Understanding Cisco Cybersecurity Operations Fundamentals

Trainings-ID: CBROPS

Zum Seminar →

Das nehmen Sie mit

Dieses Seminar vermittelt Sicherheitskonzepte, gängige Netzwerk- und Anwendungsvorgänge und -angriffe sowie die zur Untersuchung von Sicherheitsvorfällen erforderlichen Datentypen. In diesem Kurs lernen Sie, wie man Warnungen und Lücken überwacht und wie man etablierte Verfahren zur Reaktion auf Vorfälle gewordenen Warnungen versteht und einsetzt. Durch eine Kombination aus Vorlesung, praktischen Übungen und Selbststudium lernen Sie die wesentlichen Fähigkeiten, Konzepte und Technologien, um ein mitwirkendes Mitglied eines Cybersicherheits-Operationszentrums (SOC) zu sein, einschließlich des Verständnisses der IT-Infrastruktur, des Betriebs und der Schwachstellen. Dieser Kurs hilft Ihnen bei der Vorbereitung auf die Zertifizierung zum Cisco Certified CyberOps Associate und die Rolle eines Cybersicherheits-Betriebsanalytikers der Junior- oder Einstiegsstufe in einem SOC.

Nach Abschluss des Kurses haben die Teilnehmer*innen Kenntnisse zu folgenden Themen:

- Wie ein Security Operations Center (SOC) funktioniert, und verschiedene Arten von Dienstleistungen, die aus der Perspektive eines Tier-1-SOC-Analysten durchgeführt werden.
- Tools zur Überwachung der Netzwerksicherheit (NSM), die dem Netzwerksicherheitsanalytiker zur Verfügung stehen.
- Daten, die dem Netzwerksicherheitsanalytiker zur Verfügung stehen.
- Grundlegende Konzepte und Anwendungen der Kryptographie.
- Sicherheitsschwachstellen im TCP/IP-Protokoll und wie diese zum Angriff auf Netzwerke und Hosts genutzt werden können.
- Allgemeine Endpunktsicherheitstechnologien

- Kill Chain und der Diamand Models für die Untersuchung von Vorfällen sowie die Verwendung von Exploit-Kits durch die Täter
- Ressourcen für die Jagd auf Cyber-Bedrohungen identifizieren.
- Notwendigkeit der Normalisierung von Ereignisdaten und der Ereigniskorrelation.
- Gemeinsame Angriffsvektoren identifizieren.
- Bösartige Aktivitäten identifizieren.
- Identifizieren von Mustern verdächtiger Verhaltensweisen.
- Untersuchungen von Sicherheitsvorfällen durchführen.
- Verwendung eines typischen Spielbuchs im SOC.
- Verwendung von SOC-Metriken zur Messung der Wirksamkeit des SOC.
- Verwendung eines Workflow-Management-Systems und der Automatisierung zur Verbesserung der Wirksamkeit des SOC.
- Typische Vorfallsreaktionspläne und die Funktionen eines typischen Computer Security Incident Response Teams (CSIRT).
- Verwendung des Vokabulars für Ereignisaufzeichnung und gemeinsame Nutzung von Vorfällen (VERIS), um Sicherheitsvorfälle in einem Standardformat zu dokumentieren.

Zielgruppen

Dieser Kurs richtet sich an Personen, die eine Rolle als Cybersicherheitsanalytiker*innen auf Associate-Ebene anstreben, sowie an IT-Profis, die Kenntnisse in Cybersicherheitsoperationen benötigen oder die die Zertifizierung Cisco Certified CyberOps Associate anstreben, einschließlich:

- Teilnehmer*innen, die einen technischen Abschluss anstreben
- IT-Fachleute
- Hochschulabsolventen mit einem technischen Abschluss

Wichtige Informationen

Dieser Kurs bereitet Sie, gemeinsam mit 1 Tag Selbstlernmaterial, auf die Prüfung Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) vor, die zur Zertifizierung Cisco Certified CyberOps Associate führt.

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis