Configure SIEM Security Operations Using Microsoft Sentinel – Intensive Training («SC5X1»)

Beginnen Sie mit den Sicherheitsoperationen von Microsoft Sentinel, indem Sie den Microsoft-Sentinel-Arbeitsbereich konfigurieren.

Dauer: 1 Tag
Preis: 900.– zzgl. 8.1% MWST
Kursdokumente: Offizielle Microsoft-Kursunterlagen auf Microsoft Learn

Inhalt

1 Erstellen und Verwalten von Microsoft-Sentinel-Arbeitsbereichen
Informieren Sie sich über die Architektur von Microsoft-Sentinel-Arbeitsbereichen, um sicherzustellen, dass Sie Ihr System so konfigurieren, dass es den Anforderungen Ihres Unternehmens an Sicherheitsabläufe entspricht.

2 Verbinden von Microsoft-Diensten mit Microsoft Sentinel
Erfahren Sie, wie Sie Protokolle von Microsoft 365 und Azure-Diensten mit Microsoft Sentinel verbinden.

3 Verbinden Sie Windows-Hosts mit Microsoft Sentinel
Eines der am häufigsten zu sammelnden Protokolle sind Windows-Sicherheitsereignisse. Erfahren Sie, wie Microsoft Sentinel dies mit dem Security Events Connector vereinfacht.

4 Bedrohungserkennung mit Microsoft Sentinel-Analysen
In diesem Modul erfahren Sie, wie Microsoft Sentinel Analytics dem SecOps-Team helfen kann, Cyberangriffe zu erkennen und zu stoppen.

5 Automatisierung in Microsoft Sentinel
Am Ende dieses Moduls werden Sie in der Lage sein, Automatisierungsregeln in Microsoft Sentinel für ein automatisiertes Incident Management zu verwenden.

6 Konfigurieren von SIEM-Sicherheitsvorgängen mit Microsoft Sentinel
In diesem Modul haben Sie gelernt, wie Sie SIEM-Sicherheitsvorgänge mit Microsoft Sentinel konfigurieren.

Key Learnings

- Beschreiben, Installieren und Verwalten der Microsoft-Sentinel-Arbeitsraumarchitektur
- Verbinden von Microsoft-Dienstkonnektoren, virtuellen Azure-Windows-Maschinen und Nicht-Azure-Windows-Hosts mit Microsoft Sentinel
- Konfigurieren des Log-Analytics-Agenten zum Sammeln von Sysmon-Ereignissen
- Erläutern der Bedeutung von Microsoft Sentinel Analytics und der verschiedenen Arten von Analyseregeln
- Erstellen von Regeln aus Vorlagen, neuen Analyseregeln und Abfragen
- Verwalten von Regeln mit Änderungen
- Erläutern und Erstellen von Automatisierungsoptionen in Microsoft Sentinel
- Erstellen und Konfigurieren eines Microsoft-Sentinel-Arbeitsbereichs
- Bereitstellen von Microsoft Sentinel Content Hub-Lösungen und Datenkonnektoren
- Konfigurieren von Microsoft-Sentinel-Datensammlungsregeln, NRT-Analytic-Regeln und Automatisierung
- Durchführen eines simulierten Angriffs zur Validierung von Analyse- und Automatisierungsregeln

Zielpublikum

Dieser Kurs richtet sich an Security-Operations-Analysten.

Zusatzinfo

Dieser Workshop ist in den Kurs AZ-500: Microsoft Azure Security Technologies integriert.

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-azure-security-engineer-associate/kurs-configure-siem-security-operations-using-microsoft-sentinel-intensive-training