Today’s webinar topic is “Securing Scientific Cyberinfrastructure: The Research Security Operations Center (ResearchSOC)” with Von Welch and the ResearchSOC leadership team. Our host is Jeannette Dopheide.

The meeting will begin shortly. Participants are muted. Click the Chat button to open the chat view and ask a question.

This meeting will be recorded.

The Trusted CI Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
Securing Scientific Cyberinfrastructure

Research Security Operations Center
The NSF Collaborative Security Response Center

Von Welch
Michael Corn
Susan Sons
Inna Kouper
Jim Marsteller
Richard Biever

Trusted CI Webinar
January 28, 2019
The ResearchSOC Team

Andrew Adams (PSC), Rich Angeletti (PSC), Ed Balas (IU), Richard Biever (Duke), Jesse Bowling (Duke), Cyd Burrows-Schilling (UCSD), Mary Conley (IU), Michael Corn (UCSD), Tom Davis (IU), Inna Kouper (IU), Mark Krenz (IU), Jim Marsteller (PSC), Scott Orr (IU), Sameer Patil (IU), Chris Rapier (PSC), Mike Stanfield (IU), Zalak Shah (IU), Susan Sons (IU), Todd Stone (IU), Von Welch (IU)

Funded by NSF Grant 1840034.
A Story About a Science Project

A fictional project, but a common and too real story.
And a Principal Investigator, Maria

Maria is reading about cybersecurity incidents and risks.
She is Concerned about Data Integrity...
And about the availability of her instrument

Eco-loons hack Thirty Meter Telescope website to help the 'natives'

Search for little green men finds them rather close to home

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

By Nicolas Perpitch
Updated 17 Oct 2017, 3:44am

Video: In a galaxy 130 million light-years away, two neutron stars collide (ABC News)
And Protecting Embargoed Announcements

Gravitational-Wave Announcement Coming on Oct. 16: What Could It Be?

By Calla Cofield, Space.com Senior Writer | October 5, 2017 07:00am ET

Get all the latest amazing astronomy pictures! Subscribe to Space.com.

Members of the LIGO team (from left to right): David Shoemaker, Rainer Weiss, Matthew Evans, Erotokritos Katsavounidis, Nergis Mavalvala and Peter Fritschel. Rainer Weiss stated on Oct. 3, 2017 that the LIGO collaboration will make an exciting announcement on Oct. 16.

Credit: Bryce Vickmark/MIT
And random attacks on her computers....
Maria turns to John, her IT lead, and asks for a cybersecurity risk management plan.
John finds help!

Using Trusted CI guidance, John is able to work with his team to develop a cybersecurity program for their project.
John turns to Lucy...

Lucy is the project’s network engineer.

John asks Lucy to install an intrusion detection system.
Lucy installs an intrusion detection system...

Lucy researches open source IDS systems, selects one, buys a computer system to run the IDS, and installs it.
Lucy feeds data from her network to the IDS...

After much reading of documentation and experimentation.
And Lucy turns on the IDS...
Lucy tunes the IDS...

Lucy learns how to program the IDS to ignore odd project traffic: e.g. SCADA, data downloads, remote access.

It takes lots of time to learn what traffic is normal.

And how to program the IDS.

And to experiment to get the IDS settings right.
False Alarms...

Lucy works to get the number of false alarms from the IDS down.
24x7?

The IDS needs to run 24x7.

But false alarms in the middle of the night quickly get old.
Hmmmmm....

Lucy gets an alert that looks strange.

It’s a real incident! The main data server for the project is mining cryptocurrency!
Now What?!
Responding

John and Lucy take the data server offline. They realize they should let the scientists know what is going on and send an email. They start fixing the system.
Meanwhile, Maria has been on a plane...

Maria, the PI, lands and gets a phone call.

“Hi Maria, this is Joe Reporter from Science Magazine, I hear your data server has been hacked?”

“Uh, I’ll have to call you back.”

We’ll leave our story here...
Incident Response for Science Challenges

Cyberinfrastructure is More Diverse

Credit: Chris Coleman, School of Computing, University of Utah
Scale of Science: Large Autonomous Facilities to...

