Start here

Tuesday, October 25, 2022 2:37 PM

Hi,

This OneNote Study Guide has been created to help you prepare for the SC-200 exam. Please note this is not an official Microsoft document.

Tabs
Overview - includes list of exam objectives and other resources. Most resources are Microsoft specific but I have included non-Microsoft links.

The exam domains each have a tab and each set of objectives have a page within the domain. I have included links to the Microsoft docs. Those can be found on the left side of the page. Additional links are on the right.

Please feel free to update and change this OneNote to help you prepare for SC-200.

Study Guide March 2024

Friday, March 15, 2024 11:20 AM

Skills measured as of March 4, 2024

Audience profile

As a candidate for this exam, you're a Microsoft security operations analyst who reduces organizational risk by:

- Rapidly remediating active attacks in cloud and on-premises environments.
- Advising on improvements to threat protection practices.
- Identifying violations of organizational policies.

As a security operations analyst, you:

- Perform triage.
- Respond to incidents.
- Manage vulnerabilities.
- Hunt for threats.
- Evaluate logs.
- Analyze threat intelligence.

You also monitor, identify, investigate, and respond to threats in cloud and on-premises environments by using:

- Microsoft Sentinel
- Microsoft Defender for Cloud
- Microsoft Defender XDR
- Third-party security solutions

In this role, you use Kusto Query Language (KQL) for reporting, detections, and investigations. You collaborate with business stakeholders, architects, cloud administrators, endpoint administrators, identity administrators, compliance administrators, and security engineers to secure the digital enterprise.

As a candidate, you should be familiar with:

- Microsoft 365
- Azure cloud services
- Windows and Linux operating systems

Skills at a glance

- Manage a security operations environment (25–30%)
- Configure protections and detections (15–20%)
- Manage incident response (35–40%)
- Perform threat hunting (15–20%)

Manage a security operations environment (25–30%)

Configure settings in Microsoft Defender XDR

- Configure a 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, including indicators and web content filtering
- Manage automated investigation and response capabilities in Microsoft Defender XDR
- Configure automatic attack disruption in Microsoft Defender XDR

Manage assets and environments

- Configure and manage device groups, permissions, and automation levels in Microsoft Defender for Endpoint
- Identify and remediate unmanaged devices in Microsoft Defender for Endpoint
- Manage resources by using Azure Arc
- Connect environments to Microsoft Defender for Cloud (by using multi-cloud account management)
- Discover and remediate unprotected resources by using Defender for Cloud
- Identify and remediate devices at risk by using Microsoft Defender Vulnerability Management

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, including log types and log retention
- Manage multiple workspaces by using Workspace manager and Azure Lighthouse

Ingest data sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
- Implement and use Content hub solutions
- Configure and use Microsoft connectors for Azure resources, including Azure Policy and diagnostic settings
- Configure bidirectional synchronization between Microsoft Sentinel and Microsoft Defender XDR
- Plan and configure Syslog and Common Event Format (CEF) event collections
- Plan and configure collection of Windows Security events by using data collection rules, including Windows Event Forwarding (WEF)

- Configure threat intelligence connectors, including platform, TAXII, upload indicators API, and MISP
- Create custom log tables in the workspace to store ingested data

Configure protections and detections (15–20%)

Configure 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 for Endpoints, including attack surface reduction (ASR) rules
- Configure cloud workload protections in Microsoft Defender for Cloud

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
- Query Microsoft Sentinel data by using ASIM parsers
- Manage and use threat indicators

Manage incident response (35–40%)

Respond to alerts and incidents in Microsoft Defender XDR

- Investigate and remediate threats to Microsoft Teams, SharePoint Online, and OneDrive
- Investigate and remediate threats in email by using Microsoft Defender for Office
- Investigate and remediate ransomware and business email compromise incidents identified by automatic attack disruption
- Investigate and remediate compromised entities identified by Microsoft Purview data loss prevention (DLP) policies
- Investigate and remediate threats identified by Microsoft Purview insider risk

policies
- Investigate and remediate alerts and incidents identified by Microsoft Defender for Cloud
- Investigate and remediate security risks identified by Microsoft Defender for Cloud Apps
- Investigate and remediate compromised identities in Microsoft Entra ID
- Investigate and remediate security alerts from Microsoft Defender for Identity
- Manage actions and submissions in the Microsoft Defender portal

Respond to alerts and incidents identified by Microsoft Defender for Endpoint

- Investigate timeline of compromised devices
- Perform actions on the device, including live response and collecting investigation packages
- 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

Configure security orchestration, automation, and response (SOAR) in Microsoft Sentinel

- 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

Perform threat hunting (15–20%)

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 in Microsoft Sentinel
- 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 and customize Microsoft Sentinel workbook templates
- Create custom workbooks that include KQL
- Configure visualizations

