INL/CON-24-78402-Revision-0

Does practice make perfect? Lessons learned from full-scale power system incident response exercise

June 2024

Megan Jordan Culler

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-78402-Revision-0

Does practice make perfect? Lessons learned from full-scale power system incident response exercise

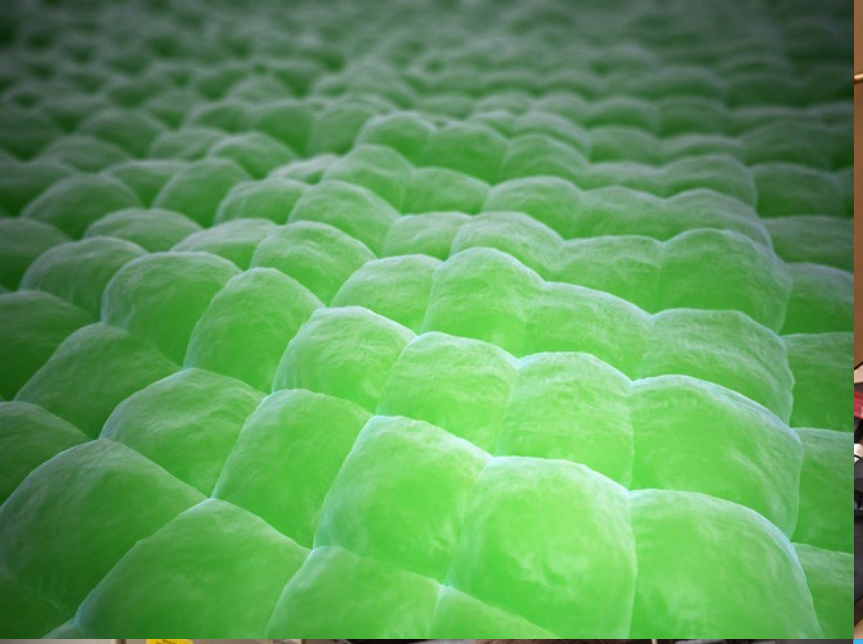
Megan Jordan Culler

June 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



June 18, 2024

Megan Culler
Infrastructure Security

Does practice make perfect?

Lessons learned from full-scale power system incident response exercise

SANS ICS Summit

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

INL/CON-24-78402

2023 Attack on Danish Critical Infrastructure

May 5 16 energy companies attacked

- Exploited known vulnerability in Zyxel firewall
  - Specific packet to port 500 over UDP decoded by Internet Key Exchange (IKE), resulted in root privileges on firewall
- Coordinated hit – all at the same time
- Knew exactly which targets to attack
- 11 companies compromised, 5 failed due to incorrect formatting
- Response:
  - Identify attacked companies and monitor for new compromises
  - Alert affected members
  - Work with supplies to apply updates
  - Share information with appropriate authorities

2023 Attack on Danish Critical Infrastructure

May 22- 14:44 Alarm at SektorCERT

- Member A downloading new software to firewall over insecure connection
- Firewall acted as part of the Mirai botnet, targeting devices in US and Hong Kong
- Encrypted C2 traffic

May 22 – 15:00 Member A enters island mode

- Reset firewall, install updates, start reconnaissance

May 22- 18:13 Member B attacked

- Less than 2 hours later, Member B enters island mode
- Late hours for SektorCERT

May 23 18:43 Member C compromised

- Infrastructure used in SSH brute force against Canadian company

2023 Attack on Danish Critical Infrastructure

May 24 – 10:27 Member D compromised

- 4 different payloads downloaded, selected one for DDoS attacks

May 24: Zyzel announces new vulnerabilities

May 24 – 10:31-10:58 3 additional members compromised

- MIPSkiller used in all cases
- Firewalls participate in more DoS

May 24 – 15:59 Member H compromised*

- Different payloads
- Member included in Mirai Moobot network

* Member H did not know they had the firewalls on their system

May 24 19:02 APT activity detected

- Indicator of Sandworm activity
- Traced to a single network packet of 1340 bytes to IP address traced to Sandworm

