Coast Guard Cyber Protection Team (CPT) Missions and Capabilities

Maritime Cyber Readiness Branch, CGCYBER

LTJG Matthew Fritz

Readiness | Resilience | Response

Maritime Cyber Readiness Branch Overview

US Coast Guard Cyber Command
Maritime Cyber Alert 03-23

October 4, 2023

Information Sharing Protocol: TLP: CLEAR (https://www.us-cert.gov/tlp)

Threat from Cl0p Ransomware Group

US Coast Guard Cyber Command
Maritime Cyber Alert 02-23

June 15, 2023

Information Sharing Protocol: TLP: CLEAR (https://www.us-

BlackBasta Ransomware Group

2023 CYBER TRENDS AND
INSIGHTS IN THE MARINE ENVIRONMENT

Coast Guard Cyber Command

Maritime Cyber Readiness Branch Roles

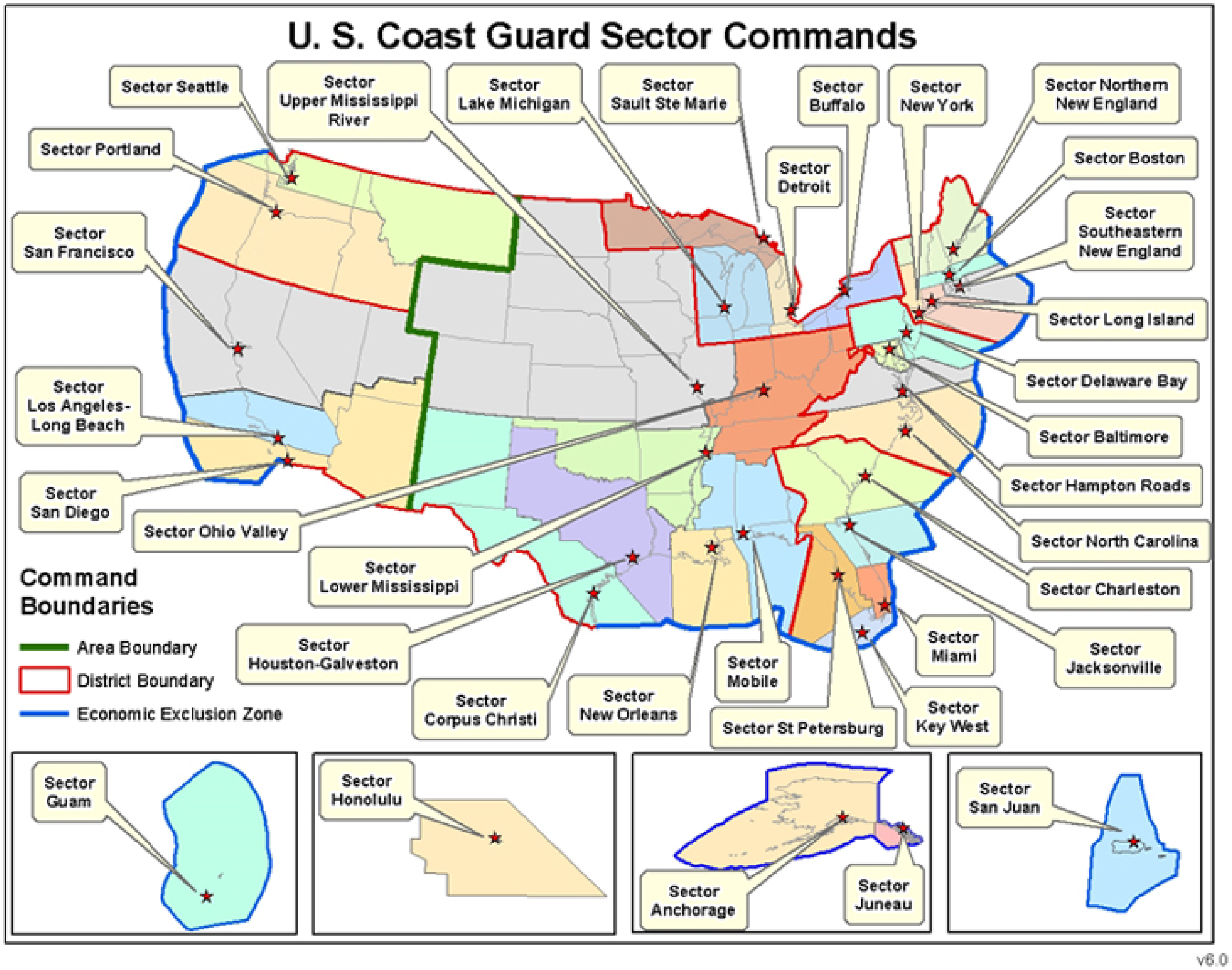
- Provides direct support to operational commanders to prevent and respond to cyber-related MTS disruptions.
- Provides outreach, engagements, and information sharing services to increase cyber literacy throughout the MTS.

Outreach Products Include:

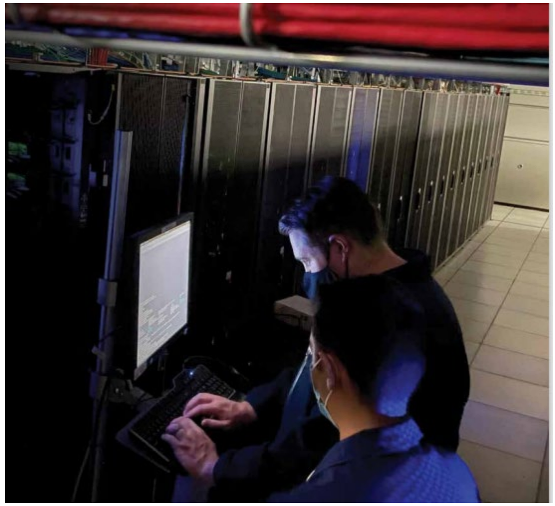
- Maritime Cyber Alert (MCA)
- Marine Safety Information Bulletins
- https://www.uscg.mil/maritimecyber
- maritimecyber@uscg.mil

Marine Transportation System Specialist - Cyber Subject Matter Experts (SME)

- **Liaison**
  - Maritime industry, interagency, Area Maritime Security Committee’s, etc
- **Advisor**
  - Help the COTP understand the cyber threat landscape and risk to the MTS.
- **Exercise Planner & Coordinator**
  - Advocate for inclusion of cybersecurity scenarios where appropriate in annual security exercises
- **Information Sharing**
  - Key communicator to foster cyber awareness, expertise & regulatory compliance



