- Shipping
  - Unauthorized Diversion or Appropriation of Freight
    - Inducing Economic Damage
      - Freight and Cargo Management Systems
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-862: Missing Authorization
        - CWE-863: Incorrect Authorization
        - CWE-294: Authentication Bypass by Capture-replay
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-502: Deserialization of Untrusted Data
        - CWE-778: Insufficient Logging
        - CWE-807: Reliance on Untrusted Inputs in a Security Decision
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-939: Improper Authorization in Handler for Custom URL Scheme
      - Cargo Tracking Devices
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-306: Missing Authentication for Critical Function
        - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor
        - CWE-522: Insufficiently Protected Credentials
        - CWE-307: Improper Restriction of Excessive Authentication Attempts
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-326: Inadequate Encryption Strength
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-603: Use of Client-Side Authentication
        - CWE-749: Exposed Dangerous Method or Function
  - Manipulation or Disabling of Cargo Tracking Systems
    - Financial Gain through Coercion
      - Dispatch Systems
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-306: Missing Authentication for Critical Function
        - CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-502: Deserialization of Untrusted Data
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
      - Onboard Entertainment Systems
        - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-306: Missing Authentication for Critical Function
        - CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
        - CWE-326: Inadequate Encryption Strength
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
    - Financial Gain through Contraband Trafficking
      - License Plate Recognition Systems
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-306: Missing Authentication for Critical Function
        - CWE-522: Insufficiently Protected Credentials
        - CWE-285: Improper Authorization
        - CWE-862: Missing Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-799: Improper Control of Interaction Frequency
        - CWE-807: Reliance on Untrusted Inputs in a Security Decision
  - Unauthorized Access to Confidential Route Data
    - Gain a Competitive Advantage
      - Enterprise Resource Planning (ERP) Systems
        - CWE-20: Improper Input Validation
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-502: Deserialization of Untrusted Data
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
      - Customer Relationship Management (CRM) Systems
        - CWE-20: Improper Input Validation
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-522: Insufficiently Protected Credentials
        - CWE-284: Improper Access Control
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
      - Navigation and Positioning Systems
        - CWE-290: Authentication Bypass by Spoofing
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-384: Session Fixation
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-920: Improper Restriction of Power Consumption
  - Intentional Disruption of Hazardous Goods Transport
    - Mitigate Environmental Impact and Promote Sustainable Practices
      - Logistics and Scheduling Software
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-306: Missing Authentication for Critical Function
        - CWE-620: Unverified Password Change
        - CWE-250: Execution with Unnecessary Privileges
        - CWE-285: Improper Authorization
        - CWE-862: Missing Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-602: Client-Side Enforcement of Server-Side Security
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-807: Reliance on Untrusted Inputs in a Security Decision
      - Industrial Control Systems (ICS) and SCADA Systems
        - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-1393: Use of Default Password
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-502: Deserialization of Untrusted Data
        - CWE-506: Embedded Malicious Code
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
  - Tampering with Shipping Documentation or Manifests
    - Commit Insurance Fraud
      - Data Storage and Processing Centers
        - CWE-118: Incorrect Access of Indexable Resource (Range Error)
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-256: Plaintext Storage of a Password
        - CWE-287: Improper Authentication
        - CWE-522: Insufficiently Protected Credentials
        - CWE-215: Insertion of Sensitive Information Into Debugging Code
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
  - Extraction of Customer Information
    - Financial Gain through Illicit Distribution
      - Public facing booking system
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-384: Session Fixation
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
  - Corporate Espionage
    - Gain a Competitive Advantage
      - Web hosting services
        - CWE-20: Improper Input Validation
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-522: Insufficiently Protected Credentials
        - CWE-250: Execution with Unnecessary Privileges
        - CWE-276: Incorrect Default Permissions
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
        - CWE-284: Improper Access Control
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-416: Use After Free
        - CWE-918: Server-Side Request Forgery (SSRF)
      - Financial Systems
        - CWE-20: Improper Input Validation
        - CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-326: Inadequate Encryption Strength
        - CWE-125: Out-of-bounds Read
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-259: Use of Hard-coded Password
        - CWE-306: Missing Authentication for Critical Function
        - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor
        - CWE-522: Insufficiently Protected Credentials
        - CWE-284: Improper Access Control
        - CWE-285: Improper Authorization
        - CWE-352: Cross-Site Request Forgery (CSRF)
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-942: Permissive Cross-domain Policy with Untrusted Domains
        - CWE-532: Insertion of Sensitive Information into Log File
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel
        - CWE-552: Files or Directories Accessible to External Parties
      - Operating Systems
        - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-732: Incorrect Permission Assignment for Critical Resource
        - CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)
        - CWE-125: Out-of-bounds Read
        - CWE-134: Use of Externally-Controlled Format String
        - CWE-346: Origin Validation Error
        - CWE-20: Improper Input Validation
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-306: Missing Authentication for Critical Function
        - CWE-522: Insufficiently Protected Credentials
        - CWE-250: Execution with Unnecessary Privileges
        - CWE-269: Improper Privilege Management
        - CWE-284: Improper Access Control
        - CWE-321: Use of Hard-coded Cryptographic Key
        - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
      - Remote Access Server
        - CWE-862: Missing Authorization
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-384: Session Fixation
        - CWE-942: Permissive Cross-domain Policy with Untrusted Domains
        - CWE-269: Improper Privilege Management
        - CWE-287: Improper Authentication
        - CWE-306: Missing Authentication for Critical Function
        - CWE-522: Insufficiently Protected Credentials
        - CWE-346: Origin Validation Error
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-922: Insecure Storage of Sensitive Information
        - CWE-311: Missing Encryption of Sensitive Data
  - Extortion of Clients
    - Financial Gain Through Extortion
      - Client databases
        - CWE-284: Improper Access Control
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-1392: Use of Default Credentials
        - CWE-209: Generation of Error Message Containing Sensitive Information
        - CWE-384: Session Fixation
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-250: Execution with Unnecessary Privileges
  - Manipulation of Vessel Positioning Data
    - Financial Gain through Cargo Theft and Smuggling
      - Navigation and Positioning Systems
        - CWE-346: Origin Validation Error
        - CWE-693: Protection Mechanism Failure
        - CWE-300: Channel Accessible by Non-Endpoint
        - CWE-284: Improper Access Control
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-521: Weak Password Requirements
  - Unauthorized Modification of Logs
    - Financial Gain through Falsification of Safety Records
      - Ship Maintenance Logging Systems
        - CWE-306: Missing Authentication for Critical Function
        - CWE-521: Weak Password Requirements
        - CWE-284: Improper Access Control
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-778: Insufficient Logging
  - Exfiltration of Credentials
    - Gather Crew Identities for Espionage, Fraud, and Unauthorized Access
      - Maritime Crew Authentication Systems
        - CWE-521: Weak Password Requirements
        - CWE-1392: Use of Default Credentials
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-384: Session Fixation
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-284: Improper Access Control
  - Compromise of Systems
    - Sabotage of Fuel Operations and Supply-Chain Disruption
      - Ship Fuel Management Systems
        - CWE-521: Weak Password Requirements
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-284: Improper Access Control
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-384: Session Fixation
        - CWE-778: Insufficient Logging
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
  - Disruption of Physical Sensors
    - Sabotage of Cargo Integrity and Supply Chain Disruptions
      - Smart Container Monitoring Systems
        - CWE-20: Improper Input Validation
        - CWE-284: Improper Access Control
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-400: Uncontrolled Resource Consumption
        - CWE-770: Allocation of Resources Without Limits or Throttling
        - CWE-798: Use of Hard-coded Credentials
        - CWE-306: Missing Authentication for Critical Function
        - CWE-345: Insufficient Verification of Data Authenticity
        - CWE-778: Insufficient Logging
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-941: Incorrectly Specified Destination in a Communication Channel
  - Sabotage of Berthing Systems
    - Compromise Maritime Operations and Cause an Economic Impact
      - Automated Berthing Control Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-284: Improper Access Control
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-384: Session Fixation
        - CWE-778: Insufficient Logging
        - CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Manipulation of Freight Platforms
    - Financial Gain Through Fraud
      - Freight Auction and Bidding Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-284: Improper Access Control
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-384: Session Fixation
        - CWE-778: Insufficient Logging
        - CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Network Compromise
    - Disruption of Maritime Operations
      - Port Network Infrastructure
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-288: Authentication Bypass Using an Alternate Path or Channel
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-284: Improper Access Control
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-384: Session Fixation
        - CWE-778: Insufficient Logging
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Unauthorized Diversion of Shipments
    - Financial Gain through Cargo Theft and Fraud
      - Logistics and Cargo Management Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-319: Cleartext Transmission of Sensitive Information

Presented with xmind