>> Microsoft Defender for Cloud

Secure Azure Services and Workloads

EGOS! the education company

Microsoft Defender for Cloud ist eine cloudnative Anwendungsschutzplattform (Cloud-Native Application Protection Platform, CNAPP) mit Sicherheitsmaßnahmen und -verfahren, die zum Schutz von cloudbasierten Anwendungen vor verschiedenen Cyberbedrohungen und Sicherheitsrisiken entwickelt wurden. Defender for Cloud kombiniert die folgenden Funktionen:

Ihr Nutzen

Defender for Cloud hilft Ihnen, bewährte Sicherheitsmethoden frühzeitig während des Softwareentwicklungsprozesses oder DevSecOps zu integrieren. Sie können Ihre Codeverwaltungsumgebungen und Ihre Codepipelines schützen und Einblicke in den Sicherheitsstatus Ihrer Entwicklungsumgebung von einem einzigen Ort aus erhalten. Defender für Cloud ermöglicht Sicherheitsteams die Verwaltung der DevOps-Sicherheit in mehreren Pipelineumgebungen.

Preis pro Teilnehmer

EUR 850,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Voraussetzungen

Für die Einrichtung von Defender for Cloud Apps benötigen Sie in Microsoft Entra ID oder Microsoft 365 die Rollen „Globaler Administrator“ oder „Sicherheitsadministrator“.

Hinweise

SC-5002,

Version: N/A

Seminarinhalte

* Überprüfen der Standards für die Einhaltung gesetzlicher Bestimmungen von Defender for Cloud
- Einführung
- Gesetzliche Compliancestandards in Defender for Cloud
- Microsoft-Benchmark für Cloudsicherheit in Defender for Cloud
- Verbessern der Einhaltung gesetzlicher Compliance in Defender for Cloud

* Aktivieren von Defender für Cloud für Ihr Azure-Abonnement
- Einführung
- Verbinden Ihrer Azure-Abonnements
- Übung: Aktivieren von Defender for Cloud für Ihr Azure-Abonnement

* Filtern von Netzwerkdatenverkehr mithilfe einer Netzwerksicherheitsgruppe über das Azure-Portal
- Einführung
- Azure-Ressourcengruppe
- Azure Virtual Network
- Filtern von Netzwerkdatenverkehr mit Netzwerksicherheitsgruppen
- Anwendungssicherheitsgruppen
- Übung: Erstellen einer virtuellen Netzwerkinfrastruktur

* Erstellen eines Log Analytics-Arbeitsbereichs für Microsoft Defender for Cloud
- Einführung
- Log Analytics-Arbeitsbereich
- Übung: Erstellen eines Log Analytics-Arbeitsbereichs für Microsoft Defender for Cloud

* Konfigurieren und Integrieren eines Log Analytics-Agents und -Arbeitsbereichs mit Defender für Cloud
- Einführung
- Sammeln von Daten aus Ihren Workloads mit dem Log Analytics-Agent
- Konfigurieren von Log Analytics-Agent und -Arbeitsbereich
- Übung: Konfigurieren und Integrieren eines Log Analytics-Agents und -Arbeitsbereichs mit Defender für Cloud

* Erkundung von Just-in-Time-Zugriff auf virtuelle Computer
- Einführung
- Grundlagndes zum Just-In-Time-Zugriff auf virtuelle Computer
- Aktivieren des Just-in-Time-Zugriffs auf virtuellen Computern
- Übung: Aktivieren des Just-in-Time-Zugriffs auf VMs

- Grundlegende Konzepte von Azure Key Vault
- Übersicht über die Azure Key Vault-Funktion für vorläufiges Löschen
- VNET-Dienstendpunkte für Azure Key Vault
- Übung: Durchführen der Wiederherstellung des vorläufigen Löschens und Bereinigen des Schutzschlüsseltresors

* Herstellen einer Verbindung mit einer Azure SQL-Server-Instanz über einen privaten Azure-Endpunkt im Azure-Portal
- Einführung
- Privater Azure-Endpunkt
- Azure Private Link
- Übung: Herstellen einer Verbindung mit einem Azure SQL-Server über einen privaten Azure-Endpunkt im Azure-Portal