TLP:CLEAR

2022 CYBER TRENDS AND INSIGHTS IN THE MARINE ENVIRONMENT

Coast Guard Cyber Command

United States Coast Guard

TLP:CLEAR

Approved for public release; distribution unlimited. Date: 22 May 2023

2022 Cyber Trends and Insights in the Marine Environment Report

FOREWORD

I am pleased to present the U.S. Coast Guard Cyber Command (CGCYBER)'s Cyber Trends and Insights in the Marine Environment (CTIME) report for calendar year 2022. As U.S. Coast Guard missions expand into the cyberspace domain and across the global maritime commons, CGCYBER remains strategically postured to protect the maritime critical infrastructure from advanced cyber threat actors. As the Commandant highlighted in the Coast Guard's 2021 Cyber Strategic Outlook, "We will employ a risk-based approach to protect the nation from threats originating in and through the maritime environment, and we will leverage the full set of our authorities; the ingenuity and leadership of our people; and the breadth of our civil, military and law enforcement partnerships to protect the nation, its waterways, and those who operate upon them from harm."

Since the Coast Guard released its first Cyber Strategy in 2015, we have observed events reinforcing that cyberspace remains a contested domain including the exploitation of Federal government information networks, attacks on maritime critical infrastructure, and adversarial efforts to undermine our democratic processes. This 2022 CTIME report serves to share some of the specific trends and insights Coast Guard Cyber Command has gathered through its partnerships with ports, facilities, vessel operators, and all levels of government on some of the common vulnerabilities and potential threat vectors to the marine environment.

Our deployable cyber forces will stand ready to augment field commanders with subject matter expertise, assessment, and incident response capabilities, as well as critical infrastructure support in the identification and mitigation of cyber risk and threats looking to harm the Marine Transportation System, the backbone of the United States' economy.

Sincerely,

John C. Vann
Rear Admiral, United States Coast Guard
Commander, Coast Guard Cyber Command

EXECUTIVE SUMMARY

The United States Coast Guard has a strong tradition of collaborating with owners and operators in the Marine Environment (ME) to provide relevant information about best practices to secure their critical systems. Since December 2020, Coast Guard Cyber Command (CGCYBER) has vastly grown its presence and increased its operational tempo to protect cyber systems underpinning the ME. The observations and findings in this report provide Coast Guard units and their port partners with relevant information to identify and address cyber risks. Coast Guard Cyber Protection Teams (CPTs) and the Maritime Cyber Readiness Branch (MCRB) developed these findings through technical engagements throughout 2022 with ME partners.

Key Takeaways

1. **CGCYBER identified similar cybersecurity deficiencies at new organizations assessed in 2022 commensurate with our 2021 CTIME Report recommendations.** 2022 CPT missions reinforced many of the same recommendations to ME organizations provided to other organizations in 2021 related to basic cyber hygiene, including implementing a **Patch Management Policy**, enforcing the principle of **Least Privilege**, and implementing a **Strong Password Policy,** or **Multi-Factor Authentication (MFA).**

2. **Emerging technologies introduce new attack vectors to the ME.** There is a rapid increase in the use of cloud-based environments and remote-access solutions for ME networks. These new technologies bring many benefits; however, they introduce risks if not implemented correctly. These risks become even more significant when cloud environments are bolted onto legacy systems or services without adequate security controls. It is essential for organizations to understand the risks of new technology and the available safeguards to mitigate those risks.

3. **Opportunistic Cyber Criminals and Advanced Persistent Threats (APTs) continue to target the ME**. Cyber criminals continue to profit from disruption of critical functions and often gain access by targeting company users with methods such as **Phishing for Information** or by **Compromising Systems with Known Exploitable Vulnerabilities (KEV)**. APTs are more focused and use a variety of tactics, ranging from exploitation of common vulnerabilities to installation of sophisticated malware. The **Cybersecurity and Infrastructure Security Agency (CISA)/CGCYBER Joint Alert AA22-174A** provides a sample of techniques discovered by CGCYBER believed to be used by APTs.

4. **Importance of Timely Information Sharing:** Timely information sharing is the most effective universal action to strengthen the ME, prevent future cyber-attacks, and enable timely response to exploitable vulnerabilities. CGCYBER observed a promising increase in voluntary reporting in 2022, but many organizations remain reluctant to report or share information with the Coast Guard or other partners. The Coast Guard continues to encourage information sharing through Department of Homeland Security (DHS)-sponsored public-private partnership groups, like Area Maritime Security Committees (AMSCs) or the Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC). These groups can facilitate this information sharing, while addressing the organization's privacy concerns.

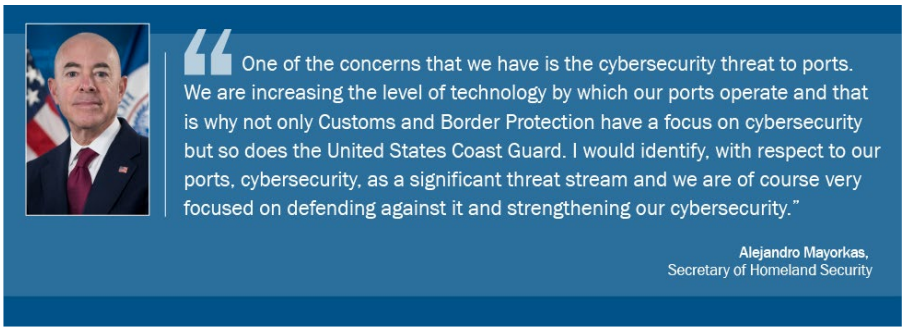
INTRODUCTION

This report provides a high-level analysis of observed cybersecurity practices and adversary activities within the ME from January 1, 2022 to December 31, 2022. The report uses recorded metrics to identify trends that will aid Coast Guard and maritime industry decision makers. These decision makers include: Coast Guard Areas/Districts/Sectors; their staffs; and maritime facility leadership 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. Awareness of these trends should improve stakeholders' ability to identify and address cyber risks within their purview.

The United States Coast Guard (Coast Guard) has been designated as the Co-Sector Risk Management Agency (SRMA) for the maritime portion of the Transportation Sector, making the Coast Guard responsible for protecting maritime Critical Infrastructure and Key Resources (CI/KR). To meet these responsibilities, the Coast Guard has been given legal authority to prevent, detect, and respond to threats endangering maritime CI/KR. Each Area, District, and Sector Commander has a Marine Transportation Systems Specialist – Cyber (MTSS-C) to advise their command on cyber risks in the ME.

CGCYBER is uniquely capable of conducting cyber operations to execute these responsibilities. CGCYBER will:

1. Provide technical assistance to State, Local, Territorial, and Tribal (SLTT) entities by enhancing Maritime Critical Infrastructure's cyber resilience within their Area of Responsibility (AOR).
2. Participate in the Critical Incident Communication (CIC) process when necessary and support Maritime Security (MARSEC) Level change processes, as needed.
3. Assist Federal/SLTT agency and private/commercial entities operations in the ME.



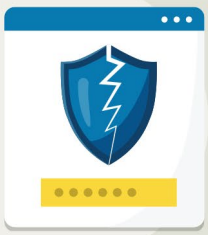
2022

TRENDS & INSIGHTS SCORECARD

20%
Increase
in cyber event reporting in CY22 compared to CY21

$4.82M
Average Cost
of a critical infrastructure data breach according to Ponemon Institute and IBM Security*

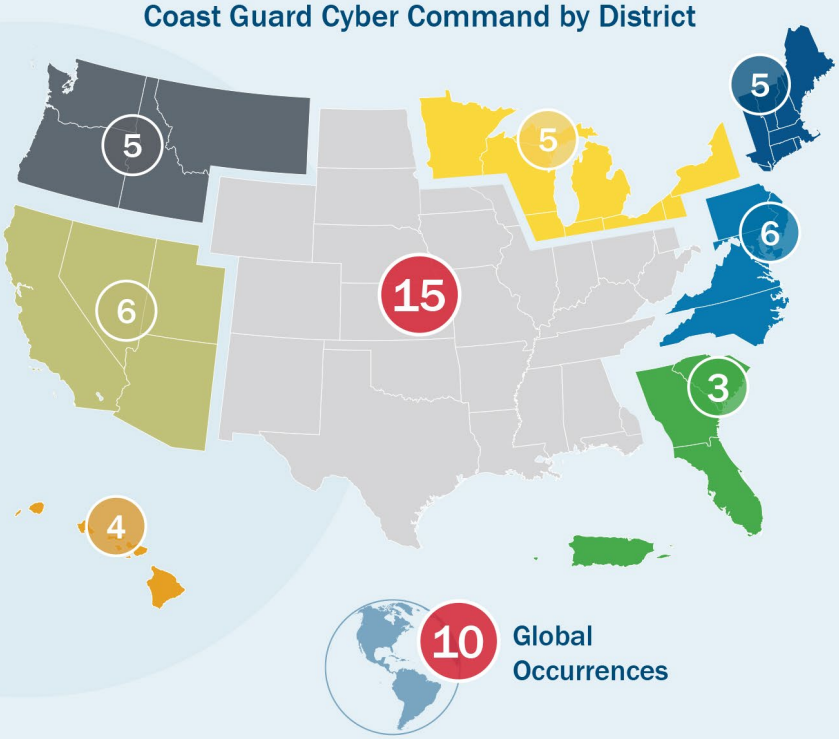
50%
of CPT missions gained initial access through **Phishing for Information**, the preferred method of Cybercriminal and MCAs



59%
success rate when Brute Force Cracking Passwords during 2022 CPT missions

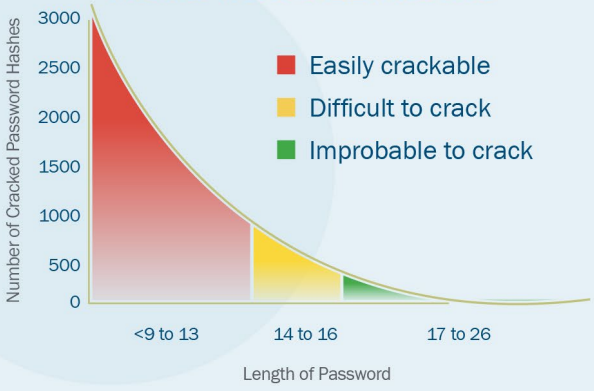
139
known exploitable vulnerabilities identified during 2022 CPT missions

Cyber Occurrences Reported to Coast Guard Cyber Command by District



Global Occurrences

Length of Cracked Password Hashes from CY22 Missions



* (2022). (rep.). Cost of a Data Breach Report 2022. Retrieved 2023, from https://www.ibm.com/downloads/cas/3R8N1DZJ.

UNDERSTANDING THE MARINE ENVIRONMENT

The ME consists of 25,000 miles of coastal and inland waterways, serving 361 ports, 124 shipyards, more than 3,700 maritime facilities, 20,000 bridges, 50,000 Federal aids to navigation, and 95,000 miles of shoreline that interconnect with critical highways, railways, airports, and pipelines, as well as undersea cables carrying 99% of U.S. communications abroad. Approximately $5.4 trillion flows through the ME annually, constituting 25% of the United States gross domestic product; 90% of U.S. imports and exports enter or exit by ship. The ME is one of the most crucial elements of the global supply chain. During the height of the COVID-19 pandemic, shipping bottlenecks at various U.S. ports, most notably Los Angeles/Long Beach, led to significant delays and rising costs. With transit times from China to Los Angeles, including the time waiting for an open berth, nearly doubling, retailers incurred approximately

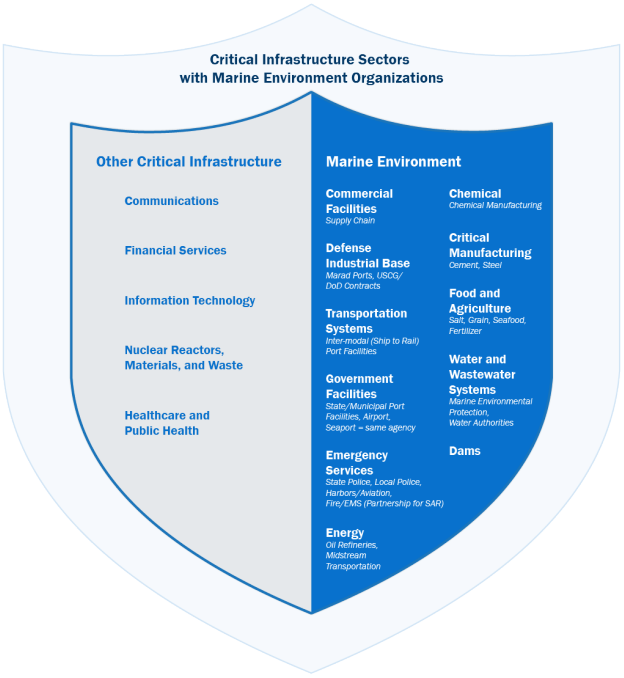
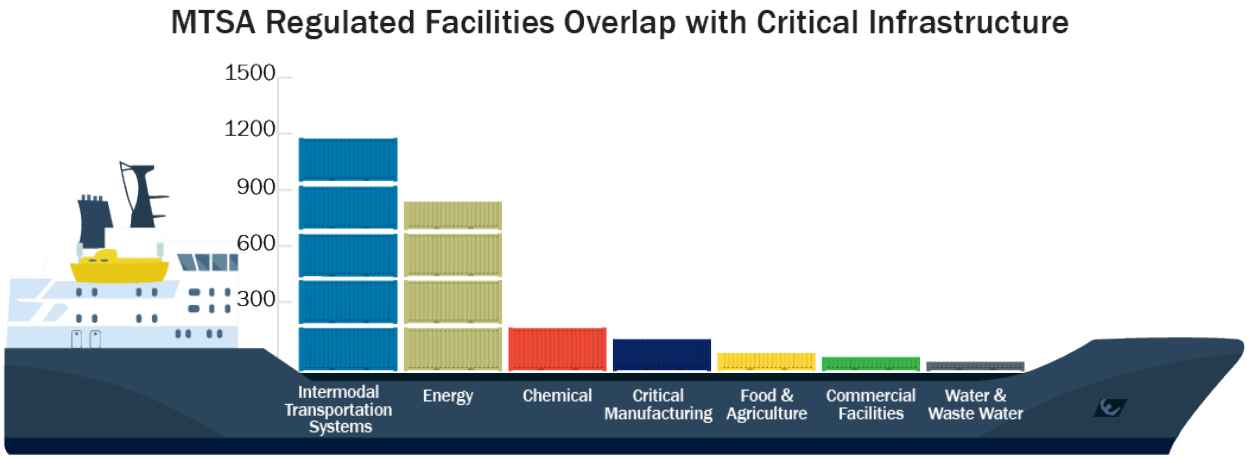


Figure 1: Critical Infrastructure Sectors with ME Organizations

$321 million in added interest due to port congestion.[1] This is in addition to the approximate quintuple increase in costs to ship a container due to the increased demand.[2]

The ME is comprised of more than ships, ports, shipyards, and other related infrastructure. Of the more than 3,700 waterfront facilities, more than half overlap with at least one other Critical Infrastructure Sector. *Figure 2: Overlap Between Maritime Transportation Security Act (MTSA) Regulated Facilities and Critical Infrastructure Sectors* provides a depiction of Coast Guard regulated facilities and what other Critical Infrastructure Sector(s) they represent.

