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

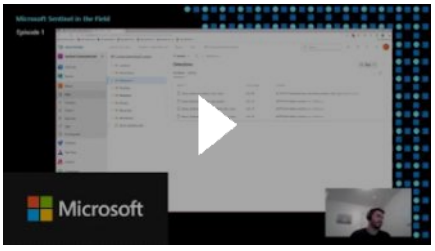
Microsoft Cybersecurity Reference Architectures
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

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

KQL Resources

Tuesday, October 25, 2022 2:02 PM

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

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

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

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

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>

Mitigate threats to the productivity environment by using Microsoft 365 Defender

Tuesday, October 25, 2022 10:42 AM

Investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive
Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams - Office 365 | Microsoft Learn

• Investigate, respond, and remediate threats to email by using Microsoft Defender for Office 365
Microsoft Defender for Office 365 - Office 365 | Microsoft Learn
Plans - Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

• Investigate and respond to alerts generated from Data Loss Prevention policies
Investigate data loss incidents with Microsoft 365 Defender | Microsoft Learn

• Investigate and respond to alerts generated from insider risk policies
Insider risk management settings - Microsoft Purview (compliance) | Microsoft Learn

- Discover and manage apps by using Microsoft Defender for Cloud Apps
What is Defender for Cloud Apps? | Microsoft Learn
Best practices for protecting your organization | Microsoft Learn

- Identify, investigate, and remediate security risks by using Defender for Cloud Apps
  - Defender for Cloud Apps anomaly detection alerts investigation guide | Microsoft Learn

Defense in depth security in Azure | Microsoft Learn

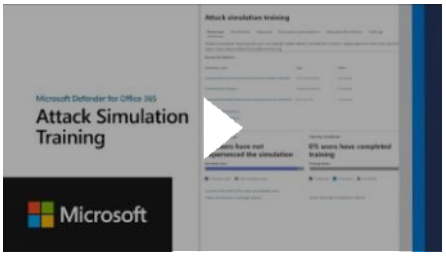
https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb

MS Defender for Cloud Apps Ops Guide :
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWYAzA

Overview - Advanced hunting | Microsoft Learn

Simulate a phishing attack with Attack simulation training | Microsoft Learn

Attack Simulation Training with Microsoft



Azure Arc | Microsoft Learn

Defender for Endpoint on Domain Controllers and restricting control
Microsoft Defender for Identity frequently asked questions
Architecture - Microsoft Defender for Identity

Continuous access evaluation in Azure AD - Microsoft Entra | Microsoft Learn

Investigate risk Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

Succeeding with Secure Access Service Edge (SASE) - Events | Microsoft Learn

Microsoft collaborates with Tenable to support federal cybersecurity efforts | Microsoft Security Blog

Mitigate endpoint threats by using Microsoft Defender for Endpoint

Tuesday, October 25, 2022 10:44 AM

Microsoft Defender for Endpoint | Microsoft Learn

Compare Microsoft endpoint security plans | Microsoft Learn

Plan 1 Overview of Microsoft Defender for Endpoint Plan 1 | Microsoft Learn
Plan 2 Microsoft Defender for Endpoint | Microsoft Learn

Manage data retention, alert notification, and advanced features

Recommend attack surface reduction (ASR) for devices
- Attack surface reduction rules reference | Microsoft Learn

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/prevent-compromised-unmanaged-devices-from-moving-laterally-in/ba-p/3482134

https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=Microsoft%20Teams

• Respond to incidents and alerts
Security alerts and incidents in Microsoft Defender for Cloud | Microsoft Learn

- Configure and manage device groups
  Create and manage device groups in Microsoft Defender for Endpoint | Microsoft Learn

- Identify devices at risk by using the Microsoft Defender Vulnerability Management
  - Microsoft Defender Vulnerability Management | Microsoft Learn
  - Dashboard insights | Microsoft Learn
- Manage endpoint threat indicators
  - Manage indicators | Microsoft Learn
- Identify unmanaged devices by using device discovery
  - Device discovery overview | Microsoft Learn

Troubleshoot Microsoft Defender for Endpoint onboarding issues | Microsoft Learn

Compare Microsoft endpoint security plans | Microsoft Learn

Windows 7 - Microsoft Lifecycle | Microsoft Learn

Onboard previous versions of Windows on Microsoft Defender for Endpoint | Microsoft Learn

