Microsoft Certified: Security Operations Analyst Associate – Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Exam SC-200: Microsoft Security Operations Analyst

Mitigate threats using Microsoft 365 Defender (25-30%)

Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365

- detect, investigate, respond, remediate Microsoft Teams, SharePoint, and OneDrive for Business threats
- detect, investigate, respond, remediate threats to email by using Defender for Office 365
- manage data loss prevention policy alerts
- assess and recommend sensitivity labels
- assess and recommend insider risk policies

Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint

- manage data retention, alert notification, and advanced features
- configure device attack surface reduction rules
- configure and manage custom detections and alerts
- respond to incidents and alerts
- manage automated investigations and remediations Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using Microsoft's Threat and Vulnerability Management solution.
- manage Microsoft Defender for Endpoint threat indicators
- analyze Microsoft Defender for Endpoint threat analytics

Detect, investigate, respond, and remediate identity threats

- identify and remediate security risks related to sign-in risk policies
- identify and remediate security risks related to Conditional Access events
- identify and remediate security risks related to Azure Active Directory

- identify and remediate security risks using Secure Score
- identify, investigate, and remediate security risks related to privileged identities
- configure detection alerts in Azure AD Identity Protection
- identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity
- identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)
- configure MCAS to generate alerts and reports to detect threats

Manage cross-domain investigations in Microsoft 365 Defender Portal

- manage incidents across Microsoft 365 Defender products
- manage actions pending approval across products
- perform advanced threat hunting

Mitigate threats using Azure Defender (25-30%)

Design and configure an Azure Defender implementation

- plan and configure an Azure Defender workspace
- configure Azure Defender roles
- configure data retention policies
- assess and recommend cloud workload protection

Plan and implement the use of data connectors for ingestion of data sources in Azure Defender

- identify data sources to be ingested for Azure Defender
- configure Automated Onboarding for Azure resources
- connect non-Azure machine onboarding
- connect AWS cloud resources
- connect GCP cloud resources
- configure data collection

Manage Azure Defender alert rules

- validate alert configuration
- setup email notifications
- create and manage alert suppression rules

Configure automation and remediation

- configure automated responses in Azure Security Center
- design and configure playbook in Azure Defender

- remediate incidents by using Azure Defender recommendations
- create an automatic response using an Azure Resource Manager template

Investigate Azure Defender alerts and incidents

- describe alert types for Azure workloads
- manage security alerts
- manage security incidents
- analyze Azure Defender threat intelligence
- respond to Azure Defender for Key Vault alerts
- manage user data discovered during an investigation

Mitigate threats using Azure Sentinel (40-45%)

Design and configure an Azure Sentinel workspace

- plan an Azure Sentinel workspace
- configure Azure Sentinel roles
- design Azure Sentinel data storage
- configure Azure Sentinel service security

Plan and Implement the use of Data Connectors for Ingestion of Data Sources in Azure Sentinel

- identify data sources to be ingested for Azure Sentinel
- identify the prerequisites for a data connector
- configure and use Azure Sentinel data connectors
- design Syslog and CEF collections
- design and Configure Windows Events collections
- configure custom threat intelligence connectors
- create custom logs in Azure Log Analytics to store custom data

Manage Azure Sentinel analytics rules

- design and configure analytics rules
- create custom analytics rules to detect threats
- activate Microsoft security analytical rules
- configure connector provided scheduled queries
- configure custom scheduled queries
- define incident creation logic

Configure Security Orchestration Automation and Remediation (SOAR) in Azure Sentinel

- create Azure Sentinel playbooks

- configure rules and incidents to trigger playbooks
- use playbooks to remediate threats
- use playbooks to manage incidents
- use playbooks across Microsoft Defender solutions

Manage Azure Sentinel Incidents

- investigate incidents in Azure Sentinel
- triage incidents in Azure Sentinel
- respond to incidents in Azure Sentinel
- investigate multi-workspace incidents
- identify advanced threats with User and Entity Behavior Analytics (UEBA)

Use Azure Sentinel workbooks to analyze and interpret data

- activate and customize Azure Sentinel workbook templates
- create custom workbooks
- configure advanced visualizations
- view and analyze Azure Sentinel data using workbooks
- track incident metrics using the security operations efficiency workbook

Hunt for threats using the Azure Sentinel portal

- create custom hunting queries
- run hunting queries manually
- monitor hunting queries by using Livestream
- perform advanced hunting with notebooks
- track query results with bookmarks
- use hunting bookmarks for data investigations
- convert a hunting query to an analytical rule