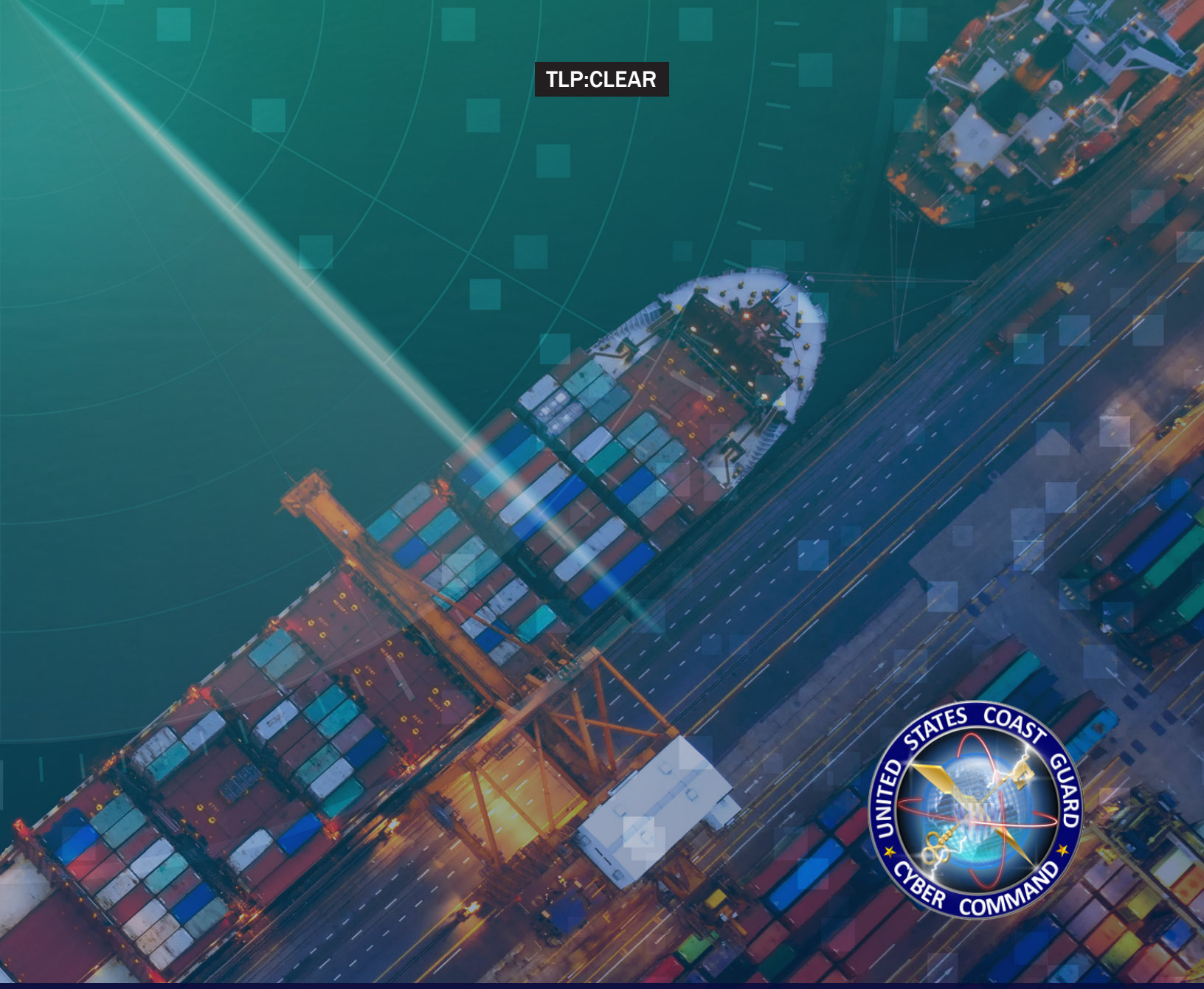
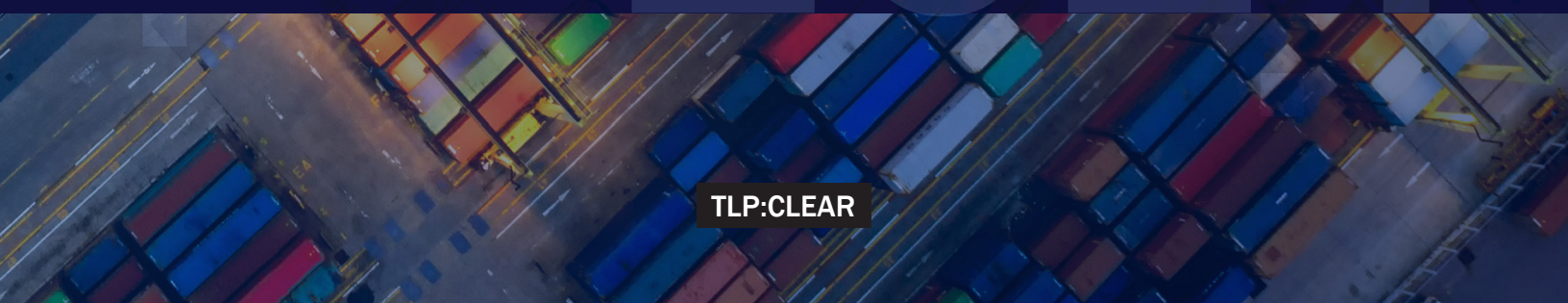
TLP:CLEAR



U.S. Coast Guard Cyber Command

Cyber Trends and Insights in the Marine Environment

2024



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.

FOREWORD

Welcome to the fourth edition of our Cyber Trends and Insights in the Marine Environment (CTIME) report. This year, we are excited to not only present our overall cyber findings from calendar year 2024, but also to include our first in-depth discussions on cloud technology and ship-to-shore (STS) cranes manufactured in China.

The Coast Guard is the leading government agency tasked with securing our nation's $5.4 trillion economic engine, the Marine Transportation System (MTS). STS cranes are essential to the movement of goods in and out of our ports. We are proud to provide the most comprehensive and publicly available technical findings on these cranes to raise awareness to the risks and provide crane operators with actionable hardening recommendations to improve their security.

In 2024, Coast Guard Cyber Command (CGCYBER) continued to adapt to the ever-changing operating environment of the MTS. We have generally observed an improving baseline cybersecurity posture across the MTS, with better password policies, growing adoption of multi-factor authentication, and better built-in tools to combat phishing. However, we have also observed adversaries adjust their tactics to find new initial attack vectors, such as focusing on stolen credentials and exploitable public-facing vulnerabilities. We have seen technological advancements in satellite networks enabling ships to always remain connected to their enterprise networks and improve their operational efficiency. Unfortunately, this constant connection has also enabled malware to rapidly spread from a company's corporate network to their ships while underway.

Over the past few years, many MTS organizations have undertaken substantial efforts to improve their cybersecurity. That said, the constantly changing cyber threat and vulnerability landscape continues to require a vigilant cyber posture. While CGCYBER is committed to leveraging the best of the Federal government's cyber capabilities to defend the MTS in this dynamic domain, it is our outstanding workforce and public and private sector partnerships that are the cornerstone of our shared effort to secure our ports and waterways against malicious cyber actors seeking to do us harm.

Semper Paratus,

Jason P. Tama
Rear Admiral, United States Coast Guard
Commander, Coast Guard Cyber Command

"The adoption of new technologies continues to drive operational efficiencies while also creating new vulnerabilities and attack vectors. CGCYBER is committed to partnering with industry to address this evolving threat landscape and protect the Marine Transportation System in cyberspace."

RDML Jason P. Tama

TABLE OF CONTENTS

TLP:CLEAR

2024 TRENDS & INSIGHTS

SCORECARD[1]

Average cost of all breaches:[2]

$4.88M

CY24 10%↑

70%

of breached organizations reported that the breach caused significant or very significant disruption

53%

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

71%

year-over-year increase in cyberattacks that used stolen or compromised credentials

73%

of partners used **Managed Security Service Providers** (MSSPs)

Default Credentials were in use at

71%

of organizations

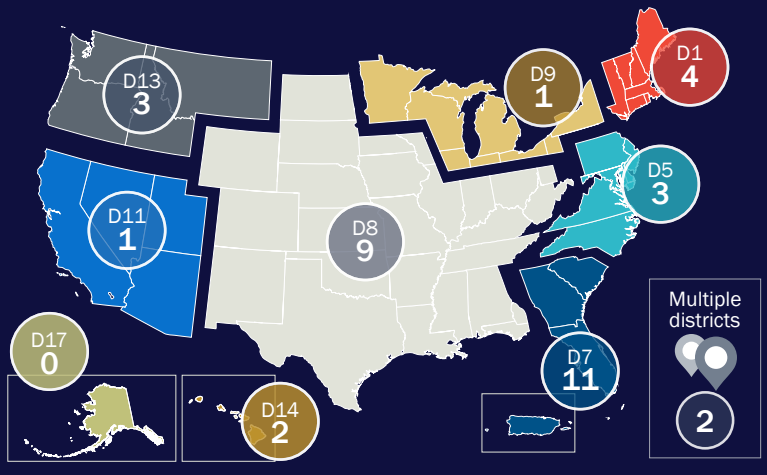
46.9%

success rate when **Brute Force Cracking Passwords** during 2024 CPT missions

190

Known Exploitable Vulnerabilities (KEVs) detected across assessments

Cyber Events Reported to Coast Guard by District



5 Most Commonly Detected KEVs:

- **CVE-2013-3900 (CVSS 7.6)**
  10 organizations
- **CVE-2023-44487 (CVSS 7.5)**
  8 organizations
- **CVE-2024-21338 (CVSS 7.8)**
  5 organizations
- **CVE-2024-21412 (CVSS 8.1)**
  5 organizations
- **CVE-2024-21351 (CVSS 7.6)**
  5 organizations

[1] Data derived from Coast Guard Cyber Protection Team Operations
[2] Source: Cost of a data breach 2024 | IBM (https://www.ibm.com/reports/data-breach)

TLP:CLEAR

EXECUTIVE SUMMARY

Coast Guard Cyber Command (CGCYBER) works with industry stakeholders across the marine environment to reduce cybersecurity risks to the Marine Transportation System (MTS). In pursuit of this goal, CGCYBER presents the fourth annual Cyber Trends and Insights in the Marine Environment (CTIME) report. This report catalogs the persistent cybersecurity risks faced by maritime owners and operators, as well as best practices to drive hardening actions and secure critical systems. The analysis and recommendations in this report are based on observations from operations, technical exchanges, and industry engagements conducted by Coast Guard Cyber Protection Teams (CPTs) and CGCYBER's Maritime Cyber Readiness Branch in 2024. We aim to provide Coast Guard units, our partners, and all stakeholders with key insights to identify and address current and emerging cyber threats.

Key Takeaways

- **Supply-chain risks and other observed vulnerabilities exist within ship-to-shore cranes manufactured in China.**
  While every crane configuration and employment method varies, through our assessments, the Coast Guard has identified several best practices that should be applied to mitigate some of the most common vulnerabilities.
- **Improved connectivity and the proliferation of networked technology create new cyber risks for vessels.**
  With improvements in satellite networks and more networked technology, vessels are more integrated with their company's enterprise networks than ever before. While there are significant operational benefits, this creates cybersecurity risks that did not exist before. Cyberattacks impacting a company's enterprise network are now far more likely to impact shipboard Information Technology (IT) systems and potentially impact vessel operations.
- **Uptick in cyber incidents and CPT missions involving cloud systems and services.**
  Cloud services are now utilized by a majority of organizations in the MTS; however, there continues to be a misunderstanding of security responsibilities. A misconception that the cloud service provider owns all the security responsibilities persists, but companies using cloud computing still retain (at least) partial responsibility for security of their systems and data.
- **The most common cybersecurity vulnerabilities observed in 2024 were similar to those highlighted in previous CTIME reports, however the baseline cybersecurity posture has improved across the MTS.**
  Widespread adoption of Multi-Factor Authentication and technical improvements against phishing have helped drive this change, but there is still much more work to do. Effective cybersecurity requires vigilance and continuous improvement.

INTRODUCTION

This report provides a high-level analysis of observed cybersecurity practices and adversary activities within the marine environment from January 1, 2024, through December 31, 2024. Across the calendar year, Coast Guard Cyber Command (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 and their staffs, as well as maritime facility leadership and management teams, including Facility Security Officers (FSOs), Information Technology (IT) Directors, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Cybersecurity Officers (CySOs) and other executives. 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 aims not only to present the data, but also to report the collaboration between the Coast Guard and maritime organizations in addressing cybersecurity risks. These partnerships have yielded numerous successes in incident responses, hunt missions, and assessments. For instance, the Coast Guard Cyber Protection Teams (CPTs) have aided maritime organizations in investigating and remediating large-scale ransomware attacks and identifying and mitigating ransomware hoax attacks. During hunt missions, CPTs have detected malicious activity and ongoing compromises, working alongside maritime industry partners to take appropriate action. Additionally, CPTs have assisted in identifying unexpected and unnecessary services connected to industry partners' operational technology environments, prompting immediate remediation. Throughout these successes, a common thread emerges: the partner organizations' commitment to enhancing their cybersecurity and their willingness to collaborate with others to achieve this goal.

What's New in 2024?

- CGCYBER's newest active-duty CPT reached Full Operational Capability and a reserve CPT was established as a new command. This brings CGCYBER to a total of three active-duty CPTs and one reserve CPT.
- Overall, there was a slight uptick in MTS partners requesting CPT support for cyber incidents. CGCYBER achieved a record high operational tempo in 2024, completing 42 total MTS missions.
- In 2023, CGCYBER expanded the scope of assessments and hunts to include Operational Technology (OT), and that trend continued in 2024. CGCYBER continues to professionalize and grow its OT capabilities, and the demand for those services has risen.
- Concerns regarding ship-to-shore (STS) cranes manufactured in China have existed for years, but 2024 saw the issue brought front and center. The Coast Guard released Maritime Security (MARSEC) directives 105-4 and 105-5, and the House Select Committee on the Chinese Communist Party released a report[3] assessing the supply chain risk posed by these cranes. CGCYBER CPTs have been assessing cranes as part of hunt and assessment

[3] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint Homeland-China Select Port Security Report-compressed.pdf

missions for several years, and this year's report contains a section dedicated to discussing our observations and recommended best practices.

- Like most industries, the maritime industry continues to adopt and expand the use of cloud technologies and services. While these offerings often include some built in cybersecurity protections, the consumers of these services still have security responsibilities. This year's report includes a section dedicated to our analysis and observations from missions involving cloud technology.
- For the first time in 2024, CGCYBER tracked which partners utilized Managed Security Service Providers (MSSP). An MSSP provides outsourced monitoring and management of security devices and systems.[4] Last year, 73% of CGCYBER CPT mission partners utilized MSSPs to manage their cybersecurity.
- Network segmentation is often one of the most important technical controls for mitigating impacts to large-scale cyber incidents. However, improper segmentation continues to be one of the most common vulnerabilities observed, particularly in OT environments.

Figure 1. *The Marine Environment Overview.*

[4] Source: Definition of Managed Security Service Provider (MSSP) - IT Glossary | Gartner (https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider)
[5] Source: Maritime Transportation System (MTS) | MARAD (dot.gov) (https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts#:~:text=America's%20Marine%20Transportation%20System%2C%20or,to%20and%20from%20the%20water.)
[6] Source: On National Maritime Day and Every Day, U.S. Economy Relies on Waterborne Shipping | Bureau of Transportation Statistics (bts.gov) (https://www.bts.gov/data-spotlight/national-maritime-day-and-every-day-us-economy-relies-waterborne-shipping)

MISSION OVERVIEW

Coast Guard Cyber Command (CGCYBER) Cyber Protection Teams (CPTs) deliver capabilities to prevent, detect, and respond to cyber threats impacting United States (U.S.) Critical Infrastructure in the Marine Transportation System (MTS). The teams deploy and operate upon request from partners in support of Coast Guard Operational Commanders and collaborate with public and private organizations globally.

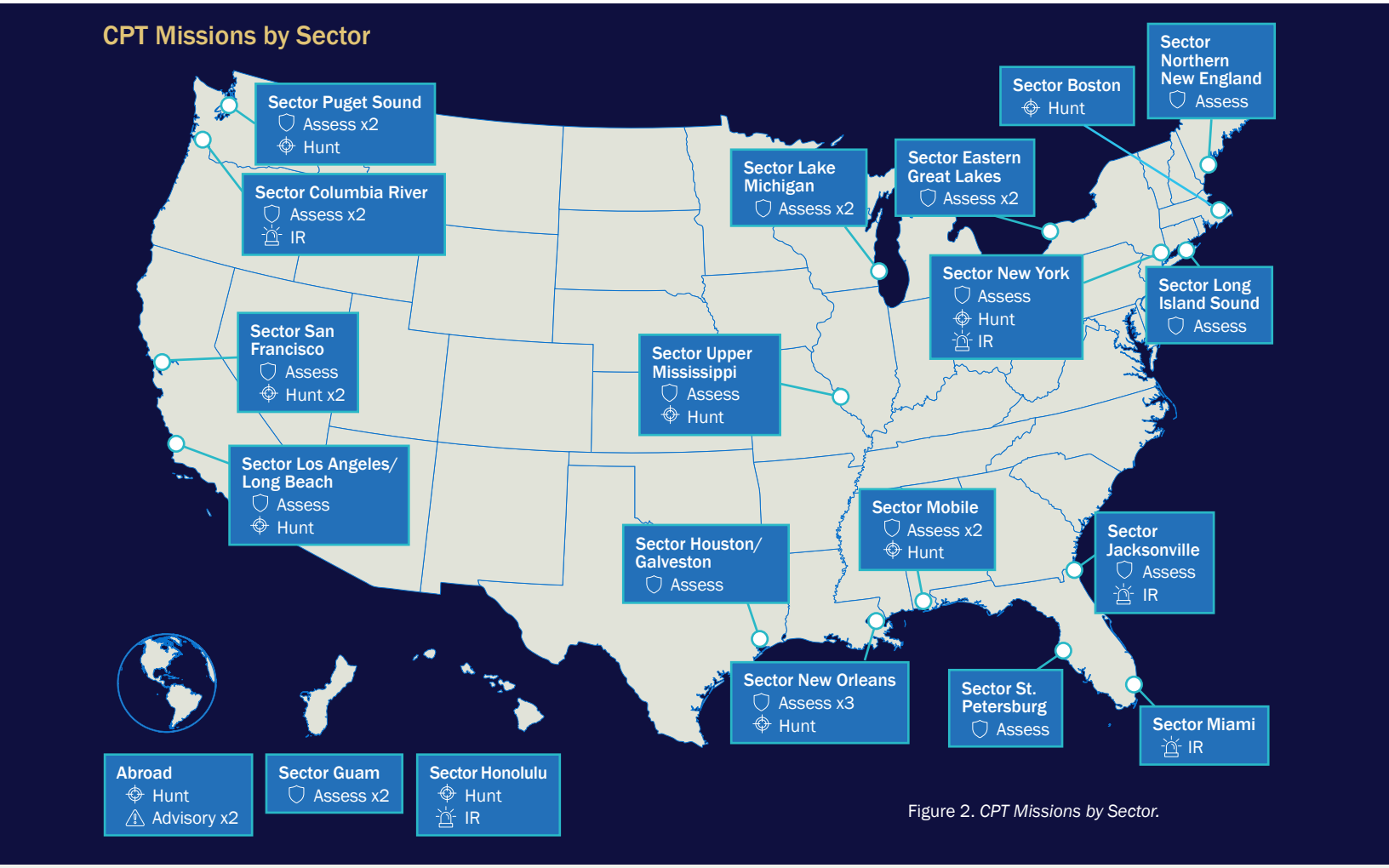


Figure 2. *CPT Missions by Sector.*

In 2024, CGCYBER completed 42 missions with industry partners. This report is based on the data and analysis collected during these missions, cross-referenced with incidents reported to the CGCYBER Maritime Cyber Readiness Branch, to provide a comprehensive understanding of current and emerging cyber threats. Figure 2 provides visual representations of CPT missions across geographic regions

MARITIME CYBER TRENDS

Coast Guard Cyber Command (CGCYBER) Maritime Cyber Readiness Branch (MCRB) offers expertise in marine safety and cybersecurity to convert details from cybersecurity incidents into quantifiable operational risks. MCRB risk analysis provides Coast Guard decision-makers critical information to accurately gauge risk and aid local units in responding to cybersecurity incidents. For each reported Marine Transportation System (MTS) cyber incident, MCRB attempts to identify the initial attack vector and then what, if anything, was done post-entry. It is important to note that the analysis MCRB conducts is contingent upon the information the impacted entity provides. With more self-reported information, we can provide members across the MTS better insights into cyber issues plaguing the industry.

In 2024, MCRB and local Coast Guard units responded to 36 reported cyber incidents. Additionally, Coast Guard Cyber Protection Teams' (CPTs) incident response services are being requested more than ever.

Cyber Incidents by District

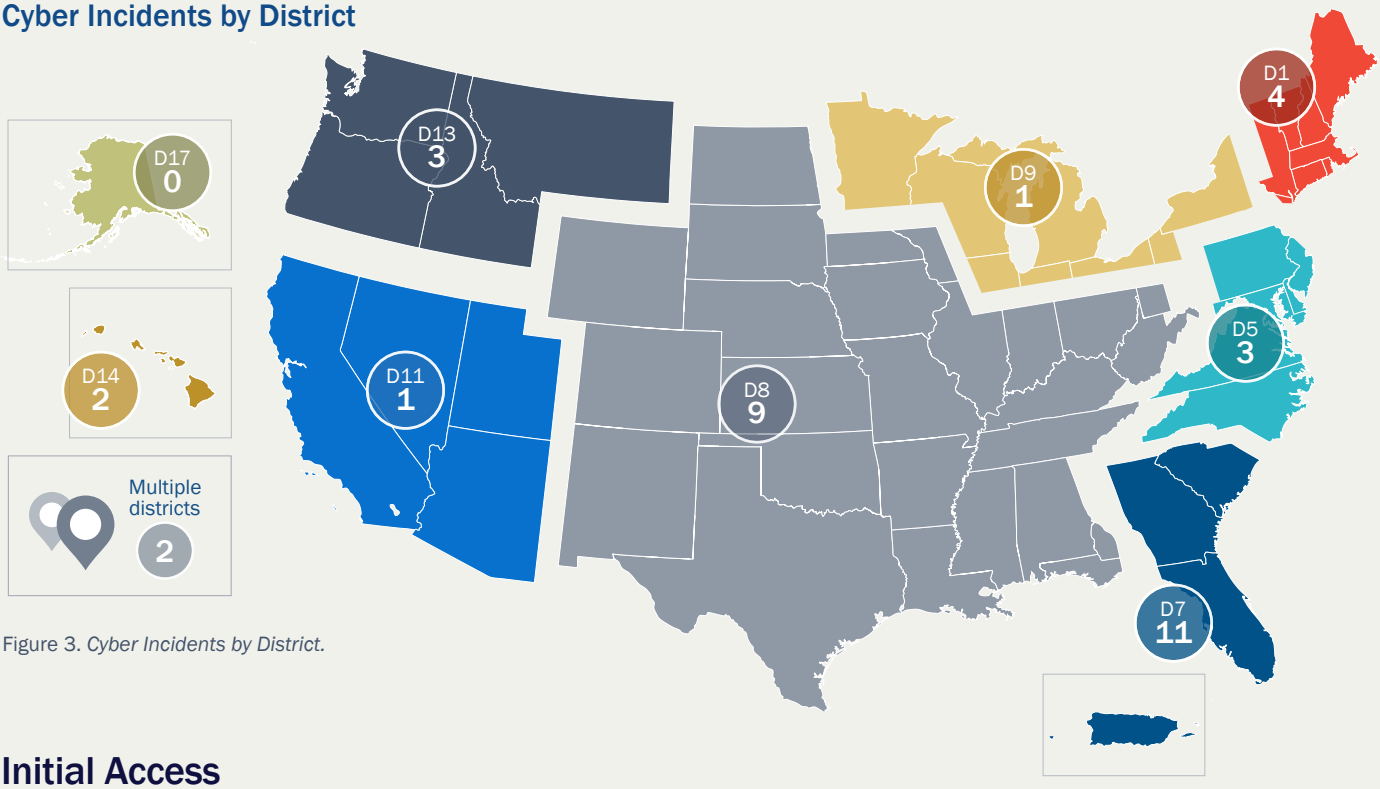


Figure 3. *Cyber Incidents by District.*

Initial Access

MTS cyber incidents involved the use of valid accounts in 42% of reported cases. Access to these accounts came from phishing, leaked credentials, and occasionally brute force cracking of weak passwords. Administrator accounts are the primary targets and their compromise often led to the most damaging cyber incidents. Phishing as an initial attack vector accounted for 25% of the reported MTS cyber incidents in 2024, highlighting the need for user awareness training for employees. Many of these cases involved business email compromises, or using

legitimate accounts to send phishing emails to internal and external contacts, making detection far more difficult and possibly expanding the impact on the MTS. Domain spoofing continues to be an issue for the MTS, where malicious cyber actors create fraudulent company websites with common functionality, such as submitting bookings and completing financial transactions with the intent to steal customer information or install malicious software on their systems.[7]

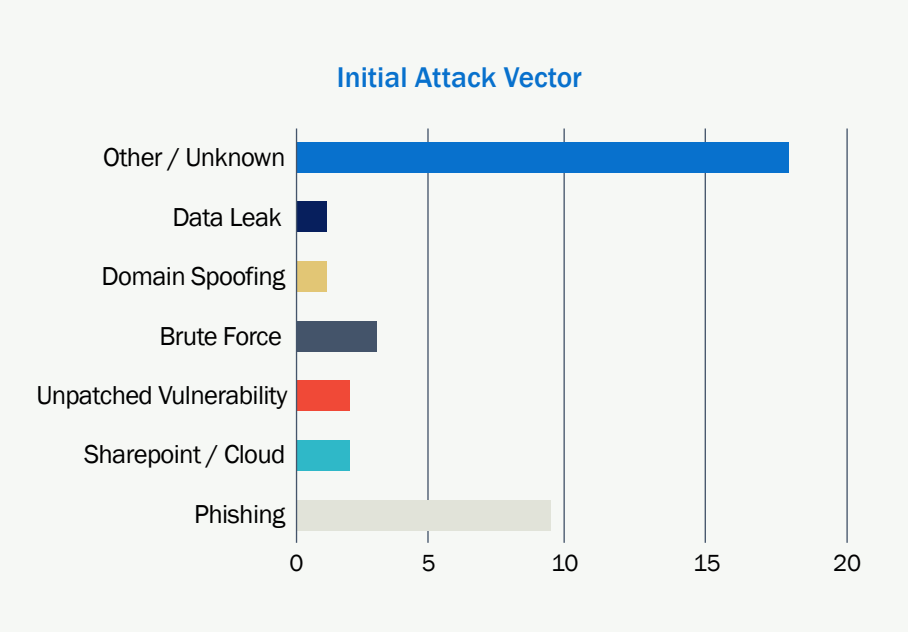


Figure 4. *Initial Attack Vector.*

Impacts

Historically, ships had minimal networked technology and limited connectivity while underway, making them logically air gapped from corporate enterprise networks. Improvements in satellite networks and modern technology aboard ships has created a situation where ships are always connected, essentially becoming another segment of the enterprise network. From a network configuration standpoint, and to an adversary enumerating the network, a ship appears the same as any other facility on the network. This integration helps drive operational efficiency but introduces new risks to vessel operations. Without the proper controls in place, a cyber incident impacting the enterprise network can also impact networked shipboard systems. This makes implementing the proper cybersecurity controls across an entire enterprise more important than ever.