[1] Source: https://maritime-executive.com/article/port-congestion-cost-shippers-millions-in-added-interest-expenses
[2] Source: https://www.bloomberg.com/graphics/2021-congestion-at-americas-busiest-port-strains-global-supply-chain/



Intermodal Transportation Systems	Consists of subsectors including maritime transportation system, aviation, motor carriers, railway, pipeline, and shipping. The transportation system is responsible for safely, efficiently, and securely moving personnel and products across the country and abroad.
Energy	Provides stable energy to the nation in support of the U.S. economy and welfare of citizens. Petroleum and LNG Terminals comprise the 2nd largest category of Coast Guard regulated facilities. Supplies fuel to transportation, electricity to households and industry, and energy sources across the nation.
Chemical	Manufactures, stores, transports, and utilizes dangerous chemicals that are an integral part of driving the missions of other critical sectors through a complex global supply chain. Includes basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products.
Critical Manufacturing	Crucial contributions to the country's economy through industries providing metals, cement, machinery, and equipment. Supports the industrial development of the country, and recovering from disasters that may occur and cause damage to infrastructure.
Food and Agriculture	Key producers of fertilizer, salt, grain, sugar, and livestock feed. Majority of sector is under private ownership, and accounts for one-fifth of nation's economy. Missions include food manufacturing, processing, and storage facilities.
Commercial Facilities	Consist of subsectors aimed at providing for the public, such as entertainment, lodging, public assembly, and events. The majority of these facilities are privately owned, with limited regulatory interaction with the Coast Guard.
Water & Waste Water	Ensures the safety of public health through ensuring the implementation of treating wastewater, protecting against contamination, and ensuring the public has access to a water supply. More than 80 percent of the US population's water supply are treated through these systems.

Figure 2: Overlap Between MTSA Regulated Facilities and Critical Infrastructure Sectors

CYBER PROTECTION TEAM MISSIONS

CPTs are the Coast Guard's deployable specialized forces delivering capability to prevent, detect, and respond to cyber threats impacting ME Critical Infrastructure. Coast Guard CPTs deploy in support of Coast Guard Operational Commanders and organizations in the ME across the World. *Figure 3: 2022 Coast Guard CPT Missions (24 total)* shows missions in the ME for 2022.

Many of the insights in this report are informed by data and analysis collected during Coast Guard CPT missions, as well as from incidents reported to the CGCYBER MCRB.

For more information on the structure and capabilities of Coast Guard CPTs and MCRB, see **Appendix A: Coast Guard Cyber Command Overview**.

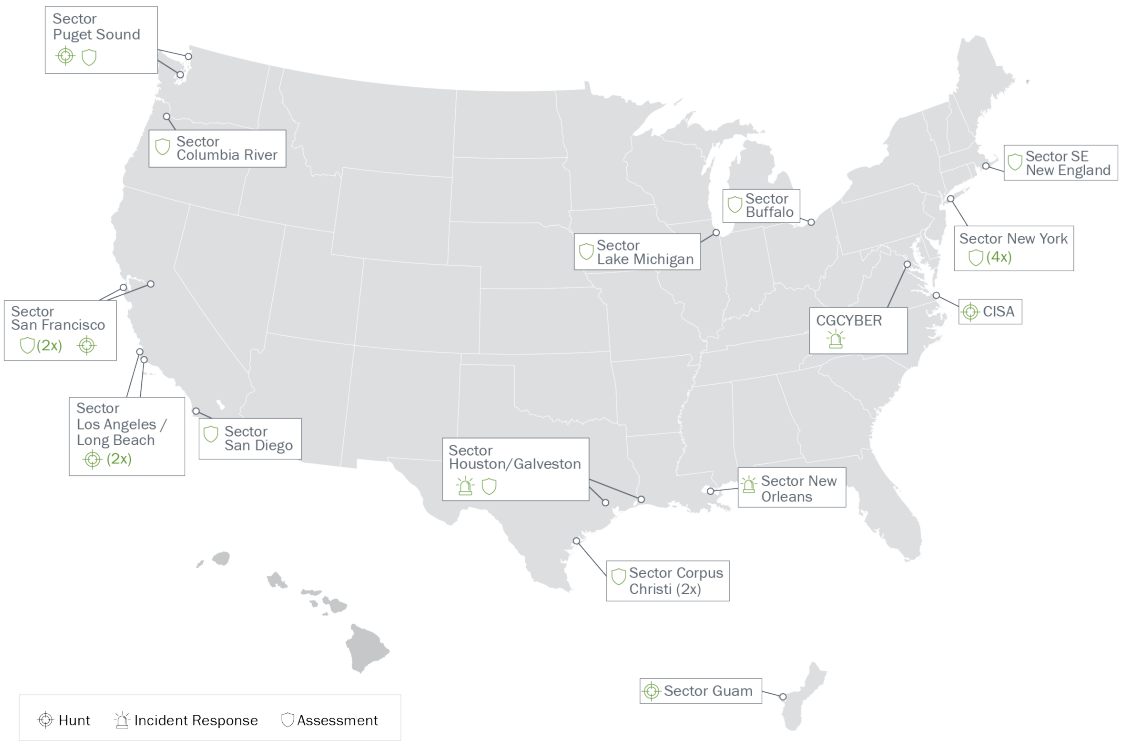


Figure 3: 2022 Coast Guard CPT Missions (24 total)

MARITIME CYBER TRENDS

In 2022, MCRB and local Coast Guard units **investigated 59 cybersecurity reports** including phishing/spoofing, ransomware attacks, and other cyber incidents. This included several large-scale incidents affecting multiple organizations at once. With more than $5.4 trillion and 90% of U.S. imports and exports flowing through the ME annually, nation state actors wishing to harm the U.S. and opportunistic cyber criminal and ransomware gangs, consistently target the ME. *Figure 4: 2022 Cyber Events Reported to Coast Guard Cyber Command* provides a visual of the investigated cybersecurity reports in 2022.

Figure 4: 2022 Cyber Events Reported to Coast Guard Cyber Command

Spear-phishing campaigns continue to proliferate across the ME. Malicious cyber actors (MCA) use techniques ranging from typo-squatted domains to account/business email compromises. These campaigns are often able to deliver malware, resulting in MCAs extorting entities within the ME for financial gain. CGCYBER's observations are bolstered by public reporting of similar campaigns targeting[3] and impersonating[4] major shipping entities. Ransomware remains a popular end game for

[3] Source: https://splash247.com/hapag-lloyd-flags-spear-phishing-attack/
[4] Source: https://www.bleepingcomputer.com/news/security/phishing-impersonates-shipping-giant-maersk-to-push-strrat-malware/

criminal gangs targeting maritime entities around the globe; the Lockbit ransomware attack against the Port of Lisbon is a prime example.[5]

Furthermore, in 2022, criminals were observed targeting back-up systems to make recovery more difficult and to increase pressure on the executive decision makers to pay the ransoms. In addition to financial extortion, these incidents often result in months of reduced operational capacity and potential reputational impacts.

> "Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, we are layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience."
>
> National Cybersecurity Strategy March 2023

Maritime shipping companies continue to be the target of all types of cyber criminals, but in 2022, CGCYBER also observed a significant increase in malicious cyber actors targeting liquified natural gas processors/distributors and petrochemical companies. These efforts included increased reconnaissance, scanning, sophisticated spear-phishing campaigns, and ransomware. The ALPHV ransomware attack against a maritime-based oil company[6] provides an example of the operation-crippling malware that MCAs employ. In this example, 13 facilities were unable to transfer onload or offload fuel causing economic disruption. Additionally, CGCYBER observed several significant cyber-attacks targeting maritime logistics integrators and technology service providers. These include the ransomware attack that shutdown operations for logistics company,[7] and a separate attack impacting more than 1,000 customers of a maritime technology provider.[8] These types of attacks are particularly concerning due to the extent of the second order impacts in the ME. Because they are integral elements of the supply chain, many other maritime organizations were affected concurrently.

Timely information sharing amongst other government agencies (OGAs), CGCYBER, and ME organizations continued to be key to identifying and disrupting MCA operations. For example, CGCYBER notified a facility of a Known Exploitable Vulnerabilities (KEV) on their network exposed to the public Internet. The subsequent Coast Guard CPT engagement with this organization resulted in the detection and removal of an MCA from the partner's network (reference Joint Alert AA22-174A listed in **Appendix C: Maritime Cyber Alerts**). Furthermore, timely information sharing with Cybersecurity and Infrastructure Security Agency (CISA), led to the detection of additional compromises by the same MCA within U.S. Critical Infrastructure.

As the Coast Guard continues to combat wrongful actions by MCAs, CGCYBER relies on cyber incident reports to the National Response Center (NRC) to activate response capabilities and increase awareness across the ME. The Coast Guard urges organizations in the ME to report all cyber incidents to the NRC. Through free-flowing multi-directional information sharing in the ME, the Coast Guard and ME organizations can best address these evolving cyber threats.

[5] Source: https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data
[6] Source: https://www.bleepingcomputer.com/news/security/german-petrol-supply-firm-oiltanking-paralyzed-by-cyber-attack
[7] Source: https://www.freightwaves.com/news/global-logistics-giant-expeditors-suffers-cyberattack-shuts-down-operations-systems
[8] Source: https://splash247.com/voyager-worldwide-hit-by-cyber-attack

ATTACK PATHS

While conducting Assess missions, Coast Guard CPTs emulate threats and employ known attack techniques to assess the organization's risk posture and reveal business impacts to support the hardening recommendations provided at the end of the mission. Most attack paths used during threat emulation consist of three to five steps that closely align with specific Tactics, Techniques, and Procedures (TTP) from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework (MITRE ATT&CK®). **Appendix E: Summary of Attack Paths** includes a full list of attack paths.

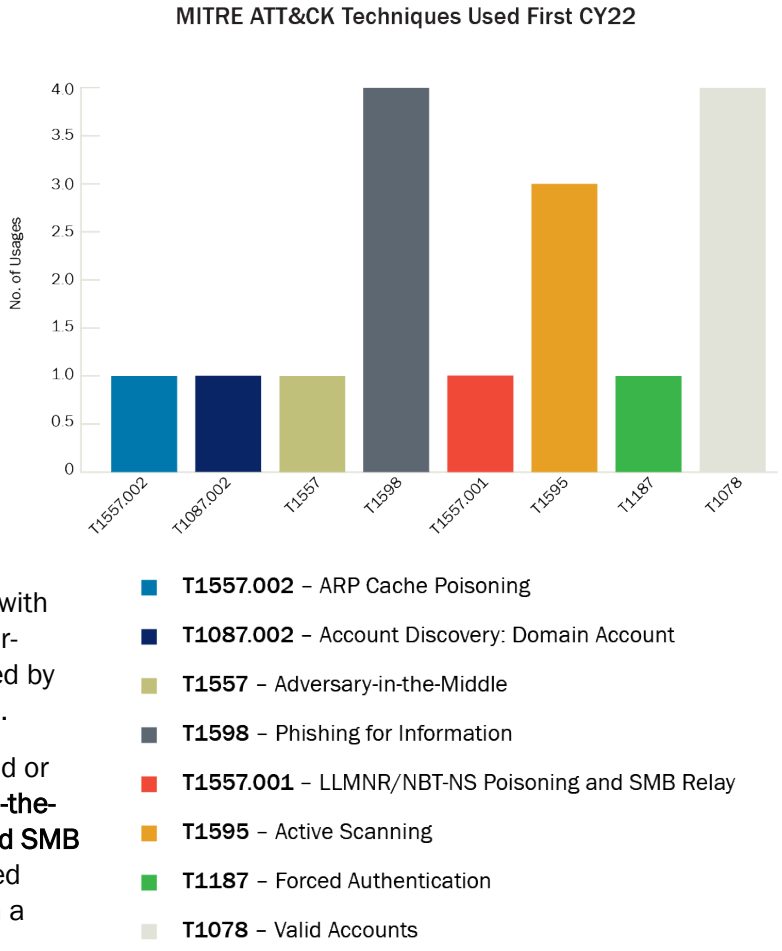


Figure 5: MITRE ATT&CK® Techniques Used First CY22

Phishing for Information (T1598) and **Valid Accounts (T1078)** were the most common initial access techniques used by CPTs during 2022 missions. This approach aligns with industry trends, which state that spear-phishing is the most common TTP used by MCAs against organizations in the ME.

