

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS 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 **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)** 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 grundlegenden Kenntnisse, die für die Ausübung der Rolle eines Cybersecurity-Analysten auf Associate-Ebene in einem bedrohungszentrierten Security Operations Center (SOC) erforderlich sind.

Diese Schulung bereitet Sie auf die Prüfung 200-201 CBROPS v1.2 vor. Bei Bestehen erhalten Sie die Cisco Certified Cybersecurity Associate Zertifizierung und die Rolle eines Junior oder Entry-Level Cybersecurity Operations Analyst in einem SOC.

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

- Erlernen Sie die grundlegenden Fähigkeiten, Techniken und Technologien sowie die praktischen Übungen, die zur Verhinderung und Abwehr von Cyberangriffen als Teil eines SOC-Teams erforderlich sind.
- Vorbereitung auf die Prüfung 200-201 CBROPS v1.2
- Verdienen Sie 30 CE-Punkte für die Rezertifizierung

Was Sie bei der Prüfung erwarten

Die 200-201 CBROPS-Prüfung ist eine 120-minütige Bewertung für die Cisco Certified CyberOps Associate-Zertifizierung und ist auf die Berufsrolle des Cybersecurity Operations Analysten auf Associate-Ebene abgestimmt. Die CBROPS-Prüfung testet das Wissen und die Fähigkeiten eines Kandidaten in Bezug auf Sicherheitskonzepte, Sicherheitsüberwachung, hostbasierte Analyse, Analyse von Netzwerkeinbrüchen sowie Sicherheitsrichtlinien und -verfahren.

Zielgruppe

Diese Schulung richtet sich an Personen, die eine Rolle als Cybersicherheitsanalytiker auf Associate-Ebene anstreben, sowie an IT-Fachleute, die Kenntnisse im Bereich Cybersicherheitsoperationen erwerben möchten, oder an Personen, die die Zertifizierung Cisco Certified CyberOps Associate anstreben:

- Studenten, die einen technischen Abschluss anstreben
- Derzeitige IT-Fachleute
- Neue Hochschulabsolventen mit technischem Abschluss

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Associate / CCNA Cybersecurity (CCNA CYBERSECURITY)

Voraussetzungen

Bevor Sie an dieser Schulung teilnehmen, sollten Sie über die folgenden Kenntnisse und Fähigkeiten verfügen:

- Vertrautheit mit Ethernet und TCP/IP-Netzwerken
- Gute Kenntnisse der Betriebssysteme Windows und Linux
- Vertrautheit mit den Grundlagen von Netzwerksicherheitskonzepten

Der folgende Cisco-Kurs kann Ihnen helfen, das Wissen zu erwerben, das Sie zur Vorbereitung auf diesen Kurs benötigen:

Implementing and Administering Cisco Solutions (CCNA) v2.2

Kursziele

Nach dieser Schulung sollten Sie in der Lage sein:

- Erläutern Sie die Funktionsweise eines SOC und beschreiben Sie die verschiedenen Arten von Dienstleistungen, die aus der Sicht eines Tier-1-SOC-Analysten erbracht werden.
- Erläuterung der Verwendung von SOC-Kennzahlen zur Messung der Wirksamkeit des SOC
- Erläuterung des Einsatzes eines Workflow-Management-Systems und der Automatisierung zur Verbesserung der Effizienz des SOC
- Beschreiben Sie die Merkmale und Funktionen des Windows-Betriebssystems
- einen Überblick über das Linux-Betriebssystem zu geben
- Verstehen gängiger Sicherheitstechnologien für Endgeräte
- Erläuterung der Tools zur Überwachung der Netzwerksicherheit (NSM), die dem Netzwerksicherheitsanalysten zur Verfügung stehen
- Beschreibung von Sicherheitslücken im TCP/IP-Protokoll und wie diese für Angriffe auf Netzwerke und Hosts genutzt werden können
- Erläuterung der Daten, die dem Netzwerksicherheitsanalysten zur Verfügung stehen
- Beschreibung der grundlegenden Konzepte und Anwendungen der Kryptographie
- Verstehen der grundlegenden Cloud-Sicherheitspraktiken, einschließlich Bereitstellungs- und Servicemodelle, gemeinsame Verantwortlichkeiten, Compliance-Rahmenwerke sowie Identitäts- und Zugriffsmanagement, um Cloud-Umgebungen effektiv gegen Cyberbedrohungen zu schützen
- Verstehen und Implementieren von fortschrittlicher Netzwerksicherheit, Datenschutz, sicherer Anwendungsbereitstellung, kontinuierlicher Überwachung und effektiven Notfallwiederherstellungsstrategien zur Sicherung von Cloud-Bereitstellungen
- Verständnis der Kill Chain und der Diamantenmodelle für die Untersuchung von Vorfällen sowie der Verwendung von Exploit-Kits durch Bedrohungakteure
- Identifizierung der gängigen Angriffsvektoren
- Identifizieren Sie bösartige Aktivitäten
- Erkennen von verdächtigen Verhaltensmustern
- Ermittlung von Ressourcen für die Jagd auf Cyber-Bedrohungen
- Erläutern Sie die Notwendigkeit der Normalisierung von Ereignisdaten und der Ereigniskorrelation
- Durchführung von Untersuchungen von Sicherheitsvorfällen

- Erklären Sie die Verwendung eines typischen Playbooks im SOC
- einen typischen Reaktionsplan für Zwischenfälle und die Funktionen eines typischen Computer Security Incident Response Teams (CSIRT) zu beschreiben

Detaillierter Kursinhalt

- Definition des Security Operations Center
- SOC-Metriken verstehen
- Verständnis von SOC-Workflow und Automatisierung
- Grundlegendes zum Windows-Betriebssystem
- Grundlagen des Betriebssystems Linux
- Verstehen von Endpunkt-Sicherheitstechnologien
- Verständnis der Netzwerkinfrastruktur und der Tools zur Überwachung der Netzwerksicherheit
- Verstehen gängiger TCP/IP-Angriffe
- Erkundung von Datentypkategorien
- Grundlegende Konzepte der Kryptographie verstehen
- Grundlagen der Cloud-Sicherheit
- Absicherung von Cloud-Bereitstellungen
- Verständnis der Vorfallsanalyse in einem bedrohungszentrierten SOC
- Identifizierung gängiger Angriffsvektoren
- Identifizierung bösartiger Aktivitäten
- Erkennen von verdächtigen Verhaltensmustern
- Identifizierung von Ressourcen für die Jagd auf Cyber-Bedrohungen
- Verstehen von Ereigniskorrelation und Normalisierung
- Durchführung von Untersuchungen zu Sicherheitsvorfällen
- Verwendung eines Playbook-Modells zur Organisation der Sicherheitsüberwachung
- Beschreiben der Reaktion auf einen Vorfall

e

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