Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

ID CCNACBR **Preis** CHF 4'495.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Cybersicherheitsanalysten auf Associate-Ebene

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Cybersecurity Associate (CCNA CYBERSECURITY)

Voraussetzungen

Für diese Schulung gibt es keine formalen Voraussetzungen. Es wird jedoch empfohlen, dass Sie vor der Teilnahme an dieser Schulung über folgende Kenntnisse und Fähigkeiten verfügen:

- Kenntnisse im Bereich Ethernet und TCP/IP-Netzwerke
- Praktische Kenntnisse der Betriebssysteme Windows und Linux
- Kenntnisse der Grundlagen von Konzepten der Netzwerksicherheit

Diese Kenntnisse werden im folgenden Cisco-Schulungsangebot vermittelt:

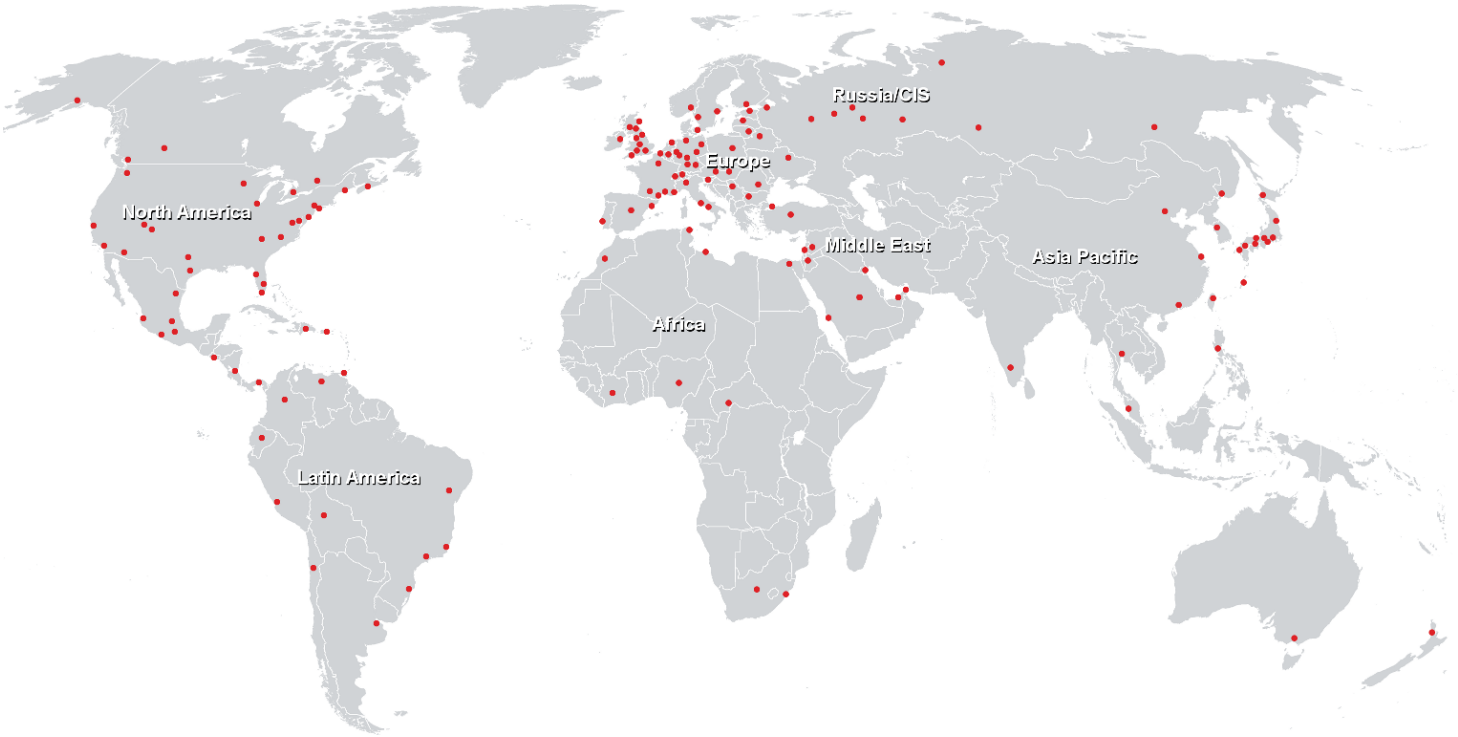
- Implementing and Administering Cisco Solutions (CCNA)

