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

Der Kurs **Understanding Cybersecurity Operations Fundamentals (CBROPS) v1.0** vermittelt ein Verständnis für die Geräte der Netzwerkinfrastruktur, den Betrieb und die Schwachstellen der Protokollsuite Transmission Control Protocol/Internet Protocol (TCP/IP). Sie lernen grundlegende Informationen über Sicherheitskonzepte, gängige Netzwerkanwendungen und Angriffe, die Betriebssysteme Windows und Linux sowie die Arten von Daten, die zur Untersuchung von Sicherheitsvorfällen verwendet werden. Nach Abschluss dieses Kurses verfügen Sie über die grundlegenden Kenntnisse, die erforderlich sind, um die Aufgaben eines Associate-Level-Cybersicherheitsanalysten in einem bedrohungszentrierten Sicherheitsoperationszentrum zu erfüllen, um das Netzwerkprotokoll zu stärken, Ihre Geräte zu schützen und die betriebliche Effizienz zu steigern. Dieser Kurs bereitet Sie auf die Zertifizierung **Cisco Certified CyberOps Associate** vor.

Zielgruppe

Dieser Kurs richtet sich an Cybersecurity-Analysten auf Associate-Ebene, die in Sicherheitszentren arbeiten.

Empfohlenes Training für die Zertifizierung zum

Cisco Certified CyberOps Associate (CCCA)

Voraussetzungen

Vor der Teilnahme an diesem Kurs sollten Sie über die folgenden Kenntnisse und Fähigkeiten verfügen:

- Fertigkeiten und Kenntnisse, die denen entsprechen, die in Implementing and Administering Cisco Solutions (CCNA) v2.1
- 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) v2.1

Kursziele

Nach der Teilnahme an diesem Kurs 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 Tools zur Überwachung der Netzwerksicherheit (Network Security Monitoring, NSM), die dem Netzwerksicherheitsanalysten zur Verfügung stehen.
- Erläutern Sie die Daten, die dem Netzwerksicherheitsanalysten zur Verfügung stehen.
- Beschreiben Sie die grundlegenden Konzepte und Anwendungen der Kryptographie.
- Beschreiben Sie Sicherheitslücken im TCP/IP-Protokoll und wie diese für Angriffe auf Netzwerke und Hosts genutzt werden können.
- Verstehen gängiger Sicherheitstechnologien für Endgeräte.
- Verstehen der Kill Chain und der Diamantenmodelle für die Untersuchung von Vorfällen sowie der Verwendung von Exploit-Kits durch Bedrohungsakteure.
- Ermittlung von Ressourcen für die Jagd auf Cyber-Bedrohungen.
- Erläutern Sie die Notwendigkeit der Normalisierung von Ereignisdaten und der Ereigniskorrelation.
- Identifizieren Sie die gängigen Angriffsvektoren.
- Identifizieren Sie bösartige Aktivitäten.
- Erkennen Sie verdächtige Verhaltensmuster.
- Durchführung von Untersuchungen von Sicherheitsvorfällen.

- Erklären Sie die Verwendung eines typischen Playbooks im SOC.
- Erläutern Sie die Verwendung von SOC-Metriken zur Messung der Wirksamkeit des SOC.
- Erläuterung des Einsatzes eines Workflow-Management-Systems und der Automatisierung zur Verbesserung der Effizienz des SOC.
- Beschreiben Sie einen typischen Reaktionsplan auf Zwischenfälle und die Funktionen eines typischen CSIRT.
- Erläuterung der Verwendung von VERIS zur Dokumentation von Sicherheitsvorfällen in einem Standardformat.
- Beschreiben Sie die Merkmale und Funktionen des Windows-Betriebssystems.
- Beschreiben Sie die Merkmale und Funktionen des Betriebssystems Linux.

Dieser Kurs wird Ihnen helfen:

- Erwerben Sie das Wissen und die Fähigkeiten zur Implementierung von Protokollen, die Ihre Netzwerkinfrastruktur modernisieren und anpassen.
- Lernen Sie in praktischen Übungen, wie Sie Sicherheitsmaßnahmen optimieren, entwerfen und konfigurieren, um Ihre Netzwerke vor Cybersecurity-Angriffen zu schützen.

Detaillierter Kursinhalt

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

Labor Gliederung

- Konfigurieren Sie die anfängliche Collaboration-Laborumgebung
- NSM-Tools zur Analyse von Datenkategorien verwenden
- Kryptographische Technologien erforschen
- TCP/IP-Angriffe erforschen
- Endpunktsicherheit erkunden
- Untersuchung der Hacker-Methodik
- Bösartigen Verkehr jagen
- Korrelieren Sie Ereignisprotokolle, PCAPs und Alarme eines Angriffs
- Untersuchen Sie Browser-basierte Angriffe
- Analysieren Sie verdächtige DNS-Aktivitäten
- Sicherheitsdaten für die Analyse auswerten
- Untersuchen Sie verdächtige Aktivitäten mit Security Onion
- Untersuchen Sie fortgeschrittene anhaltende Bedrohungen
- SOC Playbooks erkunden
- Erkunden Sie das Windows-Betriebssystem
- Erkunden Sie das Linux-Betriebssystem

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