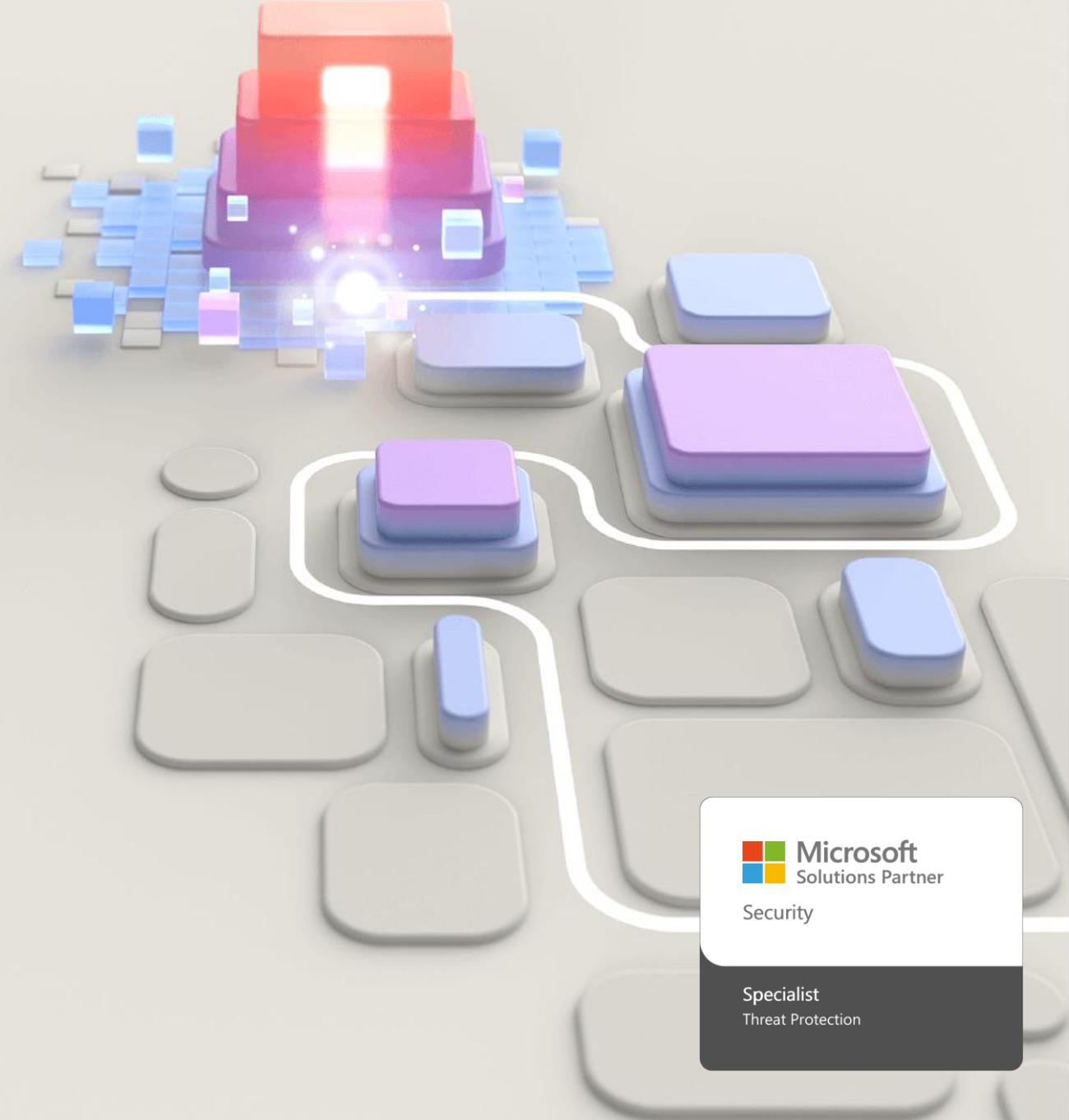




Swiss Post
Cybersecurity

Configure SIEM security operations using Microsoft Sentinel



Agenda



- Create and manage Microsoft Sentinel workspaces
- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel

Create and manage Microsoft Sentinel workspaces

Learning Objectives

After completing this module, you will be able to:

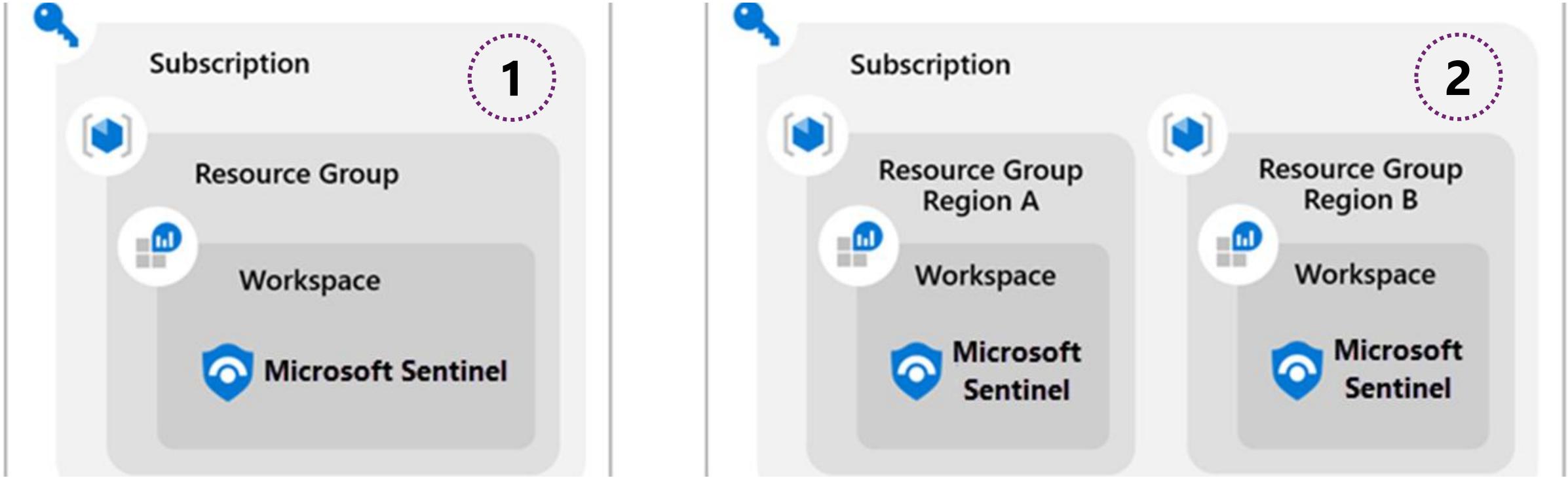
- 1** Describe Microsoft Sentinel workspace architecture
- 2** Install Microsoft Sentinel workspace
- 3** Manage a Microsoft Sentinel workspace



Introduction

- Deploying the Microsoft Sentinel environment involves designing a workspace configuration to meet your security and compliance requirements. The provisioning process includes creating a Log Analytics workspace and configuring the Microsoft Sentinel options.
- You're a Security Operations Analyst working at a company that is implementing Microsoft Sentinel. You're responsible for setting up the Microsoft Sentinel environment to meet the company requirement to minimize cost, meet compliance regulations, and provide the most manageable environment for your security team to perform their daily job responsibilities.
- You start by understanding the Microsoft Sentinel workspace's architecture. After you've decided on your workspace implementation options, you create your first Microsoft Sentinel workspace.

