Microsoft Security Operations Analyst – Intensive Training («SC200»)

Lernen Sie, wie Sie mit Microsoft Azure Sentinel, Azure Defender und Microsoft 365 Defender Bedrohungen untersuchen, auf sie reagieren und sie aufspüren können.

Dauer: 4 Tage
Preis: 3'400.– zzgl. 8.1% MWST
Kursdokumente: Offizielle Microsoft-Kursunterlagen und Microsoft Learn
Herstellercode: SC-200

Inhalt

In diesem Kurs lernen Sie, wie Sie mit diesen Technologien Cyberbedrohungen abwehren können. Insbesondere werden Sie Azure Sentinel konfigurieren und verwenden sowie die *Kusto Query Language* (*KQL*) zur Erkennung, Analyse und Berichterstellung einsetzen. Der Kurs wurde für Personen konzipiert, die in einer Security Operations Job-Rolle arbeiten und hilft den Lernenden bei der Vorbereitung auf die Prüfung SC-200: Microsoft Security Operations Analyst.

Kursmodule:

Einführung in den Bedrohungsschutz von Microsoft 365

- In diesem Modul lernen Sie, wie Sie die in Microsoft 365 Defender integrierte Bedrohungsschutzsammlung verwenden.

Abmildern von Incidents mithilfe von Microsoft 365 Defender

- Erfahren Sie, wie das Microsoft-365-Defender-Portal eine einheitliche Ansicht von Vorfällen in der Microsoft-365-Defender-Produktfamilie bereitstellt.

Schützen Ihrer Identitäten mit Azure AD Identity Protection

- Verwenden Sie die erweiterte Erkennung und Beseitigung von identitätsbasierten Bedrohungen, um Ihre Azure Active Directory-Identitäten und -Anwendungen vor Angriffen zu schützen.

Remediate risks with Microsoft Defender for Office 365 (aktuell nur auf englisch verfügbar)

- Learn about the Microsoft Defender for Office 365 component of Microsoft 365 Defender.

Schützen Sie Ihre Umgebung mit Microsoft Defender for Identity

- Kennenlernen der Microsoft Defender for Identity-Komponente von Microsoft 365 Defender.

Sichern Ihrer Cloud-Apps und -Dienste mit Microsoft Defender for Cloud Apps

- Microsoft Defender for Cloud Apps ist ein Cloud Access Security Broker (CASB), der in mehreren Clouds ausgeführt wird. Dieser Dienst bietet umfassende Sichtbarkeit, Kontrolle bei der Datenübertragung, und modernste Analysen, die Cyberbedrohungen in all Ihren Clouddiensten erkennen und abwehren. Erfahren Sie, wie Sie Defender for Cloud Apps in Ihrer Organisation verwenden.

Reagieren auf Warnungen zur Verhinderung von Datenverlust mithilfe von Microsoft 365

- Als Security Operations Analyst sollten Sie die Begriffe und Warnungen im Zusammenhang mit Compliance verstehen. Erfahren Sie, wie Warnungen zur Verhinderung von Datenverlust Ihnen bei

der Untersuchung helfen, um den gesamten Umfang eines Vorfalls zu ermitteln.

Manage insider risk in Microsoft Purview (aktuell nur auf englisch verfügbar)

- Microsoft Purview Insider Risk Management helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Untersuchen von Bedrohungen mithilfe von Überwachungsfeatures in Microsoft 365 Defender und Microsoft Purview Standard

- In diesem Modul wird die Suche nach überwachten Aktivitäten mithilfe der Microsoft-Purview-Überwachungslösung (UAL) untersucht, einschliesslich des Exportierens, Konfigurierens und Anzeigens der Überwachungsprotokolldatensätze, die aus einer Überwachungsprotokollsuche abgerufen wurden.

Untersuchen von Bedrohungen mithilfe der Überwachung in Microsoft 365 Defender und Microsoft Purview (Premium)

- In diesem Modul werden die Unterschiede zwischen der Microsoft-Purview-Überwachung (Standard) und der Überwachung (Premium) sowie die wichtigsten Funktionen der Überwachung (Premium) untersucht, einschliesslich der Setupanforderungen, der Aktivierung der Überwachungs-Protokollierung, dem Erstellen von Aufbewahrungs-Richtlinien für Überwachungs-Protokolle und dem Durchführen forensischer Untersuchungen.

Untersuchen von Bedrohungen mit der Inhaltssuche in Microsoft Purview

- In diesem Modul wird erläutert, wie Sie im Microsoft-Purview-Complianceportal nach Inhalten suchen. Dabei werden die Suchfunktionen näher erläutert, zum Beispiel das Anzeigen und Exportieren von Suchergebnissen oder das Konfigurieren der Suchberechtigungs-Filterung.