In 2024, 25% of reported incidents were ransomware, a decrease compared to 42% in 2023. CGCYBER attributes some of this decrease to concerted efforts from the cybersecurity community to thwart ransomware gangs.[8] While there was an apparent drop in reported successful ransomware incidents within the MTS, the average cost of a data breach across all critical infrastructure sectors in 2024 was 10% higher than in 2023.[9] Ransomware continues to be profitable for threat actors and threatens impacted organizations with more devastating effects. For example, one of the most significant ransomware incidents that MCRB investigated was against a combined seaport and airport. This attack impacted services at the airport including baggage, check-in kiosks, and ticketing for approximately one week, with residual effects lasting months after the incident. The attack was associated with the cyber-criminal group Rhysida. Rhysida operates using Ransomware-as-a-Service (RaaS) by developing ransomware to lease out to malicious cyber actors, who then share profits with Rhysida. Successful ransomware

[7] Source: CGCYBER MaritimeCyberBulletin 03-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Bulletin 03-24_Spoofed_Business_Website.pdf)
[8] Source: FBI, global police partners take down LockBit, prolific ransomware gang (https://www.axios.com/2024/02/19/lockbit-ransomware-takedown-operation)
[9] Source: Cost of a data breach 2024 | IBM (https://www.ibm.com/reports/data-breach)

attacks can exfiltrate sensitive data, degrade company operations and reputation, and impact U.S. critical infrastructure. As demonstrated by a large percentage of observed incidents involving ransomware, an increased cost associated with ransomware incidents, and the observation of criminal organizations not seen in prior years, financial gain remains a primary motivator for malicious cyber actors.

Additionally in 2024, CGCYBER continued to observe a rise in reported attacks by nation state actors. A nation state actor is a well-resourced, highly capable threat actor backed by a government or state entity. They often have various political and economic motivations and conduct cyber espionage, data theft, and system disruption. For example, Russian military cyber actors were reportedly found responsible for targeting critical infrastructure across the globe to include government, finance, transportation systems, energy, and healthcare sectors. Their methods included scanning, data exfiltration, and website defacement against organizations providing aid to Ukraine.[10] Furthermore, cyber espionage attributed to the China-based threat group Mustang Panda utilized remote access trojans to target various cargo shipping companies in countries across the globe including those in Norway, Greece, and the Netherlands.[11] As referenced in last year's CTIME report, China-based threat actor Volt Typhoon remains relevant. Volt Typhoon uses "living off the land" techniques[12] in which they rely on existing tools and features in the target environment, such as valid user accounts, with the intent to remain undiscovered within networks for long periods of time and conduct extensive reconnaissance against targets. In 2024, the U.S. Government also uncovered a broad and significant cyber espionage campaign by the China group Salt Typhoon targeting major telecommunications companies.

To combat these malicious cyber actors, timely information sharing among CGCYBER, other government agencies, and maritime organizations continues to be critical for identifying and disrupting malicious cyber activity. CGCYBER distributes information sharing products found in Appendix A to provide awareness on cyber trends and threats along with recommendations and resources to assist the MTS in hardening its cybersecurity posture. CGCYBER relies on cyber incident reports to the National Response Center (NRC)[13] to activate response capabilities and increase awareness across the MTS. It is important for all organizations in the MTS to report cyber incidents to the NRC to better address these evolving cyber threats. The NRC can be contacted at 1-800-424-8802.

Information Sharing

In coordination with the FBI, CISA, and the MTS Information Sharing and Analysis Center (MTS-ISAC), CGCYBER notified an MTS partner of a possible attack on their network. As a result of this timely information sharing, the company was able to identify the intrusion and initiate incident response actions to minimize the impacts.

[10] Source: CGCYBER Maritime Cyber Bulletin 03-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Bulletin 04-24_Russian_Military_Cyber_Threat_Actors_Targeting_Critical_Infrastructure 24SEP2024.pdf)
[11] Source: China-linked group uses malware to try to spy on commercial shipping, new report says (nbcnews.com) (https://www.nbcnews.com/news/world/china-linked-group-malware-spy-commercial-shipping-cargo-report-eset-rcna152129)
[12] Source: Identifying and Mitigating Living Off the Land Techniques (https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf)
[13] Call 1-800-424-8802 to report incidents to the NRC.

ASSESSMENTS

Overview

Coast Guard Cyber Command (CGCYBER) conducted 24 assessment missions during calendar year 2024. While conducting assessments, Cyber Protection Teams (CPTs) emulate threats and employ known attack techniques to assess an organization's risk posture and highlight business impacts. These missions included 15 conventional assessments focused on only Information Technology (IT) and business systems, and 9 assessments where operational technology (OT) was in scope. This section discusses attack paths and findings from these assessments.

CPT Assessment Services

External Assessment. This service aims to determine what exploitable vulnerabilities exist within a company's external security boundary. The CPTs use various tools and techniques to scan for exploitable vulnerabilities, such as unpatched software, misconfigured systems, and weak passwords.

Phishing Assessment. The CPTs use phishing campaigns to determine the susceptibility of staff and infrastructure to phishing attacks and assess the impact of a phished user workstation on the internal network.

Internal Assessment. This stage aims to determine what impact an attacker could have after gaining an initial foothold in a network (unprivileged user-level access). CPTs focus on pivoting within the network, escalating privileges, and establishing persistence to assess the company's security posture and demonstrate what impacts an unprivileged user could have.

Operational Technology Assessment. CPTs conduct passive OT assessments to determine what vulnerabilities or misconfigurations an attacker could utilize to impact the systems controlling industrial processes. Additionally, as part of this service CPTs attempt to map the overall flow of OT data, validate OT network protections, and identify network traffic anomalies within the OT networks.

[14] https://attack.mitre.org/techniques/T1589/001/
[15] https://attack.mitre.org/techniques/T1190/

Key Findings

External Assessments

During the external assessment, the most common MITRE ATT&CK® technique found is Gather Victim Identify Information: Credentials (T1589.001[14]). During mission preparation activities, CPTs search through commercial threat intelligence sources as well as information for sale on the dark web to identify potential information to be used on the assessment. In many cases there are credentials for sale that can be used to access a partner's resources and gain initial access to a partner's network. CPTs are also able to Exploit Public Facing Application (T1190[15]) and gain initial access through the exploitation of public-facing unpatched or legacy services. These are often the most critical findings of a CPT report, as these vulnerabilities offer attackers initial access to the partner's network.

Phishing Campaigns

Phishing for Information (T1598[16]) remains an effective initial access vector, allowing analysts to capture credentials and use Valid Accounts (T1078[17]) to operate without detection; however, CPTs have observed a noted increase in phishing defenses across all partners. In 45% of assessments, CPTs gained initial access through phishing for credentials and exploiting valid accounts, which is a decrease from the 66% in 2023. CPTs found that approximately 37% of mission partners had Multi-Factor Authentication (MFA) enabled; however, in roughly half of these cases, CPTs were able to bypass MFA through the phishing campaign Push Bombing/Multi-Factor Authentication Request Generation (T1621[18]) or Steal Web Session Cookie (T1539[19]). This highlights the need for Phishing Resistant MFA implementation.[20]

Internal Assessments

After gaining access to a mission partner's network, CPTs were able to establish persistence, pivot throughout the network, and escalate privileges through various methods. During this year's assessments, CPTs captured 17,000 password hashes and cracked 46% of the hashes within 96 hours, Brute Force: Password Cracking (T1110.002[21]), a decrease from 60% in 2023. This Password Cracking was completed using consumer grade hardware and opensource software that any adversary could utilize. This highlights the need for strong and complex passwords. Another method used was Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001[22]). CPTs were successful in using this method in 33% of the missions. Default Credentials (T1078.001[23]) was also found to be a common vulnerability with CPTs detecting and leveraging them in 71% of missions. This was again a decrease from 2023, where CPTs observed default accounts in 94% of partner networks; however, this remains alarming as it continues to offer adversaries attack vectors either for initial access or movement throughout the network.

Operational Technology Assessments

Throughout OT assessments, CPTs identified many of the same vulnerabilities identified in IT assessments. The most common finding on OT networks was Default Credentials (T0812[24]), emphasizing the need for cyber hygiene on OT networks. Additionally, most OT networks were found to be running Unsupported Software and Legacy Hardware. This aged hardware and software often included Known Exploited Vulnerabilities (KEVs), significantly increasing the risk of these OT network segments. Furthermore, more than half of the partners with OT network segments had an incorrect understanding of their OT network segmentation. These partners believed either that their OT networks were unable to access the internet, or that their OT network segment could not be reached from the IT network; however, in most cases the assessments proved that these assumptions were incorrect. These misconceptions further stress the need for cyber security practices on these networks; they are typically not monitored like IT systems are and and not isolated in the way system owners expect.

[16] https://attack.mitre.org/techniques/T1598/
[17] https://attack.mitre.org/techniques/T1078/
[18] https://attack.mitre.org/techniques/T1621/
[19] https://attack.mitre.org/techniques/T1539/
[20] Source: Stopping the Attack Cycle at Phase One (https://www.cisa.gov/sites/default/files/2023-10/Phishing Guidance - Stopping the Attack Cycle at Phase One_508c.pdf)
[21] https://attack.mitre.org/techniques/T1110/002/
[22] https://attack.mitre.org/techniques/T1557/001/
[23] https://attack.mitre.org/techniques/T1078/001/
[24] https://attack.mitre.org/techniques/T0812/

Major Changes to Password Standard

Password Management: NIST SP 800-63 Revision 4
NIST SP 800-63-4 Second Public Draft | CSRC[25]

NIST has released a draft update to the SP 800-63 Digital Identify Guidelines, highlighting the importance of password management. Here are some recommendations from the publication:

Complexity Reduction: Avoid using complex password requirements. Instead, focus on using long, easy-to-remember passwords that are difficult for attackers to guess.

Avoiding Periodic Resets: Avoid requiring users to change their passwords periodically. Instead, encourage users to create strong, unique passwords that they can remember and use for an extended period of time.

Screening Passwords Against Compromised Lists: Screen passwords against lists of known compromised passwords.

Encourage Long Passwords: Encourage users to create long passwords that are at least 12 characters in length. Longer passwords are more difficult for attackers to guess and are less likely to be compromised.

Red Sky in the Morning
(Sailors take warning)

In 2023, a USCG CPT performed a proactive assessment mission with a partner that operates multiple Coast Guard-regulated facilities. The team highlighted numerous critical and high-severity findings, including overprivileged accounts, patch management issues, weak password policies, administrator password reuse, and weak network segmentation; however, the organization did not fully address these findings, and in 2024, they suffered a ransomware attack. The attackers exploited public-facing systems and some of the same vulnerabilities highlighted in the assessment to deploy malware throughout the organization's environment.

[25] https://csrc.nist.gov/news/2024/nist-sp-800-63-4-2pd-digital-identity-guidelines#:~:text=Revision%204%20of%20NIST's%20Special,world%20implications%20of%20online%20risks.

Conclusion

Key findings were similar to previous years, but baseline cybersecurity defenses have improved. This year, CGCYBER CPTs reported fewer cracked passwords, fewer clicks and collected credentials on phishing campaigns, and less detection of default credentials. This may indicate companies are becoming more resilient to phishing and other common cyber exploits. However, businesses should continue to strengthen cybersecurity measures and regularly assess and update them to stay ahead of emerging threats. Figure 5 lists the Top 12 Mitigations and CGCYBER's rough approximation of implementation difficulty. Appendix F contains more details for the recommended mitigations.

