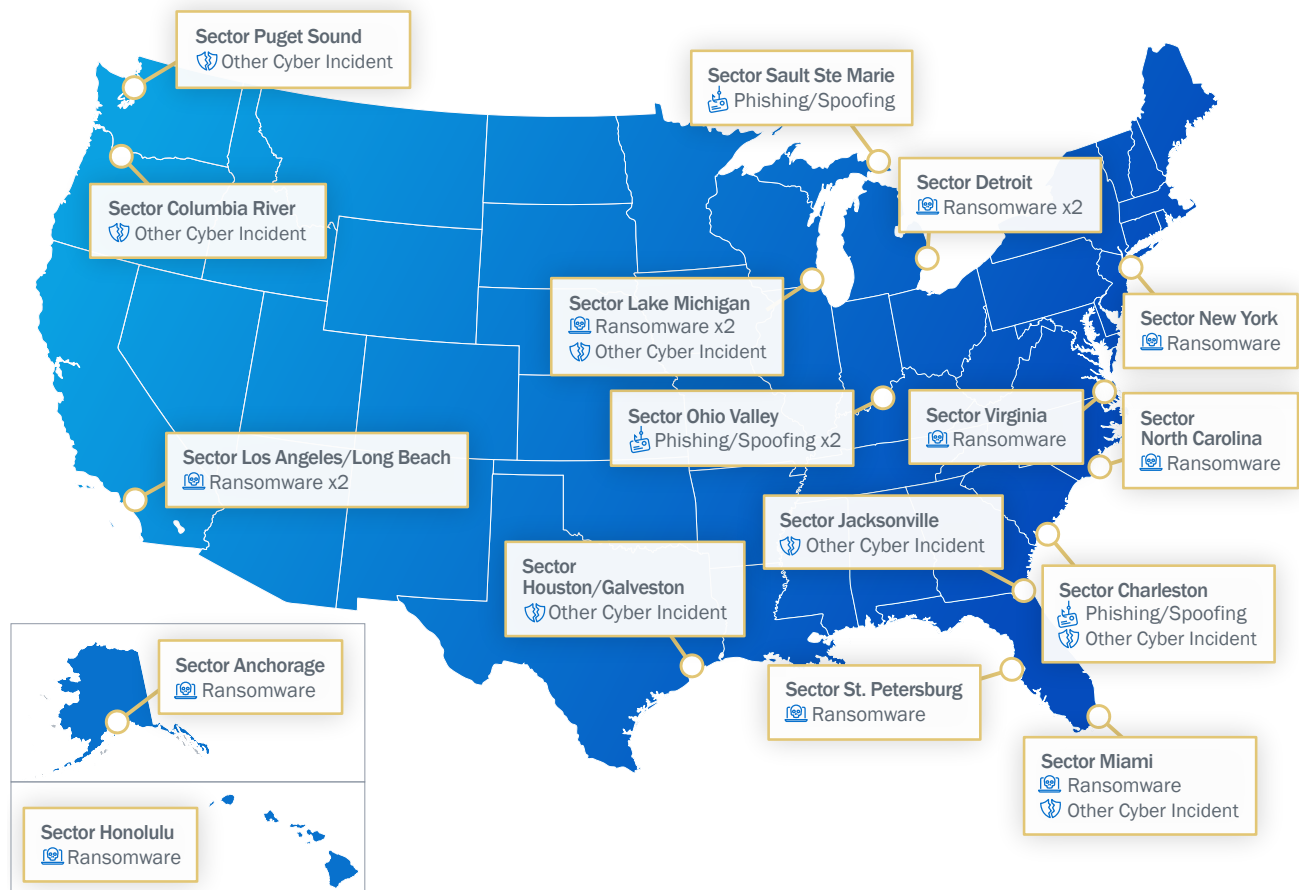


Figure 5. 2023 Cyber Events Investigated by MCRB and Local Coast Guard Units

MCRB categorizes reported cyber incidents into three categories.

1. **Ransomware:** A type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access.⁷
2. **Phishing/Spoofing:** Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, or access to a larger computerized system through a fraudulent solicitation in email or on a web site. The perpetrator typically masquerades as a legitimate business or reputable person. Spoofing is a technique for faking the sending address of a transmission to gain illegal/unauthorized entry into a secure system.⁸
3. **Other Cyber Incidents:** Any incident that does not fall into the above categories such as: Business Email Compromise, Structured Query Language (SQL) Injection, etc.

Ransomware incidents continue to proliferate. MCRB observed an 80% increase in the number of incidents in 2023 (18) compared to 2022 (10). Furthermore, malicious cyber actors were observed using more sophisticated techniques. One such technique includes a new partial encryption method where actors can change how much of a file is encrypted by ransomware. This technique makes the ransomware harder to discover by anti-malware solutions and increase the speed at which the adversary can encrypt victim files. In addition to financial extortion, these incidents often result in months of reduced operational capacity and potential reputational impacts.

Significant Ransomware Incidents in 2023

Port of Lisbon suffered from a ransomware attack that took down its website and internal computer systems. The malicious cyber actor reportedly stole financial reports, audits, budgets, contracts, cargo information, ship logs, and port documentation.⁹

Major European oil port terminals including SEA-Tank Terminal, which has storage facilities in Antwerp, and the cross-border Dutch and Belgian Amsterdam-Rotterdam-Antwerp oil trading hub were unable to process barges while oil prices were already at a seven year high.¹⁰

Reported Cyber Incident Trends

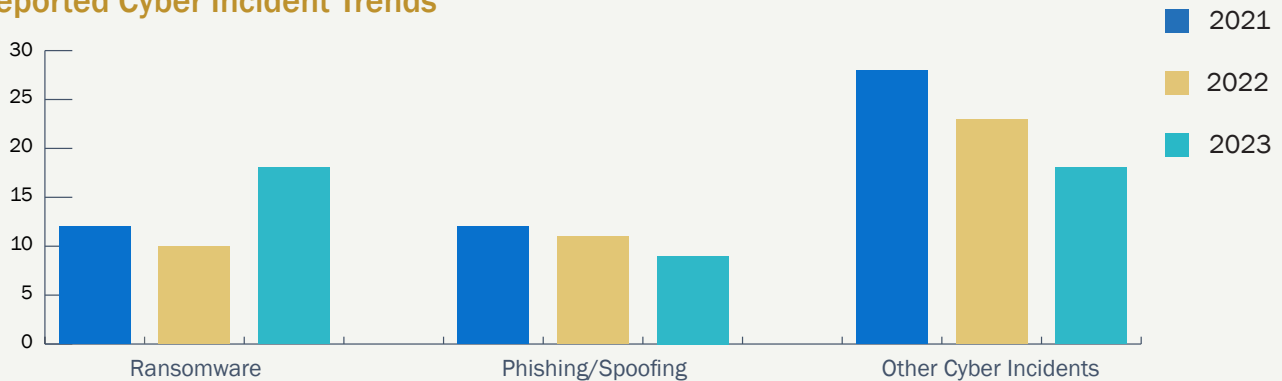


Figure 6. Reported Cyber Incidents from 2021-2023

⁷ Source: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>

⁸ Source: <https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary>

⁹ Source: <https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data>

¹⁰ Source: <https://www.securityweek.com/european-oil-port-terminals-hit-cyberattack/>

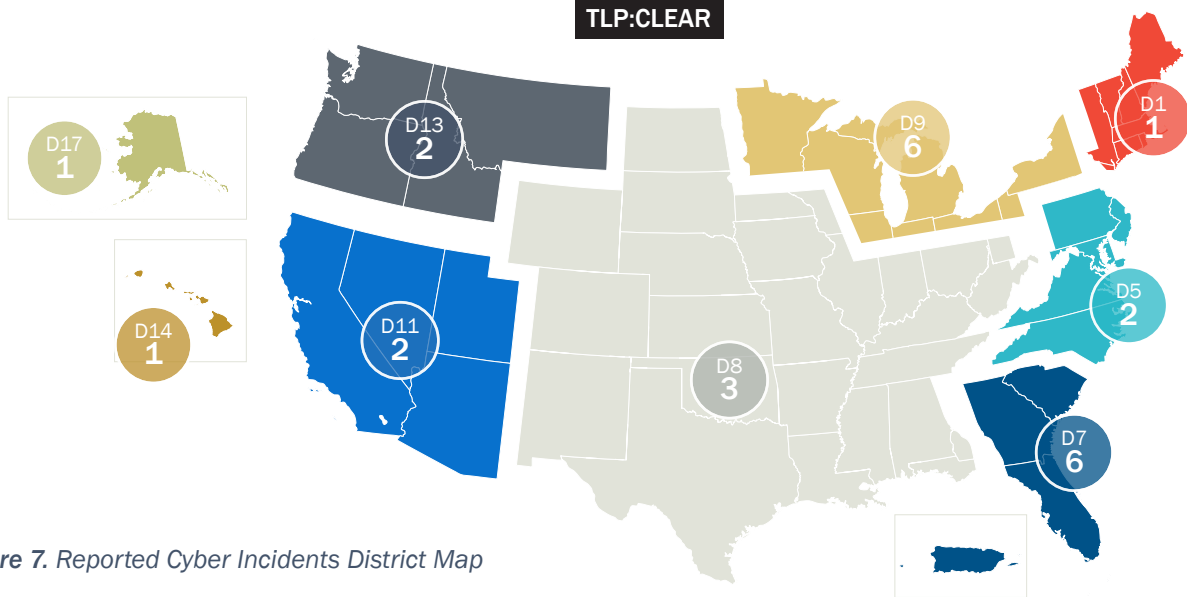


Figure 7. Reported Cyber Incidents District Map

Reported Cyber Incidents by Region Year over Year

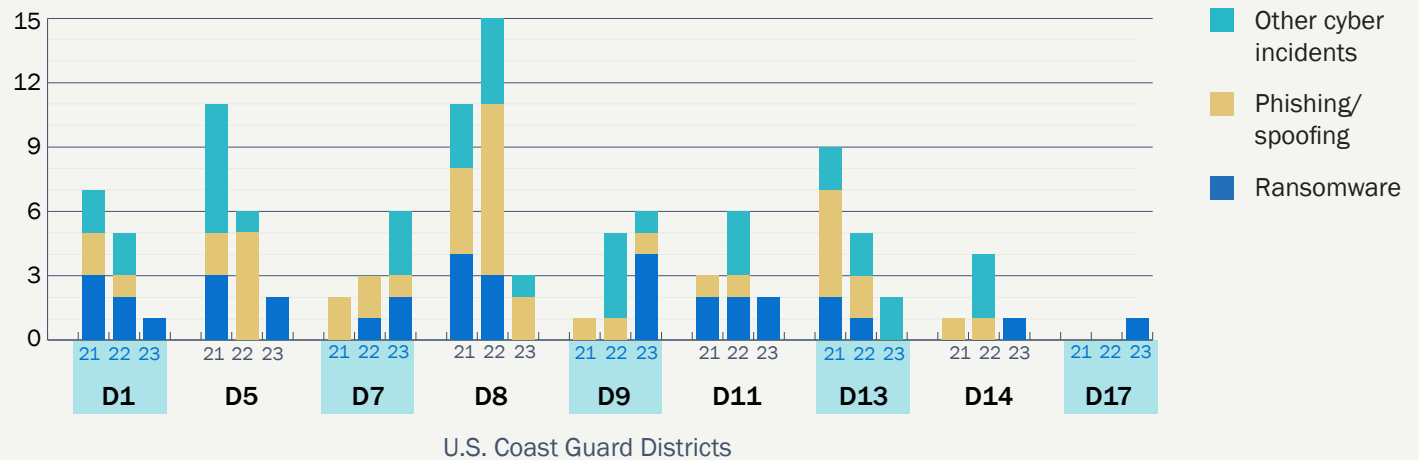


Figure 8. Reported Cyber Incidents by Region

Malicious cyber actors used a wide range of techniques to deliver effects and extort entities within the ME for financial gain or economic disruption. CGCYBER’s observations are bolstered by public reporting of similar campaigns targeting and impersonating major shipping entities. MCRB has observed a similar number of phishing/spoofing events in 2023 compared to other years. In 2023, 22% of incidents were phishing/spoofing events compared to 25% in 2022 and 20% in 2021.

continue to use in efforts to disrupt maritime operations. A DoS attack is when an attacker floods a target network with traffic causing it to crash or not respond, thereby denying legitimate users’ access. In April of 2023, the Port of Halifax in Nova Scotia and the ports of Montreal and Quebec in the province of Quebec had their websites taken out of commission by a DoS attack.¹¹ In this case, although operations were unhindered, it is important to have redundancy and countermeasures in place to reduce the operational impact of DoS attacks.

When it comes to other types of cyber incidents, Denial of Service (DoS) is a method attackers

¹¹ Source: <https://www.porttechnology.org/news/cyber-attacks-hit-canada-websites-down-for-three-major-ports/>

Maritime shipping companies continue to be targeted by cyber criminals. However, MCRB has also observed a significant increase in malicious cyber actors targeting maritime logistics integrators and technology service providers. Specific incidents in 2023 included ransomware attacks that significantly impacted global fortune 500 company, ABB Ltd.¹² and others.

In addition to targeting maritime logistics integrators and technology service providers, malicious cyber actors have also been observed exploiting vulnerabilities in public facing systems to obtain initial access to the networks of entities in the ME. For example, Microsoft reported that the threat actor Volt Typhoon was observed gaining unauthorized access to U.S. Critical Infrastructure provider networks by exploiting vulnerabilities in internet-facing devices.¹³ After gaining initial access, Volt Typhoon threat actors would leverage use of native administrative tools and capabilities, known as living off the land techniques, to find information on systems, discover additional devices, and exfiltrate data. Beyond Volt Typhoon, CLOP Ransom Gang were also observed exploiting vulnerabilities in internet-facing devices, specifically Progress Software's managed file transfer solution known as MOVEit Transfer. CLOP has been observed gaining initial access to MOVEit Transfer databases using an SQL injection vulnerability and leveraging their unauthorized access to steal data.¹⁴ Together,

these cases highlight the importance of properly protecting internet-facing devices, quickly patching devices for known vulnerabilities, and limiting internet-facing devices to only those that are necessary.