- Large Synoptic Survey Telescope (LSST)
- IceCube
- Gemini
- LIGO
...Small-to-medium embedded projects
Cyberinfrastructure is Highly Collaborative

[Diagram showing various network connections and bandwidths (100 Gb/s, 40 Gb/s, 30 Gb/s, 10 Gb/s)]
Detecting and Handling Cybersecurity Intrusions Requires Specialized Skills

US lawmakers introduce bill to fight cybersecurity workforce shortage

Report claims US public and private sectors had over 300,000 cybersecurity-related job openings between April 2017 and March 2018.

- Network engineering
- IDS administration
- Threat intelligence
- Incident response
- 24x7

The ResearchSOC Strategy
ResearchSOC Goal

Serve as a Collaborative Security Response Center whose expertise and resources are leveraged by the entire research and education community to:

1. Improve the cybersecurity posture of scientific cyberinfrastructure, and

2. Raise awareness of security threats facing the scientific community.
Tuning, Tailoring, and Training for Science
ResearchSOC Approach to Tackle...

Scale of Science: Large Autonomous Facilities to...

Large Synoptic Survey Telescope (LSST)

IceCube

Gemini

LIGO
- Process and Create Cyber Threat Intelligence
- Notify Member Incident Response Teams
- Communicate and Share Information
- Conduct Proactive Threat Hunting
- Analyze Security Events
- Monitor and Triage Security Events
- Provide Call Center Services
“Security teams continually strive to identify and mitigate all vulnerabilities in order to maintain a strong security posture...”
“An attacker only needs to find one to exploit...”
Vulnerability Identification Service at the
Three Rivers Optical Exchange (3ROX)

R&E networks are under constant scanning by malicious actors attempting to identify and subsequently exploit CI vulnerabilities – weaknesses that can be exploited by an attacker to perform unauthorized actions.

• Built upon Three Rivers Optical Exchange (3ROX) Cybersecurity Service

• Based on ‘OpenVAS’ framework - Full Featured vulnerability scanner. Daily updates with over 50,000 vulnerability tests.
Vulnerability Identification Service

Probes externally from your network

Identifies:

- Misconfigured software
- Exploitable software
- Unnecessary services/exposed devices
Vulnerability Identification Service

- Initial ‘discovery’ scan to enumerate network connected assets
- Scheduled scanning
- On demand scanning
ResearchSOC Approach to Tackle...

...Small-to-medium embedded projects
Threat Intelligence - STINGAR

Shared Threat Intelligence for Network Gatekeeping with Automated Response
Attacking methodology

1. **Reconnaissance**
   - Scan for EternalBlue
2. **Exploit**
   - Access system and steal password hashes
3. **Maintain**
   - Create account or take over admin account
4. **Extend**
   - Attack more computers

It only takes 1 computer or account to give an attacker access
Identifying threats to protect your network

Sharing Threat Intelligence for Network Gatekeeping with Automated Response

• Make use of:
  • Network sensors
  • Network metadata system logs files

• To identify:
  • Attackers
  • Compromised machines and accounts

• AND block:
  • Via network security appliances in place

• AND share:
  • Threat intelligence with other groups
STINGAR in the enterprise

Data collected near-real time

Analysis occurs between 1 min (most sources) and 5 min (network flow data)

Block lists generated every 3 minutes

Sensor Data Aggregator
- Syslog services
- Honeypot data
- NetFlow captures
- DenyHosts data
- IDS data

Threat Analyzer

Threat Repository

Block lists generated every 3 minutes

Honeypot

Normal
Data
Attack
Control

Data flows to
Network Firewall insertion
Host Firewall insertion
Network Firewall insertion
“Black hole” routing
IPS insertion

Planned
< 3 seconds
30 min
Impact: alert data

- In 2016, began blocking on Threat Intelligence from external sources
- At the same time, we began blocking based off internally developed intelligence
- The result was less “noise” in the industry tools for analysts to sift through
Measuring impact across institutions
STINGAR and RSOC

- Deploy sensors (honeypots) to identify malicious traffic
- Information fed to RSOC and lab for active response (blocking) and correlation with vulnerable scan information
- Participation in active threat intelligence sharing community to benefit from what other institutions see
Building A CI Threat Intelligence Network

CyberInfrastructure Threat Intelligence Network

Other sources
• SCADA Threats
• Community Contributions
• Trusted CI
• ...