2023 Attack on Danish Critical Infrastructure

May 25 – 1:22 Member I compromised

- Included single packet to another suspected Sandworm server

May 25 – 8:22 2 new attacks (Members J and K)**

- Many different payloads tried
- May be a new attacker

**Member K chose not to patch firewall, resulting in repeated compromises by different attackers in following days

May 25 – 11:45 Member I loses visibility

- Remote comms to 3 locations lost
- Sent out teams for manual operation

May 25 – 12:00 Coordinated response

- SecktorCERT contacts National Center for Cybercrime and Center for Cyber Security
- Sent analysts out to members to gather information
- Shut down all internet connections, but keep firewalls on

Highlights

- ✓Early intrusion sign not always detected
- ✓Hard to be prepared even when you know it’s coming
- ✓Cooperation is key
- ✓Late hours called out as unusual factor

Trends in energy sector threats

[2010] Stuxnet

- Very aggressive
- Targeted specific version/configuration of PLCs

[2015] Industroyer / CrashOverride

- Framework targeting 4 OT protocols
- First known malware targeting electric grid
- Persistent backdoors
- Pre-defined timer for execution
- Included DoS against relays and wiper tool

[2017] Triton

- Designed to manipulate safety instrumented systems
- Only affected specific Schneider Triconix safety system
- Modifies in-memory firmware to execute arbitrary code
- Only works if controller is in “program” mode instead of “run” mode
- Bugs in malware allowed it to be discovered before execution

[2022] Incontroller/ Pipedream

- 3 modules targeting Schneider PLC, Omcron PLC, OPCUA protocol
- Capabilities include disrupting, modifying, and disabling safety controllers

[2022] Industroyer2

- Targeted IEC-60870-4-104
- Customized configurations to modify malware behavior to specific devices (i.e. relays) in target environment
- Enhanced reproducibility against different environments

- ➢ Targeting protocols, not devices
- ➢ Flexible and extensible
- ➢ Accompanied by wipers

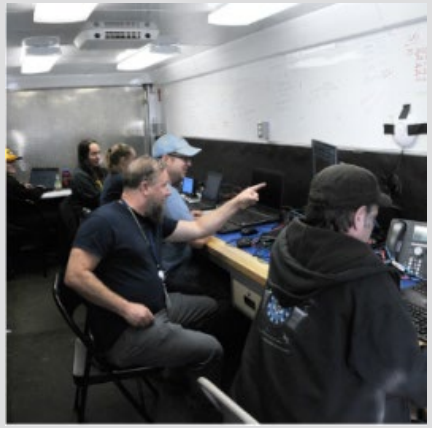
Trends in Targeting and Vulnerability Exploitation in Clean Energy

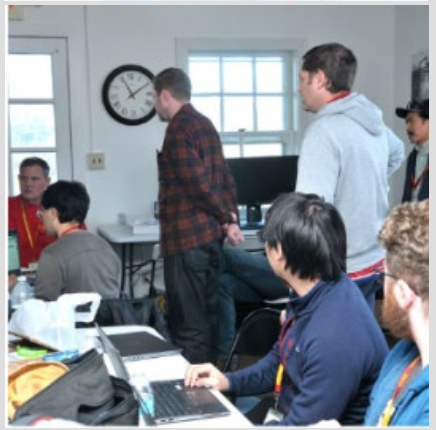
- Weak credentials
  - Weak requirements
  - Hard-coded credentials
  - Passwords derived from available information
  - Plaintext storage
  - Weak encryption or authentication
- Web page vulnerabilities allowing arbitrary code execution
- Cross-site scripting vulnerabilities
- Unauthorized access to sensitive files
- Web apps were the most targeted service type followed by remote management protocols
- 5 OT protocols were constantly targeted (Modbus was a third of attacks, DNP3 was about 18%)
- RATs and information stealers were the most popular malware types

- Make sure the fix is really a fix
- Best practices for storing sensitive information (i.e. passwords)
- Web portal security

What is the goal of full-scale exercises?