Timely information sharing among CGCYBER, other government agencies, and ME organizations continues to be key to identifying and disrupting malicious cyber actors. For example, from information shared by the Cybersecurity and Infrastructure Security Agency (CISA), CGCYBER notified an organization of a KEV¹⁵ on their infrastructure exposed to the internet. As a result, the company was able to identify unsuccessful attacks against their network and take action to mitigate future risk.

As the Coast Guard continues to combat illicit actions by malicious cyber actors, CGCYBER relies on cyber incident reports to the National Response Center (NRC) to activate response capabilities and increase awareness across the ME. Regulations require reporting by some entities of cyber incidents, but the Coast Guard urges all organizations in the ME to report all cyber incidents to the NRC. Through free-flowing multi-directional information sharing in the ME, the Coast Guard and ME organizations can best address these evolving cyber threats.

DP World, a stevedore company in Australia, disconnected from the internet following a cybersecurity breach that was detected on Friday November 10th, 2023. This attack significantly reduced the operational capabilities of the company, which manages about 40% of the goods that flow in and out of Australia, affecting its container terminals in Melbourne, Sydney, Brisbane and Western Australia's Fremantle.¹⁶

¹² Source: <https://new.abb.com/news/detail/103405/abb-provides-details-about-it-security-incident>

¹³ Source: <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

¹⁴ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>

¹⁵ Source: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

¹⁶ Source: <https://www.porttechnology.org/news/cyber-attacks-hit-canada-websites-down-for-three-major-ports/>

ATTACK PATHS USED ON ASSESSMENTS

While conducting assessments, CPTs emulate threats and employ known attack techniques to assess an organization's risk posture and highlight business impacts. These techniques are chained together to develop an Attack Path, allowing the CPTs to show how an attacker could move from initial access to full compromise of the network.

These Attack Paths are presented to support hardening recommendations provided at the end of the mission. Most Attack Paths used during threat emulation consist of three to five steps that align with specific Tactics, Techniques, and Procedures (TTPs) from the MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK®). [Appendix D: Summary of Attack Paths](#) includes a full list of all attack paths used by CPTs in 2023.

Common Initial Access Techniques

In 66% of assessments in 2023, [Phishing for Information \(T1598\)](#) provided CPTs credentials for an initial access vector. As was true in 2021 and 2022, this remains the most common initial access technique used by CPTs. Furthermore, this aligns with incident reports received by CGCYBER, which highlight that phishing remains a common TTP used against organizations in the ME.

Similarly, [Valid Accounts \(T1078\)](#) were used in 50% of assessments to allow CPTs to gain access to networks. These Valid Accounts were collected either through leaked credentials, [Gather Victim Identity Information: Credentials \(T1589.001\)](#), or the use of [Default Accounts \(T1078.001\)](#). In the majority of instances where CPTs found the use of Default Accounts, the accounts were used on critical externally facing network devices, meaning not only did the devices have Default Accounts, but the devices were also accessible to

anyone with internet access. This highly critical finding offers attackers an initial access vector to a network via a native process with little effort required.

Common Privilege Escalation Techniques

Also, remaining common, CPTs utilized [Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay \(T1557.001\)](#)¹⁷ in 72% of assessments. Upon having established initial access, CPTs were able to use this technique to capture hashed credentials and escalate privileges. This remains CPTs' most common privilege escalation technique as in most cases, the captured credentials included those of a Domain Administrator. Additionally, in missions where OT was within scope of the mission, 42% of the OT networks were accessed by CPTs using this technique.

Once password hashes were captured, generally either through [Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay \(T1557.001\)](#) or [OS Credential Dumping \(T1003\)](#), CPTs utilized [Brute Force: Password Cracking \(T1110.002\)](#) to crack hashes and gain the plain text passwords. In 89% of assessments, CPTs were able to crack password hashes, and where CPTs were able to crack a Domain Administrator account, the teams used these [Valid Accounts \(T1078\)](#) to access critical business systems and OT systems.

¹⁷ Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS), Server Message Block (SMB)

TOP 5 FINDINGS FROM ASSESSMENTS

This section highlights the Top 5 Findings CPTs observed during 2023 assessments. The Mitigations for these findings can be found in [Appendix F: Mitigations](#). Additionally, Appendix F includes a full breakdown of techniques used as Publicly Exploitable or Internally Exploitable findings.

Phishing for Information (T1598)

Phishing for Information is related to the **Phishing Technique (T1566)**; however, instead of attempting to use the email for malicious code execution, **Phishing for Information** is used to gain useful information, such as a username and password, from the phished user. During assessments, CPTs sent emails masquerading as various agents from the partner's organization (generally from the IT Department) with a link that would send users to a simulated malicious login portal created by the CPTs to capture user credentials. 10.8% of all phishing emails sent during threat emulation resulted in a click by a user. Additionally, of those who clicked the link, 6.7% of users provided credentials when requested.

Valid Accounts (T1078)

The most common initial access technique used during Assess missions was Valid Accounts. On CPT missions, Valid Accounts were gathered from publicly available sources, Gather Victim Identity Information: Credentials (T1589.001), or from using related techniques such as Phishing for Information, **Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)**, or **Steal or Forge Kerberos Tickets: Kerberoasting (T1558)**.

Additionally, once credentials were obtained, CPTs were able to bypass MFA mechanisms on several missions



In October of 2023, CISA, NSA, FBI, and Multi-State Information Sharing and Analysis Center (MS-ISAC) released the *Phishing Guidance: Stopping the Attack Cycle at Phase One*¹⁹ guide. This guide outlines techniques used by malicious actors and provides guidance for stakeholders to help prevent successful phishing attacks.

due to weak implementations. In 2022, CISA published a guide for Implementing Phishing Resistant MFA.¹⁸ [Figure 9](#) (next page), illustrates forms of MFA from weakest to strongest.

¹⁸ Source: <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>

¹⁹ Source: https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf

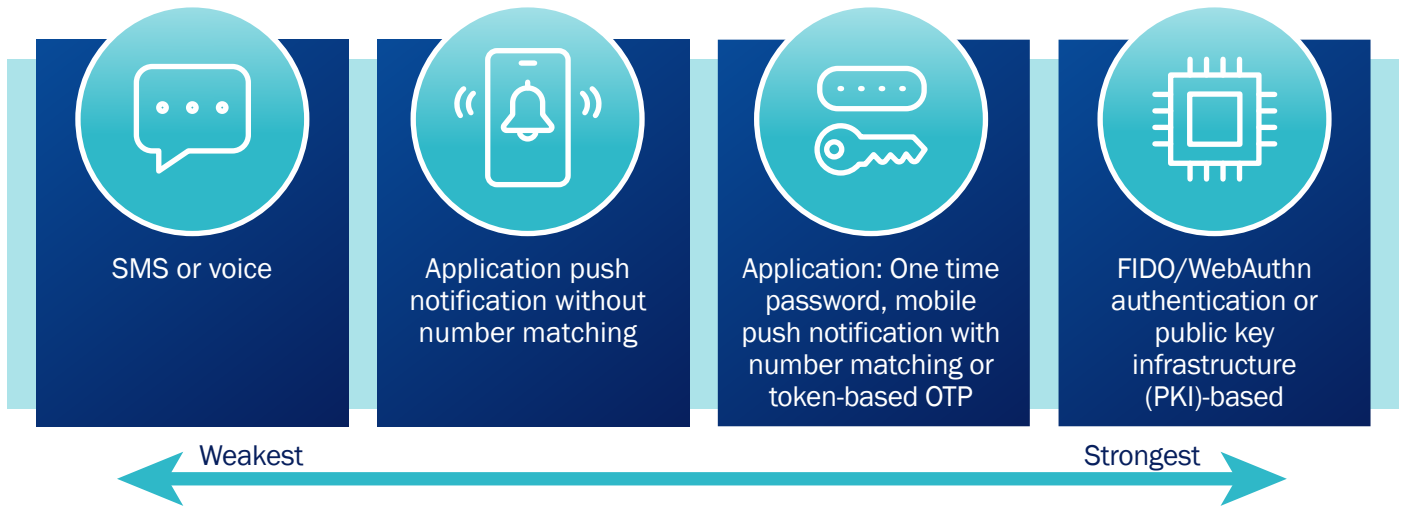


Figure 9. Spectrum of MFA Implementation

CPTs were able to bypass MFA implementations using short message service or Voice and Application Push notifications without number matching.

Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)

CPTs found that organizations remain vulnerable to LLMNR/NBT-NS Poisoning and SMB Relay attacks. These attacks leverage legacy protocols used for host identification to harvest credentials from within a network. LLMNR/NBT-NS Poisoning consists of an attacker inside the network responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) and directing traffic to an adversary-controlled system. Then, once a legitimate user attempts to access the portion of the network that is redirected to the adversary-controlled system, the adversary can use a myriad of techniques to directly obtain hashed or even sometimes plaintext credentials. [Figure 10](#) illustrates this process.

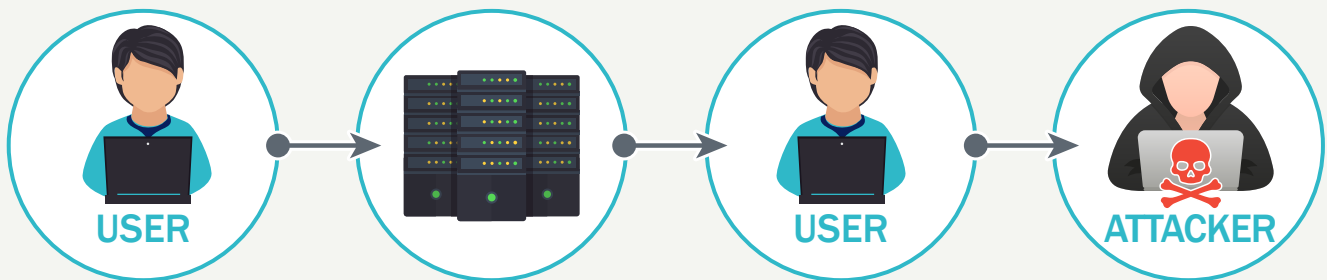


Figure 10. Adversary in the Middle-LLMNR/NBT-NS Poisoning and SMB Relay

If the adversary captures a password hash, they can pivot to the **Brute Force: Password Cracking** technique to determine the plaintext credentials.

Brute Force: Password Cracking (T1110.002)

The National Institute of Standards and Technology (NIST) Special Publication 800-63 Digital Identity Guidelines²⁰ recommends password policies include password length and password complexity requirements. Additionally, the NIST 800-63 provides suggestions for enforcement and consequences when not followed. Across the CY23 CPT missions, CPTs had little to no difficulty cracking passwords with a length of 12 characters or less. [Table 1](#) below provides metrics for average password policies across the ME.

Password History	Average Minimum Password Length	Lockout Threshold	MFA Enabled	Shared Admin Passwords	Default Passwords
83% of partners enforced password history as a complexity requirement	7 characters long	47% of partners did not have lockout threshold for failed attempts	44% of partners had MFA implemented	41.1% of partners reused admin passwords across accounts	94.4% of partners were found to have default credentials in use

Table 1. Averages of Observed Passwords

For over 17,000 discovered password hashes, CPTs were able to crack hashes for 60.1% of all passwords using hybrid dictionary and ruleset-based password cracking. As can be seen in the above table, the average minimum password length requirement enforced by organizations was only seven characters long. Of the cracked passwords, 97.1% of passwords had at least three complexity requirements (uppercase letter, lowercase letter, number, symbol), meaning that the complexity requirements were ineffective in creating strong passwords.

As was the case in 2022, CPT assessments validate NIST’s recommendation that **password length is the primary factor in characterizing password strength**.²¹ Our ruleset-based password cracking was able to detect most complexity techniques utilized in user-created passwords, making complexity requirements less effective. Updated NIST guidance²² recommends that “users should be encouraged to make their passwords as lengthy as they want” up to 64 characters. CISA’s 2023 password guidance for businesses recommends that user passwords be at least 16 characters long.

²⁰ Source: <https://pages.nist.gov/800-63-3/sp800-63b.html#sec5>

²¹ NIST SP800-63B: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

²² CISA’s 2023 password guidance for businesses: <https://www.cisa.gov/secure-our-world/require-strong-passwords>

²³ Source: <https://www.cisa.gov/secure-our-world/require-strong-passwords#:~:text=Provide%20an%20enterprise%20level%20password,for%20the%20password%20manager%20itself>

²⁴ Source: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Passwords Cracked	CPTs cracked 60.1% of all passwords captured in less than one week
Complexity of Cracked Passwords	Of the cracked passwords, 97.1% of passwords had at least three complexity requirements (uppercase letter, lowercase letter, number, symbol)
Length of Cracked Passwords	91.4% of all cracked passwords were 12 characters or less in length

Table 2. Password Cracking Observations

Additionally, CISA recommends²³ providing an enterprise-level password manager to encourage employees to use strong passwords and discourage employees for reusing passwords.²⁴

Patch Management

Vendors regularly release patches and updates to address existing and emerging security threats. These patches address various levels of risk, which are evaluated using the Common Vulnerability Scoring System (CVSS). The CVSS assigns vulnerabilities a score based on their severity. Failure to apply the latest patches can leave the system open to attack from publicly available exploits. The risk presented by missing patches and updates can vary; however, the most critical of vulnerabilities are those that are proven to be exploitable. These vulnerabilities are listed in CISA's KEV Catalog.²⁵ **Figure 11: Top KEVs Detected During CY23 Assess Missions** represents the vulnerabilities from the KEV Catalog most detected during CPT Assess missions. As can be seen, none of the most common KEVs are new, in fact the most recent KEV listed was released in September of 2021 and the average age of all the KEVs discovered was more than 5 years old. KEVs were detected in 61% of CPT assessments, which seems to indicate that many organizations within the ME are struggling to keep pace with regular software updates.

