SC-200 Microsoft Security Operations Analyst, Part 4 of 9: Microsoft Defender for Cloud

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 wit Azure services, DB, Storage
basic understanding of Scripting concepts

Runtime: 02:01:19

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%) .

This course covers Mitigate threats using Microsoft Defender for Cloud.

Course outline:

Plan for Cloud Workload Protections
- Introduction
- Plan for Cloud Workload Protections
- Microsoft Defender for Cloud Explained
- Cloud workload Protections
- Summary

Cloud Workload Protections
- Introduction
- Cloud workload protections in Microsoft Defender
- Microsoft Defender for Servers
- Microsoft Defender for App Service
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Key Vault
- Microsoft Defender for Resource Manager
- Microsoft Defender for Kubernetes
- More Protections
- Summary

Connect Azure Assets To Microsoft Defender for Cl
- Introduction
- Connect Azure Assets To Microsoft Defender for Cl
- Manage Resources
- Demo: Asset Inventory
- How to Use Asset Inventory
- Demo Auto Provisioning
- Connect non-Azure resources to Microsoft Defender
- Protect non-Azure Resources
- Connect AWS Accounts
- Demo: Service
- Create AWS Cloud Connector
- Connect GCP Cloud Connector
- Summary

Security Alerts for Defender for Cloud
- Introduction
- Security Alerts in Microsoft Defender for Cloud
- Security Alerts Explained
- Understand Alert Types
- Demo: Alerts
- Summary