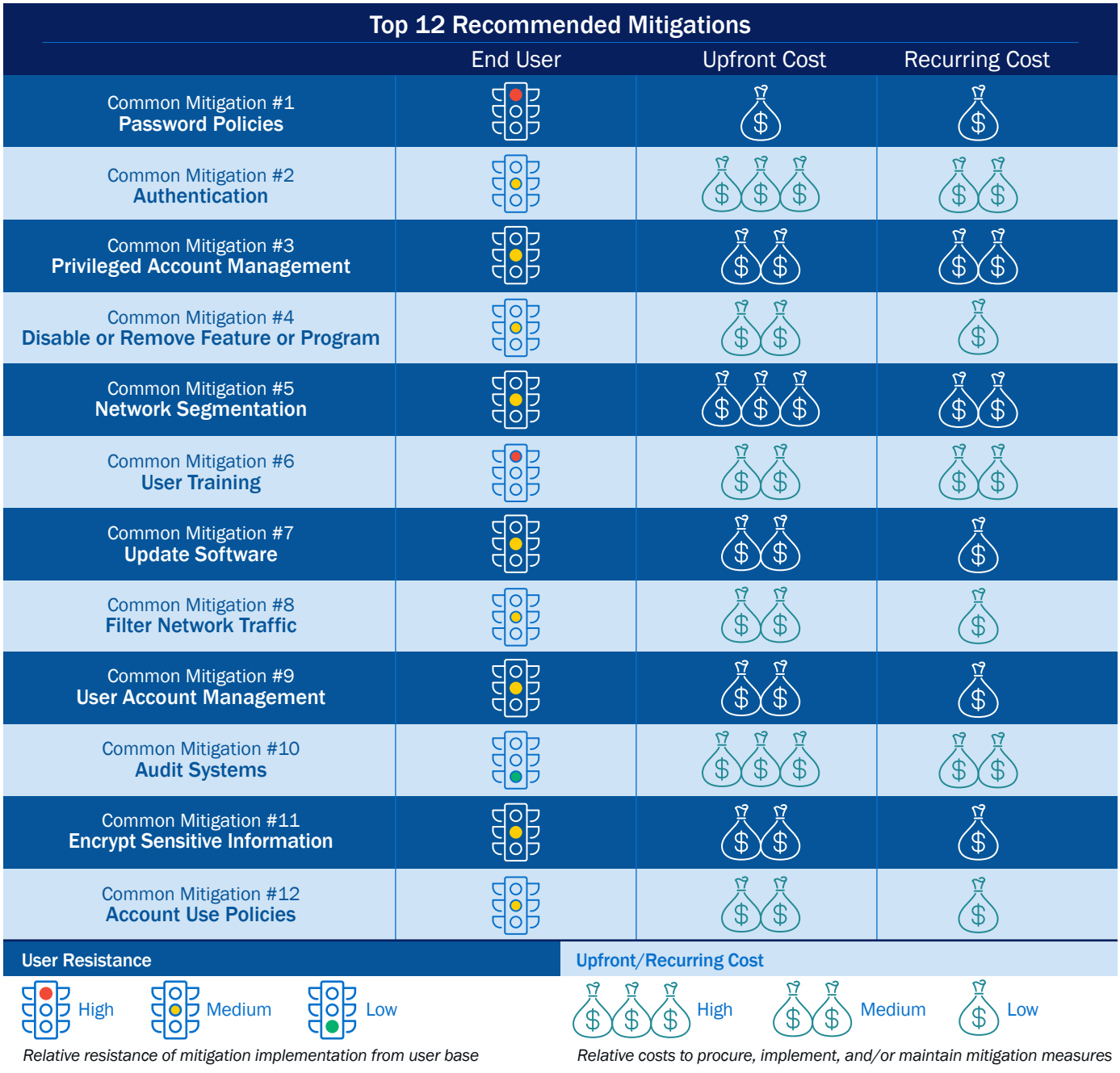


Figure 5. *Top 12 Mitigations.*

HUNT AND INCIDENT RESPONSE

Overview

In 2024, Coast Guard Cyber Command (CGCYBER) successfully completed 15 domestic hunt and incident response missions. Based on these missions, several trends and insights emerged:

- CGCYBER saw an increase in the number of incident response missions, indicating higher demand for Cyber Protection Team (CPT) support during incidents.
- For incident response missions, less than half of mission partners had Endpoint Detection and Response (EDR) capabilities.
- For incident response missions, CPTs observed that attackers typically exploited public-facing systems through unpatched Known Exploitable Vulnerabilities (KEVs), utilized valid accounts (due to weak password policies or poor privileged account management), or leveraged weaknesses/vulnerabilities in cloud infrastructure.
- Recurring trends across these missions include the presence of end-of-life systems, shared passwords, default credentials, cleartext credentials, unmanaged mobile devices, insecure protocols, weak logging, and weak password policies.
- CPTs discovered malicious cyber activity on mission partner networks during 3 of the 10 domestic hunt missions in 2024.

Underway Making Way

In 2024, we were engaged in our first ransomware incident in which shipboard networks were included in the ransom encryption phase. Malicious actors gained initial access to the partner's corporate network through a password guessing attack targeting a VPN account with a common name and a weak password. The attackers then moved laterally, exploiting unpatched backup servers with Remote Code Execution (RCE) vulnerabilities. They proceeded to fortify access, exfiltrate data, and deploy encryption software across the network.

The mission partner's vessels were logically connected to the corporate network, and vessel servers were included in the encryption phase. A CPT was deployed at the request of the mission partner. The CPT identified the attack path, provided hardening recommendations, and went onboard one of the partner's vessels to validate proper IT/OT segmentation. We are pleased to report that the partner had excellent IT/OT segmentation on their vessels, which prevented the operational capabilities of the vessels from being impacted. This incident highlights the importance of proper IT/OT segmentation and the need for organizations to take a holistic approach to cybersecurity, ensuring that all components of their network are secure.

Conclusion

The following chart summarizes all Hunt and Incident Response missions conducted this year.

Mission Type	Sector	Compromise Detected	Operational Technology	Time to Detect	Cloud Services
Hunt	Energy	No	Yes	N/A	Yes
Hunt	Chemical	Yes	No	> 90 days	Yes
Hunt	Transportation (maritime port)	No	Yes	N/A	No
Hunt	Transportation (maritime)	No	No	N/A	Yes
Hunt	Transportation (maritime)	No	No	N/A	Yes
Hunt	Transportation (maritime)	Yes	No	> 90 days	No
Hunt	Energy	Yes (Command and Control)	Yes	> 90 days	Yes
Hunt	Energy	No	Yes	N/A	Yes
Hunt	Transportation (maritime)	No	No	N/A	No
Hunt	Transportation (maritime)	No	Yes	N/A	No
Incident Response	Transportation (maritime)	No	Yes	N/A	Yes
Incident Reponse	Chemical	Yes (Ransomware)	Yes	< 30 days	Yes
Incident Reponse	Transportation (maritime)	Yes (Ransomware)	Yes	< 7 days	No
Incident Reponse	Transportation (maritime)	No	Yes	N/A	No
Incident Reponse	Emergency Response (maritime)	Yes (Ransomware)	No	48 hours	Yes

Table 1. *Hunt and Incident Response Missions.*

CLOUD COMPUTING

Background

Cloud computing services are categorized into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Understanding their differences is essential for determining responsibilities in security, management, and usage. IaaS provides infrastructure like servers, storage, and networking; users manage their applications and data but are responsible for securing them.[26] PaaS offers a platform for application development, with the provider managing infrastructure and maintenance, while users focus on coding and securing their applications.[27] SaaS is a fully managed solution where the provider handles everything, and users primarily access and use the software securely, though they must still ensure secure user management, data protection, and access controls.[28]

Key Takeaways

Maritime organizations are increasingly dependent on cloud computing services, but a misconception persists that the cloud service provider owns all the security responsibilities.
It is crucial companies using cloud computing understand their security responsibilities and how to avoid the common pitfalls.

While these are common models across most providers, each service provider implements them slightly differently. For example, the Azure Division of Responsibility[29] is shown to the right in Figure 6, as it is the most relevant to the Marine Transportation System (MTS) as described in the next section.

Even at the SaaS level, the customer is still responsible for some management activities, meaning if an organization does not fully grasp its responsibilities in cloud environments, it cannot accurately understand its cyberattack surface. Failing to understand these distinctions can lead to serious consequences, such as data breaches, regulatory non-compliance, or misuse of cloud resources.

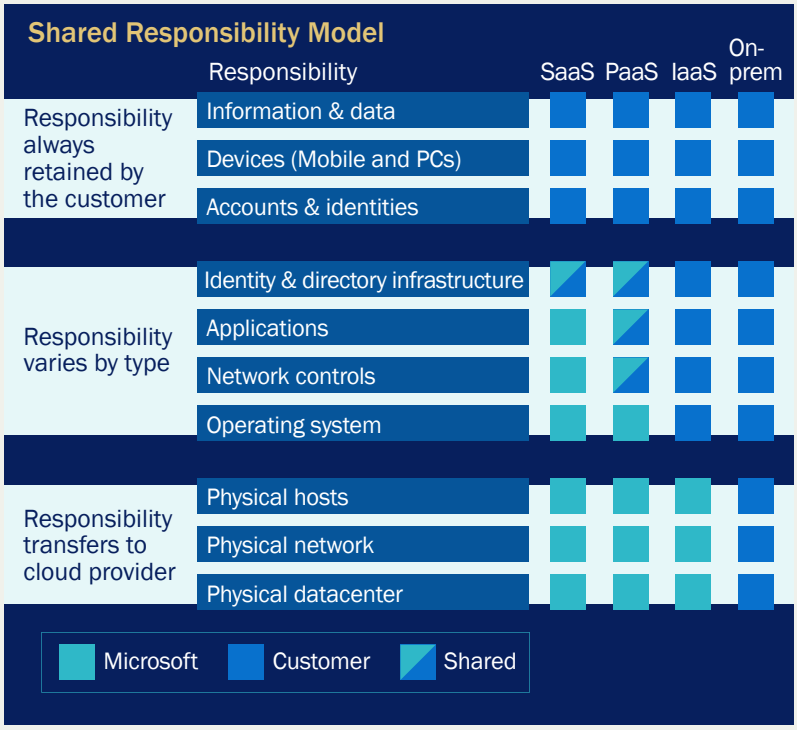


Figure 6. *Shared Responsibility in the Cloud – Microsoft Azure | Microsoft Learn.*

[26] Source: https://csrc.nist.gov/glossary/term/infrastructure_as_a_service
[27] Source: https://csrc.nist.gov/glossary/term/platform_as_a_service
[28] Source: https://csrc.nist.gov/glossary/term/software_as_a_service
[29] Source: Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn (https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility)

Overview

Over the last calendar year, 53% of Coast Guard Cyber Command (CGCYBER) partners used cloud-based infrastructure to meet business or operational requirements. Overall, the two most observed cloud service providers were Microsoft Azure and Amazon Web Services (AWS). A significant majority (80%) of partners relied upon the Microsoft 365 application suite for business operations. Additionally, Microsoft Entra (a.k.a. Azure Active Directory) was very common, and is used for Authentication and Authorization for access to cloud infrastructure. MTS partners primarily use AWS for data storage, back-ups, and hosting custom applications. Figure 7 shows a breakdown of the observed uses of cloud providers across the MTS and relative popularity. Furthermore, CGCYBER observed Malicious Cyber Actors (MCA) attempting to gain access to cloud infrastructure on 40% of incident response missions. Only through good network segmentation and proper identity access management can organizations defend their cloud resources.

As a general finding, CPTs observed a lack of understanding of standard cloud service offerings and the associated responsibilities for an organization. Partners were often unsure of what their vendor provided versus what they were responsible for managing. To best understand cloud risk, CPTs recommend reviewing contracts and subscription agreements with cloud service providers, as well as running regular configuration scans. CPTs utilize open-source cloud scanning tools such as Prowler (Prowler | GitHub[30]) and tools from the Cybersecurity and Infrastructure Security Agency's (CISA) Secure Cloud Business Applications (SCuBA) Project (SCuBA Project | CISA[31]). By having a clear understanding of the responsibilities tied to each cloud service model, organizations can manage risks more effectively and apply appropriate controls to protect their data and applications.

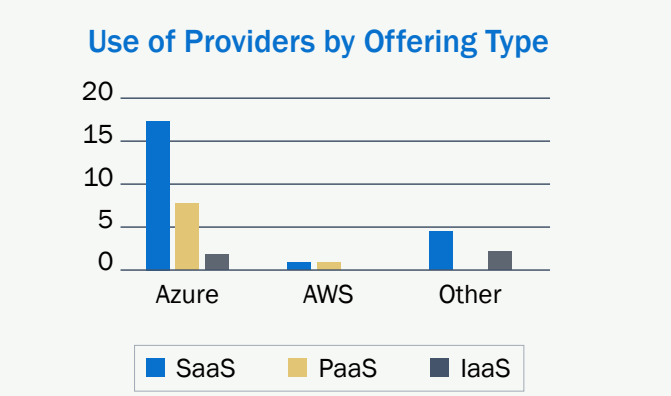


Figure 7. *Use of Providers by Offering Type.*

Consolidated Findings

Over the past year, Coast Guard CPTs have frequently identified vulnerabilities in Identity and Access Management (IAM), the framework for managing user access to cloud resources. IAM ensures only authorized users can access specific assets; however, effective implementation requires strong policies and controls. This includes using Multi-Factor Authentication (MFA), applying least privilege principles, and regularly auditing access logs to detect threats. These practices help safeguard sensitive data, reduce unauthorized access risks, and ensure compliance while maintaining cloud operations efficiently. Figure 8 shows the most common IAM vulnerabilities noted by CPTs in cloud infrastructure.

