SC-200 Microsoft Security Operations Analyst, Part 7 of 9: Microsoft Sentinel Logging

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: 51:10

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 Connect logs to Microsoft Sentinel.

Course outline:

Connect Data to Sentinel using Data Connectors
- Introduction
- Connect Data to Microsoft Sentinel using Data Con
- Ingest Log Data
- Demo: Data Connectors
- Describe Data Connector Providers
- View Connected Hosts
- Demo: Hosts
- Connect Microsoft 365 Defender to Microsoft Senti
- Office 365 Connector
- Demo: Office Connector
- Connect Microsoft Services to Microsoft Sentinel
- Demo: Connect Services
- Azure AD Identity Protection
- Summary

Connect Windows Hosts to Sentinel
- Introduction
- Connect Windows Hosts to Microsoft Sentinel
- Plan for Windows Hosts Security Events Connector
- Demo: Security Events Legacy
- Connect CEF logs to Microsoft Sentinel
- Plan common Event Format Connector
- Connect External Solution with CEF Connector
- Demo: Common Event Format
- Connect Syslog data to Microsoft Sentinel
- Collect Data from Linux-based Sources
- Demo: Linux
- Connect Threat Indicators to Microsoft Sentinel
- Plan for Threat Intelligence Connectors
- Connect Threat Intelligence Connector
- Demo: Intelligence Platform
- Summary