Microsoft Security Operations Analyst

CODICE	SC-200T00
DURATA	4 gg
PREZZO	1.590,00 €
EXAM	

DESCRIZIONE

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.

TARGET

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 Azure Sentinel, Azure Defender, 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.

PREREQUISTI

- 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.

CONTENUTI

- Mitigate threats using Microsoft Defender XDR
- Mitigate threats using Microsoft Copilot for Security
- Mitigate threats using Microsoft Purview
- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft Defender for Cloud
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Configure your Microsoft Sentinel environment
- Connect logs to Microsoft Sentinel
- Create detections and perform investigations using Microsoft Sentinel
- Perform threat hunting in Microsoft Sentinel