Get started with your Microsoft Defender for Endpoint deployment | Microsoft Learn

Onboard devices and configure Microsoft Defender for Endpoint capabilities | Microsoft Learn

Offboard devices from the Microsoft Defender for Endpoint service | Microsoft Learn

• Manage automated investigations and remediations
Automation levels in automated investigation and remediation | Microsoft Learn
Review remediation actions following automated investigations | Microsoft Learn

• Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution

• Manage endpoint threat indicators
Create indicators | Microsoft Learn

• Recommend security baselines for devices
Settings list for the Microsoft Defender for Endpoint security baseline in Microsoft Intune - Microsoft Intune | Microsoft Learn

Mitigate identity threats

Tuesday, October 25, 2022 10:44 AM

What is Azure Active Directory Identity Protection? - Microsoft Entra | Microsoft Learn

- Mitigate security risks related to Azure AD Identity Protection events

Risk policies - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn
Investigate risk Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn
Remediate risks and unblock users in Azure AD Identity Protection - Microsoft Entra | Microsoft Learn

- Mitigate risks related to Azure Active Directory events
  What is Microsoft Defender for Identity? - Microsoft Defender for Identity | Microsoft Learn

• Identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity
What is Microsoft Defender for Identity? | Microsoft Learn

• Identify and remediate security risks related to conditional access events
What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn
Common Conditional Access policies - Azure Active Directory - Microsoft Entra | Microsoft Learn

What is Privileged Identity Management? - Microsoft Entra ID Governance | Microsoft Learn

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

Tuesday, October 25, 2022 10:44 AM

Manage incidents and automated investigations across Microsoft 365 Defender portal
What is Microsoft 365 Defender? | Microsoft Learn

• Manage investigation and remediation actions in the Action Center
Investigate and respond with Microsoft 365 Defender | Microsoft Learn
Investigate incidents in Microsoft 365 Defender | Microsoft Learn

- Identify threats by using KQL

Overview - Advanced hunting | Microsoft Learn
Learn the advanced hunting query language in Microsoft 365 Defender | Microsoft Learn

• Identify and remediate security risks using Microsoft Secure Score
Microsoft Secure Score | Microsoft Learn

• Analyze threat analytics in the Microsoft 365 Defender Portal
Threat analytics in Microsoft 365 Defender | Microsoft Learn

• Configure and manage custom detections and alerts
Create and manage custom detection rules in Microsoft 365 Defender | Microsoft Learn

Report spam, non-spam, phishing, suspicious emails and files to Microsoft | Microsoft Learn

Admin review for user reported messages | Microsoft Learn

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

Tuesday, July 25, 2023 4:07 PM

- Perform threat hunting by using UnifiedAuditLog
  - Audit log activities | Microsoft Learn

- Perform threat hunting by using Content Search
  - Investigate threats with Content search in Microsoft Purview - Training | Microsoft Learn
  - Get started with Content search | Microsoft Learn

Guided Demos

Wednesday, October 26, 2022 11:52 AM

Mitigate threats using Microsoft Defender for Endpoint

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)

Implement and maintain cloud security posture management

Tuesday, July 25, 2023 4:18 PM

- Assign and manage regulatory compliance policies, including Microsoft cloud security benchmark (MCSB)
  - Overview of the Microsoft cloud security benchmark | Microsoft Learn

- Improve the Defender for Cloud secure score by remediating recommendations
  - Reference table for all recommendations - Microsoft Defender for Cloud | Microsoft Learn
  - Improving your security posture with recommendations - Microsoft Defender for Cloud | Microsoft Learn
  - Implement security recommendations - Microsoft Defender for Cloud | Microsoft Learn

- Configure plans and agents for Microsoft Defender for Servers
  - Protect your servers with Defender for Servers - Microsoft Defender for Cloud | Microsoft Learn

- Configure and manage Microsoft Defender for DevOps
  - Microsoft Defender for DevOps - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

Configure environment settings in Defender for Cloud

Tuesday, October 25, 2022 10:45 AM

What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn

Plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspaces
Organize subscriptions into management groups and assign roles to users for Microsoft Defender for Cloud | Microsoft Learn
Grant and request tenant-wide permissions in Microsoft Defender for Cloud | Microsoft Learn
Onboard a management group to Microsoft Defender for Cloud | Microsoft Learn

