Microsoft

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

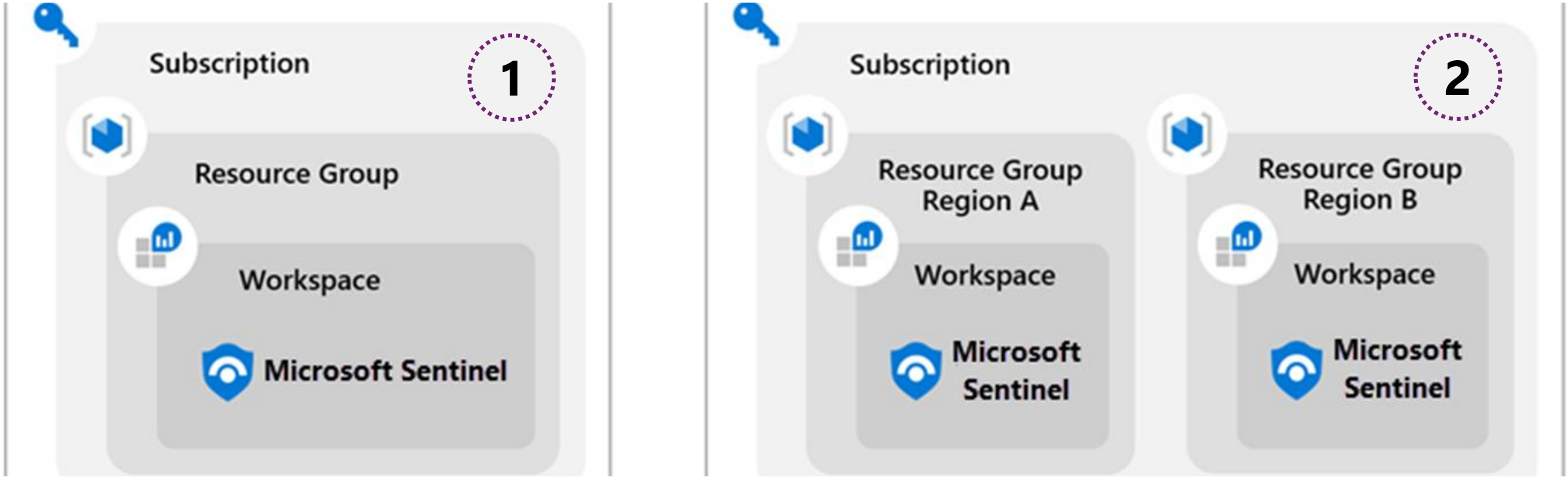
After completing this module, you will be able to:

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.

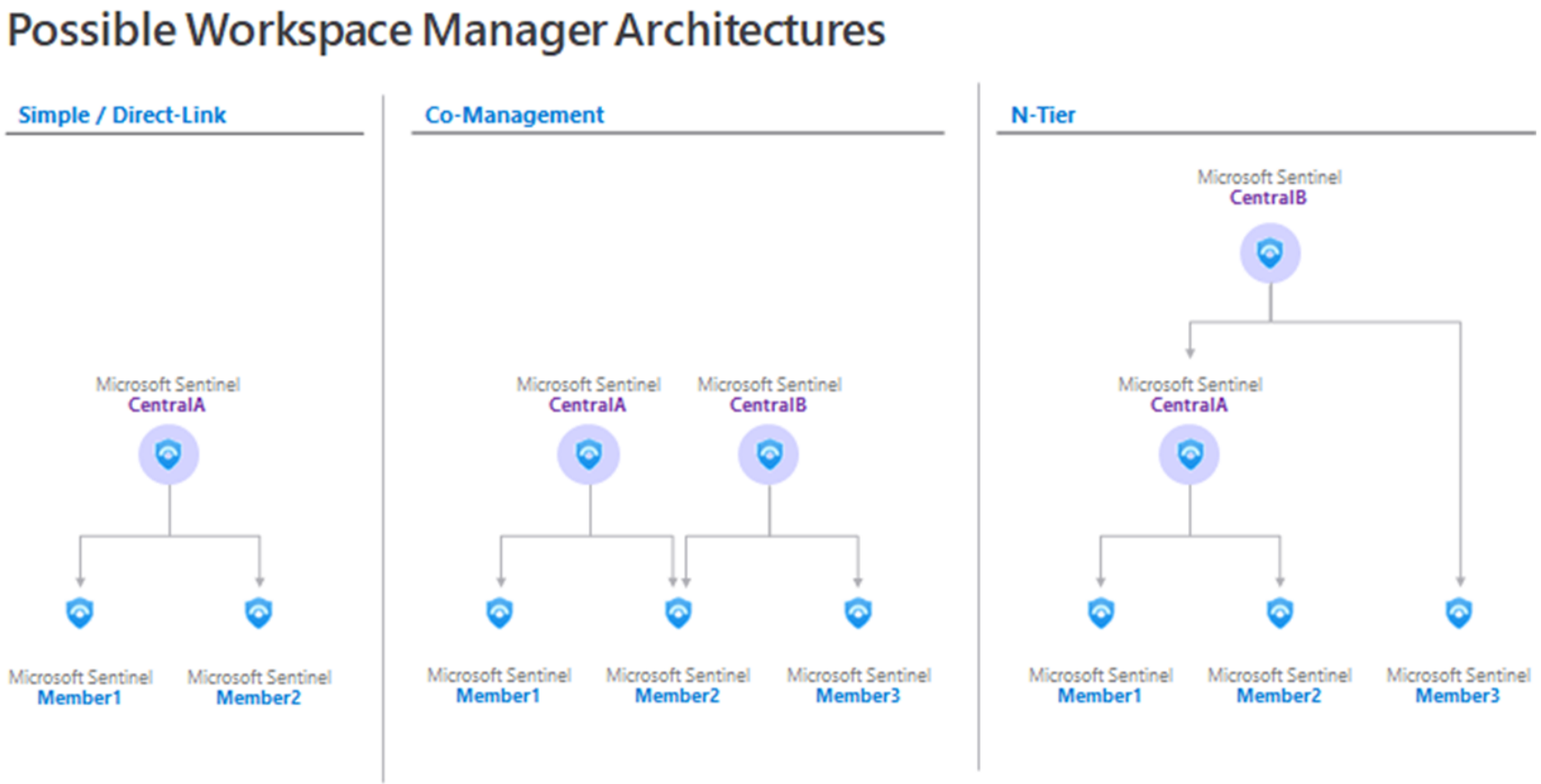
# Plan for the Microsoft Sentinel workspace



