SC-200T00-A

Microsoft Security Operations Analyst

32 horas | Microsoft 365 | Microsoft

INTRODUÇÃO

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.

OBJETIVO DO CURSO

–

PÚBLICO-ALVO

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.

PRÉ-REQUISITOS

Prerequisites

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

CONTEÚDO PROGRAMÁTICO

Course outline

- Module 1: SC-200: Mitigate threats using Microsoft 365 Defender
- Module 2: SC-200: Mitigate threats using Microsoft Defender for Endpoint
- Module 3: SC-200: Mitigate threats using Microsoft Defender for Cloud
- Module 4: SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Module 5: SC-200: Configure your Microsoft Sentinel environment
- Module 6: SC-200: Connect logs to Microsoft Sentinel
- Module 7: SC-200: Create detections and perform investigations using Microsoft Sentinel