>> Microsoft Defender XDR

Defend against Cyberthreats

Microsoft Defender für Endpoint ist eine umfassende Sicherheitslösung von Microsoft, die speziell für Unternehmen entwickelt wurde. Sie schützt Endgeräte (wie PCs, Laptops, Server) vor Bedrohungen und bietet Funktionen wie Erkennung, EDR und KI-gestützte Bedrohungsanalyse.

Ihr Nutzen

Sie erlernen die Implementierund von Microsoft Defender for Endpoint-Umgebung zum Verwalten von Geräten, führen Sie Untersuchungen zu Endpunkten durch, verwalten Sie Vorfälle in Defender XDR, und nutzen Sie die erweiterte Bedrohungssuche mit KQL (Kusto-Abfragesprache), um einzelne Bedrohungen zu erkennen.

Voraussetzungen

Windows Client Administrations-Kenntnisse

Preis pro Teilnehmer

EUR 850,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

SC-5004,

Version: N/A

Seminarinhalte

* Incidents in Microsoft Defender behandeln
- Arbeiten mit dem Defender Portal
- Verwalten von Incidents
- Incidents erforschen
- Verwalten von Alerts
- Automatisierte Investigation
- Actions Center
- Advanced Hunting
- Entra Sign-In Logs
- Secure Store
- Threat Analyics und Reports

* Deployment von Defender for Endpoint
- Umgebung bereitstellen
- Onboarding von Devices
- Zugriffsrechte verwalten
- Device Groups
- Advanced Features

* Alerts und Detections verwalten
- Alert Notification
- Alert Supression
- Verwalten von Indikatoren

* Automatisierung
- Automation Uploads
- Automatisierte Investigation und Remediation
- Blockieren von Devices

* Device Investigation
- Arbeiten mit der Device List
- Behaviour Blocking
- Device Discovery