

# SC-200 Microsoft Security Operations Analyst, Part 5 of 9: Kusto Query Language

page 1

**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 with Azure services, DB, Storage

basic understanding of Scripting concepts

**Runtime:** 01:11:34

**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 Kusto Query Language queries for Microsoft Sentinel.

## Course outline:

### Construct KQL Statements for Microsoft Sentinel

- Introduction
- Construct KQL statements for Microsoft Sentinel
- Demo: KQL
- Summary

### Analyze Query Results

- Introduction
- Analyze query results
- Demo: Analyze Query Results
- Build Multi-Table queries in KQL
- Demo: Multi-table Queries
- Use Join Operator
- Work with string data using KQL
- Extract Data from Unstructured String Fields
- Summary