SC-200 Microsoft Security Operations Analyst, Part 6 of 9: Configure Microsoft Sentinel

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: 59:26

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 Configure Microsoft Sentinel.

Course outline:

Microsoft Sentinel Overview
- Introduction
- Microsoft Sentinel Overview
- Sentinel Explained
- How Sentinel Works
- When to Use Sentinel
- Create and Manage Microsoft Sentinel workspaces
- Single Tenant Workspace
- Demo: Workspaces
- Summary

Query Logs in Microsoft Sentinel
- Introduction
- Query logs in Microsoft Sentinel
- Understand Sentinel Tables
- Demo: Logs Window
- Use Watchlists in Microsoft Sentinel
- Plan for Sentinel Watchlist
- Demo: Create Watchlist
- Use Threat Intelligence in Microsoft Sentinel
- Define Threat Intelligence
- Demo: Manage Threat Indicators
- Summary