MSEC-2 - MOC SC-200T00 - MICROSOFT SECURITY OPERATIONS ANALYST

Categoria: **MS Security**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
4 Giorni	MS Security	Microsoft Certified Trainer	Professionista IT	Microsoft

OBIETTIVI

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.

PREREQUISITI

-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

CONTENUTI

Introduction to Microsoft 365 threat protection

Mitigate incidents using Microsoft 365 Defender

Protect your identities with Azure AD Identity Protection

Remediate risks with Microsoft Defender for Office 365

Safeguard your environment with Microsoft Defender for Identity

Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Respond to data loss prevention alerts using Microsoft 365

Manage insider risk in Microsoft Purview

Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview Standard

Investigate threats using audit in Microsoft 365 Defender and Microsoft Purview (Premium)

Investigate threats with Content search in Microsoft Purview

Protect against threats with Microsoft Defender for Endpoint

Deploy the Microsoft Defender for Endpoint environment

Implement Windows security enhancements with Microsoft Defender for Endpoint

Perform device investigations in Microsoft Defender for Endpoint

Perform actions on a device using Microsoft Defender for Endpoint

Perform evidence and entities investigations using Microsoft Defender for Endpoint

Configure and manage automation using Microsoft Defender for Endpoint

Configure for alerts and detections in Microsoft Defender for Endpoint

Utilize Vulnerability Management in Microsoft Defender for Endpoint

Plan for cloud workload protections using Microsoft Defender for Cloud

Connect Azure assets to Microsoft Defender for Cloud

Connect non-Azure resources to Microsoft Defender for Cloud

Manage your cloud security posture management

Explain cloud workload protections in Microsoft Defender for Cloud

Remediate security alerts using Microsoft Defender for Cloud

Construct KQL statements for Microsoft Sentinel

Analyze query results using KQL

Build multi-table statements using KQL

Work with data in Microsoft Sentinel using Kusto Query Language

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

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

Threat detection with Microsoft Sentinel analytics

Automation in Microsoft Sentinel

Security incident management in Microsoft Sentinel

Identify threats with Behavioral Analytics

Data normalization in Microsoft Sentinel

Query, visualize, and monitor data in Microsoft Sentinel

Manage content in Microsoft Sentinel

Explain threat hunting concepts in Microsoft Sentinel

Threat hunting with Microsoft Sentinel

Use Search jobs in Microsoft Sentinel

Hunt for threats using notebooks in Microsoft Sentinel

INFO

Esame: SC-200 - Microsoft Security Operations Analyst
Materiale didattico: Materiale didattico ufficiale Microsoft in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)