CPTs have also observed a variety of other cloud security misconfigurations across the MTS. Misconfigured cloud settings can lead to severe issues, including compromised data security and operational inefficiencies. When cloud resources are not correctly configured, vulnerabilities such as unrestricted access permissions, inadequate encryption, or improper network segmentation may be exposed. These missteps can result in

[30] https://github.com/prowler-cloud/prowler
[31] https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

unauthorized access, data breaches, and significant financial losses. Poorly configured cloud environments may also cause performance problems or unanticipated downtime, disrupting critical services and impacting business continuity. Ensuring that cloud settings are correctly managed and regularly reviewed is essential for maintaining secure and reliable infrastructure. Figure 9 shows the security misconfigurations observed by CGCYBER over the past year.

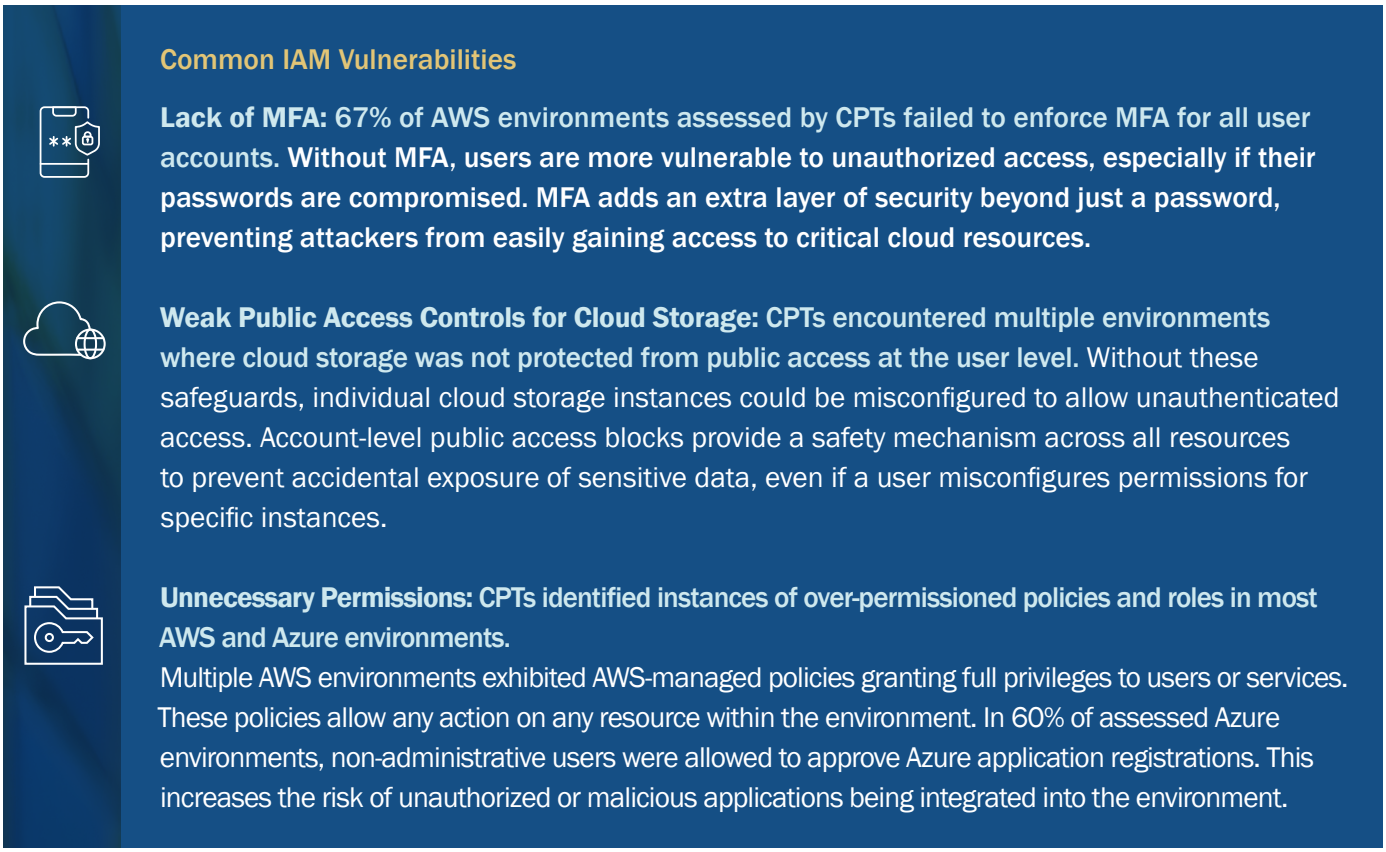


Figure 8. *Most Common IAM Vulnerabilities Noted by CPTs in Cloud Infrastructure.*

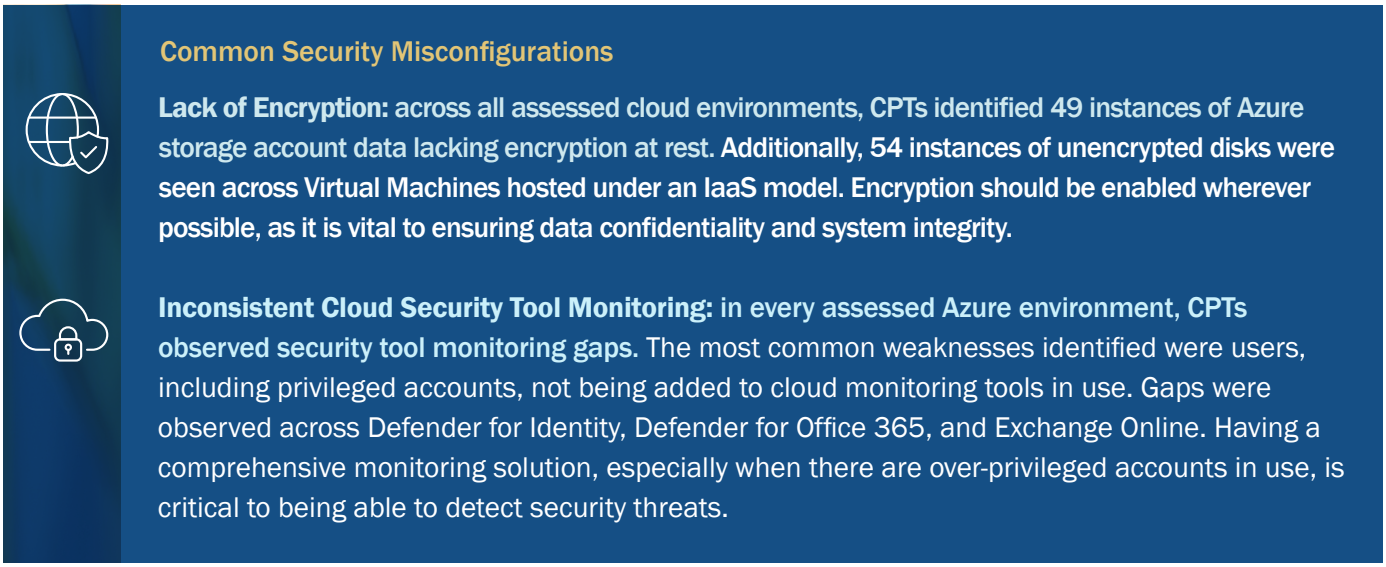


Figure 9. *Security Misconfigurations Observed by CGCYBER in the Past Year.*

Recommended Best Practices

Overall, the CPT findings mirror issues that impact cloud users generally. In March 2024, CISA and the National Security Agency (NSA) released five joint Cybersecurity Information Sheets to address similar issues and provide organizations with recommended best practices and mitigations to improve the security of their cloud environments (Cloud Security Best Practices | CISA[32]). CPTs recommend that all organizations that rely on cloud services review these for best practices. To address these findings, organizations should prioritize hardening in these three areas, which align with those best practices:

Implement Secure Cloud Identity and Access Management

- Use Phishing-Resistant MFA
  - Avoid exploitable MFA, such as simple push notifications vs number matching
  - Avoid MFA solutions allowing for key exportation
- Enforce Least Privilege and Just-in-Time Access Control
  - Grant users and apply only the permissions they need and when they need it
  - Regularly audit permissions to prevent privilege creep
- Use Conditional Access Policies
  - Employ context-based access control (ex. georestrictions)
  - Ensure policies are regularly reviewed, updated, and tested
- Secure and Monitor Identity Federation Servers
  - Use Hardware Security Modules to secure keys and certificates
  - Deploy EDR solutions and perform regular auditing

Implement Cloud Network Segmentation and Encryption

- Encrypt Data in Transit
  - Use TLS 1.2 or later for connections between cloud resources and clients
  - Prefer IPSec over TLS-based VPNs for secure tunneling
- Implement Micro-Segmentation
- Use Private Connectivity Options
  - Use direct network connections offered by cloud providers
  - Use private API endpoints unexposed to the Internet
- Enforce Virtual Networking and Access Controls
  - Use Virtual Private Clouds (VPCs) to logically isolate cloud resources
  - Assign granular firewall rules to different instances
  - Apply least privilege for control access to networking resources

Secure Data in the Cloud

- Encrypt Data at Rest
  - Manage encryption keys using a Key Management System or Hardware Security Module
- Use Role-Based and Attribute-Based Access Control
  - Limit wildcard permissions and consider using data tagging
  - Continuously audit access policies
- Limit Attack Surface
  - Configure object storage with restrictive policies by default
  - Allow public access only by exception
- Implement Backup and Recovery Solutions
  - Use immutable backups
  - Regularly test backup restoration
- Understand Cloud Service Provider Data Retention Policies
  - Review service agreements

[32] https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices

SHIP-TO-SHORE CRANES MANUFACTURED IN CHINA

Background

What are Ship-to-Shore cranes?

Ship-to-Shore (STS) cranes are colossal steel structures weighing nearly 2000 tons. They are self-propelled through powerful electric motors, and are built to hoist containers weighing up to 100 tons from cargo ships as high as 200 feet in the air. These machines are essential to load and unload container ships in all major ports across the world. According to UN Trade and Development (UNCTAD)[33] 70% of non-bulk cargo worldwide is transported on container ships.

Key Takeaways

Ship-to-shore (STS) cranes manufactured in China present a risk to the Marine Transportation System (MTS).

The U.S. is dependent on cranes manufactured by a Chinese state-owned enterprise which presents a significant supply chain risk. Further, extensive analysis conducted by Coast Guard Cyber Protection Teams (CPTs) has revealed vulnerabilities that could enable a malicious cyber actor the ability to disrupt port operations. All crane operators should take steps to mitigate this risk.

US Reliance on Cranes Manufactured in China

The United States has been increasingly reliant on cranes manufactured in China. According to the September 12, 2024 Investigation by the House Select Committee on the Communist Chinese Party[34], approximately 80% of STS cranes used in the United States are manufactured by Shanghai Zhenhua Heavy Industries Co., Ltd., (ZPMC), a Chinese state-owned enterprise (SOE). SOEs are controlled by the government of China and have access to reduced-cost labor and subsidized pricing for materials such as steel, allowing them to manufacture and sell cranes at non-competitive prices to capture an overwhelming global market share. Further, under China's Cybersecurity Law Article 5, critical infrastructure operators such as ZPMC must allow Chinese authorities to review source code, store their data within China, and permit comprehensive inspections by Chinese authorities. There are other China-based companies that manufacture cranes; however, ZPMC constitutes the majority of such cranes in the United States and across the globe.

[33] https://unctad.org/system/files/official-document/rmt2023ch1_en.pdf
[34] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint Homeland-China Select Port Security Report-compressed.pdf

ZPMC cranes contain a variety of components sourced from different countries. Frequently, these subcomponents are integrated within China during the assembly process before being shipped to their final destination. This integration within China, combined with the requirements placed on SOEs to cooperate with the Chinese government, creates the potential for a supply chain compromise. Such a compromise could grant China remote access to conduct espionage or manipulate U.S.-based cranes and enable them to disrupt port operations and cause physical damage/harm.

The following graphic shows an approximate distribution of STS cranes manufactured in China across the United States.