From <https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/sc-200>

Additional Links

Tuesday, October 25, 2022 10:50 AM

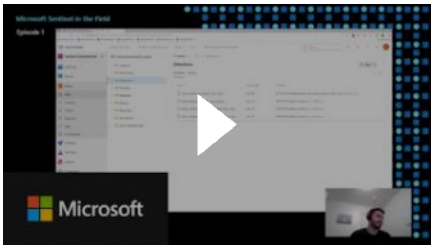
Microsoft Cybersecurity Reference Architectures
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

Sentinel documentation on GitHub. Fantastic Resource
azure-docs/articles/sentinel at main · MicrosoftDocs/azure-docs (github.com)

Log Analytics Demo
https://aka.ms/lademo

Microsoft Security YouTube Channel
Microsoft Security - YouTube

Microsoft Sentinel in the Field
Managing security content as code - Microsoft Sentinel in the Field #1



Microsoft 365 Defender Overview
Microsoft 365 Defender Playlist

Defender for MS 365 Playlist
Microsoft Defender for Office 365

https://github.com/Azure/Azure-Sentinel

SC-900
https://learn.microsoft.com/en-us/certifications/exams/sc-900

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Introduction - OWASP Cheat Sheet Series

Zen and the Art of Threat Hunting
https://www.microsoft.com/en-us/security/blog/2020/06/25/zen-and-the-art-of-threat-hunting/

http://download.microsoft.com/download/6/3/A/63AFA3DF-BB84-4B38-8704-B27605B99DA7/Microsoft%20SDL%20Cryptographic%20Recommendations.pdf

Microsoft Security Development Lifecycle Practices

Microsoft Learn Cloud Games | Microsoft Learn

Home | M365 Maps

HOWTO: Set an alert to notify when an Azure AD emergency access account is used - The things that are better left unspoken (dirteam.com)

Governance
https://learn.microsoft.com/en-us/azure/governance/

Sentinel Pricing
https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

Security Portals and admin centers
Microsoft security portals and admin centers | Microsoft Learn

PCI Data Security Standards
https://learn.microsoft.com/en-us/compliance/regulatory/offering-pci-dss

EASM
https://www.microsoft.com/en-us/security/business/cloud-security/microsoft-defender-external-attack-surface-management

Query multiple log analytics workspaces
https://techcommunity.microsoft.com/t5/itops-talk-blog/querying-multiple-log-analytics-workspace-at-once/ba-p/990843

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cross-workspace-query

Sentinel Hunting Query Pack
https://danielchronlund.com/2022/10/03/sentinel-hunting-query-pack-dcsecurityoperations/

Closing the Cybersecurity skills gap - Microsoft
https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

Azure AD Pricing
https://www.microsoft.com/en-ca/security/business/identity-access/azure-active-directory-pricing?rtc=1

Azure Free Account
https://azure.microsoft.com/en-ca/free/

MS 365 Business
https://www.microsoft.com/en-ca/microsoft-365/business/compare-all-microsoft-365-business-products

Office 365 E5
https://www.microsoft.com/en-us/microsoft-365/enterprise/office-365-e5?activetab=pivot%3aoverviewtab

Office 365 E3
https://www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot%3aoverviewtab

Azure Pricing Calculator
https://azure.microsoft.com/en-us/pricing/calculator/

Azure Sentinel SOC Process Framework Workbook
Demo: Azure Sentinel SOC Process Framework Workbook with Rin Ure

https://github.com/Azure/Azure-Sentinel/wiki/SOC-Process-Framework

Connect Hybrid machines to Azure at Scale
https://learn.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

New Microsoft Incident Response team guide shares best practices for security teams and leaders | Microsoft Security Blog

Purview Resources

Monday, March 18, 2024 3:29 PM

[Mastering Microsoft Purview Retention Policies: Your Ultimate Guide | Peter Rising MVP]

[Exploring Microsoft Purview for data governance]

[The Microsoft Purview Data Loss Prevention Ninja Training is here! - Microsoft Community Hub]

Learning Path

[SC-400: Implement Information Protection in Microsoft 365 - Training | Microsoft Learn]

Purview
[Learn about Microsoft Purview | Microsoft Learn]

Purview Free for Governance
[Get started with the free version of Microsoft Purview governance solutions | Microsoft Learn]

Purview Licensing
[Microsoft Purview eDiscovery - Service Descriptions | Microsoft Learn]

KQL Resources

Tuesday, October 25, 2022 2:02 PM

Learning Kusto Query Language - A tool for performance test engineers (microsoft.com)

https://squaredup.com/blog/kusto-table-joins-and-the-let-statement/

Microsoft KQL Learning Path Data analysis in Azure Data Explorer with Kusto Query Language - Training | Microsoft Learn

Storm KQL Tutorial Tutorial: Learn common Kusto Query Language operators - Azure Data Explorer | Microsoft Learn

KQL quick reference | Microsoft Learn

rod-trent/MustLearnKQL: Code included as part of the MustLearnKQL blog series (github.com) - includes a free pdf book

KQL/kql_cheat_sheet_v01.pdf at master · marcusbakker/KQL (github.com)

John Savill Kusto Query Language (KQL) Overview

KQL in Sentinel Kusto Query Language in Microsoft Sentinel | Microsoft Learn

UTC to local time
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/datetime-utc-to-local-function
datetime_utc_to_local(*from*,*timezone*)

