Microsoft 365 - Microsoft Security Operations Analyst with Defender XDR

Course code: MOC SC-200

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

At course completion students will be able

Explain how Microsoft Defender for Endpoint can remediate risks in your environment

Create a Microsoft Defender for Endpoint environment

Configure Attack Surface Reduction rules on Windows 10 devices

Perform actions on a device using Microsoft Defender for Endpoint

Investigate domains and IP addresses in Microsoft Defender for Endpoint

Investigate user accounts in Microsoft Defender for Endpoint

Configure alert settings in Microsoft Defender for Endpoint

Explain how the threat landscape is evolving

Conduct advanced hunting in Microsoft 365 Defender

Manage incidents in Microsoft 365 Defender

Explain how Microsoft Defender for Identity can remediate risks in your environment

Investigate DLP alerts in Microsoft Cloud App Security

Explain the types of actions you can take on an insider risk management case

Configure auto-provisioning in Azure Defender

Remediate alerts in Azure Defender

Construct KQL statements

Filter searches based on event time, severity, domain, and other relevant data using KQL

Extract data from unstructured string fields using KQL

Manage an Azure Sentinel workspace

Use KQL to access the watchlist in Azure Sentinel

Manage threat indicators in Azure Sentinel

Explain the Common Event Format and Syslog connector differences in Azure Sentinel

Connect Azure Windows Virtual Machines to Azure Sentinel

Configure Log Analytics agent to collect Sysmon events

Create new analytics rules and queries using the analytics rule wizard

Create a playbook to automate an incident response

Use queries to hunt for threats

Observe threats over time with livestream

Prerequisities

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 - Microsoft Security Operations Analyst with Defender XDR

Knowledge in extent of the courses which are listed in the bellow sections Previous Courses and Related Courses

Good understanding of TCP/IP and DNS technologies

Course outline

Protect against threats with Microsoft Defender for Endpoint

Deploy the Microsoft Defender for Endpoint environment

Implement Windows 10 security enhancements with Microsoft Defender for Endpoint

Manage alerts and incidents in Microsoft Defender for Endpoint

Perform device investigations in Microsoft Defender for Endpoint

Perform actions on a device using Microsoft Defender for Endpoint

Perform evidence and entities investigations using Microsoft Defender for Endpoint

Configure and manage automation using Microsoft Defender for Endpoint

Configure for alerts and detections in Microsoft Defender for Endpoint

Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint

Introduction to threat protection with Microsoft 365

Mitigate incidents using Microsoft 365 Defender

Protect your identities with Azure AD Identity Protection

Remediate risks with Microsoft Defender for Office 365

Safeguard your environment with Microsoft Defender for Identity

Secure your cloud apps and services with Microsoft Cloud App Security

Respond to data loss prevention alerts using Microsoft 365

Manage insider risk in Microsoft 365

Plan for cloud workload protections using Azure Defender

Explain cloud workload protections in Azure Defender

Connect Azure assets to Azure Defender

Connect non-Azure resources to Azure Defender

Remediate security alerts using Azure Defender

Construct KQL statements for Azure Sentinel

Analyze query results using KQL

Build multi-table statements using KQL

Work with data in Azure Sentinel using Kusto Query Language

Introduction to Azure Sentinel

Create and manage Azure Sentinel workspaces

Query logs in Azure Sentinel

Use watchlists in Azure Sentinel

Utilize threat intelligence in Azure Sentinel

Connect data to Azure Sentinel using data connectors

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 - Microsoft Security Operations Analyst with Defender XDR

Connect Microsoft services to Azure Sentinel

Connect Microsoft 365 Defender to Azure Sentinel

Connect Windows hosts to Azure Sentinel

Connect Common Event Format logs to Azure Sentinel

Connect syslog data sources to Azure Sentinel

Connect threat indicators to Azure Sentinel

Threat detection with Azure Sentinel analytics

Threat response with Azure Sentinel playbooks

Security incident management in Azure Sentinel

Use entity behavior analytics in Azure Sentinel

Query, visualize, and monitor data in Azure Sentinel

Threat hunting with Azure Sentinel

Hunt for threats using notebooks in Azure Sentinel

Preparation for Microsoft certification

Most Microsoft certification exams do not require students to attend an official MOC course in order to pass the exam.

This applies to all certifications except for MCM

Official Microsoft MOC courses as well as our own GOC courses are good ways of preparation for Microsoft certifications such as MCP, MTA, MCSA, MCSE or MCM

This does not mean that official MOC courses would serve as the only necessary praparation. The primary goal of an MOC course is to provide for sufficient theoretical knowledge and practical experience to effectively work with the related product

MOC courses usually cover most of the topics required by their respective certification exams, but often do not give every topic the same amount of time and emphassis as may be required to completelly pass the exam

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