CyberStrike™ LIGHTS OUT

PRACTICAL TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS

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

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. These systems were designed and deployed for different threats than encountered 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

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

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

Hands-on Exercises

The CyberStrike™ training features live exercises using real equipment and scenarios routinely experienced by utility owners and operators:

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

CyberStrike™ LIGHTS OUT

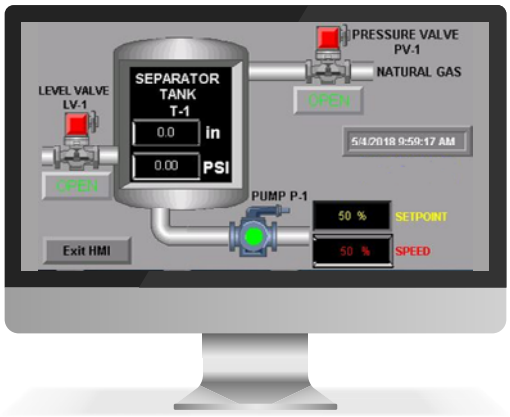
The CyberStrike™ LIGHTS OUT training workshop was designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting industrial control systems. This training offers participants a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine.

This workshop is offered as a virtual event either with live or self-guided online instruction. Participants are guided through a series of exercises that challenge the participant to defend equipment they routinely encounter within their industrial control systems (ICSs) against a cyberattack. Specifically, participants will achieve the following course objectives:

1. Describe the 2015 and 2016 Ukraine cyber events
2. Reconstruct a cyber-event using the cyber-kill chain
3. Discuss guidance and mitigation concepts
4. Describe the importance of prevention.

Tools Used During Workshop

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



Continuing Education Units (CEUs)

The training organization is accredited by the International Accreditors for continuing Education and Training (IACET) and is accredited to issue IACET Continuing Education Units (CEUs). Upon completion of this training, trainees will be granted 0.8 CEUs. This number is based on 7.5 hours of student engagement. At the conclusion of this training, trainees will receive a certificate of completion which can be used to provide evidence of completion of continuing education requirements.

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

22-50524-01_r2