From <https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/datetime-utc-to-local-function>

Join Operator
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/joinoperator?pivots=azuredataexplorer

Kusto Query to extract useful fields from Azure Firewall
https://gist.github.com/marknettle/13fd0c49fe9eeb400572b279790f78bf

Extract Function
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/extractfunction

https://dev.to/omiossec/introduction-to-kusto-query-language-kql-in-azure-monitor-2cpd

https://www.sqlservercentral.com/articles/an-introduction-to-kusto-query-language-kql

https://www.kustoking.com/basic-searching-and-string-operators/

https://azure-training.com/azure-data-science/the-kusto-query-language/

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/schema-entities/

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/concepts/

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/sqlcheatsheet

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/makelist-aggfunction

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/tutorial?pivots=azuremonitor

From <https://teams.microsoft.com/multi-window/?agent=electron&version=22111412800>

Splunk to Kusto
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/splunk-cheat-sheet

SQL to Kusto

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/sqlcheatsheet

Learning Kusto Query Language A tool for performance test engineers
https://techcommunity.microsoft.com/t5/testingspot-blog/learning-kusto-query-language-a-tool-for-performance-test/ba-p/2308480

SC-200 Learning Paths

Monday, October 24, 2022 9:39 AM

SC-200: Mitigate threats using Microsoft 365 Defender
https://learn.microsoft.com/en-us/training/paths/sc-200-mitigate-threats-using-microsoft-365-defender/

SC-200: Mitigate threats using Microsoft Defender for Endpoint
https://learn.microsoft.com/en-us/training/paths/sc-200-mitigate-threats-using-microsoft-defender-for-endpoint/

SC-200: Mitigate threats using Microsoft Defender for Cloud
https://learn.microsoft.com/en-us/training/paths/sc-200-mitigate-threats-using-azure-defender/

SC-200: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
https://learn.microsoft.com/en-us/training/paths/sc-200-utilize-kql-for-azure-sentinel/

SC-200: Configure your Microsoft Sentinel environment
https://learn.microsoft.com/en-us/training/paths/sc-200-configure-azure-sentinel-environment/

SC-200: Connect logs to Microsoft Sentinel
https://learn.microsoft.com/en-us/training/paths/sc-200-connect-logs-to-azure-sentinel/

SC-200: Create detections and perform investigations using Microsoft Sentinel
https://learn.microsoft.com/en-us/training/paths/sc-200-create-detections-perform-investigations-azure-sentinel/

SC-200: Perform threat hunting in Microsoft Sentinel
https://learn.microsoft.com/en-us/training/paths/sc-200-perform-threat-hunting-azure-sentinel/

Additional Training Resources

Microsoft Certification Poster
Become Microsoft Certified

ESI Azure Training Journey (microsoft.com)

Learn Live | Microsoft Learn

E-Books
Resource search results | Microsoft Azure

Ninja Training

Thursday, November 17, 2022 2:11 PM

Defender Ninja Training
Microsoft Defender for Cloud Apps Ninja Training | June 2022 - Microsoft Community Hub
Microsoft Defender for Identity Ninja Training - Microsoft Community Hub
Become a Microsoft Defender for Endpoint Ninja - Microsoft Community Hub

Microsoft Cloud App Security
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/the-microsoft-cloud-app-security-mcas-ninja-training-march-2021/ba-p/1877343

Complete Sentinel Ninja Level 400 training
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-ninja-the-complete-level-400/ba-p/1246310

