SC-200 Microsoft Security Operations Analyst, Part 9 of 9: Microsoft Sentinel Threat Hunting

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: 31:26

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 Threat hunting in Microsoft Sentinel.

Course outline:

Threat Hunting Concepts in Microsoft Sentinel

- Introduction
- Threat Hunting Concepts in Microsoft Sentinel
- Cybersecurity Threat Hunting
- Develop Threat Hunting Hypothesis
- Threat Hunting with Microsoft Sentinel
- Hunt Using Built-in Queries
- Demo: Quries
- Observe Threats Over TIme
- Demo: Observe Threats
- Notebooks in Microsoft Sentinel
- Hunt with Notebooks
- Create a Notebook
- Demo: Create Notebook
- Explore Notebook
- Summary