SAND2022-13748C

NNSA Center of Excellence (CoE) in Cyber Threat Intelligence

Jacob Caswell (SNL)

Kevin Hamilton (LLNL)

NLIT 2022

October 19th, 2022

Albuquerque, NM

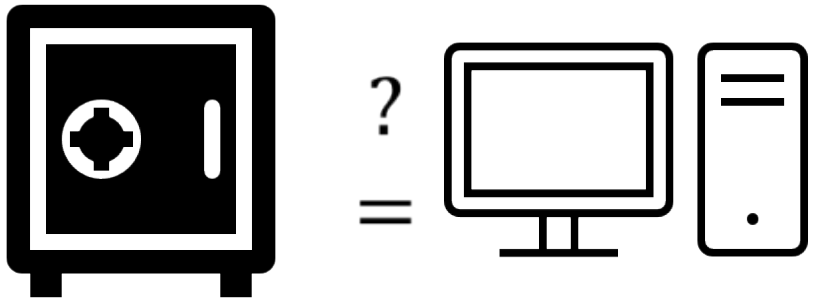
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Perspectives on Threat Hunting

There is no true substitute for **experience** and **network** in a cyber threat hunter.

Experience



Network

In the face of attrition, **preserving, fostering, and sharing these attributes is essential**.

Perspectives on Threat Hunting

How can we share these attributes?

Experience

- Where possible, use shared tools and procedures
- Otherwise, use standard interfaces
- Don’t throw out case file after the case is closed
- Codify past experience so that its application may be automated

Network

- Foster a community that rewards technical exchange and mentorship
- Identify and pursue opportunities for hunters to grow their networks
- Work to break down barriers to sharing and collaborating
- Focus on building relationships rooted in trust

NNSA CoE Participating Sites

What is the NNSA CoE?

- An effort to **preserve, foster, and share** the NNSA's threat hunters' **experience** and **network**…
- … To effectively:
  - Harden the NNSA's overall cyber environment
  - Increase enterprise situational awareness
  - Advance the knowledge and skills required to develop advanced cyber capabilities
- Operated in service of NA-IM
- Managed by a Board of Governors consisting of participating site CISOs
- Participating threat hunters engage in weekly meetings to:
  - Characterize and assess threats from open source intelligence
  - Participate in threat-informed and open hunting
  - Brief stakeholders on our findings and risk models

NNSA CoE Approach to Threat Intelligence

- Threat Intelligence is a process that drives the prioritization and dissemination of:
  - Results from **Tactical** threat hunting and incident response
  - **Operational** threat modelling
  - **Strategic** investment
- It provides an interface to share **experience** with your **network** (and vice-versa)
- **Inputs**: information from open, closed source feeds, technical findings, and operational models
- **Produces**: structured findings to inform **tactical**, **operational**, and **strategic** stakeholders
- **Impact**:
  - Hunters can more effectively hunt for, identify, and analyze threats
  - Operational partners can apply the hunters' findings to their mission
  - Strategic stakeholders' investments are informed by the broader risk environment

NNSA CoE Approach to Threat Hunting

- The Hunt Team:
  - Facilitates **direct access** for all sites to the shared experts across the complex
  - Interfaces directly with the Cyber Threat Intelligence team to prioritize hunts
  - Draws from shared data and tools where available
  - Federates their search and shares information in agreed upon formats
  - Provides regular technical exchanges on their findings and processes
  - Feeds their findings and observations back to the CTI team for analysis
  - Partners directly with IARC to operationalize hunting and coordination with other entities (e.g., iJC3)
  - Outlines and iterates on best practices for threat hunting in federated environments

NNSA CoE Going Forward

- Continue to improve upon the federated CTI and Threat Hunting process
- Develop new platforms to share data, findings, and analyses
  - Especially in compliance EO14028, related memos
- Expand partnerships across DOE

Contacts:

- Scott Engelson, NNSA OCIO, CISO
  - scott.engelson@nnsa.doe.gov
- Matt Myrick, LLNL, Chair of the Board
  - myrick3@llnl.gov
- Jacob Caswell, SNL, Technical Project Manager
  - jcaswel@sandia.gov
- Corey Reitz, SNL, Functional Project Manager
  - csreitz@sandia.gov