Plan for the Microsoft Sentinel workspace

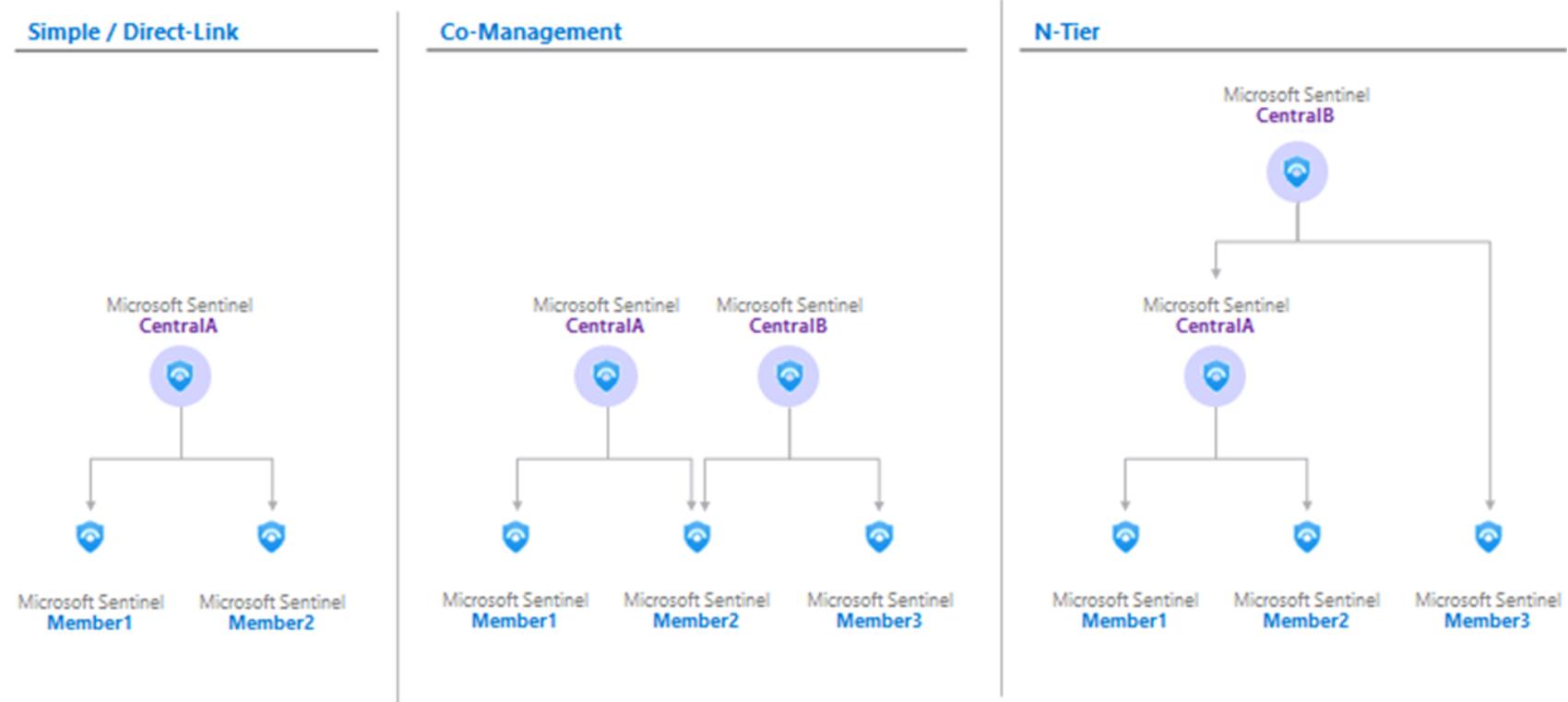


1. Single-Tenant with a single Microsoft Sentinel Workspace
2. Single-Tenant with regional Microsoft Sentinel Workspaces
3. Multi-Tenant – Sentinel Workspace manager or Azure Lighthouse (next slides)

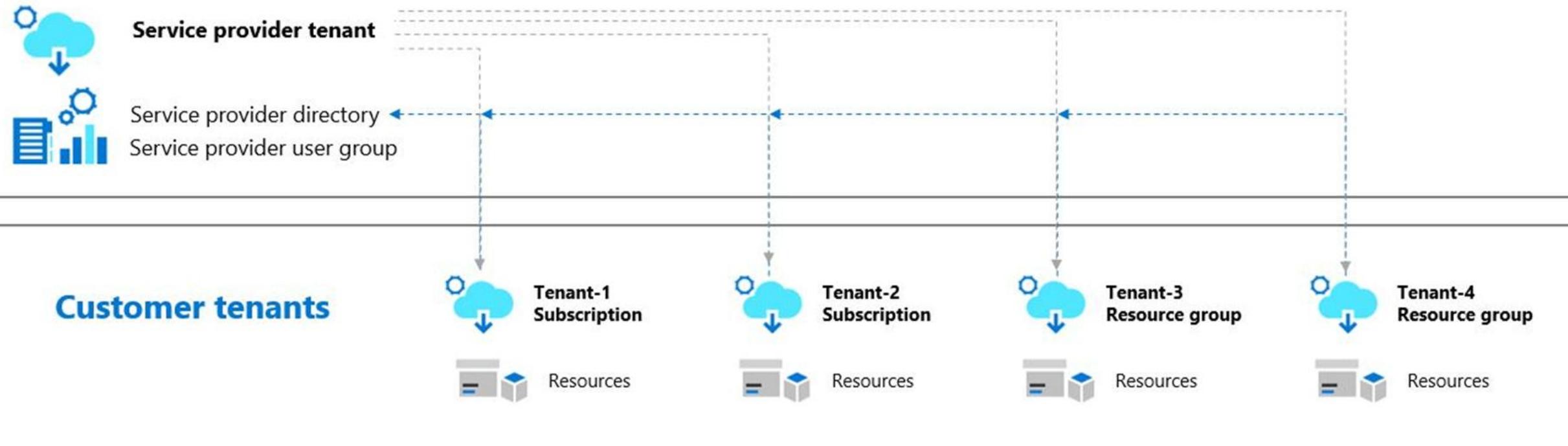
Centrally manage workspaces with Workspace manager

Microsoft Sentinel's Workspace manager enables users to centrally manage multiple Microsoft Sentinel workspaces within one or more Azure tenants. The Central workspace (with Workspace manager enabled) can consolidate content items to be published at scale to Member workspaces. *Workspace manager is enabled in settings.*

Possible Workspace Manager Architectures



Manage workspaces across tenants using Azure Lighthouse

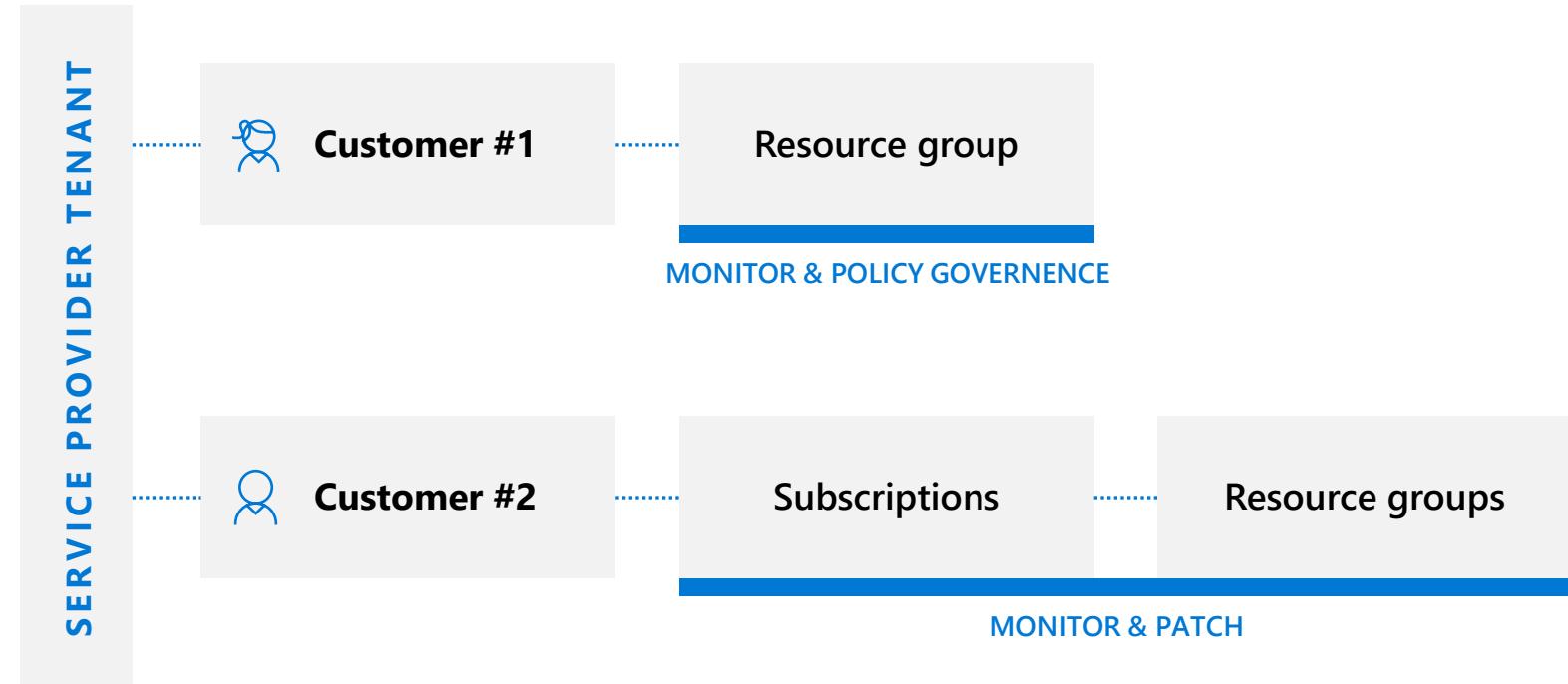


If you manage Microsoft Sentinel workspaces (and other Azure resources) across multiple Azure AD tenants, Azure Lighthouse provides access to subscription level management tools. Azure Lighthouse allows you to select all the subscriptions containing workspaces you manage.

Manage workspaces across tenants using Azure Lighthouse

**Microsoft Sentinel
Workspace manager**

- Microsoft Sentinel's Workspace manager enables users to centrally manage multiple Microsoft Sentinel workspaces within one or more Azure tenants.



Azure Lighthouse

- Implementing Azure Lighthouse provides the option to enable your access to the tenant.

Multiple tenants managed by Azure Lighthouse

Azure Lighthouse allows greater flexibility to manage resources for multiple customers without having to sign in to different accounts in different tenants. For example, a service provider may have two customers with different responsibilities and access levels. By using Azure Lighthouse, authorized users can sign in to the service provider's tenant to access these resources.

Create a Microsoft Sentinel workspace



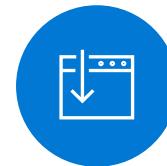
Start the creation process

1. At the search bar, search for Sentinel, then select **Microsoft Sentinel**.
2. The Microsoft Sentinel Workspaces shows a list of the current workspaces. Select the **+ add** button.



Create and configure a Log Analytics Workspace

1. The next page, **Add Microsoft Sentinel to a workspace** will display a list of available Log Analytics workspaces to add Microsoft Sentinel. Select the **+ create a new workspace** button.
2. The Basics tab includes: Subscription, Resource Group, Name, Region.
3. Select the **Review + Create** button and then select the **Create** button.



Add Microsoft Sentinel to the workspace

The "Add Microsoft Sentinel to Workspace" screen will now appear after you've completed the previous steps.

1. Wait for the newly created "Log Analytics Workspace" to appear in the list.
2. Select the newly created Log Analytics workspace. And select the **Add** button.

Interactive Lab Simulation: Click the [link](#) to start the lab simulation.

Understand Microsoft Sentinel permissions and roles

Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Microsoft Sentinel-specific roles

All Microsoft Sentinel built-in roles grant read access to the data in your Microsoft Sentinel workspace:

- **Microsoft Sentinel Reader**
- **Microsoft Sentinel Responder**
- **Microsoft Sentinel Contributor**
- **Microsoft Sentinel Automation Contributor**

Additional roles and permissions

- Working with playbooks to automate responses to threats
- Giving Microsoft Sentinel permissions to run playbooks
- Connecting data sources to Microsoft Sentinel
- Guest users assigning incidents
- Creating and deleting workbooks

Azure roles and Azure Monitor Log Analytics roles

- Azure roles grant access across all your Azure resources. They include Log Analytics workspaces and Microsoft Sentinel resources:
 - Owner
 - Contributor
 - Reader
- Log Analytics roles grant access across all your Log Analytics workspaces:
 - Log Analytics Contributor
 - Log Analytics Reader

Manage Microsoft Sentinel settings

Microsoft Sentinel environment settings are managed in two areas. In Microsoft Sentinel and in the Log Analytics workspace where Microsoft Sentinel resides. To configure Data Retention:

The screenshot shows the 'Usage and estimated costs' page in the Microsoft Log Analytics workspace. The 'Data Retention' tab is highlighted with a red box. On the right, there's a configuration panel for data retention.

Data Retention (Days): A slider is set to 30 days. Below it, text states: "Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more](#)".

Usage Charts: A bar chart titled "Billable data ingestion per solution" shows data for Nov 11 and Nov 15. The Y-axis ranges from 0MB to 5MB. The X-axis shows dates Nov 11 and Nov 15. A large red bar for Nov 15 reaches approximately 4.5MB.

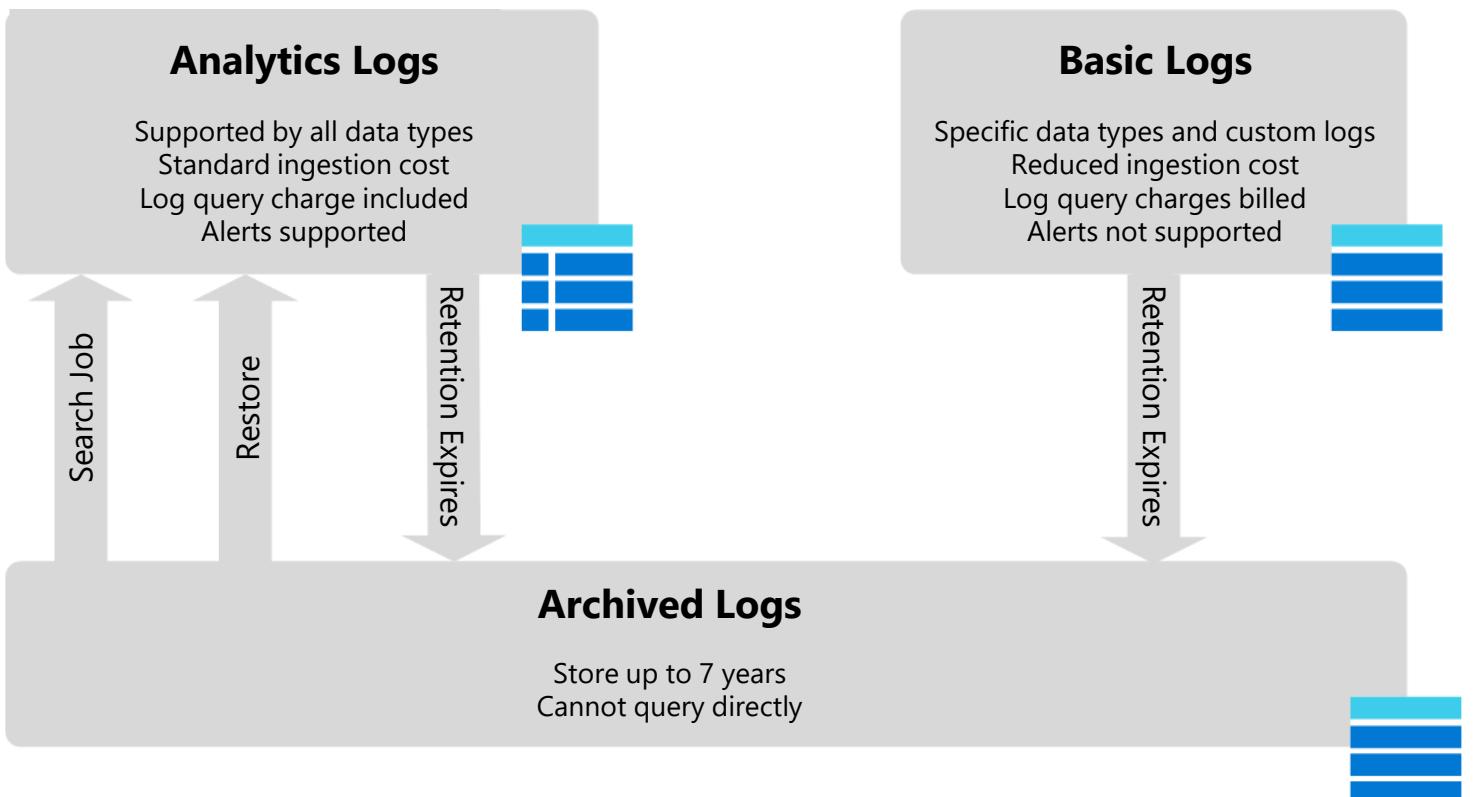
Data ingested per solution (last 90 days): A blue progress bar indicates data ingestion levels for various solutions over the last 90 days.

