Securing Ship Automation & Control Systems

Identify and mitigate cyberthreats and operational issues

Shipping and maritime industries are heavily dependent on integrated digital systems for everything from navigation to engine monitoring. Modern ships are floating cities with electric power generation, fuel dissemination and water treatment as well as other networked systems like HVAC, video surveillance and automated safety controls. With these expansive technologies, the damage a cyber incident can cause to critical systems is difficult to quantify but can be substantial.

The Challenge

The rapid shift toward automation and digital controls has improved efficiency and safety, but these new technologies have also opened up ship networks to increased cyber and operational threats. Shipowners and operators must ensure that cyber risks are appropriately addressed in existing safety management systems. Failure to comply with IMO 2021 may result in the denial of port access or even ship detentions.[1]

Potential impacts [from a cyber-attack] could be safety-related, operational, environmental-related, financial, reputational and compliance-related.[1]

As one of the most safety-conscious industries, the maritime industry follows strict classification rules and operational regulations to ensure that everything possible occurs to prevent hazardous situations. Considering that the average maritime operation includes myriad advanced sensors, systems and applications, the ongoing monitoring and security management of these applications is a monumental task.

Maritime operators need to quickly collect and aggregate security and operational data from the entire ship's control and automation systems to maintain safety and operational reliability, and to keep up with an evolving threat landscape.

The Framework

The International Maritime Organization (IMO) prescribes three documents as guidelines for maritime cybersecurity. In order of priority:

- **1: Guidelines on Cyber Security Onboard Ships**, issued by BIMCO, CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, OCIMF, IUMI and World Shipping Council
- **2: NIST Critical Infrastructure US Federal Government Cyber Security Framework**
- **3: ISO 27001:2013 "IT Management Process"**

Compliance with IMO 2021 can help prevent denial of port access and ship detentions and possibly save costs. "For owners operating in the EU, the added benefit of adopting the robust IMO cybersecurity measures is mitigating the risk of data breaches which, under the General Data Protection Regulation (GDPR), can lead to administrative fines of up to 20 million euros or 4% of a company's total global turnover of the preceding fiscal year, whichever is higher."[2]

IMO Resolution MSC.428(98) makes clear that an approved Safety Management System (SMS) should incorporate cyber risk management that meets the objectives and functional requirements of the International Safety Management (ISM) Code.[3] The guidance provided in the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) provides high-level recommendations regarding the elements of an appropriate cyber risk management program. Forescout can provide guidance documents to help reconcile how these requirements can be satisfied.

The Forescout Platform for Maritime Cyber Resilience:

Forescout eyeInspect (formerly SilentDefense™) and the Forescout platform provide maritime operators with complete device visibility and advanced threat detection for all marine control networks and monitoring applications. This expansive view of a ship's entire digital network increases the speed of detecting anomalies and threats while enhancing

SOLVING ONBOARD IMO CHALLENGES

Protect ISM Code 1.2.2.2

- True-up hardware inventory
- True-up software inventory
- Map data flows
- Secure configurations for all hardware
- Audit logs

Detect ISM Code 9.1

- Unauthorized access to network or critical systems
- Unauthorized use of administrator privileges, personal devices, or removable media
- Suspicious network activity
- Validation of malware and network protection procedures

Respond to ISM Code 10.3

- Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state.