Cyber Protection Teams



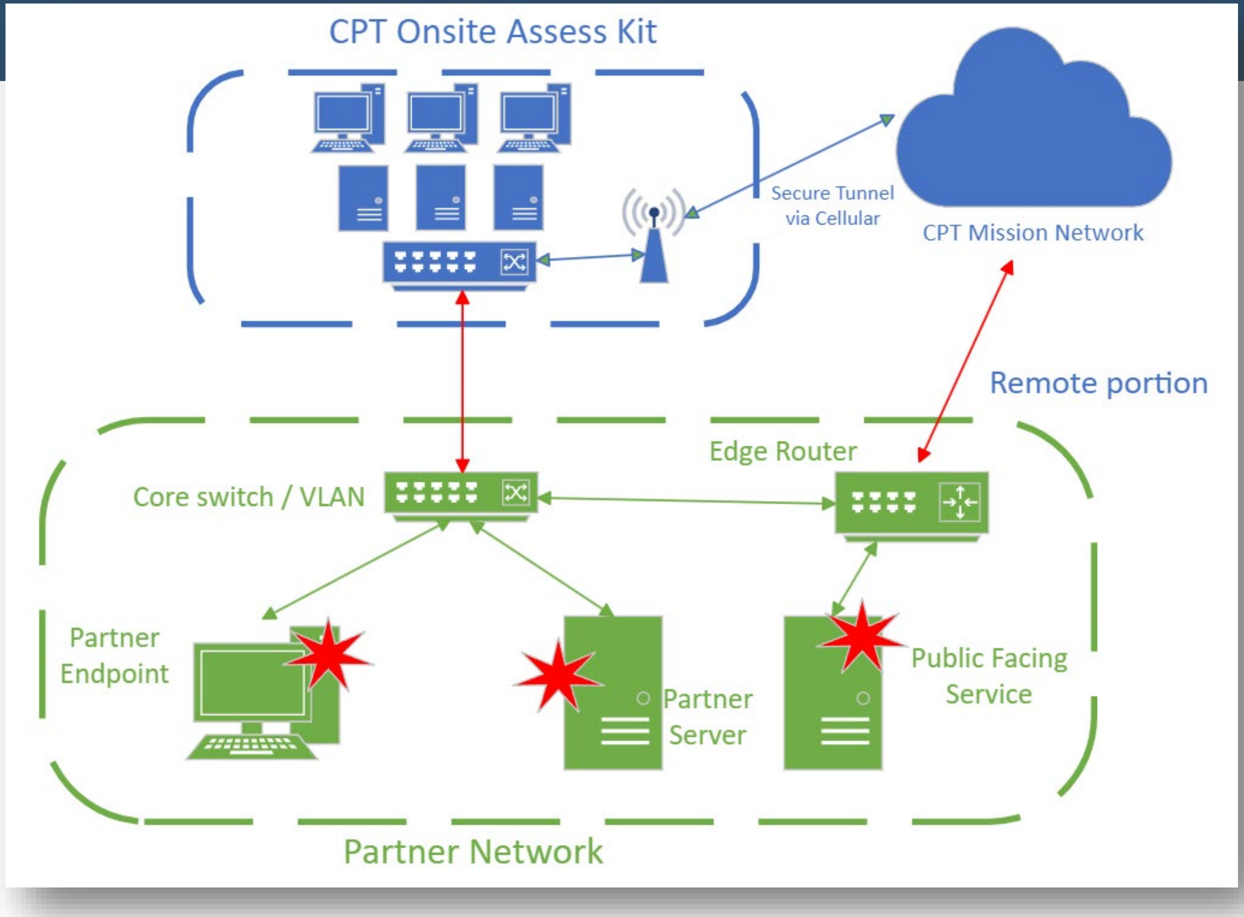
- **USCG Cyber Protection Teams:**
- Based in Washington, D.C. and Alameda, CA
- Support local Captains of the Port in cyber missions
- Three CPTs (39 Members Each)
  - 9 Deployable Elements in total (3 per CPT)
  - Intelligence and mission support elements

- **Team Composition**
- Active Duty Coast Guard Officers and Enlisted
- Government Civilians

- **Team Experience and Background**
- Trained to DOD joint standards/qualifications
- Wide range of industry standard training and certifications
- 8-12+ months of Department of Defense cyber training
- Previous positions at CISA, USCYBER, and NSA

Assessment Mission Overview

- **Goal**: identify & prioritize vulnerabilities for remediation. Identify the most viable *attack path* an adversary would use to compromise your network.
- **What we do**: use penetration testing & vulnerability assessment techniques.
    - Remote: phishing (clicks & credential harvesting), web penetration testing, external enumeration.
    - On-Site: active scanning, credential dumps & analysis, local network attacks, domain exploitation, application exploitation.
- **We may request**: network diagrams, configuration files, application documentation, privileged account creation.



Technical Scoping Call(s)

Remote Mission Portion (1 week)

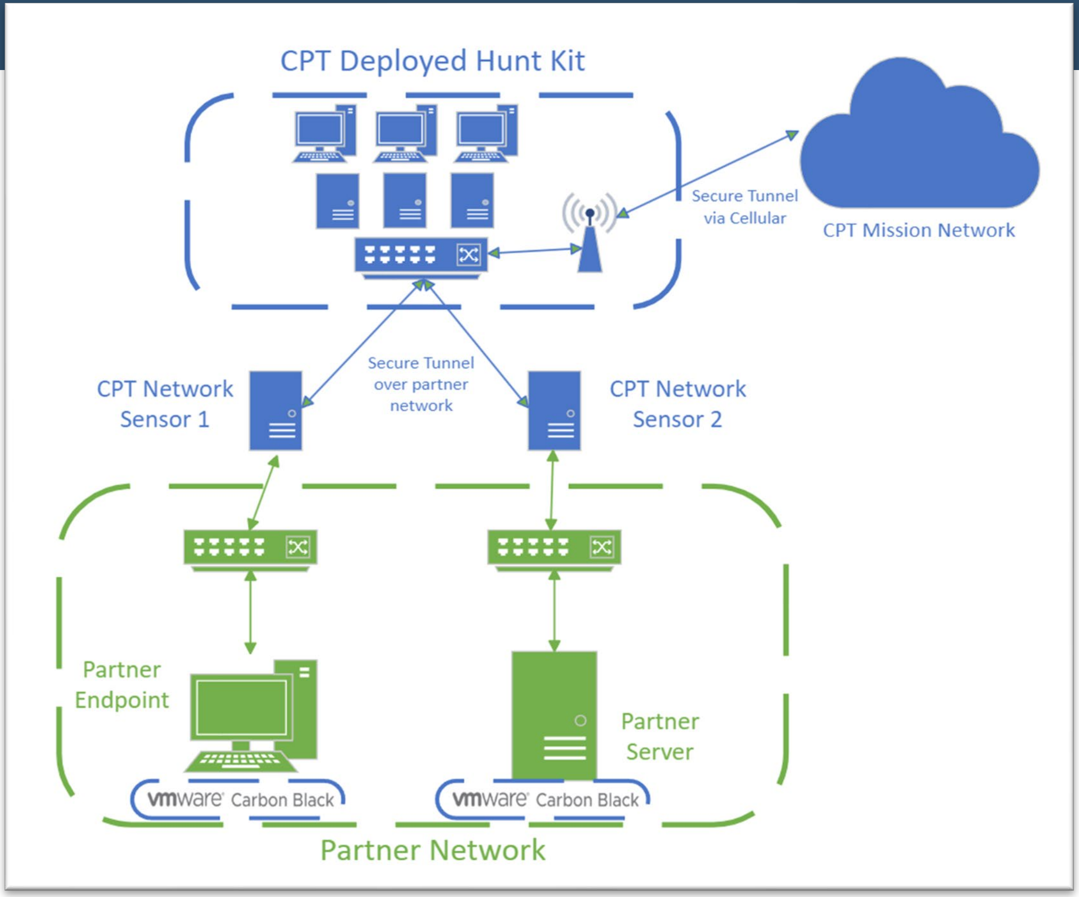
On-site Mission Portion (1 week)

Daily Partner Syncs

Mission Report (~45 days after mission conclusion)

