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

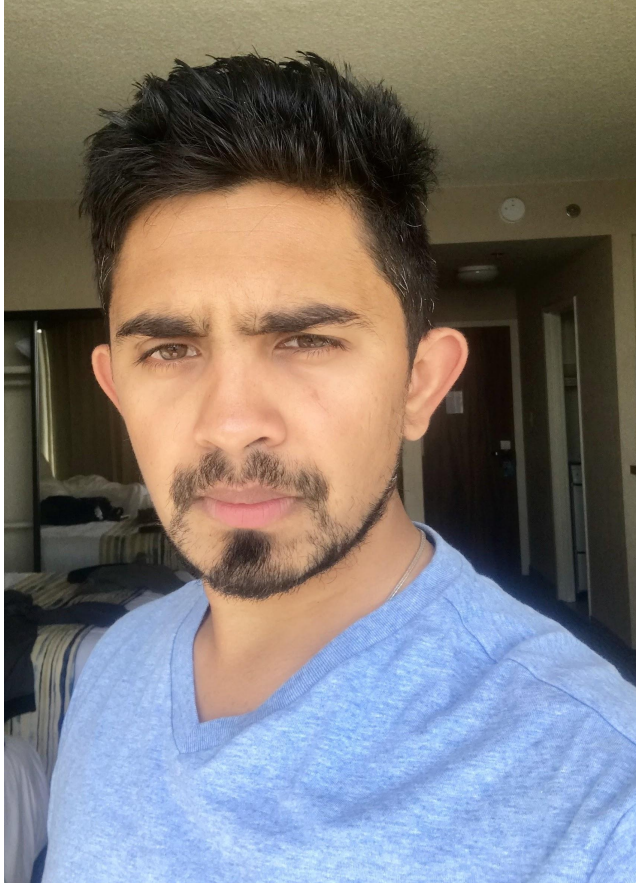# arfsec@iu.edu

OmniSOC

Mikeal Jones

- **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

Chris Lauderbaugh

- Security Analyst at OmniSOC
- 10+ years of experience in IT/Cybersecurity
- Worked in the medical and defense industries before joining OmniSOC
- Areas of expertise:
  - Digital Forensics
  - Cybersecurity Intelligence

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.**
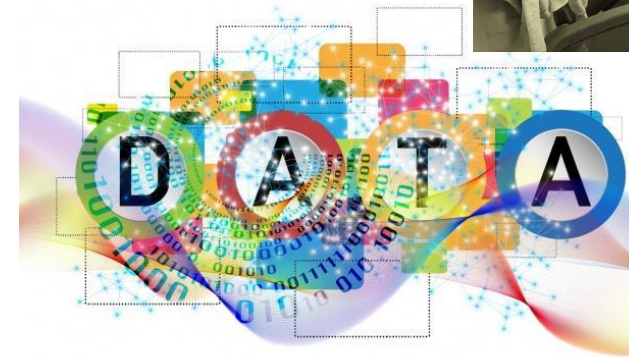
OmniSOC

Continuing Projects:

- CRMP and compliance documentation
- 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

OmniSOC

Continuing Projects (cont.):

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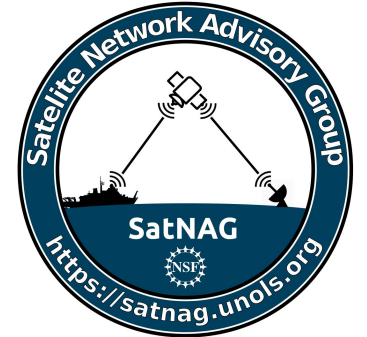
OmniSOC

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.

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 and in two weeks the Endeavor

2024 OmniSOC Activities Report

- Overview of activities and high level metrics
- No "dirty laundry"
- Review and comment on draft:
  - Starting 2024-12-02
  - Ending 2024-12-11
  - Only ARF members may review
  - Request access: arfsec@iu.edu
- Available to any ARF member upon request
- Made available to NSF 2024-12-13

OmniSOC

OmniSOC

Thank you for your attention.
Questions?

arfsec@iu.edu

OmniSOC

omnisoc.iu.edu