Annex 3

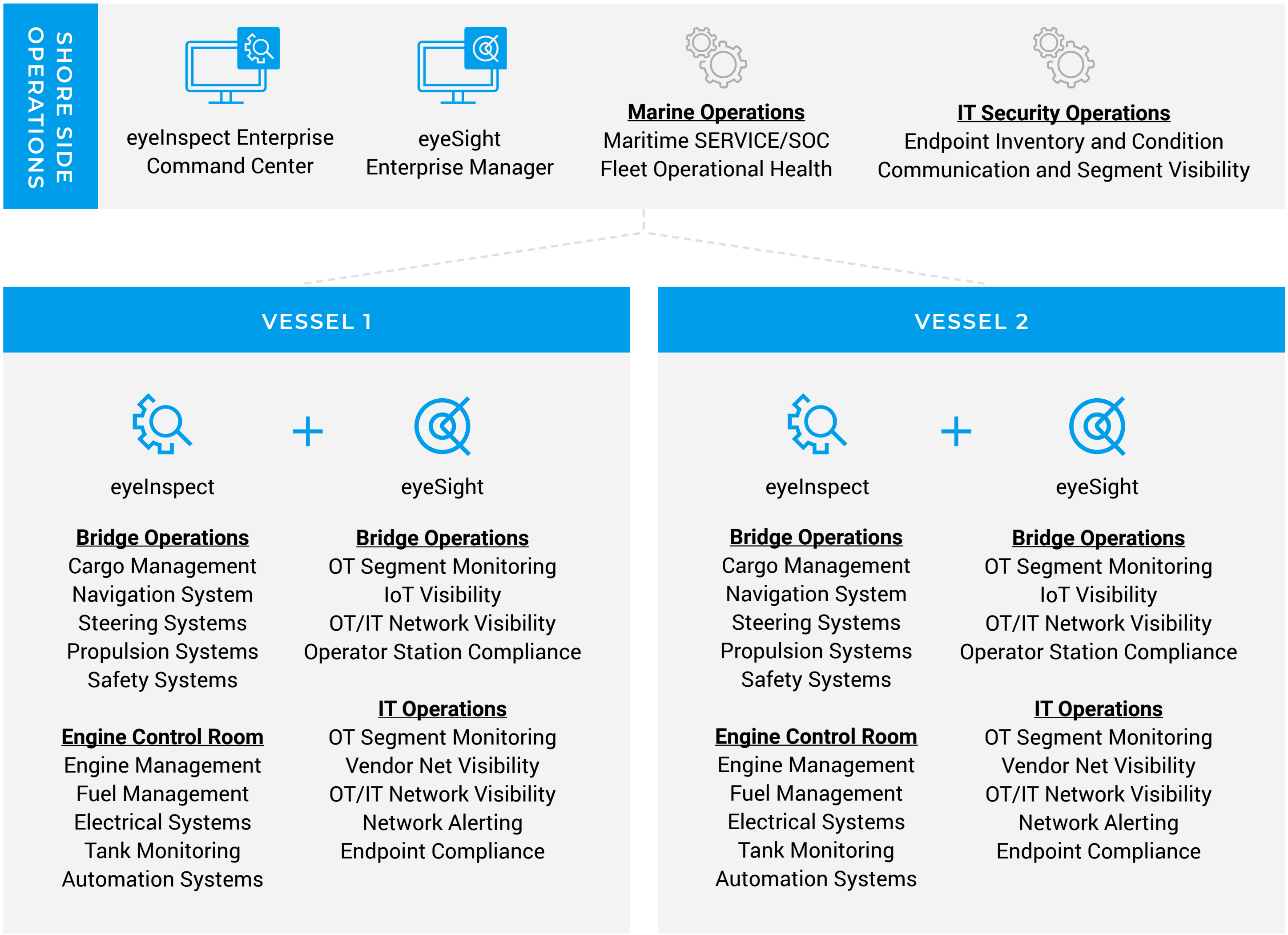
- Monitoring data activity
- Network intrusion detection (alerting)
- Intrusion protection system (alerting)
- Network segmentation
- Multiple layer strategy
- Defense-in-depth approach
- Vulnerabilities in commonly used protocols

response and remediation across critical alarms to I/O and IP device networks. With eyeInspect, operators in port or at sea can mitigate or prevent operational issues before they lead to potentially dangerous incidents.

For a fleet view, the Enterprise Command Center (ECC) provides global visibility and risk management for a whole fleet of ships from a single pane of glass. The ECC transmits relevant data from the field up to the enterprise level – enabling analysis of any incident in detail, including the devices involved and the context of the alert.

The benefits of Forescout eyeInspect extend far beyond conventional cybersecurity to offer asset owners in the maritime industry the power of complete operational technology (OT) network visibility and system integration with legacy and new bridge control systems.