Service Mappings

Tuesday, December 13, 2022 12:31 PM

Azure AD	Cloud management. Houses tenants. B2C, B2B. Azure AD Connect. Supports SCIM.
PHS	Hash of a hash. Authentication occurs in the cloud. Password writeback keeps password changes synced Device writeback enabled conditional access in AD FS.
PTA	Authentication occurs on-premises. Requires authentication agent(s) on premises. Use when password policies, and sign-in hours are required.
Federation	Requires federated proxy server and federation servers. Required when using Smart cards.
Identity Protection	Leaked Credentials
Identity Governance aka Entra	PIM, Privileged Access Lifecycle. P2 license
Defender for Endpoint	DLP, Endpoint protection. Live response.
Defender for Cloud	Cloud Security Posture Management. Azure, AWS and GCP. Secure Score, recommendations, vulnerability assessments, file integri ty monitoring.
Defender for Office 365	Phishing, training
Defender for IoT	Manage IoT resources. Asset discovery, threat detection and response. Agent or network sensor.
Defender for MS 365	Detection, prevention, investigation and response across email, endpoints, identities and applications.
Defender for Identity	Lateral movement, User Behavior and Activities. Used for on-prem, requires sensors.
Microsoft Purview	Govern, protect, manage data. Classification. Identify sensitive data i.e. credit card. Locates sensitive data. eDiscovery=Pr emium sku
Azure Sphere	IoT. Secure MCU, Linux OS.
Intune	Onboard devices can be used in conjunction with Configuration manager.
Configuration Manager	Onboard devices can be used in conjunction with Intune.
Azure AD App Proxy	Secure remotes access to on-prem web apps.
Azure Sentinel	SIEM/SOAR. Pulls from log analytics. Has connectors to various stores. Uses KQL for hunting, etc. Recommendations, workbooks, playbooks.
Azure ARC	Manage resources on-premises via Azure.
Azure Stack	Extends Azure services to other environments and remote locations.
Azure Lighthouse	Cross-tenant management.
Azure Bastion	Secure RDP to vms in Azure. Removes the requirement for public IP on the vms.
Azure Firewall	L3-L7 filtering and threat intelligence feeds. Known malicious Ips and FQDNs. Premium sku includes TLS filtering, IDPS, URL filt ering. Traffic is denied by default.
Network Security Groups	Allows deny traffic to subnet and/or network interface.
Private Endpoint	Connect to an Azure resource directly from vnet. Uses a private IP. Services include Azure Storage, Cosmos DB, SQL DB. Requir es a Private Link.
DDOS Protection	Infrastructure protection already enabled. Enhanced protection requires Azure DDoS Protection Plan $$
Azure Key Vault	Keys, secrets and certificates. Management plane = manage key vault, Data plane = manage data in the key vault.
Azure Automation Update Management	Patch management. Scheduling and managing updates.
Azure Blueprints	ARM Templates, Policies, Resource Groups, Role Assignments. Automated environment setup.
Desired State Configuration	Configuration of guest OS.
Azure Policy	Enforcing and auditing of the environment. IE location of resources, enforcing Tags, applying compliance requirements.
Virtual Machine	Secure using Azure Disk Encryption Linux=DmCrypt, Windows=Bitlocker. Backup vms. Use JIT. Protect using Defender for Cloud. U se File Integrity monitoring.
Storage	Use HTTPs over HTTP, enable Secure Transfer required. Limit access to SAS tokens. Regenerate keys (MS managed or customer man aged). Uses Server Side Encryption (SSE) by default, can't be turned off.
JIT	Allow access via a port. Can time restrict and/or restrict to ip range.
Information Rights Management	Control what can be done to data. IE restrict copy, print, forward.

Logic Apps Links

Thursday, January 19, 2023 11:20 AM

Overview - Azure Logic Apps | Microsoft Learn

Training
Build automated workflows to integrate data and apps with Azure Logic Apps - Training | Microsoft Learn

Study Guide - July 2023

Tuesday, July 25, 2023 3:36 PM

Candidates should be familiar with Microsoft 365, Azure cloud services, and Windows and Linux operating systems.

- Mitigate threats by using Microsoft 365 Defender (25–30%)
- Mitigate threats by using Defender for Cloud (15–20%)
- Mitigate threats by using Microsoft Sentinel (50–55%)

Mitigate threats by using Microsoft 365 Defender (25–30%)

Mitigate threats to the Microsoft 365 environment by using Microsoft 365 Defender

- Investigate, respond, and remediate threats to Microsoft Teams, SharePoint Online, and OneDrive
- Investigate, respond, and remediate threats to email by using Microsoft Defender for Office 365
- Investigate and respond to alerts generated from data loss prevention (DLP) policies
- Investigate and respond to alerts generated from insider risk policies
- Discover and manage apps by using Microsoft Defender for Cloud Apps
- Identify, investigate, and remediate security risks by using Defender for Cloud Apps

Mitigate endpoint threats by using Microsoft Defender for Endpoint

- Manage data retention, alert notification, and advanced features
- Recommend attack surface reduction (ASR) for devices
- Respond to incidents and alerts
- Configure and manage device groups
- Identify devices at risk by using the Microsoft Defender Vulnerability Management
- Manage endpoint threat indicators
- Identify unmanaged devices by using device discovery

Mitigate identity threats

- Mitigate security risks related to events for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Mitigate security risks related to Azure AD Identity Protection events
- Mitigate security risks related to Active Directory Domain Services (AD DS) by using Microsoft Defender for Identity

Manage extended detection and response (XDR) in Microsoft 365 Defender

- Manage incidents and automated investigations in the Microsoft 365 Defender portal
- Manage actions and submissions in the Microsoft 365 Defender portal
- Identify threats by using KQL
- Identify and remediate security risks by using Microsoft Secure Score
- Analyze threat analytics in the Microsoft 365 Defender portal
- Configure and manage custom detections and alerts

Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview

- Perform threat hunting by using UnifiedAuditLog
- Perform threat hunting by using Content Search

Mitigate threats by using Defender for Cloud (15–20%)

Implement and maintain cloud security posture management

- Assign and manage regulatory compliance policies, including Microsoft cloud security benchmark (MCSB)
- Improve the Defender for Cloud secure score by remediating recommendations
- Configure plans and agents for Microsoft Defender for Servers
- Configure and manage Microsoft Defender for DevOps