Defender for Cloud Planning and Operations Guide | Microsoft Learn
Access & application controls tutorial - Microsoft Defender for Cloud | Microsoft Learn

• Configure Microsoft Defender for Cloud roles
User roles and permissions - Microsoft Defender for Cloud | Microsoft Learn

• Assess and recommend cloud workload protection
Security alerts and incidents in Microsoft Defender for Cloud | Microsoft Learn
Agentless scanning of cloud machines using Microsoft Defender for Cloud | Microsoft Learn

- Enable Microsoft Defender plans for Defender for Cloud
  - Protect your resources with Defender CSPM plan on your subscription - Microsoft Defender for Cloud | Microsoft Learn
- Configure automated onboarding for Azure resources
  - Connect your Azure subscriptions - Microsoft Defender for Cloud | Microsoft Learn
- Connect compute resources by using Azure Arc
  - Connect on-premises machines - Microsoft Defender for Cloud | Microsoft Learn
- Connect multicloud resources by using Environment settings
  - Connect your AWS account to Microsoft Defender for Cloud | Microsoft Learn
  - Connect your non-Azure machines to Microsoft Defender for Cloud | Microsoft Learn
  - Quickstart: Connect your GitHub repositories to Microsoft Defender for Cloud | Microsoft Learn
  - Connect your GCP project to Microsoft Defender for Cloud | Microsoft Learn
  - Quickstart: Connect your Azure DevOps repositories to Microsoft Defender for Cloud | Microsoft Learn

Permissions in Microsoft Defender for Cloud | Microsoft Learn

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide#at-service-onboarding

https://learn.microsoft.com/en-us/partner-center/gdap-introduction

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-roles-and-azure-ad-roles/ba-p/2363647

ASR https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide

https://learn.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use

Important changes coming to Microsoft Defender for Cloud | Microsoft Learn

What is Microsoft Intune | Microsoft Learn

Respond to alerts and incidents in Defender for Cloud

Tuesday, October 25, 2022 10:46 AM

• Set up email notifications
Configure email notifications for Microsoft Defender for Cloud alerts | Microsoft Learn

• Create and manage alert suppression rules
Using alerts suppression rules to suppress false positives or other unwanted security alerts in Microsoft Defender for Cloud | Microsoft Learn

• Design and configure workflow automation in Microsoft Defender for Cloud
Workflow automation in Microsoft Defender for Cloud | Microsoft Learn

• Remediate alerts and incidents by using Microsoft Defender for Cloud recommendations
Manage security incidents - Microsoft Defender for Cloud | Microsoft Learn

• Manage security alerts and incidents
Stream your alerts from Microsoft Defender for Cloud to Security Information and Event Management (SIEM) systems and other monitoring solutions | Microsoft Learn

• Analyze Microsoft Defender for Cloud threat intelligence reports
Microsoft Defender for Cloud threat intelligence report | Microsoft Learn

Older objectives for reference - Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud

Tuesday, October 25, 2022 10:45 AM

Identify data sources to be ingested for Microsoft Defender for Cloud
Overview of Microsoft Defender for Servers | Microsoft Learn
Container security with Microsoft Defender for Cloud | Microsoft Learn
Enable database protection for your subscription | Microsoft Learn
Microsoft Defender for App Service - the benefits and features | Microsoft Learn
Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn
Microsoft Defender for Key Vault - the benefits and features | Microsoft Learn
Microsoft Defender for Resource Manager - the benefits and features | Microsoft Learn
Microsoft Defender for DNS - the benefits and features | Microsoft Learn
Microsoft Defender for DevOps - the benefits and features | Microsoft Learn

• Configure automated onboarding for Azure resources

• Connect multi-cloud and on-premises resources
Connect your AWS account to Microsoft Defender for Cloud | Microsoft Learn
Connect your non-Azure machines to Microsoft Defender for Cloud | Microsoft Learn
Quickstart: Connect your GitHub repositories to Microsoft Defender for Cloud | Microsoft Learn
Connect your GCP project to Microsoft Defender for Cloud | Microsoft Learn
Quickstart: Connect your Azure DevOps repositories to Microsoft Defender for Cloud | Microsoft Learn