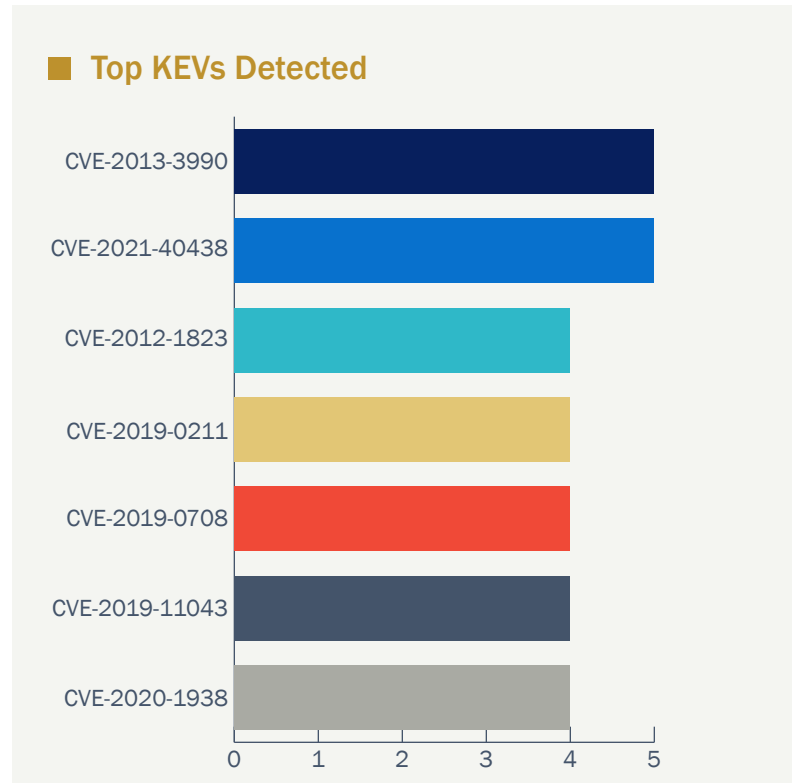


Figure 11. Top KEVs Detected

Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, we are layering new functionality and technology onto already intricate and brittle systems at the expense of security resilience.

– National Cybersecurity Strategy, March 2023²⁶

Of further concern, one of the two most common KEVs detected, CVE-2021-40438 was routinely detected on externally facing web servers, offering any attacker the ability to gain access to an organizations network from anywhere in the world. [Appendix C: Known Exploitable Vulnerabilities Detected on CPT Missions](#) contains descriptions of these vulnerabilities.

²⁵ Source: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

²⁶ Source: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

Use of Living off the Land

Recent reporting has continued to highlight the use of Living off the Land TTPs by malicious cyber actors. These TTPs include the use of built-in network tools combined with the exploitation of new or existing vulnerabilities to achieve initial access, escalate privileges, and meet their objectives while also avoiding detection. The findings discussed in this section are also often utilized by these actors. In order to best harden networks and prepare for response actions, CGCYBER recommends organizations review the above listed Findings as well as the Mitigations and Logging recommendations detailed in CISA's Cybersecurity Advisory (CSA): [AA23-144a](#).²⁷ Additionally, actors utilizing Living off the Land are reportedly targeting the Active Directory database (Ntds.dit) for potential exfiltration. This file contains critical information needed to manage a network including data such as user accounts and password information. Organizations should review the locations where their Ntds.dit is stored to ensure protections and logging are in place. To detect malicious Living off the Land activity, organizations should start with establishing an accurate baseline of how system utilities are used in an environment, retain logs for extended periods, and then investigate uses that differ from that baseline.



In May of 2023, CISA, NSA, FBI, and key international partners released a Joint Cybersecurity Advisory: *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* | CISA.²⁸ This advisory highlights the use of Living off the Land TTPs by the Volt Typhoon actor and the actors observed actively targeting networks across U.S. critical infrastructure sectors.

Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides.

– National Cybersecurity Strategy, March 2023²⁹

²⁷ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>

²⁸ Source: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

²⁹ Source: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

HUNT & INCIDENT RESPONSE RECAP

In 2023, Coast Guard CPTs completed seven Hunt and Incident Response (IR) missions in the ME, and two cooperative Hunt engagements with the Department of Defense (DOD) and partners for a total of nine missions.

Hunt and IR missions differ significantly from CPT assessments. Assessments are designed to highlight weaknesses and vulnerabilities, while Hunt and IR missions are designed to find malicious cyber activity (MCA) on a network. Hunt missions require a deliberate approach with a highly tailored deployment of a sensor suite composed of network, endpoint, and cloud-environment detection tools. IR missions occur at a much more rapid pace and the timeframe, and tools used are dependent on the details of the incident. [Figure 12](#) outlines the activities of CPT Hunt Missions.

■ Timeline of CPT Hunt Missions

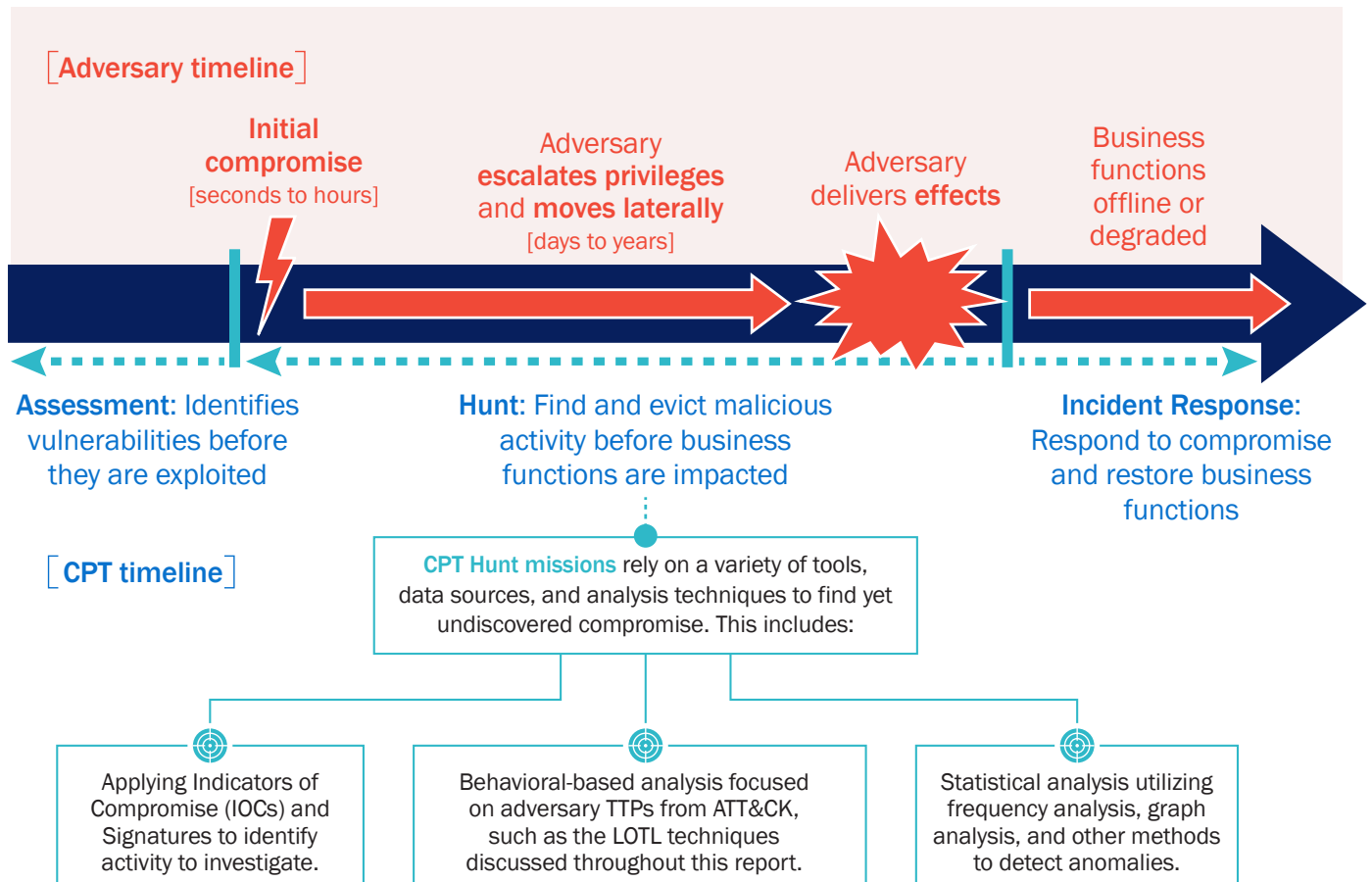


Figure 12. Timeline of CPT Hunt Missions

The following trends and insights were identified based on the 2023 Hunt and IR missions:

- The number of ME Hunt and IR missions remained consistent with 2022, but CGCYBER’s tactics and technologies have continued to evolve. Hunt mission length on average increased by approximately 200% in 2023.
- Four out of the seven missions in the ME were with partners without endpoint detection and response (EDR) capability. This put endpoints at risk and made it difficult for the local network defenders to detect most adversary techniques without third party assistance.
- The observed adversary attack paths were consistent with assessment results. The initial access techniques observed were **Phishing, Valid Credentials** (taking advantage of weak password policies), and **Exploit Public-Facing Application** (against unpatched or end-of-life systems).
- The top vulnerabilities and corresponding mitigation recommendations were also consistent with Assessment results. Top mitigation recommendations were to implement **strong password policies** and **MFA, privileged account management, network segmentation**, and to **patch/update systems**.

Table 3: 2023 Hunt and IR Mission Summary provides an overview of missions in the ME and the corresponding critical infrastructure sector. “Compromise detected” indicates whether MCA was identified with a high degree of confidence. “Time to Detect” identifies the estimated time between initial compromise and detection. “Operational Technology” indicates if OT critical to core business functions was connected to the network and within scope of the mission. “Cloud services” indicates if cloud-based technology critical to core business functions was connected to the network and within scope of the mission.








Mission Type	Sector	Compromise Detected	Operational Technology	Time to Detect	Cloud Services
 Hunt	Transportation (maritime)	Yes	No	>90 days	Yes (multiple providers)
 Hunt	Transportation (maritime port)	No	Yes	N/A	Yes (multiple providers)
 Hunt	Transportation (maritime port)	No	Yes	N/A	Yes
 Hunt	Transportation (maritime port)	No	Yes	N/A	No
 Hunt	Energy	Yes	Yes	>90 days	No
 Hunt	Water and Wastewater	Yes	Yes	>90 days	No
 Incident Response	Information Technology	Yes (Ransomware)	No	48 hours	No

Table 3. 2023 Hunt and IR Mission Summary

SECURING OPERATIONAL TECHNOLOGY

Much of today's OT evolved from the insertion of new IT capabilities into existing physical systems. Improvements in cost and performance have encouraged this evolution and resulted in many of today's "smart" technologies.³⁰

While this has increased the connectivity and efficiency of these systems it has also introduced new risks. Mitigations previously used to secure legacy OT systems such as physical security controls and complete network isolation are becoming obsolete as new smart technologies are being integrated with legacy systems. As a result, the path to exploiting these legacy systems has become simpler. Cybersecurity controls need to be considered when introducing new technology, not just for the new system, but for all systems with which it will integrate.

Over the past year, CPTs have focused additional attention towards assessing and providing hardening recommendations for OT systems. Across the various critical infrastructure sectors that make up the ME, CPT's found three common vulnerabilities present in almost every OT network.

There's control systems that are talking to the internet, components, cranes that have been bought overseas. They have, you know, components from countries that could potentially have malign intent. And so ensuring that the cyber readiness of the system is adequate is a role that the Coast Guard is engaged in. And, you know, we work with – we work regularly with the industry on exactly that.³¹

– ADM Linda Fagan, April 2023

1. Improperly Segmented Networks

- Lack of necessary access control making it easy to traverse from IT to OT networks
- Lack of demilitarized zones (DMZs) enabling direct connections between IT and OT networks and in some cases between the Internet and OT networks
- Lack of understanding of interconnections that may exist. Often OT networks are managed by different personnel than IT networks. This dynamic can lead to miscommunication and presents challenges to securing both

2. Use of End-of-Life Software

- 78% of CPT missions examining OT found End-of-Life software in use
- The most common End-of-Life system was the Windows 7 Operating System (OS)
- With the increased exposure of connected OT systems, an adversary can more easily access and exploit the vulnerable software within OT networks

3. Use of Legacy Protocols

- 78% of CPT missions examining OT found legacy protocols in use
- Legacy protocols such as Telnet and Server Message Block protocol 1 (SMBv1.0) are unencrypted making reconnaissance and lateral movement much easier for an adversary

³⁰ Source: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

³¹ Source: <https://www.csis.org/analysis/beyond-americas-coastline-conversation-admiral-linda-fagan-27th-commandant-united-states>

Hardening OT

The first step to hardening OT is to address the three most common vulnerabilities identified above:

1. Improper Network Segmentation
 - Audit all communications both to and from the OT network. Limit to maximum extent possible
 - Implement DMZs between networks.
 - Implement strict access control to OT
2. Use of End-of-Life Software
 - Audit all software running in the OT environment
 - Replace OS or software that is no longer supported where possible
 - Implement additional controls such as complete isolation or additional monitoring where software cannot be replaced
3. Use of Legacy Protocols
 - Upgrade to newer, more secure protocols
 - Upgrade hardware when older hardware is incompatible

Fixing these common issues is only the beginning as risks to OT Networks continue to grow. OT/industrial control system (ICS) devices and designs are publicly available, often incorporate vulnerable IT components, and include external/remote connections that increase their attack surfaces. Malicious cyber actors targeting OT are doing so with specific objectives in mind and dedicating significant resources to achieving

their goals. While it is impossible to prevent yourself from being targeted, the following best practices identified by the National Security Agency (NSA) and CISA³² can help counter some adversary activity.