Hunt Mission Overview

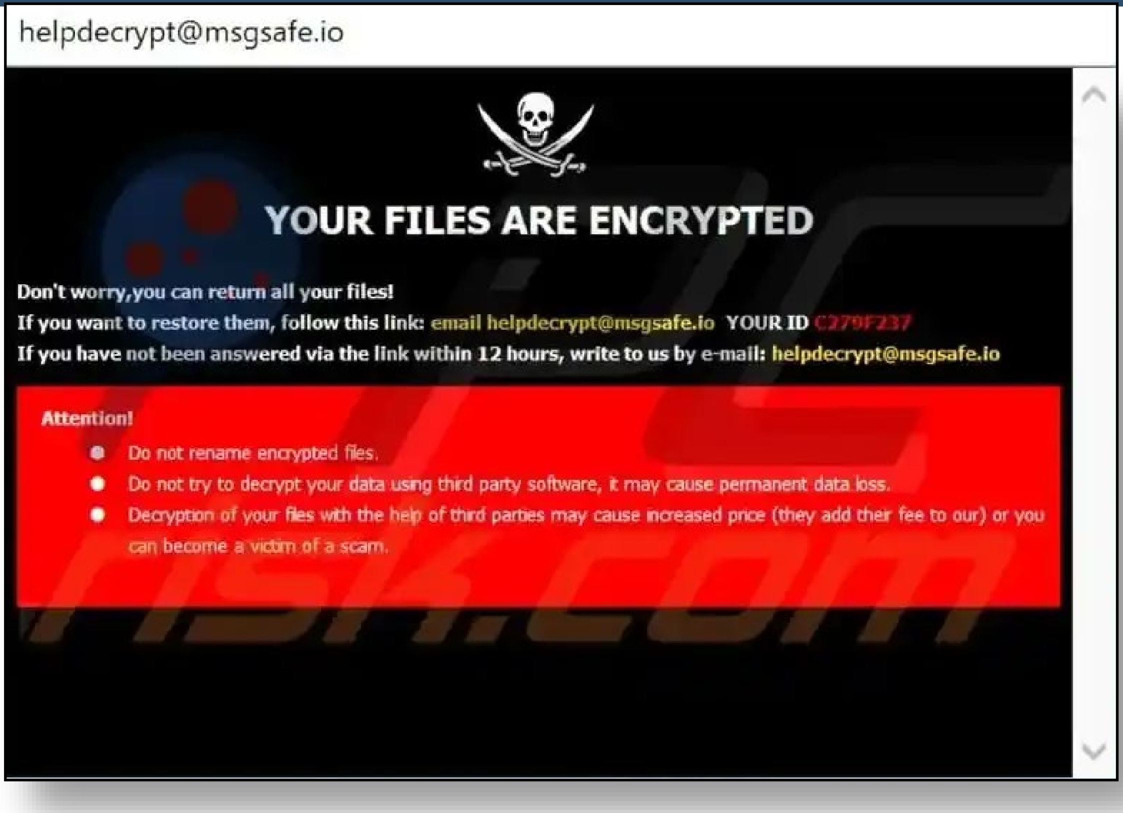
- **Goal**: identify malicious cyber activity (MCA) and/or provide network hardening recommendations.
- **What we do**: install sensors (network & host), passively collect data, and analyze it on our kit.
  - If MCA is identified, we can help transition to incident response (IR) activities.
- **We may request**: network diagrams, configuration files, application documentation.



Technical Scoping Call → Pre Deployment Site Survey (PDSS) → Sensor Install (~2 weeks prior to mission start) → Mission Start: Team onsite to conduct hunt activities → Daily Partner Syncs → Mission Report (~45 days after mission conclusion)

Incident Response

- **Goal:** After a mission partner in the MTS experience a cyber incident (ransomware, data breach, cyber effects), perform analysis to determine initial access, lateral movement & privilege escalation, and extent of data exfiltration.
- **What we do:**
  - Connect mission partner with intelligence community & other government agencies (FBI, CISA, etc).
  - Take & analyze forensic images.
  - Analyze network & host logs.
  - Advise on hardening activities based on incident.
- **We may request:**
  - Forensic images.
  - Logs (host, network, appliances).
  - Network diagrams.



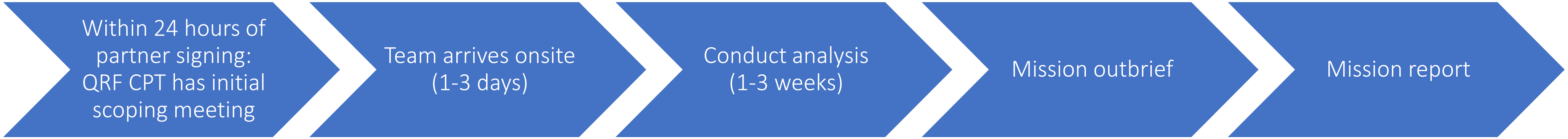
helpdecrypt@msgsafe.io

YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID C279F237
If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.



Within 24 hours of partner signing: QRF CPT has initial scoping meeting

Team arrives onsite (1-3 days)

Conduct analysis (1-3 weeks)

Mission outbrief

Mission report

Assessment+ (Operational Technology)

- **Goal:** Safely assess sensitive Operational Technology (OT) systems in conjunction with in-scope IT systems.
- **What we do:**
  - Normal assessment profile on in-scope IT network.
  - Install passive sensors on OT portions of the network:
    - Analyze traffic to determine cross talk between IT/OT networks.
    - Identify OT assets, determine baseline behavior.
    - Identify exploitable/vulnerable protocols when possible.
    - Validate OT network architecture through passive sensors.
  - For IT hosts on the OT network (e.g. Human Machine Interfaces): conduct authenticated scanning to determine vulnerabilities.

Deployment Technology

In one DMSS Kit:

- Tool and data processing capacity to execute CPT missions on 10K+ endpoints
- CPT Maintains several kits to support multiple deployments

Hardware	
High Performance Servers	Individual Computing Platform
Network Connection and Access	Switches/Routers/Gateways
Isolation Capability	Taps/Forensic Bridges/Forensic Docks
Software Capabilities	
Vulnerability Assessment	Threat Emulation
Endpoint Detection	Forensic Assessment
Network Detection	Remote Connectivity
Admin and Intel	Distributed Data Analysis

CPT Mission Overview

Mission	Format	Personnel	Pre-Mission Scoping (Signed RTA)	Deliverable
Assessment	1 Week Remote (Washington D.C.) 1 Week On-Site	1 Element Lead 4-8 Operators 1 Intel Support	4-8 Weeks	• Risk and Vulnerability Assessment Report • Hardening Advice
Hunt	1-3 Day Sensor placement 2 Weeks On-Site	1 Element Lead 4-8 Operators 1 Intel Support	4-8 Weeks	• Detailed Findings Summary Report • Hardening Advice
Incident Response	~1-3 Weeks, but varies based on the scope and severity of the incident.	1 Element Lead 1-3 Operators Intel Support	<24 Hours	• Technical Forensics Report • Remediation Advice

Email maritimecyber@uscg.mil to discuss the specifics of the request and how CPT can assist.

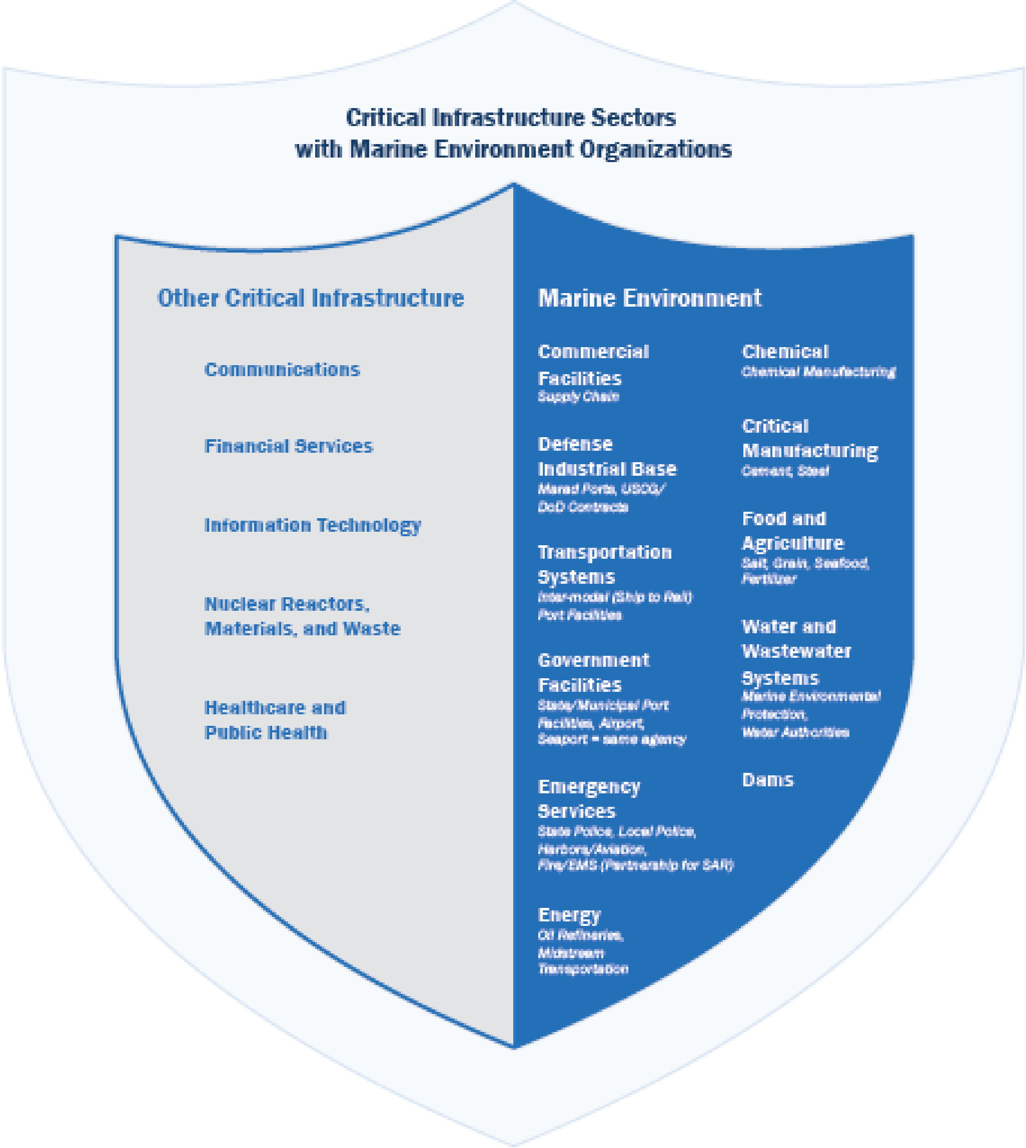
2023 Cyber Trends and Insights in the Marine Environment

