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.

ResearchSOC

- Previously an NSF funded project, became part of OmniSOC as part of sustainability plan.
- Bundle of OmniSOC services specially suited for research projects and facilities.
- In addition ARF has a Virtual CISO, and Virtual Cybersecurity Services (VCS) team.

Meet the team!

arfsec@iu.edu

OmniSOC

Projects:

- Cybersecurity risk management
  - CRMP documentation
  - IR Policy / Procedures
- Monitoring network data.
  - Marlink feed covers most of the ships.
  - Corelight NIDS and OmniSOC Data Aggregators at a few operators.
    - We would really like to add more.
- Deploying STINGARv2 Honeypots
  - Two ships have them deployed.
  - VMs or Raspberry Pi
- Participating in the Fleet FortiNet firewall/network project
  - Great opportunity to upgrade network security!
  - We'll hear more about this later.

Cyber-Infrastructure Working Group (CIWG)

- Attend and participate! We have a great bunch of people, but we can always use more!
- Hear about projects and discuss solutions to challenges!
- Find help and resources.

OmniSOC

Thank you for your attention.

Questions?

arfsec@iu.edu

OmniSOC

omnisoc.iu.edu