# Performing CyberOps Using Cisco Security Technologies

Trainings-ID: CBRCOR

CBRCOR: 350-201

Zum Seminar →

## Das nehmen Sie mit

Dieses Training behandelt die Grundlagen, Methoden und Automatisierung von Cybersecurity Operations. Die Kenntnisse, die Sie in diesem Kurs erwerben, bereiten Sie auf die Rolle des Information Security Analysten in einem Security Operations Center (SOC) Team vor.
Sie lernen grundlegende Konzepte und deren Anwendung in realen Szenarien kennen und erfahren, wie Sie Playbooks bei Incident Response (IR) einsetzen können. Der Kurs zeigt Ihnen, wie Sie mit Hilfe von Cloud-Plattformen und einer SecDevOps-Methodik die Automatisierung für die Sicherheit nutzen können. Sie lernen die Techniken zur Erkennung von Cyberangriffen, zur Analyse von Bedrohungen und zur Erstellung geeigneter Empfehlungen zur Verbesserung der Cybersicherheit.

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

- Arten der Serviceabdeckung innerhalb eines SOC und die damit verbundenen betrieblichen Verantwortlichkeiten
- Vergleich der Überlegungen zum Sicherheitsbetrieb von Cloud-Plattformen
- Allgemeine Methoden der Entwicklung, Verwaltung und Automatisierung von SOC-Plattformen
- Asset-Segmentierung, Segregation, Netzwerk-Segmentierung, Mikro-Segmentierung und der jeweiligen Ansätze als Teil der Asset-Kontrollen und -Schutzmaßnahmen
- Zero Trust und damit verbundenen Ansätzen als Teil von Asset-Kontrollen und Schutzmaßnahmen
- Untersuchung von Vorfällen mithilfe von Security Information and Event Management (SIEM) und/oder Security Orchestration and Automation (SOAR) im SOC durchführen

- Verwendung verschiedener Arten von zentralen Sicherheitstechnologieplattformen für die Sicherheitsüberwachung, Untersuchung und Reaktion
- die DevOps- und SecDevOps-Prozesse zu beschreiben
- Gängige Datenformate, z. B. JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV)
- API-Authentifizierungsmechanismen
- Analysieren des Ansatzes und der Strategien zur Erkennung von Bedrohungen während der Überwachung, Untersuchung und Reaktion
- Bekannte Indikatoren für eine Gefährdung (Indicators of Compromise, IOCs) und Angriffsindikatoren (Indicators of Attack, IOAs) zu ermitteln
- Interpretation der Abfolge von Ereignissen während eines Angriffs auf der Grundlage der Analyse von Traffic Patterns
- Beschreiben der verschiedenen Sicherheitstools und ihrer Grenzen für die Netzwerkanalyse (z. B. Tools zur Paketaufzeichnung, Traffic Analyse Tool, Netzwerkprotokollanalyse)
- Analyse von anomalem Benutzer- und Entitätsverhalten (UEBA)
- Proaktive Bedrohungssuche nach bewährten Verfahren durchführen

## Das nehmen Sie mit

Dieses Training behandelt die Grundlagen, Methoden und Automatisierung von Cybersecurity Operations. Die Kenntnisse, die Sie in diesem Kurs erwerben, bereiten Sie auf die Rolle des Information Security Analysten in einem Security Operations Center (SOC) Team vor.
Sie lernen grundlegende Konzepte und deren Anwendung in realen Szenarien kennen und erfahren, wie Sie Playbooks bei Incident Response (IR) einsetzen können. Der Kurs zeigt Ihnen, wie Sie mit Hilfe von Cloud-Plattformen und einer SecDevOps-Methodik die Automatisierung für die Sicherheit nutzen können. Sie lernen die Techniken zur Erkennung von Cyberangriffen, zur Analyse von Bedrohungen und zur Erstellung geeigneter Empfehlungen zur Verbesserung der Cybersicherheit.

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

- Arten der Serviceabdeckung innerhalb eines SOC und die damit verbundenen betrieblichen Verantwortlichkeiten

- Vergleich der Überlegungen zum Sicherheitsbetrieb von Cloud-Plattformen
- Allgemeine Methoden der Entwicklung, Verwaltung und Automatisierung von SOC-Plattformen
- Asset-Segmentierung, Segregation, Netzwerk-Segmentierung, Mikro-Segmentierung und der jeweiligen Ansätze als Teil der Asset-Kontrollen und -Schutzmaßnahmen
- Zero Trust und damit verbundenen Ansätzen als Teil von Asset-Kontrollen und Schutzmaßnahmen
- Untersuchung von Vorfällen mithilfe von Security Information and Event Management (SIEM) und/oder Security Orchestration and Automation (SOAR) im SOC durchführen
- Verwendung verschiedener Arten von zentralen Sicherheitstechnologieplattformen für die Sicherheitsüberwachung, Untersuchung und Reaktion
- die DevOps- und SecDevOps-Prozesse zu beschreiben
- Gängige Datenformate, z. B. JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV)
- API-Authentifizierungsmechanismen
- Analysieren des Ansatzes und der Strategien zur Erkennung von Bedrohungen während der Überwachung, Untersuchung und Reaktion
- Bekannte Indikatoren für eine Gefährdung (Indicators of Compromise, IOCs) und Angriffsindikatoren (Indicators of Attack, IOAs) zu ermitteln
- Interpretation der Abfolge von Ereignissen während eines Angriffs auf der Grundlage der Analyse von Traffic Patterns
- Beschreiben der verschiedenen Sicherheitstools und ihrer Grenzen für die Netzwerkanalyse (z. B. Tools zur Paketaufzeichnung, Traffic Analyse Tool, Netzwerkprotokollanalyse)
- Analyse von anomalem Benutzer- und Entitätsverhalten (UEBA)
- Proaktive Bedrohungssuche nach bewährten Verfahren durchführen

## Zielgruppen

- Cybersecurity Engineers und Investigators
- Incident Manager
- Incident Responders
- Network Engineers
- SOC-Analysten, die derzeit auf Einstiegsebene arbeiten und mehr als 2 Jahre Erfahrung haben

## Termine & Optionen

| Datum | Dauer | Ort | Angebot | Preis |
|---|---|---|---|---|
| 17.02.2025–21.02.2025 | 5 Tage | Wien | Trainingspreis (Vor Ort) | € 3.950,– |
| 17.02.2025–21.02.2025 | 5 Tage | Wien | Trainingspreis (Online) | € 3.950,– |
| 06.10.2025–10.10.2025 | 5 Tage | Wien | Trainingspreis (Vor Ort) | € 3.950,– |
| 06.10.2025–10.10.2025 | 5 Tage | Wien | Trainingspreis (Online) | € 3.950,– |