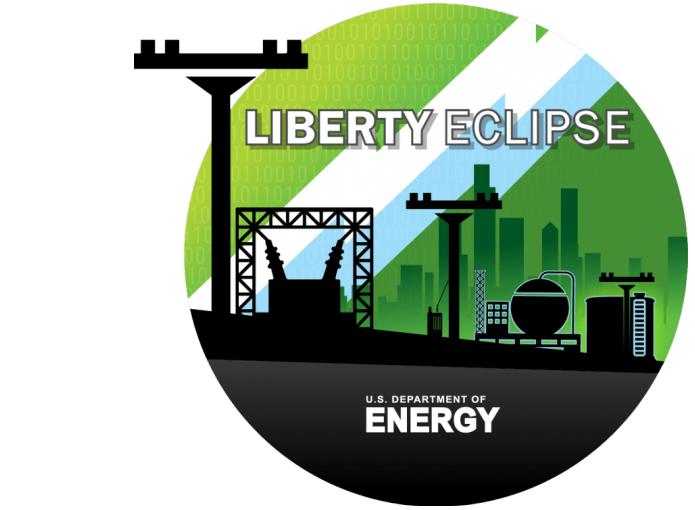
Practice	Response plans must be put into practice
Validate	Validate existing plans, policies, procedures, and capabilities
Collaborate	Test how different organizations and agencies will collaborate in response to an emergency (Government, Nonprofit, Private sector)
Improve	Identify resource requirements, capacity constraints, and potential areas for improvement
Train	Train junior staff on real world scenarios





Liberty Eclipse

- Annual cybersecurity preparedness exercise that brings together federal partners, and operational technology (OT) and cybersecurity experts from the energy sector to validate the security of their cyber defense systems, plans, policies, and procedures in a scaled environment.
- Full-scale exercise with utility participants
- Energized, but disconnected, test bed
- Red team, led by INL, executes scenarios on components found in real systems requiring coordinated response from cybersecurity teams (SOC) and power operations teams (Ops Center)

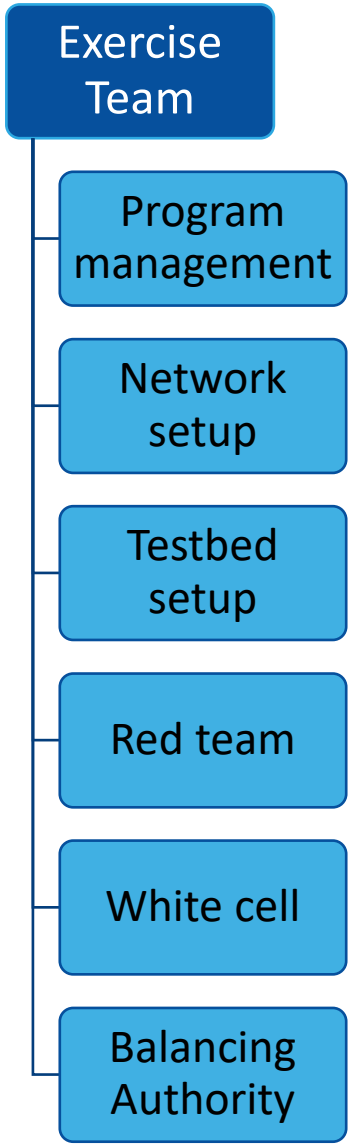


Testbed leverages commercial protection and control devices using systems commonly found in utility substations across the country.

Do you have the right people tools, practice, and preparation?