OK button: A blue "OK" button is located at the bottom right of the configuration panel.

Configure logs

There are three primary log types in Microsoft Sentinel:

- Analytics Logs
- Basic Logs
- Archive Logs



To access archived data, you must first retrieve data from it in an Analytics Logs table using one of the following methods:

- Search Jobs
- Restore

Knowledge check



1 Where is your log data stored?

- Microsoft Sentinel Workspace
- Azure Lighthouse
- Log Analytics workspace

2 Which Microsoft Sentinel security role can create workbooks?

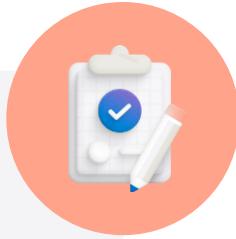
- Microsoft Sentinel Responder
- Microsoft Sentinel Reader
- Microsoft Sentinel Contributor

3 Why is it important to set the region when creating the Log Analytics workspace?

- Specifies where the log data will be stored.
- Specifies the timezone the data will be displayed in.
- Specifies the log retention period

Summary

You should have learned how the Microsoft Sentinel provisioning process includes creating a Log Analytics workspace and configuring the Microsoft Sentinel options.



You should now be able to:

- Describe Microsoft Sentinel workspace architecture
- Provision a Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Resources

You can learn more by reviewing the following.

- [Become a Microsoft Sentinel Ninja](#)
- [Microsoft Tech Community Security Webinars](#)

Connect Microsoft services to Microsoft Sentinel

Learning Objectives

After completing this module, you will be able to:

- 1** Install solutions from the content hub
- 2** Connect Microsoft services data connectors
- 3** Explain how connectors auto-create incidents in Microsoft Sentinel



Introduction

- You connect Microsoft 365 and Azure services to the Microsoft Sentinel workspace using the provided data connectors. The data connectors are included in out-of-the-box (OOTB), or built-in Content Hub solutions.
- You're a Security Operations Analyst working at a company that implemented Microsoft Sentinel. You'll connect Microsoft 365 and Azure services to Microsoft Sentinel.
- Based on your previously documented connector plan, you use the Content Hub to install the solutions that include the specific connectors. As you activate the connectors, you notice the option to have incidents created from the Microsoft Entra ID Protection service. You don't follow the recommended option to create incidents as you plan to activate the incident creation rule with custom options later in your implementation process.

Content hub solutions

Solutions can include:

- Data Connectors
- Parsers
- Workbooks
- Analytic Rules
- Hunting Queries
- Notebooks
- Watchlists
- Playbooks
- Azure Logic Apps custom connectors

Microsoft Sentinel | Content hub ...
Selected workspace: '

Refresh Install/Update Delete Guides & Feedback

338 Solutions 272 Standalone contents 17 Installed 9 Updates

search... Status : All Content type : All Support : All Provider : All Category : All Content sources : All

Content title	Content source	Provider	Support	Category	Status	Content type
Amazon Web Services FEATURED	Solution	Amazon Web S...	Microsoft	Security - Cloud Security	Analytics rule (56) Data connector (2) +2	Analytics rule Data connector +2
Analytics Health & Audit FEATURED	Standalone		Microsoft	IT Operations, Platform		Workbook
Azure Activity FEATURED	Solution	Microsoft	Microsoft	IT Operations	Installed Updates	Analytics rule (13) Data connector +2
Cisco Umbrella FEATURED	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security - ...	Installed	Analytics rule (10) Data connector +4
DNS Essentials FEATURED PREVIEW	Solution	Microsoft	Microsoft	Networking		Analytics rule (8) Hunting query (10) +2
Google Cloud Platform IAM FEATURED	Solution	Google	Microsoft	Cloud Provider, Identity		Analytics rule (10) Data connector +4
Log4j Vulnerability Detection FEATURED	Solution	Microsoft	Microsoft	Application, Security - Automation (SOAR...)		Analytics rule (4) Hunting query (10) +3
Microsoft Defender for Cloud FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection	Installed	Analytics rule Data connector (2)
Microsoft Defender XDR FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection	Installed Updates	Analytics rule (10) Data connector +2
Microsoft Entra ID FEATURED	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR)	Installed Updates	Analytics rule (62) Data connector +2
Network Session E... FEATURED PREVIEW	Solution	Microsoft	Microsoft	Security - Network		Analytics rule (7) Hunting query (4) +3
SAP applications FEATURED	Solution		Microsoft	Cloud Provider, Software	Installed Updates	
Security Threat Essentials FEATURED	Solution	Microsoft	Microsoft	Security - Others		Analytics rule (7) Hunting query (2)

Showing 1 to 30 of 610 results

Ingest log data with Data connectors

To collect log data, you need to connect your data sources with Microsoft Sentinel Connectors. You install Content Hub Solutions that include the data connectors.

Microsoft Sentinel | Content hub

Selected workspace: ''

Search Refresh Install/Update Delete Guides & Feedback

General

Solutions: 338 | Standalone contents: 272 | Installed: 17 | Updates: 9

Logs News & guides Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub** (highlighted with a red box)
- Repositories (Preview)
- Community

Configuration

- Workspace manager (Preview)
- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

Search... Status : All Content type : All Support : All Provider : All Category : All Content sources : All

Content title	Content source	Provider	Support	Category	Status	Content type
AWS Amazon Web Services FEATURED	Solution	Amazon Web S...	Microsoft	Security - Cloud Security		
Analytics Health & Audit FEATURED	Standalone		Microsoft	IT Operations, Platform		
Azure Activity FEATURED	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (13)	
Cisco Umbrella FEATURED	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security - ...		
DNS Essentials FEATURED PREVIEW	Solution	Microsoft	Microsoft	Networking		
Google Cloud Platform IAM FEATURED	Solution	Google	Microsoft	Cloud Provider, Identity		
Log4j Vulnerability Detection FEATURED	Solution	Microsoft	Microsoft	Application, Security - Automation (SOAR...)		
Microsoft Defender for Cloud FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection		
Microsoft Defender XDR FEATURED	Solution	Microsoft	Microsoft	Security - Threat Protection	Analytics rule (10)	
Microsoft Entra ID FEATURED	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR)	Analytics rule (62)	
Network Session E... FEATURED PREVIEW	Solution	Microsoft	Microsoft	Security - Network		
SAP applications FEATURED	Solution		Microsoft	Cloud Provider, Software		

< Previous Page 1 of 21 Next > Showing 1 to 30 of 610 results.

Azure Activity

Microsoft Provider Microsoft Support Version 2.0.6

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)
- There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, Workbooks: 1, Analytic Rules: 12, Hunting Queries: 14

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Content type 13 Analytics rule 1 Data connector 14 Hunting query

1 Workbook

Category IT Operations

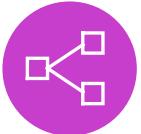
Pricing Free

Manage Actions View details

Plan for Microsoft services connectors



Microsoft 365 connector: The Configuration option allows for the sending of Exchange, SharePoint, and Teams data.



Microsoft Entra ID: Has two configuration options for Sign-On logs and Audit logs.



Microsoft Entra ID Protection: Integrates Microsoft Entra ID Protection alerts with Microsoft Sentinel when connected.



Azure Activity: The Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure.

