Microsoft Copilot for Security («SCP01»)

Die Teilnehmenden tauchen ein in Generative AI für Sicherheits-Technologien. Sie werden sehen, wie Gen AI beim Umgang mit fortgeschrittenen Angreifern helfen kann. Das Verständnis und die Nutzung von Gen AI können die SOC-Leistung erheblich verbessern.

Dauer: 1 Tag
Preis: 900.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursunterlagen (Englisch)

Inhalt

Modul 1 – Einrichten von Sicherheit mit AI

- Einsatz von *Copilot for Security* und Azure OpenAI.

Modul 2 – Endpunktschutz mit *Copilot for Security*

- Erstellen und implementieren benutzerdefinierter Sicherheitsrichtlinien, die mit ihren individuellen Anforderungen und Compliance-Standards übereinstimmen.
- Definieren von Regeln, Konfigurationen und Parametern, die vorgeben, wie Endpunkte geschützt, überwacht und auf sie zugegriffen werden soll.

Modul 3 – *Copilot for Security* im SOC

- Kontinuierliche Überwachung von Endpunkten auf Anzeichen von bösartigen Aktivitäten.
- Automatisieren von Triage und Priorisierung von Vorfällen.
- Anreicherung der Erkennungsfunktionen mit Informationen über neue Bedrohungen und Schwachstellen.
- KI-gesteuerte Untersuchung und Reaktion.

Praktische Übungen

Der Kurs wird von Übungen begleitet, in denen die Teilnehmenden *Copilot for Security* testen können.

- Übung 1: Einrichten von Sicherheit mit AI
- Übung 2: Ausführen von Angriffen
- Übung 3: Untersuchung und Reaktion mit *Copilot for Security*
- Übung 4: Endpunktschutz mit *Copilot for Security*

Key Learnings

- Vorteile von AI für die Sicherheit
- Wie AI von Angreifern genutzt wird
- Wie *Copilot für Sicherheit* funktioniert
- Wie *Copilot für Sicherheit* in SOC eingesetzt wird

Methodik & Didaktik

- Der Kurs umfasst Demo-Vorlesungen und praktische Übungen
- Online oder vor Ort; der Hauptunterschied besteht darin, dass in Vor-Ort-Kursen in der Regel mehr Diskussionen stattfinden

Zielpublikum

Sicherheitsanalysten, Sicherheitsingenieure, Penetrationstester

Zusatzinfo

Integrationen: Copilot lässt sich mit verschiedenen Microsoft-Produkten integrieren, darunter:

- Unified Security Operations Platform: Kombiniert XDR- und SIEM-Funktionen.
- Microsoft Sentinel: Sammelt Sicherheitsdaten und korreliert Warnungen.
- Microsoft Defender XDR: Hilft bei der Verhinderung und Erkennung von domänenübergreifenden Cyberangriffen.
- Microsoft Intune: Entschärft Cyberbedrohungen für Geräte und verbessert die Compliance.
- Microsoft Defender Threat Intelligence: Versteht Cyber-Bedrohungen und deckt verdächtige Infrastrukturen auf.
- Microsoft Entra: Hilft beim Schutz von Identitäten und beim sicheren Zugriff.
- Microsoft Purview: Bietet Governance-, Schutz- und Compliance-Lösungen für Daten.

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-copilot/kurs-microsoft-copilot-for-security