CBRTHD - CONDUCTING THREAT HUNTING AND DEFENDING USING CISCO TECHNOLOGIES FOR CYBEROPS

Course Code: 860025

The Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) training guides you to a proactive security search through networks, endpoints, and datasets.

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.

What You'll Learn

After completing this course you should be able to:

- 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

Who Needs to Attend

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

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)

CBRTHD - CONDUCTING THREAT HUNTING AND DEFENDING USING CISCO TECHNOLOGIES FOR CYBEROPS

Course Code: 860025

VIRTUAL CLASSROOM LIVE	$5,950 CAD	5 Day

Virtual Classroom Live Outline

Threat Hunting Theory

- Threat Hunting Concepts
- Threat Hunting Types
- Conventional Threat Detection vs Threat Hunting

Threat Hunting Concepts, Frameworks and Threat Models

- Cybersecurity Concepts
- Common Threat Hunting Platforms
- Threat Hunting Frameworks
- Threat Modeling
- Case Study: Use the PASTA Threat Model

Threat Hunting Process Fundamentals

- Threat Hunting Approaches
- Threat Hunting Tactics and Threat Intelligence
- Defining Threat Hunt Scope and Boundaries
- Planning the Threat Hunt Process

Threat Hunting Methodologies and Procedures

- Investigative Thinking
- Identify Common Anomalies
- Analyze Device and System Logs
- Determine the Best Threat Hunt Methods
- Automate the Threat Hunting Process

Network-Based Threat Hunting

- Operational Security Considerations

- Performing Network Data Analysis and Detection Development
- Performing Threat Hunting in the Cloud

Endpoint-Based Threat Hunting

- Threat Hunting for Endpoint-Based Threats
- Acquiring Data from Endpoint
- Performing Host-Based Analysis

Endpoint-Based Threat Detection Development

- Analyze Endpoint Memory
- Examining Systems Memory Using Forensics
- Developing Endpoint Detection Methods
- Uncovering New Threats, Indicators and Building TTPs

Threat Hunting with Cisco Tools

- Threat Hunting with Cisco Tools
- Cisco XDR Components

Threat Hunting Investigation Summary: A Practical Approach

- Conducting a Threat Hunt

Reporting the Aftermath of a Threat Hunt Investigation

- Measure the Success of a Threat Hunt
- Report Your Findings
- Threat Hunting Outcomes

Virtual Classroom Live Labs

- Discovery Lab 1: Categorize Threats with MITRE ATTACK Tactics and Techniques
- Discovery Lab 2: Compare Techniques Used by Different APTs with MITRE ATTACK Navigator
- Discovery Lab 3: Model Threats Using MITRE ATTACK and D3FEND
- Discovery Lab 4: Prioritize Threat Hunting Using the MITRE ATTACK Framework and Cyber Kill Chain
- Discovery Lab 5: Determine the Priority Level of Attacks Using MITRE CAPEC
- Discovery Lab 6: Explore the TaHiTI Methodology
- Discovery Lab 7: Perform Threat Analysis Searches Using OSINT
- Discovery Lab 8: Attribute Threats to Adversary Groups and Software with MITRE ATTACK
- Discovery Lab 9: Emulate Adversaries with MITRE Caldera
- Discovery Lab 10: Find Evidence of Compromise Using Native Windows Tools
- Discovery Lab 11: Hunt for Suspicious Activities Using Open-Source Tools and SIEM
- Discovery Lab 12: Capturing of Network Traffic
- Discovery Lab 13: Extraction of IOC from Network Packets
- Discovery Lab 14: Usage of ELK Stack for Hunting Large Volumes of Network

Data
- Discovery Lab 15: Analyzing Windows Event Logs and Mapping Them with MITRE Matrix
- Discovery Lab 16: Endpoint Data Acquisition
- Discovery Lab 17: Inspect Endpoints with PowerShell
- Discovery Lab 18: Perform Memory Forensics with Velociraptor
- Discovery Lab 19: Detect Malicious Processes on Endpoints
- Discovery Lab 20: Identify Suspicious Files Using Threat Analysis
- Discovery Lab 21: Conduct Threat Hunting Using Cisco Secure Firewall, Cisco Secure Network Analytics, and Splunk
- Discovery Lab 22: Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
- Discovery Lab 23: Initiate, Conduct, and Conclude a Threat Hunt

