Microsoft Security Operations Analyst

Length: 4 days
Format: Classroom
Time: Day

About This Course

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.

Required Exams

Audience Profile

Course Objectives

* Architecting and managing a cloud-native SIEM (Microsoft Sentinel).
* Automating enterprise security orchestration via Logic Apps and playbooks.
* Writing custom detection and hunting logic using Kusto Query Language (KQL).
* Operating an AI-accelerated Security Operations Center (SOC).

Outline

Module 1: Mitigate threats using Microsoft Defender XDR * Introduction to Microsoft Defender XDR: Exploring extended detection and response capabilities across identity, endpoints, cloud apps, and data.
* Incident Management: Investigating and remediating multi-stage, multi-domain attacks and managing timelines.
* Microsoft Defender for Office 365: Remediating malicious emails, attachments, and utilizing automatic attack disruption.

* Identity Protection: Managing identity protection policies in Microsoft Entra ID and tracking compromised credentials.
* Microsoft Defender for Identity: Safeguarding on-premises Active Directory environments and tracking lateral movement.
* Microsoft Defender for Cloud Apps: Securing cloud applications, handling shadow IT, and resolving SaaS security alerts.

Module 2: Mitigate threats using Microsoft Security Copilot * Generative AI in the SOC: Understanding AI agents and core features of Microsoft Security Copilot.
* Embedded Security AI: Using natural language prompts to summarize incidents, analyze scripts, and build reports faster.
* Use Cases: Automating common analyst workflows and streamlining digital forensics.

Module 3: Mitigate threats using Microsoft Purview * Data Loss Prevention (DLP): Investigating, triaging, and responding to sensitive data exposure alerts.
* Insider Risk Management: Detecting malicious or inadvertent internal threats and reviewing risky employee behaviors.
* Audit and eDiscovery: Conducting forensic searches using Microsoft Purview Audit.

Module 4: Mitigate threats using Microsoft Defender for Endpoint * Deployment & Environment Setup: Configuring Defender for Endpoint environments, device groups, and permission structures.
* Attack Surface Reduction (ASR): Setting up rules to prevent malware infections at the device level.
* Forensic Actions: Running isolation protocols, live response sessions, and searching domains/IPs on endpoint devices.

Module 5: Mitigate threats using Microsoft Defender for Cloud * Cloud Security Posture Management (CSPM): Evaluating environments against regulatory compliance standards.
* Workload Protections: Remediating multi-cloud threats (Azure, AWS, and GCP) and setting up auto-provisioning.

Module 6: Create queries for Microsoft Sentinel using Kusto Query Language (KQL) * KQL Fundamentals: Writing logic to filter, structure, and query security logs.
* Advanced Extractions: Utilizing string operators, functions, and watchlists to manipulate raw log data.

Module 7: Configure your Microsoft Sentinel environment * Workspace Design: Planning architecture, managing roles, and setting data retention tiers.
* Data Ingestion: Deploying data connectors (such as AMA, WEF, Syslog, and CEF) to collect enterprise logs.
* Analytic Rules: Engineering automated threat detection rules using the wizard.
* Workbooks & Dashboards: Building visual dashboards to monitor threats over time.

Module 8: Respond and hunt in Microsoft Sentinel * Incident Triage: Managing incidents through case

management and assigning severity.

* Automation: Creating automation rules and building playbooks to respond to alerts without manual input.

* Proactive Threat Hunting: Designing hypotheses, launching livestreams, and scanning logs for indicators of compromise (IOCs).