Microsoft Security Operations Analyst

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Microsoft Security Operations Analyst

Course Modules

1. **Manage a security operations environment**

Configure settings in Microsoft Defender XDR

- Connection from Defender XDR to a Sentinel workspace
- Configure alert and vulnerability notification rules
- Configure Microsoft Defender for Endpoint advanced features
- Configure endpoint rules settings
- Manage automated investigation and response capabilities
- Automatic attack disruption in Microsoft Defender XDR

Manage assets and environments

- Manage device groups, permissions, and automation levels
- Identify and remediate unmanaged devices
- Manage resources by using Azure Arc
- Connect environments to Microsoft Defender for Cloud
- Discover and remediate unprotected resources
- Identify and remediate devices at risk

Design and configure a Microsoft Sentinel workspace

- Plan a Microsoft Sentinel workspace
- Configure Microsoft Sentinel roles
- Specify Azure RBAC roles for Microsoft Sentinel configuration
- Design and configure Microsoft Sentinel data storage
- Manage multiple workspaces

Microsoft Security Operations Analyst

Ingest data sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
- Configure and use Microsoft connectors for Azure resources
- Bidirectional sync bet MS Sentinel & Microsoft Defender XDR
- Bidirectional sync bet MS Sentinel to Microsoft Defender
- Config Syslog & Comm Event Format (CEF) event collections
- Plan and configure collection of Windows Security events

2. Configure protections and detections

Config protections in Microsoft Defender security technologies

- Configure policies for Microsoft Defender for Cloud Apps
- Configure policies for Microsoft Defender for Office
- Configure security policies for Microsoft Defender (ASR) rule
- Configure cloud workload protections in Microsoft Defender

Configure detection in Microsoft Defender XDR

- Configure and manage custom detections
- Configure alert tuning
- Configure deception rules in Microsoft Defender XDR

Configure detections in Microsoft Sentinel

- Classify and analyze data by using entities
- Configure scheduled query rules, including KQL
- Configure near-real-time (NRT) query rules, including KQL
- Manage analytics rules from Content hub
- Configure anomaly detection analytics rules
- Configure the Fusion rule
- Manage and use threat indicators

3. Manage incident response

Respond to alerts and incidents in Microsoft Defender XDR

- Remediate threats to Microsoft Teams, SharePoint Online, etc.,
- Investigate and remediate threats in email
- Remediate ransomware and business email compromise
- Investigate and remediate compromised entities identified
- Threats identified by Microsoft Purview insider risk policies
- Investigate and remediate alerts and incidents identified
- Investigate and remediate security risks identified
- Remediate compromised identities in Microsoft Entra ID
- Remediate security alerts frm Microsoft Defender for Identity
- Manage actions & submissions in the MS Defender portal

Respond to alerts and incidents identified

- Investigate timeline of compromised devices
- Perform actions on the device
- Perform evidence and entity investigation

Enrich investigations by using other Microsoft tools

- Investigate threats by using unified audit Log
- Investigate threats by using Content Search
- Perform threat hunting by using Microsoft Graph activity logs

Manage incidents in Microsoft Sentinel

- Triage incidents in Microsoft Sentinel
- Investigate incidents in Microsoft Sentinel
- Respond to incidents in Microsoft Sentinel

Security orchestration, automation, and response (SOAR)

- Create and configure automation rules
- Create and configure Microsoft Sentinel playbooks
- Configure analytic rules to trigger automation
- Trigger playbooks manually from alerts and incidents
- Run playbooks on On-premises resources

4. Perform threat hunting

Hunt for threats by using KQL

- Identify threats by using Kusto Query Language (KQL)
- Interpret threat analytics in the Microsoft Defender portal
- Create custom hunting queries by using KQL

Hunt for threats by using Microsoft Sentinel

- Analyze attack vector coverage by using the MITRE ATT&CK
- Customize content gallery hunting queries
- Use hunting bookmarks for data investigations
- Monitor hunting queries by using Livestream
- Retrieve and manage archived log data
- Create and manage search jobs

Analyze and interpret data by using workbooks

- Activate & customize Microsoft Sentinel workbook templates
- Create custom workbooks that include KQL
- Configure visualizations

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474