Kursziele

- Erläutern Sie die grundlegenden Aspekte von SOCs, einschliesslich ihrer Arten, ihrer wichtigsten Funktionen und der wesentlichen Kennzahlen zur Messung ihrer Wirksamkeit
- Anwendung grundlegender Sicherheitsprinzipien und Risikomanagementkonzepte zur Bewertung und zum Schutz der Unternehmensressourcen
- Vergleichen und wenden Sie verschiedene Zugriffskontrollmodelle an, um Netzwerkressourcen zu schützen und unternehmensinterne Richtlinien durchzusetzen
- Unterscheiden Sie zwischen verschiedenen Cloud-Bereitstellungs- und Servicemodellen und erläutern Sie die geteilte Verantwortung für die Sicherheit in Cloud-Umgebungen
- Erläutern Sie die grundlegenden Konzepte der Kryptografie, unterscheiden Sie zwischen verschiedenen kryptografischen Algorithmen und erklären Sie, wie kryptografische Prinzipien in realen Protokollen und Systemen angewendet werden, einschliesslich Schlüsselaustausch, digitaler Signaturen und SSL/TLS
- Die grundlegenden Komponenten und Funktionsweisen des Windows-Betriebssystems für die Sicherheitsanalyse identifizieren und beschreiben
- Die grundlegenden Komponenten und Funktionsweisen des Linux-Betriebssystems im Hinblick auf die Sicherheitsanalyse identifizieren und beschreiben
- Nutzung von Befehlszeilenschnittstellen (CLIs) für grundlegende Systeminteraktionen, die Dateiverwaltung und sicherheitsrelevante Aufgaben sowohl in Windows- als auch in Linux-Umgebungen
- Erläutern Sie die Funktionsweise grundlegender Netzwerkprotokolle und zeigen Sie deren Auswirkungen auf die Sicherheit auf
- Beschreiben und unterscheiden Sie verschiedene Netzwerksicherheitsmassnahmen und deren Anwendung beim Schutz der Netzwerkinfrastruktur
- Zwischen verschiedenen Intrusion Detection- und Prevention-Systemen (IDS/IPS) unterscheiden und deren Ausgabedaten für die Sicherheitsüberwachung auswerten
- Beschreiben und vergleichen Sie verschiedene Endpoint-Sicherheitslösungen und deren Wirksamkeit gegen gängige Bedrohungen
- Verschiedene Akteure im Bereich der Cyberbedrohungen anhand ihrer Motive, Fähigkeiten und gängigen Taktiken identifizieren und kategorisieren
- Erläutern Sie die Phasen des klassischen „Cyber Kill Chain“-Modells und identifizieren Sie die Aktionen der Angreifer in den einzelnen Phasen.
- Das MITRE ATT&CK-Framework zur Analyse und Zuordnung von Cyberbedrohungen anwenden, dessen Struktur und Anwendung erläutern und es nutzen, um die Erkennung von Bedrohungen, die Reaktion auf Vorfälle und die Kommunikation innerhalb einer Security-Operations-Umgebung zu verbessern
- Verschiedene Angriffsvektoren im Bereich Social Engineering identifizieren und beschreiben, einschliesslich solcher, die durch generative KI verstärkt werden
- Beschreiben Sie grundlegende Netzwerkangriffstechniken,

die Schwachstellen in Protokollen ausnutzen
- Beschreiben Sie komplexe Angriffsvektoren und neue Bedrohungen in der aktuellen Cybersicherheitslandschaft
- Verschiedene Arten von Daten aus der Netzwerksicherheitsüberwachung (NSM) identifizieren und erläutern sowie deren Rolle bei der Untersuchung von Vorfällen darlegen
- Verschiedene Protokollquellen aus Betriebssystemen, Netzwerkgeräten und Sicherheitstools identifizieren und auswerten
- Erläutern Sie die Funktionsweise von NetFlow und dessen Einsatz als Sicherheitsinstrument zur Netzwerküberwachung und Erkennung von Anomalien
- Beschreiben Sie gängige Angriffe auf Webanwendungen und die entsprechenden Ausnutzungsmethoden
- Anwendung fortschrittlicher Protokollanalyseverfahren zur Auswertung von Sicherheitsdaten und zur Erkennung von Mustern verdächtigen Verhaltens
- Führen Sie eine Paketerfassungsanalyse durch und wenden Sie digitale forensische Verfahren an, um Sicherheitsvorfälle zu untersuchen. Konzentrieren Sie sich dabei auf das 5-Tupel und die Zeitstempel, um Korrelationen mit anderen Protokollen herzustellen, da dies Ihr wichtigstes Werkzeug für die Netzwerkforensik ist.
- Ergebnisse der Malware-Analyse erläutern und Frameworks für Bedrohungsinformationen bei Sicherheitsuntersuchungen anwenden
- Erläutern Sie die Architektur, die Kernfunktionen und die bewährten Verfahren für die Implementierung von SIEM-Lösungen zur effektiven Sicherheitsüberwachung
- Erläutern Sie die Funktionen und gängigen Anwendungsfälle von SOAR-Plattformen zur Automatisierung und Optimierung der Reaktion auf Sicherheitsvorfälle.
- Erläutern Sie die Cisco XDR-Plattform, ihre Kernfunktionen, Merkmale und Komponenten für die einheitliche Erkennung und Bekämpfung von Bedrohungen.
- Unterscheiden Sie zwischen den älteren und den aktuellen NIST-Leitlinien zur Incident Response (Sonderveröffentlichungen NIST SP 800-61 Rev. 2 und NIST SP 800-61 Rev. 3), beschreiben Sie die Kernkomponenten der Incident Response im Einklang mit dem NIST CSF 2.0-Rahmenwerk und legen Sie dar, inwiefern diese Vorgehensweisen die CMMC-Anforderungen für die Verteidigungsindustriebasis (DIB) erfüllen
- Beschreiben Sie die Aufgaben, Kategorien und operativen Dienste von Computer Security Incident Response Teams (CSIRTs)
- Erläutern Sie das Konzept von Playbooks für die Sicherheitsüberwachung und deren Komponenten zur Standardisierung der Reaktion auf Vorfälle
- Anwendung verschiedener Methoden zur Bedrohungssuche, um versteckte Bedrohungen innerhalb eines Netzwerks proaktiv zu identifizieren und zu mindern

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