

SC-200 Microsoft Security Operations Analyst, Part 2 of 9: Microsoft 365 Defender

page 1

Meet the expert: Cristian Calinescu is a Microsoft certified Azure Solutions Architect Expert, Senior Infrastructure Engineer and Infrastructure Security Operations Manager.

Prerequisites: Basic understanding of Microsoft 365, environment, security, compliance and identity products.

Windows 10/11

familiarity with Azure services, DB, Storage

basic understanding of Scripting concepts

Runtime: 02:59:25

Course description: The SC-200 Microsoft Security Operations Analyst exam measures your ability to accomplish the following technical tasks: mitigate threats using Microsoft 365 Defender (25-30%); mitigate threats using Microsoft Defender for Cloud (25-30%); and mitigate threats using Microsoft Sentinel (40-45%) .

Course outline:

Threat Protection with Microsoft 365 Defender

- Introduction
 - Threat Protection with Microsoft 365 Defender
 - Introduction to Threat Protection
 - Common Threats
 - Defender Architecture
 - Incidents in Microsoft 365 Defender
 - Defender Portal
 - Demo: Defender Portal
 - Summary
- Azure AD Identity Protection
 - What are Risks
 - Identity Protection Workflow
 - Investigate Risks
 - Unblock Users
 - Microsoft Defender for Cloud Apps
 - Cloud Discovery
 - Conditional Access App Control
 - Classify and Protect Sensitive Information
 - Summary

Advanced Hunting

- Introduction
 - Advanced Hunting
 - Demo: Advanced Hunting
 - Threat Hunting
 - Threat Hunting within Network
 - Consult Microsoft Threat Experts
 - Summary
- Respond to DLP Alerts
 - Introduction
 - Respond to DLP Alerts
 - Data Loss Prevention Components
 - Demo: Alerts and Compliance Policy
 - SManage Insider Risk Management in Microsoft 365
 - Insider Risk
 - Common Risk Scenarios
 - Risk Management Workflow
 - Manage Risk Policies
 - Demo: Risk
 - Summary

Remediate risks with Microsoft 365 Defender

- Introduction
- Remediate Risks
- Automate - Investigate - Remediate
- Simulate Attacks
- Microsoft Defender for Identities
- Monitor and Profile user Behavior Activities
- Identify Suspicious Activities
- Configure Microsoft Defender for Identity Sensors
- Summary

Azure AD Identity Protection

- Introduction