

# CORSO MOC SC-200 MICROSOFT SECURITY OPERATIONS ANALYST

DURATA: 4 GIORNI

## PROGRAMMA

### MODULE I: 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 II: 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 III: 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 IV: 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

## CONTACT

 info@nexsys.it

 www.nexsys.it



# CORSO MOC SC-200 MICROSOFT SECURITY OPERATIONS ANALYST

DURATA: 4 GIORNI

## MODULE V: 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 VI: 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 VII: 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 VIII: 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

[Scopri di più sul Corso MOC SC-200 Microsoft Security Operations Analyst](#)

### CONTACT

info@nexsys.it

www.nexsys.it