Performing CyberOps Using Cisco Security Technologies (CBRCOR)

ID CBRCOR **Preis** 3.950,– € (exkl. MwSt.) **Dauer** 5 Tage

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Die Schulung **Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)** führt Sie durch die Grundlagen, Methoden und Automatisierung von Cybersecurity-Operationen. Das Wissen, das Sie in dieser Schulung erwerben, bereitet 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 sowie den Einsatz von Playbooks bei der Formulierung einer Incident Response (IR). In der Schulung 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 Abgabe geeigneter Empfehlungen zur Verbesserung der Cybersicherheit.

Dieses Training bereitet Sie auf die Prüfung 350-201 CBRCOR v1.2 vor. Bei Bestehen erhalten Sie die Cisco Certified Specialist - Cybersecurity Core Zertifizierung und erfüllen die Kernprüfungsanforderung für das Cisco Certified Cybersecurity Professional / CCNP Cybersecurity (CCNP CYBERSECURITY)

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

- Entwicklung grundlegender Cybersecurity-Fähigkeiten in den Bereichen SOC-Betrieb, Erkennung von Bedrohungen und Reaktion auf Vorfälle durch praktische Übungen und Szenarien
- Sammeln Sie praktische Erfahrungen mit führenden Sicherheitstools wie Cisco XDR, Splunk Phantom und Firepower NGFW
- Erlernen von Automatisierungs- und SecDevOps-Praktiken zur Verbesserung der Effizienz und Effektivität von Sicherheitsabläufen
- Vorbereitung auf die Prüfung 350-201 CBRCOR v1.2
- Erwerben Sie 40 CE-Punkte für die Rezertifizierung

Was Sie bei der Prüfung erwartet

Performing Cybersecurity Using Cisco Security Technologies (350-201 CBRCOR) v1.2 ist eine 120-minütige Prüfung, die mit der Cisco Certified Specialist - Cybersecurity Core Zertifizierung verbunden ist und die Kernprüfungsanforderungen für die Cisco Certified Cybersecurity Professional Zertifizierung erfüllt.

Diese Prüfung prüft Ihr Wissen über die wichtigsten Cybersecurity-Vorgänge, einschließlich:

- Grundlagen der Cybersicherheit
- Techniken
- Prozesse
- Automatisierung

Zielgruppe

Obwohl es keine zwingenden Voraussetzungen gibt, ist der Kurs besonders für die folgenden Zielgruppen geeignet:

- Cybersecurity-Ingenieur
- Cybersecurity-Ermittler
- Vorfallsmanager
- Ansprechpartner für Vorfälle
- Netzwerktechniker
- SOC-Analysten, die derzeit auf Einstiegsebene tätig sind und über mindestens 1 Jahr Erfahrung verfügen

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Professional / CCNP Cybersecurity (CCNP CYBERSECURITY)

Voraussetzungen

Obwohl es keine zwingenden Voraussetzungen gibt, sollten Sie über die folgenden Kenntnisse verfügen, um von diesem Kurs profitieren zu können:

- Vertrautheit mit UNIX/Linux-Shells (bash, csh) und Shell-Befehlen
- Vertrautheit mit den Such- und Navigationsfunktionen von Splunk
- Grundlegende Kenntnisse der Skripterstellung unter Verwendung von Python, JavaScript, PHP o.ä.

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

- Implementing and Administering Cisco Solutions (CCNA) v2.2
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Kursziele

- Beschreiben Sie die Arten der Dienstabdeckung innerhalb einer SOC und die damit verbundenen operativen Verantwortlichkeiten
- Vergleich der Sicherheitsaspekte von Cloud-Plattformen
- Beschreiben Sie die allgemeinen Methoden der Entwicklung, Verwaltung und Automatisierung von SOC-Plattformen
- Beschreibung der Segmentierung von Vermögenswerten, der Segregation, der Netzwerksegmentierung, der Mikrosegmentierung und der jeweiligen Ansätze als Teil der Kontrolle und des Schutzes von Vermögenswerten
- Beschreiben Sie Zero Trust und damit verbundene Ansätze als Teil der Vermögenskontrolle und des Vermögensschutzes
- Durchführung von Vorfallsuntersuchungen unter Verwendung 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
- Beschreiben Sie die DevOps- und SecDevOps-Prozesse
- Beschreiben Sie die gängigen Datenformate (z. B. JavaScript Object Notation (JSON), HTML, XML und Comma-Separated Values (CSV)).
- Beschreiben Sie API-Authentifizierungsmechanismen
- Analyse des Ansatzes und der Strategien zur Erkennung von Bedrohungen während der Überwachung, Untersuchung und Reaktion
- Ermitteln bekannter Indikatoren für die Gefährdung (IOCs) und Indikatoren für Angriffe (IOAs)
- Interpretation der Abfolge von Ereignissen während eines Angriffs auf der Grundlage einer Analyse der Verkehrsmuster
- Beschreiben Sie die verschiedenen Sicherheitstools und ihre Grenzen für die Netzwerkanalyse (z. B. Tools zur Paketaufzeichnung, zur Analyse des Datenverkehrs und zur Analyse von Netzwerkprotokollen)
- Analysieren Sie anomales Nutzer- und Entitätsverhalten (UEBA)
- Proaktive Bedrohungssuche nach bewährten Verfahren

Detaillierter Kursinhalt

- Verstehen von Risikomanagement und SOC-Operationen
- Analytische Prozesse und Playbooks verstehen
- Verständnis der Sicherheitsverantwortung des Cloud-Service-Modells
- Verstehen der Vermögenswerte der Unternehmensumgebung
- Verstehen von APIs
- Verständnis der SOC-Entwicklungs- und Bereitstellungsmodelle
- Untersuchen von Paketaufzeichnungen, Protokollen und Verkehrsanalysen
- Untersuchen von Endpunkt- und Appliance-Protokollen
- Implementierung der Bedrohungsabstimmung
- Praktiken der Bedrohungsforschung und Bedrohungsanalyse
- Durchführung von Sicherheitsanalysen und Berichten in einem SOC
- Grundlagen der Malware-Forensik
- Grundlagen der Bedrohungsjagd
- Untersuchung von und Reaktion auf Vorfälle

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