Dragos™ **Training**

Assessing, Hunting, and Monitoring Industrial Control System (ICS) Networks

Course Overview

Assessing, Hunting, and Monitoring ICS Networks is an intensive 5-day, hands-on course that covers industrial control system (ICS) basics, ICS cybersecurity best practices, assessing industrial environments, ICS threat hunting, and industrial network monitoring. In addition to its classroom component, this course includes many hands-on labs and activities to reinforce the concepts learned.

Who Should Attend

- IT and OT security professionals seeking to increase their knowledge of ICS cybersecurity best practices and Dragos' industrial security methodologies and technologies
- IT security professionals who want to expand their knowledge of industrial environments and how securing them differs from IT environments

Course Facilities, Instructors, Location

- Dragos' state-of-the-art Training Center includes multiple ICS cyber ranges and individual training stations with mini control system kits that enable true hands-on learning and deep reinforcement of the course curriculum.
- Course instructors are drawn from Dragos' team of ICS cybersecurity experts: industry practitioners, who as members of the U.S. Intelligence Community and private sector industrial companies, have encountered the challenges the industry faces securing industrial control systems and surrounding infrastructure.
- The Dragos Training Center is located in Hanover, Maryland, conveniently located near Baltimore-Washington International (BWI) Airport and the BWI Amtrak station.

Prerequisites

- Linux operating system fundamentals, including basic command line usage
- Conceptual knowledge of programming/scripting
- Solid grasp of essential networking concepts (OSI model, TCP/IP, networking devices, and transmission media)
- Understanding of basic security concepts (e.g., malware, intrusion detection systems, firewalls, and vulnerabilities)
- Some familiarity with network traffic inspection tools (Wireshark, TShark, or tcpdump) is highly recommended

Dragos™ **Training**

Course Details

Students will receive hands-on and instructor-led training incorporating real-world case studies and exercises designed to reinforce concepts learned. Students will be placed in various roles designed to give context to the learning, as well as frame hands-on activities. As security and OT personnel for *Acme Water & Power (AWP)*, students will face scenarios including an OT engineer role, a Red Team role, and a Security Operations Center (SOC) analyst role, using real control systems and industrial data through labs and exercises.

MODULE 1: Intro to Industrial Systems and Networks

Students will learn about the various types of ICS environments, as well as their functions and compositions. Other topics covered will include: ICS network architectures, various types of devices, industrial programming languages such as ladder logic, and ICS communication protocols such as ModbusTCP, DNP3, and Profinet.

MODULE 2: Assessing Industrial Environments

Students will act as a Red Team member and learn how to safely assess ICS environments. Four types of assessments will be covered: architecture review, vulnerability assessment, penetration testing, and red team. Students will use purpose-built red team virtual machines to assess their environments.

MODULE 3: Tools, Strategies, and Techniques for Successful Hunting in ICS

Students will learn Dragos' threat hunting methodologies, including: planning, hypothesis generation, collecting and analyzing data, and automating lessons learned post hunt. They will then act as threat hunters through a variety of scenarios covering industrial networks and network/host artifacts.

MODULE 4: ICS Monitoring and Security Operations

Students will be exposed to attacks modeled off of real-world advanced threats while acting as SOC analysts, performing continuous monitoring, investigation, case management and other SOC-related responsibilities.

CPE Credits

Continuing professional education credits are free of charge and are awarded based on proficiency testing.

Pricing

Dragos customers: $3000*

Non-Dragos customers: $4500

* Excluding Dragos CyberLens and Dragos Training

Course Dates, Registration, and More Information

Visit dragos.com/training/ to see the course schedule and sign up to attend.

Contact Information

1745 Dorsey Road
Hanover, MD, 21076 USA
dragos.com | info@dragos.com