SC-200T00 Microsoft Security Operations Analyst

churchillsquareconsulting.virtualinstructorledtraining.com/courses/sc-200t00-microsoft-security-operations-analyst/

Introduction:

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Objectives:

Explain how Microsoft Defender for Endpoint can remediate risks in your environment
Administer a Microsoft Defender for Endpoint environment
Configure Attack Surface Reduction rules on Windows devices
Perform actions on a device using Microsoft Defender for Endpoint
Investigate domains and IP addresses in Microsoft Defender for Endpoint
Investigate user accounts in Microsoft Defender for Endpoint
Configure alert settings in Microsoft 365 Defender
Conduct hunting in Microsoft 365 Defender
Manage incidents in Microsoft 365 Defender
Explain how Microsoft Defender for Identity can remediate risks in your environment
Investigate DLP alerts in Microsoft Defender for Cloud Apps
Explain the types of actions you can take on an insider risk management cases
Configure auto-provisioning in Microsoft Defender for Cloud Apps
Remediate alerts in Microsoft Defender for Cloud Apps
Construct KQL statements
Filter searches based on event time, severity, domain, and other relevant data using KQL
Extract data from unstructured string fields using KQL
Manage a Microsoft Sentinel workspace
Use KQL to access the watchlist in Microsoft Sentinel
Manage threat indicators in Microsoft Sentinel
Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel
Connect Azure Windows Virtual Machines to Microsoft Sentinel
Configure Log Analytics agent to collect Sysmon events

Create new analytics rules and queries using the analytics rule wizard
Create a playbook to automate an incident response
Use queries to hunt for threats
Observe threats over time with livestream

Course Outline:

1 – Mitigate threats using Microsoft 365 Defender

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Remediate risks with Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Protect your identities with Azure AD Identity Protection
- Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365

2 – Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

3 – Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Workload protections in Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

4 – Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

5 – Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel

- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

6 – Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

7 – Create detections and perform investigations using Microsoft Sentinel

- Threat detection with Microsoft Sentinel analytics
- Security incident management in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- User and entity behavior analytics in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

8 – Perform threat hunting in Microsoft Sentinel

- Threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Enroll in this course

£2,380.00

Select a start date for your 4 Days course

- 2023-01-30 09:00:00_2023-02-02 17:00:00
- 2023-04-04 09:00:00_2023-04-07 17:00:00
- 2023-06-06 09:00:00_2023-06-09 17:00:00