1. **Limit exposure of system information** - To the extent possible, avoid disclosing information about system hardware, firmware, and software in any public forum
2. **Identify and secure remote access points** - Many vendor-provided devices maintain access capabilities as an auxiliary function. Creating a full “connectivity inventory” is a critical step in securing access to a given system
3. **Limit tools and scripts** - Limit access to network and control system application tools and scripts to legitimate users performing legitimate tasks on the control system
4. **Conduct regular security audits** - Perform an independent security audit of systems, especially of third-party vendor access points and systems. Do not solely depend on the views, opinions, and guidance of the vendor/integrator that designed, developed, or sold the system
5. **Implement a dynamic network environment** - Static network environments provide malicious actors with persistent knowledge of the system. Periodically making manageable network changes can go a long way to disrupt previously obtained access by a malicious actor

Digital systems help make the marine transportation system the most economical, efficient, environmentally friendly way to transport products worldwide. These same digital systems also create complicated interdependencies, vulnerabilities and risks, and their prevalence in the industry is only growing.³³

– Rear Admiral Wayne Arguin, Assistant Commandant for Prevention Policy

³² Source: https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF

³³ Source: <https://www.maritime-executive.com/magazine/combating-maritime-cyberattacks>

■ Securing Your Operational Technology Environment

IT

Impacts

- Initial Access, Persistence, Privilege Escalation

Questions to Consider

- What are my most critical IT systems?

Mitigations

- Limit Exposure of System Information, Conduct Regular Security Audits, Implement a Dynamic Network Environment

DMZ

Impacts

- Lateral Movement, Initial Access (OT), Persistence (OT)

Questions to Consider

- How do I limit communications between IT and OT?

Mitigations

- Identify and Secure Remote Access Points, Restrict Tools and Scripts, Conduct Regular Security Audits, Implement a Dynamic Network Environment

Operational Management

Impacts

- Command and Control (OT), Inhibit Response Function (OT), Impair Process Control (OT)

Questions to Consider

- Who is responsible for OT Security? Who is responsible for system updates? What does our agreement say?

Mitigations

- Identify and Secure Remote Access Points, Restrict Tools and Scripts, Conduct Regular Security Audits, Implement a Dynamic Network Environment

Field Level

Impacts

- Loss of availability, loss of control, Loss of Productivity and Revenue, Denial of Control

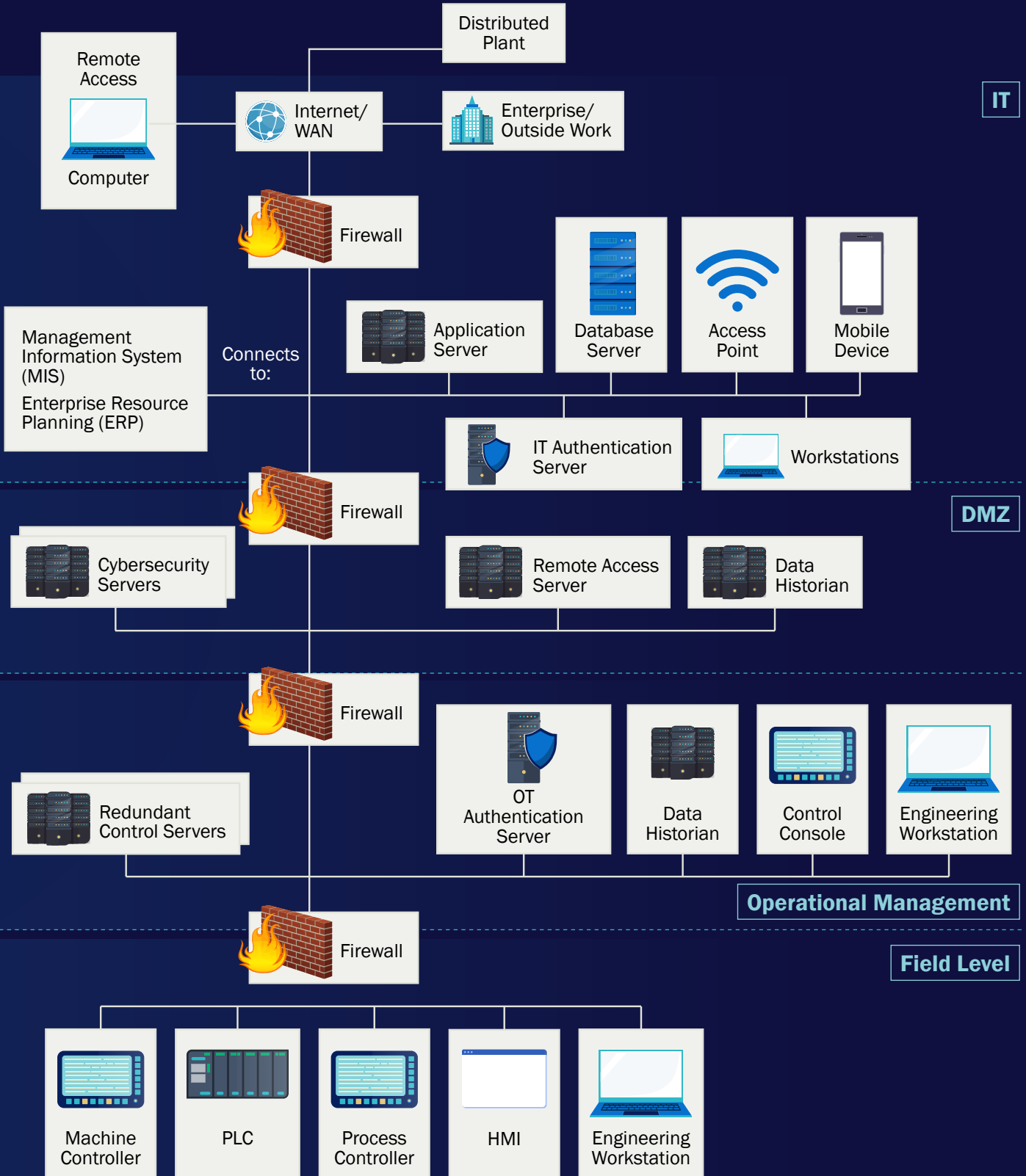
Questions to Consider

- What are my most critical OT systems? What disaster recovery and business continuity plans do I have in place?

Mitigations

- Identify and Secure Remote Access Points, Conduct Regular Security Audits

Figure 13. Securing Your Operational Technology Environment



IT

DMZ

Operational Management

Field Level

PORT SECURITY GRANT PROGRAM

The Port Security Grant Program (PSGP) is one of four grant programs the Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) leverage to focus their transportation infrastructure security activities. These grant programs are part of a comprehensive set of measures authorized and appropriated by the Congress and awarded by the Executive Branch to help strengthen the nation’s critical infrastructure.³⁴

Since 2013, enhancing cybersecurity has been an eligible program priority area. PSGP priority areas are set annually and are listed in the DHS Notice of Funding Opportunity (NOFO) available at <https://www.fema.gov/>. The PSGP provides funds to state, local, and private sector maritime partners to support increased port-wide risk management and to protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. The PSGP is subject to the annual appropriations process and awards project funding on a competitive basis across multiple priority areas, including cybersecurity. While there is no guarantee for funding, CGCYBER encourages those eligible entities within the ME to apply for the grant program as a potential source of funding to improve cybersecurity across the MTS. **Figure 15:** FY23 Port Security Grants Awards show that in FY23, the PSGP granted \$12,948,400 to cyber based projects, of which 20% received CPT assistance.

■ Port Security Grant Program Average Funding Awarded to Cyber Projects

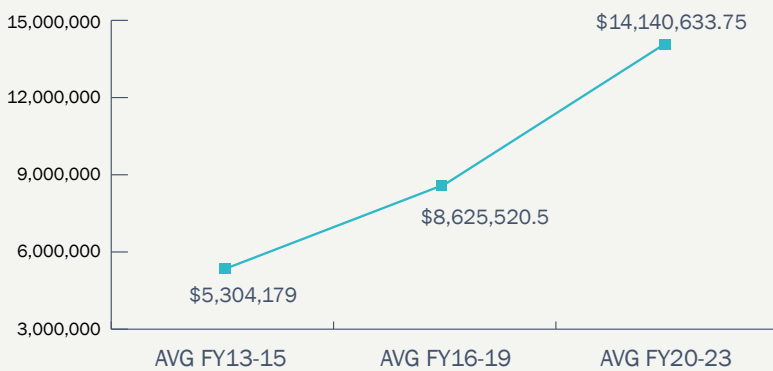


Figure 14. PSGP Average Funding Awarded

■ FY23 Port Security Grants

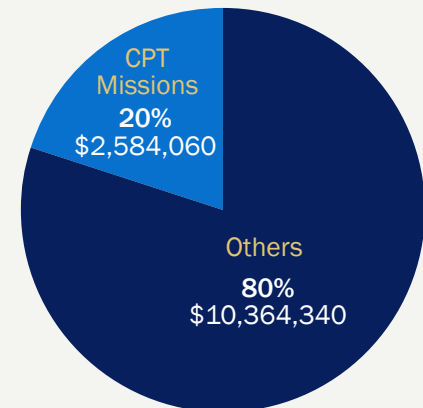


Figure 15. FY23 Port Security Grants Awards

Total funding awarded to cyber based projects during the first five years compared to the past five years shows an average increase of \$5.64M in funding awarded, consistent with a DHS-wide push for increased cybersecurity readiness.³⁵

³⁴ Source: <https://www.fema.gov/print/pdf/node/652255>

³⁵ Source: <https://www.fema.gov/grants/preparedness/port-security#totals>

LOOK AHEAD TO 2024

Ransomware on the Rise: Cybercrime will Continue to Impact the ME

In 2023, a variety of new vulnerabilities impacted the ME and novel threat actors targeted these vulnerabilities. ME organizations often employ network-connected software and hardware specialized for maritime functions, in which vulnerability identification and patching may be slower than for mainstream IT applications.

Reported ransomware incidents within the ME increased markedly from 2022 to 2023. MCRB received more reports of ransomware incidents in the first quarter of 2023 than all of 2022. Based on CPT mission and cyber events investigated by MCRB, financial incentives appear to have remained the driving motivation behind most threat activity in the ME, which is consistent with 2023 industry reports on ransomware.³⁶ The financial impact to compromised organizations also remained high.³⁷ Based on the spike in the number of reported ransomware incidents in the ME, the continued financial incentives for threat actors, and the vulnerabilities impacting technologies within the ME, it is likely that financially motivated cybercrime will continue to be of significant impact in 2024. The Coast Guard expanded its capacity for cyber operations in 2023 and plans to expand partnerships with industry partners in the ME and Government stakeholders to combat this trend of ransomware and cybercrime.

³⁶ Verizon found that 94.6% of data breaches in 2023 were financially motivated, and that 24% of data breaches involved ransomware (Source: [verizon.com/dbir/](https://www.verizon.com/dbir/)).

³⁷ This finding is also consistent with Industry reports. IBM identified the average cost of a data breach to be \$4.45 million in 2023, an increase of 2.3% from 2022 (Source: <https://www.ibm.com/account/reg/signup?formid=urx-52258>).

³⁸ Mitre ATLAS™ is a research project based on the widely used Mitre ATT&CK™ framework. More information is available at [MITRE | ATLAS™ \(https://atlas.mitre.org/\)](https://atlas.mitre.org/).

Artificial Intelligence and the ME

New Artificial Intelligence (AI) models and algorithms have the capability to deliver benefits to business operations in the ME. Over the last two years, Coast Guard CPTs have already encountered multiple ME organizations leveraging AI-enabled software to improve prediction models for the flow of goods, and for cybersecurity threat monitoring and detection. As with any new technology, AI applications may also introduce new vulnerabilities. Cybersecurity risks from AI can be grouped into two general categories:

1. **Cybersecurity risks of AI-enabled systems.** AI-enabled systems usually require access to large quantities of sensor or operational data to produce the desired insights. This may require internet connectivity, elevated privileges, and/or connections to sensitive OT systems. These features could make AI-enabled systems attractive targets for malicious actors. The MITRE ATLAS™³⁸ has already identified more than 50 attacker techniques that can be used to target AI models.
2. **Threats from malicious actors using AI.** AI-based technology can be used to support traditional goals of malicious actors. Advances in generative AI may lead to an increase in the sophistication of social-engineering attacks that leverage **phishing**, social media, phone calls/voice authentication, or images. AI models or algorithms may also be developed by more advanced threat actors to discover new vulnerabilities, automate portions of the attack process, or evade detection.

Adoption of AI-based technology within the ME is likely to continue to increase. Although understanding of the cybersecurity risks and mitigations is in its infancy, ME organizations should still apply known cybersecurity best practices to AI-enabled systems. This includes minimizing interfaces directly exposed to the Internet, monitoring system activity, and implementing strict access control policies. CGCYBER will continue to advance its understanding of these technologies and determine how to better assess, monitor, and utilize new AI-based systems.

Smart Port Technologies

From 2021 to 2023, Coast Guard CPTs and MCRB have observed an increasing use of the term “Smart Port” or “Smart Port Technologies” by both Industry and Government stakeholders. The use of the term “Smart Port” varies depending on the source, but the underlying goal is to leverage emerging technology to automate port operations, improve the efficiency and reliability of port systems, and ultimately realize financial gains. Below are some technology trends based on Coast Guard CPT and MCRB observations that could be categorized under the Smart Port umbrella:

1. Ports are utilizing new connection technologies to connect more systems to the network, increase bandwidth, and decrease latency. Connection technologies include 5G cellular, improved Wi-fi technology, expanding Satellite constellations (such as Starlink™), and network modules to adapt Microcontroller-based devices to be network-

connected (such as with Azure Sphere™). These connection technologies have allowed maritime entities to connect systems responsible for crane operations, identifying and transporting containers, and physical access control to the network. Additionally, within the ME, this trend has been observed in enhanced network connectivity between Terminal Operating System (TOS) software, crane systems, maritime vessels, and ICS's for power, water, and manufacturing processes.

