CyberStrike Workshop

HANDS-ON TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS

CYBER STRIKE
Sponsored by the U.S. Department of Energy

ABOUT THE WORKSHOP

The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE), in collaboration with the Electricity Information Sharing and Analysis Center and Idaho National Lab (INL), has developed the CyberStrike workshop to enhance the ability of energy sector owners and operators in the U.S to prepare for a cyber incident impacting industrial control systems. The training offers attendees a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. The instruction platform challenges course participants to defend against a cyberattack on the equipment they routinely encounter within their industrial control systems.

The CyberStrike Workshops help owners and operators to:

- Understand and manage the multifaceted interdependencies between the Nation's energy infrastructure and other critical infrastructure
- Detect and respond within compressed timelines to prevent highly impactful consequences
- Develop top-tier defenders to mitigate sophisticated threat actors

Workshop attendees are guided through a series of exercises/labs in groups of five or six operators. Modules reference industry experiences, best practices, and lessons learned. These references help operators understand the Ukraine cyber incident from a technical perspective to enhance cyber preparedness.

TRAINING LABS/ MODULES

- Open Source Intelligence
- Denial of Service
- Controlling the Human Machine Interface
- Bypassing the Human Machine Interface
- Firmware Analysis
- Passive Man in the Middle Attack
- Active Man in the Middle Attack
- Defender Mitigations

TARGET AUDIENCE

The workshop is tailored to energy sector owner and operator staff who work in the following areas:

- Control room operational technology personnel
- Critical infrastructure protection-focused technical staff
- Energy Management System (EMS) support
- Operating personnel
- Cybersecurity staff

For more information about the CyberStrike Workshop, please contact Brian Marko (Brian.Marko@hq.doe.gov) and Amanda Sramek (Amanda.Sramek@hq.doe.gov).

INL Idaho National Laboratory

LESSONS LEARNED

- **Cyber contingency analysis** (continuous analysis and preparing the system for the next event)
- **Cyber failure planning** (modeling and testing cyber system response to network and asset outages)
- **Cyber conservative operations** (intentionally eliminating planned and unplanned changes, as well as stopping any potentially impactful processes)
- **Cyber load shed** (eliminating all unnecessary network segments, communications, and cyber assets that are not operationally necessary)
- **Cyber RCA** (Root Cause Analysis forensics to determine how an impactful event occurred and ensure it is contained)
- **Cyber blackstart** (cyber asset base configurations and bare metal build capability to restore the cyber system to a critical service state)
- **Cyber mutual aid** (ability to utilize ISACs, peer utilities, law enforcement and intelligence agencies, as well as contractors and vendors to respond to large scale events)

ADDITIONAL RESOURCES FOR THE UKRAINE CYBER INCIDENTS

- **NCCIC/ICS-CERT INCIDENT ALERT**: IR-Alert-H-16-043-01P UKRAINIAN POWER OUTAGE EVENT, February 12, 2016 (TLP=GREEN) https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
  - High-level summary of the incident elements and Mitigation guidance
  - Detection pointers & indicators (IOCs)
- **NERC E-ISAC:** Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced By Recent International Events, February 9, 2016 (TLP=RED)
  - Tactics used by actors with mitigation options
- **ICS-CERT BlackEnergy YARA signature:** https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01E
- **Initial Findings of the U.S. Delegation** examining the events of December 23rd 2015, Power Point Presentation, February 2016
- **E-ISAC & SANS Defense Use Case:** https://www.esisac.com/api/documents/4199/publicdownload

TOP TEN THINGS YOU CAN DO NOW

1. Review internal IR plans
2. Identify and review electronic access points
3. Review/develop full system restore capabilities
4. Develop procedure to disconnect
5. Establish relationships with DOE, FBI, and DHS.
6. Register and test access ONG-ISAC, DNG-ISAC, and E-ISAC access
7. Review alerts, documents, and NERC Level 2 alert response progress.
8. Participate in exercises.
9. Work with NERC to train operators.
10. Ask for help.

TOOLS USED DURING WORKSHOP

- Kali Linux
- Maltego CE
- Shodan
- Metasploit
- Nmap
- VNC Viewer
- Ettercap
- Wireshark

For more information about the CyberStrike Workshop, please contact Brian Marko (Brian.Marko@hq.doe.gov) and Amanda Sramek (Amanda.Sramek@hq.doe.gov).

INL Idaho National Laboratory