Introduction

Scott Dickerson
- Executive Director of MTS-ISAC
- 20+ years Intel, Info Sharing, Cybersecurity
- USCG Cyber Command, Navy Cyber Defense Operations Command, Private Sector Maritime Stakeholders

Peter Lund
- VP of Product Management at Industrial Defender
- 15+ years of experience in IT and OT security
- Worked at KVH Industries
Agenda

- The Maritime Cyber Threat Landscape
- Potential Impacts of a Cyber Attack
- Information Technology vs. Operational Technology
- Emerging Cybersecurity Compliance Standards for Ports
- OT Cybersecurity Best Practices
- Recommendations & Key Takeaways
The Maritime Cyber Threat Landscape

**Actors**
- State level
- Criminal
- Insiders
- Activists

**Motivations**
- Political / Strategic
- Financial / Smuggling
- Revenge / Unintentional
- Ideological

**Objectives**
- Data, Information
- Funding source
- Smuggling
- Disrupt / Destroy
- Media / Attention
Potential Impacts of a Cyber Attack Against Maritime OT

Organizational
- Can place significant strain on multiple teams involved in operations, IT, customer service, etc. - this is an organizational challenge
- Financial and/or reputational impacts

Supply Chain
- Impacts to both upstream and downstream maritime stakeholders
- Intermodal disruptions as well as impacts to other critical infrastructure

Safety & Security
- Environmental / hazardous material incidents
- Availability and integrity of cranes, pumps, etc.
- Access controls – gates, CCTV, etc.
IT vs. OT Security: What’s the Difference?

♦ The goal of information technology (IT) security is to protect the confidentiality of data flowing between connected devices. IT devices include:

♦ Employee workstations
♦ Tablets
♦ Telecommunications equipment
♦ Servers in a data center

♦ The goal of operational technology (OT) security is to ensure the availability and integrity of systems that control physical processes. OT devices includes things like:

♦ Power systems
♦ Programmable logic controllers
♦ Cranes
♦ Building devices

♦ Because OT systems are different from traditional IT computing systems, you need to approach cybersecurity differently, too.

♦ More sensitive to intrusive security methods, like scanning
♦ Insecure by design - most devices have built-in remote access for vendors and third parties to perform maintenance
♦ Operate in real-time and can have physical consequences
Emerging Cybersecurity Compliance Standards

NVIC 01-20

ISPS

ENISA

Colonial Pipeline incident impacts—new regs will likely affect ports
OT Cybersecurity Best Practices

- It all starts with knowing **everything** about your devices, including:
  - Where they are
  - What’s on them
  - What they talk to
  - Who can access them
  - What their vulnerabilities are
  - What a healthy baseline looks like
How Do I Collect OT Asset Information?

ACTIVE

Agents

Pros:
- The most comprehensive data collection – identify anything
- Easy to manage centrally
- No credentials required

Cons:
- Requires installation and resources on the endpoint

Agentless/Native Querying

Pros:
- Second most comprehensive data collection method
- Leverages the same collection methods created by the device vendor
- Can be done from a centralized data collector

Cons:
- Requires routable connections to device and credentials
## How Do I Collect OT Asset Information?

### PASSIVE

<table>
<thead>
<tr>
<th>Offline Collection</th>
<th>Network Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros:</strong></td>
<td><strong>Pros:</strong></td>
</tr>
<tr>
<td>◇ Serial/air-gapped assets with no other way to get</td>
<td>◇ Quick to deploy if the infrastructure supports it</td>
</tr>
<tr>
<td>◇ If config file processed, still more accurate than spreadsheets</td>
<td>◇ Quickly find unknown IP based assets</td>
</tr>
<tr>
<td>◇ Only as good as last copy of config from device</td>
<td>◇ Threat Intel</td>
</tr>
<tr>
<td>◇ Manual work, but can be part of normal routine if planned correctly</td>
<td><strong>Cons:</strong></td>
</tr>
<tr>
<td></td>
<td>◇ Limited ability to collect data</td>
</tr>
<tr>
<td></td>
<td>◇ May require multiple sensors and SPAN/TAP/Mirror Ports in the target networks</td>
</tr>
<tr>
<td></td>
<td>◇ Not comprehensive enough for a compliance program or vulnerability management</td>
</tr>
</tbody>
</table>
What Else Is Important?

- Vulnerability identification and management
- Threat detection capabilities
- Visibility and monitoring of 3rd party maintenance actions
- Built-in compliance reporting for your standard
- Integration with existing cybersecurity infrastructure (SIEM, etc.)
Recommendations & Key Takeaways

Organizations should seek to manage risk across people, process and technology
- Appoint a named cybersecurity leader
- Align security strategy with business roadmap to promote safe, secure and resilient operations

Cyber hygiene controls are first step to reducing risk
- After that, detection of anomalous activity, threat hunting, and information sharing reduce ability for adversaries to "live" in networks and decrease risk of catastrophic cyberattacks

Third party / vendor risk management needs to improve
- Software inventory should include Software Bill of Materials (SBOM)
- Monitor third-party maintenance activity
- Information sharing can improve detection and response
Questions?