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

ID CBRTHD   **Preis** 3.890,– € (exkl. MwSt.)   **Dauer** 5 Tage

Kursüberblick

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

Zielgruppe

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

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Professional (CCNP CYBERSECURITY)

Voraussetzungen

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) v2.2](#)

- [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)](#)
- [Performing CyberOps Using Cisco Security Technologies (CBRCOR)](#)

Kursziele

- 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

Detaillierter Kursinhalt

- 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

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services
✓ Highend-Technologietraining
✓ Business- & Softskill-Training
✓ Consulting Services
✓ Managed Training Services
✓ Digitale Lernlösungen
✓ Content-Entwicklung
✓ Remote Labs
✓ Talentprogramme
✓ Eventmanagement-Services

Trainingsmethoden
✓ Klassenraumtraining
✓ Instructor-Led Online Training
✓ FLEX Classroom – Klassenraum und ILO kombiniert
✓ Onsite & Customized Training
✓ E-Learning
✓ Blended & Hybrid Learning
✓ Mobiles Lernen

Technologien und Lösungen
✓ Digitale Transformation
✓ Artificial Intelligence (AI)
✓ Cloud
✓ Networking
✓ Cyber Security
✓ Wireless & Mobility
✓ Modern Workplace
✓ Data Center
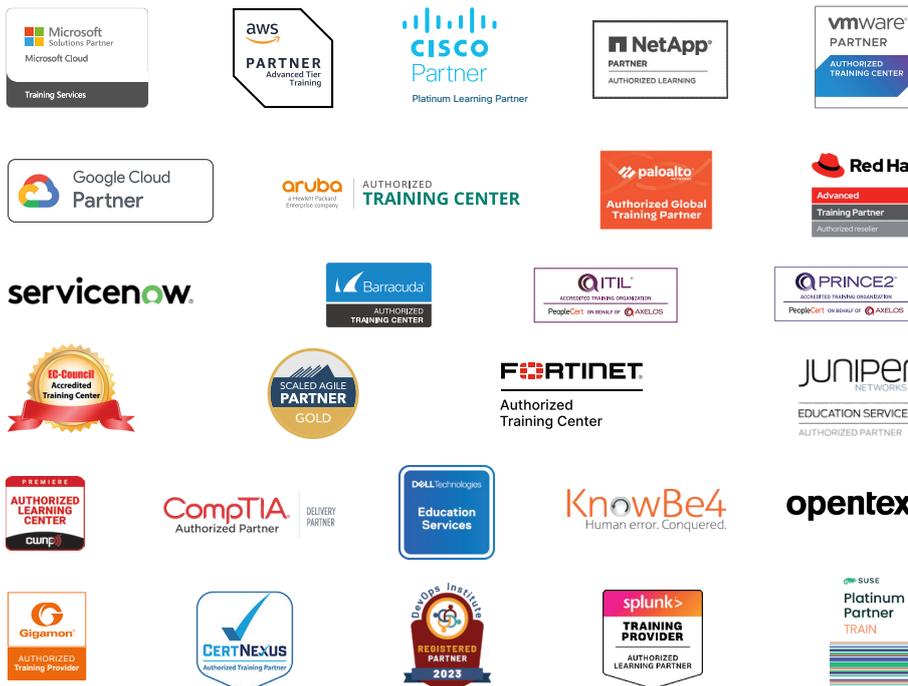
Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610

info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080

info@flane.ch / www.flane.ch