• Configure data collections
Overview of the extensions that collect data from your workloads | Microsoft Learn

How to evaluate Azure Arc-enabled servers with an Azure VM - Azure Arc | Microsoft Learn

https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/3-develop-integration-points-architecture

One pager listing agent required for specific workload in D4C
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-multicloud-security-determine-multicloud-dependencies#what-agent-do-i-need

https://learn.microsoft.com/en-us/azure/defender-for-cloud/exempt-resource#find-recommendations-with-exemptions-using-azure-resource-graph

Guided Demo

Wednesday, October 26, 2022 11:54 AM

Mitigate threats using Microsoft Defender for Cloud

Demo link: https://mslearn.cloudguides.com/guides/Protect%20your%20hybrid%20cloud%20with%20Azure%20Security%20Center

https://www.microsoft.com/videoplayer/embed/RE4bOeh?rel=0

Design and configure a Microsoft Sentinel workspace

Tuesday, October 25, 2022 10:46 AM

Best practices for Microsoft Sentinel | Microsoft Learn
Cloud feature availability for commercial and US Government customers | Microsoft Learn

Learning with the Microsoft Sentinel Training Lab - Microsoft Community Hub

Manage Microsoft Sentinel workspaces at scale - Azure Lighthouse | Microsoft Learn

Plan a Microsoft Sentinel workspace
Design your Microsoft Sentinel workspace architecture | Microsoft Learn
Manage access to Microsoft Sentinel data by resource | Microsoft Learn
Hybrid security monitoring with Microsoft Sentinel - Azure Architecture Center | Microsoft Learn
Manage Microsoft Sentinel workspaces at scale - Azure Lighthouse | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn

• Configure Microsoft Sentinel roles
Quickstart: Onboard in Microsoft Sentinel | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn

• Design and configure Microsoft Sentinel data storage, including log types and log retention
Microsoft Sentinel data connectors | Microsoft Learn
Use entities to classify and analyze data in Microsoft Sentinel | Microsoft Learn
Plan costs, understand Microsoft Sentinel pricing and billing | Microsoft Learn
Configure data retention for logs in Microsoft Sentinel or Azure Monitor | Microsoft Learn
When to use Basic Logs - Microsoft Sentinel | Microsoft Learn
•

Become a Microsoft Sentinel Ninja Become a Microsoft Sentinel Ninja: The complete level 400 training - Microsoft Community Hub

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

To archive a Log Analytics workspace in Microsoft Sentinel, you can use the Archive tier in Azure Monitor Logs. This tier allows you to retain data for up to seven years in a low-cost archived state. You can also use Azure Data Explorer for long-term retention of Microsoft Sentinel logs. Additionally, you can set fine-grained retention periods by using table-level retention settings.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/move-workspace-region
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/move-workspace

Migrate to the Azure Monitor agent (AMA) from the Log Analytics agent (MMA/OMS) for Microsoft Sentinel | Microsoft Learn

Monitor the health of your Microsoft Sentinel data connectors | Microsoft Learn
If you reconnect a Microsoft Sentinel data connector, it may cause duplicated data.To avoid duplicated data, you can disconnect the connector before reconnecting it. To disconnect the connector, you can use the Azure portal or the DISCONNECT API.

https://learn.microsoft.com/en-us/azure/architecture/example-scenario/data/sentinel-threat-intelligence

https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=commitment-tier

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?tabs=portal-1%2Cportal-2

https://learn.microsoft.com/en-us/azure/sentinel/basic-logs-use-cases

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

https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Event IDs Windows security event sets that can be sent to Microsoft Sentinel | Microsoft Learn
https://learn.microsoft.com/en-us/azure/sentinel/partner-integrations

Sentinel and CLI https://learn.microsoft.com/en-us/cli/azure/sentinel?view=azure-cli-latest

Lockheed Martin https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Extend Microsoft Sentinel across workspaces and tenants | Microsoft Learn

AZ-305: Design identity, governance, and monitor solutions - Training | Microsoft Learn

Comparing AWS and Azure regions and zones - Azure Architecture Center | Microsoft Learn