Similarly, once the teams either gained or were given initial access, **Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)** were the most used techniques to gain access from within a network.

Nine of the thirteen CPT standard attack paths relied on the **Brute Force: Password Cracking** technique to gain the account credentials for privilege escalation or lateral movement. The password hashes used for **Brute Force: Password Cracking** were attained using **Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay**, **Steal or Forge Kerberos Tickets: Kerberoasting**, and several **Credential Dumping** sub-techniques including **Security Account Manager**, **NTDS.DIT**, and **/etc/passwd and /etc/shadow.**

Example Assess Mission Storyboard

Critical Vulnerabilities
- Easily crackable passwords
- PII disclosure

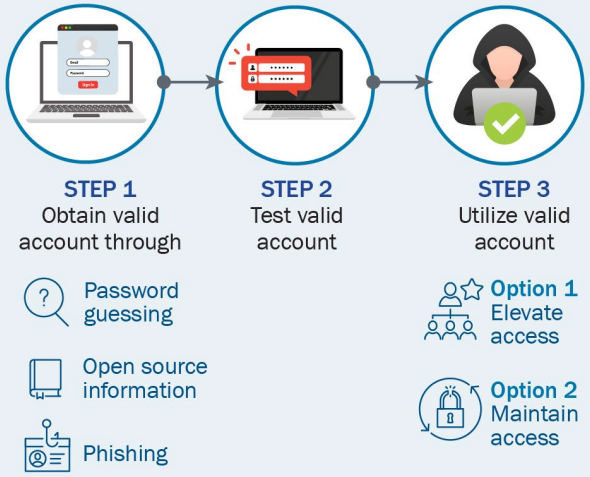
High Vulnerabilities
- Elevated service account privileges
- Admin password reuse

Medium Vulnerabilities
- Insecure default configuration

Phase 1: Spearphishing Link

Phase 2: Phishing for Information

Phase 3: Valid Accounts



Day 1
External network mapping / phishing set-up

Day 2
External vulnerability scanning / phishing testing

Day 3
External web application testing

Day 4
External network penetration testing

Day 5
Travel to location

Day 6
Internal network mapping

Day 7
Insider threat scenario / internal vulnerability scanning

Day 8
Internal penetration testing / lateral movement

Day 9
Wireless assessment

Day 10
Technical exchange / out-brief

FINDINGS

As shown below in *Table 1: Mitigation Status – CY21 & CY22 Comparison*, Marine Transportation System (MTS) partners Fully or Partially Mitigated 93% of all findings within six-months of receiving a CPT Assess mission, an 11% increase from 2021. Other than a slight decrease in Partially Mitigated findings, which is believed to be a result of the increase in Fully Mitigated, all remediation efforts improved from 2021 to 2022. These metrics validate the conclusion that organizations in the ME can take quick and effective action to reduce their attack surface, particularly if they understand the business impacts associated with the risks.

All Findings	CY21	CY22[9]
Fully Mitigated	48%	62% ↑
Partially Mitigated	33%	31% ↓
Accepted Risk	5%	0% ↓
False Positive	2%	0% ↓
No Action Taken to Date	12%	8% ↓

Table 1: Mitigation Status - CY21 & CY22 Comparison

The table shown in **Appendix F: Summarized Findings of 2022 CPT Assess Missions** categorizes our results into Publicly Exploitable and Internally Exploitable findings.

Phishing for Information

Phishing for Information is a sub-technique of the Phishing Technique. **Phishing for Information** is categorized as a reconnaissance technique by the MITRE Corporation rather than an initial access technique. Instead of attempting to use the email for malicious code execution, **Phishing for Information** is used to gain useful information, such as a username and password, from the phished user. During Coast Guard CPT missions, 9.3% of all phishing emails sent during threat emulation resulted in a click by a user. Additionally, of those users who clicked the link, 76.4% of users provided credentials when requested. Due to the unpredictability of a specific user acting after receiving a phishing email, this technique may be more successful for non-targeted phishing campaign compared to a spear-phishing campaign targeting specific users.

According to IBM Security's "Cost of a Data Breach Report 2022," compromised credentials were the most common cause for data breaches. On average, when MCAs employed **Phishing for Information**, it took organizations an average of 327 days to detect (longest time to identify compared to other vectors) and had the average highest cost per data breach at $4.83 million, not including amounts paid for ransom.[10] This data reinforces the severity of the most common finding detected by Coast Guard CPTs.

Related Mitigations:

- Common Mitigation #6: User Training
- Software Configuration (configure Sender Policy Framework (SPF)/DomainKeys Identified Mail (DKIM)/Domain-based Message Authentication Reporting and Conformance (DKIM) for mail server)

[9] Based on data for first half of CY22
[10] Source: https://www.ibm.com/downloads/cas/3R8N1DZJ

Valid Accounts

The most common initial access technique used during Assess missions was **Valid Accounts**. **Valid Accounts** were often gathered from publicly available sources or from using related techniques such as **Phishing for Information, Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay,** or **Steal or Forge Kerberos Tickets: Kerberoasting**. Coast Guard CPTs gained initial access to the target networks using gathered account information.

Related Mitigations:

- Common Mitigation #1: Password Policies
- Common Mitigation #4: Privileged Account Management
- Common Mitigation #6: User Training
- Common Mitigation #7: User Account Management
- Application Developer Guidance

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

LLMNR/NBT-NS Poisoning and SMB Relay attacks leverage antiquated features used for host identification to harvest credentials from within a network. LLMNR/NBT-NS Poisoning consists of an attacker inside the network responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) and directing traffic to an adversary-controlled system. Then, once the requestor attempts to access the adversary-controlled system, the adversary can use a myriad of techniques to directly obtain hashed or even sometimes plaintext credentials. If the adversary captures a password hash, they can pivot to the **Brute Force: Password Cracking** technique to determine the plaintext credentials.

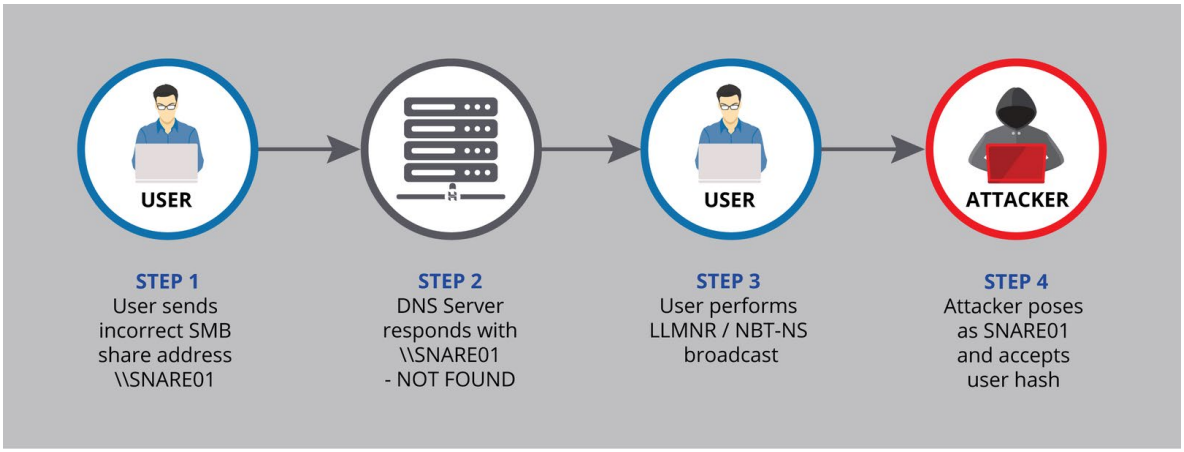


Figure 6: Adversary in the Middle-LLMNR/NBT-NS Poisoning and SMB Relay

Related Mitigations:

- Common Mitigation #3: Filter Network Traffic
- Network Segmentation
- Network Intrusion Prevention
- Disable or Remove Feature or Program

Brute Force: Password Cracking

A weak password policy can result in an attacker gaining unauthorized access to a system or application. According to the National Institute of Standards and Technology (NIST) Special Publication 800-63 Digital Identity Guidelines, a strong password policy includes password length and password complexity. It also contains suggestions for enforcement and consequences when not followed (lost system access). A good password policy can protect an organization from brute force password cracking, guessing, and reuse. *Figure 7: Length of Cracked Password Hashes from CY22 Missions* illustrates the number of successfully cracked hashes across the length of the password from CPT missions. As can be seen, the longer the password, the more difficult the hash is to crack.

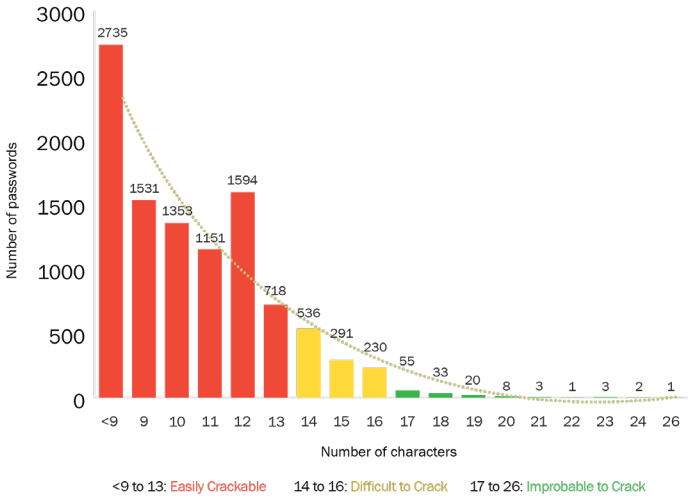


Figure 7: Length of Successfully Cracked Password Hashes from CY22 Missions

For over 17,000 discovered password hashes, CPTs were able to crack hashes for 60.1% of all passwords using hybrid dictionary and ruleset-based password cracking. The median password length of all cracked passwords was ten characters. CPTs were unable to determine the length of any password that was unsuccessfully cracked. CPTs were able to pre-calculate and successfully crack the hashes for all passwords less than eight characters in length.

Of the cracked passwords, 97.1% of passwords had at least three complexity requirements (uppercase letter, lowercase letter, number, symbol) showing that most users implement these requirements into their passwords in predicable ways without increasing the overall difficulty to crack the password. Our Assess missions validate NIST's recommendation that **password length is the primary factor in characterizing password strength.**[11] Our ruleset-based password cracking was able to detect most complexity techniques used in user-created passwords. Only 198 recovered passwords were seven characters or less. This is attributed to compliance with NIST's minimum password recommendation of eight characters or more. However, in comparison to the NIST standard, the U.S. Department of Defense (DOD) requires a minimum fifteen-character password length for all accounts when the user or application cannot support multi-factor authentication.

Related Mitigations:

- Common Mitigation #1: Password Policies
- Common Mitigation #2: Multi-Factor Authentication

[11] Source: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

Steal or Forge Kerberos Tickets: Kerberoasting

Applications often require user accounts to operate, known as Service Accounts. Service Accounts use elevated privileges to perform a business function. MCAs leverage techniques such as "AS-REP Roasting" (related to Authentication Server Requests) and **Kerberoasting** to abuse legitimate functionality and attain a copy of the Service Account's password hash. If the service account has a weak password, the MCA can crack this password using the **Brute Force: Password Cracking** technique and access systems using the Service Account credentials. *Figure 8: Kerberoasting* illustrates the basic process flow of a **Kerberoasting** attack.

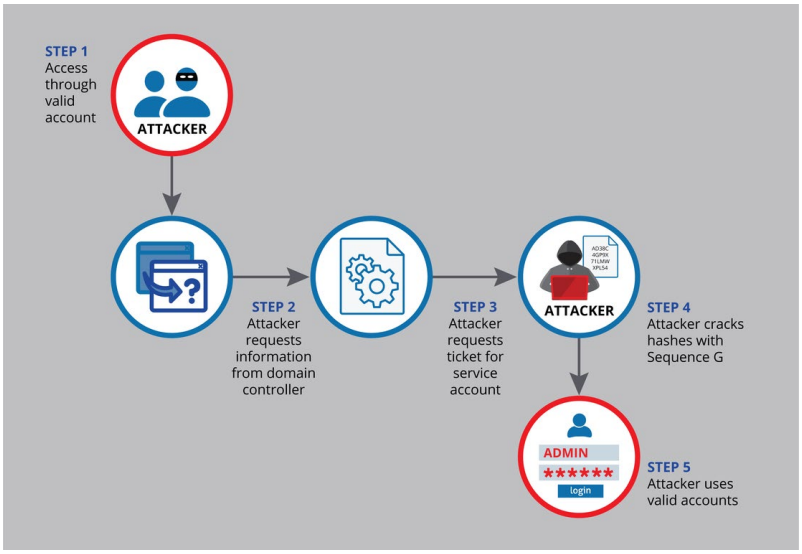


Figure 8: Kerberoasting

For simplicity, administrators often use existing administrator accounts as Service Accounts or create a new account and add the new Service Account to an existing administrator group, such as Domain Administrators. This often allows MCAs to leverage these unnecessary permissions to gain full control over an enterprise.

Related Mitigations:

- Common Mitigation #1: Password Policies
- Common Mitigation #4: Privileged Account Management
- Encrypt Sensitive Information (Enable AES Kerberos encryption)

Patch Management

Vendors release patches and updates to address existing and emerging security threats and address multiple levels of criticality. Failure to apply the latest patches can leave the system open to attack from publicly available exploits. The risk presented by missing patches and updates can vary; however, the most critical of vulnerabilities are those that are proven exploitable. These vulnerabilities are listed in CISA's KEV Catalog.[12]

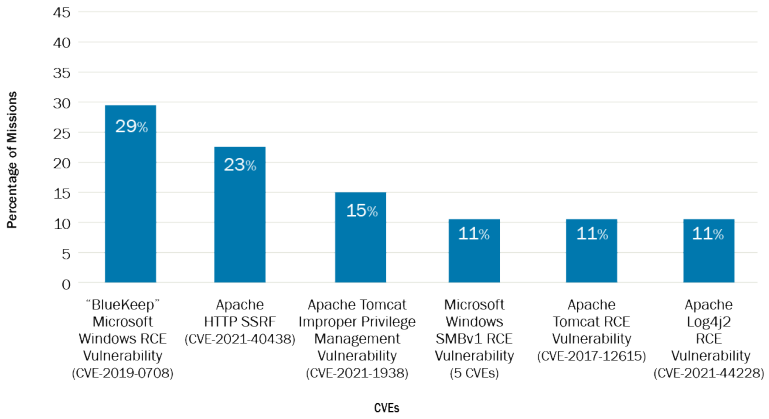


Figure 9: Top KEV Detected During CY22 Assess Missions

Figure 9: Top KEV Detected During CY22 Assess Missions represents the vulnerabilities from the KEV Catalog detected during CPT Assess missions.

In addition to the presence of KEVs in these networks, CPTs regularly observed a lack of network filtering (see **Common Mitigation #3: Filter Network Traffic**) or network segmentation. These security architecture concerns show that if an adversary could exploit a vulnerability at one of these sub-organizations, they could easily pivot into and throughout the internal environment of the organization. **Appendix G: Known Exploitable Vulnerabilities Detected on CPT Missions** contains descriptions of these vulnerabilities.

Related Mitigations:

- Common Mitigation #4: Privileged Account Management
- Common Mitigation #5: Update Software
- Application Isolation and Sandboxing
- Disable or Remove Feature or Program
- Execution Prevention
- Exploit Protection
- Network Segmentation
- Threat Intelligence Program
- Vulnerability Scanning

[12] Source: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

MITIGATIONS

In addition to the common findings, the attack paths from each mission are documented in **Appendix E: Summary of Attack Paths** to show the specific attack path steps tied to the appropriate corresponding MITRE ATT&CK® technique. These attack paths demonstrate steps taken to gain initial access, move through a network, and deliver cyber effects. Coast Guard CPTs apply real-world techniques to demonstrate how vulnerabilities can be chained together to deliver a debilitating effect, as well as to highlight the business impact that an MCA could cause.

CGCYBER tabulated a complete list of all reported common findings and common attack path steps to drive recommended mitigation actions. For Common Findings, the CPTs mapped each finding directly to one or more MITRE ATT&CK® mitigation recommendations. In the attack paths, each step maps to a MITRE ATT&CK® technique and one or more MITRE ATT&CK® mitigation recommendations. "Mapped Findings" represents all mitigations associated with the CPTs' findings, while "Mapped Techniques" represents mitigations directly associated with CPT threat emulation that could be replicated by an MCA to gain further access within the organization's environment. CGCYBER determined 16 successful attack paths from threat emulation or detection during a Hunt mission. **Appendix F: Summarized Findings of 2022 CPT Assess Missions** contains detailed Attack Path data, *Table 2: Common Mitigation Recommendations* summarizes this data. **Appendix H: Common Mitigations** contains greater detail on each mitigation recommendation to organizations normally included in CPT Mission Reports. *Figure 10: Common Mitigations User Resistance & Costs* provides a snapshot of typical levels of user resistance, upfront costs, and reoccurring costs to common mitigations.

Mitigation Recommendation	Mapped Findings		Mapped Techniques	
	CY21	CY22	CY21	CY22
Password Policies	44 (1st)	73 (1st)	35 (1st)	62 (1st)
Multi-Factor Authentication	22 (4th)	43 (2nd) ↑	18 (3rd)	28 (5th) ↓
Filter Network Traffic	New	39 (3rd) ↑	New	Not Observed
Privileged Account Management	31 (2nd)	32 (4th) ↓	23 (2nd)	46 (2nd)
Update Software	19 (6th)	26 (5th) ↑	4	Not Observed ↓
User Training	15 (7th)	25 (6th) ↑	15 (4th)	44 (3rd) ↑
User Account Management	New	24 (7th) ↑	New	35 (4th) ↑
Account Use Policies	New	24 (8th) ↑	New	N/A

Table 2: Common Mitigation Recommendations

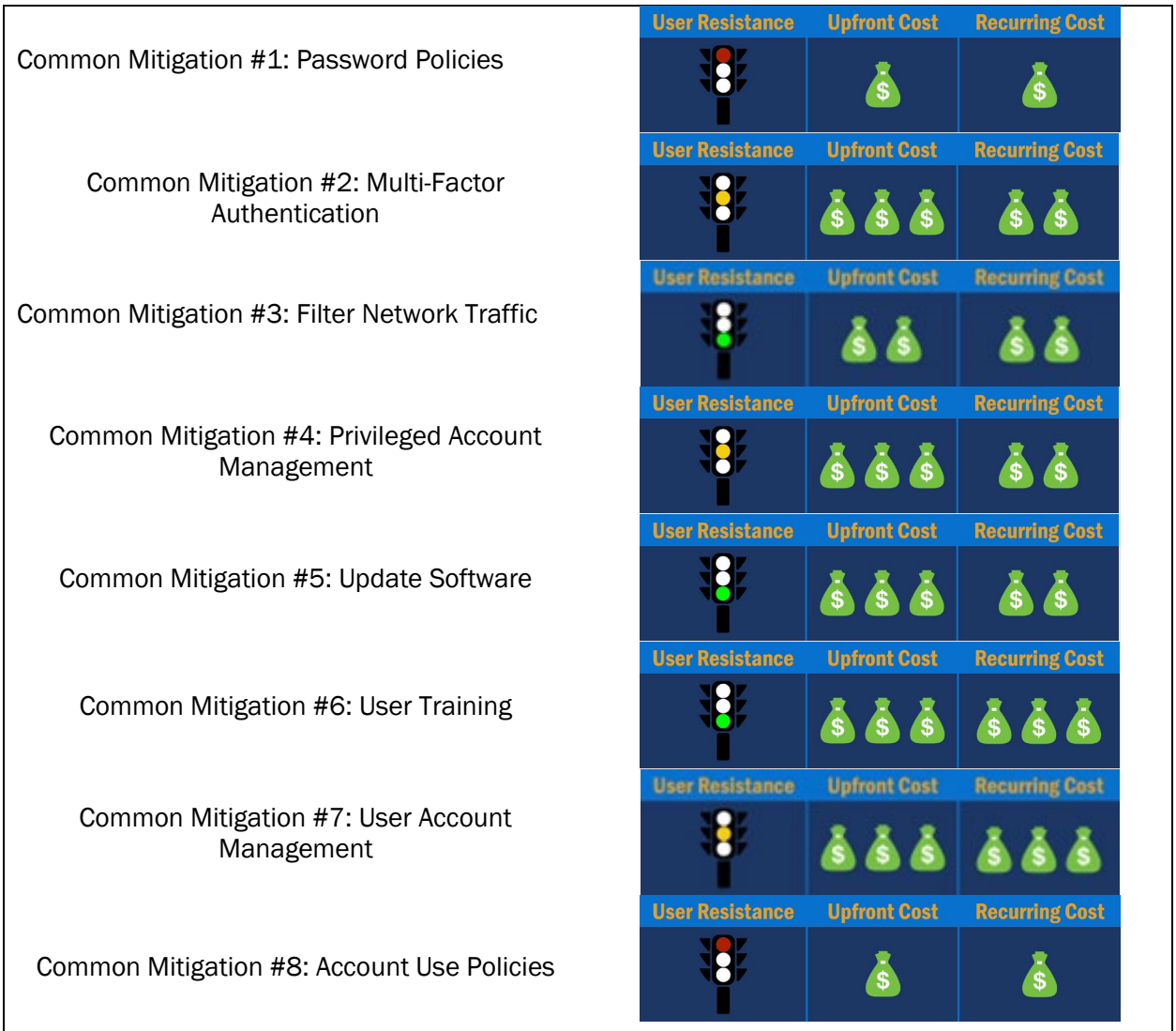


Figure 10: Common Mitigations User Resistance & Costs

RECOMMENDED FURTHER ACTIONS

Enabling Hardening and Assessing Risk Posture

Coast Guard CPT Assessment

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

CISA's Cyber Hygiene Service

CISA offers vulnerability scanning services to help organizations reduce their exposure to cyber threats by taking a proactive approach to mitigating attack vectors.[13] Additionally, CISA recommends organizations further protect themselves by identifying assets that are searchable via online tools and taking steps to reduce that exposure.[14]

Port Security Grant Program

The Port Security Grant Program (PSGP) is one of four grant programs the DHS and Federal Emergency Management Agency (FEMA) leverage to focus their transportation infrastructure security activities. These grant programs are part of a comprehensive set of measures authorized and appropriated by Congress and awarded by the Executive Branch to help strengthen the nation's critical infrastructure. Enhancing cybersecurity was identified as a priority area for Fiscal Year (FY) 2022 within the public "DHS Notice of Funding Opportunity (NOFO) Fiscal Year 2022 PSGP" published on https://www.fema.gov/. The PSGP provides funds to state, local, and private sector maritime partners to support increased port-wide risk management and to protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. The PSGP is subject to the annual appropriations process and awards project funding on a competitive basis across multiple priority areas, including cybersecurity.

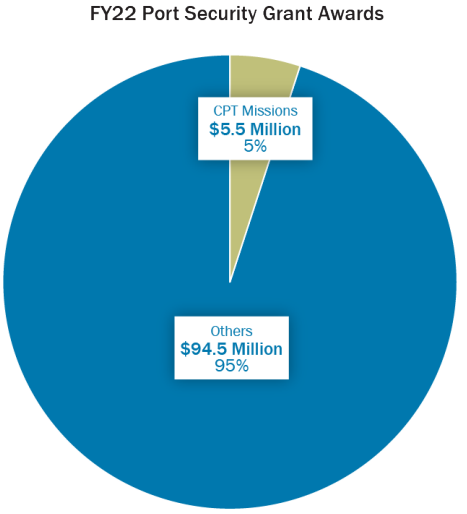


Figure 11: FY22 Port Security Grants Awards

Figure 11: FY22 Port Security Grants Awards show that in FY 2022, the PSPG granted $5.5 million to 17 organizations where Coast Guard CPTs conducted missions. This was a 77% increase from FY 2021. CGCYBER encourages MTS entities to apply for the grant program as a potential source of funding to improve cybersecurity across the MTS.[15]

[13] Source: https://www.cisa.gov/cyber-hygiene-services
[14] Source: https://www.cisa.gov/publication/stuff-off-search
[15] Source: https://www.fema.gov/grants/preparedness/about

State and Local Cybersecurity Grant Program (SLCGP)

On September 16, 2022, DHS announced a cybersecurity specific grant program offering $185 million of potential funding for MTS organizations owned or operated on behalf of state, local and territorial (SLT) governments. The State and Local Cybersecurity Grant Program (SLCGP) is intended to help eligible organizations address cybersecurity risks and threats to information systems. This offers another potential source of funding to improve cybersecurity within the MTS.[16]

Responding to Cyber Incidents in the Marine Environment

National Response Center

The Coast Guard recommends that MTSA-regulated facilities and vessel owners/operators list the NRC's 24-hour hotline, **1-800-424-8802**, in their facility/vessel security plans for reporting maritime security and cybersecurity incidents to the Coast Guard. The NRC recommends all reports be made via this telephone hotline to record all pertinent information. Please be advised that the NRC no longer provides an email address on its website for reporting incidents. Additional reporting guidance is provided within Coast Guard Policy Letter 08-16, "Reporting Suspicious Activities and Breaches of Security."[17] The policy letter outlines the requirements for MTSA-regulated vessels and facilities to report security incidents, in accordance with the Maritime Transportation Security Act of 2002.

Coast Guard CPT Incident Response

The NRC or local Coast Guard Sector can engage CGCYBER for additional support. Coast Guard CPTs maintain a team ready to deploy anywhere in the world on short notice provided the MTSA-regulated facility completes a Request for Technical Assistance legal agreement with the CGCYBER. *Figure 12: Coast Guard CPT Incident Response Process* depicts the sequence of events and reporting chain for reported cyber incidents involving MTS entities.

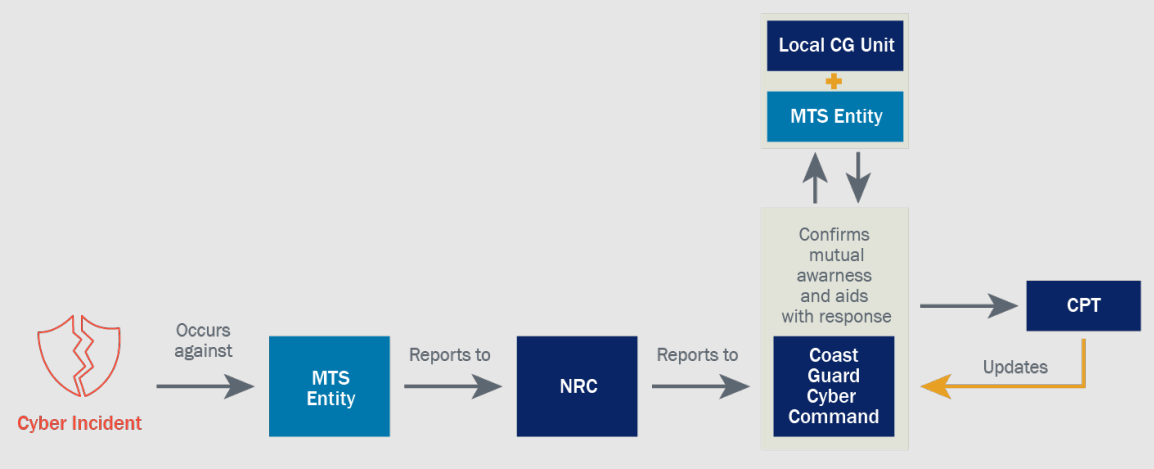


Figure 12: Coast Guard CPT Incident Response Process

[16] Source: https://www.cisa.gov/cybergrants
[17] Source: https://www.dco.uscg.mil/Portals/10/Cyber/Cyber-Readiness/CG-5P%20Policy%20Letter%2008-16%20-%20Reporting%20Suspicious%20Activity%20and%20BoS.pdf?ver=2020-05-26-173911-100&timestamp=1590758815625

LOOK AHEAD TO 2023/2024

With the rise of technology, development and trends will continue to advance and expand the ME's cyber-attack surface. However, implementation and adaptation of emerging technologies is vital for organizations within the ME to remain up to date. To efficiently improve the cyber risk posture of the marine environment, the Coast Guard, ME partners, and other government stakeholders should work collectively to deter and respond to adversarial threats in cyberspace.

> "Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides."
>
> National Cybersecurity Strategy March 2023

Impact of Cloud on the Marine Environment

Through our engagements with organizations in the ME, the Coast Guard has noticed a significant trend in the transition to cloud-based email and office productivity services. As shown in *Figure 13: Cloud Based Email Providers Used in the ME*, Coast Guard CPTs observed 85% of organizations using "cloud-based" or externally hosted email solutions. This transition provides many benefits for organizations, and it transfers some responsibility from the organization to the software-as-a-service provider. Organizations can now worry less about cyber activities such as Patch Management and instead focus on business operations.

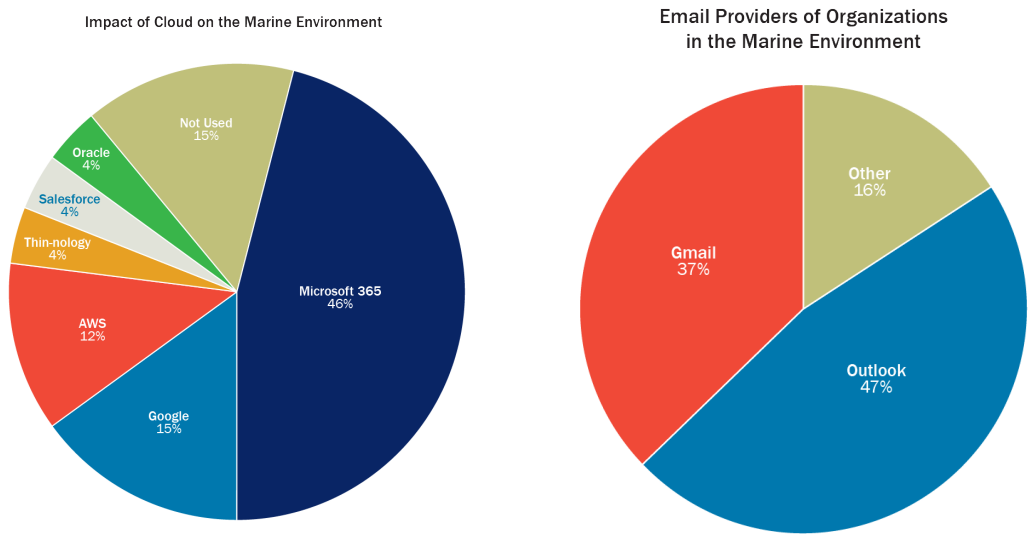


Figure 13: Cloud Based Email Providers Used in the ME

However, the transition to cloud services creates a new attack surface, and when improperly implemented, the new solution can create significant risks to the organization. Cloud-based email services can expose an organization's email login to the public Internet. Password spraying and credential harvesting attacks are common tactics used by MCAs to gain access to Valid Accounts. When federated with on-premises directory services or virtual private network (VPN) authentication, cloud email services may be targeted to gain credentials for further access into an organization's on-premises environment. In other words, an improperly configured cloud-based email solution could offer an MCA a new vector into an organization's internal network. Business email compromise (BEC) can also be used directly for financial crimes, data theft, and high-impact, low-complexity disruptions to organizations.

If organizations are transitioning to cloud-based services, it is important to consult vendor documentation for security best practices. Organizations should **enable MFA for all cloud accounts** as soon as possible. Below resources provide recommendations for securing the most frequently seen cloud service, Microsoft 365/Azure:

1. CISA Alert AA20-120A: Microsoft Office 365 Security Recommendations, https://www.cisa.gov/uscert/ncas/alerts/aa20-120a
2. Microsoft Secure Score (an automate d self-assessment for M365 and Azure Services), https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide
3. Microsoft 365 and Azure Active Directory Fundamentals, "Quick Security Wins" section, https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/
4. Security Defaults in Azure AD, https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
5. Secure your business data with Microsoft 365, https://learn.microsoft.com/en-us/microsoft-365/business-premium/secure-your-business-data?view=o365-worldwide

Advances in Technology and Emerging Threats

The Internet of Things (IoT) and advancements in cloud technology connects ports and ships through sensors and remote monitoring devices. These advances allow for improved communication, monitoring, and data collection. However, they also increase the number of endpoints open to exploitation and expand the attack surface targeted by adversaries. Although these connections allow for better collaboration within the industry, they also create more terrain that cybersecurity professionals must defend. The future of connectivity must coincide with equal investments in improved network defenses if organizations want to safely enjoy the efficiencies gained by this new technology.

Automation and artificial intelligence (AI) advances in port operations leverage massive amounts of data across an enterprise to streamline the processes for operational technology (OT). These advances also depend on increased integration between OT and Information Technology (IT) networks. This interdependency creates new vulnerabilities for OT network defenders by increasing the opportunities for adversaries to access these sensitive systems starting from the Internet. Industry partners will need to implement safety controls, network segmentation, and various other defenses to mitigate these vulnerabilities.

The centralization of software and use of managed service providers for handling port and shipping operations provides company executives with unprecedented oversight across their enterprise and new insights into their operations, giving them access to data necessary to make decisions. However, these centralized service providers can be targets of malicious actors wishing to impact thousands of companies at once, evidenced by the SolarWinds compromise of 2020.[18] Industry specific software providers, such as ship management software, may also be targeted to impact a huge portion of the MTS at once. Each organization must recognize the risks of using third-party vendors, understand their dependencies on various technologies, and have contingencies in place to maintain operations in the event of an MCA attack on the third-party vendor.

As the MTS' dependence on technology continues to grow, so too will the cyber threats. Securing our nation's critical infrastructure depends on more collaboration between government and industry to face these threats head-on. CGCYBER will continue to expand outreach and information sharing, develop our own capabilities, and provide support to critical infrastructure in the identification and mitigation of cyber risks.

> "Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruption. Our factories, power grids, and water treatment facilities, among other essential infrastructure, are increasingly shedding old analog control systems and rapidly bringing online digital operational technology (OT)."
>
> National Cybersecurity Strategy March 2023

[18] Source: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

APPENDIX A: COAST GUARD CYBER COMMAND OVERVIEW

Coast Guard Cyber Command

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

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

To meet Line of Effort 2, "Protect the MTS," CGCYBER formed and established CPTs and the MCRB.

Cyber Protection Teams

CPTs are 39-person teams structured as a deployable special force. CPTs can deploy to augment Coast Guard Commanders in the execution of time-critical or nationally significant prevention and response cyber activities.

The Coast Guard currently has four CPTs with one to three deployable elements each (as some teams are not fully operational yet):

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

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

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

A standard CPT operation involves close coordination with the supported Operational Commander with a duration of two to eight weeks depending on the specific circumstances. Coast Guard CPTs completed more than 52 cyber operations since December 2020. The pace of CPT operations continues to increase as the Coast Guard expands its cyber capabilities.

Maritime Cyber Readiness Branch

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

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

APPENDIX B: OPERATIONAL TECHNOLOGY IN PORTS

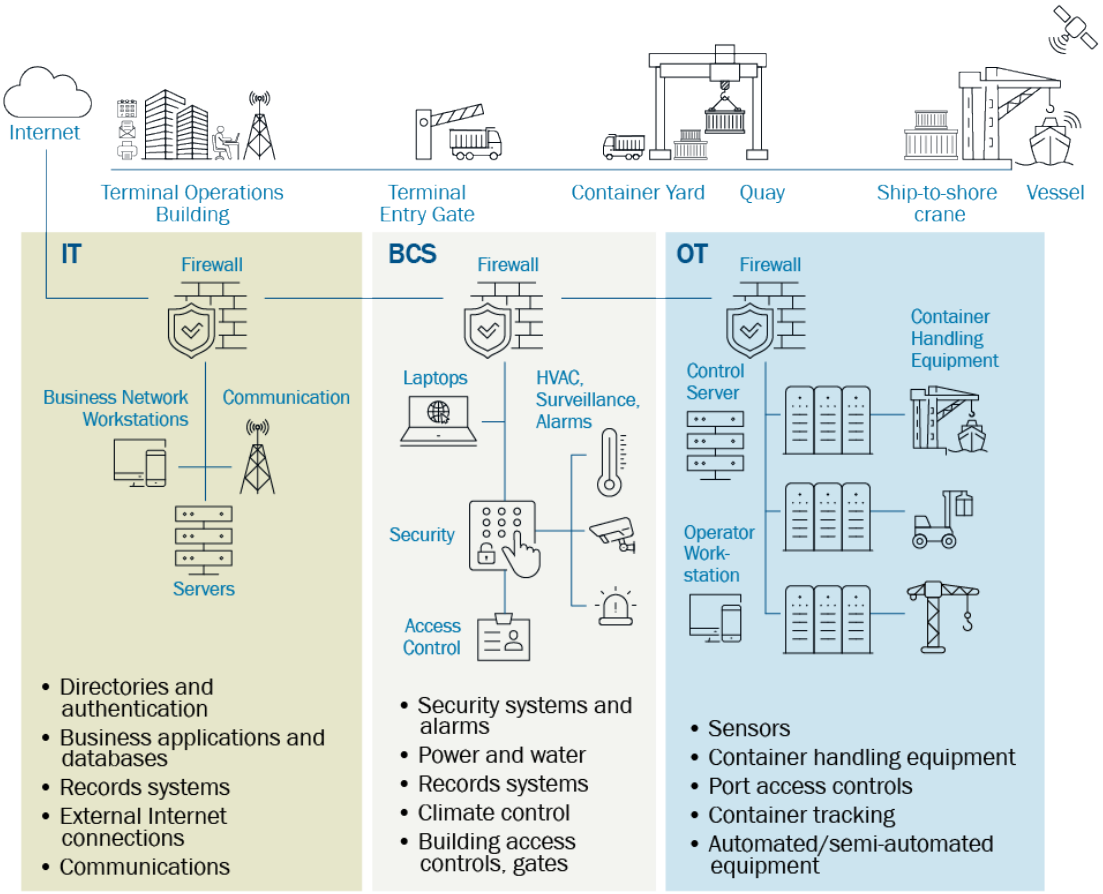


Figure 14: Operational Technology in Ports

As described in the Maritime Cyber Assessment and Annex Guide, IT and OT systems are very different. Each system has a unique purpose and relies on different technologies and protocols. Understanding what systems exist in an MTS facility, associated vulnerabilities for each system, and the consequences of a failure, will help organizations coordinate efforts for planning and protecting against cyberattacks.

- **IT** controls the flow of information across an organization. The purpose is to support connections between networks, and manage computers, data, and employee communication in a secure way. System security and integrity are top priorities, with system availability secondary.

- **OT** controls industrial applications and interactions with the physical environment and is tied directly to business operations. Availability/uptime are the top priority for OT systems because a disruption will immediately impact business operations and possibly revenue.

- **Building Control Systems (BCS)** are a **subset** of OT, which include energy-management systems, physical-security access-control mechanisms such as Transportation Worker

Identification Credentials (TWIC) readers, and fire-alarm systems. These systems are directly responsible for safety and security of personnel at a facility and should be separated from other OT systems when laying out the network architecture.

A recommended best-practice is to implement strict network segmentation among IT, OT, and BCS systems. The most secure method is to implement physical, air-gapped separation where no traffic can route between networks. However, due to business requirements, this is not always feasible. In physically air-gapped networks, it is still important to implement boundary protections for Internet-connected services as well as cybersecurity monitoring controls across the different networks.

If physically air-gapping networks is not operationally feasible, the networks should be logically separated using some form of boundary protection. Extreme care and attention should be used to ensure the boundary protection prevents unauthorized traffic between the networks. Boundary protection systems such as firewalls are critical, as is providing adequate protections for email servers, Internet-facing web, business application servers, email clients, and web browsers on desktop systems.

APPENDIX C: MARITIME CYBER ALERTS

Maritime Cyber Alert 01-22

Spoofed Business Websites

Summary: The Coast Guard has observed a recent uptick in MCAs using spoofed business websites to target the MTS. Multiple MTS partners have discovered well-constructed, fake websites masquerading as their legitimate business websites. These sites are presumably created to steal information from or install malware on customers' devices interacting with the sites. These spoofed websites are not designed to impact the maritime organization directly, but to resemble watering-hole style attacks where the intended targets are individuals and entities visiting the site. The spoofed websites are professional in appearance and quite sophisticated; some even present as .com domains. This level of detail can make it difficult to discern a real site from a fraudulent one.[19]

Maritime Cyber Alert 02-22

Released as TLP-GREEN MCA.

Maritime Cyber Alert 03-22

Threat from Cyber Criminal Group "KILLNET"

Summary: The Coast Guard observed malicious activity linked to a cyber-criminal campaign targeting critical infrastructure in Europe and threatening the United States energy sector's segment in the MTS. These threats were discovered via dark-web posts made by the Russian-based cyber-criminal and hacktivist group known as KILLNET. KILLNET is one of many hacktivist groups whose malicious cyber activity increased in the wake of the Russia's invasion of Ukraine. The group gained notoriety for their Distributed Denial of Service (DDoS) attacks against numerous U.S. Critical Infrastructure and Government websites.[20]

CISA/CGCYBER Joint Alert AA22-174A

Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems

Summary: CISA and CGCYBER released a joint Cybersecurity Advisory (CSA) to warn network defenders that cyber threat actors, including state-sponsored APT actors, continue to exploit CVE-2021-44228 (Log4Shell)[21] in VMware Horizon® and Unified Access Gateway (UAG) servers to obtain initial access to organizations that did not apply available patches or workarounds.[22]

[19] Source: https://www.dco.uscg.mil/Portals/9/Maritime%20Cyber%20Alert%2001-22%20TLP%20WHITE.pdf
[20] Source: https://www.dco.uscg.mil/Portals/9/Maritime%20Cyber%20Alert%2003-22%20KILLNET%20TLP%20WHITE.pdf
[21] Source: https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[22] Source: https://us-cert.cisa.gov/ncas/alerts/aa22-174a

APPENDIX D: OBSERVED CYBER CRIMINAL ORGANIZATIONS

Malicious Actor	Overview
Killnet	Killnet is one of many hacktivist groups whose malicious cyber activity increased in the wake of Russia's invasion of Ukraine. The group gained notoriety for their DDoS attacks against numerous U.S. Critical Infrastructure and Government websites. Killnet has primarily targeted public facing websites, but other targets include logistics and operations support systems and IoT devices. Their claimed attacks continue to focus on DDoS, but it should not be assumed those are their only capabilities.
ALPHV	ALPHV is a highly customizable ransomware that allows for a broad range of targets on Windows™, Linux®, and ESXi™ environments. APLHV operators are active across a broad range of targets. Typically, ransomware operators avoid critical infrastructure entities to limit attention to themselves from the government and law enforcement agencies. ALPHV however, has a history of targeting U.S. oil, gas, and energy companies, and continues to demonstrate interest in targeting critical infrastructure for financial gain. The group claims it is an advertiser for, or affiliate of, multiple ransomware groups, including REvil, Darkside, Egregor, and LockBit. ALPHV is the first ransomware known to be written in the Rust™ programming language. Rust™ can be difficult to detect by network sensors, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). Additionally, Rust™ allows for broader control features, such as additional execution and attack options with better safety levels and higher performance rates. These features improve the operators' chances of a successful intrusion. One notable characteristic of ALPHV operators is their ability to create highly tailored executables for intended targets. This technique contributes to

	ALPHV's reputation of sophisticated attack patterns across different environments. ALPHV also offers special features to increase the likelihood of success, including outsourced solutions for calling victims or their competitors about the leak; botnet(s) for DDoS attacks; access to Graphics Processing Units (GPU) data center(s), dictionaries and rules to instigate a brute force attack; and distributed onion storage that allows the operators to negotiate with victims. Finally, if its victims fail to pay the requested ransom, the exfiltrated data is uploaded to ALPHV's dark web website. Proof of successful data exfiltration is commonly posted to the group's website to convince victims to pay the ransom before all the stolen data is released.
Royal	Royal Ransomware group is believed to be comprised of experienced MCAs from other ransomware groups, indicated by their previous use of different variants like BlackCat and ZEON. They have since rebranded as "Royal" and started using their own encryptors. Royal's operation used various TTPs to gain initial access to networks, including targeted callback phishing attacks and exploiting vulnerabilities in victims' custom web applications. There are two techniques unique to Royal: a way of partial encryption and multithreaded encryption.[23] Typically, ransomwares base partial encryption on the file size, encrypting the same way based on a set percentage. Royal's unique spin enables the user to set a specific percentage and lower the amount of encrypted data even with large files, making it possible to avoid detection even longer. For multithreading, Royal first utilizes an Application Programming Interface (API) call to GetNativeSystemInfo to identify the number of processors. Then they multiply the total by two and create threads, enabling for rapid encryption.
LockBit	LockBit has grown rapidly since emerging in 2019. Through their professional operations and affiliate programs, they have demonstrated staying power.

[23] Source: https://www.darkreading.com/attacks-breaches/royal-ransomware-novel-spin-encryption-tactics

	Using ransomware-as-a-service, constantly developing and adapting it, as well as active recruitment of affiliates to spread their network, has helped them stay ahead of competition. LockBit 3.0 is the latest known version of their ransomware. The first (known) use was in June 2022. It resembles DarkSide or BlackMatter, and appears to actively hide from detection. Some of the recent innovations for the group include a bug bounty program, offering rewards to anyone who can find bugs in their ransomware. Additionally, one of their affiliate programs has offered up to $1 million for researchers who can identify members of their group to minimize anything that puts their operations at risk.
BlackBasta	The BlackBasta group initially appeared in April 2022, and has quickly grown, especially in the final quarter of 2022. It is highly likely that BlackBasta is a rebranded group formed from former members of the infamous Conti group. In a very short time the group has amassed nearly 50 victims in the US, UK, New Zealand, Australia, and Canada. While the group's motivations are mostly monetary, their willingness and desire to target critical infrastructure and MTS/MTS-related facilities makes it necessary to be familiar with their capabilities and to be able to defend against such attacks. BlackBasta utilizes proprietary ransomware software written in C++ that encrypts local files. The attack chain begins with a spearfishing email containing a malicious disk image file that starts the execution of Qakbot. The malware uses basta as the extension for encrypted files. BlackBasta actors have also developed a Linux variant designed to strike VMware ESXi virtual machines (VMs) running on enterprise servers, putting it on par with other groups such as LockBit and Hive. The group utilizes double extortion to plunder sensitive information from the targets and threatens to publish the stolen data unless the victim makes a digital payment.

APPENDIX E: SUMMARY OF ATTACK PATHS

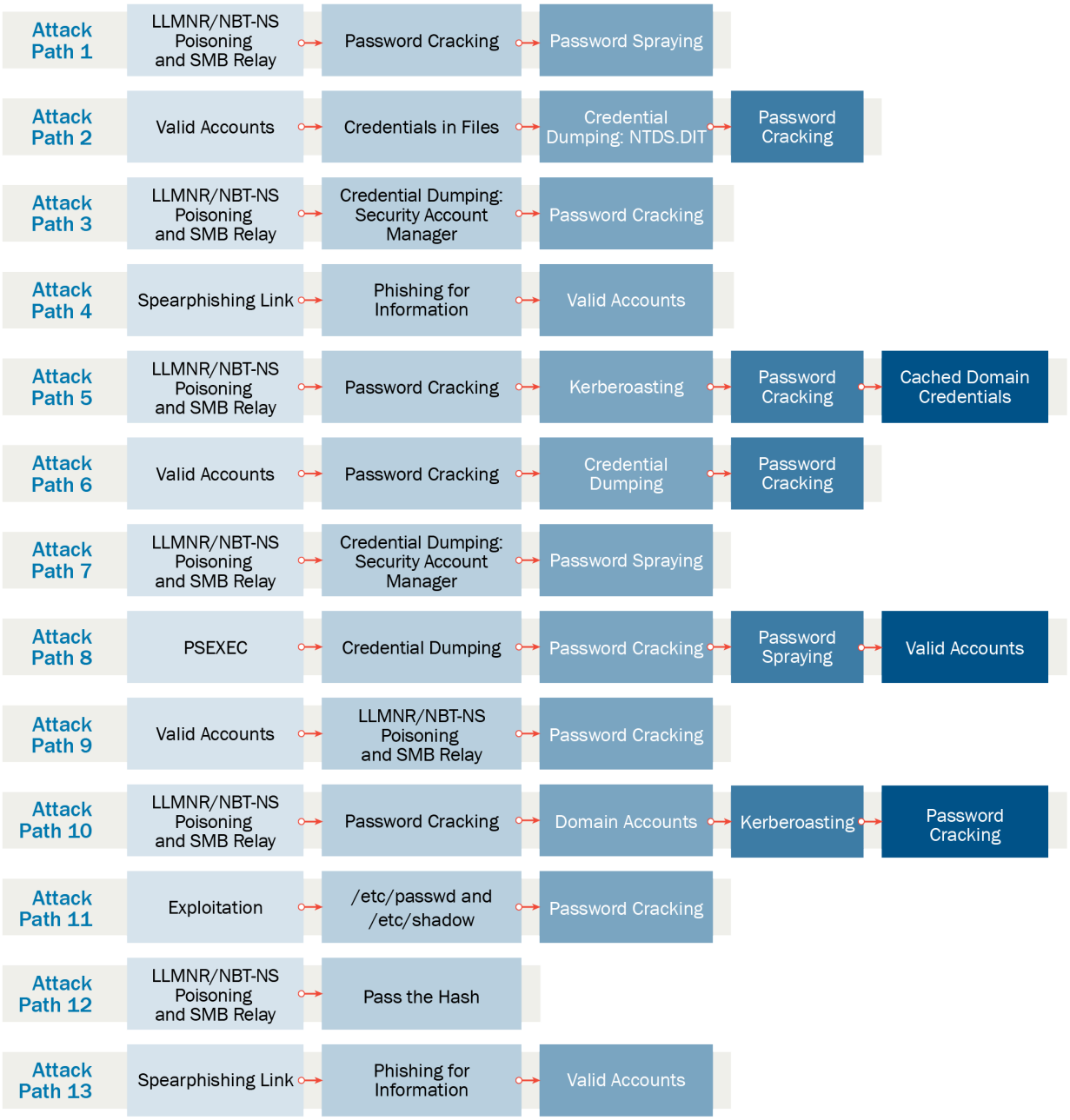


Figure 15: Attack Path Examples

APPENDIX F: SUMMARIZED FINDINGS OF 2022 CPT ASSESS MISSIONS

Table 3: MITRE ATT&CK® Techniques used on 2022 CPT Missions provides the total counts of MITRE ATT&CK® Techniques used during the 2022 CPT Missions.

MITRE Technique	Internal	External	Total
Brute Force: Password Cracking	11	1	12
Valid Accounts: Default Accounts	12	0	12
Mitigation: Password Policy	11	0	11
Mitigation: Update Software	10	0	10
Brute Force: Password Cracking	10	0	10
Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	6	2	8
User Execution: Malicious Link	0	8	8
Steal or Forge Kerberos Tickets: Kerberoasting	7	0	7
Mitigation: Privileged Access Management	6	0	6
Network Shares Discovery	6	0	6
Phishing: Spearphishing Link	0	6	6
Mitigation: Network Segmentation	6	0	6
Modify Authentication Process	4	0	4
Exposed Public-Facing Application	3	1	4
Mitigation: Update Software	4	0	4
Internal Spear-phishing	4	0	4
Valid Accounts: Domain Accounts	4	0	4
Valid Accounts: Local Accounts	4	0	4
Network Denial of Service	3	0	3
Account Discovery: Domain Account	3	0	3
Data from Local Shared Drive	2	1	3
Mitigation: Password Policy	3	0	3
Drive-by Compromise	1	2	3

MITRE Technique	Internal	External	Total
Mitigation: Encrypt Sensitive Information	2	1	3
Modify Authentication Process	3	0	3
Exposed Public-Facing Application	3	0	3
Unsecured Credentials: Credentials in Files	2	0	2
Mitigation: Data Loss Prevention	2	0	2
Unsecured Credentials	2	0	2
Indirect Command Execution	1	1	2
Mitigation: Encrypt Sensitive Information	1	1	2
Steal or Forge Kerberos Tickets: Kerberoasting	2	0	2
Develop Capabilities: Digital Certificates	1	0	1
Remote Services	1	0	1
Mitigation: Encrypt Sensitive Information	1	0	1
Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	1	0	1
OS Credential Dumping: Cached Domain Credentials	1	0	1
Adversary-in-the-Middle: DHCP Spoofing	1	0	1
Modify Authentication Process	1	0	1
Valid Accounts: Default Accounts	1	0	1
Steal or Forge Kerberos Tickets: Kerberoasting	1	0	1
Valid Accounts: Default Account	1	0	1

Table 3: MITRE Techniques used on 2022 CPT Missions

APPENDIX G: KNOWN EXPLOITABLE VULNERABILITIES DETECTED ON CPT MISSIONS

Common Microsoft KEV

"BlueKeep" Microsoft Windows Remote Desktop Remote Code Execution Vulnerability			
CVE-2019-0708	CVSS: 9.8	CWE-416	Occurrences: 41
Description: A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using Remote Desktop Protocol (RDP) and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability.'			
Example: In 2019, researchers from University of Rijeka and Kobe University demonstrated the disruption of a ship's Electronic Chart Display and Information System (ECDIS) by exploiting the BlueKeep vulnerability on board a Japanese training vessel.[24]			

Microsoft SMBv1 Remote Code Execution/Information Disclosure Vulnerability (multiple CVEs)			
CVE-2017-0143 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	CVSS: 8.1	CWE-20 CWE-200	Occurrences: 15
Description: The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." Vulnerabilities labeled CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, CVE-2017-0146, and CVE-2017-0148 are all similar.			
Example: In 2017, NotPetya malware exploited SMBv1 vulnerabilities resulting enterprise-wide disruptions to A.P. Møller – Mærsk A/S networks.[25]			

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

[25] Source: Greenberg, Andy. *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.* Anchor, 2019.