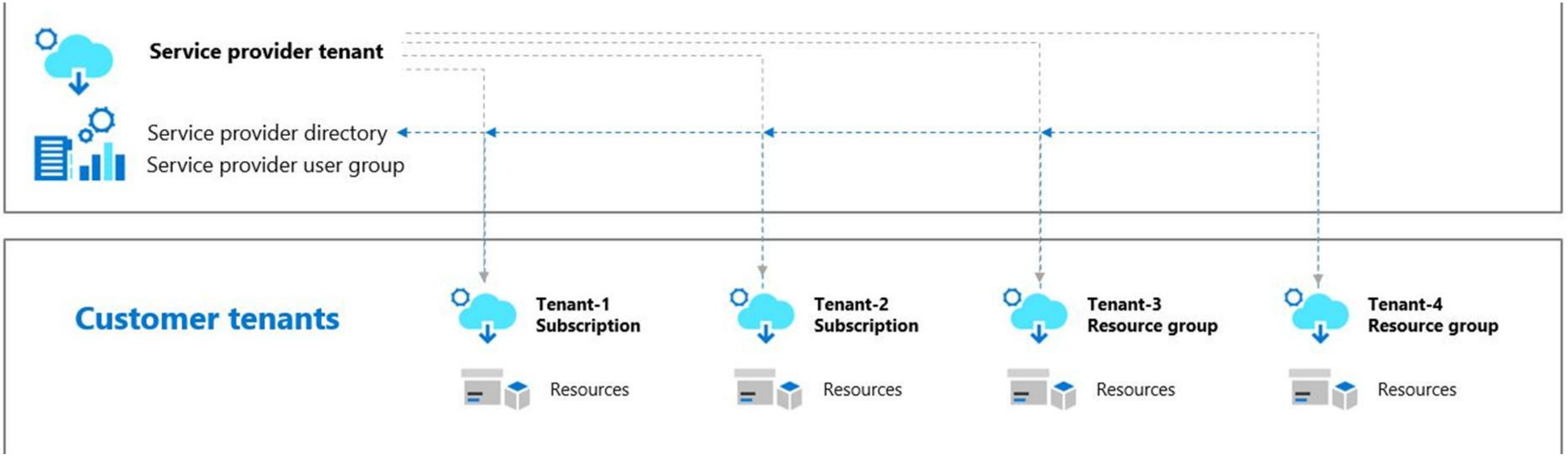

1. Single-Tenant with a single Microsoft Sentinel Workspace
2. Single-Tenant with regional Microsoft Sentinel Workspaces
3. Multi-Tenant – Sentinel Workspace manager or Azure Lighthouse (next slides)