2. Leveraging cloud-based computing, storage, and other cloud provider services. CGCYBER's 2022 CTIME Report outlined the rapid adoption of cloud services by ME organizations. The trend continued in 2023, with most CPT mission partners using at least one cloud hosting provider to meet core business functions.
3. An increased emphasis on remote collection and use of sensor data from the physical world.
4. Leveraging more complex algorithms (that may or may not rely on AI-based modeling) to develop business insights, and in some cases control port processes.

As Smart Port Technologies are increasingly relied upon in 2024 and the years ahead, connecting a diverse range of devices and increasing automation of port operations means the impact of a cybersecurity compromise could increase significantly. Understanding the risks present in Smart Port Technologies, and implementing strong security measures, will be crucial to maintaining safe and reliable U.S. port operations.

Conclusion

The analysis and recommendations presented in this report provide a roadmap towards a more secure and resilient ME. In this era of unprecedented connectivity, securing our critical infrastructure is imperative. By embracing these insights and taking decisive action, we can navigate the future with confidence, support the flow of trade, and protect the MTS.

APPENDIX A

MARTIME CYBER ALERTS

Maritime Cyber Alerts

01-23 Threat from People's Republic of China State-Sponsored Cyber Actor VOLT TYPHOON

This Maritime Cyber Alert details the threat from the PRC state-sponsored cyber actor VOLT TYPHOON to the MTS. It identifies the TTPs of the group, as well as mitigation measures MTS partners should take.³⁹

02-23 BlackBasta Ransomware Group

This Maritime Cyber Alert provides information on the Ransomware as-a-Service (RaaS) group known as BlackBasta. It details the criminal organization's motives, known activities in the MTS, mitigation measures MTS partners can take, and the known indicators of compromise (IOCs).⁴⁰

03-23 Threat from CIOp Ransomware Group

This Maritime Cyber Alert provides information on the RaaS group known as CIOp. It details the criminal organization's motives, tactics, targeted applications and systems utilized by the group against MTS partners, mitigation measures MTS partners can take, and the known IOCs.⁴¹

Maritime Cyber Bulletins

01-23 Threats to OT and Shoreside Transportation Operations

This Maritime Cyber Bulletin provides information on two potential threats to MTS entities. The first is a reported cyber incident that impacted Estes Express Lines, a Less-than-Truckload (LTL) shipping company which could have a downstream impact to MTS partners due to disruption in cargo movement. The second addresses vulnerabilities affecting Rockwell Automation Products which are used in Liquefied Natural Gas (LNG) infrastructure and operations within the MTS.⁴²

02-23 Critical Cisco IOS XE Software Web User Interface (UI) Privilege Escalation Vulnerability Identified

This Maritime Cyber Bulletin provides information on a previously unknown exploit when users of Cisco's IOS XE software enable the web UI and expose it to the internet or to untrusted networks. Recommendations and resources available to help mitigate the threat posed by this CRITICAL vulnerability.⁴³

³⁹ Source: <https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Alert%2001-23%20VOLT%20TYPHOON%20TLP%20CLEAR.pdf>

⁴⁰ Source: <https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Alert%2002-23%20BLACKBASTA%20TLP%20CLEAR.pdf>

⁴¹ Source: <https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Alert%2003-23%20TLP%20CLEAR.pdf>

⁴² Source: <https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Bulletin%2001-23.pdf>

⁴³ Source: <https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Bulletin%2002-23%20TLP-CLEAR.pdf>

APPENDIX B

OBSERVED CYBER CRIMINAL ORGANIZATIONS

MCRB observed or received reports of the following actors while conducting cyber event investigations in the ME during 2023.

ALPHV/BlackCat

ALPHV/BlackCat uses ransomware to encrypt files, threatens to delete files, and then threatens to conduct a Distributed Denial of Service (DDoS) attack if payment is not made to pressure victims to pay the ransom. For example, in 2023 ALPHV/BlackCat compromised a shipping company and gained access to information including personal data, financial/accounting information, and logistics documents.

Royal

Royal Ransomware is believed to be comprised of experienced malicious cyber actors from other ransomware groups. Royal utilizes multi-extortion methods such as data theft, harassment, and DDoS attacks. For example, in 2023 Royal compromised an offshore drilling company and exfiltrated sensitive information including employee documentation, contracts, and information on key projects.

LockBit

LockBit was one of the most active groups in 2023, using RaaS. The group is known to ask for a ransom for sensitive information as well as a ransom for the encryption key. For example, in 2023 LockBit compromised a shipping company with the extent of the compromise currently unreported.

BlackBasta

BlackBasta utilizes double extortion; ransoming decryption keys and threatening to post sensitive information online. BlackBasta primarily targets English speaking countries. For example, in 2023 BlackBasta compromised a vessel operation company gaining access to the corporate network and sensitive finance and logistics information.

BianLian

BianLian has shifted focus to primarily data exfiltration ransoms rather than data encryption. For example in 2023, BianLian compromised a port facility and exfiltrated sensitive data from e-mail accounts. BianLian reportedly demanded a ransom for approximately \$470,000.

CLOP

CLOP utilizes double extortion; ransoming the decryption key and threatening to publicize sensitive information. In 2023, using of a previously unknown exploit for cloud infrastructure, CLOP compromised thousands of companies, including some organizations in the ME. The victim list does not mean the facilities were successfully exploited; however, CLOP has been using a name-and-shame tactic to demand ransom.

Ransom Cartel

The Ransom Cartel has been linked to REvil ransomware group, performing double extortion attacks, and deploying RaaS. In 2023, the group compromised an organization closely linked to the ME, resulting in the shutdown of software servers and degrading associated web-based systems.

APPENDIX C

KNOWN EXPLOITABLE VULNERABILITIES DETECTED ON CPT MISSIONS

This appendix contains all the vulnerabilities from CISA's KEV Catalog observed at more than one organization. Information for these vulnerabilities comes from the NIST National Vulnerability Database, <https://nvd.nist.gov/>.

Common Microsoft KEV

Microsoft WinVerifyTrust function Remote Code Execution

CVE-2013-3900

CVSS: 7.6

CWE-20

Occurrences: 5

Description: The WinVerifyTrust function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate Portable Executable (PE) file digests during Authenticode signature verification, which allows remote attackers to execute arbitrary code via a crafted PE file, aka "WinVerifyTrust Signature Validation Vulnerability."

"BlueKeep" Microsoft Windows Remote Desktop Remote Code Execution Vulnerability

CVE-2019-0708

CVSS: 9.8

CWE-416

Occurrences: 34

Description: A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using Remote Desktop Protocol (RDP) and sends specially crafted requests, aka "Remote Desktop Services Remote Code Execution Vulnerability."

Example: In 2019, researchers from University of Rijeka and Kobe University demonstrated the disruption of a ship's Electronic Chart Display and Information System (ECDIS) by exploiting the BlueKeep vulnerability on board a Japanese training vessel.⁴⁴

⁴⁴ Source: Svilicic, Boris, et al. "Maritime cyber risk management: An experimental ship assessment." The Journal of Navigation 72.5 (2019): 1108-1120. https://www.researchgate.net/profile/Matthew-Rooks/publication/330917771_Maritime_Cyber_Risk_Management_An_Experimental_Ship_Assessment/links/5c6a2f63299bf1e3a5af0d16/Maritime-Cyber-Risk-Management-An-Experimental-Ship-Assessment.pdf

Microsoft SMBv1 Remote Code Execution/Information Disclosure Vulnerability (multiple CVEs)

<p>CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148</p>	<p>CVSS: 8.1</p>	<p>CWE-20 CWE-200</p>	<p>Occurrences: 21</p>
<p>Description: The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka “Windows SMB Remote Code Execution Vulnerability.” Vulnerabilities labeled CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, CVE-2017-0146, and CVE-2017-0148 are all similar.</p>			
<p>Example: In 2017, NotPetya malware exploited SMBv1 vulnerabilities resulting enterprise-wide disruptions to A.P. Møller – Mærsk A/S networks.⁴⁵</p>			

Common Apache KEV

Apache HTTP Server-Side Request Forgery (SSRF)

<p>CVE-2021-40438</p>	<p>CVSS: 9.0</p>	<p>CWE-918</p>	<p>Occurrences: 32</p>
<p>Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache Hypertext Transfer Protocol (HTTP) Server 2.4.48 and earlier.</p>			
<p>Example: CISA reported the presence of this vulnerability within Apache HTTP Servers used as part of Siemens OT networks.⁴⁶</p>			

⁴⁵ Source: Greenberg, Andy. Sandworm: A new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers. Anchor, 2019.

⁴⁶ Source: <https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-06>

Apache Tomcat Improper Privilege Management “GhostCat” Vulnerability

CVE-2020-1938

CVSS: 9.8

N/A

Occurrences: 21

Description: When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50, and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed returning arbitrary files from anywhere in the web application and processing any file in the web application as a Java Server Pages (JSP). Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defense-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51, or 7.0.100 or later. Several changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51, or 7.0.100 or later will need to make configuration changes to their configurations.

Example: HelpNet Security reported GhostCat as the 6th most common exploited vulnerability in the wild for calendar year 2020.⁴⁷

Apache Tomcat Remote Code Execution Vulnerability

CVE-2017-12617

CVSS: 8.1

CWE-434

Occurrences: 15

Description: When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46, and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the read-only initialization parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

Example: According to Threat Post, CVE-2017-12617 was the most common publicly exploitable vulnerability throughout 2017 related to products using Apache Tomcat as the underlying web container.⁴⁸

⁴⁷ Source: <https://www.helpnetsecurity.com/2021/02/03/2020-top-exploited-vulnerabilities/>

⁴⁸ Source: <https://threatpost.com/securing-network-perimeter/175043/>

Apache Log4j2 Remote Code Execution Vulnerability

CVE-2021-44228	CVSS: 10	CWE-917 CWE-400 CWE-20 CWE-502	Occurrences: 15
<p>Description: Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) Java Naming and Directory Interface (JNDI) features used in configuration, log messages, and parameters do not protect against attacker-controlled Lightweight Directory Access Protocol (LDAP) and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.</p>			
<p>Example: According to Mandiant, this vulnerability was one of the Top 10 vulnerabilities exploited to target chemical and critical manufacturing companies in late 2021.⁴⁹</p>			

Apache HTTP Server Privilege Escalation Vulnerability

CVE-2019-0211	CVSS: 7.8	CWE-416	Occurrences: 3
<p>Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with Multi-processing module (MPM) event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.</p>			

⁴⁹ Source: Mandiant Advantage. (2022). (publication). Industry Snapshot: Chemicals & Materials (Q4 2021). Retrieved 2023, from <https://advantage.mandiant.com/reports/22-00001271>

Other Technologies KEV

Apache HTTP Server-Side Request Forgery (SSRF)

CVE-2012-1823

CVSS: 7.5

CWE-20

Occurrences: 2

Description: sapi/cgi/cgi_main.c in hypertext Preprocessor (PHP) before 5.3.12 and 5.4.x before 5.4.2, when configured as a Common Gateway Interface (CGI) script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

PHP FastCGI Process Manager (FPM) Buffer Overflow Vulnerability

CVE-2019-11043

CVSS: 9.8

CWE-120
CWE-787

Occurrences: 2

Description: In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for Fast Common Gateway Interface (FCGI) protocol data, thus opening the possibility of remote code execution.⁵⁰

⁵⁰ Source: <https://nvd.nist.gov/vuln/detail/CVE-2019-11043>

APPENDIX D

SUMMARY OF CPT ATTACK PATHS

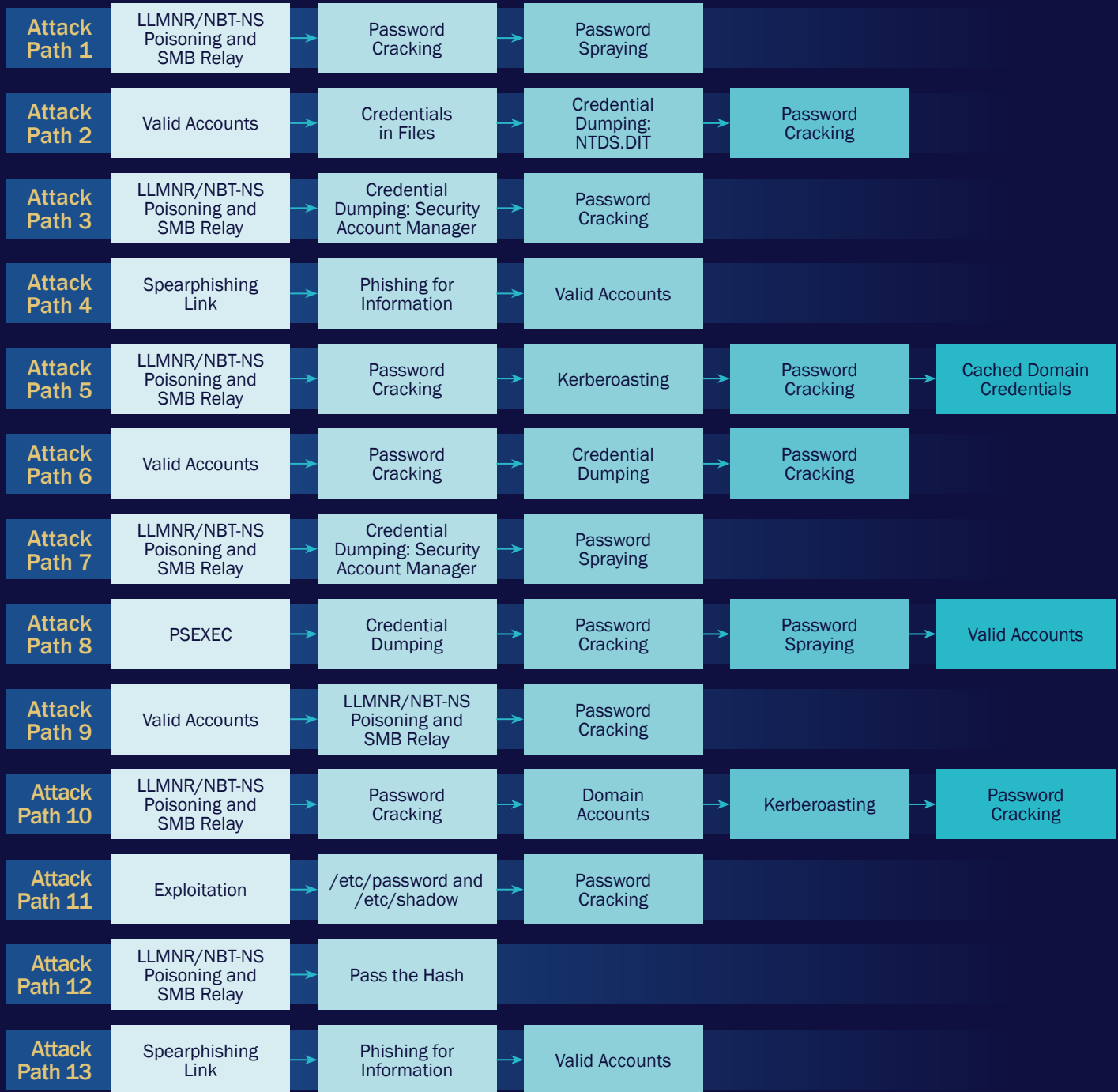


Figure 16. Attack Path Examples

APPENDIX E

SUMMARIZED FINDINGS OF 2023 CPT ASSESS MISSIONS

Table 4: MITRE ATT&CK® Techniques used on 2023 CPT Missions provides the total counts of MITRE ATT&CK® Techniques used during the 2023 CPT Missions.