Connect the Microsoft 365 connector

The Microsoft 365 connector provides insight into ongoing user activities.

To view the connector page, do these steps:

1. Select Data connectors page in Sentinel.
2. Select **Microsoft 365**.
3. Then select the **Open connector** page on the preview pane.
4. Under the section labeled Configuration, mark the Office 365 activity logs' checkboxes to connect to Microsoft Sentinel.
5. Select **Apply Changes**.

The screenshot shows the Microsoft 365 (formerly, Office 365) connector configuration page. On the left, there's a preview pane showing basic information about the connector, including its status as 'Not connected', the provider as 'Microsoft', and the last log received. It also displays the description, which highlights that the connector provides insight into ongoing user activities like file downloads and access requests. Below this are sections for 'Content source' (Microsoft 365), 'Author' (Microsoft), and 'Related content' (2 workbooks, 3 queries, 14 analytics rules templates). A chart titled 'Data received' shows a steady stream of data from January 3 to January 7. On the right, under the 'Instructions' tab, there are two main sections: 'Prerequisites' and 'Configuration'. The 'Prerequisites' section lists required permissions: 'Workspace' (read and write) and 'Tenant Permissions' ('Global Administrator' or 'Security Administrator'). The 'Configuration' section allows users to connect Microsoft 365 activity logs to Microsoft Sentinel by selecting checkboxes for Exchange, SharePoint, and Teams, and then clicking 'Apply Changes'. Below this, there's a note about previously connected tenants and a 'Save' button.

Connect the Microsoft Entra ID connector

Gain insights into Microsoft Entra ID by connecting Audit and Sign in logs to Microsoft Sentinel to gather insights around Microsoft Entra ID scenarios.

To view the connector page, do these steps:

1. Select Data connectors page in Microsoft Sentinel.
2. Select **Microsoft Entra ID**
3. Then select the **Open connector** page on the preview pane.
4. Mark the checkboxes next to the logs you want to stream into Microsoft Sentinel, and select **Connect**.

The screenshot shows the Microsoft Entra ID connector configuration page. On the left, there's a summary card with 'Connected Status' (Microsoft Provider, 4 days ago), a 'Description' section, and a 'Last data received' timestamp (12/01/23, 11:59 AM). It also shows 'Content source' (Microsoft Entra ID), 'Author' (Microsoft), and 'Version' (1.0.0). Below this are 'Related content' links for workbooks, queries, and analytics rules templates. A line chart at the bottom tracks 'Data received' over time, showing a peak of 31 on December 1st. On the right, the 'Instructions' section lists requirements for 'Diagnostic Settings' and 'Tenant Permissions'. The 'Configuration' section allows selecting log types to stream to Microsoft Sentinel, with 'Sign-in Logs' checked. A note indicates that a P1 or P2 license is required for sign-in data. A list of available log types includes Audit Logs, Non-Interactive User Sign-In Log (Preview), Service Principal Sign-In Logs (Preview), Managed Identity Sign-In Logs (Preview), Provisioning Logs (Preview), ADFS Sign-In Logs (Preview), User Risk Events (Preview), Risky Users (Preview), Network Access Traffic Logs (Preview), Risky Service Principals (Preview), and Service Principal Risk Events (Preview). A blue 'Apply Changes' button is at the bottom.

Connect the Microsoft Entra ID Protection connector

Microsoft Entra ID Protection provides a consolidated view of at-risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to autoremediate future events.

To view the connector page, do these steps:

1. Select Data connectors page.
2. Select **Microsoft Entra ID Protection**.
3. Then select the **Open connector** page on the preview pane.
4. Select **Connect** to start streaming the Microsoft Entra ID Protection alerts.
5. Select whether alerts from Microsoft Entra ID Protection automatically generate incidents by selecting **Enable**.

Microsoft Entra ID Protection

Not connected Status Microsoft Provider Last Log Received

Description Microsoft Entra ID Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Entra ID Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.

Get Microsoft Entra ID Premium P1/P2 >

Last data received --

Related content 0 Workbooks 2 Queries 1 Analytics rules templates

Data received Go to log analytics

100
80
60
40
20
0

November 29 December 1 December 3

Total data received 0

Data types SecurityAlert (IPC) --

Instructions

Prerequisites To integrate with Microsoft Entra ID Protection make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** Microsoft Entra ID Premium P2

Configuration Microsoft Entra ID Protection alerts to Microsoft Sentinel Connect Microsoft Entra ID Protection to Microsoft Sentinel.

The alerts are sent to this Microsoft Sentinel workspace.

Connect

Create incidents - Recommended! Create incidents automatically from all alerts generated in this connected service. Enable

Connect the Azure Activity Data Connector

The Azure Activity connector requires the subscription owner role and uses Azure Policy Assignments. It streams data to the *AzureActivity* table in the Sentinel Log Analytics workspace.

Azure Activity ...

Azure Activity

Connected Status Microsoft Provider 9 minutes ago Last Log Received

Description

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received 08/02/23, 10:50 AM

Content source Azure Activity Version 2.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Related content 0 Workbooks 2 Queries 14 Analytics rules templates

Data received

Go to log analytics

Total data received 1.07 k

Data types AzureActivity 08/02/23, 10:50 AM

Instructions

Prerequisites

To integrate with Azure Activity make sure you have:

- ✓ **Workspace:** read and write permissions.
- ℹ **Policy:** owner role assigned for each policy assignment scope.
- ℹ **Subscription:** owner role permission on the relevant subscription

Configuration

This connector has been updated to use the diagnostics settings back-end pipeline, which provides increased functionality and better consistency with resource logs. Connectors using this pipeline can also be governed at scale by Azure Policy. Learn more about the new [Azure Activity connector](#). Follow the instructions below to upgrade your connector to the diagnostics settings pipeline.

1. Disconnect your subscriptions from the legacy method

The subscriptions listed below are still using the older, legacy method. You are strongly encouraged to upgrade to the new pipeline. To do this, click on the 'Disconnect All' button below, before proceeding to launch the Azure Policy Assignment wizard.

You don't have subscriptions using the legacy method, please move to step 2

Disconnect All

2. Connect your subscriptions through diagnostic settings new pipeline

This connector uses Azure Policy to apply a single Azure Subscription log-streaming configuration to a collection of subscriptions, defined as a scope. Follow the steps for this resource type.

Launch the Azure Policy Assignment wizard and follow the steps.

- In the **Basics** tab, click the button with the three dots under **Scope** to select your resources assignment scope.
- In the **Parameters** tab, choose your Microsoft Sentinel workspace from the **Log Analytics workspace** drop-down list, and leave marked as "True" all the parameters.
- To apply the policy on your existing resources, select the **Remediation tab** and mark the **Create a remediation task** checkbox.

Launch Azure Policy Assignment wizard>

Knowledge check



1 Which table (data type) would you query for the Microsoft Entra ID data?

- OfficeActivity
- SigninLogs
- SecurityAlert

2 Which table (data type) would you query for the Microsoft 365 data?

- OfficeActivity
- SecurityAlert
- SigninLogs

3 Which table (data type) would you query for the Microsoft Entra ID Protection data?

- OfficeActivity
- SigninLogs
- SecurityAlert

Summary

You should have learned how to connect Microsoft 365 and Azure services to the Microsoft Sentinel workspace using the provided data connectors.



You should now be able to:

- Connect Microsoft services connectors
- Explain how connectors autoreate incidents in Microsoft Sentinel

Resources

You can learn more by reviewing the following.

- [Become a Microsoft Sentinel Ninja](#)
- [Microsoft Tech Community Security Webinars](#)

Connect Windows hosts to Microsoft Sentinel

Learning Objectives

After completing this module, you will be able to:

- 1** Connect Azure Windows Virtual Machines to Microsoft Sentinel
- 2** Connect non-Azure Windows hosts to Microsoft Sentinel
- 3** Configure Log Analytics agent to collect Sysmon events



Introduction

- You're a Security Operations Analyst working at a company that implemented Microsoft Sentinel. You must collect event log data from Windows Hosts. The hosts could be located on-premise or as a virtual machine in Azure.
- You collect data from Windows devices using the provided Microsoft Sentinel data connectors. The connectors offer options to control which events to collect.
- Your Security Operations team also relies on event data created by the Sysmon tool installed on some of the Windows Hosts. You'll configure the Windows hosts to send event data to Microsoft Sentinel. You also need to ensure that the Sysmon events are available to be used in detection rules.
- By the end of this module, you'll be able to connect Windows devices to the Microsoft Sentinel workspace using the provided data connector.

