

Der Kurs Performing Cybersecurity Using Cisco Security Technologies (CBRCOR) führt Sie durch die Grundlagen, Methoden und Automatisierung von Cybersicherheitsvorgängen. Die Kenntnisse, die Sie in diesem Kurs erwerben, bereiten Sie auf die Rolle des Information Security Analyst in einem Security Operations Center (SOC)-Team vor.

Sie lernen grundlegende Konzepte und deren Anwendung in realen Szenarien kennen und lernen, wie Sie Playbooks bei der Formulierung einer Incident Response (IR) nutzen können. Der Kurs vermittelt Ihnen, wie Sie Automatisierung für die Sicherheit mithilfe von Cloud-Plattformen und einer SecDevOps-Methodik einsetzen. Sie lernen die Techniken kennen, um Cyberangriffe zu erkennen, Bedrohungen zu analysieren und geeignete Empfehlungen zur Verbesserung der Cybersicherheit zu geben.

Dieser Kurs bringt Ihnen auch 40 Continuing Education (CE) Credits für die Rezertifizierung und bereitet Sie auf das 350-201 CBRCOR Core Exam innerhalb der Zertifizierung CCNA Cybersecurity vor.

Kursinhalt

- Describe the types of service coverage within a SOC and operational responsibilities associated with each
- Compare security operations considerations of cloud platforms
- Describe the general methodologies of SOC platforms development, management, and automation
- Describe asset segmentation, segregation, network segmentation, microsegmentation, and approaches to each, as part of asset controls and protections
- Describe Zero Trust and associated approaches, as part of asset controls and protections
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC
- Use different types of core security technology platforms for security monitoring, investigation, and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats (e.g., JavaScript Object Notation (JSON), HTML, XML, and Comma-Separated Values (CSV))
- Describe API authentication mechanisms
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
- Interpret the sequence of events during an attack based on analysis of traffic patterns
- Describe the different security tools and their limitations for network analysis (e.g., packet capture tools, traffic analysis tools, and network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

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 Lernoberfläche integriert.

Zielgruppe

Der Kurs eignet sich besonders für folgende Zielgruppen:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC-Analysten, die derzeit auf Einstiegsstufe tätig sind und mindestens 1 Jahr Erfahrung haben

Bei erfolgreichem Abschluss des Exams erhalten Sie die Zertifizierung „Cisco Certified Specialist – Cybersecurity Core“ und erfüllen die Kernprüfungsanforderungen für die Zertifizierung „Cisco Certified Cybersecurity Professional“.

Voraussetzungen

Obwohl es keine zwingenden Voraussetzungen gibt, sollten Sie folgende Kenntnisse mitbringen, um von diesem Kurs in vollem Umfang profitieren zu können:

- Vertrautheit mit UNIX/Linux-Shell (bash, csh) und Shell-Befehlen
- Vertrautheit mit den Splunk-Such- und Navigationsfunktionen
- Grundkenntnisse der Skripterstellung mit Python, JavaScript, PHP oder ähnlichem.

Empfohlene Cisco-Angebote, die Ihnen bei der Vorbereitung auf diesen Kurs helfen können:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Implementing and Administering Cisco Solutions (CCNA)

Kursziel

Bereiten Sie sich auf die Prüfung CBROPS vor. Sie erlernen grundlegende Cybersicherheitskompetenzen in den Bereichen SOC-Betrieb, Bedrohungserkennung und Incident Response anhand praxisnaher Übungen und Szenarien. Sammeln Sie praktische Erfahrungen mit führenden Sicherheitstools wie Cisco XDR, Splunk Phantom und Firepower NGFW. Lernen Sie Automatisierungs- und SecDevOps-Verfahren kennen, um die Effizienz und Effektivität Ihrer Sicherheitsmaßnahmen zu verbessern.

Bearbeitungszeit

ca. 30 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/CBRC

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 € 1.000,-

Training Preise zzgl. MwSt.

Termine in Deutschland 5 Tage € 3.950,-

Termine in Österreich 5 Tage € 3.950,-

Online Training 5 Tage € 3.950,-

Termin/Kursort Kurssprache Deutsch

06.07.-10.07.26 Frankfurt 02.11.-06.11.26 Online

06.07.-10.07.26 Online 02.11.-06.11.26 Wien

Inhaltsverzeichnis

CBRCOR – Performing Cybersecurity Using Cisco Security Technologies

Course Outline

Understanding Risk Management and SOC Operations
Understanding Analytical Processes and Playbooks
Understanding Cloud Service Model Security Responsibilities
Understanding Enterprise Environment Assets
Understanding APIs
Understanding SOC Development and Deployment Models
Investigating Packet Captures, Logs, and Traffic Analysis
Investigating Endpoint and Appliance Logs
Implementing Threat Tuning
Threat Research and Threat Intelligence Practices
Performing Security Analytics and Reports in a SOC
Malware Forensics Basics
Threat Hunting Basics
Performing Incident Investigation and Response

Lab Outline

Explore Cisco XDR
Explore Splunk Phantom Playbooks
Evaluate Assets in a Typical Enterprise Environment
Fix a Python API Script
Create Bash Basic Scripts
Examine Cisco Firepower Packet Captures and PCAP Analysis
Validate an Attack and Determine the Incident Response
Submit a Sample to Cisco Secure Malware Analytics for Analysis
Endpoint-Based Attack Scenario Referencing MITRE ATTACK®
Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
Investigate IOCs using Cisco XDR
Explore the ThreatConnect Threat Intelligence Platform
Track the TTPs of a Successful Attack Using a TIP
Reverse Engineer Malware
Perform Threat Hunting
Conduct an Incident Response