Apr 6 - 10, 2026 | 8:30 AM - 4:30 PM EDT

CBRTHD - CONDUCTING THREAT HUNTING AND DEFENDING USING CISCO TECHNOLOGIES FOR CYBEROPS

Course Code: 860025

ON-DEMAND	$1,225 CAD

On-Demand Outline

Threat Hunting Theory

- Threat Hunting Concepts
- Threat Hunting Types
- Conventional Threat Detection vs Threat Hunting

Threat Hunting Concepts, Frameworks and Threat Models

- Cybersecurity Concepts
- Common Threat Hunting Platforms
- Threat Hunting Frameworks
- Threat Modeling
- Case Study: Use the PASTA Threat Model

Threat Hunting Process Fundamentals

- Threat Hunting Approaches
- Threat Hunting Tactics and Threat Intelligence
- Defining Threat Hunt Scope and Boundaries
- Planning the Threat Hunt Process

Threat Hunting Methodologies and Procedures

- Investigative Thinking
- Identify Common Anomalies
- Analyze Device and System Logs
- Determine the Best Threat Hunt Methods
- Automate the Threat Hunting Process

Network-Based Threat Hunting

- Operational Security Considerations

- Performing Network Data Analysis and Detection Development
- Performing Threat Hunting in the Cloud

Endpoint-Based Threat Hunting

- Threat Hunting for Endpoint-Based Threats
- Acquiring Data from Endpoint
- Performing Host-Based Analysis

Endpoint-Based Threat Detection Development

- Analyze Endpoint Memory
- Examining Systems Memory Using Forensics
- Developing Endpoint Detection Methods
- Uncovering New Threats, Indicators and Building TTPs

Threat Hunting with Cisco Tools

- Threat Hunting with Cisco Tools
- Cisco XDR Components

Threat Hunting Investigation Summary: A Practical Approach

- Conducting a Threat Hunt

Reporting the Aftermath of a Threat Hunt Investigation

- Measure the Success of a Threat Hunt
- Report Your Findings
- Threat Hunting Outcomes

On-Demand Labs

- Discovery Lab 1: Categorize Threats with MITRE ATTACK Tactics and Techniques
- Discovery Lab 2: Compare Techniques Used by Different APTs with MITRE ATTACK Navigator
- Discovery Lab 3: Model Threats Using MITRE ATTACK and D3FEND
- Discovery Lab 4: Prioritize Threat Hunting Using the MITRE ATTACK Framework and Cyber Kill Chain
- Discovery Lab 5: Determine the Priority Level of Attacks Using MITRE CAPEC
- Discovery Lab 6: Explore the TaHiTI Methodology
- Discovery Lab 7: Perform Threat Analysis Searches Using OSINT
- Discovery Lab 8: Attribute Threats to Adversary Groups and Software with MITRE ATTACK
- Discovery Lab 9: Emulate Adversaries with MITRE Caldera
- Discovery Lab 10: Find Evidence of Compromise Using Native Windows Tools
- Discovery Lab 11: Hunt for Suspicious Activities Using Open-Source Tools and SIEM
- Discovery Lab 12: Capturing of Network Traffic
- Discovery Lab 13: Extraction of IOC from Network Packets
- Discovery Lab 14: Usage of ELK Stack for Hunting Large Volumes of Network

Data
- Discovery Lab 15: Analyzing Windows Event Logs and Mapping Them with MITRE Matrix
- Discovery Lab 16: Endpoint Data Acquisition
- Discovery Lab 17: Inspect Endpoints with PowerShell
- Discovery Lab 18: Perform Memory Forensics with Velociraptor
- Discovery Lab 19: Detect Malicious Processes on Endpoints
- Discovery Lab 20: Identify Suspicious Files Using Threat Analysis
- Discovery Lab 21: Conduct Threat Hunting Using Cisco Secure Firewall, Cisco Secure Network Analytics, and Splunk
- Discovery Lab 22: Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
- Discovery Lab 23: Initiate, Conduct, and Conclude a Threat Hunt

CBRTHD - CONDUCTING THREAT HUNTING AND DEFENDING USING CISCO TECHNOLOGIES FOR CYBEROPS

Course Code: 860025

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.