SC-200 Microsoft Security Operations Analyst, Part 3 of 9: Microsoft Defender for Endpoint

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: 02:12:43

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 Endpoint.

Course outline:

Protect against threats for Endpoint
- Introduction
- Protect against threats with Microsoft Defender f
- Microsoft Defender for Endpoint Explained
- Security Operations
- Deploy Microsft Defender for Endpoint environment
- Create your Environment
- Onboard Devices
- Demo: Onboard Device
- Manage Access
- Configure Device Groups
- Demo Create Device Group
- Summary

Windows Security Enhancements
- Introduction
- Implement Windows Security Enhancements
- Attack Surface Reduction
- Enable Attack Surface Reduction Rules
- Demo: Enable ASR
- Device Investigations
- Device Inventory List
- Investigate Devices
- Demo: Devices
- Behavioral Blocking
- Endpoint Detection
- Demo: Enable EDR
- Summary

Perform Actions on a Device
- Introduction
- Perform actions on a device
- Device Actions
- Investigation Package
- Initiate Live Response Session
- Live Response Commands
- Demo: Live Response Session
- Perform evidence and entities investigations
- Investigate File
- Demo: Investigate File
- Summary

Configure and Manage Automation
- Introduction
- Configure and manage automation
- Configure Advanced Features
- Demo: Advanced Features
- Block at Risk Devices
- Configure alerts and detections
- Demo: notification Alert
- Threat and Vulnerability Management
- Summary