# 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.*



# 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.

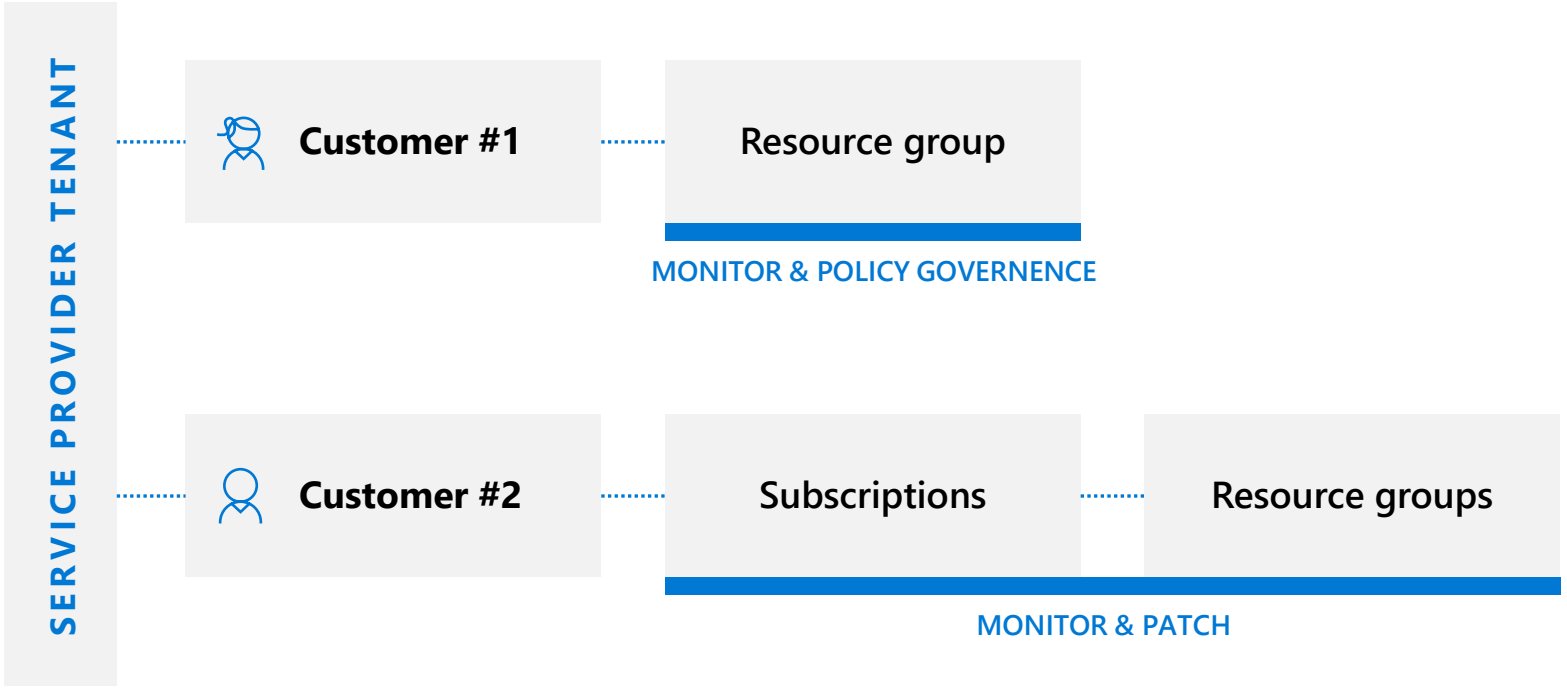
# Manage workspaces across tenants using Azure Lighthouse

## 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

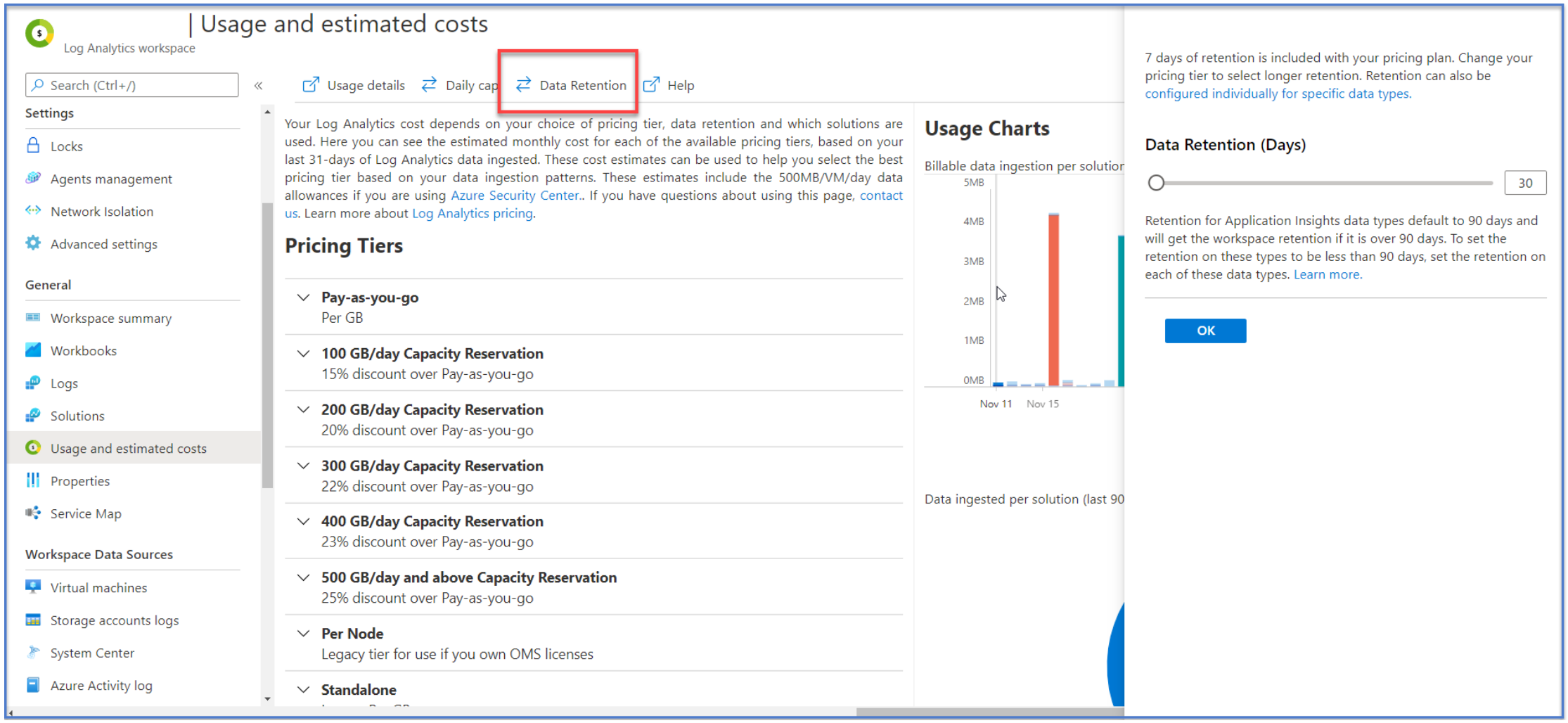
- Working with playbooks to automate responses to threats
- Giving Microsoft Sentinel permissions to run playbooks
- Connecting data sources to Microsoft Sentinel
- Guest users assigning incidents
- Creating and deleting workbooks