NSF CI Community

ResearchSOC
OmniSOC
STINGAR
3ROX
ResearchSOC Approach to Tackle...

Cyberinfrastructure is Highly Collaborative
Improve Security Practice by Enabling Research

- Intrusion detection and prevention
- Network and threat analysis
- Security and privacy policies
ResearchSOC Strategy

• Survey the needs of cybersecurity researchers

• Curate and document the needed data

• Re-use existing solutions to provide secure access to data

• Build awareness of the data and its potential
Researcher Needs and Access Timeline

- **Spring 2019**: Pilot Interviews
- **Fall 2019**: Surveys / Interviews
- **Spring 2020**: Student Engagement Workshop
- **Spring 2021**: Researcher Engagement Workshop
Intrusion Detection Requires Specialized Skills

US lawmakers introduce bill to fight cybersecurity workforce shortage

Report claims US public and private sectors had over 300,000 cybersecurity-related job openings between April 2017 and March 2018.
Approach #1: Enable Higher Education Information Security Offices to Serve Research

College and university information security offices (ISOs) are challenged in their understanding of the specialized needs of research projects. ResearchSOC will reach out to ISOs to educate them on the motivations and techniques for engaging with and protecting research projects on their campuses.

https://events.educause.edu/security-professionals-conference/2019

Look for ResearchSOC at EDUCAUSE SPC 2019!
Classical Enterprise Security vs. Research Support

1. Inventory your environment
2. Write policies
3. Impose Controls

1. Understand the Science Workflow
2. Understand the issues such as reproducibility, data sharing, federation
3. Recognize and embrace research culture in Higher Ed
4. Talk to Faculty

Research CI are custom built cars
ResearchSOC Workshops

- Annual 4 day Workshops (in lovely San Diego)
- Conference aligned workshops (starting May 11th at Educause SPC)
- Supporting participants ala Research Facilitator community
- Targeting CISO’s, Security Architects, and Security professionals that support researchers

Sample Curriculum

- Day 1: Overview of sponsored programs (how research projects work); facilitation training
- Days 2-3: Table top security plan development with actual PIs
- Day 4: Review and develop artifacts and collaborative support

https://events.educause.edu/security-professionals-conference/2019
Approach #2: Build a Community of Research Cybersecurity Practitioners

Enterprise Participation Home

Background

REN-ISAC membership guidelines are under-going some changes. For many years, we’ve had to turn away Member Representative nominees who did not meet our criteria for operational security. Given the evolving nature of information security, it has become clear that REN-ISAC needs to involve the talents of colleagues who don’t necessarily manage defensive systems or provide incident response. Information security requires planning, policy, training, support & communications, compliance, risk assessment, and much more. That’s why we are rolling out Enterprise Participation, or EP. But don’t worry -- we aren’t throwing out our previous guidelines. We’re simply making room for security practitioners who don’t meet our traditional focus on operational security.
Timeline and Initial Clients

- **2019**
  - Project start
  - Development of tech and contracts; outreach to InfoSec and Researchers

- **2020**
  - Beta Testing

- **2021**
  - Sustainability and for-fee services
For More Information

rsoc@iu.edu
https://researchsoc.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.

Thank you to pexels.com for images.
Questions?
Please take our survey
About the Trusted CI Webinar series

To view presentations, join the discuss mailing list, or submit requests to present, visit: https://trustedci.org/webinars

The next webinar is February 25th at 11am Eastern.
Topic: Anticipatory Cyber Defense via Predictive Analytics, Machine Learning and Simulation
Speaker: Shanchieh (Jay) Yang