>> Microsoft 365

Security Operations Analyst

EGOS! the education company

Defender ist nicht nur mehr die Client-Endpoint Sicherheitslösung sondern schützt auch die unterschiedlichen Cloud Services von Microsoft und andere On-Premise Systeme.

Ihr Nutzen

Nach diesem Seminar können Sie die verschiedenen Defender Produkte (Endpoint, Microsoft 365 und Azure) konfigurieren und damit ein App Security Framework bereitstellen und verwalten. Sie erlernen Thread Hunting mittels KQL und Azure Sentinel.

Voraussetzungen

Microsoft 365, Administration~9868

Windows Server / Client und Active Directory-Kenntnisse sowie Grundkenntnisse von M365/Azure Security Komponenten von Vorteil

Preis pro Teilnehmer

EUR 2450,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Hinweise

SC-200T00,

Version: 365

Seminarinhalte

1. Tag
* Microsoft Defender for Endpoint
- Die Endpoint Umgebung bereitstellen
- Windows 10 Security Funktionen mit Defender
- Alerts und Incidents verwalten
- Device Investigation
- Device Actions
- Beweissicherung
- Automatisierung verwalten
- Alerts konfigurieren

* Microsoft 365 Defender
- Funktionen von Microsoft 365 Defender
- Azure Ad Identity Protection
- Advanced Hunting und Risiken beheben
- Schutz der Umgebung mit Defender for Identity
- Cloud App Security konfigurieren
- Insider Risk Management mit M365

2. Tag
* Azure Defender
- Die Funktionen von Azure Defender
- Das Azure Security Center
- Auto-Provisioning und manuelles Provisioning
- Non-Azure Machines
- Alerts, Remediation und Response

* Azure Sentinel abfragen
- Einführung in Kusto Query Language (KQL)
- Ergebnisse analysieren
- Multi-Table-Statements in KQL

3. Tag
* Azure Sentinel konfigurieren
- Was ist Azure Sentinel?
- Workspaces erstellen und verwalten
- Logs abfragen
- Watchlists
- Threat Intelligence und Indicators

* Logs zu Azure Sentinel anbinden
- Was sind Data Connectors?
- Microsoft Services verbinden
- M365 Defender verbinden
- Windows Hosts einbinden
- Common Event Format Logs
- syslog Daten einbinden

4. Tag
* Detect and Response
- Threat Detection mit Sentinel Analytics
- Threat Response mit Sentinel Playbooks
- Incident Management
- Entity Behaviour
- Abfragen, Visualisierung und Monitoring

* Threat Hunting
- Hunting Konzepte in Azure Sentinel
- Hunting Hypothesis
- Queries für das Hunting nutzen
- Livestream
- API Libraries für Advanced Hunting
- Notebooks erstellen und nutzen

Unsere BildungsberaterInnen stehen Ihnen gerne zur Verfügung. Innsbruck +43 (0)512 36 47 77.