Common Apache KEV

Apache HTTP Server-Side Request Forgery (SSRF)			
CVE-2021-40438	CVSS: 9.0	CWE-918	Occurrences: 32
Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.			
Example: CISA reported the presence of this vulnerability within Apache HTTP Servers used as part of Siemens OT networks.[26]			

Apache Tomcat Improper Privilege Management "GhostCat" Vulnerability			
CVE-2020-1938	CVSS: 9.8	N/A	Occurrences: 21
Description: When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50, and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed returning arbitrary files from anywhere in the web application and-processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defense-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51, or 7.0.100 or later. Several changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51, or 7.0.100 or later will need to make configuration changes to their configurations.			
HelpNet Security reported GhostCat as the 6th most common exploited vulnerability in the wild for calendar year 2020.[27]			

Apache Tomcat Remote Code Execution Vulnerability			
CVE-2017-12617	CVSS: 8.1	CWE-434	Occurrences: 15
Description: When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46, and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the read-only initialization parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.			
According to Threat Post, CVE-2017-12617 was the most common publicly exploitable vulnerability throughout 2017 related to products using Apache Tomcat as the underlying web container.[28]			

[26] Source: https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-06
[27] Source: https://www.helpnetsecurity.com/2021/02/03/2020-top-exploited-vulnerabilities/
[28] Source: https://threatpost.com/securing-network-perimeter/175043/

Apache Log4j2 Remote Code Execution Vulnerability			
CVE-2021-44228	CVSS: 10	CWE-917, Improper Neutralization of Special Elements used in an Expression Language Statement CWE-400, Uncontrolled Resource Consumption CWE-20, Improper Input Validation CWE-502, Deserialization of Untrusted Data	Occurrences: 15
Description: Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.			
According to Mandiant, this vulnerability was one of the Top 10 vulnerabilities exploited to target chemical and critical manufacturing companies in late 2021.[29]			

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

APPENDIX H: COMMON MITIGATIONS

Common Mitigation #1: Password Policies

A password policy is a set of rules and guidelines that dictate how users should create and manage their passwords for a given system or organization. Password policies are put in place to ensure the security and integrity of systems and the data they contain. Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose easily-guessed passwords. One effective technique is to use pass phrases; using multiple words can add significant length to a password but still require significant mathematical computation to crack. Password managers offer greater security and convenience for the use of passwords to access online services. Greater security is achieved principally through the capability of most password manager applications to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault.[30]

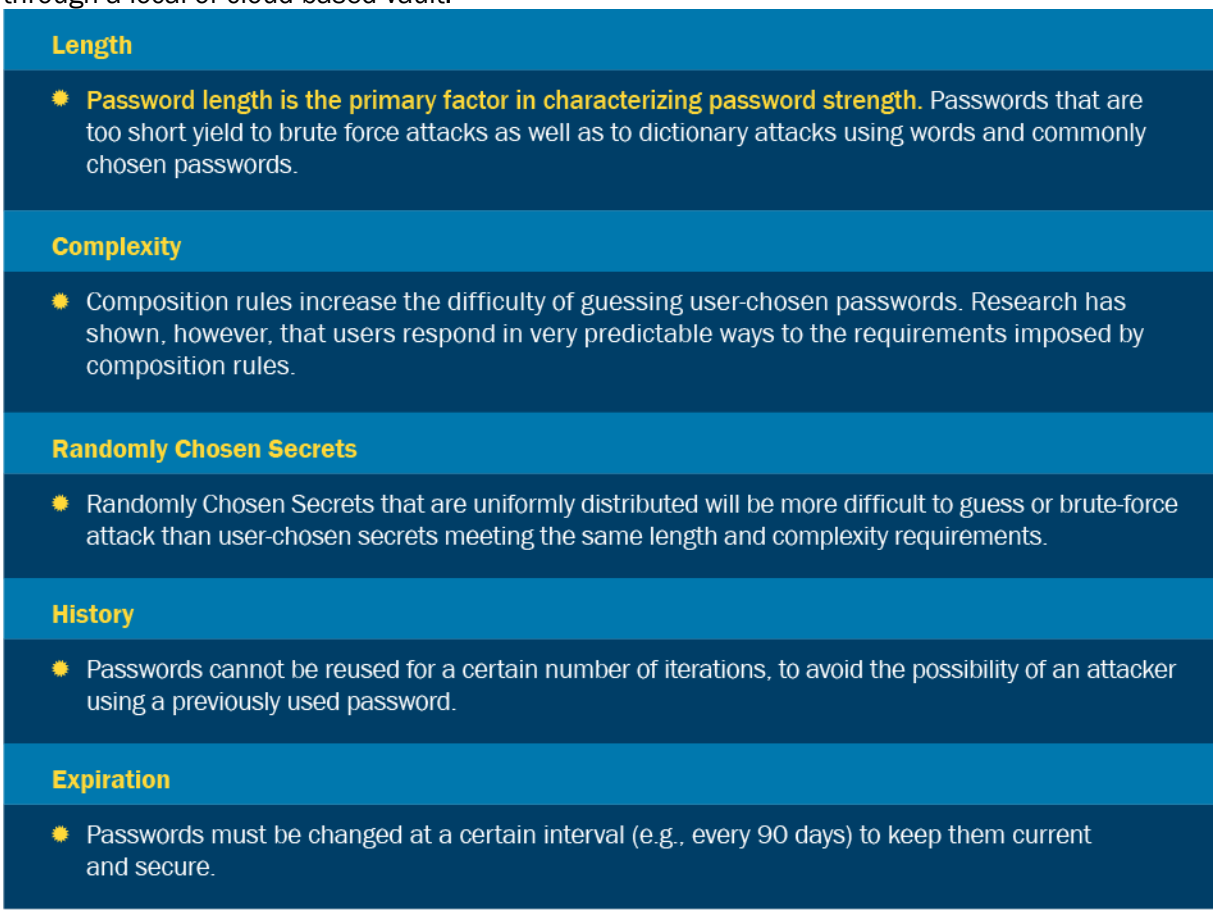


Figure 16: Password Policy Recommendations

[30] Source: NIST Special Publication 800-63 Digital Identity Guidelines, available at: https://pages.nist.gov/800-63-3/

Service (non-user) Accounts:

- Ensure strong password length (**ideally 25+ characters**) and complexity for service accounts (non-user accounts) and that these passwords periodically expire.[31]
- Also consider using Group Managed Service Accounts or another third-party product such as password vaulting.

Figure 17: Password Strength Perspectives depicts analysis published by Randall Munroe on xkcd.com and provides a visual representation of secure password policies.[32]

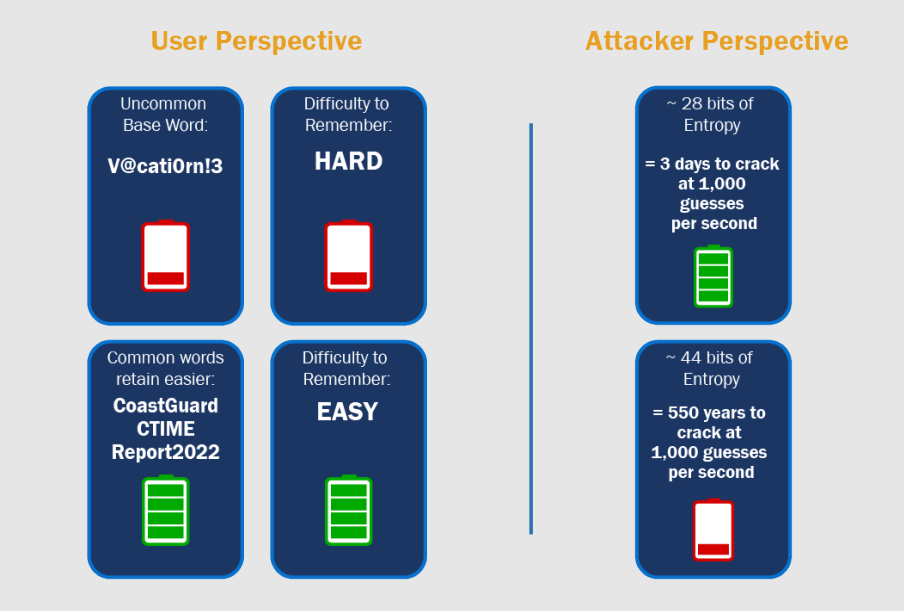


Figure 17: Password Strength Perspectives

[31] Source: https://sbscyber.com/resources/kerberoasting-the-potential-dangers-of-spn-accounts
[32] Source: https://xkcd.com/936/

Common Mitigation #2: Multi-Factor Authentication

MFA is a security method in which a user is required to provide multiple forms of identification to access a system or account.

MFA typically involves at least two of the following three authentication factors:[33]

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

To enable MFA, implement two or more means to authenticate to a system, such as a username, password, and a token from a physical smart card or token generator. A common example of MFA is using a password (something the user knows) in combination with a fingerprint scan or a code sent to the user's phone (something the user has or something the user is).

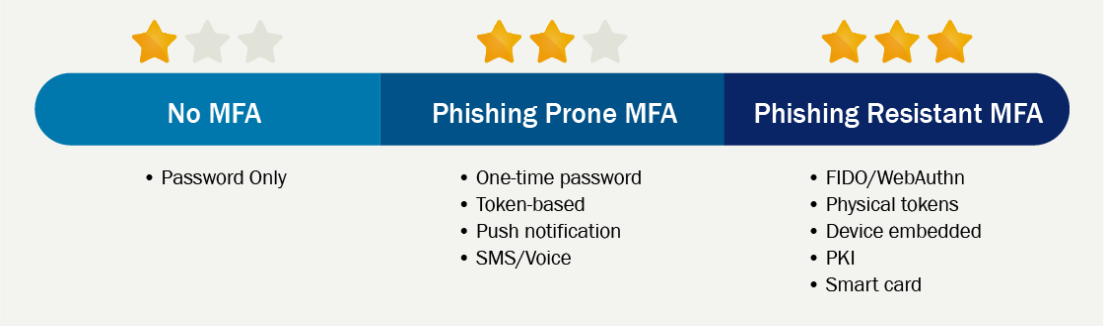


Figure 18: MFA Implementation Strength

MCAs deploy several techniques to bypass or misuse some common MFA methods. These attack vectors include SS7 Interception, Credential Harvesting, Push Bombing, and SIM Swapping.[34]

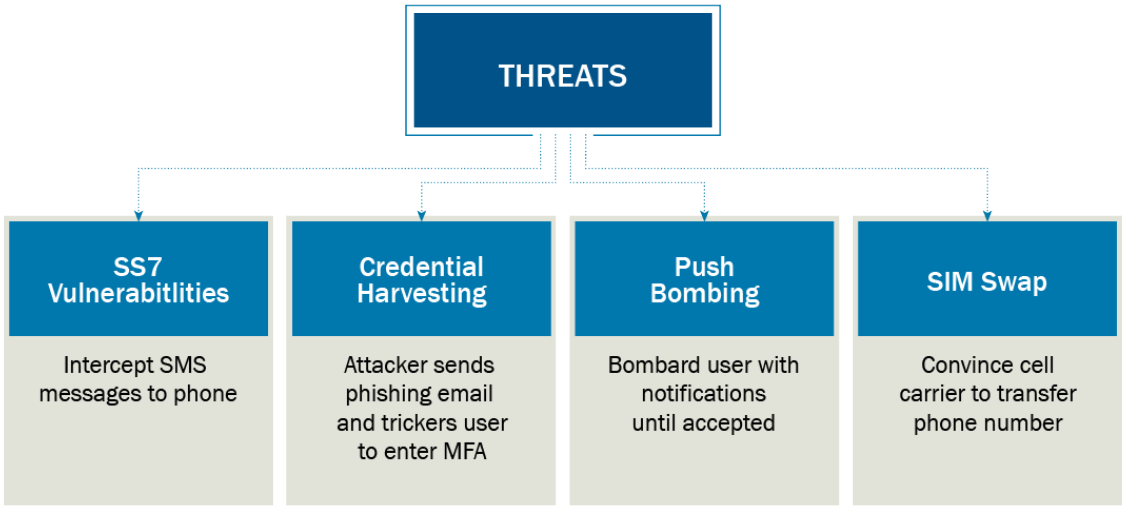


Figure 19: MFA Bypass Techniques used by Threats

[33] Source: NIST Special Publication 800-63 Digital Identity Guidelines, available at: https://pages.nist.gov/800-63-3/
[34] Source: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Common Mitigation #3: Filter Network Traffic

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

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

Figure 20: Network Traffic Filtering provides use cases for filtering network traffic. Keep in mind every network is different and network traffic filtering should be adapted to each individual network.

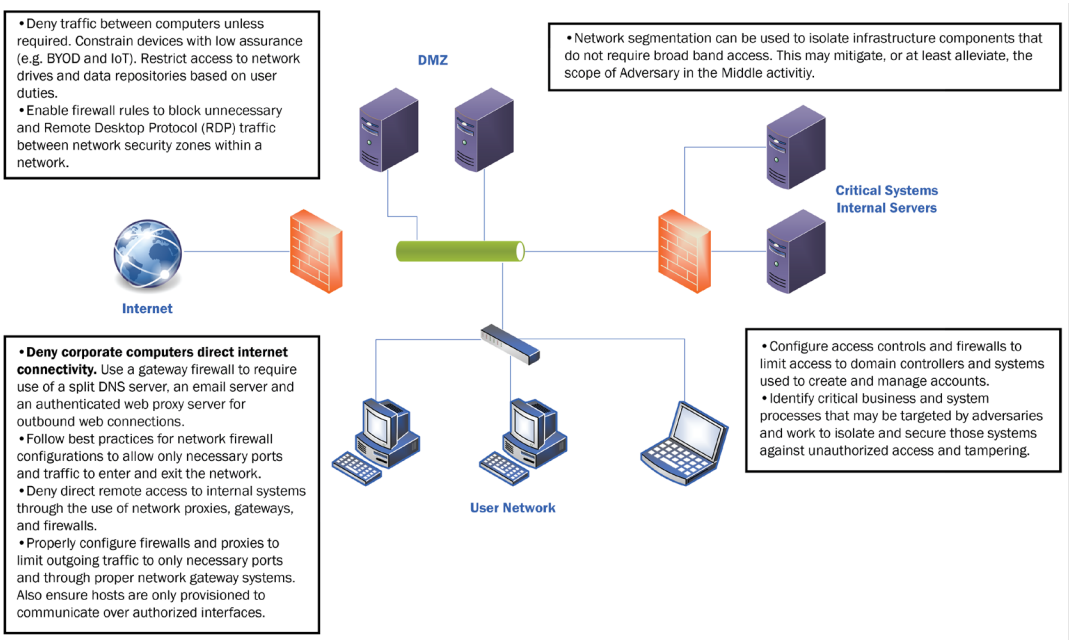


Figure 20: Network Traffic Filtering

Network traffic can be filtered three different ways (inbound, outbound, and protocol-based). Implementation is accomplished by either network appliances or configured directly on the endpoint. Below offers some general guidance for organizations looking to implement network traffic filtering.[35]

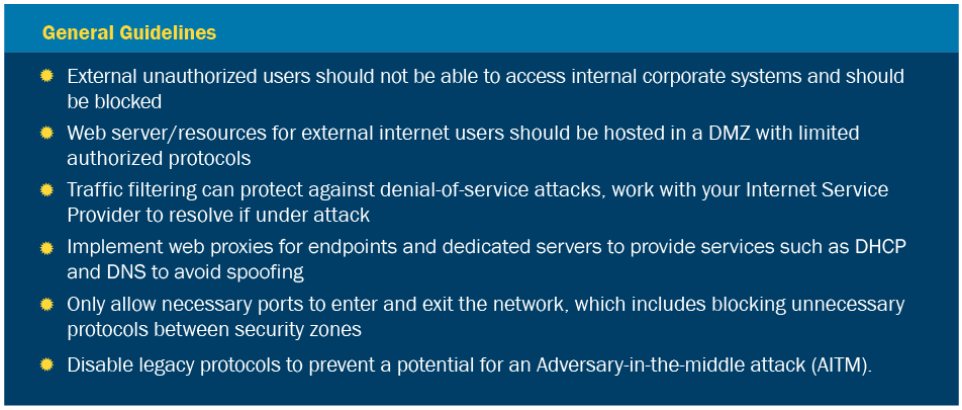


Figure 21: Network Traffic Filtering General Guidelines

[35] Source: https://attack.mitre.org/mitigations/M1037/

Common Mitigation #4: Privileged Account Management

Privileged account management is a critical element of security and compliance. It helps protect sensitive data and resources, meet regulatory requirements, and improve efficiency by limiting unnecessary access and permissions. Privilege account management is the process of creating, managing, and monitoring privileged accounts in a computer system or network. A privileged account is an account that has more access and permissions than regular user accounts. Privileged accounts include administrator accounts, root accounts, and service accounts.

The main goal of privilege account management is to reduce the risk of security breaches and other malicious actions by controlling access to sensitive data and resources. This can be done by implementing strict access controls, such as password policies, two-factor authentication, and limiting the number of privilege accounts, as depicted in *Figure 22: Privileged Account Management (PAM) Access Controls.*

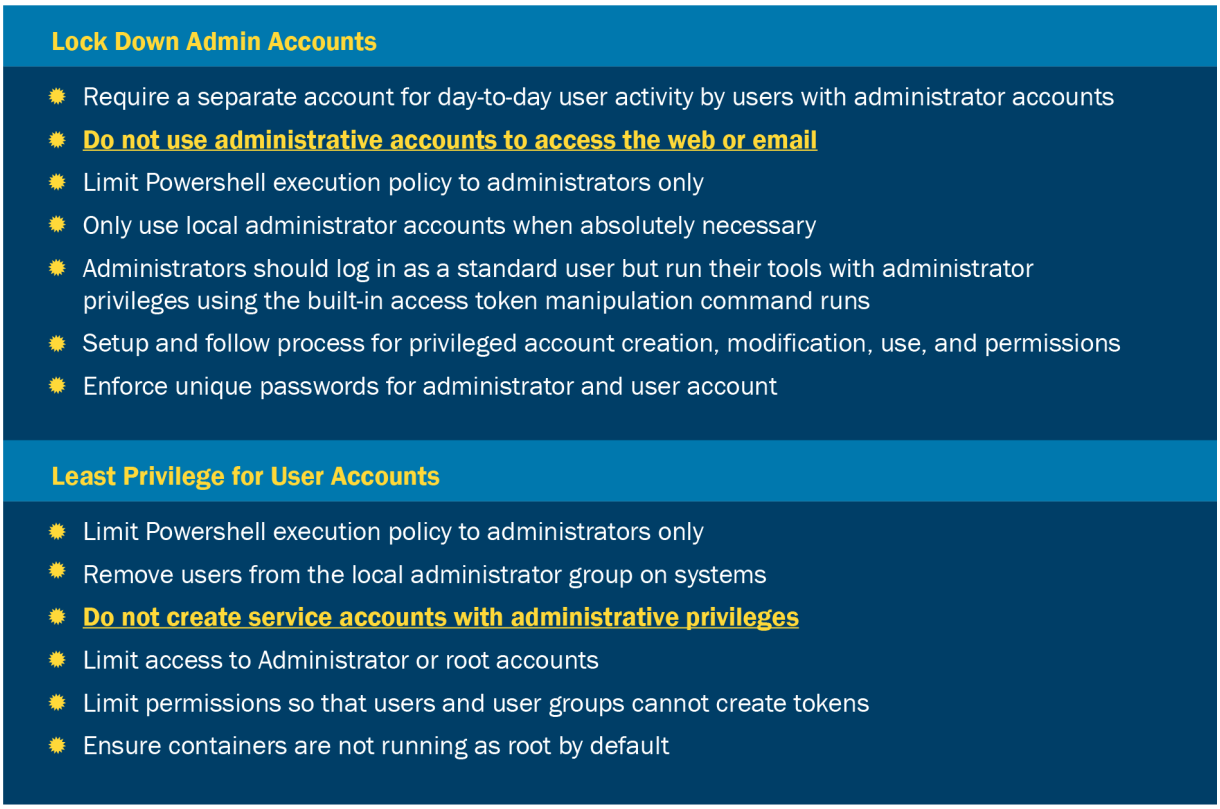


Figure 22: Privileged Account Management (PAM) Access Controls

Common Mitigation #5: Update Software

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

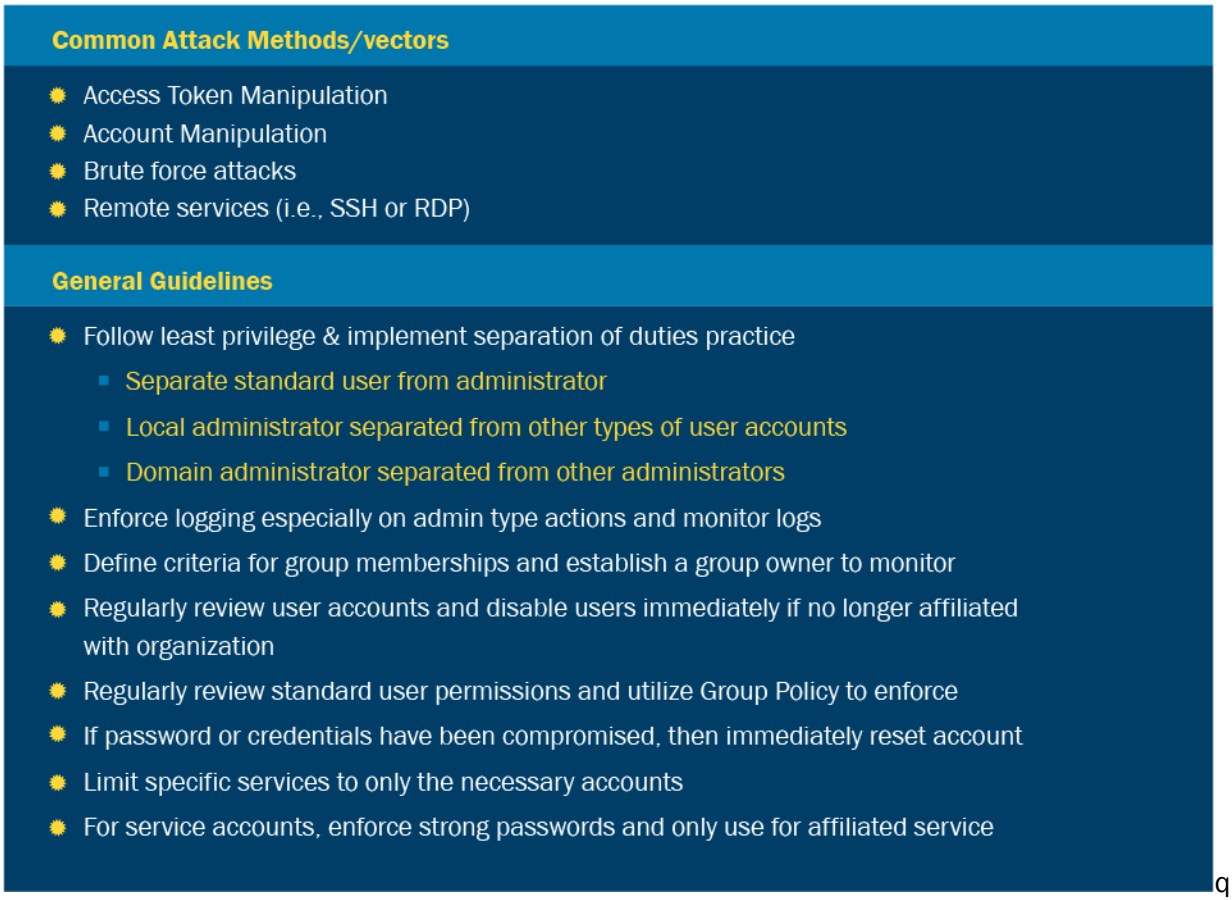
Common Mitigation #6: User Training

User training is a vital mitigation factor because it helps to educate users about the risks and threats. User training minimizes the likelihood of human error and enables compliance with regulatory requirements. By providing training on topics such as safe browsing, email security, and password management, users are better equipped to identify and mitigate potential security risks. *Figure 23: User Training - Best Practices* identifies some standard cyber hygiene best practices for average users.

Figure 23: User Training-Best Practices

Common Mitigation #7: User Account Management

User account management is managing "the creation, use, and permissions associated to user accounts" from MITRE ATT&CK®.[36] User account management should follow the principle of least privilege and separation of duties.[37]



q

Figure 24: User Account Management and General Guidelines

[36] Source: https://attack.mitre.org/mitigations/M1018/ https://attack.mitre.org/mitigations/M1018/
[37] Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Common Mitigation #8: Account Use Policies

Account Use Policies refers to configuring "features related to account use like login attempt lockouts, specific login times, etc." from MITRE ATT&CK®.[38]

Figure 25: Account Use Policies - Common Attack Methods & General Guidelines[39]

[38] Source: https://attack.mitre.org/mitigations/M1036
[39] Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Common Detections: Logging

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

Process & Process Metadata

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

User Accounts

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

Network Traffic

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

Application Log Content

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

Command Execution

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

Figure 26: Detection/Logging Recommendations

APPENDIX I: LIST OF ACRONYMS

AI	Artificial Intelligence
AJP	Apache Jserv Protocol
AMSC	Area Maritime Security Committees
AOR	Area of Responsibility
API	Application Programming Interface
APT	Advanced Persistent Threat
AS-REP	Authentication Server Request
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BCS	Building Control System
BEC	Business Email Compromise
BIOS	Basic input/output System
CGCYBER	U.S. Coast Guard Cyber Command
CI/KR	Critical Infrastructure and Key Resources
CIC	Critical Incident Communication
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPT	Cyber Protection Team
CSA	Cybersecurity Advisory
CTIME	Cyber Trends and Insights in the Marine Environment
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CySO	Cybersecurity Officers
DDoS	Distributed Denial of Service (DDoS)
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name System
DOD	Department of Defense
ECDIS	Electronic Chart Display and Information System
EMP	Enterprise Mission Platform
FEMA	Federal Emergency Management Agency
FOC	Full Operational Capability
FSO	Facility Security Officer
FY	Fiscal Year
GPU	Graphics Processing Unit
IDS	Intrusion Detection Systems
IOC	Initial Operational Capability
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IT	Information Technology
JNDI	Java Naming and Directory Interface

KEV	Known Exploitable Vulnerabilities
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
MARSEC	Maritime Security
MCA	Malicious cyber actors
MCRB	Maritime Cyber Readiness Branch
ME	Marine Environment
MFA	Multi-Factor Authentication
MTS-ISAC	Maritime Transportation System Information Sharing and Analysis Center
MTSS-C	Maritime Transportation Systems Specialist – Cyber
NBT-NS	NetBIOS Name Service
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
NRC	National Response Center
OGA	Other Government Agencies
OT	Operational Technology
PAM	Privileged Account Management
PSGP	Port Security Grant Program
RDP	Remote Desktop Protocol
SLCGP	State and Local Cybersecurity Grant Program
SLT	State, Local, and Territorial
SLTT	State, Local, Territorial, and Tribal
SMB	Server Message Block
SRMA	Sector Risk Management Agency
TTP	Tactics, Techniques, and Procedures
TWIC	Transportation Workers Identification Credentials
UAG	Unified Access Gateway
VM	Virtual Machine
VPN	Virtual Private Network

APPENDIX J: TABLE OF FIGURES

APPENDIX K: TABLE OF TABLES