MASK-34 - MOC SC-5001 - CONFIGURE SIEM SECURITY OPERATIONS USING MICROSOFT SENTINEL

Categoria: **Applied Skills**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
1 Giorni	Applied Skills	Microsoft Certified Trainer	Professionista IT	Microsoft

OBIETTIVI

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses.

PREREQUISITI

-Fundamental understanding of Microsoft Azure
-Basic understanding of Microsoft Sentinel
-Experience using Kusto Query Language (KQL) in Microsoft Sentinel

CONTENUTI

Create and manage Microsoft Sentinel workspaces

Connect Microsoft services to Microsoft Sentinel

Connect Windows hosts to Microsoft Sentinel

Threat detection with Microsoft Sentinel analytics

Automation in Microsoft Sentinel

Configure SIEM security operations using Microsoft Sentinel

INFO

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)