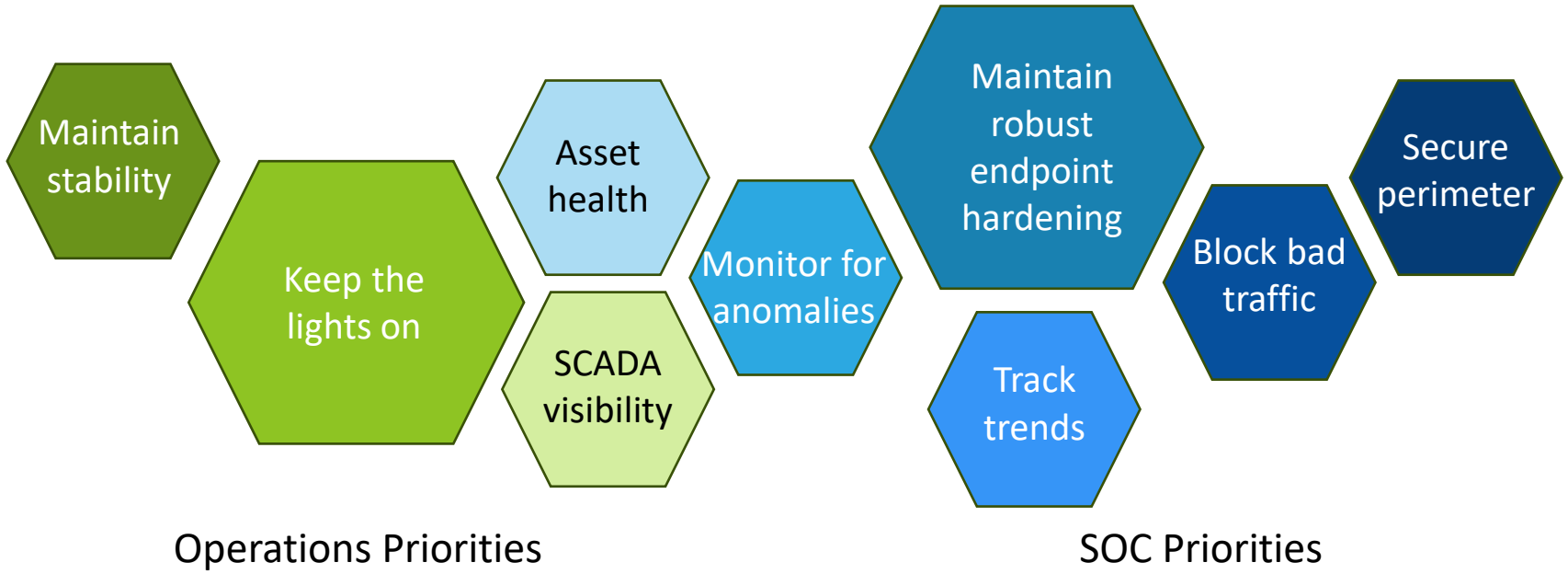
Incident Response Practice Teams

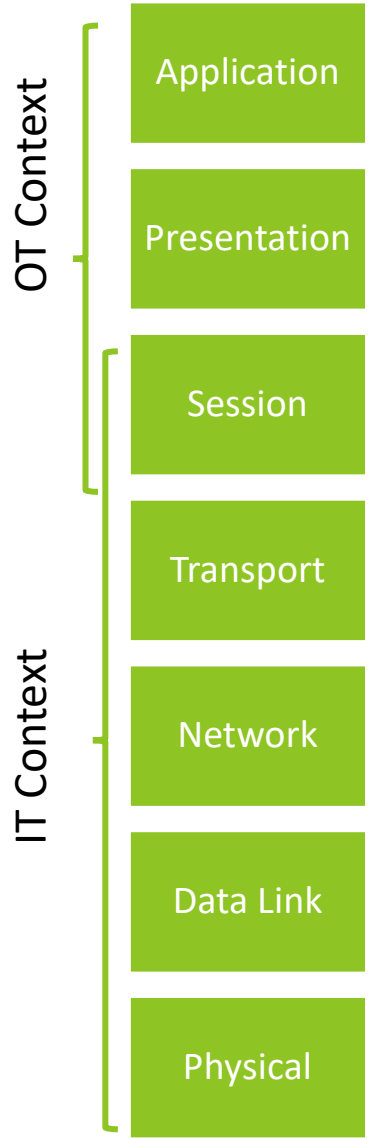
Ops Center	SOC	Strategic Partners	National Guard
• Keep loads powered • Monitor system health • Manage generation with balancing authority	• Monitor enterprise and OT networks • Detect and respond to red team activity	• Active participation • Assist Ops Center and SOC	• Cyber units • OT training • Familiarity with OT equipment • Data collection • Self-evaluations



SOC and Ops Teams Interactions

- SOC detected adversarial activity on OT systems but had no idea what it meant operationally.
- How do they warn the operations team?