Mission Type	2022	2023
Brute Force: Password Cracking	22	30
Valid Accounts	12	23
Phishing: Spearphishing Link	6	18
Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	8	15
Exposed Public-Facing Application	4	8
Data from Local Shared Drive	3	6
OS Credential Dumping: Cached Domain Credentials	1	4
Modify Authentication Process	3	3
Unsecured Credentials	2	3
Steal or Forge Kerberos Tickets: Kerberoasting	7	2
Account Discovery: Domain Account	3	2
Network Shares Discovery	6	1
Modify Authentication Process	4	1
Drive-by Compromise	3	1
Indirect Command Execution	2	1
User Execution: Malicious Link	8	0
Network Denial of Service	3	0
Develop Capabilities: Digital Certificates	1	0
Remote Services	1	0

Table 4. MITRE ATT&CK® Techniques Used by Year

APPENDIX F MITIGATIONS

Mitigation Actions from Partners

Six months following CPT assessments, partners are asked to provide a status of their actions in response to the recommend CPT Mitigations. As shown below in [Table 5: Mitigation Status – CY21, CY22, and CY23 Comparison](#), in 2023 partners Fully or Partially Mitigated 79% of all findings.

All Findings	CY21	CY22	CY23 ⁵¹
Fully Mitigated	48%	52%	33% ↓
Partially Mitigated	33%	36%	46% ↑
Accepted Risk	5%	3%	14% ↑
False Positive	2%	1%	0% ↓
No Action Taken to Date	12%	8%	7% ↓

Table 5. Mitigation Status – CY21, CY22, & CY23 Comparison

Of note in CY23, CPTs made an adjustment to the gathering of metrics post assessment. In CY21 and CY22, the follow-up interviews were completed six months after the delivery of the report, which were provided 60 days after the team completed the out-brief, ultimately resulting in gathering the metrics at approximately eight months post assessment. However, in CY23, the follow-up interviews were conducted six months after the assessment out-brief. This is believed to have caused a shift in the metrics resulting in a significant percentage of mitigation actions shifting more to the Partially Mitigated category as organizations had less time to review and complete the recommended mitigations.

Another noteworthy trend was the sharp increase in Accepted Risks, up 14% from last year. CPTs attribute this to the significant increase of OT assessed this year. The lifecycle for OT is generally much longer than IT, and as discussed earlier in the report, OT is commonly found to be running End-of-Life software. CPTs believe that this combined with the expense and business impacts that come with replacing OT, resulted in organizations accepting more risks than in previous years.

Most Common Findings

CGCYBER tabulated a complete list of all reported findings documented in assessments and mapped each finding directly to one or more MITRE ATT&CK[®] mitigation recommendations. [Table 6: Common Mitigation Recommendations](#) (next page) summarizes this data and compares this years findings to those found in 2021 and 2022. “Mapped Findings” represents the mitigations associated with the CPTs’ findings, and the following discussion on Common Mitigations contains greater detail for each mitigation.

⁵¹ Based on data for first half of CY23

Mitigation Recommendation	Mapped Findings		
	CY21	CY22	CY23
Password Policies	1 st	1 st	1 st (-)
Multi-Factor Authentication	4 th	2 nd	2 nd (-)
Privileged Account Management	—	4 th	3 rd ↑
Disable or Remove Feature or Program	—	13 th	4 th ↑
Network Segmentation	—	10 th	5 th ↑
User Training	7 th	6 th	6 th ↓
Update Software	6 th	5 th	7 th ↓
Filter Network Traffic	—	3 rd	8 th ↓
User Account Management	—	7 th	9 th ↓
Audit Systems	—	12 th	10 th ↑

Table 6. Common Mitigation Recommendations

As can be seen above, the top three most common recommended mitigations remain fairly stable from last year and are centered around issues found with Authentication and Authorization weaknesses. Making the biggest jump this year was Disable or Remove Feature or Program. CPTs attribute this to the addition of OT to the scope of most assessments where (as discussed earlier in the report) legacy protocols were identified. Overall, however, the recommendations identified similar actions to that of the 2022 report.

Of note, in October 2023, CISA released “CSA AA23-278A: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations.”⁵² This CSA shared findings from assessments, hunts, and incident response activities conducted by NSA and CISA teams. The findings discussed in CSA AA23-278A are very similar CGCYBER’s top mitigations based on CPT missions. This similarity suggests that the most common vulnerabilities and needed mitigations are consistent across all U.S. critical infrastructure.

⁵² Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

Common Mitigations

To address those findings and mitigations discussed earlier in this appendix, organizations should review this section. **Figure 17: Common Mitigations User Resistance & Costs** provides a snapshot of typical levels of user resistance, upfront costs, and recurring costs to common mitigations.

Top 10 Recommended Mitigations			
	User Resistance	Upfront Cost	Recurring Cost
Common Mitigation #1 Password Policies			
Common Mitigation #2 Authentication			
Common Mitigation #3 Privileged Account Management			
Common Mitigation #4 Disable or Remove Feature or Program			
Common Mitigation #5 Network Segmentation			
Common Mitigation #6 User Training			
Common Mitigation #7 Update Software			
Common Mitigation #8 Filter Network Traffic			
Common Mitigation #9 User Account Management			
Common Mitigation #10 Audit Systems			

User Resistance
Relative resistance of mitigation implementation from user base

Low Medium High

Upfront/Recurring Costs
Relative costs to procure, implement, and/or maintain mitigation measures

Low Medium High

Figure 17. Common Mitigations User Resistance & Costs

Common Mitigation #1: Password Policies

A password policy is a set of rules and guidelines that dictate how users should create and manage their passwords for a given system or organization. Password policies are put in place to ensure the security and integrity of systems and the data they contain. Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose easily guessed passwords. One effective technique is to use pass phrases; using multiple words can add significant length to a password but still require significant mathematical computation to crack. Password managers offer greater security and convenience for the use of passwords to access online services. Greater security is achieved principally through the capability of most password manager applications to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault.⁵³



LENGTH

Password length is the primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.



COMPLEXITY

Composition rules increase the difficulty of guessing user-chosen passwords. Research has shown, however, that users respond in very predictable ways to the requirements imposed by composition rules.



RANDOMLY CHOSEN SECRETS

Randomly chosen secrets that are uniformly distributed will be more difficult to guess or brute-force attack than user-chosen secrets meeting the same length and complexity requirements.



HISTORY

Passwords cannot be reused for a certain number of iterations to avoid the possibility of an attacker using a previously used password.



EXPIRATION

Passwords must be changed at a certain interval (e.g., every 90 days) to keep them current and secure.

Figure 18. Password Policy Recommendations

⁵³ Source: NIST Special Publication 800-63 Digital Identity Guidelines, available at: <https://pages.nist.gov/800-63-3/>

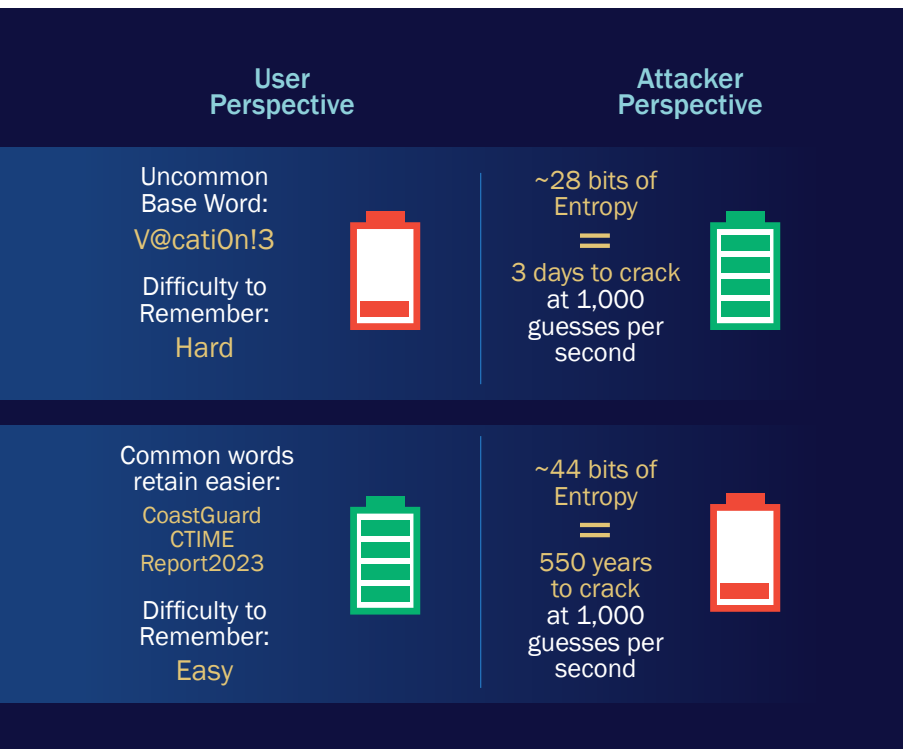


Figure 19. Password Strength Perspectives

Service (non-user) Accounts:

- Ensure strong password length (**ideally 25+ characters**) and complexity for service accounts (non-user accounts) and that these passwords periodically expire.⁵⁴
- Also consider using Group Managed Service Accounts or another third-party product such as password vaulting.

Figure 19: Password Strength Perspectives depicts analysis published by Randall Munroe on xkcd.com and provides a visual representation of secure password policies.⁵⁵

For additional technical steps for mitigations, network defenders should reference *Table 9: Recommendations for Network Defenders to Mitigate Poor Credential Hygiene* from CISA's CSA [AA23-287A](#).⁵⁶

Common Mitigation #2: Multi-Factor Authentication

MFA is a security method in which a user is required to provide multiple forms of identification to access a system or account. MFA typically involves at least two of the following three authentication factors:⁵⁷

- Something the user knows, such as a password or a PIN.
- Something the user has, such as a security token or a smartphone.
- Something the user is, such as a fingerprint or a facial recognition.

To enable MFA, implement two or more means to authenticate to a system, such as a username, password, and a token from a physical smart card or token generator. A common example of MFA is using a password (something the user knows) in combination with a fingerprint scan or a code sent to the user's phone (something the user has or something the user is). Malicious cyber actors deploy several techniques to bypass or misuse some common MFA methods. These attack vectors include Signaling System Seven (SS7) Interception, Credential Harvesting, Push Bombing, and Subscriber Identify Module (SIM) Swapping.⁵⁸ *Figure 20* (next page) maps the techniques an adversary may use to bypass MFA.

⁵⁴ Source: <https://sbscyber.com/resources/kerberoasting-the-potential-dangers-of-spn-accounts>

⁵⁵ Source: <https://xkcd.com/936/>

⁵⁶ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

⁵⁷ Source: NIST Special Publication 800-63 Digital Identity Guidelines, available at: <https://pages.nist.gov/800-63-3/>

⁵⁸ Source: <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>

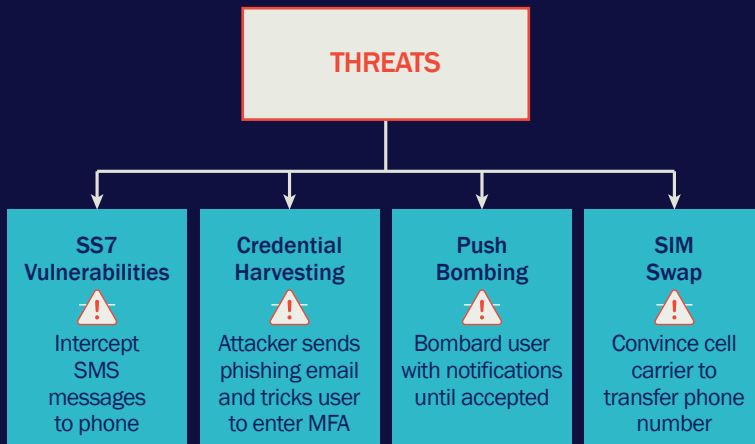


Figure 20. MFA Bypass Techniques Used by Threats

For additional technical steps for mitigations, network defenders should reference *Table 7: Recommendations for Network Defenders to Mitigate Weak or Misconfigured MFA Methods* from CISA's CSA [AA23-287A](#).⁵⁹

Common Mitigation #3: Privileged Account Management

Privileged account management is the process of creating, managing, and monitoring privileged accounts in a computer system or network. Privileged accounts are those accounts with elevated permissions or access rights, granting users the ability to perform actions that could significantly impact the security and functionality of a network. These accounts include administrator accounts, root accounts, and service accounts and are usually given to personnel who require elevated privileges to carry out their responsibilities such as system administrators and IT managers. As a result of these elevated permissions, privileged accounts pose a high-security risk if not properly monitored and

controlled. Malicious cyber actors often target these accounts, and if they gain the elevated privileges, they can exploit the accounts to compromise sensitive data, manipulate systems, and execute malicious activities.

