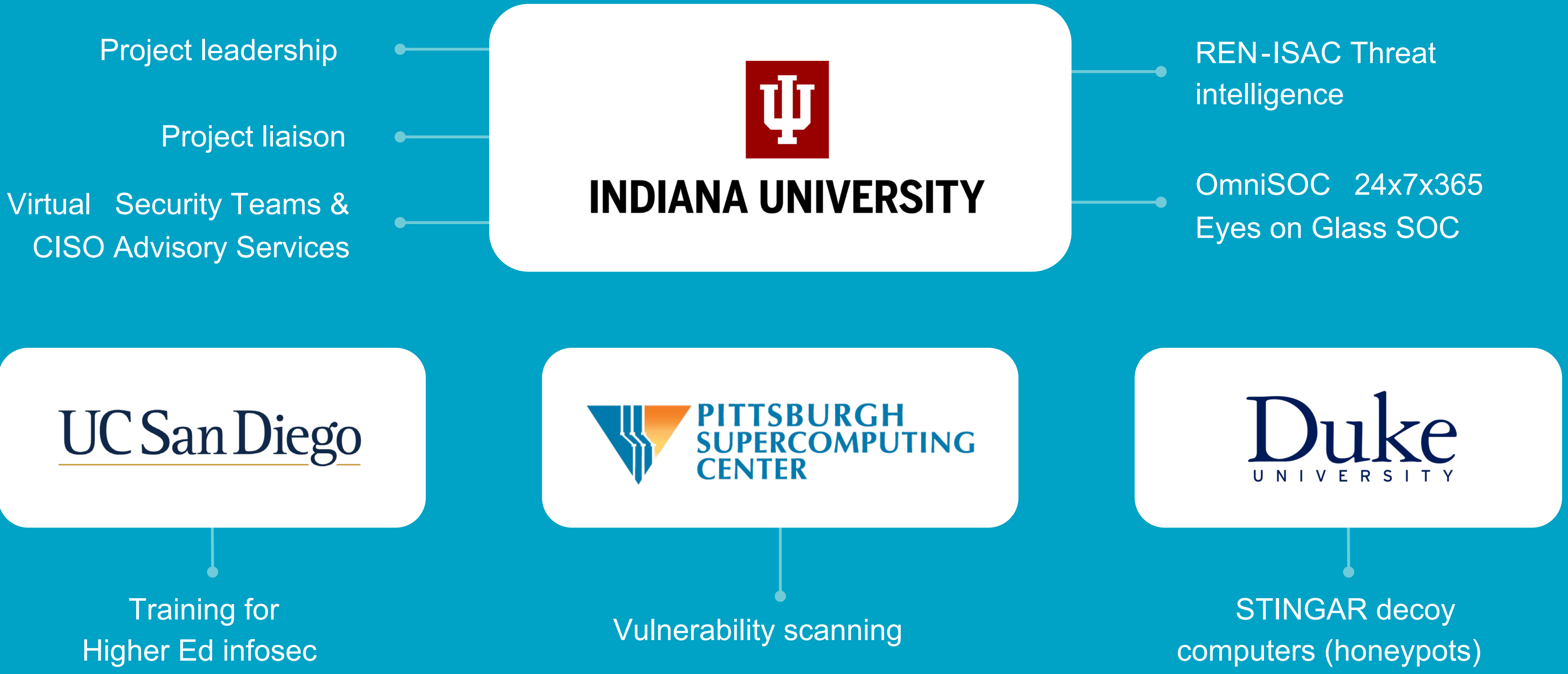
ResearchSOC

researchsoc.iu.edu

Who is ResearchSOC?



INDIANA UNIVERSITY

Project leadership

Project liaison

Virtual Security Teams &
CISO Advisory Services

REN-ISAC Threat
intelligence

OmniSOC 24x7x365
Eyes on Glass SOC

UC San Diego

Training for
Higher Ed infosec

PITTSBURGH SUPERCOMPUTING CENTER

Vulnerability scanning

Duke UNIVERSITY

STINGAR decoy
computers (honeypots)

ResearchSOC complements Trusted CI

ResearchSOC - focused on operations & services

- Operational services and related training for NSF CI
- Threat Intelligence Network and Community of Practice
- Enabling cybersecurity research
- Outreach to Higher Ed Infosec regarding research CI

Trusted CI - focused on programs & community

- Creating comprehensive cybersecurity programs
- Community building and leadership
- Understanding specific challenges of software assurance, privacy, etc.
- Training and best practices

About OmniSOC

- Shared cybersecurity operations center for research & higher education (R&E).
- Founded June 2017 by 5 Big 10AA schools. Operational February 2018.
- NSF MF customers include NRAO, Gemini, and GAGE
- Average 7 TB data daily from 17 feeds
- 2.7 PB data & 4.65 trillion events since inception
- Elastic is key tech partner

OmniSOC:

- Is higher ed & research’s only collaborative multi -state institution security operations center.
- Is the only collaborative SOC supporting NSF research.
- Is the only SOC with a multi -state institution data sharing agreement for researchers.
- Has #1 Higher Ed threat hunting team in the country.