Understanding the Marine Environment

The ME consists of:

- 25,000 miles of coastal and inland waterways
- 361 ports
- 124 shipyards
- Over 20,000 bridges,
- Over 50,000 Federal aids to navigation
- 95,000 miles of shoreline
- supports the flow of approximately $5.4 Trillion in goods and services
- 90% of U.S. imports and exports entering or exiting by ship

All interconnected and overlapping with other critical infrastructure sectors.



Critical Infrastructure Sectors
with Marine Environment Organizations

Other Critical Infrastructure

Communications

Financial Services

Information Technology

Nuclear Reactors, Materials, and Waste

Healthcare and Public Health

Marine Environment

Commercial Facilities
Supply Chain

Defense Industrial Base
Marad Ports, USCG/ DoD Contracts

Transportation Systems
Inter-modal (Ship to Rail) Port Facilities

Government Facilities
State/Municipal Port Facilities, Airport, Seaport = same agency

Emergency Services
State Police, Local Police, Harbors/Aviation, Fire/EMS (Partnership for SAR)

Energy
Oil Refineries, Midstream Transportation

Chemical
Chemical Manufacturing

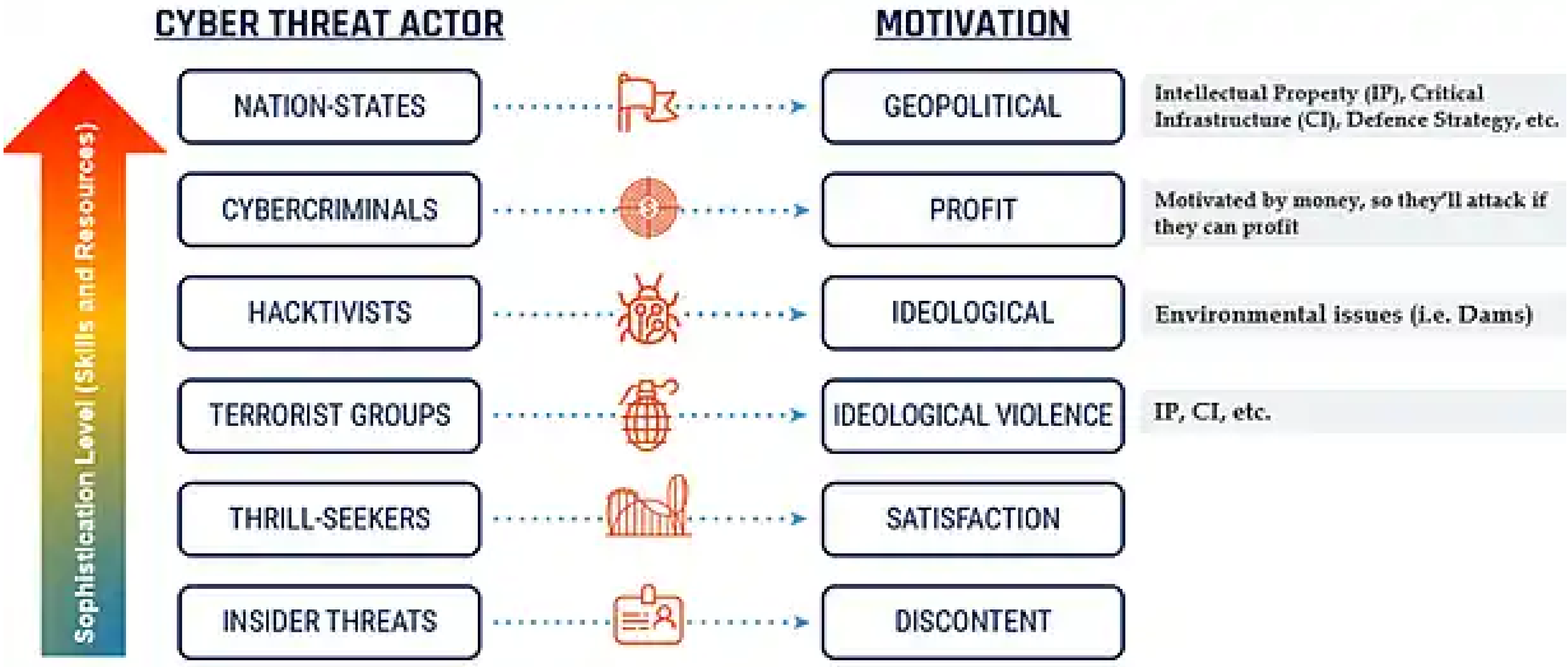
Critical Manufacturing
Cement, Steel

Food and Agriculture
Salt, Grain, Seafood, Fertilizer

Water and Wastewater Systems
Marine Environmental Protection, Water Authorities

Dams

Threat Landscape



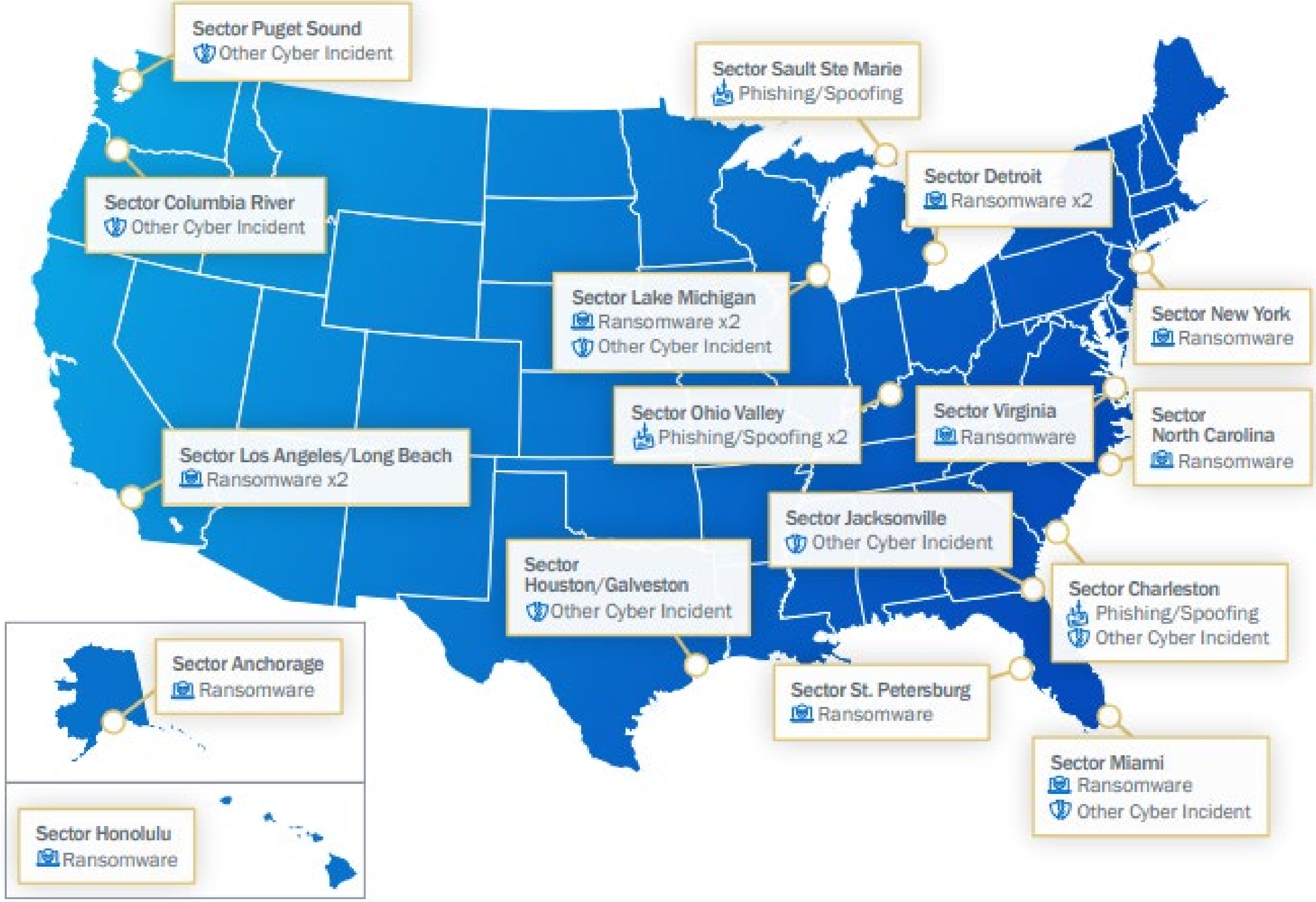
CYBER THREAT ACTOR	MOTIVATION	
NATION-STATES	GEOPOLITICAL	Intellectual Property (IP), Critical Infrastructure (CI), Defence Strategy, etc.
CYBERCRIMINALS	PROFIT	Motivated by money, so they'll attack if they can profit
