

Microsoft 365 - detekce bezpečnostních incidentů a jejich zvládnutí

Kód kurzu: MOC SC-200

Čtyřdenní pokročilý kurz je určen IT specialistům a pracovníkům SOC, a věnuje se správě Azure, Microsoft 365 a Microsoft Defender technologií určených ke sledování bezpečnosti, vyhledávání bezpečnostních událostí jak v síťové infrastruktuře tak na koncových bodech a učí studenty, jak události vyhodnocovat a jak se chovat k incidentům, které z událostí vyhodnotí.

Pobočka	Dnů	Cena kurzu	ITB
Praha	4	29 600 Kč	40
Brno	4	29 600 Kč	40
Bratislava	4	1 320 €	40

Uvedené ceny jsou bez DPH.

Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
G 26.05.2025	4	29 600 Kč	Prezenční	CZ/SK	Gopas Praha Prezenční
G 23.06.2025	4	1 320 €	Online	CZ/SK	Gopas Bratislava Online
G 23.06.2025	4	29 600 Kč	Online	CZ/SK	Gopas Praha Online
26.08.2025	4	29 600 Kč	Prezenční	CZ/SK	Gopas Praha Prezenční
16.09.2025	4	1 320 €	Prezenční	CZ/SK	Gopas Bratislava Prezenční
18.11.2025	4	29 600 Kč	Prezenční	CZ/SK	Gopas Praha Prezenční
01.12.2025	4	1 320 €	Online	CZ/SK	Gopas Bratislava Online

Uvedené ceny jsou bez DPH.

Předpokládané vstupní znalosti

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

Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

Ochrana proti hrozbám pomocí Microsoft Defender for Endpoint

Nasazení Microsoft Defender for Endpoint

Využití rozšíření a vylepšení ve Windows 10 pomocí Microsoft Defender for Endpoint

Sledování a správa varování a událostí Microsoft Defender for Endpoint

Vyšetřování incidentů na zařízeních pomocí Microsoft Defender for Endpoint

Provádění vzdálených zásahů na zařízeních pomocí Microsoft Defender for Endpoint

Sběr elektronických důkazů a vyšetřování incidentů na zařízeních pomocí Microsoft Defender for Endpoint

Automatizace úkolů a činností v Microsoft Defender for Endpoint

Varování a detekce a jejich nastavení v Microsoft Defender for Endpoint

Technologie Threat and Vulnerability Management v Microsoft Defender for Endpoint

Ochrany proti hrozbám v Microsoft 365

Zmírnění a minimalizace rizik za pomoci Microsoft 365 Defender

Ochrana uživatelských účtů a identit pomocí Azure AD Identity Protection

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 - detekce bezpečnostních incidentů a jejich zvládní

Snižování rizik pomocí Microsoft Defender for Office 365
Ochrana prostředí pomocí Microsoft Defender for Identity
Bezpečnost cloudových aplikací pomocí Microsoft Cloud App Security
Reakce na varování z technologií ochrany proti úniku informací (data leakage prevention - DLP) Microsoft 365
Rizika útoku insiderů (inside job) v Microsoft 365
Vysvětlení ochrany cloudové infrastruktury v Azure Defender
Připojení cloudových prostředků k Azure Defender
Připojení ne-cloudových prostředků k Azure Defender
Řešení bezpečnostních událostí a varování v Azure Defender
Vytváření vyhledávacích dotazů KQL v Azure Sentinel
Analýza výstupů vyhledávání pomocí KQL
Vytváření více-tabulkových dotazů v KQL jazyku
Práce s daty přes KQL (Kusto Query Language) v Azure Sentinel
Vytváření a správa pracovních prostorů v Azure Sentinel
Protokoly vyhledávání v Azure Sentinel
Sledovací seznamy v Azure Sentinel
Technologie Threat Intelligence v Azure Sentinel
Připojování datových zdrojů do Azure Sentinel
Připojení služeb Microsoft do Azure Sentinel
Připojení výstupů Microsoft 365 Defender do Azure Sentinel
Připojení Windows počítačů do Azure Sentinel
Připojení protokolů v Common Event Format do Azure Sentinel
Připojení protokolů ze Syslog do Azure Sentinel
Připojení indikátorů hrozeb do Azure Sentinel
Detekce hrozeb pomocí Azure Sentinel analytiky
Reakce na incidenty a hrozby pomocí Azure Sentinel
Řízení bezpečnostních incidentů pomocí Azure Sentinel
Analytika chování entit pomocí Azure Sentinel
Dotazování, vyhledávání, vizualizace a sledování informací v Azure Sentinel
Zachytávání hrozeb v Azure Sentinel
Poznámkové bloky a jejich úloha ve vyhledávání hrozeb v Azure Sentinel

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

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 - detekce bezpečnostních incidentů a jejich zvládnutí

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



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