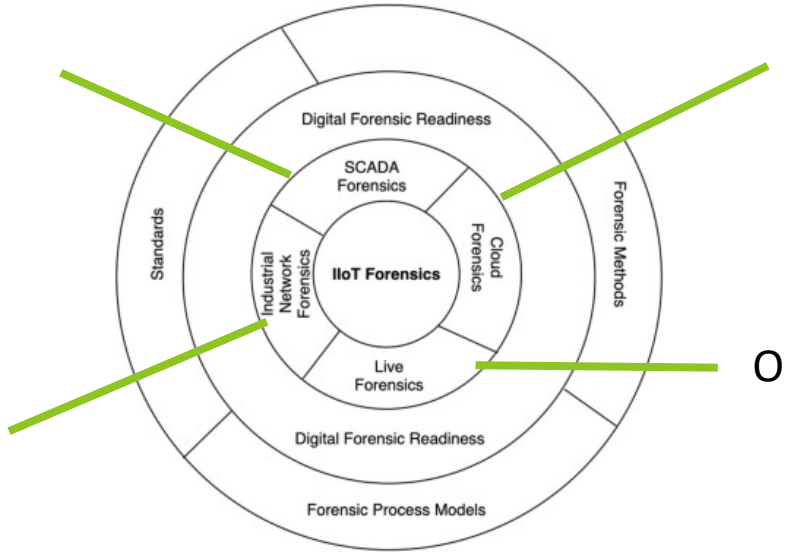
Lesson Learned: Promote more interaction and communication between SOC and Ops Center.

Forensics

- "We know you bricked this device, but we don't know how."

Operations, OT sec

Vendors, IT sec



IT sec, OT sec

Operations, OT sec

Diagram highlights different types of forensics and various layers of abstraction. Potential responsible parties for various devices/networks highlighted.

DE-FOA-0003223

Topic Area 1- Address Forensic Analysis of Infected Renewable Systems

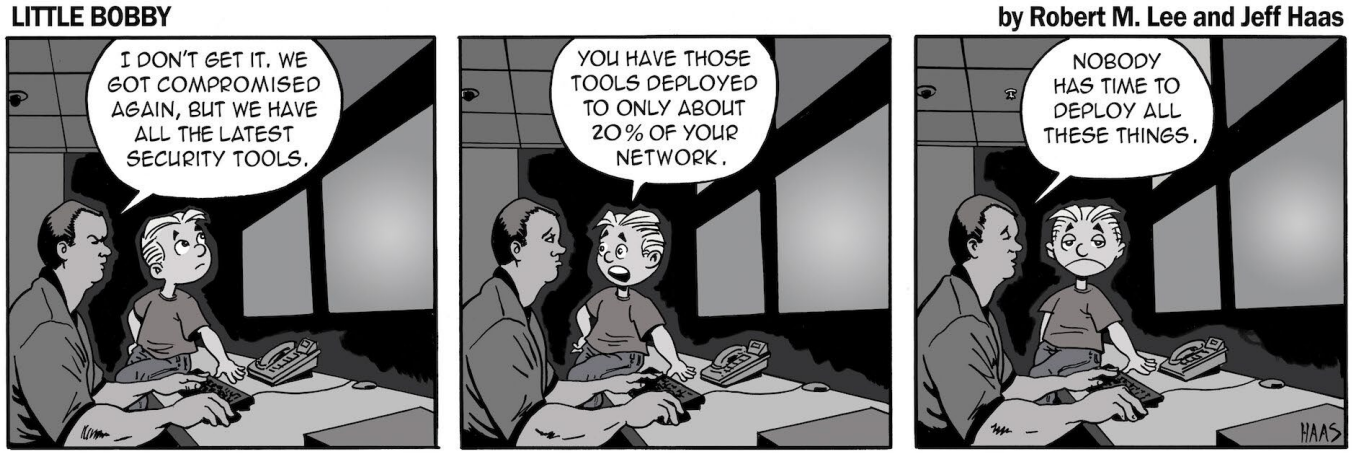
Goal: Research, develop, and demonstrate advanced cybersecurity applications and technology to enhance the capability to conduct forensic analysis of affected renewable energy systems and operational technology devices.