## 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

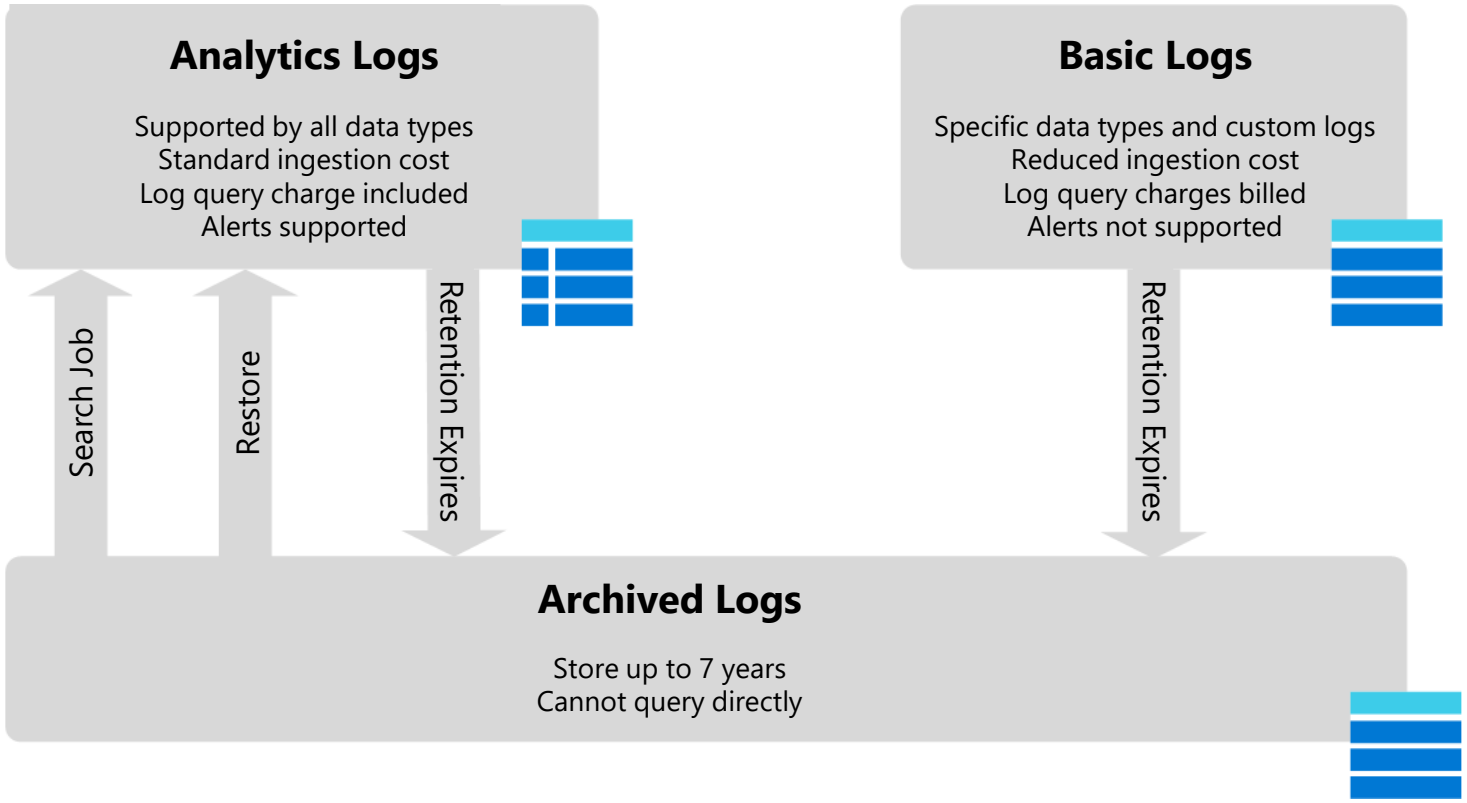
## Microsoft Sentinel environment settings are managed in two areas. In Microsoft Sentinel and in the Log Analytics workspace where Microsoft Sentinel resides. To configure Data Retention:



# 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

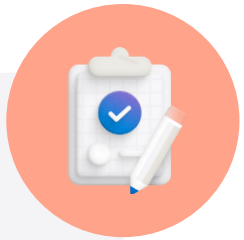
**2** **Which Microsoft Sentinel security role can create workbooks?**

- ☐ 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

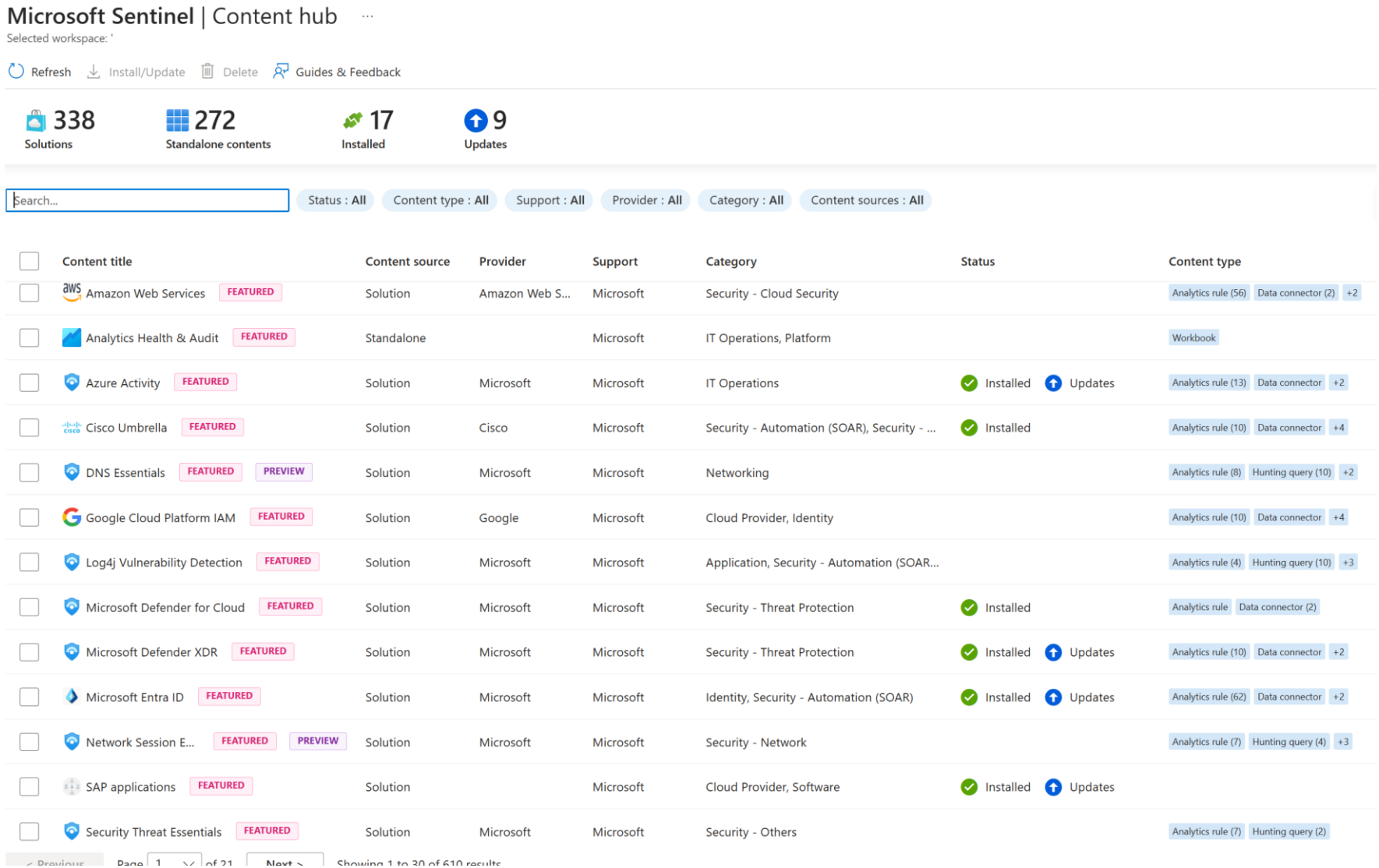
# Introduction

- 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

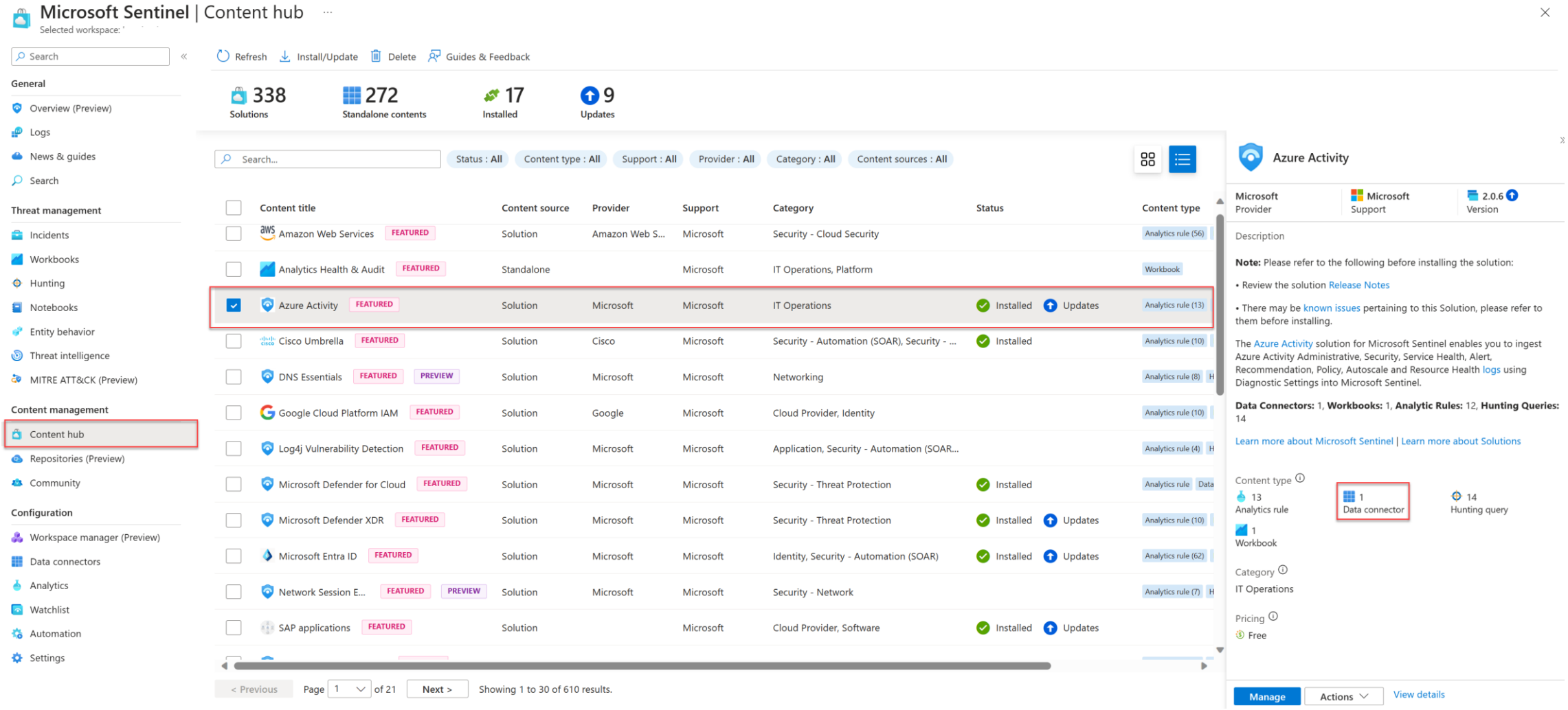
## Solutions can include:

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



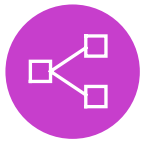
# Ingest log data with Data connectors

## 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.



# 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.

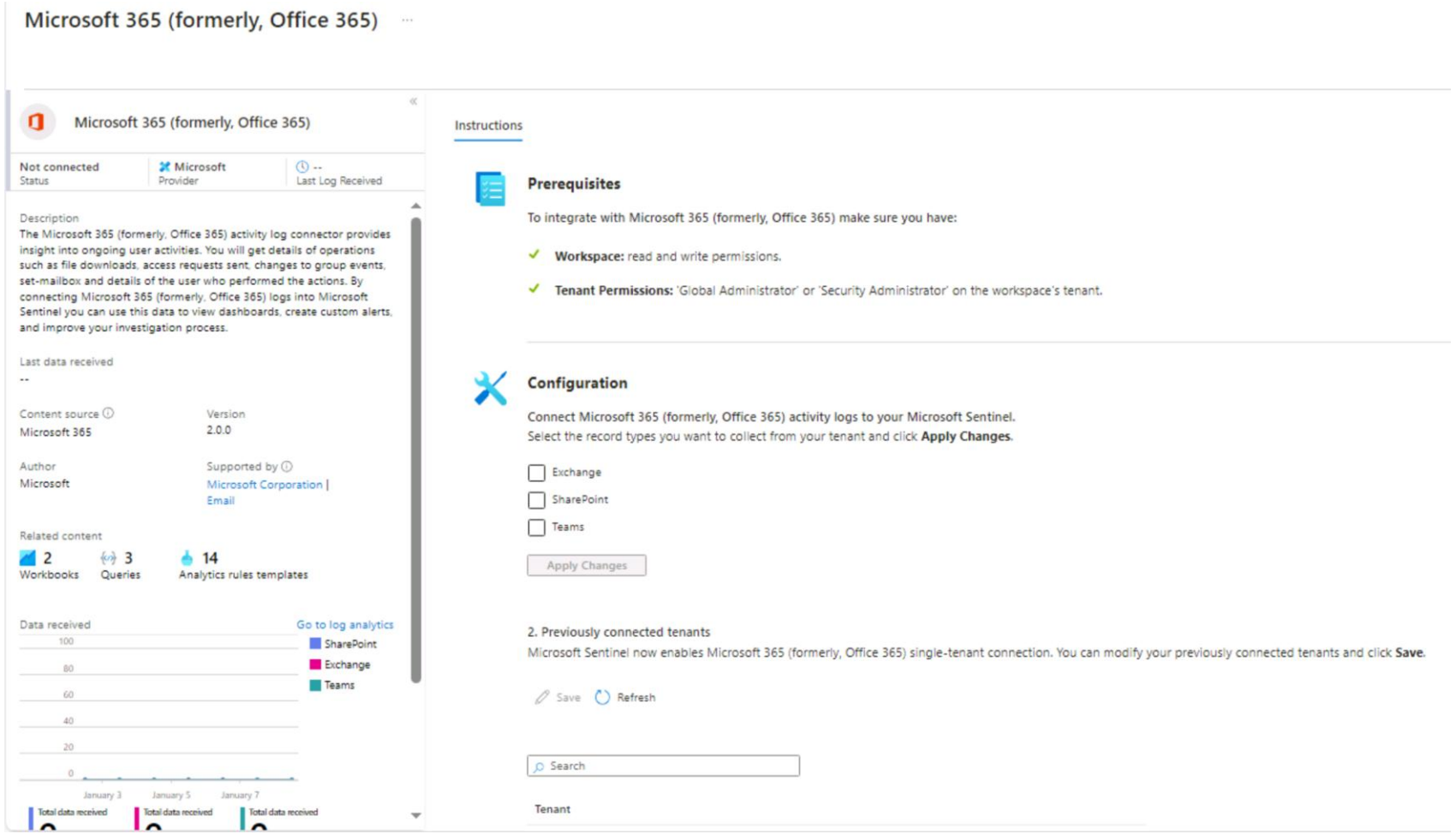
**Azure Activity:** The Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure.