Protect against threats with Microsoft Defender for Endpoint (aktuell nur auf englisch verfügbar)

- Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Bereitstellen der Microsoft Defender für Endpunkt-Umgebung

- Hier erfahren Sie, wie Sie die Microsoft Defender für Endpunkt-Umgebung bereitstellen, einschliesslich des Onboardings von Geräten und der Sicherheits-Konfiguration.

Implementieren von Windows-Sicherheitsverbesserungen mit Microsoft Defender für Endpunkt

- Microsoft Defender für Endpunkt bietet verschiedene Tools, mit denen Sie Risiken beseitigen können, indem Sie die Oberfläche für Angriffe verringern, ohne die Benutzer-Produktivität einzuschränken. Erfahren Sie mehr über die Verringerung der Angriffsfläche mit Microsoft Defender für Endpunkt.

Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt

- Microsoft Defender für Endpunkt bietet umfassende Geräteinformationen, einschliesslich forensischer Informationen. Hier erfahren Sie mehr über die Informationen, die Ihnen über Microsoft Defender für Endpunkt zur Verfügung stehen und bei Untersuchungen hilfreich sind.

Ausführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender für Endpunkt

- Erfahren Sie, wie Microsoft Defender für Endpunkt die Remotefunktionen zum Einbeziehen von Geräten und Sammeln forensischer Daten bereitstellt.

Untersuchen von Beweisen und Entitäten mithilfe von Microsoft Defender für Endpunkt

- Dieser Artikel enthält Informationen zu den Artefakten in Ihrer Umgebung sowie dazu, in welchem Zusammenhang diese Artefakte zu anderen Artefakten und Warnungen stehen, die Erkenntnisse über die allgemeinen Auswirkungen auf Ihre Umgebung liefern.

Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt

- Erfahren Sie, wie Sie die Automatisierung in Microsoft Defender für Endpunkt durch Verwalten der Umgebungseinstellungen konfigurieren.

Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt

- Erfahren Sie, wie Sie Einstellungen zur Verwaltung von Warnungen und Benachrichtigungen konfigurieren. Ausserdem erfahren Sie, wie Sie Indikatoren im Rahmen des Erkennungsprozesses aktivieren.

Verwenden des Sicherheitsrisikomanagements in Microsoft Defender für Endpunkt

- Hier erfahren Sie mehr über die Schwachstellen in Ihrer Umgebung, indem Sie das Bedrohungs- und Sicherheitsrisikomanagement von Microsoft Defender für Endpunkt verwenden.

Planen von Workloadschutz in der Cloud mit Microsoft Defender für Cloud

- Erfahren Sie mehr über den Zweck von Microsoft Defender für Cloud und die Aktivierung des Systems.

Verbinden von Azure-Ressourcen mit Microsoft Defender für Cloud

- Hier erfahren Sie, wie Sie verschiedene Azure-Ressourcen mit Microsoft Defender für Cloud verbinden, um Bedrohungen zu erkennen.

Verbinden Azure-fremder Ressourcen mit Microsoft Defender für Cloud

- Hier erfahren Sie, wie Sie Ihrer Hybridumgebung Funktionen von Microsoft Defender für Cloud hinzufügen.

Verwalten Ihrer Cloud-Security-Posture-Management-Instanz

- Microsoft Defender für Cloud, Cloud Security Posture Management (CSPM) bietet Einblicke in anfällige Ressourcen und eine Anleitung zur Härtung.

Workloadschutz in der Cloud mit Microsoft Defender für Cloud

- Erfahren Sie mehr über den von Microsoft Defender für Cloud bereitgestellten Schutz und das Erkennen von Bedrohungen für jede Cloudworkload.

Beheben von Sicherheitswarnungen mit Microsoft Defender für Cloud

- Erfahren Sie, wie Sie Sicherheitswarnungen in Microsoft Defender für Cloud beheben.

Erstellen von KQL-Anweisungen für Microsoft Sentinel

- KQL ist die Abfragesprache, die der Untersuchung von Daten zum Erstellen von Analysen und Arbeitsmappen sowie der Ausführung von Hunting-Vorgängen in Microsoft Sentinel dient. Im Folgenden finden Sie Informationen darüber, wie Sie mithilfe der grundlegenden KQL-Anweisungsstruktur komplexe Anweisungen erstellen.

Analysieren von Abfrageergebnissen mithilfe von KQL

- Hier erfahren Sie, wie Sie Daten in einer KQL-Anweisung zusammenfassen und visualisieren. Dies ist die Grundlage zum Erstellen von Erkennungen in Microsoft Sentinel.

