Detect the Attacker

Course overview

This scenario-driven course is for defenders of industrial control systems. Delivered in person at the Idaho National Laboratory's Idaho Falls campus, this four-day training will elevate your professional expertise. Participants will master a comprehensive threat-detection methodology, enhancing their skills in detecting, correlating and analyzing cyberthreats within industrial environments.

What you'll learn

In this training, you will:

- Leverage cyberthreat intelligence.
- Map data sources to improve detection.
- Develop a comprehensive view of your assets and their critical interdependencies.
- Understand the roles, tools and workflows for a successful security of operations center.
- Analyze common industrial control system network protocols.
- Think like an adversary and test potential threats.
- Engage in proactive threat detection with real-world scenarios.
- Test your skills in a coordinated cyberattack simulation involving "hactivists," corporate competitors and state actors.

For more information and to register for the course:
https://inl.gov/national-security/ics-cybersecurity-training/

Questions?
Contact: ICSTraining@inl.gov

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Detect the Attacker

Course schedule

Day 1

- Explore MITRE ATT&CK® and ATT&CK Navigator.
- Map data sources using ATT&CK Navigator.
- Identify critical assets and attack surfaces with Zenmap and NetBox.
- Learn SOC roles and best practices.

Day 2

- Analyze industrial control system protocols and network activity for malicious traffic.

Day 3

- Develop and test attack hypotheses.
- Practice threat detection in an industrial setting.
- Use structured approaches for detection (Snort rules), correlation (Kibana dashboard), and traffic analysis (Malcolm and Security Onion).

Day 4

- Capture the flag: Apply your skills to detect, investigate and analyze information technology and operation technology traffic in a live simulation under attack.

For more information and to register for the course:
https://inl.gov/national-security/ics-cybersecurity-training/

Questions?
Contact: ICSTraining@inl.gov

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

25-50587