CyberStrike™ Training Program

PRACTICAL TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS

Why CyberStrike™?

In today's technologically advanced environment, the substations, generation centers, compressor stations, pumping sites, and control rooms that are responsible for our nation's critical infrastructure systems are connected to the internet and vulnerable to cyberattacks. Hacking organizations around the world have already proven they can turn off the electricity to hundreds of thousands of homes by remotely accessing and changing the command settings of operational technology. But these control systems are responsible for managing the infrastructure we rely on for providing safe and reliable production, transport, and storage of energy. Many of these systems were designed and deployed for different threats than the ones emerging today. Adversaries are also flexible and capable of changing their tactics swiftly. Our risk management practices for cybersecurity must keep pace with these changing conditions. With expensive price tags, long production lead times and lifespans that last several decades, replacing existing equipment is a difficult and costly endeavor.

To reduce the consequences of cyber-physical attacks, the U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response (CESER), in collaboration Idaho National Laboratory (INL), developed the CyberStrike™ training program. This program works to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting operational technology.

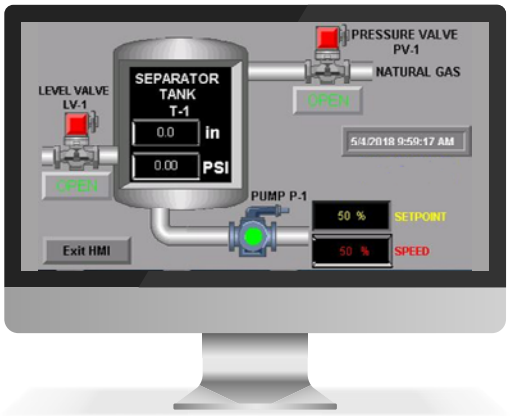
Target Audience

Energy sector owner and operator staff in the following areas:

- Control room operation
- Technology personnel
- Critical infrastructure protection
- Focused technical staff
- Energy Management System (EMS) support
- Operating personnel
- Cybersecurity staff

Tools Used During Workshop

- Kali Linux
- MiniMega
- hping3
- OpenPLC
- EditorMetasploit
- Nmap
- VNC Viewer
- Ettercap
- Wireshark



CyberStrike™ LIGHTS OUT and NEMISIS Workshops

The CyberStrike™ LIGHTS OUT training workshop was designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting industrial control systems. This training offers participants a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. During this training participants are guided through a series of exercises that challenge course participants to defend against a cyberattack on the equipment they routinely encounter within their industrial control systems (ICSs).

The CyberStrike™ NEMESIS training workshop builds on lesson learned in the CyberStrike™ LIGHTS OUT workshop and applies current and emerging threats to the scenarios. This training offers an in-depth look at the tactics, techniques, and procedures (TTPs) used by the most sophisticated cyber adversary groups targeting industrial control systems (ICS) today. The NEMESIS workshop is designed to adapt and change as new incidents are uncovered or as new ICS-specific threats emerge, keeping the workshop content as current and helpful as possible.

Various Hands-On Exercises

- Open-Source Intelligence
- Denial of Service
- Firmware Analysis
- Defender Mitigations
- Ladder Logic
- Passive and Active Man in the Middle Attack
- Credential Harvesting
- HMI Breakout
- Controlling and Bypassing the Human Machine Interface
- Data Exfiltration
- Malware Detection
- Ransomware

Continuing Education Units

CyberStrike™ is accredited to issue IACET Continuing Education Units (CEUs). Upon completion of the LIGHT OUT training, trainees will be granted 0.8 CEUs

Disclaimer: Training personnel do not discriminate based on race, color, religion, national origin, sexual orientation, physical or mental disability, or gender expression/identity. Additionally, they do not possess proprietary interest in any product, instrument, device, service or material discussed in this course.

For More Information

Visit www.inl.gov/cyberstrike

WATCH A VIDEO

https://www.youtube.com/watch?v=ZvMf5eHg89s

To schedule a training, contact cyberstrike@inl.gov

22-50524-03_r3