HACKTIVISTS	IDEOLOGICAL	Environmental issues (i.e. Dams)
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE	IP, CI, etc.
THRILL-SEEKERS	SATISFACTION	
INSIDER THREATS	DISCONTENT	

Source: https://gca.isa.org/blog/common-ics-cybersecurity-myth-5-financially-motivated-cyberattacks

MCRB Incident Observations

THREAT

- Spoofing/Phishing
  - Spear-Phishing Campaigns
  - Typo-squatted Domains
- Ransomware
  - Evolving Techniques
  - Targeting Back-up Systems
- Other
  - Structured Query Language (SQL) Injection
  - Denial-of-Service
  - Brute Force
  - Etc.



Coast Guard Investigated 46 Cybersecurity incident reports in 2023

Observed Cyber Criminal Organizations

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.

Observed Cyber Criminal Organizations Cont.

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.

CTIME 2023 – Key Takeaways

Takeaway 1

Significant uptick of reported Advanced Persistent Threats targeting the Marine Environment (ME)

Takeaway 2

Ransomware incidents continue to surge in 2023

Takeaway 3

CGCYBER identified similar cybersecurity deficiencies that were in the two previous CTIME reports

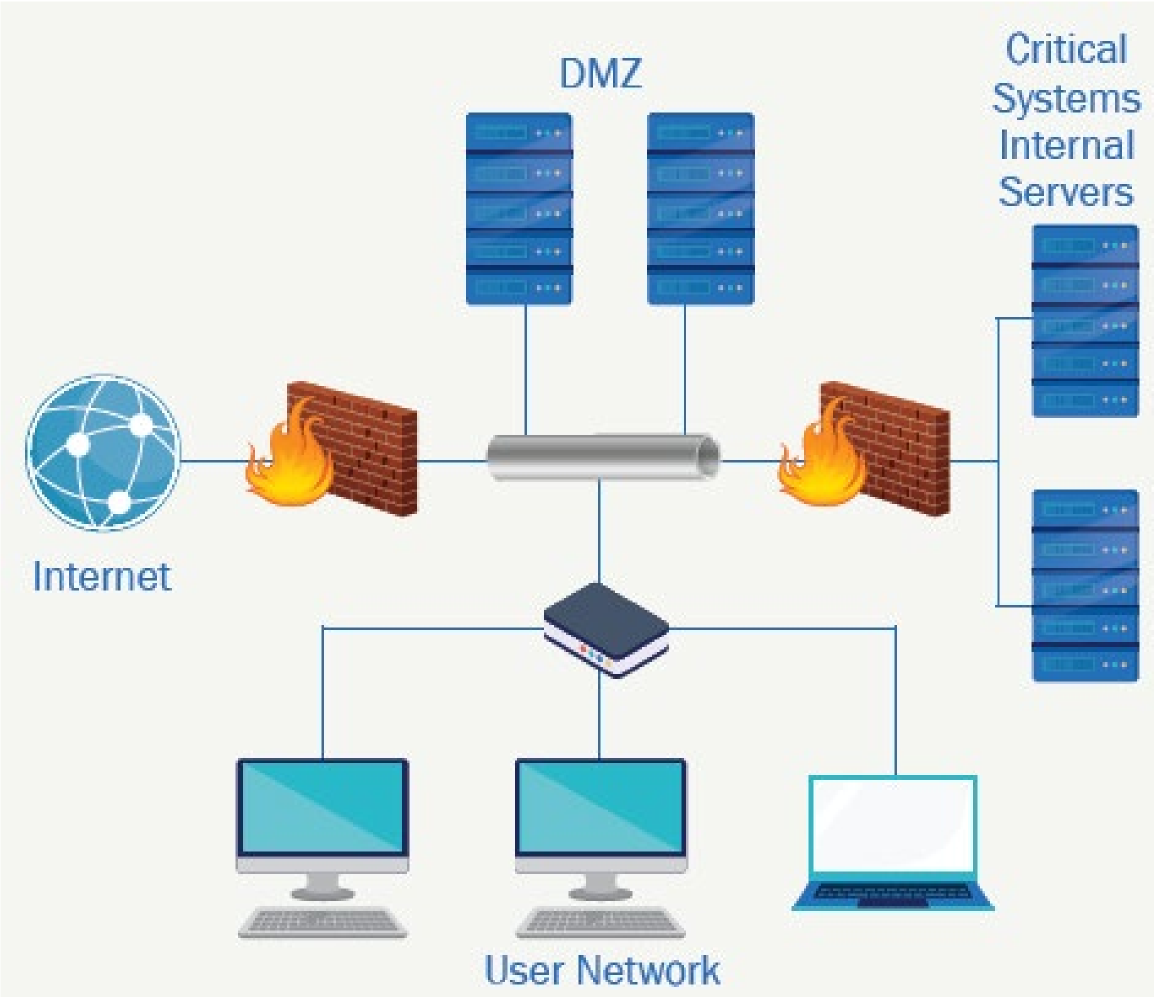
Takeaway 4

Network-connected Operational Technology (OT) introduces attack vectors to the ME

CPT Findings and Mitigations

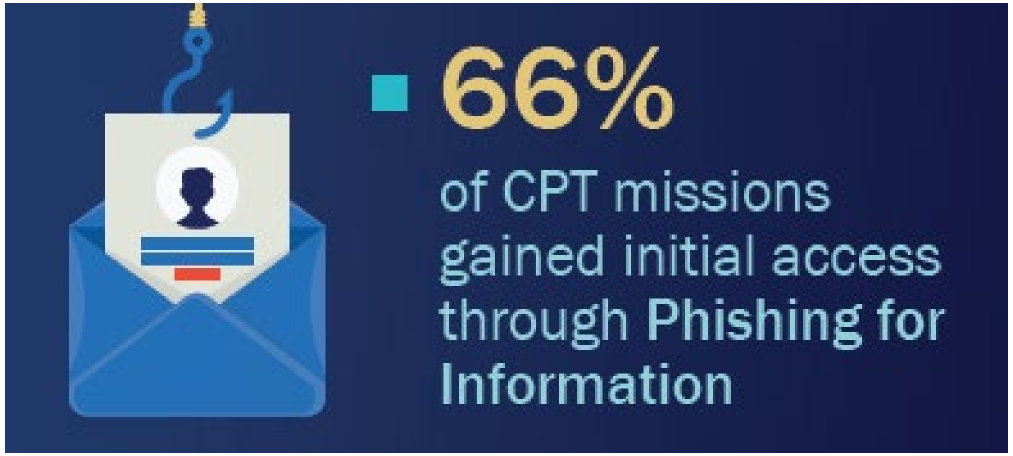
Top Findings from CPT Assessments

- Common initial access techniques:
  - Phishing for Information
  - Valid Accounts
- Common Privilege Escalation Techniques:
  - Adversary-in-the-Middle
  - Brute Force Password Cracking
- Other Common Observations:
  - Known Exploitable Vulnerabilities (KEVs)
  - Living off the Land

