

Microsoft 365 - detekcia bezpečnostných incidentov a ich zvládanie

Kód kurzu: MOC SC-200

Štvordňový pokročilý kurz sa venuje správe Azure, Microsoft 365 a Microsoft Defender technológií určených k sledovaniu bezpečnosti, vyhľadávaniu bezpečnostných udalostí ako v sieťovej infraštruktúre, tak na koncových bodoch a učí účastníkov, ako udalosti vyhodnocovať a ako sa správať k incidentom, ktoré z udalostí vyhodnotia.

Pobočka	Dní	Katalógová cena	ITB
Praha	4	29 600 Kč	40
Brno	4	29 600 Kč	40
Bratislava	4	1 320 €	40

Všetky ceny sú uvedené bez DPH.

Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
03.03.2025	4	1 320 €	Prezenčný	CZ/SK	Gopas Bratislava Prezenční
G 22.04.2025	4	29 600 Kč	Prezenčný	CZ/SK	Gopas Praha Prezenční
16.06.2025	4	1 320 €	Online	CZ/SK	Gopas Bratislava Online
16.06.2025	4	29 600 Kč	Online	CZ/SK	Gopas Praha Online

Všetky ceny sú uvedené bez DPH.

Predpokladané vstupné znalosti

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

Dobrá znalosť technológií TCP/IP a DNS

Osnova kurzu

Ochrana proti hrozbám pomocou Microsoft Defender for Endpoint

Nasadenie Microsoft Defender for Endpoint

Využitie rozšírení a vylepšení vo Windows 10 pomocou Microsoft Defender for Endpoint

Sledovanie a správa varovaní a udalostí Microsoft Defender for Endpoint

Vyšetrovanie incidentov na zariadeniach pomocou Microsoft Defender for Endpoint

Vykonávanie vzdialených zásahov na zariadeniach pomocou Microsoft Defender for Endpoint

Zber elektronických dôkazov a vyšetrovanie incidentov na zariadeniach pomocou Microsoft Defender for Endpoint

Automatizácia úloh a činností v Microsoft Defender for Endpoint

Varovanie a detekcia a ich nastavenie v Microsoft Defender for Endpoint

Technológie Threat and Vulnerability Management v Microsoft Defender for Endpoint

Ochrany proti hrozbám v Microsoft 365

Zmiernenie a minimalizácia rizík pomocou Microsoft 365 Defender

Ochrana užívateľských účtov a identít pomocou Azure AD Identity Protection

Znižovanie rizík pomocou Microsoft Defender for Office 365

Ochrana prostredia pomocou Microsoft Defender for Identity

Bezpečnosť cloudových aplikácií pomocou Microsoft Cloud App Security

Reakcie na varovania z technológií ochrany proti úniku informácií (data leakage prevention - DLP) Microsoft 365

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



Copyright © 2020 GOPAS, a.s.,

All rights reserved

Microsoft 365 - detekcia bezpečnostných incidentov a ich zvládanie

Riziká útoku insiderov (inside job) v Microsoft 365
Vysvetlenie ochrany cloudovej infraštruktúry v Azure Defender
Pripojenie cloudových prostriedkov k Azure Defender
Pripojenie ne-cloudových prostriedkov k Azure Defender
Riešenie bezpečnostných udalostí a varovaní v Azure Defender
Vytváranie vyhľadávacích dotazov KQL v Azure Sentinel
Analýza výstupov vyhľadávania pomocou KQL
Vytváranie viac tabuľkových dotazov v KQL jazyku
Práca s dátami cez KQL (Kusto Query Language) v Azure Sentinel
Vytváranie a správa pracovných priestorov v Azure Sentinel
Protokoly vyhľadávania v Azure Sentinel
Sledovacie zoznamy v Azure Sentinel
Technológie Threat Intelligence v Azure Sentinel
Pripájanie dátových zdrojov do Azure Sentinel
Pripojenie služieb Microsoft do Azure Sentinel
Pripojenie výstupov Microsoft 365 Defender do Azure Sentinel
Pripojenie Windows počítačov do Azure Sentinel
Pripojenie protokolov v Common Event Format do Azure Sentinel
Pripojenie protokolov zo Syslog do Azure Sentinel
Pripojenie indikátorov hrozieb do Azure Sentinel
Detekcia hrozieb pomocou Azure Sentinel analytiky
Reakcie na incidenty a hrozby pomocou Azure Sentinel
Riadenie bezpečnostných incidentov pomocou Azure Sentinel
Analytika správania entít pomocou Azure Sentinel
Dotazovanie, vyhľadávanie, vizualizácia a sledovanie informácií v Azure Sentinel
Zachytávanie hrozieb v Azure Sentinel
Poznámkové bloky a ich úloha vo vyhľadávaní hrozieb v Azure Sentinel

Príprava na certifikačné skúšky

Pri certifikačných skúškach Microsoft platí, že okrem certifikácie MCM nie je účasť na oficiálnom MOC kurze nevyhnutnou podmienkou pre zloženie skúšky. Oficiálne kurzy MOC spoločnosti Microsoft a aj naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky spoločnosti Microsoft, ako sú MTA, MCP, MCSA, MCSE, alebo MCM. Primárnym cieľom kurzu však nie je priamo príprava na certifikačnú skúšku, ale zvládnutie teoretických princípov a osvojenie si praktických zručností potrebných na efektívnu prácu s daným produktom. MOC kurzy zvyčajne pokrývajú takmer všetky oblasti požadované pri príslušných 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) alebo elektronický self-test softvér.

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



Copyright © 2020 GOPAS, a.s.,
All rights reserved