Microsoft Security Operations Analyst (SC-200T00)

ID SC-200T00 **Preis** CHF 2'990.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

Der Microsoft Security Operations Analyst arbeitet mit Projektbeteiligten im Unternehmen zusammen, um IT-Systeme des Unternehmens zu schützen. Ihr Ziel ist es, Risiken für das Unternehmen zu verringern, indem sie aktive Angriffe in der Umgebung schnell abwehren, Empfehlungen zur Verbesserung der Bedrohungsschutzmethoden aussprechen und Verstösse gegen die Unternehmensrichtlinien an die zuständigen Stellen weiterleiten. Zu den Zuständigkeiten gehören das Verwalten und Überwachen von sowie das Reagieren auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in ihrer Umgebung. Zu den Aufgaben dieser Rolle gehört in erster Linie das Untersuchen, Reagieren und Suchen nach Bedrohungen mithilfe von Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern. Da der Security Operations Analyst die operative Ausgabe dieser Tools nutzt, ist er auch ein wichtiger Stakeholder beim Konfigurieren und Bereitstellen dieser Technologien.

Empfohlenes Training für die Zertifizierung zum

Microsoft Certified: Security Operations Analyst Associate (MCSOAA)

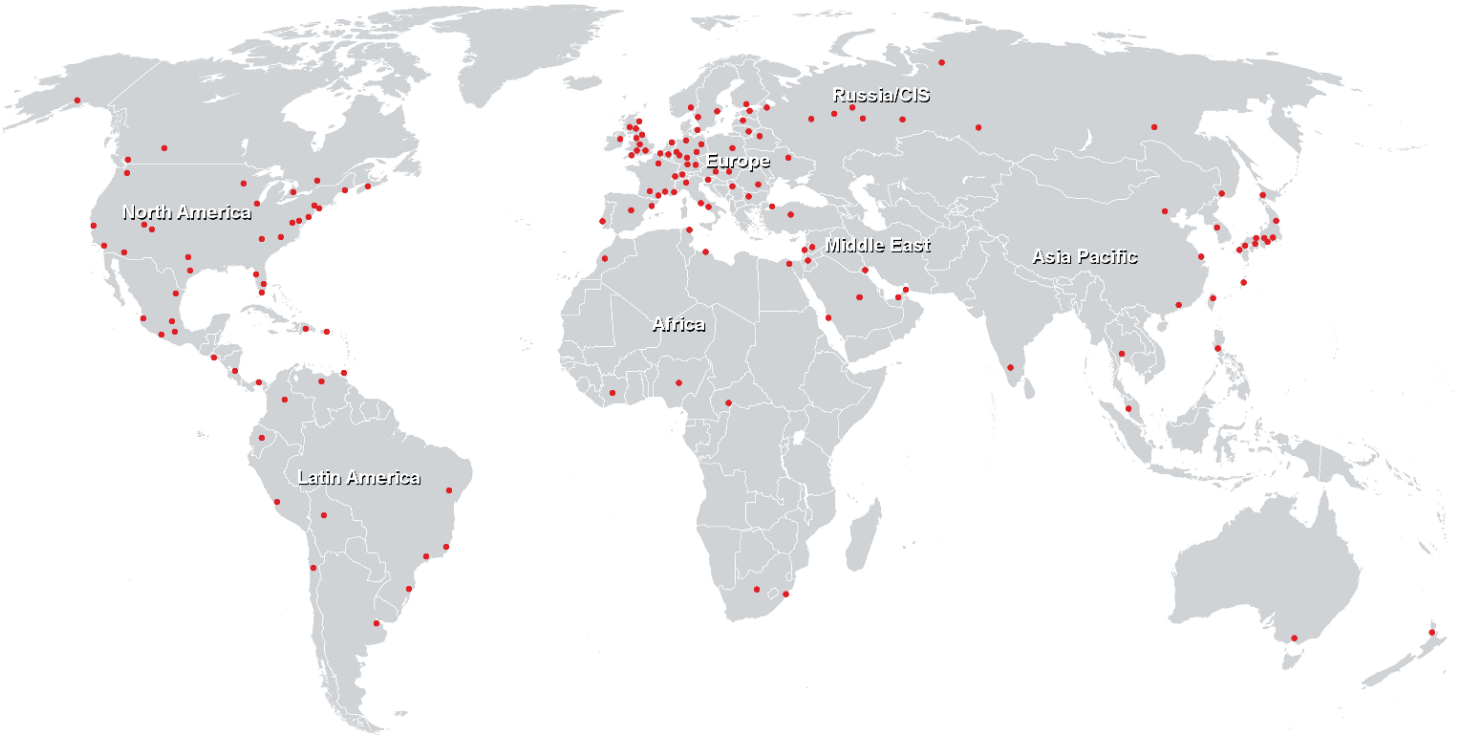
Kursinhalt

- Einführung in den Microsoft Defender XDR-Bedrohungsschutz
- Abmildern von Incidents mithilfe von Microsoft 365 Defender
- Schützen Ihrer Identitäten mit Microsoft Entra ID Protection
- Remediate risks with Microsoft Defender for Office 365
- Schützen Sie Ihre Umgebung mit Microsoft Defender for Identity
- Sichern Ihrer Cloud-Apps und -Dienste mit Microsoft Defender for Cloud Apps
- Reagieren auf Warnungen zur Verhinderung von Datenverlust mithilfe von Microsoft 365
- Manage insider risk in Microsoft Purview
- Beschreiben von Microsoft Copilot für Sicherheit
- Beschreiben der Kernfunktionen von Microsoft Copilot für Security
- Beschreiben der eingebetteten Erfahrungen von Microsoft Copilot for Security
- Untersuchen von Bedrohungen mithilfe von Überwachungsfeatures in Microsoft Defender XDR und Microsoft Purview Standard
- Untersuchen von Bedrohungen mithilfe der Überwachung in Microsoft Defender XDR und Microsoft Purview (Premium)
- Untersuchen von Bedrohungen mit der Inhaltssuche in Microsoft Purview
- Protect against threats with Microsoft Defender for Endpoint
- Bereitstellen der Microsoft Defender für Endpunkt-Umgebung
- Implementieren von Windows-Sicherheitsverbesserungen mit Microsoft Defender für Endpunkt
- Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt
- Ausführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender für Endpunkt
- Untersuchen von Beweisen und Entitäten mithilfe von Microsoft Defender für Endpunkt
- Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt
- Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt
- Verwenden des Sicherheitsrisikomanagements in Microsoft Defender für Endpunkt
- Planen von Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Verbinden von Azure-Ressourcen mit Microsoft Defender für Cloud
- Verbinden Azure-fremder Ressourcen mit Microsoft Defender für Cloud
- Verwalten Ihrer Cloud Security Posture Management-Instanz
- Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Beheben von Sicherheitswarnungen mit Microsoft Defender für Cloud
- Erstellen von KQL-Anweisungen für Microsoft Sentinel
- Analysieren von Abfrageergebnissen mithilfe von KQL
- Erstellen von Anweisungen mit mehreren Tabellen mithilfe von KQL
- Arbeiten mit Daten in Microsoft Sentinel mithilfe der Kusto-Abfragesprache
- Einführung in Microsoft Sentinel

- Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen
- Abfragen von Protokollen in Microsoft Sentinel
- Verwenden von Watchlists in Microsoft Sentinel
- Verwenden der Threat Intelligence in Microsoft Sentinel
- Verbinden von Daten mit Microsoft Sentinel mithilfe von Datenconnectors
- Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel
- Verbinden von Microsoft Defender XDR mit Microsoft Sentinel
- Verbinden von Windows-Hosts mit Microsoft Sentinel
- Verbinden von Common Event Format-Protokollen mit Microsoft Sentinel
- Verbinden von Syslog-Datenquellen mit Microsoft Sentinel
- Verbinden von Bedrohungsindikatoren mit Microsoft Sentinel
- Bedrohungserkennung mit Microsoft Sentinel-Analysen
- Automatisierung in Microsoft Sentinel
- Reaktion auf Bedrohungen mit Microsoft Sentinel-Playbooks
- Verwaltung von Sicherheitsvorfällen in Microsoft Sentinel
- Identifizieren von Bedrohungen mithilfe der Verhaltensanalyse
- Datennormalisierung in Microsoft Sentinel
- Abfragen, Visualisieren und Überwachen von Daten in Microsoft Sentinel
- Verwalten von Inhalten in Microsoft Sentinel
- Erläutern der Bedrohungssuchkonzepte in Microsoft Sentinel
- Bedrohungssuche mit Microsoft Sentinel
- Verwenden von Suchaufträgen in Microsoft Sentinel
- Suchen von Bedrohungen mithilfe von Notebooks in Microsoft Sentinel

Microsoft Security Operations Analyst (SC-200T00)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch