SC-200T00 - Microsoft Security Operations Analyst

Microsoft - Microsoft Security - Virtualizzazione e Cloud

Durata:	Lingue:	Certificazione:
4 Giorni	**Italiano**	**Microsoft Certified: Microsoft Security Operations Analyst**

ITCore Group

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com

Descrizione del corso

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft 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.

Skills gained

Due to this course, students will learn how:
• 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
• Explain how the threat landscape is evolving
• Conduct advanced 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 case
• 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

Audience profile

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Prerequisites

• Basic understanding of Microsoft 365
• Fundamental understanding of Microsoft security, compliance, and identity products
• Intermediate understanding of Windows 10
• Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
• Familiarity with Azure virtual machines and virtual networking
• Basic understanding of scripting concepts.

Programma

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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