



Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)

What you'll learn in this course

The Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) training is a 5-day Cisco threat hunting training that introduces and guides you to a proactive security search through networks, endpoints, and datasets to hunt for malicious, suspicious, and risky activities that may have evaded detection by existing tools. In this training, you will learn the core concepts, methods, and processes used in threat hunting investigations. This training provides an environment for attack simulation and threat hunting skill development using a wide array of security products and platforms from Cisco and third-party vendors.

This training prepares you for the 300-220 CBRTHD v1.0 exam. If passed, you earn the Cisco Certified Specialist – Threat Hunting and Defending certification and satisfy the concentration exam requirement for the Cisco Certified CyberOps Professional certification. This training also earns you 40 credits towards recertification.

Course duration

- Instructor-led training: 5 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 5 days of video instruction with hands-on lab practice

Who should enroll

- Security Operations Center staff
- Security Operations Center (SOC) Tier 2 Analysts
- Threat Hunters
- Cyber Threat Analysts
- Threat Managers
- Risk Managements

How to Enroll

To enroll in the CBRTHD course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

Course details

Outline

1. Threat Hunting Theory
2. Threat Hunting Concepts, Frameworks, and Threat Models
3. Threat Hunting Process Fundamentals
4. Threat Hunting Methodologies and Procedures
5. Network-Based Threat Hunting
6. Endpoint-Based Threat Hunting
7. Endpoint-Based Threat Detection Development
8. Threat Hunting with Cisco Tools
9. Threat Hunting Investigation Summary: A Practical Approach
10. Reporting the Aftermath of a Threat Hunt Investigation

Prerequisites

The knowledge and skills you are expected to have before attending this training are:

- General knowledge of networks
- Cisco CCNP Security certification

These skills can be found in the following Cisco Learning Offerings:

- Implementing and Administering Cisco Solutions (CCNA)
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)
- Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)