Configure environment settings in Defender for Cloud

- Plan and configure Defender for Cloud settings, including selecting target subscriptions and workspaces
- Configure Defender for Cloud roles
- Assess and recommend cloud workload protection
- Enable Microsoft Defender plans for Defender for Cloud
- Configure automated onboarding for Azure resources
- Connect compute resources by using Azure Arc
- Connect multicloud resources by using Environment settings

Respond to alerts and incidents in Defender for Cloud

- Set up email notifications
- Create and manage alert suppression rules
- Design and configure workflow automation in Defender for Cloud
- Remediate alerts and incidents by using Defender for Cloud recommendations
- Manage security alerts and incidents
- Analyze Defender for Cloud threat intelligence reports

Mitigate threats by using Microsoft Sentinel (50–55%)

Design and configure a Microsoft Sentinel workspace

- Plan a Microsoft Sentinel workspace
- Configure Microsoft Sentinel roles
- Design and configure Microsoft Sentinel data storage, including log types and log retention

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentinel

- Identify data sources to be ingested for Microsoft Sentinel
- Configure and use Microsoft Sentinel connectors for Azure resources, including Azure Policy and diagnostic settings
- Configure Microsoft Sentinel connectors for Microsoft 365 Defender and Defender for Cloud
- Design and configure Syslog and Common Event Format (CEF) event collections
- Design and configure Windows security event collections
- Configure threat intelligence connectors
- Create custom log tables in the workspace to store ingested data

Manage Microsoft Sentinel analytics rules

- Configure the Fusion rule
- Configure Microsoft security analytics rules
- Configure built-in scheduled query rules
- Configure custom scheduled query rules
- Configure near-real-time (NRT) query rules
- Manage analytics rules from Content hub
- Manage and use watchlists
- Manage and use threat indicators

Perform data classification and normalization

- Classify and analyze data by using entities
- Query Microsoft Sentinel data by using Advanced Security Information Model (ASIM) parsers
- Develop and manage ASIM parsers

Configure security orchestration automated response (SOAR) in Microsoft Sentinel

- Create and configure automation rules
- Create and configure Microsoft Sentinel playbooks

- Configure analytic rules to trigger automation rules
- Trigger playbooks manually from alerts and incidents

Manage Microsoft Sentinel incidents

- Create an incident
- Triage incidents in Microsoft Sentinel
- Investigate incidents in Microsoft Sentinel
- Respond to incidents in Microsoft Sentinel
- Investigate multi-workspace incidents

Use Microsoft Sentinel workbooks to analyze and interpret data

- Activate and customize Microsoft Sentinel workbook templates
- Create custom workbooks
- Configure advanced visualizations

Hunt for threats by using Microsoft Sentinel

- Analyze attack vector coverage by using MITRE ATT&CK in Microsoft Sentinel
- Customize content gallery hunting queries
- Create custom 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

Manage threats by using entity behavior analytics

- Configure entity behavior settings
- Investigate threats by using entity pages
- Configure anomaly detection analytics rules

From <https://learn.microsoft.com/en-us/certifications/resources/study-guides/SC-200>

Security Copilot

Thursday, March 21, 2024 3:24 PM

Microsoft Security Copilot in advanced hunting | Microsoft Learn
Microsoft Security Copilot in Microsoft Defender XDR | Microsoft Learn

Kusto Query Language (KQL) plugins in Microsoft Security Copilot | Microsoft Learn

Configure settings in Microsoft Defender XDR

Thursday, March 21, 2024 12:52 PM

- Configure a connection from Defender XDR to a Sentinel workspace
  - Connect Microsoft Sentinel to Microsoft Defender XDR (preview) | Microsoft Learn
-
- Configure alert and vulnerability notification rules
  - Configure vulnerability email notifications in Microsoft Defender for Endpoint | Microsoft Learn

- Configure Microsoft Defender for Endpoint advanced features
  - Configure advanced features in Microsoft Defender for Endpoint | Microsoft Learn

- Configure endpoint rules settings, including indicators and web content filtering
  Attack surface reduction rules reference | Microsoft Learn
  Web content filtering | Microsoft Learn

- Manage automated investigation and response capabilities in Microsoft Defender XDR
  - Automated investigation and response in Microsoft Defender XDR | Microsoft Learn

- Configure automatic attack disruption in Microsoft Defender XDR
  - Configure automatic attack disruption capabilities in Microsoft Defender XDR | Microsoft Learn

Manage assets and environments

Thursday, March 21, 2024 12:54 PM

- Configure and manage device groups, permissions, and automation levels in Microsoft Defender for Endpoint
  - Create and manage device groups in Microsoft Defender for Endpoint | Microsoft Learn
    Use automated investigations to investigate and remediate threats | Microsoft Learn
    Assign user access | Microsoft Learn
    Create and manage roles for role-based access control | Microsoft Learn

- Identify and remediate unmanaged devices in Microsoft Defender for Endpoint
  - Unmanaged device protection capabilities are now generally available (microsoft.com)

- Manage resources by using Azure Arc
  - Azure Arc overview - Azure Arc | Microsoft Learn