The strategy

A targeted combination of technologies and services to support scientific research and education

OmniSOC
+
Three Rivers Optical Exchange
+
STINGAR
+
Virtual Teams & CISO Advisory

Science focused

Tuning
+
Tailoring
+
Training

ResearchSOC

Where we started

- Providing 24/7/365 eyes -on -glass SOC services to NSF Major Facilities.
- Integrating honeypots and vulnerability scans into network and other SOC feeds.
- Personalized support to help each facility onboard and collect the right data to make monitoring effective.

Where we’re going

- Expanding our new Virtual Cybersecurity Services options to ensure that clients have support in handling whatever comes next
- Working with researchers who can push the edges of information security practice using our data
- Experimenting with new technologies and practices to enhance our services to clients, and intelligence we can share with the broader community
- Bringing these services to as many scientific facilities as possible

The Plan

Staff

0.5 FTE vCISO + 1.0 FTE security team
Emergency “Red Phone” team

Services

ResearchSOC Core Services

Infrastructure

Security monitoring appliances for datacenter, ground station, and testing

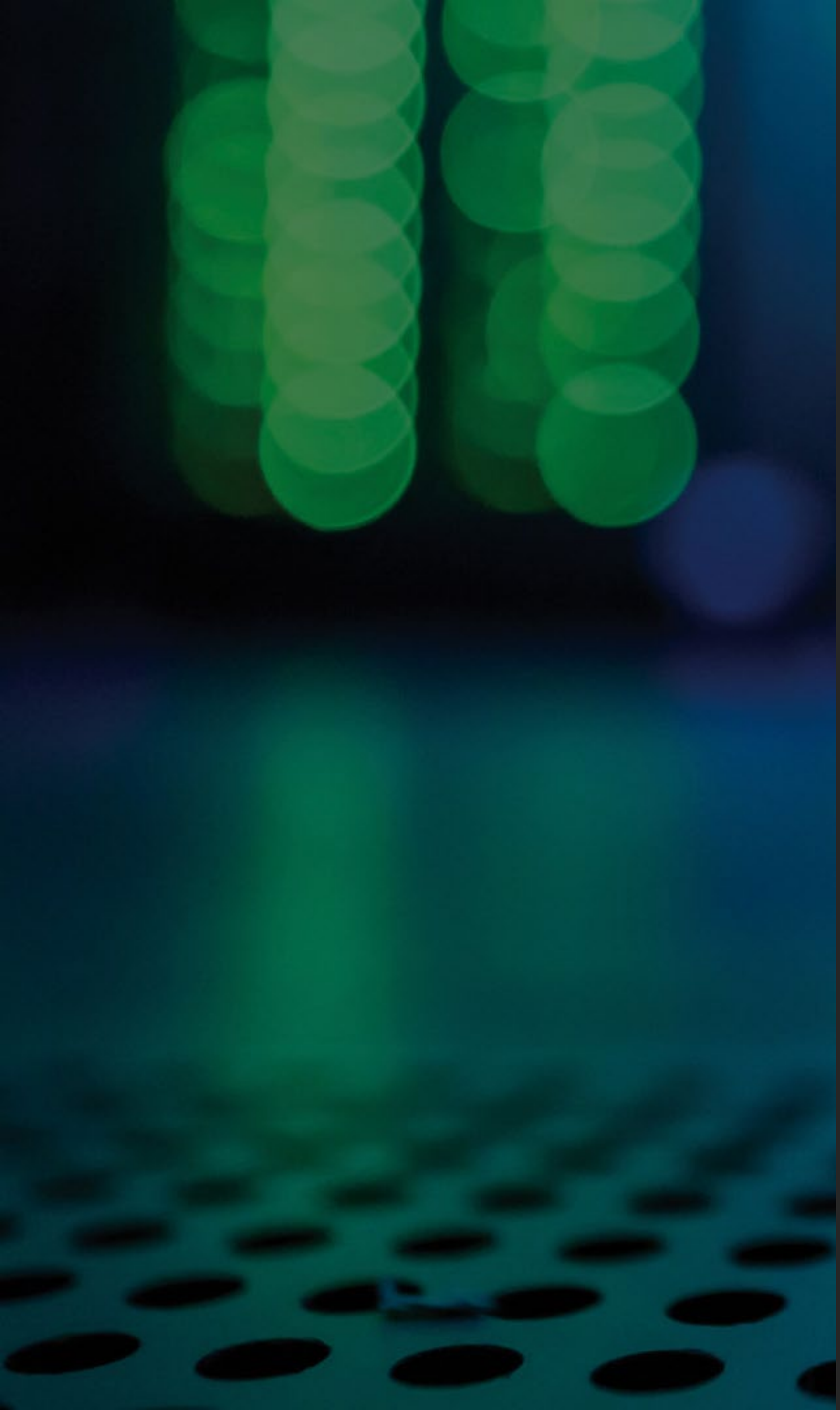
The Plan

Year 1

1. Establish basic monitoring and integrate services
2. Experiment with security architecture for the fleet
3. Familiarize ResearchSOC staff with ARF
4. Build program fundamentals