Plan for Windows hosts security events

Data Ingestion Options using Content Hub Solutions

**Windows Security Events
(via AMA) Solution**

**Windows server DNS (via
AMA) Solution**

**Windows Forwarded
Events Solution**

These solutions install data connectors for AMA and use data collection rules (DCR)

Windows Security Events via AMA Connector

Benefits:

- Manage collection settings at scale
- Azure Monitoring Agent shared with other solutions
- Security & performance improvements
- Cost savings by using data collection rules

Limitations:

- Some features are currently available only in public preview

Requirements:

- Data Collection Rules (DCR)
- Non-Azure VM's/devices require Azure Arc

Windows Security Events via AMA Connector

Microsoft Sentinel | Content hub

Selected workspace:

Search Refresh Install/Update Delete Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub
- Repositories (Preview)
- Community

Configuration

- Workspace manager (Preview)
- Data connectors

302 Solutions 262 Standalone contents 0 Installed 0 Updates

Windows Security

Status : All Content type : All Support : All Provider : All Category : All

Content sources : All

Content title	Content source	Provider	Support	Category	Status
Azure AD Health Monitoring Agent Registry	Standalone	Community	Identity, Security - Others		
Azure AD Health Service Agents Registry	Standalone	Community	Identity, Security - Others		
Windows Security Events	Solution	Microsoft	Microsoft	Security - Threat Protection	

Windows Security Events

Microsoft Provider Microsoft Support 2.0.4 Version

Description

Note: There may be known issues pertaining to this Solution, please refer to them before installing.

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends Installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31.2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2 Workbooks: 2 Analytic Rules: 20 Hunting: 1

Install View details

< Previous Page 1 of 1 Next > Showing 1 to 3 of 3 results.

Connect using the Security Events via Legacy Agent Connector

The Security Events via Legacy Agent connector lets you stream all security events from your Windows systems (servers and workstations, physical and virtual) to your Microsoft Sentinel workspace.

You can select which events to stream from among the following sets:

- All events
- Common
- Minimal
- None

The screenshot shows the 'Security Events via Legacy Agent' configuration page in Microsoft Azure. The left pane displays a summary of the connection status ('Not connected'), provider ('Microsoft Provider'), and last log received. It also includes a description of the connector's purpose, related content (9 workbooks, 1 query, 73 analytics rules templates), and a chart showing data received over time (Nov 23 to Nov 27). The right pane contains sections for 'Prerequisites' (listing workspace and data source permissions) and 'Configuration'. In the 'Configuration' section, step 1 is about downloading and installing the agent (noting logs are collected only from Windows agents). Step 2 is about selecting event streams, with 'None' selected. There are also sections for choosing the installation location (Azure Windows Virtual Machine or non-Azure Windows Machine) and applying changes.

Collect Sysmon event logs

System Monitor (Sysmon) is a Windows system service, and device driver that remains resident across system reboots to monitor and log system activity to the Windows event log once installed on a system.

It provides detailed information about process creations, network connections, and changes to file creation time.

The screenshot shows the Microsoft Azure Log Analytics workspace interface. On the left, there's a sidebar with various icons and a search bar at the top. The main area is titled "SecMonLAW | Legacy agents management". It has sections for "Windows event logs", "Windows performance counters", "Linux performance counters", "Syslog", and "IIS Logs". Under "Windows event logs", there's a table with columns for "Log name" (System, Microsoft-Windows-Sysmon/Operational), "Error" (checkboxes checked for both), "Warning" (checkboxes checked for both), and "Information" (checkboxes checked for both). There are also "Apply" and "Discard changes" buttons at the bottom of the table. The URL in the browser is "https://attclass.logAnalytics.azure.com/resourceGroups/SecMonLAW/providers/Microsoft.Insights/eventLogs?api-version=2015-05-01&logName=System&category=Information×pan=PT1H&orderby=Time%20desc&size=1000&format=JSON".

Knowledge check



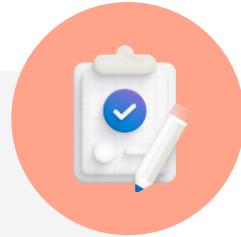
- 1 Which connector do you use to collect Windows security events?**
 - Windows Security Events via AMA
 - Common Event Format
 - Syslog

- 2 To collect Sysmon events with the Security Events via Legacy Agent connector, what is the log name used to collect it in advanced settings?**
 - Microsoft-Windows-Sysmon/Operational
 - Microsoft-Windows-Sysmon/Events
 - Microsoft-Windows-Sysmon/Logs

- 3 When managing or creating a data connector, Data Collection Rule (DCR) what tabs are always configured?**
 - Event
 - Resource and Collect
 - XPath

Summary

You should have learned how to connect Windows devices to the Microsoft Sentinel workspace using the provided data connectors. The connector offers options to control which events to collect.



You should now be able to:

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

Resources

You can learn more by reviewing the following.

- [Become a Microsoft Sentinel Ninja](#)
- [Microsoft Tech Community Security Webinars](#)
- [Microsoft Defender for Cloud data collection with the Azure Monitor Agent \(AMA\)](#)

Threat detection with Microsoft Sentinel analytics

Learning Objectives

After completing this module, you will be able to:

- 1** Explain the importance of Microsoft Sentinel Analytics
- 2** Explain different types of analytics rules
- 3** Create rules from templates
- 4** Create new analytics rules and queries using the analytics rule wizard
- 5** Manage rules with modifications

Introduction

- Microsoft Sentinel Analytics provides an intelligent solution that you can use to detect potential threats and vulnerabilities in your organizations.
- In this module, you'll understand the importance of using Microsoft Sentinel Analytics, create, and implement analytics rules from existing templates, create new rules and queries using the wizard, and manage rules with modifications.
- By the end of this part, you'll be able to set up analytics rules in Microsoft Sentinel to help the SecOps team identify and stop cyberattacks.

What is Microsoft Sentinel Analytics?

Microsoft Sentinel Analytics provides several functionalities that you can use to implement security for the data and resources at Contoso.

With the proper analytics rule, you can get insights into where an attack originated from, what resources were compromised, potential data lost, along with the timeline for the incident.

You can create analytics rules from the **Analytics** home page. You can access the **Analytics** page in Microsoft Sentinel from the navigation pane.

The screenshot shows the Microsoft Sentinel Analytics interface. The left sidebar includes sections for Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), Content management (Content hub, Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors, Analytics, Watchlist, Automation, Settings), and a main search bar. The main area displays 333 Active rules. A summary bar shows the distribution of rules by severity: High (198), Medium (398), Low (73), and Informational (17). Below this, a table lists rules with columns for Severity, Name, Rule type, Status, Tactics, Techniques, and Source. One specific rule is highlighted: "Brute force attack against user credentials (...)" with Medium Severity, Custom Content Source, and Enabled Status. The right side provides detailed information about this rule, including its ID (d39cf416-3050-4f39-bae0-f9f54be05c4c), description (Identifies evidence of brute force activity against a user based on multiple authentication failures and at least one successful authentication within a given time window. Note that the query does not enforce any sequence, and does not require the successful authentication to occur last.), tactics and techniques (Credential Access), and links for Edit and Compare with template.