The main objective of privileged account management is to reduce the risk of security breaches and other malicious actions by controlling access to sensitive data and resources. This can be done by implementing strict access controls, such as password policies, two-factor authentication, and limiting the number of privileged accounts, as depicted in *Figure 21: Privileged Account Management (PAM) Access Controls* (next page).

⁵⁹ Source: <https://pages.nist.gov/800-63-3/>

LOCK DOWN ADMIN ACCOUNTS

- Require a separate account for day-to-day user activity by users with administrator accounts
- **Do not use administrative accounts to access the web or email**
- Limit Powershell execution policy to administrators only
- Only use local administrator accounts when absolutely necessary
- Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runs
- Set up and follow process for privileged account creation, modification, use, and permissions
- Enforce unique passwords for administrator and user account

LEAST PRIVILEGE FOR USER ACCOUNTS

- Limit Powershell execution policy to administrators only
- Remove users from the local administrator group on systems
- **Do not create service accounts with administrative privileges**
- Limit access to Administrator or root accounts
- Limit permissions so that users and user groups cannot create tokens
- Ensure containers are not running as root by default

Figure 21. Privileged Account Management (PAM) Access Controls

For additional technical steps for mitigations, network defenders should reference *Table 7: Recommendations for Network Defenders to Mitigate Improper Separation of User/Administrator Privilege* from CISA's CSA [AA23-287A](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-287a).⁶⁰

Common Mitigation #4: Disable or Remove Feature or Program

Disabling or removing features or programs is a proactive mitigation that involves identifying and addressing potential security vulnerabilities by either deactivating specific software functionalities or removing unnecessary programs. This mitigation is crucial for minimizing an organization's attack surface, reducing the likelihood of exploitation, and enhancing overall network security.

⁶⁰ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-287a>

Vulnerability Reduction

- Review all running features or programs and identify those not essential to business operations. Disabling or removing unnecessary features or programs reduces the number of potential entry points for attackers.
- Vulnerabilities within software components can serve as gateways for malicious activities, and by mitigating these risks, organizations can significantly enhance their overall security posture.

Minimize Attack Surface

- Every enabled feature or installed program increases the attack surface. Mitigating through disabling or removal narrows this attack surface, making it more challenging for attackers to find and exploit vulnerabilities.
- Zero-day exploits target vulnerabilities that are unknown to the software vendor, making them particularly dangerous. By proactively disabling unnecessary features or removing obsolete programs, organizations reduce the risk of falling victim to such exploits, as attackers have fewer opportunities to exploit unknown vulnerabilities.

Implement Software Lifecycle Management

- Organizations should implement a Software Lifecycle Management Process to review software and plan for upgrades and/or replacement. Over time, software features become obsolete or unsupported, exposing organizations to increased security risks. By regularly reviewing and mitigating security threats through the removal or disabling of outdated features and programs, organizations ensure that their systems stay current and resilient against evolving threats.

Common Mitigation #5: Network Segmentation

Network Segmentation involves dividing enterprise networks into segments or subnetworks to enhance security by controlling access and restricting communications between different segments. This approach aims to prevent lateral movement of threats, limit the impact of a potential breach, and improve overall network resilience. In the event of a security breach, attackers often seek to move laterally within the network to escalate their privileges and reach valuable assets. Network Segmentation acts as a barrier, restricting the lateral movement of threats and preventing them from easily traversing the entire network. By dividing the network into segments, organizations can compartmentalize risks. If a security incident occurs in one segment, it does not automatically compromise the security of other segments. This containment strategy reduces

the overall risk exposure and helps in localizing and addressing security issues more effectively. Additionally, Network Segmentation enables organizations to implement more granular access controls based on user roles, device types, or specific security requirements. This ensures that users and devices only have access to the resources necessary for their functions, reducing the attack surface and potential points of vulnerability.

Network Segmentation can isolate critical assets and sensitive data from the broader network. Organizations should establish a list of Critical Assets, and then create segmented zones for those assets. This can contain potential security incidents, preventing unauthorized access to vital resources and minimizing the impact of a breach. Additionally, organizations

should review connections between IT and OT networks. CPTs were regularly able to gain access to OT networks from IT networks despite assurances from local network administrators that there were no connections.

For additional technical steps for mitigations, network defenders should reference *Table 4: Recommendations for Network Defenders to Mitigate Lack of Network Segmentation* from CISA's CSA [AA23-287A](#).⁶¹

Common Mitigation #6: User Training

User training is a vital mitigation factor because it helps to educate users about the risks and threats. User training minimizes the likelihood of human error and enables compliance with regulatory requirements. By providing training on topics such as safe browsing, email security, and password management, users are better equipped to identify and mitigate potential security risks. *Figure 22: User Training – Best Practices* identifies some standard cyber hygiene best practices for average users.

- **PASSWORD REUSE**
Don't reuse the same password on multiple websites/applications
- **DRIVE-BY COMPROMISE**
Lock your computer and, if applicable, remove smart card when not in use
- **CREDENTIALS IN CLEAR-TEXT**
Don't store passwords in unencrypted files
- **SPEARPHISHING LINKS**
Don't click on unrecognized links
- **SPEARPHISHING ATTACHMENTS**
Don't open attachments from unrecognized senders
- **DOMAIN SQUATTING**
Look out for websites with certificate errors; it may be a fake website
- **CREDENTIAL HARVESTING**
Make sure you are on a legitimate site when entering a username/password
- **UNAUTHORIZED APPLICATIONS**
Don't use unauthorized applications without approval

Figure 22. User Training – Best Practices

Common Mitigation #7: Update Software

- Perform regular software updates to mitigate exploitation risk.
- Ensure operating systems and browsers are using the most current version.
- Update password managers regularly by employing patch management for internal enterprise endpoints and servers.
- Keep system images and software updated and migrate to Simple Network Management Protocol version 3 (SNMPv3).
- Update all browsers and plugins and use modern browsers with security features turned on.
- Update software regularly by employing patch management for externally exposed applications and internal enterprise endpoints and servers.
- Patch the Basic input/output System (BIOS) and other firmware as necessary to prevent successful use of known vulnerabilities.
- Update software regularly to include patches that fix Dynamic Link Library (DLL) side-loading vulnerabilities.

⁶¹ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

For additional technical steps for mitigations, network defenders should reference *Table 5: Recommendations for Network Defenders to Mitigate Poor Patch Management* from CISA's CSA [AA23-287A](#).⁶²

Common Mitigation #8: Filter Network Traffic

Filtering network traffic is an important aspect of network security and management. It provides the following benefits:

- Protects the network and authorized users from malicious traffic.
- Improves network performance, security, and monitoring.
- Provides the ability to enforce compliance requirements.

Figure 23: *Network Traffic Filtering* provides use cases for filtering network traffic. Keep in mind, every network is different and network traffic filtering should be adapted to each individual network.

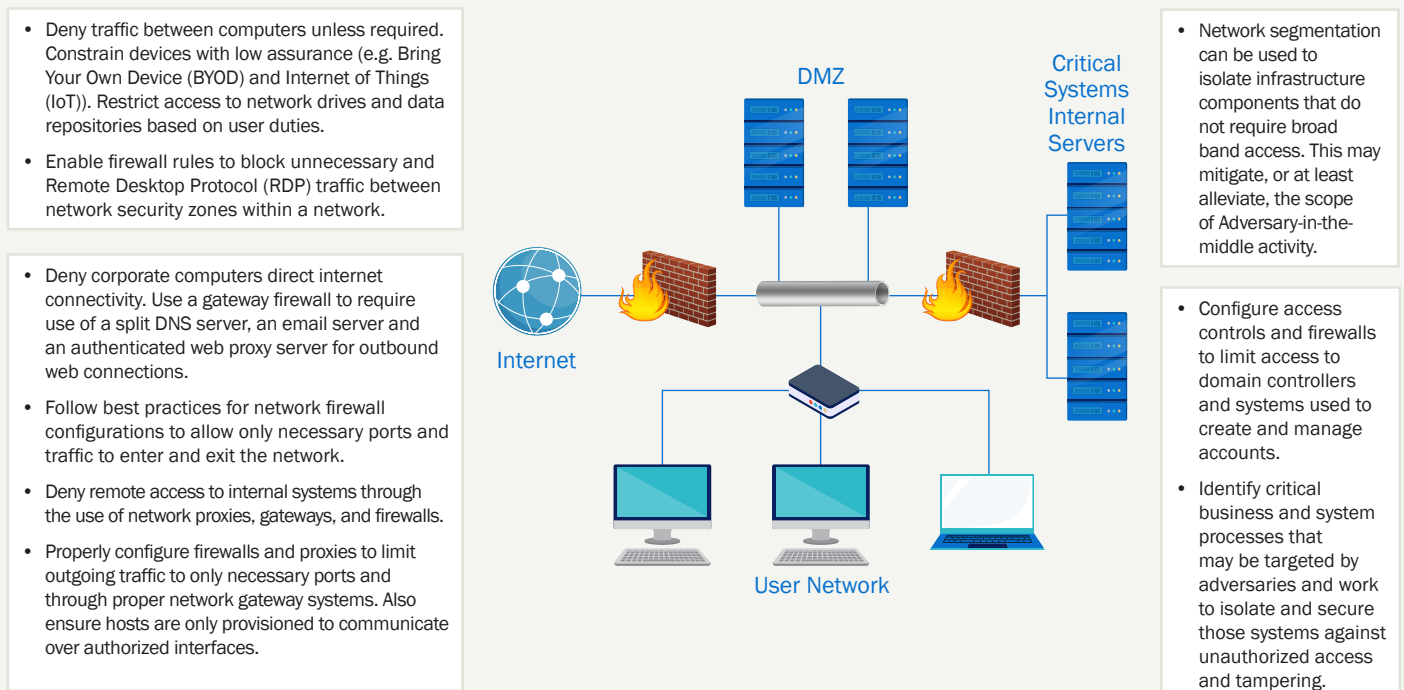


Figure 23. *Network Traffic Filtering*

Network traffic can be filtered three different ways, inbound, outbound, and protocol-based. Implementation is generally accomplished by either network appliances or configured directly on the endpoint. *Figure 24* (next page) offers some general guidance for organizations looking to implement network traffic filtering.⁶³

For additional technical steps for mitigations, network defenders should reference *Table 4: Recommendations for Network Defenders to Mitigate Lack of Network Segmentation* from CISA's CSA [AA23-287A](#).⁶⁴

⁶² Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

⁶³ Source: <https://attack.mitre.org/mitigations/M1037/>

⁶⁴ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

GENERAL GUIDELINES

- External unauthorized users should not be able to access internal corporate systems and should be blocked
- Web server/resources for external internet users should be hosted in a DMZ with limited authorized protocols
- Traffic filtering can protect against denial-of-service attacks, work with your Internet Service Provider to resolve if under attack
- Implement web proxies for endpoints and dedicated servers to provide services such as DHCP and DNS to avoid spoofing
- Only allow necessary ports to enter and exit the network, which includes blocking unnecessary protocols between security zones
- Disable legacy protocols to prevent a potential for an Adversary-in-the-middle attack (AITM)

Figure 24. Network Traffic Filtering General Guidelines

Common Mitigation #9: User Account Management

User account management is managing “the creation, use, and permissions associated to user accounts” from MITRE ATT&CK®.⁶⁵ This is related to Privileged Account Management, but focused on the fact that accounts should follow the principle of least privilege and separation of duties.⁶⁶

COMMON ATTACK METHODS/VECTORS

- Access Token Manipulation
- Account Manipulation
- Brute Force Attacks
- Remote Services (i.e., SSH or RDP)

GENERAL GUIDELINES

- Follow least privilege & implement separation of duties practice
 - Separate standard user from administrator
 - Local administrator separated from other types of user accounts
 - Domain administrator separated from other administrators
- Enforce logging, especially on admin type actions and monitor logs
- Define criteria for group memberships and establish a group owner to monitor
- Regularly review user accounts and disable users immediately if no longer affiliated with organization
- Regularly review standard user permissions and utilize Group Policy to enforce
- If password or credentials have been compromised then immediately reset account
- Limit specific services to only the necessary accounts
- For service accounts, enforce strong passwords and only use for affiliated service

Figure 25. User Account Management and General Guidelines

⁶⁵ Source: <https://attack.mitre.org/mitigations/M1018/> <https://attack.mitre.org/mitigations/M1018/>

⁶⁶ Source: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

For additional technical steps for mitigations, network defenders should reference *Table 6: Recommendations for Network Defenders to Mitigate Bypass of System Access Controls* from CISA's CSA [AA23-287A](#).⁶⁷

Common Mitigation #10: Audit Systems

Auditing systems is a fundamental practice in cybersecurity that involves a regular review of systems to evaluate existing vulnerabilities, configurations, and access controls. The primary goal of auditing systems is to ensure the integrity, confidentiality, and availability of information.

Vulnerability Audits

- Organizations should conduct regular vulnerability checks to identify potential security vulnerabilities within an organization's infrastructure
- Many organizations rely automated vulnerability scanning products to conduct the audits. This significantly improves the timeliness of the audits, and most can be scheduled to run during off-hours to limit potential network/resource impacts.

Configuration Audits

- Organizations should audit system configurations to ensure enterprise-wide policies are being enforced and systems are secured as expected.
- Organizations should also audit local access controls to prevent unauthorized users from obtaining and maintaining persistent access.

Detection of Anomalous Activities

- Organizations should conduct audits of local logs to review system performance, access records, and user activities.
- Organizations should also ensure changes in system configurations are monitored as unauthorized or unintended changes can introduce security risks, and auditing systems. Reviewing these logs allows organizations to promptly identify and rectify any alterations that could compromise the integrity of the IT environment.

Common Detections: Logging

In addition to mitigations, MITRE ATT&CK[®] also provides detection recommendations. *Figure 26: Detection/Logging Recommendations* (next page) summarizes the recommended detection techniques to successfully capture the MITRE ATT&CK[®] techniques used in the attack path steps.