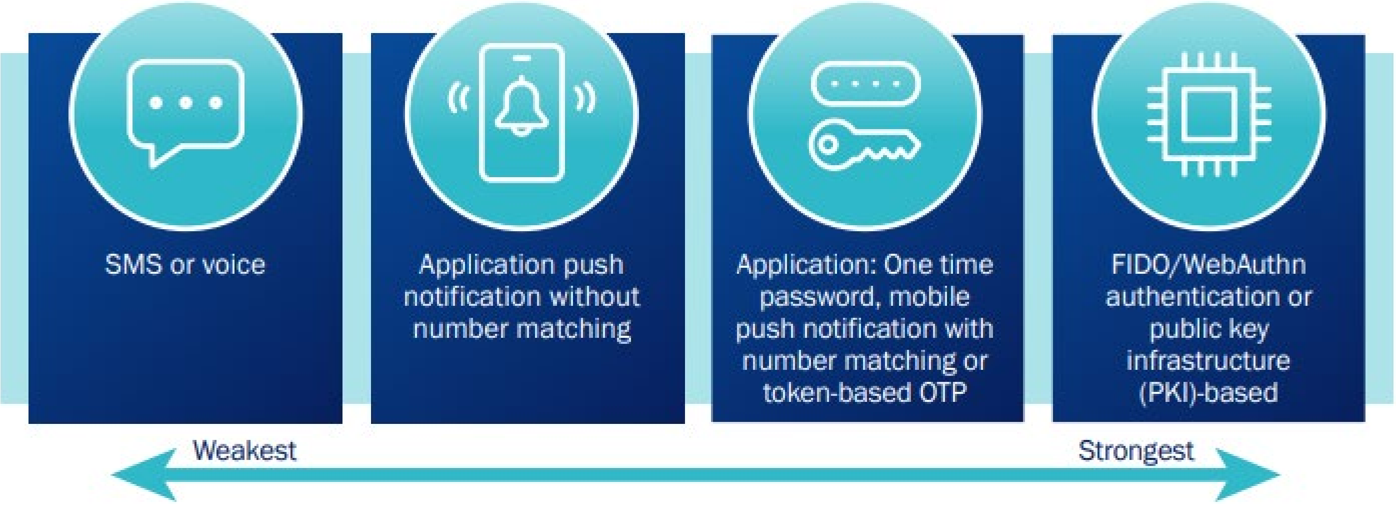


Phishing for Information & Valid Accounts

- Phishing is used to gain useful information, such as a username and password, from the phished user.
- Using Valid Accounts was the most common initial access technique used during Assess missions. These were often gathered from publicly available sources or from Phishing for Information.
- 10.8% of all phishing emails resulted in a click by a user, of those who clicked the link, 6.7% of users provided credentials when requested.



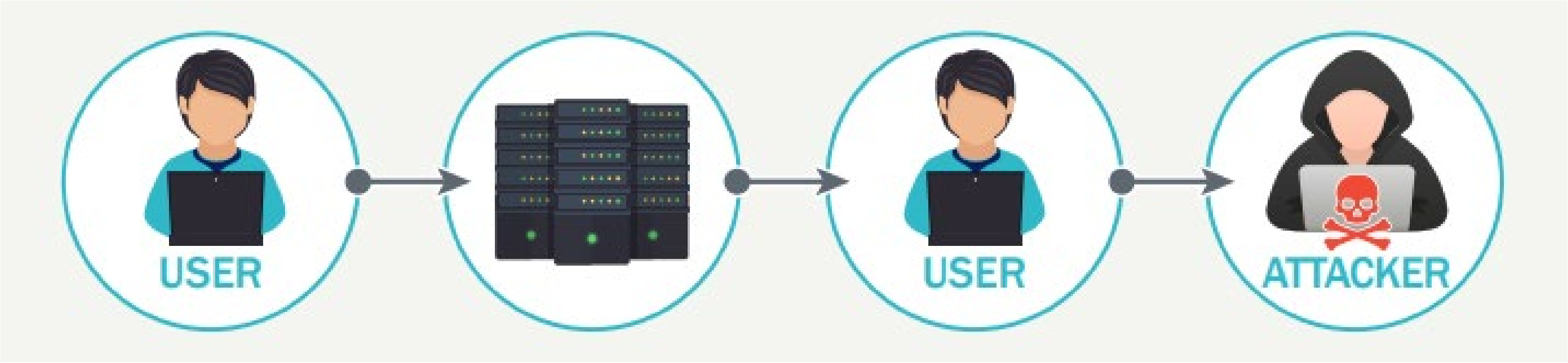
66% of CPT missions gained initial access through Phishing for Information


SMS or voice
Application push notification without number matching
Application: One time password, mobile push notification with number matching or token-based OTP
FIDO/WebAuthn authentication or public key infrastructure (PKI)-based
Weakest
Strongest

Spectrum of MFA Implementation

Adversary-in-the-Middle

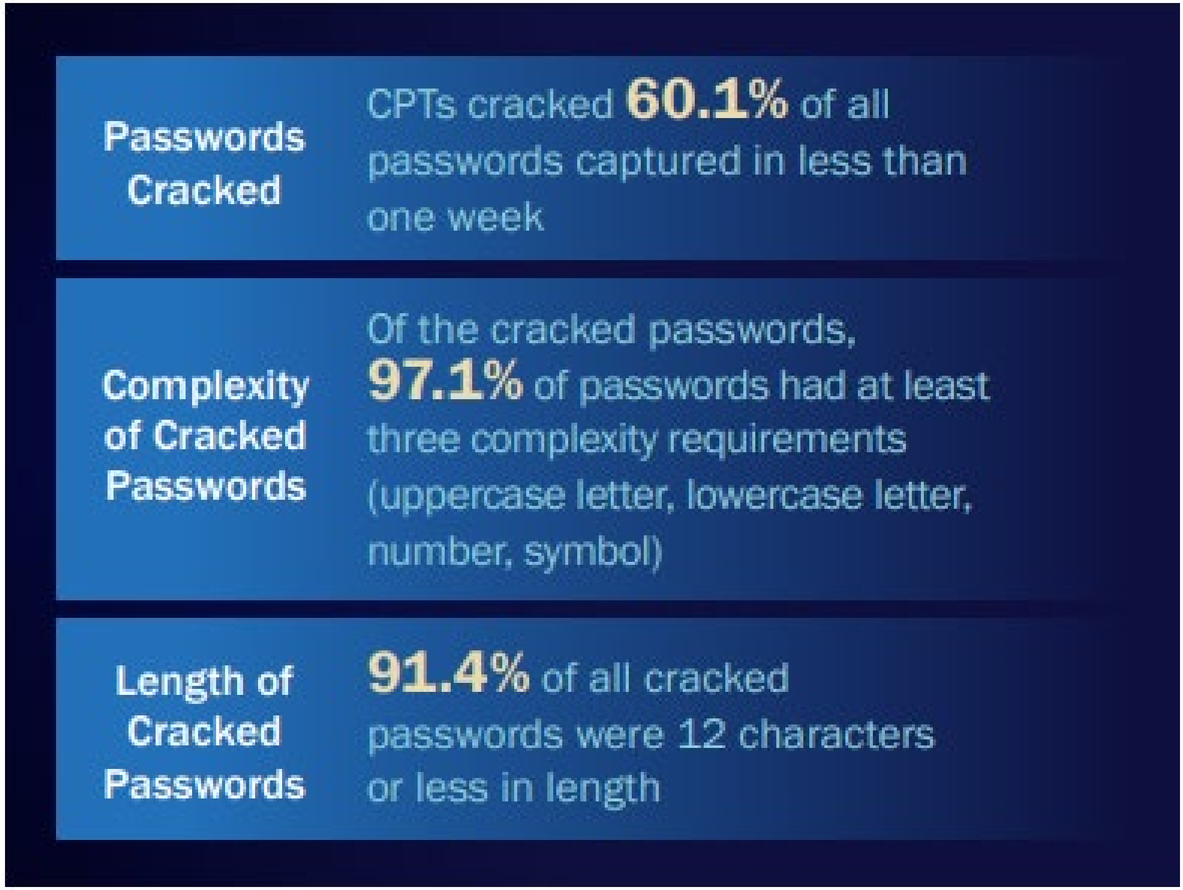
- Adversary-in-the-Middle techniques consist of **an attacker inside the network responding and directing traffic to an adversary-controlled system** to directly obtain hashed or even sometimes plaintext credentials.
- Used in 72% of CPT assessments and was the most common privilege escalation technique used by the CPTs.
- Once a hash is captured, the adversary will pivot to password cracking techniques to determine the plaintext credentials.



