How’s Our Industrial Cybersecurity?
Ask OT!

Katherine Brocklehurst
Senior Director, Claroty

Gregory Villano
Superintendent, IACS
IACS Security Office
Cybersecurity Incident Response Team

SANS Oil & Gas Summit
October 2-3, 2018
From a Tonka forklift operator in 1975 to a part-time offshore OT cyber guy.....
Key Driver - Customer Requirements
Note to Self: This is a Trend (and should be...)

Thick Customer Requirements Document for ICS security

• "Hey Greg, we do all this, right?"

• Later, management understood the cyber risks in fleet and rigs 😊
Goal: Protect $700M offshore drilling vessels and crew from cyberthreats, internal and external
Project Complexity – Rigs, Vessels, Vendors, Applications

Thruster Control
Dynamic Positioning
Power Management
DrillingCntl. Systems
Blowout Preventer
Pre-Project Status

• No coherent policies/procedures in place for OT security
• No way to enforce the policies/procedures
• No visibility into OT cyber risks - multi-vendor assets, communications and networks on vessels
• No control over remote access to ICS and other assets on rigs or vessels by our guys or our vendors
• Not sure about what services or tools were available in market...

“Two Guys” to get it all done
Objectives and Drivers

• Increase safety of vessel and crew
• Fulfill Existing Contractual Requirements (= $funding)
• Zero impact on operations
• Provide compliance for anticipated regulations
• Create structure and training for OT cybersecurity
Cross-Functional Project Team

- Key - Led by OT
- Stakeholders to help drive requirements and approach
- Team Members
  - OT
  - Management
  - IT - “persuaded” to join
  - 3rd party vendors
  - Included physical security personnel
  - Decided as a team to create an OT SOC
Capabilities Needed

- Asset Inventory/Discovery
- 24/7 365 Monitoring – Immediate Visibility
  - Who’s doing what to what
  - Communications – Satellite
  - Context and Control
- Secure Remote Access – to control access for 3rd party/system vendors
- Configuration and Patch Management
  - PLC Firmware Upgrades
  - Stage patches to WSUS servers on vessel
- Real-time anomaly & threat detection/security intelligence and incident response
Not Everything is Russian Attackers

• Real-Time Monitoring:
  • Security Incidents
  • Process Integrity Issues
  • Operational Mistakes
  • Important/Risky Changes

• Consolidated Global View
• Validation/Testing/Training
Final Outcomes

- 55 Pages of Policies/Procedures
- Creation of Secure Operations Center in Houston
- Managed ICS Security Service
  - 24x7x365 on 5 ships around the globe
  - “Follow the sun” continuous monitoring solution
- Advanced Security Monitoring & Detection System
  - Real-Time Monitoring Console
  - Secure Remote Access (for Vendors)
Post-Project

- OT Cybertraining for vessel personnel
- Advanced 2-day training for electrical crews
- Tabletop exercises
- Red team attack of entire company

“Never Ending Story”
…This just in!

Thank You!

gvillano@moranshipping.com
Maritime Cybersecurity
Research Engineer
www.moranshipping.com