Supply Chain Attacks

Supply chain attacks have proven to be highly effective in recent history, affecting both hardware and software supply chains. For example, in 2020, the Russian Foreign Intelligence Service compromised the code base of the SolarWinds cybersecurity product and distributed the compromised software to nearly 18,000 customers. Using this access, they targeted a small subset of high-value customers for espionage purposes.[35]

Another example included a several years-long scheme where hundreds of millions of dollars' worth of counterfeit Cisco network switches were procured by civilian and government entities, including for use in military aircraft. These devices were not manufactured by Cisco, but rather low-quality switches built in China and Hong Kong. In June 2023, the Justice Department obtained a guilty plea, six years and six months in prison, and $100 million dollars in restitution for this case.[36]

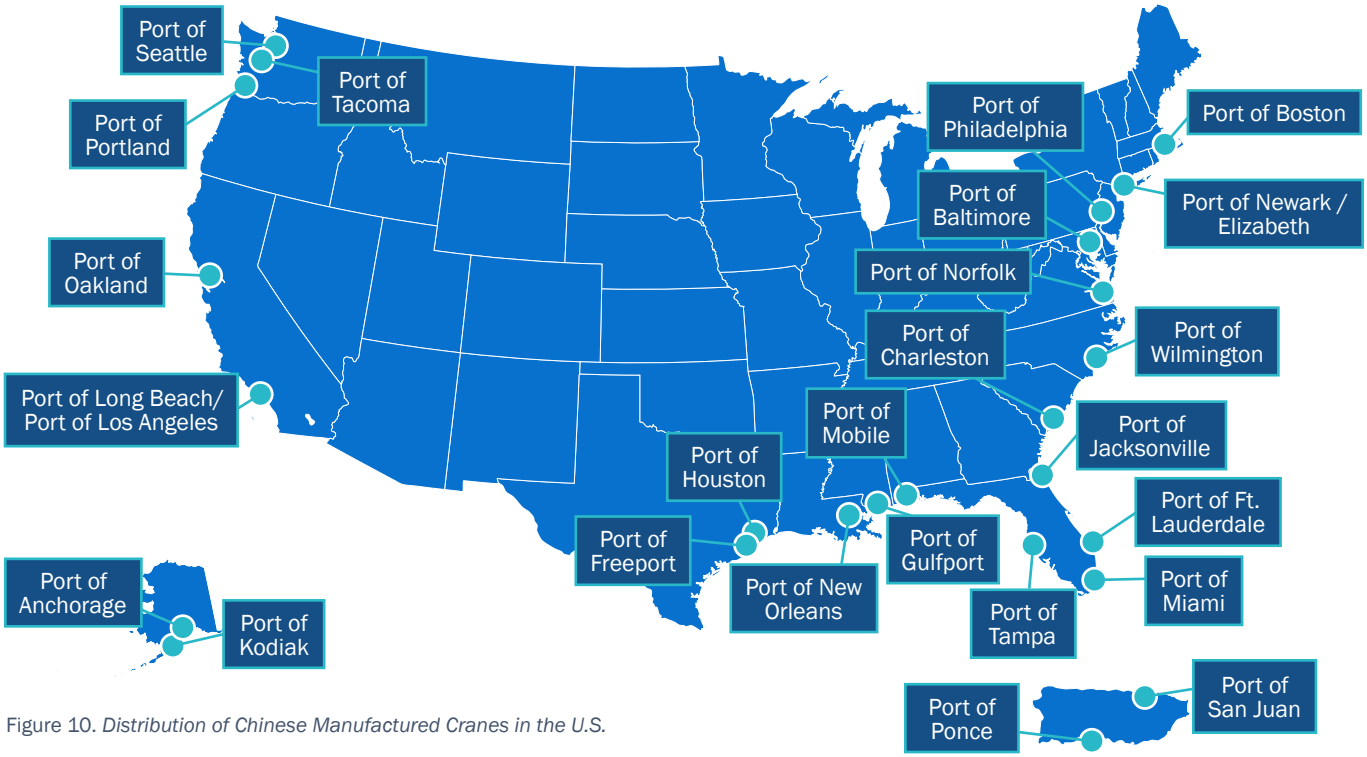


Figure 10. *Distribution of Chinese Manufactured Cranes in the U.S.*

[35] Source: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
[36] Source: https://www.justice.gov/archives/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment

Overview

A modern STS crane is a complicated system of systems. Below is a review of the essential components necessary for understanding CPT cybersecurity findings and their impacts.

- **Spreader** – The device at the end of a crane's cabling that attaches to containers. These devices are named "spreaders" because they can adjust their length to match containers of different lengths.
- **Elevator** – Cranes have small elevators, similar in size to elevators at building construction sites, which allow operators to ascend/descend from the cabin without climbing the stairs.
- **Boom** – The arm that extends out from the crane over a ship. The boom is raised when a crane is not in operation and prior to a container ship's arrival to ensure collisions do not occur. The cabin travels along the boom.
- **Gantry** – The beam structure that supports the crane's trolley and hoist. The gantry provides a stable platform for the crane's lifting equipment and helps to ensure that the crane can safely and accurately lift and move heavy loads.
- **Trolley** – A mobile platform that moves along the crane's gantry, allowing the crane to position its hoist and lifting equipment over the desired location. The trolley typically carries the hoist, spreader, and other lifting equipment, and is designed to move smoothly and precisely along the gantry.
- **Cabin** – This is where the crane's human machine interfaces (HMIs) are housed. The crane operator sits inside of the cabin which trollies along the boom, over a ship, with the spreader hanging directly below the cabin. This allows the crane operator to observe the spreader as it is lowered or raised to transport a container.

Modern STS Crane Features

- **Anti-sway** - automatically controls the movement of the cabin to precisely counteract the sway. This allows even novice crane operators to match the transfer of containers per hour rate of their vastly more experienced counterparts.
- **Optical Character Recognition (OCR)** - uses Internet Protocol (IP)-based cameras on a crane to read information printed on the exterior of containers. This information can be fed into a Terminal Operating System (TOS) to increase port automation and improve inventory accuracy.
- **Wireless remote control** - enables crane technicians to take full control of all crane functions, superseding all other control, including from an operator in the cabin.
- **Fully autonomous STS cranes** - claim to be capable of performing nearly autonomous full cargo transfers of container ships. CGCYBER is unaware of any US ports currently utilizing this feature.

Figure 11. *Crane Wireless Remote Control.*

- **Electric Motors** – Most cranes have four to six medium voltage industrial electric motors in the equipment room that power crane operations, with an additional large motor at separate locations to power gantry movement.
- **Equipment Room** – This is a prominent structure situated at the apex of the crane, located on the shoreside of the stationary section of the boom. It houses large reels of steel cabling that facilitate the movement of the cabin along the boom and enable the raising and lowering of the spreader. Additionally, the equipment room contains Variable Frequency Drives (VFDs) for controlling the electrical motors. The crane's Programmable Logic Controllers (PLCs) and industrial switches are also housed within this room.
- **Crane Monitoring Station (CMS)** – The number and location of CMS computers varies. Traditionally, there will be at least two, one in the cabin and one in the equipment room. Some cranes may have a CMS located in a small room at the base of the crane which technicians use to avoid scaling a crane.
- **Crane remote operator location** – Frequently there is an electrical box located at the base of the crane which contains buttons and switches to control some of the crane functions. These controls align with some of the controls available in the cabin, but not all features can be controlled from this location.
- **Quay** – Lanes where trucks drive under the crane to be loaded/unloaded.

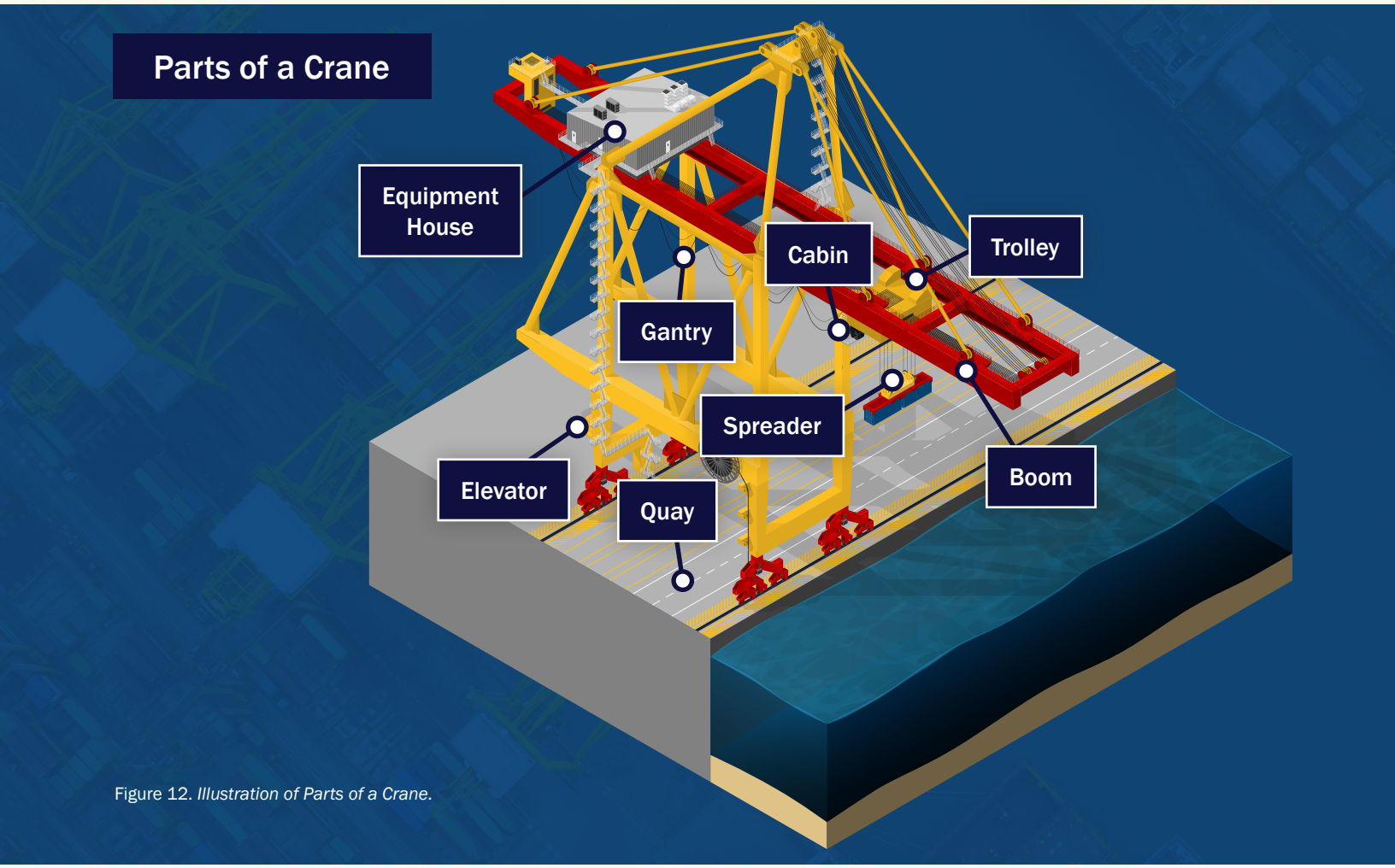


Figure 12. *Illustration of Parts of a Crane.*

Consolidated Findings

CPTs have executed missions across seven Commercial Strategic Seaports[37] involving cranes manufactured in China. The Coast Guard is the leading government agency assessing cybersecurity for cranes manufactured in China, conducting 11 missions and spending hundreds of days sensored on cranes. CPTs note that the depth of sensoring varies from mission to mission. For example, some missions included sensors placed within cranes to include the crane's industrial switch that directly communicates to operational technology (OT) elements via PROFINET or similar OT protocols, while other missions included sensors at the IP gateway to a network that includes multiple cranes.

Most Common Findings

Our most common findings for STS crane networks are similar to our common findings for *any* OT system: improper network segmentation, legacy software, and identity/access management. In all cases, CPTs recommended mitigations to better isolate the STS cranes and reduce remote access threat vectors.

STS Crane Common Findings

1. **Improper network segmentation:**
   a. Inadequate firewall/routing table configurations.
   b. Improper isolation between Virtual Local Area Networks (VLANs).
   c. Lack of proper monitoring and logging of inbound/outbound network traffic.
   d. Secure Shell (SSH) exposed to public internet.
   e. External network access of monitoring workstation.
2. **Legacy protocols:**
   a. Link-Local Multicast Name Resolution (LLMNR) – Highly susceptible to brute forcing, pass-the-hash, and remote code execution attacks. Deprecated in April 2022.
   b. Server Message Block version 1 (SMBv1) – Allows for relay attacks, remote code execution, and enumeration. Deprecated in June 2013.
   c. Virtual Network Computing (VNC), Telnet, and File Transfer Protocol (FTP) – Transmission of credentials and other data in plaintext.
3. **End of Life Operating Systems:**
   a. Windows XP Embedded SP2 EoL was January 11, 2011.
   b. Windows Server 2003 EoL was July 14, 2015.
   c. Windows 7 EoL was January 14, 2020.
   d. Cisco 2950 EoL was October 20, 2013.
4. **Weak password policy and improper account privileges:**
   a. Non-essential use of elevated access.
   b. Shared passwords and accounts, including administrator accounts.
   c. Password reuse.
   d. Weak password policy/complexity.
   e. Easily crackable/guessable passwords.
   f. Authentication bypass.
   g. Default passwords.
   h. Cleartext credentials.
5. **Unexpected services – "upgrades" not included (or realized by crane owner) in original contract:**
   a. Cellular modems on crane spreaders.
   b. Security camera systems.