For additional recommendations to improve network monitoring, network defenders should reference *Table 3: Recommendations for Network Defenders to Mitigate Insufficient Internal Network Monitoring* from CISA's CSA [AA23-287A](#).⁶⁸

⁶⁷ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

⁶⁸ Source: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

PROCESS & PROCESS METADATA

- Process Modification: Changes made to a process, or its contents, typically to write and/or execute code in the memory of the target process (ex. Sysmon **EID 8**)
- Process Creation: Birth of a new running process (ex. Sysmon **EID 1** or Windows **EID 4688**)
- Process Termination: Exit of a running process (ex. Sysmon **EID 5** or Windows **EID 4689**)
- Process Access: Opening of a process by another process, typically to read memory of the target process (ex. Sysmon **EID 10**)

USER ACCOUNTS

- Authentication: An attempt by a user to gain access to a network or computing resource, often by providing credentials (ex. Windows **EID 4625** or `/var/log/auth.log`)
- Creation: Initial construction of a new account (ex. Windows **EID 4720** or `/etc/passwd` logs)
- Modification/Deletion:
 - Removal of an account (ex. Windows **EID 4726** or `/var/log access/authentication` logs)
 - Changes made to an account, such as permissions and/or membership in specific groups (ex. Windows **EID 4738** or `/var/log access/authentication` logs)
- Metadata: Contextual data about an account, which may include a username, user ID, environmental data, etc.

NETWORK TRAFFIC

- Data transmitted across a network (ex. Web, DNS, Mail, File, etc.), that is either summarized (ex. Netflow and/or captured as raw data in an analyzable format (ex. PCAP)
- Network connection creation: Initial construction of a network connection, such as capturing socked information with a source/destination IP and port(s) (ex. Windows **EID 5156**, Sysmon **EID 3**, or Zeek `conn.log`)
- Network traffic content: Logged network traffic data showing both protocol header and body values (ex. PCAP)
- Network traffic flow: Summarized network packet data, with metrics, such as protocol headers and volume (ex. Netflow or Zeek `http.log`)

APPLICATION LOG CONTENT

- Prioritize for critical high-risk business systems
- Logging, messaging, and other artifacts provided by third-party services (ex. metrics, errors, and/or alerts from mail/web applications)

COMMAND EXECUTION

- Invoking a computer program directive to perform a directive to perform a specific task (ex. Windows **EID 4688** of `cmd.exe` showing command-line parameters `~/.bash_history`, or `~.zsh_history`)

Figure 26. Detection/Logging Recommendations

APPENDIX G

COAST GUARD CYBER COMMAND OVERVIEW

Coast Guard Cyber Command

The mission of CGCYBER is to conduct operations and deliver effects in and through cyberspace to defend Coast Guard Cyberspace, enable Coast Guard Operations, and protect the MTS. CGCYBER maintains three Strategic Lines of Effort:

1. Defend and operate the U.S. Coast Guard Enterprise Mission Platform (EMP).
2. Protect the MTS.
3. Operate In and Through Cyberspace.

To meet Line of Effort 2, “Protect the MTS,” CGCYBER created the MCRB as well as the Coast Guard CPTs within the Cyber Effects and Protection Division.

Cyber Protection Teams

CPTs are 39-person teams structured as a deployable force. CPTs can deploy to augment Coast Guard Commanders in the execution of time-critical or nationally significant prevention and response cyber activities. The Coast Guard currently has four CPTs with three deployable elements each:

- 1790 CPT is based in Washington, D.C., and attained Full Operational Capability (FOC) in May 2021.
- 2013 CPT is based in Washington, D.C., and attained FOC in August 2022.
- 2003 CPT is based in Alameda, CA. CGCYBER established the team in August 2022.
- 1941 CPT is the first Coast Guard Reserve CPT. The team was established in August 2022.

CPTs deploy in support of Coast Guard Operational Commanders and mission-partners through three core mission types:

1. Assessment: Providing threat emulation, vulnerability enumeration, and hardening recommendations.
2. Hunt Missions: Proactively identifying adversary presence on networks and systems.
3. Incident Response: Consisting of interagency coordination, forensic support, and remediation guidance.

A standard CPT operation involves close coordination with the supported Operational Commander with a duration of two to eight weeks depending on the specific circumstances. Coast Guard CPTs completed more than 100 cyber operations since December 2020. The pace of CPT missions continues to increase as the Coast Guard expands its cyber capabilities.

Maritime Cyber Readiness Branch

Modeled after the Coast Guard's National Centers of Expertise, the MCRB is focused on raising cybersecurity readiness, resilience, and response postures throughout the MTS. MCRB members form a uniquely qualified cross-functional team, combining both marine safety expertise and cyber incident response proficiency to translate complex cybersecurity details into measurable operational risk.

The MCRB provides direct support to Operational Commanders at Sectors, Districts, and Areas to enhance the Coast Guard's ability to prevent and respond to cyber-related MTS disruptions. When a security incident is cybersecurity-related, the MCRB plays a crucial role in helping operational field units assess risk. Working with MTS organizations, the MCRB also provides outreach, engagements, and information sharing services to increase cyber literacy at our ports. When an organization is compromised, the MCRB investigates, working with other government agencies and industry partners to notify the victim, identify next steps, recommend mitigation action (to include CPT support), and obtain status updates until the issue is resolved and business operations are restored.

APPENDIX H

LIST OF ACRONYMS

AI	Artificial Intelligence
AJP	Apache Jserv Protocol
BIOS	Basic Input/Output System
CGCYBER	U.S. Coast Guard Cyber Command
CGI	Common Gateway Interface
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Coast Guard	United States Coast Guard
CPT	Cyber Protection Team
CSA	Cybersecurity Advisory
CTIME	Cyber Trends and Insights in the Marine Environment
CVSS	Common Vulnerability Scoring System
CySO	Cybersecurity Officers
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DOD	Department of Defense
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
EDR	Endpoint Detection and Response
EMP	Enterprise Mission Platform
FCGI	Fast Common Gateway Interface
FEMA	Federal Emergency Management Agency
FOC	Full Operational Capability
FSO	Facility Security Officer
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
IOC	Initial Operational Capability
IR	Incident Response
IT	Information Technology

JNDI	Java Naming and Directory Interface
JSP	Java Server Pages
KEV	Known Exploitable Vulnerabilities
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LNG	Liquefied Natural Gas
LTL	Less-than-Truckload
MCRB	Maritime Cyber Readiness Branch
ME	Marine Environment
MFA	Multi-Factor Authentication
MITRE ATT&CK®	MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework
MPM	Multi-Processing Module
MTS-ISAC	Multi-State Information Sharing and Analysis Center
MTS	Maritime Transportation System
MTSS-C	Marine Transportation Systems Specialist – Cyber
NBT-NS	NetBIOS Name Service
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
NRC	National Response Center
NSA	National Security Agency
OS	Operating System
OT	Operational Technology
PAM	Privileged Account Management
PE	Portable Executable
PHP	Hypertext Preprocessor
PRC	People’s Republic of China
PSGP	Port Security Grant Program
RaaS	Ransomware-as-a-Service
RDP	Remote Desktop Protocol
SIM	Subscriber Identity Module
SMB	Server Message Block
SNMPv3	Simple Network Management Protocol version 3
SQL	Structured Query Language
SRMA	Sector Risk Management Agency
SS7	Signaling System Seven
TTP	Tactics, Techniques, and Procedure
UI	User Interface

APPENDIX I

LIST OF FIGURES

Figure 1. Critical Infrastructure Sectors with ME Organizations	9
Figure 2. 2023 Coast Guard CPT Missions	10
Figure 3. CPT Missions per Critical Infrastructure Sector	11
Figure 4. CPT Missions by Type Year over Year	11
Figure 5. 2023 Cyber Events Investigated by MCRB and Local Coast Guard Units.....	12
Figure 6. Reported Cyber Incidents from 2021-2023	13
Figure 7. Reported Cyber Incidents District Map	14
Figure 8. Reported Cyber Incidents by Region	14
Figure 9. Spectrum of MFA Implementation	18
Figure 10. Adversary in the Middle-LLMNR/NBT-NS Poisoning and SMB Relay	18
Figure 11. Top KEVs Detected	20
Figure 12. Timeline of CPT Hunt Missions	22
Figure 13. Securing Your Operational Technology Environment	26
Figure 14. PSGP Average Funding Awarded.....	28
Figure 15. FY23 Port Security Grants Awards	28
Figure 16. Attack Path Examples	38
Figure 17. Common Mitigations User Resistance & Costs	42
Figure 18. Password Policy Recommendations	43
Figure 19. Password Strength Perspectives	44
Figure 20. MFA Bypass Techniques Used by Threats	45
Figure 21. Privileged Account Management (PAM) Access Controls.....	46
Figure 22. User Training – Best Practices	48
Figure 23. Network Traffic Filtering.....	49
Figure 24. Network Traffic Filtering General Guidelines.....	50
Figure 25. User Account Management and General Guidelines.....	50
Figure 26. Detection/Logging Recommendations	52
Figure 27. Coast Guard CPT Incident Response Process.....	60

APPENDIX J

LIST OF TABLES

Table 1. Averages of Observed Passwords.....	19
Table 2. Password Cracking Observations	19
Table 3. 2023 Hunt and IR Mission Summary.....	23
Table 4. MITRE ATT&CK® Techniques Used by Year	39
Table 5. Mitigation Status – CY21, CY22, & CY23 Comparison	40
Table 6. Common Mitigation Recommendations.....	41

By embracing these insights and taking decisive action, we can navigate the future with confidence, support the flow of trade, and protect the MTS.



CYBER SUPPORT RESOURCES

Enabling Hardening and Assessing Risk Posture

Coast Guard CPT Assessments and Hunts

CGCYBER offers CPT assessments and Hunt missions to organizations within the ME. If an organization would like to request a CPT mission, they should reach out to the local Coast Guard Sector's MTSS-C. If unsure of how to contact the local MTSS-C, they should reach out to CGCYBER's MCRB (maritimecyber@uscg.mil), who can provide the proper contact information.

CISA's Cyber Hygiene Service

CISA offers vulnerability scanning services to help organizations reduce their exposure to cyber threats by taking a proactive approach to mitigating attack vectors. Additionally, CISA recommends organizations further protect themselves by identifying assets that are searchable via online tools and taking steps to reduce that exposure. For more information please visit <https://www.cisa.gov/cyber-hygiene-services>.

Coast Guard CPT Incident Response

The NRC or local Coast Guard Sectors can engage CGCYBER for additional support. Coast Guard CPTs maintain a team ready to deploy on short notice anywhere in the world provided the affected organization completes a legal agreement with CGCYBER. CPT Incident Response missions are generally focused on providing forensic analysis and advising organizations on containment, eradication, and recovery actions. *Figure 27: Coast Guard CPT Incident Response Process* depicts the sequence of events and reporting chain for reported cyber incidents involving MTS entities.

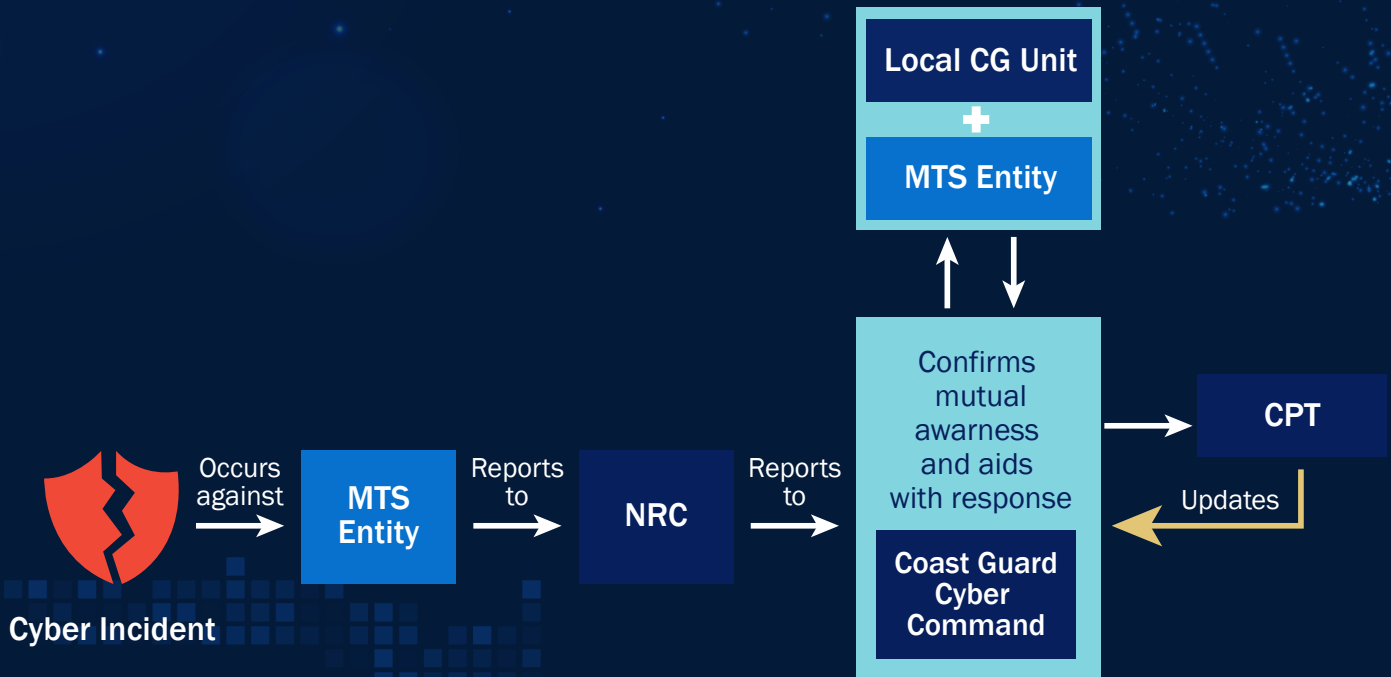


Figure 27. Coast Guard CPT Incident Response Process