Integrate Azure Data Explorer for long-term log retention | Microsoft Learn
Analyze usage in a Log Analytics workspace in Azure Monitor - Azure Monitor | Microsoft Learn

Understand Microsoft Sentinel tables
Understand common tables
Understand Microsoft 365 Defender tables

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

Microsoft Sentinel Pricing | Microsoft Azure

Cyber Kill Chain® | Lockheed Martin

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

Tuesday, October 25, 2022 10:47 AM

Out-of-the-box (OOTB) content centralization changes - Microsoft Sentinel | Microsoft Learn

Migrate to the Azure Monitor agent (AMA) from the Log Analytics agent (MMA/OMS) for Microsoft Sentinel | Microsoft Learn

Identify data sources to be ingested for Microsoft Sentinel
Microsoft Sentinel data connectors | Microsoft Learn

Custom data ingestion and transformation in Microsoft Sentinel | Microsoft Learn

• Configure and use Microsoft Sentinel connectors for Azure resources, including Azure Policy and diagnostic settings
Connect Microsoft Sentinel to Azure, Windows, and Microsoft services | Microsoft Learn
Azure security baseline for Microsoft Sentinel | Microsoft Learn
Turn on auditing and health monitoring in Microsoft Sentinel | Microsoft Learn

Log Analytics agent overview - Azure Monitor | Microsoft Learn

Azure Monitor Agent overview - Azure Monitor | Microsoft Learn
Resources for creating Microsoft Sentinel custom connectors | Microsoft Learn

• Configure Microsoft Sentinel connectors for Microsoft 365 Defender and Microsoft Defender for Cloud
Microsoft 365 Defender integration with Microsoft Sentinel | Microsoft Learn
Microsoft Sentinel integration with Defender for Cloud Apps | Microsoft Learn

Ingest from Blob Storage
To ingest data from Azure Blob Storage into Microsoft Sentinel, you can use the Azure Blob Storage data connector. The Azure Blob Storage data connector allows you to stream and filter events from Azure Blob Storage logs.

• Design and configure Syslog and CEF event collections
Troubleshoot a connection between Microsoft Sentinel and a CEF or Syslog data connector | Microsoft Learn
Get CEF-formatted logs from your device or appliance into Microsoft Sentinel | Microsoft Learn
Connect Syslog data to Microsoft Sentinel | Microsoft Learn

Create a codeless connector for Microsoft Sentinel | Microsoft Learn

• Design and configure Windows Security event collections
Find your Microsoft Sentinel data connector | Microsoft Learn

Use Logstash to stream logs with pipeline transformations via DCR-based API | Microsoft Learn

- Configure threat intelligence connectors
  - Connect your threat intelligence platform to Microsoft Sentinel | Microsoft Learn
  - Understand threat intelligence in Microsoft Sentinel | Microsoft Learn
- Create custom log tables in the workspace to store ingested data

LightHouse
https://azure.microsoft.com/en-us/products/azure-lighthouse/#overview
https://learn.microsoft.com/en-us/azure/lighthouse/overview

Workspace Manager
Manage multiple Microsoft Sentinel workspaces with workspace manager | Microsoft Learn

To ingest tenant application logs, database, VM, and network logs to Log Analytics Workspace (LAW), you can use the Logs Ingestion API in Azure Monitor . This API allows you to send external data to a Log Analytics workspace with a REST API. You can create a custom table in a Log Analytics workspace and direct the data to the target table using a data collection rule (DCR)
Here are the steps required to configure the Logs ingestion API:

1. Create a Microsoft Entra application to authenticate against the API.

2. Create a data collection endpoint (DCE) to receive data.

3. Create a custom table in a Log Analytics workspace. This is the table you'll be sending data to. As part of this process, you will create a data collection rule (DCR) to direct the data to the target table.

4. Give the AD application access to the DCR.

5. Use sample code to send data to using the Logs ingestion API.

You can find a detailed tutorial on how to send data to Azure Monitor Logs with Logs ingestion API on the Azure portal . Additionally, you can also refer to the following resources for more information on ingesting logs to LAW:

Getting Started with Collecting and Managing Azure Logs.
https://betterstack.com/community/guides/logging/azure-logging/.