Erstellen von Anweisungen mit mehreren Tabellen mithilfe von KQL

- Hier erfahren Sie, wie Sie mit KQL mit mehreren Tabellen arbeiten.

Arbeiten mit Daten in Microsoft Sentinel mithilfe der Kusto-Abfragesprache

- Erfahren Sie, wie Sie mithilfe der Kusto-Abfragesprache (*Kusto Query Language, KQL*) aus Protokollquellen erfasste Zeichenfolgendaten bearbeiten.

Einführung in Microsoft Sentinel

- Das Einrichten und Konfigurieren herkömmlicher SIEM-Systeme (Security Information & Event Management) erfordert in der Regel viel Zeit. Ausserdem sind diese Systeme nicht unbedingt für Cloud-Workloads konzipiert. Microsoft Sentinel ermöglicht es Ihnen, sich anhand Ihrer Cloud- und lokalen Daten schnell wertvolle sicherheitsrelevante Erkenntnisse zu verschaffen. Dieses Modul unterstützt Sie beim Einstieg.

Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen

- Im Folgenden finden Sie Informationen darüber, wie Sie mit der Architektur von Microsoft-Sentinel-Arbeitsbereichen Ihr System so konfigurieren, dass die Anforderungen an die Sicherheits-Anforderungen Ihrer Organisation erfüllt werden.

Abfragen von Protokollen in Microsoft Sentinel

- Als Security Operations Analyst müssen Sie die Tabellen, Felder und Daten verstehen, die in Ihrem Arbeitsbereich erfasst werden. Hier erfahren Sie, wie Sie die am häufigsten genutzten Datentabellen in Microsoft Sentinel abfragen.

Verwenden von Watchlists in Microsoft Sentinel

- Hier erfahren Sie, wie Sie in Microsoft Sentinel Watchlists erstellen. Dabei handelt es sich um eine benannte Liste importierter Daten. Nach der Erstellung können Sie die benannte Watchlist auf einfache Weise in KQL-Abfragen verwenden.

Verwenden der Threat Intelligence in Microsoft Sentinel

- Hier erfahren Sie, wie Sie mit der Seite „Threat Intelligence“ von Microsoft Sentinel-Bedrohungsindikatoren verwalten können.

Verbinden von Daten mit Microsoft Sentinel mithilfe von Datenconnectors

- Zum Verbinden von Protokolldaten werden in erster Linie die von Microsoft Sentinel bereitgestellten Datenconnectors verwendet. Dieses Modul liefert einen Überblick über die verfügbaren Datenconnectors.

Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel

- Hier erfahren Sie, wie Sie eine Verbindung von Microsoft-365- und Azure-Dienstprotokollen mit Microsoft Sentinel herstellen.

Verbinden von Microsoft 365 Defender mit Microsoft Sentinel

- Erfahren Sie mehr über die Konfigurations-Optionen und Daten, die von Microsoft Sentinel Connectors für Microsoft 365 Defender bereitgestellt werden.

Verbinden von Windows-Hosts mit Microsoft Sentinel

- Sicherheitsrelevante Windows-Ereignisse gehören zu den am häufigsten erstellten Protokollen. Hier erfahren Sie, wie Microsoft Sentinel das Generieren von Protokollen mithilfe des Sicherheitsereignis-Connectors vereinfacht.

Verbinden von Common Event Format-Protokollen mit Microsoft Sentinel

- Bei den meisten von Anbietern bereitgestellten Connectors kommt der CEF-Connector zum Einsatz. In diesem Modul erhalten Sie Informationen zu den Konfigurationsoptionen des Common Event Format-Connectors (CEF).

Verbinden von Syslog-Datenquellen mit Microsoft Sentinel

- Hier erfahren Sie mehr über die Konfigurations-Optionen der Syslog-Datensammlungsregel des Azure Monitor-Agents für Linux, mit denen Sie Syslog-Daten analysieren können.

Verbinden von Bedrohungsindikatoren mit Microsoft Sentinel

- Im Folgenden finden Sie Informationen darüber, wie Sie mithilfe der bereitgestellten Datenconnectors eine Verbindung zwischen Threat-Intelligence-Indikatoren und dem Microsoft-Sentinel-Arbeitsbereich herstellen.

Bedrohungserkennung mit Microsoft-Sentinel-Analysen

- In diesem Modul haben Sie erfahren, wie Microsoft Sentinel Analytics das SecOps-Team beim Erkennen und Bekämpfen von Cyberangriffen unterstützen kann.

Automatisierung in Microsoft Sentinel

- Am Ende dieses Moduls können Sie Automatisierungsregeln in Microsoft Sentinel verwenden, um die Verwaltung von Incidents zu automatisieren.

