AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

Understanding Cisco Cybersecurity Operations Fundamentals
CCNACBR

Dauer	5 Tage 18.10.2027
Kursstart/Status	18.10.2027 08:30-12:00 / 13:00-16:30
Kursort	ExperTeach online
Kosten	CHF 4345.00 Der Team Captain des Kunden muss die CLCs spätestens drei Arbeitstage vor Kursstart bei Cisco im Learning Locator eingelöst haben. Ist dies nicht der Fall, so wird die Kursteilnahme über normale Rechnungsstellung verrechnet.
Sprache	Deutsch
Dokumentation	Es wird immer die aktuellste Version geschult. Offizielle Cisco Kurs- und Labunterlagen in Englisch.

Überblick

Bitte beachten Sie: Am 03. Februar 2026 wurde das Examen 200-201 CBROPS umbenannt in 200-201 CCNACBR: Understanding Cisco Cybersecurity Operations Fundamentals. Im Rahmen dieses umfangreichen Updates wurde die Schulung im Juli 2026 dann ebenfalls von „Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.2“ in „Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR) v2.0“ umbenannt. Auch die Lernziele und Produktnamen wurden entsprechend aktualisiert.

Das Training vermittelt ein Verständnis für die Geräte der Netzwerkinfrastruktur, den Betrieb und die Schwachstellen der TCP/IP-Protokollsuite sowie für die grundlegenden Konzepte der Informationssicherheit, für den Betrieb und die Angriffe gängiger Netzwerkanwendungen, für die Betriebssysteme Windows und Linux und für die Arten von Daten, die zur Untersuchung von Sicherheitsvorfällen verwendet werden.

Nach Abschluss dieser Schulung verfügen Sie über die erforderlichen Grundkenntnisse, um die Aufgaben eines Cybersecurity Analyst auf Associate-Ebene in einem bedrohungsorientierten Security Operations Center (SOC) wahrzunehmen.

Voraussetzungen

Für diese Schulung gibt es keine Voraussetzungen. Es wird jedoch empfohlen, dass Sie über folgende Kenntnisse und Fähigkeiten verfügen, bevor Sie an dieser Schulung teilnehmen:

- Kenntnisse im Bereich Ethernet- und TCP/IP-Netzwerke
- Praktische Kenntnisse der Betriebssysteme Windows und Linux
- Kenntnisse der Grundlagen von Netzwerksicherheitskonzepten

Der Kurs CCNA - Implementing and Administering Cisco Solutions kann Ihnen helfen, diese Kenntnisse zu erwerben.

Lernziel

- Diese Schulung bereitet Sie auf die Prüfung „200-201 CCNACBR v1.2“ vor. Bei erfolgreichem Bestehen erhalten Sie die Zertifizierung „Cisco Certified Network Associate (CCNA) Cybersecurity“ und können als Junior- oder Einsteiger-Analyst für Cybersicherheitsoperationen in einem SOC tätig werden.
- Erwerben Sie grundlegende Kenntnisse und praktische Erfahrungen zur Prävention und Abwehr von Cyberangriffen als Teil eines SOC-Teams.
- Eignen Sie sich das erforderliche Grundwissen an, um als Cybersicherheitsanalyst auf Einstiegsebene in einem bedrohungsorientierten SOC zu arbeiten.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Verstehen Sie wichtige Sicherheitskonzepte, darunter Betriebssysteme, Endpunktsicherheit, Netzwerküberwachung, Kryptografie und Grundlagen der Cloud-Sicherheit.
- Entwickeln Sie durch Übungen und Simulationen praktische Fähigkeiten in den Bereichen Bedrohungserkennung, Untersuchung von Vorfällen sowie der Anwendung von SOC-Playbooks und Reaktionsplänen.

Zielgruppe

Dieser Kurs richtet sich an Cybersecurity Analysts auf Associate-Ebene, die in Security Operation Centers arbeiten.