[37] https://www.maritime.dot.gov/ports/national-port-readiness-network-nprn

Recommended Best Practices

Administrative Controls

- **Scrutinize contract language** that requires remote access, installation of cellular modems, or other third-party maintenance procedures. Conduct routine physical audits to verify compliance with contractual agreements. The partners with the best crane security postures have been aggressive in challenging these access requirements through the contracting process.
- Establish policies and procedures to **restrict remote access from third-party vendors to minimum necessary**. If required, consider compensating controls to mitigate the risk this remote access introduces.
- If the cranes' systems are fully physically isolated (aka air-gapped) then **identify a single port and cable that can provide connectivity to the crane network**. Policy should dictate under what circumstances this connection can be made, by whom, and notification should be provided to cybersecurity personnel monitoring the network. When the purpose for crane connectivity has concluded, the systems should be disconnected and network isolation validated.
- **Establish and enforce user account management** policies in accordance with general best practices.[38]
- **Avoid shared accounts and enable non-repudiation.**[39] User and administrator accounts should not be shared.
- **Implement principle of least privilege**. If a user requires administrator level access, a separate admin account should be created for performing specific administrator actions. All user and admin accounts should have the least level of privilege necessary.
- **Enforce a password policy** in accordance with the National Institute of Science & Technology (NIST) Special Publication 800-63B.

Malicious Cyber Activity (MCA)?
While we have observed many significant vulnerabilities on STS cranes manufactured in China that a threat actor could exploit to disrupt crane/port operations, Coast Guard CPTs have not observed any active malicious cyber activity (MCA) on these crane systems. There may be a few reasons for this:

1. Most CPT crane missions have been focused on identifying exploitable vulnerabilities and risks associated with crane systems/networks as opposed to a identifying active MCA.
2. We expect any MCA to take the form of living off the land techniques, using built-in features of the crane systems to appear as legitimate activity. Without implementing some of the best practices listed here, including account non-repudiation and centralized logging, it is difficult to discern normal network activity from MCA with any certainty.

All this underscores the importance of removing any potential supply chain-induced access channels (cellular modems, remote maintenance, poor network segmentation).

[38] Source: Cybersecurity Performance Goals (https://www.cisa.gov/cybersecurity-performance-goals-cpgs)
[39] Source: non-repudiation - Glossary | CSRC (https://csrc.nist.gov/glossary/term/non_repudiation)

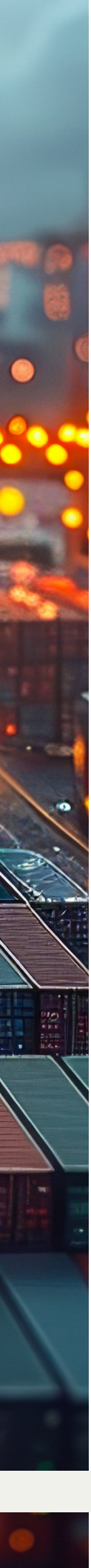
Technical Controls

- **Implement network segmentation.** If a physical separation or air-gap is not feasible, partners should strive to implement best practices discussed in the 2023 CTIME[40] including:
  - Multiple layers of network security should exist between a crane's IT and OT systems.
  - A firewall should be present at the boundary point of a crane network and be properly configured to implicitly deny all inbound and outbound traffic and explicitly allow only very specific traffic to transit the firewall.
  - Ensure the crane network exists in an isolated VLAN. All routing tables must ensure this VLAN and the crane IP schema is only communicable within the VLAN. If IPv6 is not in use, then it should be disabled on all hosts and explicitly blocked in all routing tables/firewalls.
- **Enable secure communications (i.e., PROFINET)** with sign and encrypt turned on for messages. Authenticating device communication makes it more difficult for a supply chain compromise to result in spoofed critical components and restricts legitimate devices to sending messages they would normally send.
- **Harden IT hosts across enterprise (both crane and non-crane networks).**
  - All IT devices should be updated to supported operating systems, if possible, with upgrades to modern hardware when hosts are no longer capable of running updated software.
  - Host-based firewalls should be enabled and configured to maximum restriction levels.
  - IT hosts should be configured to send logs to a centralized location. **Centralized logging** is essential for identifying malicious or unauthorized activity.
- Implement security best practices on **the entirety of the port's network infrastructure** – beyond the crane.
  - Legacy and deprecated protocols should be disabled. Partners should have full knowledge of the remote access methods used on their networks.
  - System and security log retention should be configured to retain logs for at least the period between log review to avoid purging unreviewed logs (at least quarterly).
- **Ensure full visibility for remote access methods.** Reduce remote access options to the bare minimum necessary and implement centralized logging.
  - If not required for operation, all cellular modems and other access points which could allow potential backdoor access (if abused) should be removed from all parts of crane.
  - If crane technicians use a remote desktop capability, a secure method like Microsoft Windows Remote Desktop Protocol (RDP) should be used, requiring access by username, password, and Multi-Factor Authentication (MFA) if possible, and only accessible from within the isolated VLAN.

Third party remote desktop tools, especially those that require cloud access or use insecure authentication by default (e.g., TeamViewer, VNC, etc.) should be avoided. For additional OT hardening recommendations please review CISA's Principles of Operational Technology Cybersecurity.[41]

[40] https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf
[41] https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security

APPENDICES



Appendix A
MARITIME CYBER INFORMATION PRODUCTS

The Coast Guard Cyber Command (CGCYBER) Maritime Cyber Readiness Branch (MCRB) generates two types of information products. These products are Maritime Cyber Alerts and Maritime Cyber Bulletins (MCB). Both products are typically TLP:CLEAR[42] and may be shared without restriction. Maritime Cyber Alerts provide specific and actionable mitigating measures for critical vulnerabilities or threat group activity. MCBs provide awareness on cyber trends and threats MCRB has observed in the Marine Transportation System (MTS) along with general recommendations and resources to assist the MTS in hardening its cybersecurity posture. To contact MCRB through email: MaritimeCyber@uscg.mil or telephone: (703) 201-0396.

Maritime Cyber Alerts Released in 2024

- **01-24 Exploitation of Ivanti Connect Secure and Policy Secure Gateways**[43]
  This Maritime Cyber Alert provides information on the known Common Vulnerability and Exposures (CVEs) for Ivanti Connect Secure and Ivanti Policy Secure solutions. It identifies targeted applications and systems, threat actor tactics, mitigation measures MTS partners can take, and the known indicators of compromise (IOCs).

Maritime Cyber Bulletins Released in 2024

- **01-24 Critical Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities Identified**[44]
  This MCB provides information on Ivanti Connect Secure and Ivanti Policy Secure vulnerabilities. It identifies recommendations and resources available to help mitigate the threat posed by this vulnerability, which has been rated CRITICAL by the Cybersecurity and Infrastructure Security Agency (CISA).
- **02-24 Threat Actors Targeting Amazon Web Services (AWS) Simple Storage Service (S3) Vulnerability**[45]
  This Maritime Cyber Bulletin provides information on ransomware actors targeting a known AWS S3 vulnerability to scam their victims into paying financial ransoms. It identifies recommendations and resources available to help mitigate the chances of suffering a ransomware attack.
- **03-24 Spoofed Business Websites**[46]
  This MCB provides guidance to maritime partners for identifying and addressing fraudulent websites masquerading as their legit websites.
- **04-24 Russian Military Cyber Actors Targeting Critical Infrastructure**[47]
  This MCB highlights Russian military cyber actors targeting U.S. and global critical infrastructure.
- **05-24 Peoples Republic of China - Cyber Espionage Campaign**[48]
  This MCB highlights Malicious actors affiliated with China that have compromised networks of multiple global telecommunications companies in a broad and significant cyber espionage campaign.

[42] Source: Traffic Light Protocol (TLP) Definitions and Usage | CISA (https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage)
[43] Source: Maritime Cyber Alert 01-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Alert 01-24 TLP CLEAR.pdf)
[44] Source: CGCYBER Maritime Cyber Bulletin 01-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Bulletin%2001-24_Ivanti_TLP-CLEAR.pdf)
[45] Source: CGCYBER Maritime Cyber Bulletin 02-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Bulletin 02-24_Ransomware_Scam_S3.pdf)
[46] Source: CGCYBER Martime Cyber Bulletin 03-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime%20Cyber%20Bulletin%2003-24_Spoofed_Business_Website.pdf)
[47] Source: CGCYBER Maritime Cyber Bulletin 04-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Bulletin 04-24_Russian_Military_Cyber_Threat_Actors_Targeting_Critical_Infrastructure 24SEP2024.pdf)
[48] Source: Maritime Cyber Bulletin 05-24 (https://www.uscg.mil/Portals/0/Images/cyber/Maritime Cyber Bulletin 05-24_PRC_Cyber_Espionage_TLP-CLEAR.pdf)

Appendix B

OBSERVED CYBER CRIMINAL ORGANIZATIONS AND MALWARE TYPES

The following criminal organizations or named malware strains were used during exploitation activities within the Marine Transportation System (MTS) via National Response Center (NRC) reports, Cyber Protection Team (CPT) missions, or publicly available incident response activities.

Organizations

Akira

Since it was first observed in 2023, Akira ransomware has compromised over 250 organizations with an estimated impact of approximately $42 million (USD).[49] In 2024, Akira compromised user accounts at a U.S. port and at multiple contracting organizations that work closely with MTS organizations.

Hunters International

Hunters International is a Ransomware-as-a-Service (RaaS) group that emerged in 2023. In 2024, Hunters International compromised a plastics production and supply company and executed PowerShell scripts attempting to exfiltrate sensitive data.

LockBit

LockBit is a RaaS group and deployed the most ransomware worldwide in 2022. LockBit ransomware was developed to be as simple as possible, appealing to malicious actors with little to no "hacking" background.[50] In 2024, LockBit was observed launching a large-scale phishing campaign against a U.S. port authority.

RansomHub

RansomHub is a RaaS group that has compromised over 200 organizations worldwide with no focus on any single industry. They have a public set of rules similar to "terms of service" for users of their malware.[51] In 2024, RansomHub compromised a shipping company and gained access to information technology onboard company owned vessels.

Rhysida

Rhysida is a RaaS group that has been active since early 2023 with primary targets being wealthy North American and European organizations. Their normal methodology is initial access approximately one (1) week before delivering effects.[52]

[49] Source: #StopRansomware: Akira Ransomware | CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a)
[50] Source: Ransomware Spotlight: LockBit | Trend Micro (US) (https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit)
[51] Source: RansomHub Ransomware Analysis, Simulation, and Mitigation - CISA Alert AA24-242A (picussecurity.com) (https://www.picussecurity.com/resource/blog/ransomhub-ransomware-cisa-alert-aa24-242a)
[52] Source: #StopRansomware: Rhysida Ransomware | CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a)

Malware Families

Raccoon Stealer

Raccoon Stealer is one of the most well-known and widely used information-stealing malware families and is sold as a subscription model for threat actors.

AndroxGh0st

AndroxGh0st is a Python scripted malware that specifically targets applications that use Laravel, an open-source Hypertext Preprocessor (PHP) based web framework. It uses various Hypertext Transfer Protocol (HTTP) methods to find initial footholds in its victims.

LOCKBIT.BLACK

LOCKBIT.BLACK is ransomware written in C programming language that can encrypt local files. Encrypted files are set to a random, seven-character filename with a fixed extension, and ransom notes are written to directories with encrypted files. In 2024, a LOCKBIT ransom note was found during a CPT mission on Server Message Block (SMB) traffic at a shipyard company.

ICEDID

ICEDID is a backdoor written in C programming language that communicates via HTTP, Hypertext Transfer Protocol Secure (HTTPS), or WebSocket. In 2024, payloads for ICEDID were seen in network logs of a shipyard company.

WARZONE

WARZONE is a backdoor written in C++ programming language that communicates via a custom protocol over Transmission Control Protocol (TCP). Its capabilities include video and screenshot capture, remote desktop, keylogging, file transfer, file execution, and reverse shell creation. In 2024, payloads for WARZONE were seen in network logs of a shipyard company.

AGENTTESLA

AGENTTESLA is a .NET-based credential stealer capable of capturing keystrokes, clipboard data, camera images, and screenshots. AGENTTESLA also targets credentials stored by applications. In 2024, payloads for AGENTTESLA were seen in network logs of a shipyard company.

POISONPLUG

POISONPLUG is a highly obfuscated, modular backdoor with plug-in capabilities. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. In 2024, POISONPLUG was found on Barracuda email servers.

SEASPRAY

SEASPRAY is a launcher written in Lua programming language that is a trojanized Barracuda email security gateway module. SEASPRAY registers an event handler for incoming email attachments. If an attachment has a filename that contains a magic value, SEASPRAY copies the file into “/tmp” directory and executes an external binary that establishes a reverse shell with the full path as a parameter.

Appendix C

KNOWN EXPLOITABLE VULNERABILITIES DETECTED ON CPT MISSIONS

This appendix contains the top observed vulnerabilities from CISA's KEV Catalog. Information for these vulnerabilities comes from the NIST National Vulnerability Database, https://nvd.nist.gov/.

