Assets identification / CATALOG FOR ASSETS

**Physical Assets:**

**a. Hull and Structure:**

- Main hull

- Superstructure

- Deck structures

**b. Machinery and Propulsion:**

- Engines (main and auxiliary)

- Propellers

- Thrusters

- Fuel systems

**c. Navigation Systems:**

- GPS receivers

- Gyrocompass

- Radar systems

- AIS (Automatic Identification System)

**d. Communication Systems:**

- VHF/UHF radios

- Satellite communication systems

- Intercom systems

**e. Safety and Emergency Equipment:**

- Lifeboats and life rafts

- Fire suppression systems

- Emergency power systems

**f. Cargo Handling Systems:**

- Cranes - Conveyors

- Cargo monitoring systems

**g. Power Systems:**

- Generators

- Electrical distribution systems

- Batteries

**Cyber Assets:**

**a. Control Systems:**

- Engine control systems

- Propulsion control systems

- Cargo control systems

**b. Communication Networks:**

- LAN (Local Area Network)

- WAN (Wide Area Network)

- Satellite networks

**c. Automation Systems:**

- Shipboard management systems

- Alarm and monitoring systems

**d. Navigation and Positioning Systems:**

- ECDIS (Electronic Chart Display and Information System)

- GPS receivers and sensors

**e. Cybersecurity Systems:**

- Firewalls

- Intrusion detection and prevention systems

- Antivirus software

**f. Remote Monitoring and Control Systems:**

- Systems allowing remote access for diagnostics and control

**g. Software Applications:**

- Operational software for navigation, communication, and cargo management

**h. Data Storage Systems:**

- Servers

- Data storage devices

**i. Authentication and Access Control Systems:**

- Biometric systems

- User access controls

**j. Satellite Communication Security:**

- Encryption systems for secure satellite communication

**What are all the physical assets that directly or indirectly connected to the cyber assets or any computational device that could be tampered or hacked in any way in maritime industry (cyber enabled ship)?**

* **Navigation Systems:** GPS receivers and other navigation systems are crucial for safe maritime operations. If compromised, they could lead to incorrect positioning, navigation errors, or even navigational spoofing.
* **Engine Control Systems:** Modern ships often have computerized engine control systems that regulate propulsion and power generation. Tampering with these systems could impact the ship's speed, fuel efficiency, or even lead to mechanical failures.
* **Communication Systems:** Satcom terminals, radio communication equipment, and other communication systems are integral to maritime operations. Unauthorized access or tampering with these systems could disrupt communication, navigation, and coordination between ships and onshore facilities.
* **Dynamic Positioning Systems:** Some vessels, especially offshore support and exploration ships, use dynamic positioning systems that rely on complex algorithms and sensors to maintain a specific position. A cyber attack on these systems could jeopardize the vessel's stability and safety.
* **Electronic Chart Display and Information Systems (ECDIS):** ECDIS systems are digital navigation charts used for voyage planning and navigation. Compromising these systems could lead to incorrect route planning, posing a risk to navigation safety.
* **Automated Identification System (AIS):** AIS is used for vessel tracking and collision avoidance. Cybersecurity breaches could lead to the manipulation of AIS data, potentially causing confusion and safety risks.
* **Cargo Handling Systems:** Automated cargo handling systems on container ships are controlled by computational devices. Unauthorized access or manipulation of these systems could lead to cargo mishandling, damage, or theft.
* **Ballast Water Management Systems:** Ships use computational devices to control ballast water management systems. Cyber attacks on these systems could impact the ship's stability and compliance with environmental regulations.
* **Emergency Communication and Safety Systems:** Distress beacons, emergency communication systems, and safety systems are critical for responding to emergencies. Cybersecurity breaches could hinder the proper functioning of these systems during critical situations.
* **Weather Monitoring Systems:** Computational devices are used for weather monitoring and forecasting on ships. Manipulation of weather data could impact route planning and decision-making, leading to unsafe conditions.
* **Satellite Communication Terminals:** Many ships rely on satellite communication for internet access, operational data exchange, and crew communication. Cyber attacks on satellite communication terminals could disrupt these essential services.

INDENTIFICATION OF THREATS

1. Malware and Ransomware:

* Threat: Malicious software and ransomware can infiltrate ship systems, leading to unauthorized access, data theft, or system disruption.
* Vulnerability: Inadequate antivirus protection and outdated software can expose ships to malware attacks.

1. Phishing Attacks:

* Threat: Social engineering attacks, such as phishing emails, can trick crew members into revealing sensitive information or clicking on malicious links.
* Vulnerability: Lack of cybersecurity awareness and training among ship personnel.

1. Unauthorized Access:

* Threat: Hackers gaining unauthorized access to ship systems, potentially manipulating navigation, communication, or control systems.
* Vulnerability: Weak or easily guessable passwords, inadequate access controls, and outdated software.

1. Denial of Service (DoS) Attacks:

* Threat: Attackers may attempt to overwhelm ship systems with excessive traffic, disrupting normal operations.
* Vulnerability: Insufficient network security measures to mitigate and handle DoS attacks.

1. Physical Tampering:

* Threat: Physical access to ship systems can lead to tampering with critical equipment or the installation of malicious hardware.
* Vulnerability: Inadequate physical security measures on board ships.

1. Supply Chain Attacks:

* Threat: Malicious actors compromising the security of third-party vendors or suppliers, leading to vulnerabilities in ship systems.
* Vulnerability: Lack of robust supply chain cybersecurity practices and vetting procedures.

1. Insider Threats:

* Threat: Malicious actions or negligence from onboard personnel can lead to security breaches.
* Vulnerability: Inadequate monitoring of employee activities, lack of employee awareness, and insufficient access controls.

1. IoT and Operational Technology (OT) Vulnerabilities:

* Threat: Exploitation of vulnerabilities in interconnected devices and operational technology systems on board.
* Vulnerability: Insecure IoT devices, outdated OT systems, and insufficient segmentation of ship networks.

1. Data Breaches:

* Threat: Unauthorized access to sensitive data, including ship routes, cargo details, and crew information.
* Vulnerability: Inadequate data encryption, storage, and transmission practices.

1. Regulatory Compliance Issues:

* Threat: Non-compliance with maritime cybersecurity regulations may result in legal and operational consequences.
* Vulnerability: Lack of awareness or adherence to industry cybersecurity standards and regulations.