Secure Azure Services and Workloads w/ Microsoft Defender for Cloud Regulatory Compliance Controls – Intensive Training («SC5X2»)

Learn about securing Azure services and workloads using Microsoft Cloud Security Benchmark controls in Microsoft Defender for Cloud via the Azure portal.

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

Inhalt

1 Filtern des Netzwerkverkehrs mit einer Netzwerksicherheitsgruppe über das Azure-Portal
In diesem Modul konzentrieren wir uns auf das Filtern des Netzwerkverkehrs mithilfe von Netzwerksicherheitsgruppen (NSGs) im Azure-Portal. Erfahren Sie, wie Sie NSGs für eine verbesserte Netzwerksicherheit erstellen, konfigurieren und anwenden.

2 Erstellen eines Log-Analytics-Arbeitsbereichs für Microsoft Defender for Cloud
In diesem Modul erfahren Sie, wie Sie einen Log Analytics-Arbeitsbereich im Azure-Portal für Microsoft Defender for Cloud erstellen und damit die Datenerfassung und Sicherheitsanalyse verbessern.

3 Einrichten von Microsoft Defender für Cloud
In diesem Modul lernen Sie, wie Sie Microsoft Defender for Cloud über das Azure-Portal implementieren, um die Sicherheit und die Erkennung von Bedrohungen in Ihrer Azure-Umgebung zu verbessern.

4 Erstellen und Integrieren eines Log-Analytics-Agenten und Arbeitsbereichs in Defender for Cloud
Dieses Modul führt Sie zur Konfiguration und Integration eines Log Analytics-Agenten mit einem Arbeitsbereich in Defender for Cloud über das Azure-Portal, um die Sicherheitsanalyse zu verbessern.

5 Konfigurieren der Azure-Key-Vault-Netzwerkeinstellungen
In diesem Modul lernen Sie, wie Sie die Netzwerkeinstellungen von Azure Key Vault über das Azure-Portal konfigurieren, um einen sicheren und kontrollierten Zugriff auf Ihre gespeicherten Geheimnisse zu gewährleisten.

6 Verbinden eines Azure-SQL-Servers mit einem Azure Private Endpoint über das Azure-Portal
Dieses Modul leitet Sie an, wie Sie einen Azure-SQL-Server über einen Azure Private Endpoint im Azure-Portal sicher verbinden und die Sicherheit der Datenkommunikation erhöhen.

Key Learnings

- Erstellen und Konfigurieren von NSGs zur Durchsetzung von Zugriffskontrollen für Azure-Ressourcen
- Priorisieren von NSG-Regeln und Nutzung von Azure-NSG-Flow-Protokollen zur Überwachung und Fehlerbehebung
- Erstellen und Konfigurieren eines Log Analytics-Arbeitsbereichs in Azure sowie benutzerdefinierte Abfragen und Warnungen zur proaktiven Erkennung von Sicherheitsbedrohungen und Vorfällen
- Einblicke in das Sammeln und Analysieren von Sicherheitsdaten aus Microsoft Defender for Cloud im Log Analytics-Arbeitsbereich gewinnen
- Verstehen der Funktionen und Vorteile von Microsoft Defender for Cloud, Microsoft Security Benchmark, Sicherheitsempfehlungen und Defender for Cloud Secure Score
- Überwachen, Schützen und Verbessern der Sicherheit von Cloud-Umgebungen
- Erforschen der MITRE-Angriffsmatrix zur Identifizierung gängiger Angriffstechniken und zur Priorisierung von Sicherheitsmassnahmen
- Verstehen des Konzepts der Brute-Force-Angriffe und der Bedeutung der Implementierung von Präventivmassnahmen
- Vertraut machen mit Just in Time Virtual Machine, um fein abgestufte Zugriffskontrollen für verbesserte Sicherheit zu implementieren
- Konfigurieren und Bereitstellen des Log Analytics-Agenten in Azure
- Konfigurieren der Netzwerkzugriffskontrolle für Azure Key Vault unter Verwendung von virtuellen Netzwerkdienst-Endpunkten und privaten Endpunkten; Konfigurieren und Erstellen eines privaten Azure-Endpunkts für Azure SQL Server im Azure-Portal
- Einblicke in die Netzwerkarchitektur und die Komponenten bei der Einrichtung eines Azure Private Endpoints
- Verstehen, wie man die Verbindung zwischen dem Azure Private Endpoint und Azure SQL Server validiert und testet
- Erkennen der Vorteile der Verwendung von Azure Private Endpoint zur Sicherung von Datenbankverbindungen und zur Isolierung des Netzwerkverkehrs

Zielpublikum

Dieser Kurs richtet sich an Azure-Administratoren und Security Engineers.

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-azure/microsoft-certified-azure-security-engineer-associate/kurs-secure-azure-services-and-workloads-w-microsoft-defender-for-cloud-regulatory-compliance-controls-intensive-training