CyberStrike FORENSIC ANALYSIS

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

Practical training for energy sector owners and operators

The CyberStrike FORENSIC ANALYSIS training workshop was designed to enhance the ability of cyber analysts accurately determine the nature of a cyber incident — how the adversary achieved its goals, the nature of their activities during the attack, and the extent of the compromise.

This workshop is offered as a live workshop or virtual event with live instruction. This training offers participants a hands-on, simulated demonstration of the post-attack landscape through a series of scenarios. Participants analyze firewall and Zeek logs, network traffic packet captures, malware signatures and suspicious files to puzzle out how different cyberattacks are created and executed.

The labs in this workshop have been developed to mimic real-world cyber incident response scenarios for industrial control systems (ICS), including:

- Watering hole malware infection
- Exfiltration of encrypted data to an internal server
- Malware scanning of a network for ICS protocols
- Command and control mechanisms from an internal, compromised server

Target Audience

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

- IT specialists
- Cybersecurity analysts
- Incident response teams
- Focused technical staff

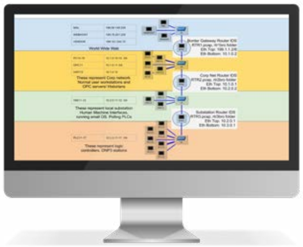
Hands-on Exercises

This workshop is broken into three main sections:

- **Warm-up Activities**
- **Lab 1: Moose Scepter Infection** – This lab's scenarios include a series of events from two different networks attacked by malware known as Moose Scepter.
- **Lab 2: Northern Ghost Infection** – In this lab, participants take on the role of a cyber incident response team at a notional electric utility in North America.

Tools Used During Workshop

- Yara
- Wireshark
- Bro/Zeek
- Sha1sum
- Volatility
- Strings
- Grep



Continuing Education Units

CyberStrike is accredited to issue IACET Continuing Education Units (CEU). Individuals earn CEU credit after completing the FORENSIC ANALYSIS training.

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

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

For More Information

Visit www.inl.gov/cyberstrike

To schedule a training, contact cyberstrike@inl.gov

WATCH A VIDEO
youtube.com/watch?v=ZvMf5eHg89s

22-50524-04_R2

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

INL Idaho National Laboratory