- Connect environments to Microsoft Defender for Cloud (by using multi-cloud account management)
  - The Defender for Cloud multicloud solution - Microsoft Defender for Cloud | Microsoft Learn

- Discover and remediate unprotected resources by using Defender for Cloud
  - Remediate security recommendations in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

- Identify and remediate devices at risk by using Microsoft Defender Vulnerability Management
  - Microsoft Defender Vulnerability Management | Microsoft Learn

Design and configure a Microsoft Sentinel workspace

Thursday, March 21, 2024 12:54 PM

- Plan a Microsoft Sentinel workspace
  - Design your Microsoft Sentinel workspace architecture | Microsoft Learn
- Configure Microsoft Sentinel roles
  - Roles and permissions in Microsoft Sentinel | Microsoft Learn
- Specify Azure RBAC roles for Microsoft Sentinel configuration
  - Roles and permissions in Microsoft Sentinel | Microsoft Learn

  Azure Sentinel Notebook on GitHub includes tutorials and examples
  Azure/Azure-Sentinel-Notebooks: Interactive Azure Sentinel Notebooks provides security insights and actions to investigate anomalies and hunt for malicious behaviors. (github.com)

  Pricing: Plan costs, understand Microsoft Sentinel pricing and billing | Microsoft Learn
- Design and configure Microsoft Sentinel data storage, including log types and log retention
  - Geographical availability and data residency in Microsoft Sentinel | Microsoft Learn
- Manage multiple workspaces by using Workspace manager and Azure Lighthouse
  - Manage multiple Microsoft Sentinel workspaces with workspace manager | Microsoft Learn

Azure Sentinel Notebook on GitHub includes tutorials and examples
Azure/Azure-Sentinel-Notebooks: Interactive Azure Sentinel Notebooks provides security insights and actions to investigate anomalies and hunt for malicious behaviors. (github.com)

Pricing: Plan costs, understand Microsoft Sentinel pricing and billing | Microsoft Learn

Ingest data sources in Microsoft Sentinel

Thursday, March 21, 2024 12:55 PM

- Identify data sources to be ingested for Microsoft Sentinel
  - Microsoft Sentinel data connectors | Microsoft Learn
  - Best practices for data collection in Microsoft Sentinel | Microsoft Learn

- Implement and use Content hub solutions
  - About Microsoft Sentinel content and solutions | Microsoft Learn

- Configure and use Microsoft connectors for Azure resources, including Azure Policy and diagnostic settings
  - Connect Microsoft Sentinel to Azure, Windows, and Microsoft services | Microsoft Learn
  - Connect Microsoft Sentinel to other Microsoft services by using diagnostic settings-based connections | Microsoft Learn

- Configure bidirectional synchronization between Microsoft Sentinel and Microsoft Defender XDR
  - Connect Microsoft Sentinel to Microsoft Defender XDR (preview) | Microsoft Learn

- Plan and configure Syslog and Common Event Format (CEF) event collections
  - Ingest Syslog and CEF messages to Microsoft Sentinel with the Azure Monitor Agent | Microsoft Learn

- Plan and configure collection of Windows Security events by using data collection rules, including Windows Event Forwarding (WEF)
  - Windows Events, how to collect them in Sentinel and which way is preferred to detect Incidents. (microsoft.com)

- Configure threat intelligence connectors, including platform, TAXII, upload indicators API, and MISP
  - Connect Microsoft Sentinel to STIX/TAXII threat intelligence feeds | Microsoft Learn

- Create custom log tables in the workspace to store ingested data
  - Collect data in custom log formats to Microsoft Sentinel | Microsoft Learn

Configure protections in Microsoft Defender security technologies

Thursday, March 21, 2024 12:53 PM

- Configure policies for Microsoft Defender for Cloud Apps
  - Control cloud apps with policies - Microsoft Defender for Cloud Apps | Microsoft Learn

- Configure policies for Microsoft Defender for Office
  - Configure anti-phishing policies in Microsoft Defender for Office 365 | Microsoft Learn

- Configure security policies for Microsoft Defender for Endpoints, including attack surface reduction (ASR) rules
  - Enable attack surface reduction rules | Microsoft Learn
-
- Configure cloud workload protections in Microsoft Defender for Cloud
  - Review workload protection in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

Configure detection in Microsoft Defender XDR

Thursday, March 21, 2024 12:55 PM

- Configure and manage custom detections
  - Create and manage custom detection rules in Microsoft Defender XDR | Microsoft Learn
- Configure alert tuning
  - Boost your detection and response workflows with alert tuning (microsoft.com)
- Configure deception rules in Microsoft Defender XDR
  - Configure the deception capability in Microsoft Defender XDR | Microsoft Learn

