

Cisco - Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Der Kurs "Cisco - Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0" führt Sie durch die Grundlagen, Methoden und Automatisierung von Cybersecurity Operations. Die Kenntnisse, die Sie in diesem Kurs erwerben, bereiten Sie auf die Rolle des Information Security Analysten in einem Security Operations Center (SOC) Team vor. Sie lernen grundlegende Konzepte und deren Anwendung in realen Szenarien kennen und erfahren, wie Sie Playbooks bei der Formulierung einer Incident Response (IR) einsetzen können. In diesem Kurs lernen Sie, wie Sie mit Hilfe von Cloud-Plattformen und einer SecDevOps-Methodik die Automatisierung für die Sicherheit nutzen können. Sie lernen die Techniken zur Erkennung von Cyberangriffen, zur Analyse von Bedrohungen und zur Erstellung geeigneter Empfehlungen zur Verbesserung der Cybersicherheit.

Mit diesem Kurs erhalten Sie außerdem 40 Fortbildungspunkte (CE) für die Rezertifizierung und werden auf die CBRCOR-Kernprüfung 350-201 vorbereitet.

Was Sie bei der Prüfung erwartet:

350-201 Performing CyberOps Using Cisco Security Technologies (CBRCOR) ist eine 120-minütige Prüfung im Rahmen der Cisco CyberOps Professional Certification. Das Multiple-Choice-Format prüft das Wissen über zentrale Cybersecurity-Operationen, einschließlich Cybersecurity-Grundlagen, Techniken, Richtlinien, Prozesse und Automatisierung.

In der Prüfung werden Kenntnisse in den folgenden Bereichen geprüft:

- Überwachung auf Cyberangriffe
- Analyse großer Datenmengen mithilfe von Automatisierungstools und -plattformen - sowohl Open Source als auch kommerziell
- Genaue Identifizierung der Art des Angriffs und Ausarbeitung eines Plans zur Schadensbegrenzung
- Szenariobasierte Fragen; z. B. werden Sie anhand eines Screenshots der Ausgabe eines Tools aufgefordert, Teile der Ausgabe zu interpretieren und Schlussfolgerungen zu ziehen.

Angesprochener Teilnehmerkreis:

- Cybersecurity Engineer
- Cybersecurity Investigator
- Incident Manager
- Incident Ansprechpartner
- Netzwerktechniker
- SOC-Analysten, die derzeit auf Einstiegsebene arbeiten und über mindestens 1 Jahr Erfahrung verfügen.

Hinweis:

Kursprache ist Deutsch, die Unterlagen sind in englischer Sprache (teilweise in digitaler Form). Dieses Seminar führen wir in Kooperation mit der Fast Lane GmbH durch.

Seminar- bzw. Schulungsinhalte

- Die Arten der Serviceabdeckung innerhalb eines SOC und die damit verbundenen operativen Verantwortlichkeiten.
- Überlegungen zum Sicherheitsbetrieb von Cloud-Plattformen vergleichen.
- Die allgemeinen Methoden der Entwicklung, Verwaltung und Automatisierung von SOC-Plattformen.
- Erläutern von Asset-Segmentierung, Segregation, Netzwerk-Segmentierung, Mikro-Segmentierung und den jeweiligen Ansätzen als Teil von Asset-Kontrollen und Schutzmaßnahmen.
- Beschreibung von Zero Trust und damit verbundenen Ansätzen als Teil von Asset-Kontrollen und -Schutzmaßnahmen.
- Durchführung von Incident-Analysen mit Hilfe von Security Information and Event Management (SIEM) und/oder Security Orchestration and Automation (SOAR) im SOC.
- Verwendung verschiedener Arten von zentralen Sicherheitstechnologieplattformen für die Sicherheitsüberwachung, Untersuchung und Reaktion.
- DevOps- und SecDevOps-Prozesse beschreiben.
- Erläuterung der gängigen Datenformate, z. B. JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Beschreiben Sie API-Authentifizierungsmechanismen.
- Analysieren des Ansatzes und der Strategien zur Erkennung von Bedrohungen während der Überwachung, Untersuchung und Reaktion.
- Bekannte Indikatoren für eine Gefährdung (Indicators of Compromise, IOCs) und Angriffsindikatoren (Indicators of Attack, IOAs).
- Interpretation der Abfolge von Ereignissen während eines Angriffs auf der Grundlage der Analyse von Verkehrsmustern.
- Beschreibung der verschiedenen Sicherheitstools und ihrer Grenzen für die Netzwerkanalyse (z. B. Tools zur Paketaufzeichnung, Tools zur Traffic-Analyse, Tools zur Analyse von Netzwerkprotokollen).
- Analyse von anomalem Benutzer- und Entitätsverhalten (UEBA).
- Proaktive Bedrohungssuche nach Best Practices durchführen.

Seminar- bzw. Schulungsvoraussetzungen

- Grundlegende Erfahrung mit UNIX/Linux-Shells (bash, csh) und Shell-Befehlen
 - Grundlegende Erfahrung mit den Such- und Navigationsfunktionen von Splunk
 - Grundlegende Kenntnisse in der Skripterstellung mit Python, JavaScript, PHP o.ä.
- Empfohlene Cisco-Angebote, die Ihnen bei der Vorbereitung auf diesen Kurs helfen können:
- Implementieren und Verwalten von Cisco-Lösungen (CCNA)
 - Cisco Cybersecurity Operations Fundamentals verstehen (CBROPS)

Seminarart

Dieses Seminar können Sie als **Präsenzseminar** oder als **Live-Online-Training** (virtuelles Präsenzseminar) buchen.

Dauer

5 Tage von 09:00 bis 17:00 Uhr

Preise

Teilnahmegebühr: ab 3.950,00 € (4.700,50 € inkl. 19% MwSt.) Preis abhängig vom Standort

Im Preis enthalten sind Kursmaterial, Pausenverpflegung, Getränke und Schulungszertifikat.

Anmeldung

Bitte [online](#) anmelden oder per [Fax](#).

Termine

Die aktuellen Termine und Standorte für Cisco - Performing CyberOps Using Cisco Security Technologies (CBRCOR) finden Sie [online](#).

Weitere Seminare

Alle Seminare finden Sie in unserer [Seminarübersicht](#).

Gerne unterbreiten wir Ihnen auch ein individuelles Angebot entsprechend Ihrer Wünsche und Vorstellungen. Senden Sie hierfür Ihre Anfrage einfach an training@pc-college.de.

Erstellt am 01.11.2024

Viele Partner für ein Ziel: Beste Leistung und Rundum-Service

Live-Online-Training

Berlin
Bremen
Dortmund
Dresden
Düsseldorf
Erfurt
Essen
Frankfurt
Freiburg
Hamburg
Hannover
Jena
Karlsruhe
Kassel
Koblenz
Köln
Krefeld
Leipzig
Mannheim
München
Münster
Nürnberg
Paderborn
Regensburg
Saarbrücken
Siegen
Stuttgart
A-Wien
CH-Basel
CH-Bern
CH-Zürich



PC-COLLEGE Zentrale Berlin

Stresemannstraße 78 (Nähe Potsdamer Platz) | D-10963 Berlin
Telefon: 0800 5777 333 / +49 (0)30 235 0000 | Fax: +49 30 2142988 | E-Mail: training@pc-college.de
Ansprechpartner*in: Stefanie Wendt und Kollegen*innen

Alle Informationen und Aktionsangebote finden Sie unter www.pc-college.de