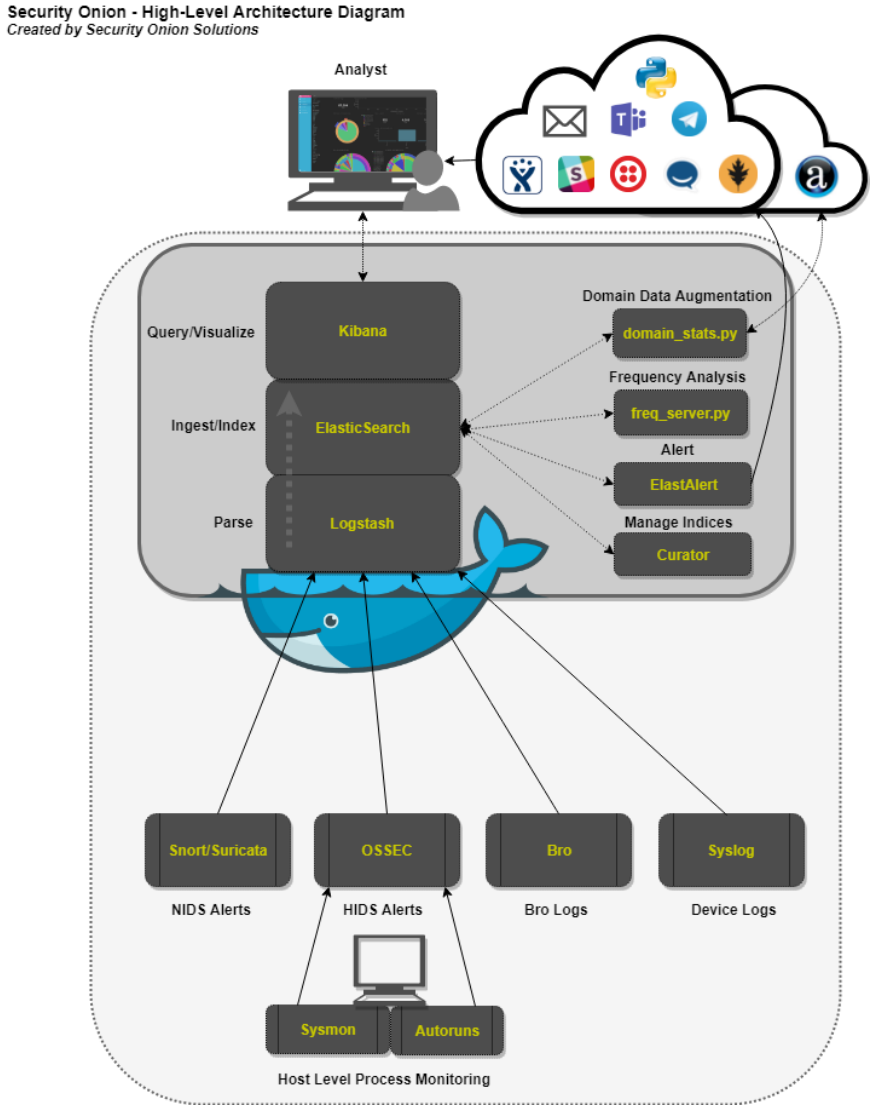
Lesson Learned: Getting stuck is not a loss. Consider what next steps would be if this happened in an operational environment

https://www.sciencedirect.com/science/article/pii/S2665910722000032

Tools

- Lots of tools available for utilities to use
- Analysts prefer what is familiar
- Barriers:
  - Setup and configuration
  - Parsing alerts
  - Full network visibility





Security Onion is one open-source tool that was available for participants to use.

Lesson Learned: Exercise is most beneficial if you can use the tools you work with. **but also a good opportunity to get exposure to new tools.

https://github.com/Security-Onion-Solutions/security-onion/wiki/Elastic-Architecture

You don’t get the answer key ahead of time (but the Exercise Team does)

White carding

- Red team had access to some credentials and pre-staged code to execute at later times.

Benefits	Drawbacks
• Allows red team to demonstrate full attack chains in a short time. • Enables consistent activity for Ops Center and SOC to investigate. • Participants can submit change requests to respond to events, which may be accepted or denied.	• Some participants felt this was red team cheating. • Some participants changed white-carded credentials without adhering to change request policies.

Lesson Learned: Need better context setting around whitecarding.

Preparation for red team activity

Different potential approaches

1. Going in blind
   - Participants do not know what is coming.
   - Most realistic “it’s just a normal day”
2. Knowing what type of activity to look for
   - Provide themes of activities to watch for each day
3. Knowing exactly what activity to look for and when

Lesson Learned: With so many types of participants, one approach is unlikely to satisfy all. Focus on realism benefits of full-scale exercise. Provide sufficient debriefs..

