
OmniSOC
The Higher Education & Research
Security Operations Center

Meet the team!




arfsec@iu.edu

OmniSOC

Mike Simpson

- **CISO for ARF**
- Senior Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - Cybersecurity Program Development & Strategy
  - Network Security
  - Digital Forensics
  - Network Penetration Testing
  - Physical Security

arfsec@iu.edu

OmniSOC

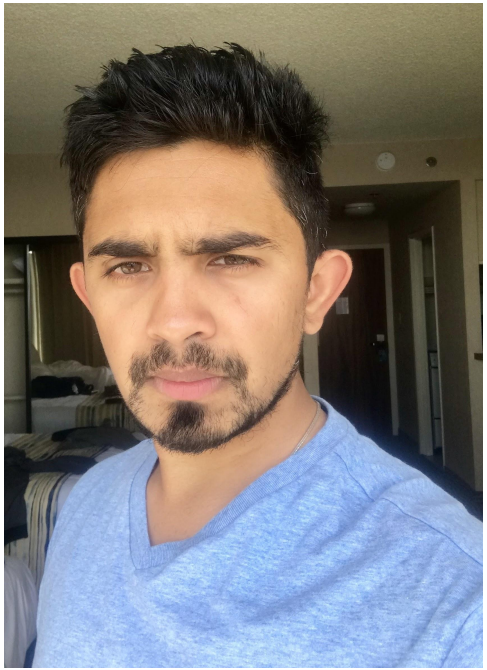
Mikeal Jones

- **Deputy CISO for ARF**
- **Leads CRMP / Compliance Documentation initiative**
- Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - IT Operational Strategy
  - Cybersecurity
  - Systems Architect + Admin

arfsec@iu.edu

OmniSOC

Ishan Abhinit



- **Leads Incident Response policy and procedures initiative**
- Senior Security Analyst at IU CACR
- 12+ years of experience in IT
- Masters degree in Cybersecurity
- Areas of expertise:
  - Cybersecurity Program Development & Strategy
  - Security Log Analysis

arfsec@iu.edu

OmniSOC

Vishal Bhardvaj

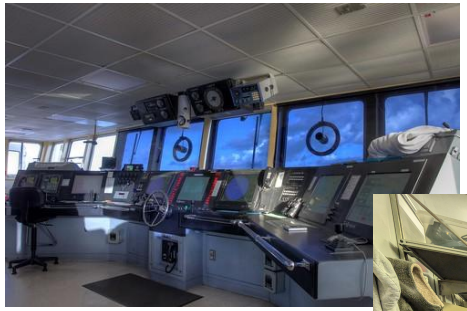
- Security Analyst at OmniSOC
- 10+ years of experience in IT
- Master of Science in Cybersecurity
- Areas of expertise:
  - Windows software development
  - Macintosh data recovery
  - Telecommunications (2G, 3G, 4G)

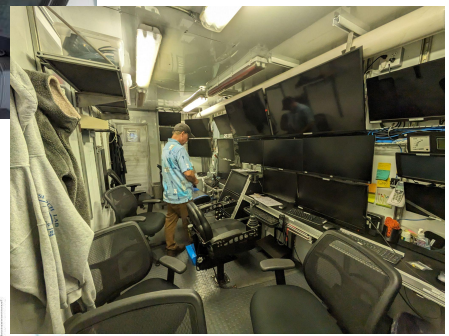
arfsec@iu.edu

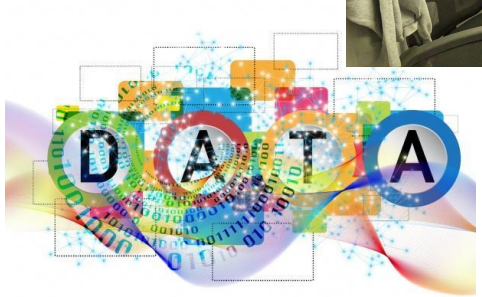
OmniSOC

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

Continuing Projects:

- CRMP and compliance documentation
- 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.
- Participating in the NextGen Firewall (NGFW) Project
  - Great opportunity to upgrade network security!
- Monitoring network data.
  - From NGFW
  - Corelight NIDS and OmniSOC Data Aggregators

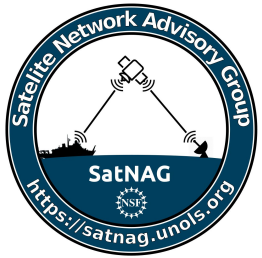
Continuing Projects (cont.):

- Deploying Forwarned STINGARv2 Honeypots
  - 8 ships have them deployed.
  - VMs or Raspberry Pi available
  - We can help with deployment
- External Network Vulnerability Scanning
- Attend ship inspections:
  - Sproul
  - Sharp
- Ship and facility visits
- **All of OmniSOC's services are already paid for and do not affect your day rate.**

OmniSOC

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 cruises on the Sikuliaq



OmniSOC

NextGen Firewall (NGFW) Project:

- In production phase
  - No longer in beta, but refinements continue to be made
- 7 ship have FortiGates and FortiAnalyzers deployed
- 3 additional ships are in the process of scheduling their deployment.
- Allows OmniSOC to monitor network traffic

OmniSOC

Use of End of Life OS and/or Software:

- Reasons:
  - OT or Science system has software that requires a fixed or out dated OS version.
  - Upgrading is prohibitively expensive or the upgrade does not exist..
- Risks - Overall increase over time.
  - **Often no security updates and known exploits**, increase likelihood of successful attack leading to spread of compromise and losing functionality, operational time, and data.
  - **Increasing difficulties integrating with systems** running up to date software. Outdated data formats may require conversation.
  - **Delays in detecting attacks or problems.**
  - **Possible increase in legal liability** and/or repercussions in case of an incident.
  - **Increased operational and maintenance costs:** spare parts or copies of the software may have to come from alternative sources or specially made. Operating the system around lack of integration or mitigation controls takes more time.

OmniSOC

Use of End of Life OS and/or Software:

- Response:
  - Plan for replacement or upgrade. Easier said than done, but often the most effective.
  - Mitigate risks while working toward replacement or upgrade.
    - Air gap or severally limit network access, both internal networks and Internet access.
    - Increase monitoring of the EoL system. May require regular manual interactions.
    - Increase the hardening of the system. Security controls needed may make operation of the system less efficient.
  - Work towards upgrading or replacement as quickly as possible.

OmniSOC

OmniSOC

Thank you for your attention.

Questions?

arfsec@iu.edu


OmniSOC
omnisoc.iu.edu