

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

ID CBROPS Preis CHF 4'670.– (exkl. MwSt.) Dauer 5 Tage

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 \(CCNA\)](#)

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 Bedrohungsakteure
- 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

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)



Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>