Types of analytics rules

- Microsoft security (incident creation rule)
- Fusion
- Machine learning (ML) Behavioral Analytics
- Threat Intelligence
- Anomaly
- Scheduled
- Near-real-time (NRT)

Microsoft Sentinel | Analytics

Scheduled query rule NRT query rule Microsoft incident creation rule

More content at Content hub

Rules by severity

High (7) Medium (7) Low (1) Informational (0)

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Source name
High	Azure VM Deletion	Scheduled	Enabled	Impact		Custom Content
High	NRT PowerShell Hunt	NRT	Enabled	Command ...		Custom Content
Medium	WindowsEventsAMA	NRT	Enabled	Privilege Es...		Custom Content
Medium	DetectStuff	NRT	Enabled	Initi... +1 ⓘ		Custom Content
Medium	New Azure Activity	NRT	Disabled	Initial Access		Custom Content
Medium	Suspicious number of resource creation or deployment...	Scheduled	Enabled	Impact	T1496	Azure Activity
High	Create incidents based on Microsoft Defender for Clo...	Microsoft Security	Enabled			Gallery Content
Medium	Sign-ins from IPs that attempt sign-ins to disabled acc...	Scheduled	Enabled	Initi... +1 ⓘ		Gallery Content
Medium	Malicious Inbox Rule - custom	Scheduled	Enabled	Pers... +1 ⓘ		Custom Content
High	Solorigate Network Beacon	Scheduled	Enabled	Command ...		Gallery Content
Medium	TestSQR	Scheduled	Enabled	Initial Access		Custom Content
High	Azure DevOps Audit Stream Disabled	Scheduled	Enabled	Defense Ev...		AzureDevOpsA...
Low	Azure AD Role Assignment Audit Trail	Scheduled	Enabled	Persistence		Custom Content
High	Create incidents based on Microsoft Defender for Clo...	Microsoft Security	Enabled			Custom Content

Previous Page 1 of 1 Next Showing 1 to 15 of 15 results

Create an analytics rule from a template: Gallery Content rules

Note: many Content Hub Solutions install analytic rule templates

Microsoft Sentinel | Analytics ...
Selected workspace: 'sentinel'

More content at Content hub

Rules by severity

3 Active rules

High (2) Medium (0) Low (1) Informational (0)

Active rules Rule templates Anomalies

Search Add filter

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics	Techniques	Source name
High	DEV-0270 New User Creation	Scheduled	Security Event... +1 ⓘ	Persistence	T1098	Gallery Content
High	AV detections related to Sp...	Scheduled	Microsoft 365 Defe...	Initial Access	T1190	Gallery Content
High	URL Added to Application f...	Scheduled	Azure Active Direct...	⊕ ↗	T1078	Gallery Content
High	Prestige ransomware IOCs ...	Scheduled	Microsoft 365... +1 ⓘ	Execution	T1203	Gallery Content
High	Identify MERCURY powersh...	Scheduled	Security Event... +1 ⓘ	Lateral Moveme...	T1570	Gallery Content
High	NOBELIUM IOCs related to ...	Scheduled	F5 Networks +11 ⓘ	Collection	T1005	Gallery Content
High	Dev-0270 Malicious Powers...	Scheduled	Security Event... +1 ⓘ	⊕ ↗	T1048 +1 ⓘ	Gallery Content
High	NRT Azure DevOps Audit St...	NRT		Defense Evasion	T1562	Gallery Content
High	AdminSDHolder Modificati...	Scheduled	Security Events via L...	Persistence	T1078	Gallery Content
High	Dev-0228 File Path Hashes ...	Scheduled		⊕ ↗	T1569 +1 ⓘ	Gallery Content

< Previous Page 1 of 10 Next >

LEARN M
About an

NOBELIUM IOCs related to FoggyWeb

High Severity Gallery Content Content source Sc Ru

Tactics and techniques

Collection (1)

Rule query

```
let iocs = externaldata(DateAdded:string IoC:string,Type:string,TLP:string) [@"h raw.githubusercontent.com/Azure/Azure-S master/Sample%20Data/Feeds/FoggyWebIOC. with (format="csv", ignoreFirstRecord=T let sha256Hashes = (iocs | where Type = "File" | select IoC)
```

Note:

- You haven't used this template yet; You can use analytics rules.
- One or more data sources used by this rule is m might limit the functionality of the rule.

Create rule

Create an analytics rule from a wizard

Creating a custom rule from a scheduled query rule type provides you with the highest level of customization. You can define your own KQL code, set a schedule to run an alert, and provide an automated action by associating the rule with a Microsoft Sentinel Playbook.

To create a scheduled query rule, in the Azure portal, under **Microsoft Sentinel**, select **Analytics**. In the header bar, select **+Create**, and then select **Scheduled query rule**.

Analytics rule wizard - Create new rule

General Set rule logic Incident settings (Preview) Automated response Review and create ...

