NSF Cybersecurity Summit 2019 presentation proposal: ResearchSOC: Cybersecurity for NSF Major Facilities Update

Title: ResearchSOC: Cybersecurity services for NSF Major Facilities--Update

Organization presenting:
The Research Security Operations Center (ResearchSOC) Award #1840034

Presenter: Susan Sons, Deputy Director, the Research Security Operations Center (ResearchSOC)

Time: 30 minutes

Abstract/Description

The National Science Foundation has invested over $7B in scientific research projects, and those projects lead the world in providing opportunities for scientific discoveries. Yet this investment and leadership are at risk, threatened by cyberattacks from malicious technology actors, some foreign-sponsored and some rogue with no agenda other than maliciousness. These projects operate in a collaborative, international, and open nature of scientific research and the projects' highly specialized instruments and high performance computing resources require an approach different than that taken to secure business or government enterprises. To successfully defend NSF research against today's evolving cyber threats, cybersecurity professionals must act differently.

This presentation will educate projects on how they can plan to utilize the capabilities of the Research Security Operations Center (ResearchSOC). Research SOC provides new operational services to address the cybersecurity threat to NSF projects, improve the overall cybersecurity posture of NSF projects, and educate program professionals and the larger research and education community on effective methods of ensuring data integrity, instrument availability, and secure research access.

Through an NSF grant funded effort involving Indiana University, Duke University, Pittsburgh Supercomputing Center and University of California San Diego, the Research Security Operations Center (RSOC) has been established to provide operational cybersecurity services for autonomous projects, including proactive threat hunting, security event monitoring and analysis, vulnerability scanning, and threat intelligence sharing.

1. Institute a community of practice and network of threat intelligence, fed by the ResearchSOC and collaborators, aggregating and disseminating tactical information and knowledge to allow for effective defense.
2. Provide outreach and training to the higher education information security community to better support embedded CI projects that don't have the independence and resources to take advantage of cybersecurity services.

3. Engage with the cybersecurity research community to advance research using the data from the ResearchSOC.

The Research Security Operations Center (ResearchSOC), launched in 2018, is a collaborative security response center that addresses the unique cybersecurity concerns of the research community. ResearchSOC helps make scientific computing resilient to cyberattacks and capable of supporting trustworthy, productive research.

The ResearchSOC does so by providing a suite of operational cybersecurity services, training, and information sharing necessary to a community as unique and variable as research and education. These services and trainings include:

OmniSOC: With two decades of experience from the GlobalNOC behind it, OmniSOC is a 24x7x365 eyes-on-glass security operations center that provides trusted and actionable intelligence to higher education institutions. GlobalNOC is based at Indiana University.

Vulnerability Identification Service at the Three Rivers Optical Exchange (3ROX). This service leverages the widely deployed open-source 'OpenVAS' framework to identify assets in need of protection. 3ROX is operated and managed by the Pittsburgh Supercomputing Center.

Sharing Threat Intelligence for Network Gatekeeping with Automated Response (STINGAR). Duke University developed STINGAR, which uses a decoy computer system for trapping or tracking hackers (known as a honeypot). STINGAR uses automation to speed responses.

Cybersecurity Best Practices for Research: The University of California San Diego will provide training and best practices for information security professionals on addressing the technical and cultural challenges in securing research in higher education.

Community of Practice: By bringing together CISOs, facilitators, cybersecurity researchers, research software engineers, cybersecurity analysts, security engineers, system administrators, and others we aim to create a community that demystifies the practice of cybersecurity for open science.

Data for cybersecurity research: ResearchSOC plans to engage with the cybersecurity research community to advance research using the data from the ResearchSOC

These services have existing infrastructure and customer bases, which ResearchSOC can leverage to more effectively and sustainably guard against cybersecurity threats.

Audience:

This training is suitable for PIs, for technical management, and for IT and security personnel working on science and CI projects.

Point of Contact this proposal:

Todd A. Stone
ResearchSOC Communications and Outreach Lead
Indiana University
toddston@iu.edu