
OmniSOC

What are we defending against?

We have data on what attackers do.

Verizon Data Breach Investigation Report (DBIR)

www.verizon.com/business/resources/reports/dbir/

There’s something weird about a distributed organization’s cybersecurity team

14 institutions, 17 vessels. Lots of variety. Our strategy:

- Build out and provide core cybersecurity capabilities for the fleet.
- Contribute to and advise on fleet-wide efforts via the CIWG and other bodies.
- Consult with operators to make local improvements.

Security Monitoring

Corelight Deployments

- SIO & UAF - Platform Engineering signed off on feed, ready for analyst use.
- R/V Thomas Thompson - Delayed due to networking and staff availability issues. Working with Corelight to resolve issues.

Marlink Feed

- Analysts have been using this, however utility is limited.
- Very difficult to develop significant confidence in investigations against this data.

Network Honeypots

Supporting infrastructure @ OmniSOC built and deployed.

Built network sensors to be ”touch-free”

Currently testing the builds for ships.

Expect to begin deploying this quarter.

Communications Planning

- Each operator gets a security mail list.
- OmniSOC uses the appropriate list for security communications to each operator.
- Content example: monthly vulnerability scan reports
- Step 0 for incident response planning.

1Q2023 Inspection Prep & CRMP

ARF CRMP Template complete

Completed SIO CRMP, cleared an NCR

Currently working with UAF (Sikuliaq) BIOS+ASU (Atlantic Explorer), UW (Thompson, Carson) to complete next CRMPs.

Upcoming

1. Firewalls
    a. Testing security monitoring with Fortinet's solutions
    b. Assisting & advising CIWG, SATNAG, & Firewalls Groups.
2. Incident Response
    a. IR plan template
    b. IR plan development assistance
    c. Security exercises to test & improve
3. Honeypots
    a. Finish testing
    b. Ship network sensors to initial sites.

Incident Response Planning

“What do we do when we find out we have a cybersecurity incident?”

1. Communications paths
2. Roles & Responsibilities
3. Process
4. Interactions with other entities

Information Asset Classification

The shortcut to figuring out the appropriate way to handle data?

Put like things together in the same bucket.

Can be simple (sensitive/non-sensitive) or complex (CUI).

Goal: as simple as possible without leaving anything important out.

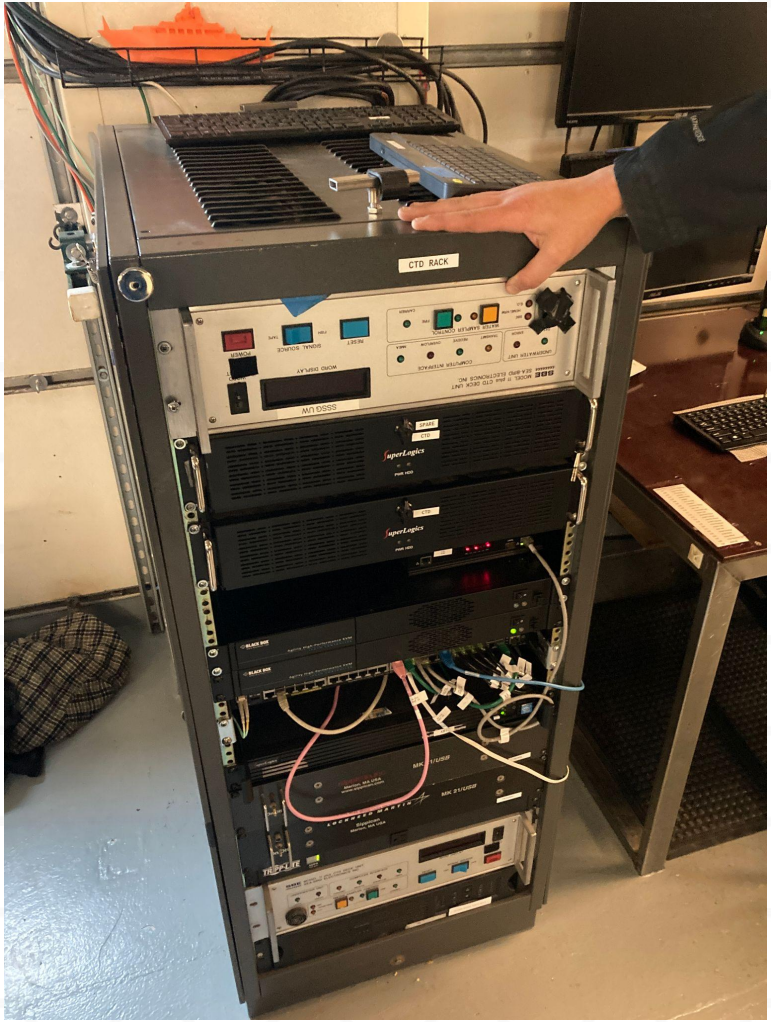
CIWG Monthly

Cyberinfrastructure Working Group

Monthly calls to include operators in discussions.

Next one is next Tuesday at 1400 Eastern / 1300 Central / 1100 Pacific / 900 Hawaii

Contact me if you'd like to attend: rlkiser@iu.edu


CTD RACK
SuperLogics
SuperLogics
TRIPP-LITE


BLUE HERON
Large Lakes Observatory
University of Minnesota Duluth

Five easy to-dos:

Basics can go a long way.

1. Don’t reuse passwords - use a password manager like 1password.
2. Apply software updates (before coming aboard)
3. Turn on multifactor authentication on accounts

Contact us!

Ryan Kiser - rlkiser@iu.edu

ARF Security Team - arfsec@iu.edu