# 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**.

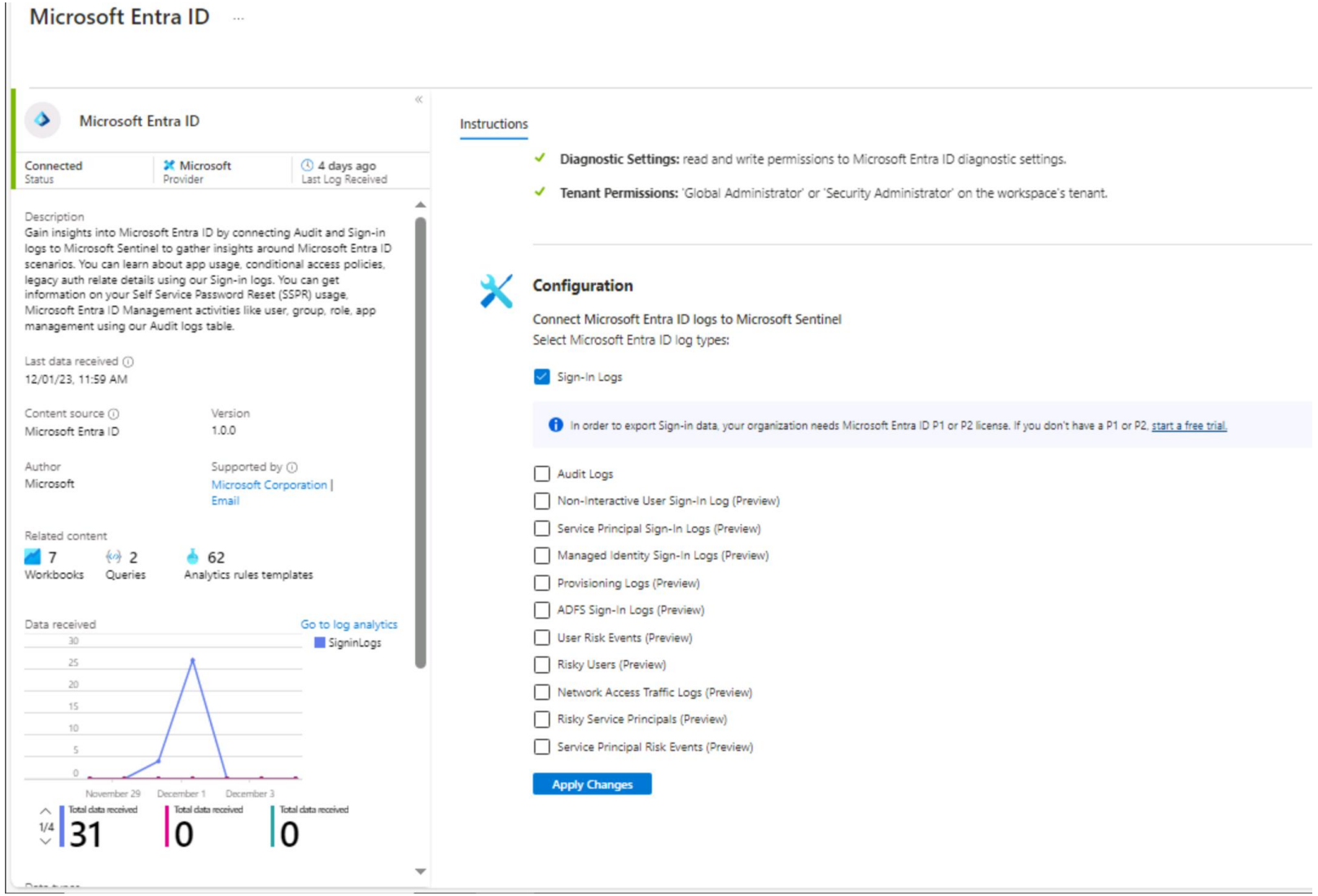


# Connect the Microsoft Entra ID connector

**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**.