Red Team Resources

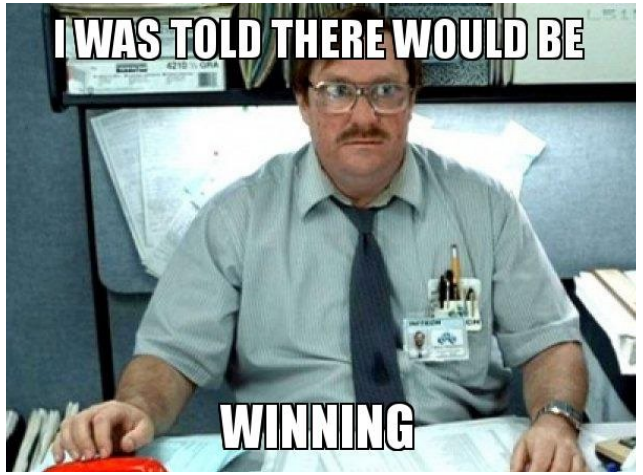
- Give the red team the resources they need.
  - Access to equipment and networks with sufficient time to develop plans for adversarial scenarios.
  - Not a hunt or penetration test activity.
- It's not a test for the red team.
  - Focus on participant experience but communicate with participants about the types of shortcuts the red team may take.
- Reality matters.
  - Don't make it too easy.
  - Consider the settings and configurations of devices.

Lesson Learned: Lead time for development, testing, and deployment for red team will create the most realistic, smoothly executed scenarios.

Gamification

Focus on the Outcome

- Gamification helps engagement
  - Friendly “news feed” allowed red team and blue team to communicate.
- Goal is to learn, not to beat the red team
  - Not a traditional red/blue exercise.
  - Not a competition across participants.
  - Blocking red team at first signs of access reduces what you learn from exercise.
- Need additional motivating factors
  - Find other metrics to evaluate success (e.g. detection rate instead of block rate)
  - Set challenges for each team.



Lesson Learned: Make sure everyone is on the same page for goal of the exercise.

Applying Lessons from Liberty Eclipse

- How well do operations teams and OT SOC teams communicate? How can you build those relationships now and promote mutual learning?

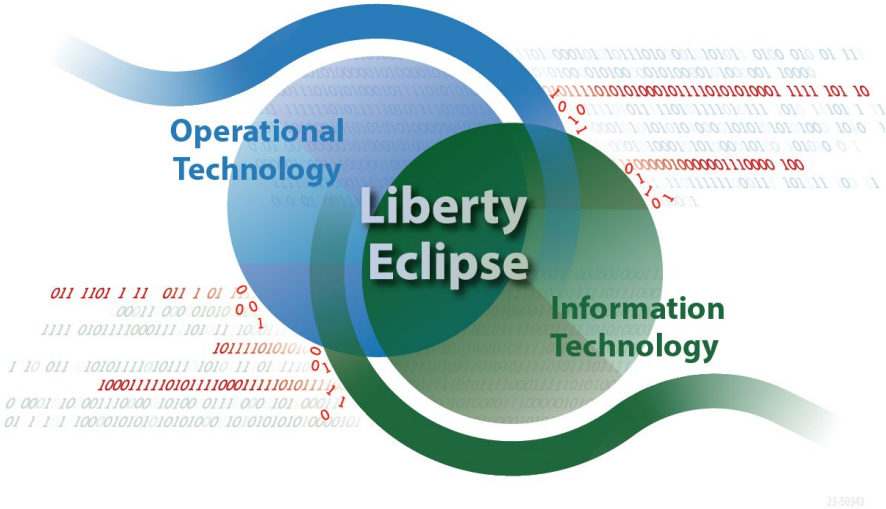
- How are you testing the visibility of security tools to ensure events of interest are captured?

- What training scenarios are available to put staff in a new environment and practice communication with different entities?

- What are the objectives of your incident response practice? How do you self-evaluate success of objectives?

Final thoughts

- Full-scale exercise puts people under pressure, get to see how they respond when it's not just on paper.
- Unique setup enables IT/OT crossover, but there is still some work to be done to bridge the IT/OT knowledge gap in response.
- Clear definition of rules of engagement and goals of the exercise benefits all.
- Realism improves the exercise, but some adjustments must be made because it is an exercise.



Learn more

- https://www.energy.gov/ceser/liberty-eclipse
- https://www.energy.gov/ceser/articles/practicing-defense-and-resilience-liberty-eclipse
- https://youtu.be/Cao8ro0F-K0

Contact: Megan Culler
Megan.Culler@inl.gov

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.