Year 2

1. Take lessons learned from year 1 about ship operations and integrate
2. Focus on security and ship architecture



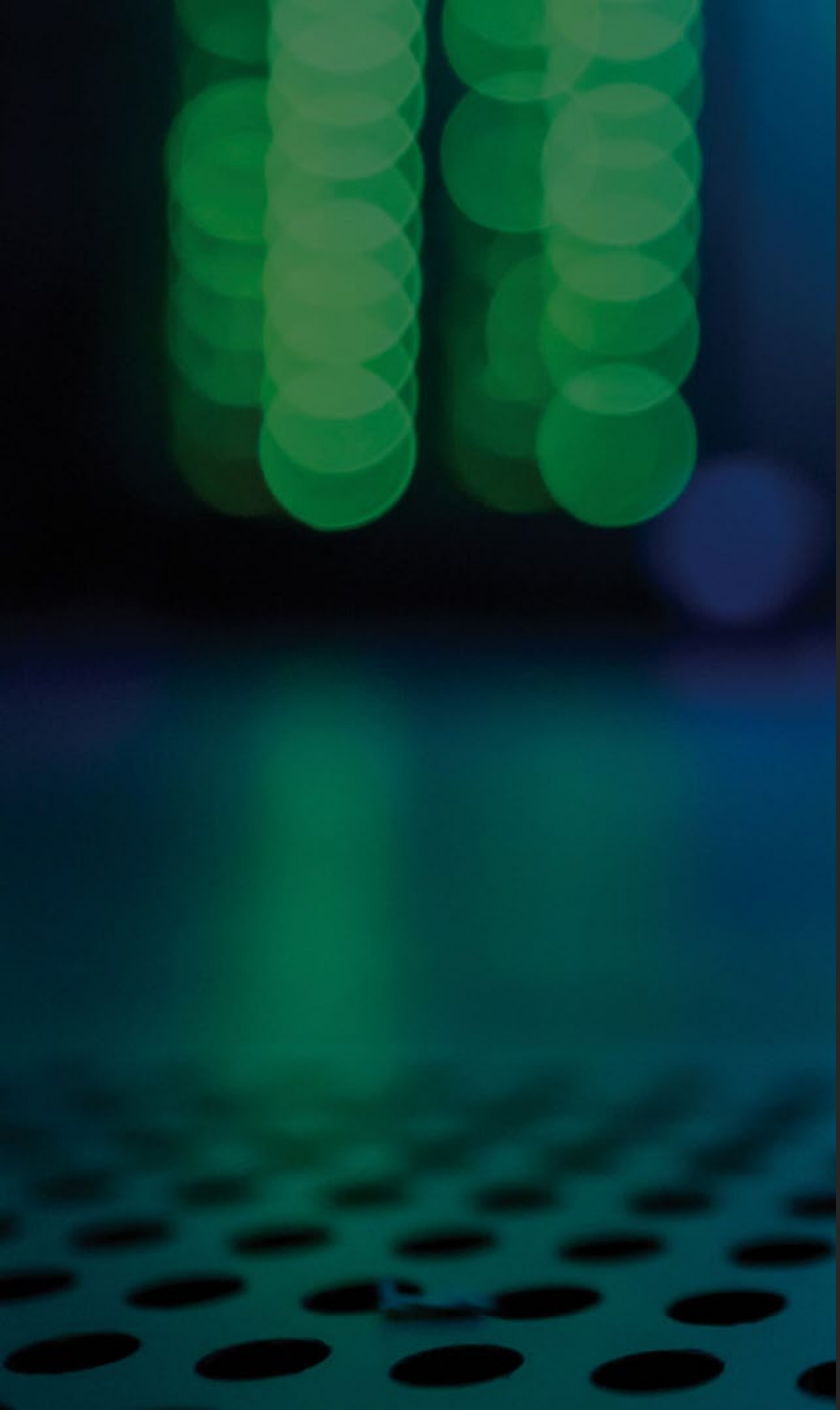
ResearchSOC

Thank you

Ryan Kiser, Senior Security Analyst

rlkiser@iu.edu

researchsoc.iu.edu



ResearchSOC

Contact us

researchsoc.iu.edu

rsoc@iu.edu

The ResearchSOC is supported by the National Science Foundation under Grant 1840034. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.