Microsoft 365 - security threat analysis, event detection and incident management

Course code: GOC239

A five-day advanced course designed for IT and SOC specialists responsible for security event detection and threat analysis in cloud and hybrid environments, as well as on user endpoints. It focuses on using tools in the Microsoft 365 and Microsoft Azure environments, specifically the Microsoft Defender XDR and Microsoft Sentinel product suites

Affiliate	Duration	Course price	ITB
Praha	5	32 500 Kč	50
Brno	5	32 500 Kč	50
Bratislava	5	1 300 €	50

The prices are without VAT.

Course terms

	Date	Duration	Course price	Type	Course language	Location
	13.04.2026	5	32 500 Kč	Telepresence	CZ/SK	GOPAS Praha
	13.04.2026	5	1 300 €	Telepresence	CZ/SK	GOPAS Bratislava
	13.04.2026	5	32 500 Kč	Telepresence	CZ/SK	GOPAS Brno
	08.06.2026	5	1 300 €	Online	CZ/SK	Online
	08.06.2026	5	32 500 Kč	Online	CZ/SK	Online

The prices are without VAT.

Pre koho je kurz určený

Kurz je určený IT profesionálom a pracovníkom dohľadu SOC (security operation center) zodpovedným za zber bezpečnostných udalostí, detekciu zraniteľností a incidentov a analýzu hrozieb

Predpokladané vstupné znalosti

Znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

Dobrá znalosť technológií TCP/IP a DNS

Metódy výučby

Odborný výklad s praktickými ukážkami, samostatné cvičenia na virtuálnych počítačoch na platformách Hyper-V, Microsoft Azure a Microsoft 365

Samostatné praktické cvičenia zaberajú obvykle aspoň tretinu času stráveného na kurze

Študijné materiály

Vlastné študentské materiály firmy GOPAS v elektronickej alebo tlačenej forme

Osnova kurzu

Čo sú hrozby a zraniteľnosti, vektory útokov, Mitre Attack Matrix

Prehľad preventívnych opatrení na zabezpečenie cloudového prostredia Microsoft

Bezpečnostné parametre užívateľských účtov a ich prihlasovacích údajov

Detekčné nástroje staníc a Microsoft 365

Microsoft Entra - ochrana používateľov a riadenie prístupu k cloudovým službám

Microsoft Defender XDR (Extended Detection and Response)

Prehľad produktov integrovaných v Defender XDR

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 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

Detekcia zraniteľností a hrozieb

Správa alertov a incidentov

Analýza incidentov a reakcie na ne

Odporúčania na zvýšenie bezpečnosti

Cloud Security Posture Management

Cloud Workload Protection Platform

Súlad so štandardmi ako je ISO 27001/27002, GDPR, NIS2, ZKB, DORA, PCI DSS

Ochrana sieťovej infraštruktúry a VPN

Paketové filtre a firewall

Zabezpečenie úložísk

Technológia Private Links

Dočasné prístupy k VM virtuálnym počítačom a služba Bastion

Sledovanie a zber dát

Plánovanie a nasadenie služby Sentinel

Inštalácia balíkov Sentinel riešenie z Content Hub

Aktivácia konektorov k službám Sentinel

Pripojenie zdrojov dát medzi on-prem a Sentinel

Pravidlá vyhľadávajúce incidenty v Sentinel

Detekcia hrozieb a ich analýza pomocou Sentinel

Automatizácia reakcií Sentinel

Hunting pomocou Sentinel

Verzia Copilot for Security

Práca s nástrojmi technológie Copilot for Security

Analýza hrozieb a incidentov promóciou Copilot for Security

Príprava na certifikačné skúšky

Pri certifikačných skúškach Microsoft platí, že okrem certifikácií MCM, nie je účasť na oficiálnom MOC kurze nutnou podmienkou pre zloženie skúšky

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 - security threat analysis, event detection and incident management

Oficiálne kurzy MOC firmy Microsoft aj naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky firmy Microsoft, ako sú MTA, MCP, MCSA, MCSE, alebo MCM

Primárnym cieľom kurzu však nie je priamo príprava na certifikačné skúšky, ale zvládnutie teoretických princípov a osvojenie si praktických zručností potrebných na efektívnu prácu s daným produktom

MOC kurzy obvykle pokrývajú takmer všetky oblasti, požadované pri zodpovedajúcich certifikačných skúškach. Ich prebratie na kurze ale nebýva daný vždy presne rovnaký čas a dôraz, ako vyžaduje certifikačná skúška

Ako ďalšiu prípravu na certifikačné skúšky je možné využiť napríklad knihy od MS Press (tzv. Self-paced Training Kit) aj 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