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

Brute Force: Password Cracking

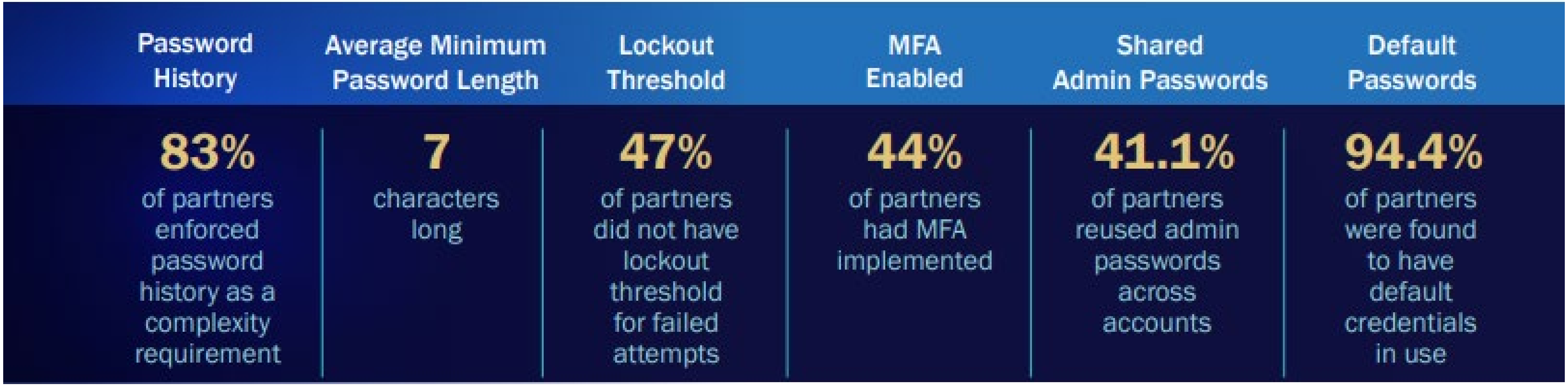
- CPT assessments validate NIST’s recommendation that **password length is the primary factor in characterizing password strength.**
- CISA’s 2023 password guidance for businesses recommends that user passwords be **at least 16 characters long.**
- CISA recommends providing an **enterprise level password manager** to encourage employees to use strong passwords and discourage employees from reusing passwords.



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

Password Cracking Observations

Brute Force: Password Cracking (Cont.)



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

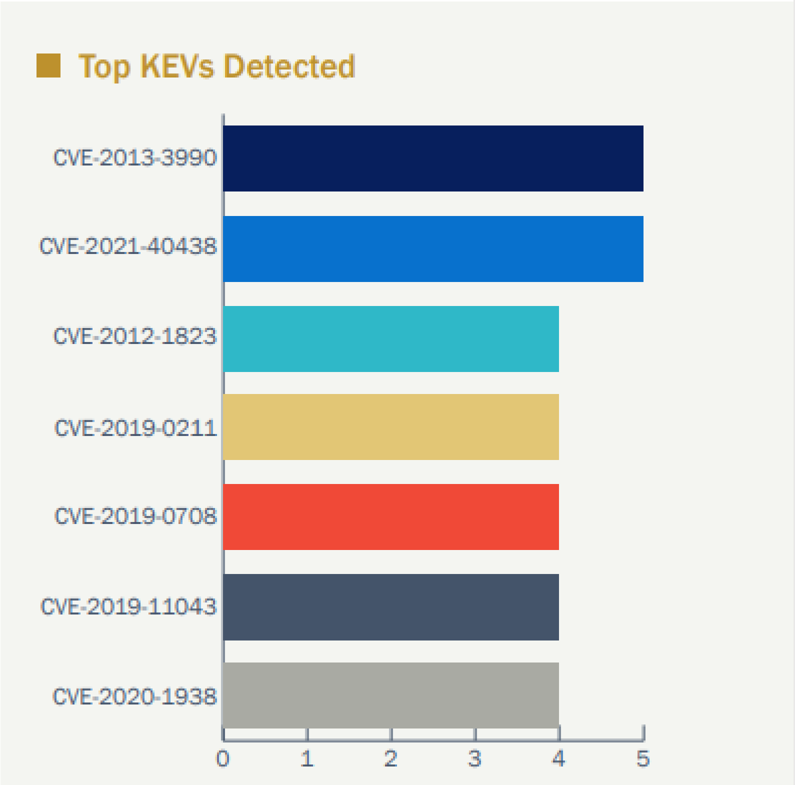
Averages of Observed Passwords

Patch Management

- The most critical of vulnerabilities are those that are proven to be exploitable. These vulnerabilities are listed in CISA's KEV Catalog.
- KEVs were detected in 61% of CPT assessments.
- None of the most common KEVs are new.
- 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**.

304

Known Exploitable Vulnerabilities (KEVs) detected across assessments



Top KEVs Detected During CY23 Assess Missions

Living off the Land

- 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**.
- Actors utilizing Living off the Land are reportedly targeting the Active Directory database (Ntds.dit) for potential exfiltration.
  - Ntds.dit file contains critical information needed to manage a network including accounts and password information.
  - Review the locations where their Ntds.dit is stored to ensure protections and logging are in place.
- Detect malicious Living off the Land activity
  - Establishing an accurate baseline of how system utilities are used in an environment,
  - Retain logs for extended periods,
  - Investigate uses that differ from that baseline.

