SC-200 Microsoft Security Operations Analyst, Part 8 of 9: Detection with 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: 01:27:34

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 Detection and investigations using Microsoft Sentinel.

Course outline:

Threat Detection with Microsoft Sentinel Analytics
- Introduction
- Threat Detection with Microsoft Sentinel Analytics
- Sentinel Analytics
- Types of Analytics Rules
- Fusion Alerts
- Typs of Analytics Rules
- Demo: Create Analytical Rule
- Security Incident managent in Microsoft Sentinel
- Key concepts
- Explain Evidence and Entities
- Investigate Incidents
- Demo: Incients
- Summary

Threat Response with Microsoft Sentinel Playbooks
- Introduction
- Threat Response with Microsoft Sentinel Playbooks
- Create Logic App
- Demo: Playbook
- Summary

Entity Behaviour Analytics in Microsoft Sentinel
- Introduction
- Entity Behaviour Analytics in Microsoft Sentinel
- Architecture Overview
- Security Driven Analytics
- Demo: Entities Timeline
- Workbooks in Microsoft Sentinel
- Sentinel Workbooks
- Demo: Sentinel Workbooks
- Summary