Microsoft 365 - analýza bezpečnostních hrozeb, detekce událostí a zvládání incidentů

Kód kurzu: GOC239

Pětidenní pokročilý kurz určený pro IT a SOC specialisty zodpovědné za detekci bezpečnostních událostí a analýzu hrozeb v cloudovém i hybridním prostředí, stejně jako na koncových zařízeních uživatelů. Je zaměřen na využití nástrojů v prostředí Microsoft 365, Microsoft Azure, konkrétně sady produktů Microsoft Defender XDR a Microsoft Sentinel

Pro koho je kurz určen

Kurz je určen IT profesionálům a pracovníkům dohledu SOC (security operation center) zodpovědným za sběr bezpečnostních událostí, detekci zranitelností a incidentů a analýzu hrozeb

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

Co jsou hrozby a zranitelnosti, vektory útoků, Mitre Attack Matrix

Přehled preventivních opatření k zabezpečení cloudového prostředí Microsoft

Bezpečnostní parametry uživatelských účtů a jejich přihlašovacích údajů

Detekční nástroje stanic a Microsoft 365

Microsoft Entra - ochrana uživatelů a řízení přístupu k cloudovým službám

Microsoft Defender XDR (Extended Detection and Response)

Přehled produktů integrovaných v Defender XDR

Microsoft Defender for Office

Microsoft Defender for Cloud Applications

Microsoft Defender for Identity

Microsoft Entra ID Protection

Microsoft Defender for Endpoint

Microsoft Sentinel (SIEM)

Microsoft Copilot for Security

Správa IoC

Microsoft Defender Vulnerability Management

Detekce zranitelností a hrozeb

Správa alertů a incidentů

Analýza incidentů a reakce na ně

Doporučení ke zvýšení bezpečnosti

Cloud Security Posture Management

Cloud Workload Protection Platform

Soulad se standardy jako je ISO 27001/27002, GDPR, NIS2, ZKB, DORA, PCI DSS

Ochrana síťové infrastruktury a VPN

Paketové filtery a firewall

Zabezpečení úložišť

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Microsoft 365 - analýza bezpečnostních hrozeb, detekce událostí a zvládání incidentů

Technologie Private Links

Dočasné přístupy k VM virtuálním počítačům a služba Bastion

Sledování a sběr dat

Plánování a nasazení služby Sentinel

Instalace balíků Sentinel rešení z Content Hub

Aktivace konektorů k službám Sentinel

Připojení zdrojů dat mezi on-prem a Sentinel

Pravidla vyhledávající incidenty v Sentinel

Detekce hrozeb a jejich analýza pomocí Sentinel

Automatizace reakcí Sentinel

Hunting pomocí Sentinel

Verze Copilot for Security

Práce s nástroji technologie Copilot for Security

Analýza hrozeb a incidentů promocí Copilot for Security

Příprava k certifikačním zkouškám

U certifikačních zkoušek Microsoft platí, že kromě certifikací MCM, není účast na oficiálním MOC kurzu nutnou podmínkou pro složení zkoušky

Oficiální kurzy MOC firmy Microsoft i naše vlastní kurzy GOC jsou vhodnou součástí přípravy na certifikační zkoušky firmy Microsoft, jako jsou MTA, MCP, MCSA, MCSE, nebo MCM

Primárním cílem kurzu ovšem není přímo příprava na certifikační zkoušky, ale zvládnutí teoretických principů a osvojení si praktických dovedností nutných k efektivní práci s daným produktem

MOC kurzy obvykle pokrývají téměř všechny oblasti, požadované u odpovídajících certifikačních zkoušek. Jejich probrání na kurzu ale nebývá dán vždy přesně stejný čas a důraz, jako vyžaduje certifikační zkouška

Jako další přípravu k certifikačním zkouškám lze využít například knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk