CyberStrike Training

PRACTICAL TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS

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

CyberStrike Training Program

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-enabled sabotage, 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

How The Course Works

The CyberStrike training program is offered as an in-person event or as a virtual course with instruction provided online. Both events involve live instruction and hands-on exercises drawing from elements of the 2015 and 2016 cyber incidents in Ukraine, as well as more recent cyber events. During the training, instructors guide participants through a series of exercises that challenge participants to defend against a cyberattack using equipment they routinely encounter within operational technology networks.

Virtual Training

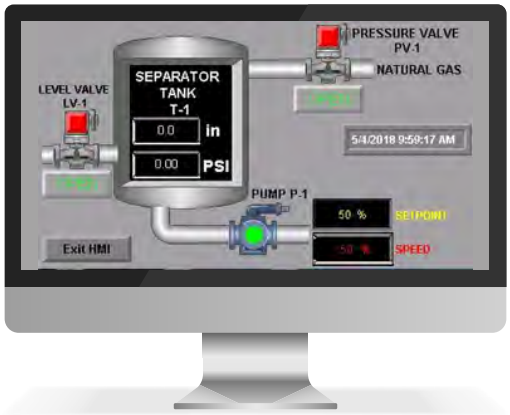
The virtual training offers participants a simulated demonstration of a cyberattack. To conduct the hands-on exercises, participants remotely connect to a live operational technology platform that includes a programmable logic controller, human machine interface and industrial ethernet switch, along with a remotely operable motor and breaker. Participants have access to a live camera feed showing the platform and its status during each exercise. Virtual training is ideal for organizations that can't meet in person due to restrictions from the COVID-19 pandemic, or when the need exists to accommodate participants spread across multiple time zones. Virtual training can be split into four-hour workshops over two days.

In-Person Training

The in-person instruction consists of an eight-hour workshop conducted in a single day. An expert cybersecurity research team ships equipment to the participants' business location, meeting or conference center, or convention hall. Then, they set up the classroom and equipment, and provide certified instruction. Participants work in teams to gain new insights into advanced cybersecurity risks, threats and solutions.

Tools Used During Workshop

- Kali Linux
- Maltego CE
- Shodan
- Metasploit
- 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 on the basis of 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