OmniSOC

The Higher Education & Research
Security Operations Center

Michael Simpson

- **CISO for ARF**
  - Leads OmniSOC's Virtual Cybersecurity Services Team for ARF
- Senior Security Analyst with OmniSOC
  - Over 20 years of experience in Higher Ed and Research
  - Nearly 15 years focused on Cybersecurity
- Staff member of Trusted CI, NSF Cybersecurity Center of Excellence

About OmniSOC

- Shared 24/7/365-capable cybersecurity operations center for research & higher education (R&E).
- Led by/located at/leverages IU: Data Centers, GlobalNOC, InfoSec team, HR, legal, office space, etc.
- Elastic is key technology partner.

Cyber-Threats to Science

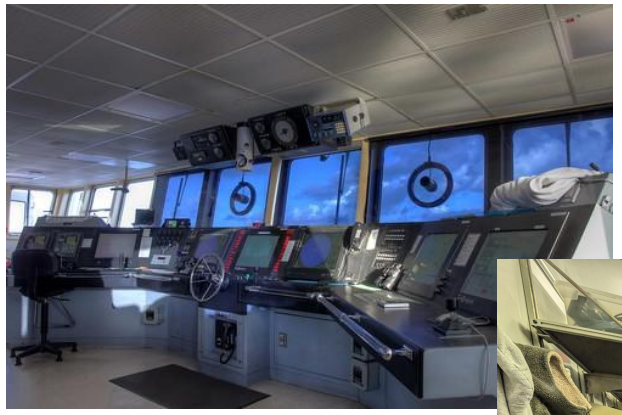
- ALMA - **No science done for nearly two months**
  - https://almascience.nrao.edu/news/alma-services-affected-by-cyberattack
- NOIRLab - **No science done for nearly two months**
  - https://noirlab.edu/public/announcements/ann23022/
- Both have had to rapidly make costly extensive changes to CI to fill the gaps in protections against attacks.

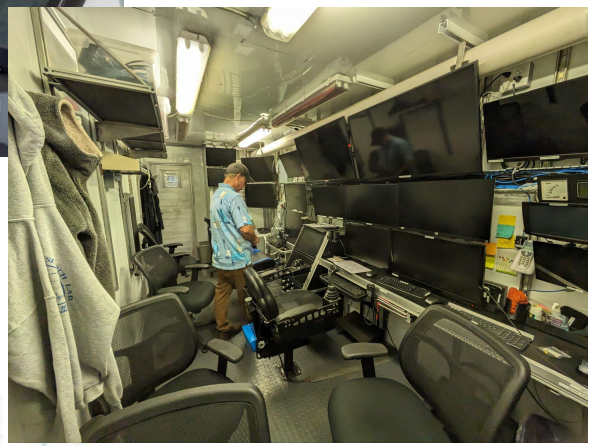
- The ships of the ARF are moving research facilities and have unique threats both physical and Cyber

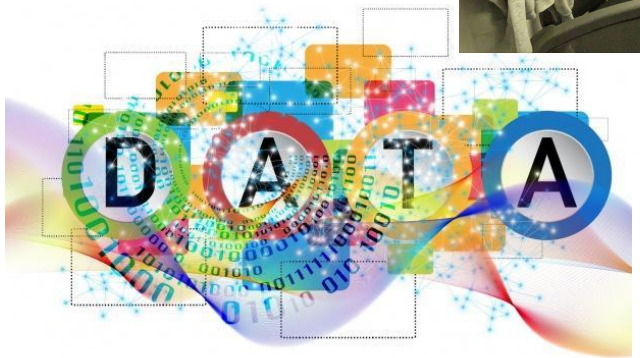
OmniSOC

Cybersecurity Enables Science

- Cybersecurity efforts Protect against threats to:
  - **Ship Operations**: safe and reliable operation of the vessel.
  - **The instruments and scientific systems** that collect and work with the data on the ships including connections between systems and back to shore.
  - **The integrity and availability of the data itself.**







OmniSOC

OmniSOC Services to ARF

- 24/7/365 Security Monitoring Capability
  - Available to ships and shoreside resources willing and able to send us monitoring data.
- Specific Security Technologies, including vulnerability scanning and honeypots
- ARF's Fleet-Wide Cybersecurity Team
  - CISO, Cybersecurity Analysts/Engineers, & Compliance Specialists
  - On-demand advice, consulting, security exercises, technology evaluation, and more
  - Contact us arfsec@iu.edu with any cybersecurity needs.

Ongoing ARF Security Activities:

- Compliance documentation guidance
  - Currently working with five operators on CRMP and POAM (LDEO, UH, BIOS, SIO, UW) including templates.
- Supporting the FortiNet Firewall and Networking project.
  - Consulting on cybersecurity matters
  - Setup monitoring of participating ships' networks through the hubs, and some security logs from the hubs' components.
  - **Most efficient way for OmniSOC to monitor ships' networks.**
  - Implementation assistance available.
- Deploying network honeypots on ships' networks.
  - These appear like real network services, but act as "door sensor" triggering an alarm if interacted with.
  - Once deployed, near zero tech time needed.
  - Deployed on ships at six operators (SIO, UAF, UW, URI, UMD, UH)
- Community Engagement:
  - Participate in CIWG
  - Presents at RVTEC Conference
  - Consult on cybersecurity and compliance:
    - Safer Seas Act
    - Observe inspections
    - Participate in training workshop

Contact Us

arfsec@iu.edu

OmniSOC