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

Category: Networking & Security | **Vendor:** Cisco

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Cisco Certified Specialist – Threat Hunting and Defending, Cisco Certified Network Professional (CCNP) Cybersecurity, Cisco Certified CyberOps Professional
Related Exam:	300-220

Course Overview

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. In this training, you will learn the core concepts, methods, and processes used in threat hunting investigations. Threat hunting involves going beyond what Security Operations Center (SOC) analysts already know or have been alerted to. Traditional cyber detection technologies will only identify malicious risks and behaviors. The art of threat hunting is about venturing into the unknown. 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. You will perform genuine threat hunting exercises within simulated network environments.

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 Network Professional (CCNP) Cybersecurity certification.

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

What to Expect in the Exam

Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (300-220 CBRTHD v1.0) is a 90-minute exam associated with the Cisco Certified Specialist – Threat Hunting and Defending certification and satisfies the concentration exam requirement for the Cisco Certified

CyberOps Professional certification.

The exam tests your knowledge of conducting threat hunting and defending, including:

- Threat modeling techniques
- Threat actor attribution techniques
- Threat hunting techniques, processes, and outcomes

About 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. In this training, you will learn the core concepts, methods, and processes used in threat hunting investigations. Threat hunting involves going beyond what Security Operations Center (SOC) analysts already know or have been alerted to. Traditional cyber detection technologies will only identify malicious risks and behaviors. The art of threat hunting is about venturing into the unknown. 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. You will perform genuine threat hunting exercises within simulated network environments.

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 Network Professional (CCNP) Cybersecurity certification.

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

What to Expect in the Exam

Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (300-220 CBRTHD v1.0) is a 90-minute exam associated with the Cisco Certified Specialist – Threat Hunting and Defending certification and satisfies the concentration exam requirement for the Cisco Certified

CyberOps Professional certification.

The exam tests your knowledge of conducting threat hunting and defending, including:

- Threat modeling techniques
- Threat actor attribution techniques
- Threat hunting techniques, processes, and outcomes

Who Should Attend

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

Prerequisites & Entry Requirements

General 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)

Learning Outcomes

Upon successful completion of this course, participants will 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

Detailed Course Outline

- 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

□□ Certification Path

Cisco Certified Specialist – Threat Hunting and Defending, Cisco Certified Network Professional (CCNP) Cybersecurity, Cisco Certified CyberOps Professional

Exam: 300-220

Skills You Will Learn:

- 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

Frequently Asked Questions

Q: What delivery options are available for Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) course helps prepare you for the Cisco Certified Specialist – Threat Hunting and Defending, Cisco Certified Network Professional (CCNP) Cybersecurity, Cisco Certified CyberOps Professional certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 300-220 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)?

Yes, we provide corporate training, dedicated training, and closed classes for Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps, Cisco Professional Level Cybersecurity - CCNP Cybersecurity, CBRTHD

Q: Why choose Nexus Human for Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)