

# CBRTHD

## Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Das Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (CBRTHD) Training ist ein 5-tägiges Cisco Threat Hunting Training, das Sie in eine proaktive Sicherheitssuche durch Netzwerke, Endpunkte und Datensätze einführt und anleitet, um nach schädlichen, verdächtigen und riskanten Aktivitäten zu suchen, die sich der Erkennung durch bestehende Tools entzogen haben. In dieser Schulung lernen Sie die wichtigsten Konzepte, Methoden und Prozesse kennen, die bei Threat Hunting-Untersuchungen zum Einsatz kommen. Diese Schulung bietet eine Umgebung für die Simulation von Angriffen und die Entwicklung von Threat Hunting-Fähigkeiten unter Verwendung einer breiten Palette von Sicherheitsprodukten und -plattformen von Cisco und Drittanbietern. Diese Schulung bereitet Sie auf die CBRTHD-Prüfung vor.

### 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
- Reporting the Aftermath of a Threat Hunt Investigation

**E-Book** Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlagen stattdessen in die Lernerfläche integriert.

### Zielgruppe

Diese Schulung ist für die folgenden Rollen konzipiert:

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

### Voraussetzungen

Folgende Kenntnisse und Fähigkeiten sollten Sie für die Teilnahme an dieser Schulung mitbringen:

- Allgemeine Kenntnisse über Netzwerke
- Cisco CCNP Security-Zertifizierung

Diese Kenntnisse können Sie in den folgenden Cisco-Lernangeboten finden:

- 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)

### Kursziel

Diese Schulung bereitet Sie auf die CBRTHD-Prüfung vor. Bei Bestehen erhalten Sie die Zertifizierung „Cisco Certified Specialist - Threat Hunting and Defending“ und erfüllen die Anforderung des Concentration Exam für die Zertifizierung „CCNP Cybersecurity“.

### Bearbeitungszeit

ca. 30 Stunden

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/CBRT](http://www.experteach.at/go/CBRT)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

### Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

### Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung € 900,-

### Training Preise zzgl. MwSt.

**Termine in Österreich** 5 Tage € 3.950,-

**Online Training** 5 Tage € 3.950,-

**Termin/Kursort** Kurssprache Deutsch

05.10.-09.10.26 Online 05.10.-09.10.26 Wien

# Inhaltsverzeichnis

## CBRTHD – Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Course outline	Conduct Threat Hunt Using Cisco XDR Control Center and Investigate
Threat Hunting Theory	Initiate, Conduct, and Conclude a Threat Hunt
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	
Reporting the Aftermath of a Threat Hunt Investigation	
Lab outline	
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	