Configure detections in Microsoft Sentinel

Thursday, March 21, 2024 12:55 PM

- Classify and analyze data by using entities
  - Use entities to classify and analyze data in Microsoft Sentinel | Microsoft Learn
- Configure scheduled query rules, including KQL
  - Monitor and optimize the execution of your Microsoft Sentinel scheduled analytics rules | Microsoft Learn
- Configure near-real-time (NRT) query rules, including KQL
  - Detect threats quickly with near-real-time (NRT) analytics rules in Microsoft Sentinel | Microsoft Learn
- Manage analytics rules from Content hub
- Configure anomaly detection analytics rules
  - Work with anomaly detection analytics rules in Microsoft Sentinel | Microsoft Learn
- Configure the Fusion rule
  - Advanced multistage attack detection in Microsoft Sentinel | Microsoft Learn
- Query Microsoft Sentinel data by using ASIM parsers
  - Use Advanced Security Information Model (ASIM) parsers | Microsoft Learn
- Manage and use threat indicators
  - Work with threat indicators in Microsoft Sentinel | Microsoft Learn

Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel | Microsoft Learn

Respond to alerts and incidents in Microsoft Defender XDR

Thursday, March 21, 2024 12:56 PM

- Investigate and remediate threats to Microsoft Teams, SharePoint Online, and OneDrive
  - Remediation actions in Microsoft Defender for Office 365 | Microsoft Learn
-
- Investigate and remediate threats in email by using Microsoft Defender for Office
  - Investigate malicious email that was delivered in Microsoft 365, find and investigate malicious email | Microsoft Learn
-
- Investigate and remediate ransomware and business email compromise incidents identified by
- automatic attack disruption
  - Automatic attack disruption in Microsoft Defender XDR | Microsoft Learn
-
- Investigate and remediate compromised entities identified by Microsoft Purview data loss prevention (DLP) policies
  - Learn about investigating data loss prevention alerts | Microsoft Learn
  - Learn about data loss prevention | Microsoft Learn
- Investigate and remediate threats identified by Microsoft Purview insider risk policies
  - Learn about insider risk management | Microsoft Learn
  - Investigate insider risk management activities | Microsoft Learn
- Investigate and remediate alerts and incidents identified by Microsoft Defender for Cloud
  - Manage and respond to security alerts - Microsoft Defender for Cloud | Microsoft Learn
-
- Investigate and remediate security risks identified by Microsoft Defender for Cloud Apps
  - Investigate cloud app risks and suspicious activity - Microsoft Defender for Cloud Apps | Microsoft Learn
-
- Investigate and remediate compromised identities in Microsoft Entra ID
  - Remediate risks and unblock users in Microsoft Entra ID Protection - Microsoft Entra ID Protection | Microsoft Learn
  - Investigate risk Microsoft Entra ID Protection - Microsoft Entra ID Protection | Microsoft Learn
-
- Investigate and remediate security alerts from Microsoft Defender for Identity
  - Microsoft Defender for Identity security alerts in Microsoft Defender XDR - Microsoft Defender for Identity | Microsoft Learn
-
- Manage actions and submissions in the Microsoft Defender portal
  - Go to the Action center to view and approve your automated investigation and remediation tasks | Microsoft Learn

Respond to alerts and incidents identified by Microsoft Defender for Endpoint

Thursday, March 21, 2024 12:56 PM

- Investigate timeline of compromised devices
  - Microsoft Defender for Endpoint device timeline | Microsoft Learn

- Perform actions on the device, including live response and collecting investigation packages
  - Take response actions on a device in Microsoft Defender for Endpoint | Microsoft Learn

- Perform evidence and entity investigation
  - Perform evidence and entities investigations using Microsoft Defender for Endpoint - Training | Microsoft Learn

Enrich investigations by using other Microsoft tools

Thursday, March 21, 2024 12:57 PM

- Investigate threats by using unified audit Log
  - Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard - Training | Microsoft Learn
  - Learn about auditing solutions in Microsoft Purview | Microsoft Learn

- Investigate threats by using Content Search
  - Get started with Content search | Microsoft Learn

- Perform threat hunting by using Microsoft Graph activity logs
  - Access Microsoft Graph activity logs (preview) - Microsoft Graph | Microsoft Learn
  - Use the Microsoft Graph API for security threat detection and protection (preview) - Microsoft Graph beta | Microsoft Learn

Manage incidents in Microsoft Sentinel

Thursday, March 21, 2024 12:57 PM

- Triage incidents in Microsoft Sentinel
  - Navigate and investigate incidents in Microsoft Sentinel | Microsoft Learn
- Investigate incidents in Microsoft Sentinel
  - Navigate and investigate incidents in Microsoft Sentinel | Microsoft Learn
- Respond to incidents in Microsoft Sentinel
  - Use tasks to manage incidents in Microsoft Sentinel | Microsoft Learn

Configure security orchestration, automation, and response (SOAR) in Microsoft Sentinel

Thursday, March 21, 2024 12:57 PM

- Create and configure automation rules
  Introduction to automation in Microsoft Sentinel | Microsoft Learn
- Create and configure Microsoft Sentinel playbooks
  - Create and customize Microsoft Sentinel playbooks from templates | Microsoft Learn
  - Create and perform incident tasks in Microsoft Sentinel using playbooks | Microsoft Learn
- Configure analytic rules to trigger automation
  - Automate threat response in Microsoft Sentinel with automation rules | Microsoft Learn
- Trigger playbooks manually from alerts and incidents
  - Use triggers and actions in Microsoft Sentinel playbooks | Microsoft Learn
- Run playbooks on On-premises resources

