CyberStrike STORMCLOUD

Practical training for energy sector owners and operators

The CyberStrike STORMCLOUD training workshop was designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting control systems associated with renewable energy technologies. This training offers participants a hands-on, simulated demonstration of cyberattacks directed at wind, solar and electric vehicles (EV).

This workshop is offered as a virtual event with live or self-guided online instruction. Participants are guided through a series of exercises that challenge them to defend equipment they routinely encounter within industrial control systems.

Hands-on Exercises

Solar Exercises

- **Lab 1:** Exploring DER (Distributed Energy Resources) Logical Interfaces
- **Lab 2:** Denial-of-Service
- **Lab 3:** Firmware Analysis
- **Lab 4:** Malicious Firmware Update
- **Lab 5:** Web Exploitation
- **Lab 6:** Smartphone App Security
- **Lab 7:** Replay and Machine-in-the-Middle Attacks
- **Lab 8:** Defense

Wind and EV modules under development.

Tools Used During Workshop

- Kali Linux
- MiniMega
- OpenPLC Editor
- Nmap
- VNC Viewer
- IEEE 2030.5
- hping3
- Ettercap
- Wireshark
- SunSpec Modbus
- Strings
- Grep

Target Audience

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

- Technology personnel
- Critical infrastructure protection
- Focused technical staff
- Operating personnel
- Cybersecurity staff

Continuing Education Units

CyberStrike is accredited to issue IACET Continuing Education Units (CEU). Individuals will earn CEUs after completing the STORMCLOUD training.

For an overview of the CyberStrike portfolio of training workshops, please see the following fact sheet: CYBERSTRIKE Overview FactSheet

For More Information

Visit www.inl.gov/cyberstrike

To schedule a training, contact cyberstrike@inl.gov

WATCH A VIDEO
youtube.com/watch?v=4G2aTzz0zKg

22-50524-08_R1