Verwaltung von Sicherheitsvorfällen in Microsoft Sentinel

- Hier erfahren Sie mehr über Sicherheitsincidents, Nachweise und Entitäten bezüglich Incidents, die Verwaltung von Incidents und die Verwendung von Microsoft Sentinel zum Behandeln von Incidents.

Identifizieren von Bedrohungen mithilfe der Verhaltensanalyse

- In diesem Modul erfahren Sie, wie Sie die Benutzer- und Entitätsverhaltensanalyse (User and Entity Behavior Analytics, UEBA) in Microsoft Sentinel verwenden können, um Bedrohungen in Ihrer Organisation zu erkennen.

Datennormalisierung in Microsoft Sentinel

- Am Ende des Moduls können Sie Bedrohungen in Ihrer Organisation mithilfe von ASIM-Parsern erkennen.

Abfragen, Visualisieren und Überwachen von Daten in Microsoft Sentinel

- In diesem Modul erfahren Sie, wie Sie Daten in Microsoft Sentinel abfragen, visualisieren und überwachen.

Verwalten von Inhalten in Microsoft Sentinel

- Am Ende des Moduls können Sie *Inhalte* in Microsoft Sentinel verwalten.

Erläutern der Bedrohungssuchkonzepte in Microsoft Sentinel

- Lernen Sie die Bedrohungssuchkonzepte in Microsoft Sentinel kennen.

Bedrohungssuche mit Microsoft Sentinel

- In diesem Modul erfahren Sie, wie Sie mithilfe von Microsoft-Sentinel-Abfragen proaktiv Bedrohungsverhaltensweisen identifizieren können. Ausserdem lernen Sie, Lesezeichen und Livestreams zum Suchen von Bedrohungen zu verwenden.

Verwenden von Suchaufträgen in Microsoft Sentinel

- In Microsoft Sentinel können Sie mithilfe eines Suchauftrags mit langer Ausführungsdauer grosse Datasets durchsuchen.

Suchen von Bedrohungen mithilfe von Notebooks in Microsoft Sentinel

- Erfahren Sie, wie Sie Notebooks in Microsoft Sentinel für die erweiterte Bedrohungssuche verwenden.

Key Learnings

- Abwehr von Bedrohungen mit Microsoft 365 Defender
- Abwehr von Bedrohungen mit Azure Defender for Cloud
- Abwehr von Bedrohungen mit Azure Sentinel

Zielpublikum

Der Microsoft Security Operations Analysts arbeiten mit den Interessenvertretern des Unternehmens zusammen, um die Informationstechnologie-Systeme des Unternehmens zu sichern. Ihr Ziel ist es, das Unternehmensrisiko zu reduzieren, indem sie aktive Angriffe in der Umgebung schnell beheben, über Verbesserungen der Praktiken zum Schutz vor Bedrohungen beraten und Verstösse gegen die Unternehmensrichtlinien an die entsprechenden Beteiligten weiterleiten. Zu den Aufgaben gehören das Bedrohungsmanagement, die Überwachung und die Reaktion auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in der gesamten Umgebung. Die Rolle untersucht in erster Linie Bedrohungen, reagiert auf sie und sucht nach ihnen mithilfe von Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender und Sicherheitsprodukten anderer Anbieter. Da die Security Operations Analysts den operativen Output dieser Tools nutzen, sind sie auch wichtige Beteiligte bei der Konfiguration und Bereitstellung dieser Technologien.

Anforderungen

- Grundlegendes Verständnis von Microsoft 365
- Grundlegendes Verständnis der Sicherheits-, Compliance- und Identitätsprodukte von Microsoft
- Mittleres Verständnis von Windows 10
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL Database und Azure Storage
- Vertrautheit mit virtuellen Maschinen und virtuellen Netzwerken in Azure
- Grundlegendes Verständnis von Scripting-Konzepten

Empfohlen wird das im folgenden Kurs erlangte Grundwissen:

- Microsoft Security, Compliance, and Identity Fundamentals – Intensive Training («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Flexible Training («SC900V»)

Zertifizierung

Dieses Intensive Training bereitet Sie vor auf:

- **Prüfung:** «SC-200: Microsoft Security Operations Analyst (beta)» für die
- **Zertifizierung:** «Microsoft Certified: Security Operations Analyst Associate»

Zusatzinfo

Wir empfehlen SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel als Selbststudium-Vorbereitung auf diesen Kurs.

Weiterführende Kurse

- Microsoft Cybersecurity Architect – Intensive Training («SC100»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-security-compliance-and-identity/microsoft-certified-security-operations-analyst-associate/kurs-microsoft-security-operations-analyst-intensive-training-sc-200