Enterprise Deployment for Cruising or Shipping



SHORE SIDE OPERATIONS

eyeInspect Enterprise Command Center

eyeSight Enterprise Manager

Marine Operations
Maritime SERVICE/SOC
Fleet Operational Health

IT Security Operations
Endpoint Inventory and Condition
Communication and Segment Visibility

VESSEL 1

eyeInspect + eyeSight

eyeInspect

Bridge Operations
Cargo Management
Navigation System
Steering Systems
Propulsion Systems
Safety Systems

Engine Control Room
Engine Management
Fuel Management
Electrical Systems
Tank Monitoring
Automation Systems

eyeSight

Bridge Operations
OT Segment Monitoring
IoT Visibility
OT/IT Network Visibility
Operator Station Compliance

IT Operations
OT Segment Monitoring
Vendor Net Visibility
OT/IT Network Visibility
Network Alerting
Endpoint Compliance

VESSEL 2

eyeInspect + eyeSight

eyeInspect

Bridge Operations
Cargo Management
Navigation System
Steering Systems
Propulsion Systems
Safety Systems

Engine Control Room
Engine Management
Fuel Management
Electrical Systems
Tank Monitoring
Automation Systems

eyeSight

Bridge Operations
OT Segment Monitoring
IoT Visibility
OT/IT Network Visibility
Operator Station Compliance

IT Operations
OT Segment Monitoring
Vendor Net Visibility
OT/IT Network Visibility
Network Alerting
Endpoint Compliance

Figure 1. Each ship is an independent and autonomous system reporting to the ECC.

Cyber Resilience for the Maritime Industry

Asset Visibility and Monitoring

Forescout eyeInspect provides continuous asset visibility across OT networks and automatically builds a detailed network map with rich asset details. Additionally, eyeInspect automatically groups relevant assets by network and/or role and provides views in multiple formats such as Purdue level and communication relationship.

eyeInspect uses a wide range of discovery capabilities that include:

- Patented deep-packet inspection of 190+ IT and OT protocols
- Continuous, configurable policy and behavior monitoring
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems

Asset Configuration Management

eyeInspect automatically collects a wide range of OT asset information, logging all configuration changes for security analysis and operational forensics. Discoverable details include network address, host name, vendor and model of the asset, serial number, OS version, firmware version, hardware version, device modules' information, and more.

Risk Management and Compliance

Now you can proactively identify vulnerable OT assets to prioritize mitigation strategies with the Asset Risk Framework, the first centrally available "impact-based" risk tool for OT/ICS networks. It saves time, improves SOC and analyst effectiveness and reduces risk by automating security and operational risk analysis. eyeInspect also includes powerful dashboards, analytics and out-of-the-box reporting tools that simplify compliance with key standards, including ISA 99/IEC 62443 and the NIST Cybersecurity Framework.

Threat Detection & Incident Response

Automate threat detection, containment and remediation with alert investigation and response tools. Dashboards and widgets enhance user collaboration, while rich alert detail supports root-cause analysis

CYBER RISK MITIGATIONS TO IMPLEMENT, ACCORDING TO THE IMO:

- Cargo management systems
- Bridge systems
- Propulsion and machinery mgmt. and power control systems
- Access control systems
- Passenger servicing and mgmt. systems
- Passenger-facing public networks
- Administrative and crew welfare systems
- Communication systems

HIGHLY REFERENCEABLE PLATFORM

- Most deployments in maritime, power & utility
- More successful large OT network-monitoring solution deployments
- Safety-certified and already in production
- Examples: Commercial cruises, offshore drilling, logistics, ports

and expedites effective, efficient response. The Enterprise Command Center (ECC) allows users to zoom in on alerts from any ship in their geo-distributed fleet to analyze an incident in detail, including the devices involved and the context of the alert.

[1] IMO (International Maritime Organization); http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

[2] https://www.tradewindsnews.com/sponsor-content/cybersecurity-at-the-fore-as-imo-2021-looms/2-1-790426

[3] https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

COMPLETE VISIBILITY INTO SHIP SYSTEMS

eyeInspect can identify and help remediate a full range of both cyber and operational threats to ships, including, but not limited to:

- Passive detection and classification of hosts
- Cyberattacks (DDoS, MITM & scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior/policy changes
- Device malfunction misconfiguration
- New and non-responsive assets
- Corrupted messages
- Unauthorized firmware downloads
- Insecure protocols
- Default credentials and insecure authentications
- Logic changes

Ready to Make Your Fleet Cyber Resilient? Schedule a demo to see how eyeInspect can help secure your ships' industrial networks.
Request a demo

Don't just see it.
Secure it.™

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeInspect salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT®
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 01_21