Azure Monitor logs with a multitenant app - Azure SQL Database. https://learn.microsoft.com/en-us/azure/azure-sql/database/saas-dbpertenant-log-analytics?view=azuresql.

Log data ingestion time in Azure Monitor - Azure Monitor. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-ingestion-time.

Manage Microsoft Sentinel analytics rules

Tuesday, October 25, 2022 10:47 AM

- Configure the Fusion Rule
  Advanced multistage attack detection in Microsoft Sentinel | Microsoft Learn

Configure Microsoft security analytics rules
Detect threats with built-in analytics rules in Microsoft Sentinel | Microsoft Learn

• Configure built-in scheduled query rules
Create custom analytics rules to detect threats with Microsoft Sentinel | Microsoft Learn

• Configure custom scheduled query rules
Create custom analytics rules to detect threats with Microsoft Sentinel | Microsoft Learn

• Manage and use watchlists
What is a watchlist - Microsoft Sentinel | Microsoft Learn
Build queries or rules with watchlists - Microsoft Sentinel | Microsoft Learn
Create watchlists - Microsoft Sentinel | Microsoft Learn

• Manage and use threat indicators
Work with threat indicators in Microsoft Sentinel | Microsoft Learn

More info on Content hub solutions and the GitHub repo Out-of-the-box (OOTB) content centralization changes - Microsoft Sentinel | Microsoft Learn

To build and publish Sentinel Solutions see Azure-Sentinel/Solutions at master · Azure/Azure-Sentinel (github.com)

Use entity behavior analytics to detect advanced threats | Microsoft Learn

briandelmsft/SentinelAutomationModules: The Microsoft Sentinel Triage AssistanT (STAT) enables easy to create incident triage automation in Microsoft Sentinel (github.com)

Sentinel Watchlist Automation Using Logic Apps - Microsoft Community Hub

Perform data classification and normalization

Tuesday, October 25, 2022 10:48 AM

Classify and analyze data by using entities
Microsoft Sentinel entity types reference | Microsoft Learn
azure-docs/entities.md at main · MicrosoftDocs/azure-docs (github.com)

• Query Microsoft Sentinel data by using Advanced SIEM Information Model (ASIM) parsers
Advanced Security Information Model (ASIM) schemas | Microsoft Learn
Normalization and the Advanced Security Information Model (ASIM) | Microsoft Learn

• Develop and manage ASIM parsers
Microsoft Sentinel Advanced Security Information Model (ASIM) parsers overview | Microsoft Learn

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-ingestion-time

Microsoft Sentinel migration: Select a target Azure platform to host exported data | Microsoft Learn

Azure-Sentinel/Parsers at master · Azure/Azure-Sentinel (github.com)

Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel

Tuesday, October 25, 2022 10:48 AM

Introduction to automation in Microsoft Sentinel | Microsoft Learn

Configure automation rules
Automate threat response in Microsoft Sentinel with automation rules | Microsoft Learn

• Create and configure Microsoft Sentinel playbooks
Automate threat response with playbooks in Microsoft Sentinel | Microsoft Learn

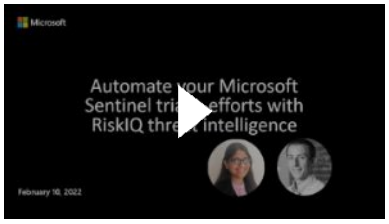
• Configure alerts and incidents to trigger automation
Automate threat response in Microsoft Sentinel with automation rules | Microsoft Learn

• Trigger playbooks manually from alerts and incidents
Use triggers and actions in Microsoft Sentinel playbooks | Microsoft Learn

Manage Microsoft Sentinel incidents

Tuesday, October 25, 2022 10:49 AM

- Create an incident
  - Create incidents from alerts in Microsoft Sentinel | Microsoft Learn
- Triage incidents in Microsoft Sentinel
  - Step 4. Respond to an incident using Microsoft Sentinel and Microsoft 365 Defender | Microsoft Learn
  - Automate Your Microsoft Sentinel Triage Efforts with RiskIQ Threat Intelligence



• Investigate incidents in Microsoft Sentinel
Investigate incidents with Microsoft Sentinel | Microsoft Learn

• Respond to incidents in Microsoft Sentinel
Relate alerts to incidents in Microsoft Sentinel | Microsoft Learn

