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

What you'll learn on this course

The Conducting Threat Hunting and Defending using Cisco Technologies for Cybersecurity (CBRTHD) training 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.

This training prepares you for the 300-220 CBRTHD exam. If passed, you earn the Cisco Certified Specialist – Threat Hunting and Defending certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Cybersecurity certification. This training also earns you 40 Continuing Education (CE) credits toward 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

How You'll Benefit

This training will help you:

- Learn how to perform 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
- Gain leading-edge career skills focused on cybersecurity
- Prepare for the 300-220 CBRTHD v1.0 exam
- Earn 40 CE credits toward recertification

Who should enroll

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

Course Objectives

- Define threat hunting and identify core concepts used to conduct threat hunting investigations
- Examine threat hunting investigation concepts, frameworks, and threat models
- Define cyber threat hunting process fundamentals
- Define threat hunting methodologies and procedures
- Describe network-based threat hunting
- Identify and review endpoint-based threat hunting
- Identify and review endpoint memory-based threats and develop endpoint-based threat detection
- Define threat hunting methods, processes, and Cisco tools that can be utilized for threat hunting
- Describe the process of threat hunting from a practical perspective
- Describe the process of threat hunt reporting

Course Outlines

- Threat Hunting Theory
- Threat Hunting Concepts, Frameworks, and Threat Models
- Threat Hunting Process Fundamentals
- Threat Hunting Methodologies and Procedures
- Network-Based Threat Hunting
- Endpoint-Based Threat Hunting
- Endpoint-Based Threat Detection Development
- Threat Hunting with Cisco Tools
- Threat Hunting Investigation Summary: A Practical Approach
- Aftermath of a Threat Hunt

Lab Outlines

- Categorize Threats with MITRE ATTACK Tactics and Techniques
- Compare Techniques Used by Different APTs with MITRE ATTACK Navigator
- Model Threats Using MITRE ATTACK and D3FEND
- Prioritize Threat Hunting Using the MITRE ATTACK Framework and Cyber Kill Chain
- Determine the Priority Level of Attacks Using MITRE CAPEC
- Explore the TaHiTI Methodology
- Perform Threat Analysis Searches Using OSINT
- Attribute Threats to Adversary Groups and Software with MITRE ATTACK

- Emulate Adversaries with MITRE Caldera
- Find Evidence of Compromise Using Native Windows Tools
- Hunt for Suspicious Activities Using Open-Source Tools and SIEM
- Capturing of Network Traffic
- Extraction of IOC from Network Packets
- Usage of ELK Stack for Hunting Large Volumes of Network Data
- Analyzing Windows Event Logs and Mapping Them with MITRE Matrix
- Endpoint Data Acquisition
- Inspect Endpoints with PowerShell
- Perform Memory Forensics with Velociraptor
- Detect Malicious Processes on Endpoints
- Identify Suspicious Files Using Threat Analysis
- Conduct Threat Hunting Using Cisco Secure Firewall, Cisco Secure Network Analytics, and Splunk
- Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
- Initiate, Conduct, and Conclude a Threat Hunt

Course Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- General knowledge of networks and network security

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)