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity  
| where OperationName == "Delete Virtual Machine"  
| where ActivityStatus == "Accepted"  
| extend AccountCustomEntity = Caller  
| extend IPCustomEntity = CallerIpAddress
```

[View query results >](#)

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

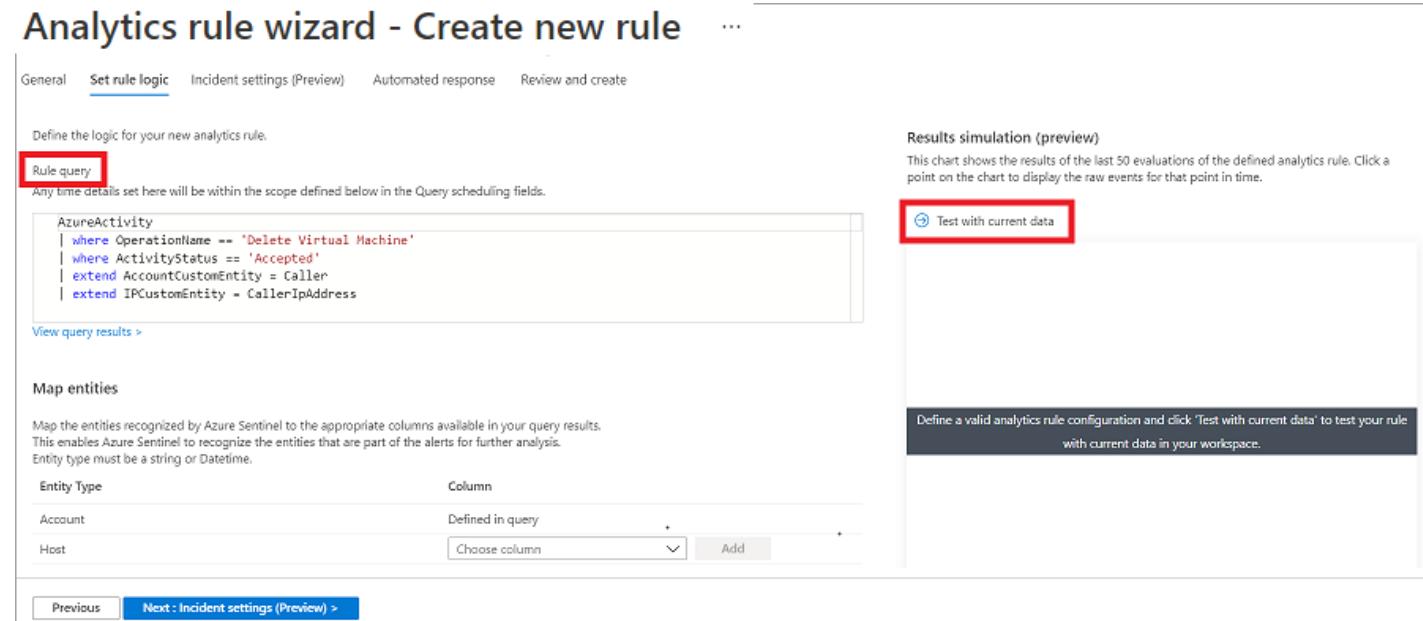
Entity Type	Column
Account	Defined in query
Host	Choose column

[Previous](#) [Next : Incident settings \(Preview\) >](#)

Results simulation (preview)
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.



Manage analytics rules

To adjust the noise and filter the more important threats detected, you should manage the analytics rules on an ongoing basis. This will help ensure that your rules remain useful and efficient in detecting potential security threats.

The screenshot shows the Microsoft Defender XDR Analytics Rules interface. At the top, there are buttons for Create, Refresh, Analytics workbooks, Rule runs (Preview), Enable, Disable, Delete, Import, Export, Guides & Feedback, and Columns. A navigation bar indicates 14 Active rules, More content at Content hub, and a Rules by severity chart showing 7 High, 7 Medium, 1 Low, and 0 Informational rules.

The main table lists 14 rules:

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last Modified
High	Azure VM Deletion	Scheduled	Enabled	Impact		Custom Content	1/9/2024, 12:45...
High	NRT PowerShell Hunt	NRT	Enabled	Command ...		Custom Content	11/27/2023, 3:3...
Medium	WindowsEventsAMA	NRT	Enabled	Privilege Es...		Custom Content	10/2/2023, 11:5...
Medium	DetectStuff	NRT	Enabled	Initi... +1 ⓘ		Custom Content	8/4/2023, 3:55...
Medium	New Azure Activity	NRT	Disabled	Initial Access		Custom Content	8/4/2023, 3:11...
Medium	Suspicious number of resource creation or deployme...	Scheduled	Enabled	Impact	T1496	Azure Activity	8/3/2023, 3:56...
High	Create incidents based on Microsoft Defender for Cl...	Microsoft Security	Enabled			Gallery Content	6/5/2023, 1:31...
Medium	Sign-ins from IPs that attempt sign-ins to disabled ac...	Scheduled	Enabled	Initi... +1 ⓘ		Gallery Content	4/4/2023, 8:46...
Medium	Malicious Inbox Rule - custom	Scheduled	Enabled	Pers... +1 ⓘ		Custom Content	3/30/2023, 5:21...
High	Solorigate Network Beacon	Scheduled	Enabled	Command ...		Gallery Content	3/30/2023, 5:21...
Medium	TestSQR	Scheduled	Enabled	Initial Access		Custom Content	12/28/2022, 11:...
High	Azure DevOps Audit Stream Disabled	Scheduled	Enabled	Defense Ev...		AzureDevOpsA...	11/15/2022, 12:...
Low	Azure AD Role Assignment Audit Trail	Scheduled	Enabled	Persistence		Custom Content	10/7/2022, 2:38...
High	Create incidents based on Microsoft Defender for Cl...	Microsoft Security	Enabled			Custom Content	9/26/2022, 2:23...
High	Advanced Multistage Attack Detection	Fusion	Enabled	Col... +11 ⓘ		Gallery Content	8/18/2022, 1:51...

A context menu is open for the first rule, 'Azure VM Deletion'. The menu items are: Info, Insights, Edit, Disable, Duplicate, Delete, and Rule runs (Preview). The 'Rule runs (Preview)' item is highlighted with a red box. To the right of the rule details, there are sections for Rule query (containing a PowerShell-like query), Rule frequency (Run query every 5 minutes), Rule period (Last 5 hours data), and Rule threshold (Trigger alert if query returns more than 0 results). A large red box highlights the 'Edit' button at the bottom right of the rule card.

Manage analytics rules

You can perform the following four actions on existing active rules:

Edit rules:

- You can modify existing rules by selecting **Edit** in the details pane.
- To edit a rule, you navigate the same pages that you did in creating the rule.

Disable rules:

- You can disable a rule when you're performing an activity that can trigger the rule alert.
- Disabled rules retain their configuration, and you can enable them again at a later time.

Duplicate rules:

- When you duplicate a rule, the rule contains all the configuration provided from the original rule.
- You can further modify the configuration based on your requirements.

Delete rules:

- Deleting the rule prompts you for confirmation before Microsoft Sentinel Analytics removes it from the set of active rules.
- Be aware that deleting a rule is permanent, and there isn't an undo feature.

Summary

In this part, you learned how Microsoft Sentinel Analytics can help SecOps to identify and stop cyberattacks.



- By using Microsoft Sentinel Analytics, the SecOps team was able to detect and analyze potential threats more effectively. They could create analytics rules that would trigger alerts. The SecOps team was then able to effectively react to the threats based on the triggered alerts.
- Without the help of Microsoft Sentinel Analytics, earlier the SecOps team wasn't able to use its time effectively on its other operations because it was spending time in manually correlating the threats and analyzing them.

Automation in Microsoft Sentinel

Learning Objectives

After completing this module, you will be able to:

- 1** Explain automation options in Microsoft Sentinel
- 2** Create automation rules in Microsoft Sentinel



Introduction

- Microsoft Sentinel, in addition to being a Security Information and Event Management (SIEM) system, is also a platform for Security Orchestration, Automation, and Response (SOAR). One of its primary purposes is to automate any recurring and predictable enrichment, response, and remediation tasks that are the responsibility of your Security Operations Center and personnel (SOC/SecOps)
- You're a Security Operations Analyst working at a company that implemented Microsoft Sentinel. You've identified an analytical rule that generates incidents that are considered Benign Positive. You would like to automatically close these incidents after generation.

Understand automation options

Automation rules

- Automation rules centralize incident handling automation.
- They automate responses for multiple analytics rules simultaneously.
- Users can automatically tag, assign, or close incidents without playbooks.
- Users can control the execution order of actions.
- Automation rules streamline automation in Microsoft Sentinel and simplify incident orchestration workflows.

Playbooks

- Playbooks automate response and remediation actions in Microsoft Sentinel.
- They integrate with internal and external systems.
- Playbooks can be triggered automatically by alerts, incidents, analytics rules, or automation rules.
- Playbooks benefit from Logic Apps' design tools, scalability, and reliability as a Tier 1 Azure service.

Create automation rules (1)



Automation blade

- The new Automation blade replaces the Playbooks blade for central management of automation rules.
- In the Automation blade, you can create, edit, enable, disable, and reorder automation rules.
- Automation rules can be applied to multiple analytics rules, offering flexibility in configuration.
- The Automation blade displays all defined rules, their status, and the analytics rules to which they apply.



Analytics rule wizard

- The Automated response tab in the analytics rule wizard manages and creates automation rules specific to the edited or created analytics rule.
- When using the Analytics blade, you can select rule types and open the rule wizard to access the Automated response tab.
- The creation of automation rules within this tab is tailored to the analytics rule you're editing, with the condition preset, while other configuration options remain accessible.



Incidents blade

- Automation rules can be created in the Incidents blade for responding to single or recurring incidents, especially for suppression purposes.
- When creating an automation rule from an incident, the rule's name, analytics rule, conditions, actions, and expiration date are pre-populated, with a default suppression action.
- Users have the flexibility to modify conditions, actions, and the expiration date according to their needs.

Create automation rules (2)



Trigger: Automation rules are triggered by the creation of an incident.



Conditions: Complex sets of conditions can be defined to govern when actions should run.



Actions: Actions can be defined to run when the conditions are met.



Expiration date: You can define an expiration date on an automation rule.



Order: You can define the order in which automation rules will run.

Knowledge check



1 Automation rules are triggered by?

- Incidents
- Connectors
- Watchlists

2 You use a Logic Apps to create a_?

- Automation rule
- Playbook
- Workbook

3 An Automation rule action can?

- Update the incident title
- Delete the incident
- Change the incident status

Summary

You should have learned how Microsoft Sentinel is also a platform for Security Orchestration, Automation, and Response (SOAR).



You should now be able to:

- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel

Resources

You can learn more by reviewing the following.

- [Become a Microsoft Sentinel Ninja](#)
- [Microsoft Tech Community Security Webinars](#)

Resources

You can learn more by reviewing the following documents.

- [Microsoft Sentinel documentation](#)
- [Quickstart: On-board Microsoft Sentinel](#)
- [Microsoft Sentinel pricing](#)
- [Permissions in Microsoft Sentinel](#)
- [Tutorial: Visualize and monitor your data](#)
- [Quickstart: Get started with Microsoft Sentinel](#)
- [What is Azure Lighthouse?](#)
- [Extend Microsoft Sentinel across workspaces and tenants](#)
- [What is Azure Resource Manager?](#)
- [Azure Foundation 4-Week Implementation](#)
- [Tutorial: Detect threats out-of-the-box](#)
- [Connect data sources](#)



Swiss Post
Cybersecurity

Thank you.