• Investigate multi-workspace incidents
Work with Microsoft Sentinel incidents in many workspaces at once | Microsoft Learn
Extend Microsoft Sentinel across workspaces and tenants | Microsoft Learn

Use Advanced Security Information Model (ASIM) parsers | Microsoft Learn

Work with threat indicators
https://learn.microsoft.com/en-us/azure/sentinel/work-with-threat-indicators

Closing Incidents and Alerts
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/closing-an-incident-in-azure-sentinel-and-dismissing-an-alert-in/ba-p/1180208#:~:text=When%20I%20use%20Azure%20Security,the%20ASC%20Alert%20remains%20active.

Detect threats with built-in analytics rules in Microsoft Sentinel | Microsoft Learn

Deploy and monitor Azure Key Vault honeytokens with Microsoft Sentinel | Microsoft Learn

Overview - Azure Logic Apps | Microsoft Learn

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

Power Automate vs Logic Apps | Microsoft Learn

Playbooks

Microsoft Sentinel - Connectors | Microsoft Learn
https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks

Use Microsoft Sentinel workbooks to analyze and interpret data

Tuesday, October 25, 2022 10:49 AM

Activate and customize Microsoft Sentinel workbook templates
Commonly used Microsoft Sentinel workbooks | Microsoft Learn
Manage your SOC better with incident metrics in Microsoft Sentinel | Microsoft Learn

• Create custom workbooks
  Azure Sentinel Workbooks 101 (with sample Workbook) - Microsoft Community Hub

Configure advanced visualizations
  Visualize collected data | Microsoft Learn
Visualize your data using Azure Monitor Workbooks in Microsoft Sentinel | Microsoft Learn

Azure Workbooks - Save as PDF (Print) - Microsoft Community Hub

Commonly used Microsoft Sentinel workbooks | Microsoft Learn
microsoft/AzureMonitorCommunity: An open repo for Azure Monitor queries, workbooks, alerts and more (github.com)

Hunt for threats using Microsoft Sentinel

Tuesday, October 25, 2022 10:49 AM

Analyze attack vector coverage by using MITRE ATT&CK in Microsoft Sentinel
- View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn

Customize content gallery hunting queries
- Microsoft Sentinel content hub catalog | Microsoft Learn

Create custom hunting queries
Hunting capabilities in Microsoft Sentinel | Microsoft Learn

Monitor hunting queries by using Livestream
Manage hunting and livestream queries in Microsoft Sentinel using REST API | 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

Old objectives

• Configure and use MSTICPy in notebooks
Advanced configurations for Jupyter notebooks and MSTICPy in Microsoft Sentinel | Microsoft Learn
Get started with Jupyter notebooks and MSTICPy in Microsoft Sentinel | Microsoft Learn

• Perform hunting by using notebooks
Hunt for security threats with Jupyter notebooks - Microsoft Sentinel | Microsoft Learn

• Track query results with bookmarks

• Use hunting bookmarks for data investigations
Use hunting bookmarks for data investigations in Microsoft Sentinel | Microsoft Learn

• Convert a hunting query to an analytical rule

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)

RBAC
https://learn.microsoft.com/en-us/azure/sentinel/resource-context-rbac
https://learn.microsoft.com/en-us/azure/sentinel/roles

Azure Custom Roles
https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Data Collection Rules
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview

Azure Sentinel Workbooks
https://github.com/Azure/Azure-Sentinel/tree/master/Workbooks

Data normalization
https://learn.microsoft.com/en-us/azure/sentinel/normalization

Aggregating Insider Risk Management
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/aggregating-insider-risk-management-information-via-azure/ba-p/1743211

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

Azure Active Directory security operations guide - Microsoft Entra | Microsoft Learn

Manage threats by using entity behavior analytics

Tuesday, July 25, 2023 4:44 PM

- Configure entity behavior settings
  - Use entity behavior analytics to detect advanced threats | Microsoft Learn
- Investigate threats by using entity pages
  - Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel | Microsoft Learn
- Configure anomaly detection analytics rules
  - Work with anomaly detection analytics rules in Microsoft Sentinel | Microsoft Learn

Guided Demos

Wednesday, October 26, 2022 11:54 AM

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

Demo creating a DCR rule from the connector