Kursinhalt

- Explain the foundational aspects of SOCs, including their types, key roles, and essential metrics for measuring effectiveness
- Apply foundational security principles and risk management concepts to assess and protect organizational assets
- Compare and apply various access control models to secure network resources and enforce organizational policies
- Differentiate between various cloud deployment and service models and explain the shared responsibility for security in cloud environments
- Explain the fundamental concepts of cryptography, differentiate between various cryptographic algorithms, and explain how cryptographic principles are applied in real-world protocols and systems, including key exchange, digital signatures, and SSL/TLS
- Identify and describe the fundamental components and operational aspects of the Windows operating system for security analysis
- Identify and describe the fundamental components and operational aspects of the Linux operating system for security analysis
- Utilize Command Line Interfaces (CLIs) for basic system interaction, file management, and security-related tasks in both Windows and Linux environments
- Explain the operations and identify the security implications of foundational network protocols
- Describe and differentiate various network security controls and their application in protecting network infrastructure
- Differentiate between various Intrusion Detection and Prevention Systems (IDS/IPS) and interpret their output for security monitoring
- Describe and compare various endpoint security solutions and their effectiveness against common threats
- Identify and categorize various cyber threat actors based on their motivations, capabilities, and common tactics
- Explain the phases of the Classic Cyber Kill Chain model and identify adversary actions within each phase
- Apply the MITRE ATT&CK Framework to analyze and map cyber threats, explain its structure and application, and leverage it to enhance threat detection, incident response, and communication within a security operations environment

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Identify and describe various social engineering attack vectors, including those enhanced by generative AI
- Describe fundamental network attack techniques that exploit protocol vulnerabilities
- Describe advanced attack vectors and emerging threats in the current cybersecurity landscape
- Identify and explain various types of Network Security Monitoring (NSM) data and their role in incident investigation
- Identify and interpret various log data sources from operating systems, network devices, and security tools
- Explain NetFlow operations and its application as a security tool for network monitoring and anomaly detection
- Describe common web application attacks and their exploitation methods
- Apply advanced log analysis techniques to interpret security data and identify patterns of suspicious behavior
- Perform packet capture analysis and apply digital forensics processes to investigate security incidents. Focus on the 5-tuple and timestamps to correlate with other logs, as this is your primary tool for network forensics
- Explain malware analysis outputs and apply threat intelligence frameworks for security investigations
- Explain the architecture, core functions, and best practices for implementing SIEM solutions for effective security monitoring
- Explain the features and common use cases of SOAR platforms for automating and streamlining incident response
- Explain the Cisco XDR platform, its core functions, features, and components for unified threat detection and response
- Differentiate between the legacy and modern NIST incident response guidance (NIST SP 800-61 Rev 2 and NIST SP 800-61 Rev 3 special publications), describe core IR components aligned with the NIST CSF 2.0 framework, and identify how these practices satisfy CMMC requirements for the Defense Industrial Base (DIB)
- Describe the roles, categories, and operational services of Computer Security Incident Response Teams (CSIRTs)
- Explain the concept of security monitoring playbooks and their components for standardizing incident response
- Apply various threat hunting methodologies to proactively identify and mitigate hidden threats within a network.

Zertifizierung

Die Prüfung zum Verständnis der Grundlagen von 200-201 CCNACBR: Understanding Cisco Cybersecurity Operations Fundamentals ist ein 120-minütiges Exam, das mit der Zertifizierung als Cisco Certified CyberSec Associate verbunden ist. Die CCNACBR-Prüfung testet die Kenntnisse und Fähigkeiten eines Kandidaten in Bezug auf Sicherheitskonzepte, Sicherheitsüberwachung, hostbasierte Analyse, Netzwerkeinbruchanalyse sowie Sicherheitsrichtlinien und -verfahren. Der Kurs „Understanding Cisco Cybersecurity Operations Fundamentals“ hilft Kandidaten, sich auf diese Prüfung vorzubereiten.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100