Security Operations Praxisworkshop

Angriffe erkennen mit Microsoft Sentinel – SOC-Praxis statt Prüfungsvorbereitung

3 Tage	Fortgeschritten	Deutsch
Kursdauer (24 UE)	Niveau	Sprache

Inhalts-Kurzbeschreibung

Security-Operations-Rollen sind chronisch unterbesetzt, das Thema hat Dringlichkeit. Dieser Workshop vermittelt praxisnah, was ein SOC-Alltag mit Microsoft Sentinel wirklich bedeutet: Analytics Rules konfigurieren, mit KQL gezielt nach Bedrohungen suchen, Incidents untersuchen und mit Playbooks automatisiert reagieren – bewusst als Hands-on-Workshop beworben, nicht als Zertifikatsvorbereitung.

Zielgruppe

Security-Analysten, SOC-Mitarbeiter und IT-Administratoren mit Sicherheitsverantwortung.

Voraussetzungen

Grundkenntnisse Azure/Microsoft 365 · Basiswissen Log Analytics/KQL von Vorteil · keine SC-200-Zertifizierung vorausgesetzt.

Kurz-Agenda (Modul-Übersicht)

Modul	Schwerpunkt	Kerninhalte (Auszug)
M1	**Security-Operations-Grundlagen**	SOC-Rollen · Detect-Investigate-Respond-Zyklus · Sentinel-Architektur
M2	**Datenquellen & Analytics Rules**	Data Connectors · Scheduled-/NRT-Analytics-Rules · Fusion-Erkennung
M3	**KQL für die Bedrohungssuche**	Threat-Hunting-Queries · Hunting-Bookmarks · Livestream
M4	**Incident-Triage & Untersuchung**	Incident-Queue · Entity-Mapping · Investigation-Graph
M5	**Automatisierung mit Playbooks**	Logic-Apps-Integration · automatisierte Reaktionen · Eindämmung
M6	**Praxisfall End-to-End**	durchgespielter Incident von Alarm bis Reaktion · Lessons Learned

Lernziele – nach diesem Kurs können Teilnehmer …

- Analytics Rules für die eigene Umgebung konfigurieren und priorisieren.
- Mit KQL gezielt nach Bedrohungen suchen.
- Einen Incident von der Erkennung bis zur Eindämmung bearbeiten.
- Reaktionen mit Playbooks automatisieren.

Investition

1.500 € pro Teilnehmer · netto · zzgl. MwSt.

Online & Präsenz: gleicher Preis · Inhouse: zzgl. Reise nach Aufwand

Format & Methodik

3 Tage à 8 Unterrichtseinheiten · Hands-on in einer Sentinel-Sandbox-Umgebung.

Trainer & Buchung

Thomas Drilling – IT-Trainer & Berater, Microsoft Certified Trainer (MCT) und Fachautor mit über 25 Jahren Erfahrung in IT-Infrastruktur, Cloud Computing und Identity-Themen. Autor zahlreicher Fachbeiträge, u. a. bei iX, c't und Heise sowie regelmäßiger Gastautor bei WindowsPro.

Kontakt & Buchung: info@drilling-it.de · www.cloudtrain.de
Formate: Inhouse vor Ort · Online-Live-Training via Microsoft Teams · Hybrid