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

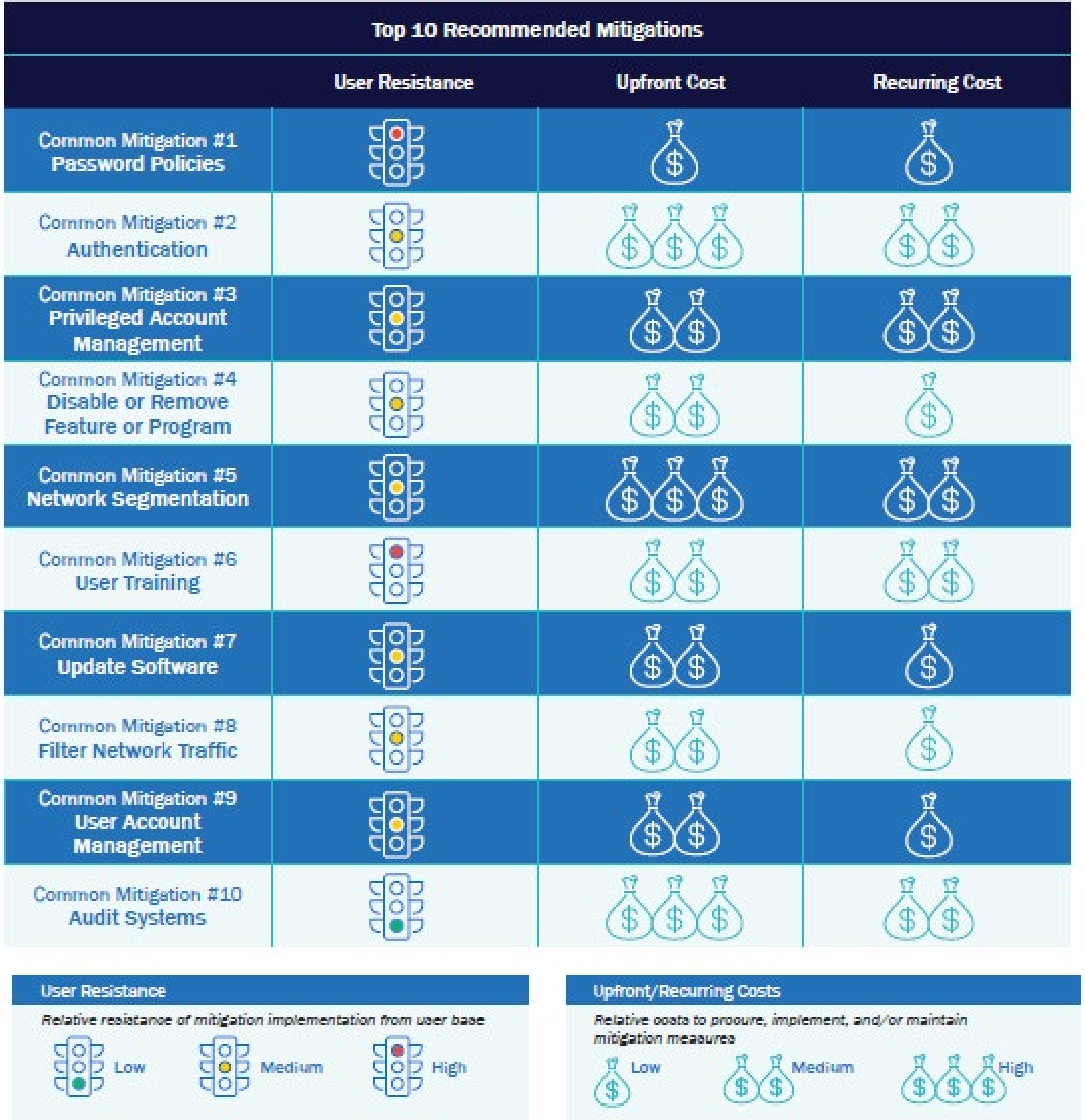
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

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

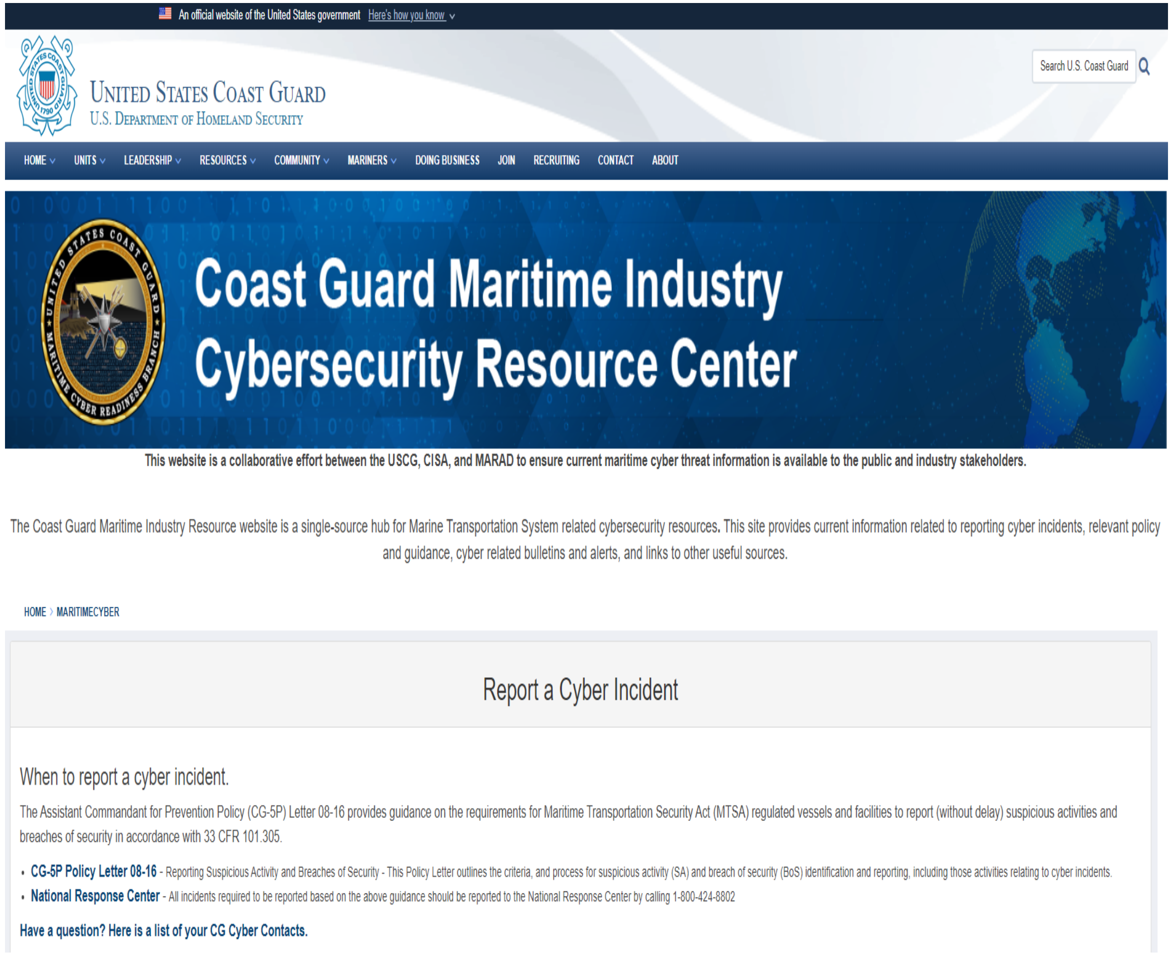
💰 Low 💰💰 Medium 💰💰💰 High

Common Mitigation Findings

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

Coast Guard Maritime Industry Cybersecurity Resource Center

- A single-source hub for Marine Transportation System related cybersecurity resources.
- Provides current information related to reporting cyber incidents, relevant policy and guidance, cyber related bulletins and alerts, and links to other useful sources.


An official website of the United States government Here's how you know
United States Coast Guard
U.S. Department of Homeland Security
Search U.S. Coast Guard
HOME
UNITS
LEADERSHIP
RESOURCES
COMMUNITY
MARINERS
DOING BUSINESS
JOIN
RECRUITING
CONTACT
ABOUT

Coast Guard Maritime Industry Cybersecurity Resource Center

This website is a collaborative effort between the USCG, CISA, and MARAD to ensure current maritime cyber threat information is available to the public and industry stakeholders.

The Coast Guard Maritime Industry Resource website is a single-source hub for Marine Transportation System related cybersecurity resources. This site provides current information related to reporting cyber incidents, relevant policy and guidance, cyber related bulletins and alerts, and links to other useful sources.

HOME › MARITIMECYBER

Report a Cyber Incident

When to report a cyber incident.

The Assistant Commandant for Prevention Policy (CG-5P) Letter 08-16 provides guidance on the requirements for Maritime Transportation Security Act (MTSA) regulated vessels and facilities to report (without delay) suspicious activities and breaches of security in accordance with 33 CFR 101.305.

- **CG-5P Policy Letter 08-16** - Reporting Suspicious Activity and Breaches of Security - This Policy Letter outlines the criteria, and process for suspicious activity (SA) and breach of security (BoS) identification and reporting, including those activities relating to cyber incidents.
- **National Response Center** - All incidents required to be reported based on the above guidance should be reported to the National Response Center by calling 1-800-424-8802

Have a question? Here is a list of your CG Cyber Contacts.

Questions?