

Understanding Cisco Cybersecurity Operations Fundamentals

 Live Online oder Präsenz

Dauer : 5 Tage (30 Stunden)

Nr. : 59612

Preis : 3.950,00 € netto

4.700,50 € inkl. 19 % MwSt.

Inhouse-Paket : Auf Anfrage

- 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 bössartiger 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
- Bössartigen 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

Wer sollte teilnehmen:

Zielgruppe

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

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'
- 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'

Trainingsprogramm

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.

Schulungsmethode

presentation, discussion, hands-on exercises, demonstrations on the system.

Hinweis

Unterlagen in Englisch