

DRAGOS 

Training

Dragos Certified User

Proprietary Statement

This material constitutes proprietary and trade secret information and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Dragos, Inc.

Copyright Statement

Copyright © 2022 Dragos, Inc. All Right Reserved

Dragos Global Headquarters

1745 Dorsey Rd
Suite R
Hanover, Maryland 21076
(855)-372-4670
www.dragos.com

Customer Support Requests

<https://portal.dragos.com/#/>

Table of Contents

Objective	1
Learning Outcomes.....	2
Delivery.....	2
Agenda	3
Day 1.....	3
Day 2.....	4
Scenarios and Labs.....	5
Labs	5
Scenarios.....	5
Certification Exam	6
Course Dates.....	6

Objective

The Dragos Certified User course is a two-day, scenario-based, purpose-built training designed to take Dragos Platform users to the intermediate level. Students will analyze the core Dragos Platform Use Cases, learn how to enable them in their production environments, and increase the time-to-value of the Dragos Platform. At the conclusion of the course, students will be eligible to take the Dragos Certified User Exam, which, if passed, will award them the Dragos Certified User Certification. This certification can be used toward CLE hours and be proudly displayed on students' resumes and LinkedIn profiles.

Learning Outcomes

The Dragos Certified User course empowers users to utilize, operationalize, and report on the core use cases of the Dragos Platform. Upon completing this course, users will be able to:

- Assess the system health of the Dragos Platform
- Develop an asset inventory
- Perform asset enrichment
- Utilize behavior analytics for threat detection
- Gain visibility into operational technology and industrial control systems
- Perform vulnerability management using the Dragos CVSS re-scoring system
- Address and tune notifications
- Conduct basic threat hunting
- Discover evidence for incident response investigations
- Perform basic Platform system administration, tuning, and troubleshooting

Delivery

The Dragos Platform Certified User course is available in two formats:

1. Virtual ILT: A virtual instructor-led course conducted completely online. Offers reduced costs for attendees and flexibility of dates.
2. On Site: An in-person two-day instructor-led course where the instructor comes to you! This custom delivery can take place at your office or other location of your choice; or, at a Dragos Training Center. Dragos Training Centers are in:
 - Hanover, Maryland (Baltimore/Washington DC suburbs)
 - Houston, Texas
 - Dubai, UAE

Agenda

Day 1

- Topic 1: Platform Benefits and Deployment
 - Benefits
 - Components and data flow
 - Deployment
- Topic 2: Navigation and Dashboards
 - Searching and filtering
 - Dashboards
 - Summary View vs. Application View
- Topic 3: Asset Inventory Application
 - Asset inventory
 - Zones
 - Asset filtering
 - Asset Details
- Topic 4: Interactive Map Application
 - Explore Map vs. Structured Map
 - Grouping and viewing assets
 - Baseline overlays
 - Protocol communications
- Topic 5: Data Explorer Application
 - Using query-focused data sets
 - Using and viewing file metadata
 - Packet captures using the task manager
- Topic 6: Notification Manager Application
 - Managing notifications
 - Creating and editing rules and cases
 - Using and managing playbooks
 - Monitoring detections
 - Dragos detection model

Day 2

- Topic 7: Content Application
 - Detections
 - Characterizations
- Topic 8: Vulnerabilities Application
 - Viewing and addressing vulnerabilities
- Topic 9: Report Manager Application
 - Report types
 - Creating and managing asset inventory reports
 - Creating and managing IOC reports
- Topic 10: Sensor Manager Application
 - Sensor monitoring
 - Network creation and sensor assignment
 - Using knowledge packs
 - Sensor health and status
- Topic 11: System Administration Application
 - User management
 - Email
 - Audit logs
 - System logs
 - Baseline settings
- Topic 12: Log Search & Visualization
 - Viewing data tables
 - Creating dashboards
- Topic 13: Documentation and Resources
 - Conclusion and Final Questions
 - Certification Exam

Scenarios and Labs

Problem-solving and hands-on skills are essential to achieving the Dragos Certified User Certification. The Certified User course contains over a dozen labs and almost a half-dozen scenarios where students will apply and demonstrate the skills they've learned. These scenarios and labs are linked to the core Dragos Use Cases and essential to successful operation of the Platform.

Labs

Lab 1	Getting Started
Lab 2	Dashboard Application
Lab 3	Asset Inventory Application
Lab 4a	Explore Map
Lab 4b	Zones and the Structured Map
Lab 5	Query-focused Datasets (QFD) Application
Lab 6a	Notification Manager Application
Lab 6b	Notification Rules
Lab 7	Content Manager Application
Lab 8	Vulnerabilities Application
Lab 9	Report Manager Application
Lab 10a	Sensor Manager Application
Lab 10b	Health + Status Tab
Lab 11	Administration Application
Lab 12	Log Search and Visualization Application

Scenarios

Scenario 1	Crown Jewel Annotation
Scenario 2	Hardware and Firmware Identification and Inventory
Scenario 3	Identifying New Assets
Scenario 4	Tuning Notifications
Scenario 5	Managing Vulnerabilities

Certification Exam

Upon successfully attending and completing all modules, students are eligible to sit for the Dragos Certified User Exam, a 50-question multiple choice exam that will test and confirm your Platform knowledge. The Exam is open book, has a time limit of 90 minutes, and requires an 80% to pass.

Those who successfully pass the Certified User Exam will achieve the Dragos Certified User Certification and become Dragos Certified Users. Certified Users will receive a certificate, a virtual badge, and early access to new Dragos information, training, and special user events.

Course Dates

Date	Time	Location
April 26-27	9 - 5 CST	Virtual
May 10-11	9 - 5 Local	In-Person, Dragos HQ
May 24-25	9 - 5 CST	Virtual
June 7-8	9 - 5 CST	Virtual
June 21-22	9 - 5 Local	In-Person, Houston
July 12-13	9 - 5 CST	Virtual
July 26-27	9 - 5 CST	Virtual
Aug 9-10	9 - 5 Local	In-Person, Chicago
Sep 13-14	9 - 5 CST	Virtual
Sep 27-28	9 - 5 Local	In-Person, SoCal

