OmniSOC

The Higher Education & Research
Security Operations Center

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.
- Average volume across all members: > 16 TB/day; > 17.2 B events/day; > 200k EPS.
- Elastic is key technology partner.

Meet the team!

arfsec@iu.edu

OmniSOC

Continuing Projects:

- CRMP and compliance documentation
- Participating in the NextGen Firewall (NGFW) Project
  - Great opportunity to upgrade network security!
- Monitoring network data.
  - Added monitoring for two ships and one more soon thanks to NGFW
  - Corelight NIDS and OmniSOC Data Aggregators
- Deploying STINGARv2 Honeypots
  - 7 ships have them deployed, soon to be eight.
  - VMs or Raspberry Pi available
  - We can help with deployment
- External Network Vulnerability Scanning

Continuing Projects (cont.):

- Attend ship inspections:
    - Endeavor
    - Thomas Thompson
- Ship and facility visits

New Projects This Year:

- Incident Response (IR) Policy & Procedures
  - Review existing
  - Work with you to create new
  - All ship operators should have them!
- Cyber-Incident Drills
  - Test IR Policies and Procedures
  - Prepare for the cyber-incident that will come.
  - Training on Friday

Community Engagement

- Consults and Participates with:
  - CIWG
  - SatNAG
  - HiSeasNet
  - NextGen Firewall (NGFW) Project
- Participates at RVTEC Conference
- Attend UNOLS Council Meetings
- Participated on the training cruise on the Sikuliaq

OmniSOC

Thank you for your attention.

Questions?

arfsec@iu.edu

OmniSOC

omnisoc.iu.edu