Hunt for threats by using KQL

Thursday, March 21, 2024 12:53 PM

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

Microsoft Security Copilot in advanced hunting | Microsoft Learn

Hunt for threats by using Microsoft Sentinel

Thursday, March 21, 2024 1:44 PM

- Analyze attack vector coverage by using the MITRE ATT&CK in Microsoft Sentinel
  - View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn
- Customize content gallery hunting queries
  - Hunting capabilities in Microsoft Sentinel | Microsoft Learn
- Use hunting bookmarks for data investigations
  - Use hunting bookmarks for data investigations in Microsoft Sentinel | Microsoft Learn
- Monitor hunting queries by using Livestream
  - Use hunting Livestream in Microsoft Sentinel to detect threats | Microsoft Learn
- Retrieve and manage archived log data
  - Restore archived logs from search - Microsoft Sentinel | Microsoft Learn
- Create and manage search jobs
  - Search across long time spans in large datasets - Microsoft Sentinel | Microsoft Learn

MSTICPy and Jupyter Notebooks in Azure Sentinel, an update - Microsoft Community Hub
Notebooks with Kqlmagic (Kusto Query Language) in Azure Data Studio - Azure Data Studio | Microsoft Learn

Azure-Sentinel-Notebooks/Sample-Notebooks at 8122bca32387d60a8ee9c058ead9d3ab8f4d61e6 · Azure/Azure-Sentinel-Notebooks (github.com)

Identify advanced threats and with UEBA
https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

Roles and permissions in Microsoft Sentinel | Microsoft Learn

I'm Being Attacked, Now What? - Microsoft Community Hub

Analyze and interpret data by using workbooks

Thursday, March 21, 2024 1:44 PM

- Activate and customize Microsoft Sentinel workbook templates
  - Visualize your data using workbooks in Microsoft Sentinel | Microsoft Learn

- Create custom workbooks that include KQL
  Get Hands-On KQL Practice with this Microsoft Sentinel Workbook - Microsoft Community Hub

- Configure visualizations
  - Visualize collected data | Microsoft Learn

Guided Demos

Wednesday, October 26, 2022 11:52 AM

Video: Microsoft Defender for Endpoint – Advanced hunting

https://www.microsoft.com/en-us/videoplayer/embed/RE4bGqo

Video: Incident Investigation

https://www.microsoft.com/en-us/videoplayer/embed/RE4qLUV?rel=0&postJsllMsg=true

Microsoft Defender for Endpoint – Onboarding clients

https://www.microsoft.com/en-us/videoplayer/embed/RE4bGqr?rel=0&postJsllMsg=true

Role-based access control – Microsoft Defender for Endpoint

https://www.microsoft.com/en-us/videoplayer/embed/RE4bJ2a?rel=0&postJsllMsg=true

Attack surface reduction – Microsoft Defender for Endpoint

https://www.microsoft.com/en-us/videoplayer/embed/RE4woug?postJsllMsg=true

Microsoft Defender for Endpoint: EDR in block mode

https://www.microsoft.com/en-us/videoplayer/embed/RE4HjW2?rel=0&postJsllMsg=true

Assess and Onboard Unmanaged Devices

https://www.microsoft.com/en-us/videoplayer/embed/RE4RwQz?postJsllMsg=true

Discover Devices

https://www.youtube.com/watch?v=TCDxICrZQa8

Microsoft Defender for Endpoint: Live response

https://www.microsoft.com/en-us/videoplayer/embed/RE4qLUW?rel=0&postJsllMsg=true

Microsoft Defender for Endpoint: Deep analysis

https://www.microsoft.com/en-us/videoplayer/embed/RE4aAYy?rel=0&postJsllMsg=true

Microsoft Defender for Endpoint: Conditional access

https://www.microsoft.com/en-us/videoplayer/embed/RE4byD1?rel=0&postJsllMsg=true

Microsoft Defender for Endpoint: Unified IoCs

https://www.microsoft.com/en-us/videoplayer/embed/RE4qLVw?rel=0&postJsllMsg=true

Video: Threat and vulnerability management: discovery & remediation

https://www.microsoft.com/videoplayer/embed/RE4qLVs?rel=0

Interactive Guide: Threat and Vulnerability Management

https://aka.ms/MSDE_TVM_IG

Microsoft Defender for Cloud Apps

https://www.microsoft.com/en-us/videoplayer/embed/RE4CMYG?postJsllMsg=true

Purview Insider Risks
Microsoft Purview Insider Risk Management (cloudguides.com)

Detect and respond to modern attacks with unified SIEM and XDR capabilities

https://aka.ms/AzureSentinel_SOC_InteractiveGuide

Discover Devices

https://www.youtube.com/watch?v=TCDxICrZQa8

Assess and Onboard Unmanaged Devices

https://www.microsoft.com/en-us/videoplayer/embed/RE4RwQz?postJsllMsg=true