Common Vulnerability and Exposure (CVE) Name	CVE ID	CVSS	CWE	Missions Observed
Microsoft WinVerifyTrust Function Remote Code Execution	CVE-2013-3900	7.6	CWE-347	10
Hypertext Transfer Protocol (HTTP)/2 Rapid Reset Attack Vulnerability	CVE-2023-44487	7.5	CWE-400	8
Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability	CVE-2024-21338	7.8	CWE-822	5
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	CVE-2024-21351	7.6	CWE-94	5
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	CVE-2024-21412	8.1	CWE-693	5
Apache HTTP Server- Side Request Forgery (SSRF)	CVE-2021-40438	9.0	CWE-918	4
Microsoft Windows Print Spooler Remote Code Execution Vulnerability	CVE-2021-34527	9.0	CWE-269	4
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	CVE-2023-36025	8.8	NA	4
Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability	CVE-2023-36033	7.8	CWE-822, CWE-119	4
Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	CVE-2023-36036	7.8	CWE-787, CWE-122	4

Table 2. *Vulnerabilities Detected on CPT Missions.*

Appendix D
SUMMARY OF ATTACK PATHS

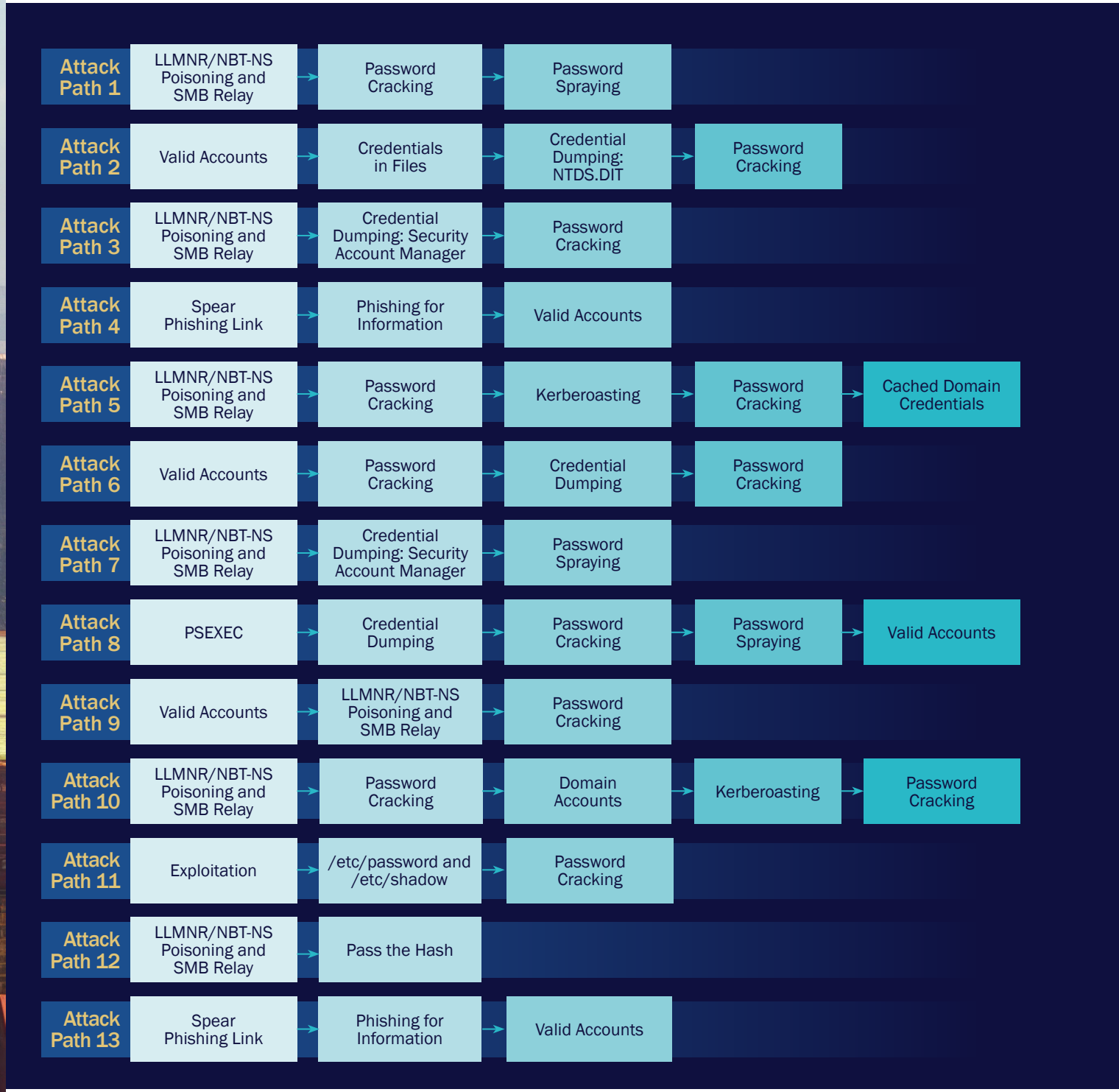


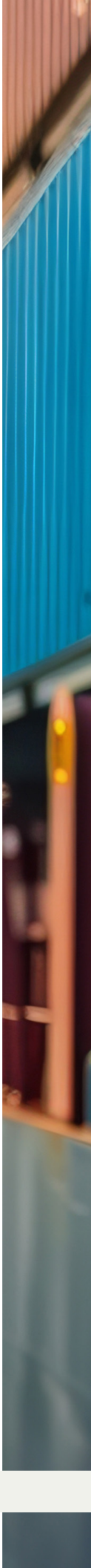
Figure 13. *Summary of Attack Paths.*

Appendix E
SUMMARIZED FINDINGS

Top 10 MITRE ATT&CK® Techniques used on 2024 CPT Missions and comparisons to previous years.

Finding	2022	2023	2024
Valid Accounts: T1078	12	23	29
Remote Services: T1210, T1021 & T1133	1	N/A	25
Brute Force: T1110	22	30	21
Adversary-in-the-Middle: T1557	8	15	15
Exploit Public Facing Application: T1190	4	8	12
Default Credentials (ICS): T0812	N/A	N/A	9
Privilege Escalation: T1068	N/A	N/A	8
Phishing: T1566	6	18	8
Password Policy: T1201	N/A	N/A	7
Unsecured Credentials: T1552	2	3	7

Table 3. *Top 10 MITRE ATT&CK® Techniques.*



Appendix F
MITIGATIONS

Mitigation Actions from Partners

Six months following Cyber Protection Team (CPT) assessments, partners are asked to provide a status of their actions in response to the recommend CPT Mitigations. As shown below in Table 4: *Mitigation Status – Calendar Year (CY) 21, CY22, CY23 and CY24 Comparison*, in 2024 partners Fully or Partially Mitigated 96% of all findings.

All Findings	CY21	CY22	CY23	CY24
Fully Mitigated	48%	52%	48%	61% (↑)
Partially Mitigated	33%	36%	38%	35% (↑)
Accepted Risk	5%	3%	9%	4% (↑)
False Positive	2%	1%	0%	0% (↓)
No Action Taken to Date	12%	8%	15%	0%

Table 4. *Mitigation Status CY21, CY22, CY23, and CY24 Comparison.*

As these metrics are built from 6-month follow-up surveys, the CY24 metrics include only the missions completed in the first half of CY24. Additionally, the responses to these follow-ups remain voluntary, and response rates have been lower relative to 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 recommendation. Table 5: *Common Mitigation Recommendations* summarizes this data and compares this year's findings to those found in 2021, 2022, and 2023. "Mapped Findings" represents the mitigations associated with the CPTs' findings, and greater detail for each mitigation can be found by searching each mitigation code here: MITRE ATT&CK®.[53]

Mitigation Recommendation	CY21	CY22	CY23	CY24
Password Policies: M1027, M0927	1st	1st	1st	1st(-)
Disable or Remove Feature or Program: M1042, M0942	N/A	13th	4th	T-2nd (↑)
Update Software: M1051, M0951	6th	5th	7th	T-2nd (↑)
User training: M1017, M0917	7th	6th	6th	4th (↑)
Encrypt Sensitive Information: M1041, M0941	N/A	N/A	N/A	T-5th (↑)
User Account Management: M1018, M0918	N/A	7th	9th	T-5th (↑)
Network Segmentation: M1030, M0930	N/A	10th	5th	T-7th (↓)
Multi-factor Authentication: M1032, M0932	4th	2nd	2nd	T-7th (↓)
Account Use Policies: M1036, M0936	N/A	N/A	N/A	T-9th (↑)
Audit: M1047, M0947	N/A	12th	10th	T-9th (↑)
Privileged Account Management: M1026, M0926	N/A	4th	3rd	T-9th (↓)

Table 5. *Common Mitigation Recommendations.*

[53] https://attack.mitre.org/

Appendix G
LIST OF ACRONYMS

AWS	Amazon Web Services
CGCYBER	Coast Guard Cyber Command
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CySO	Cybersecurity Officers
CPT	Cyber Protection Team
FEMA	Federal Emergency Management Agency
IOCs	Indicators of Compromise
IT	Information Technology
MCRB	Maritime Cyber Readiness Branch
MFA	Multi-Factor Authentication
MTS	Marine Transportation System
NIST	National Institute of Standards and Technology
NRC	National Response Center
NSA	National Security Agency
OT	Operational Technology
USCG	United States Coast Guard
ZPMC	Shanghai Zhenhua Heavy Industries Co.

CYBER SUPPORT RESOURCES

Enabling Hardening and Assessing Risk Posture

Coast Guard CPT Assessments and Hunts

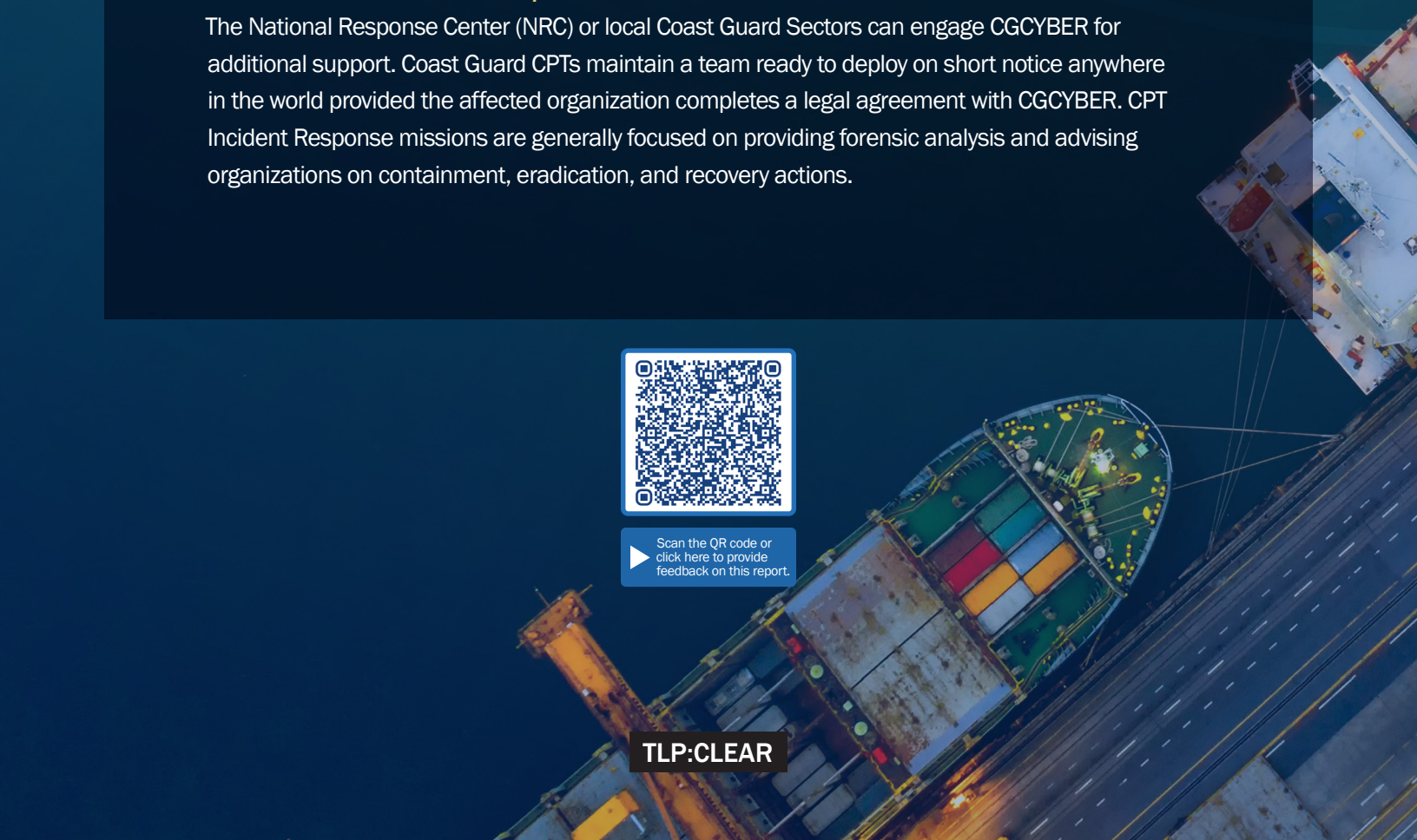
Coast Guard Cyber Command (CGCYBER) offers Cyber Protection Team (CPT) assessments and hunt missions to organizations within the MTS. If an organization would like to request a CPT mission, they should reach out to the local Coast Guard Sector's Maritime Transportation Security Specialist-Cyber (MTSS-C). 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.

Cybersecurity & Infrastructure Security Agency (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 National Response Center (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.



Scan the QR code or click here to provide feedback on this report.