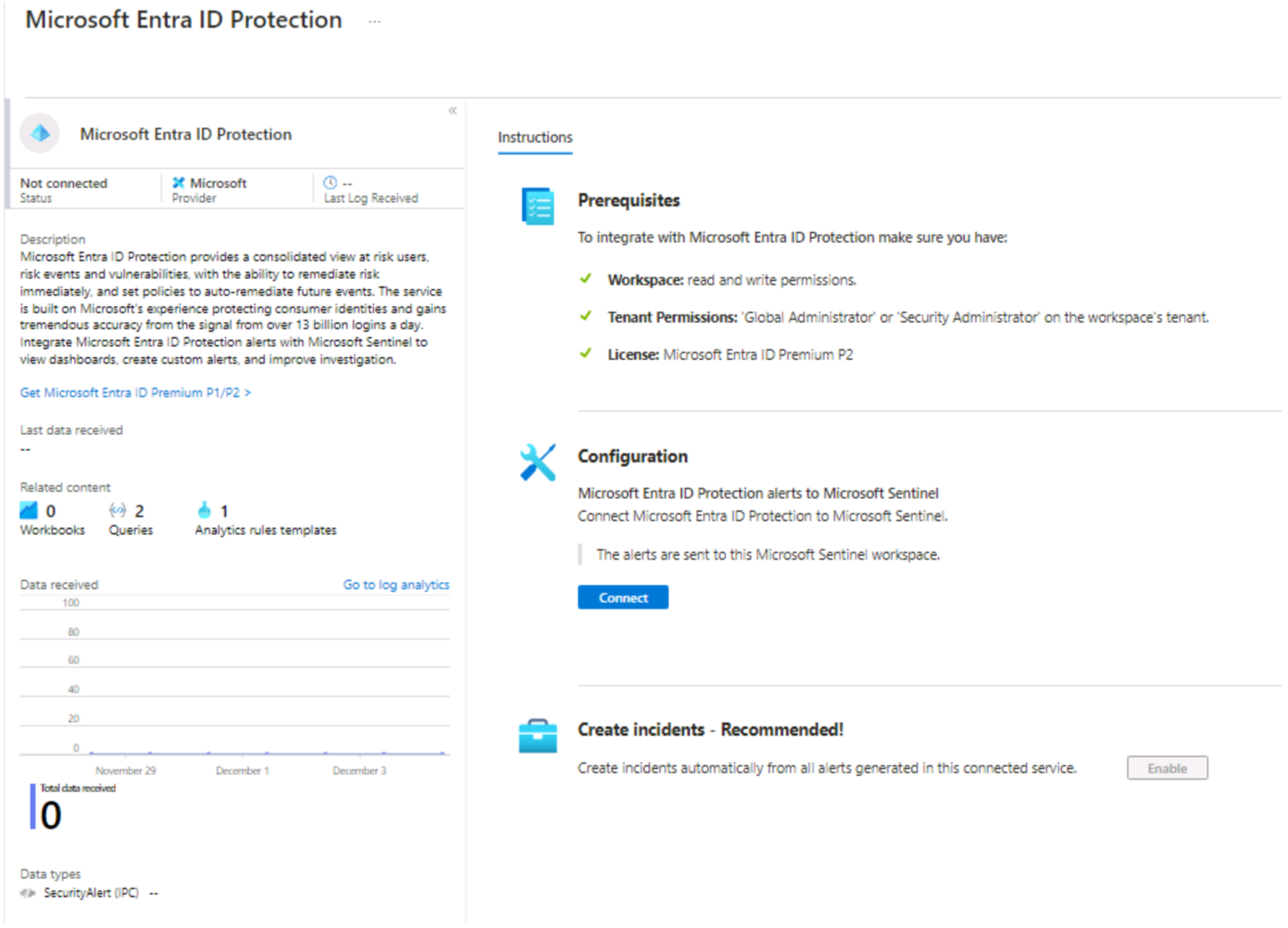


# Connect the Microsoft Entra ID Protection connector

**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.**

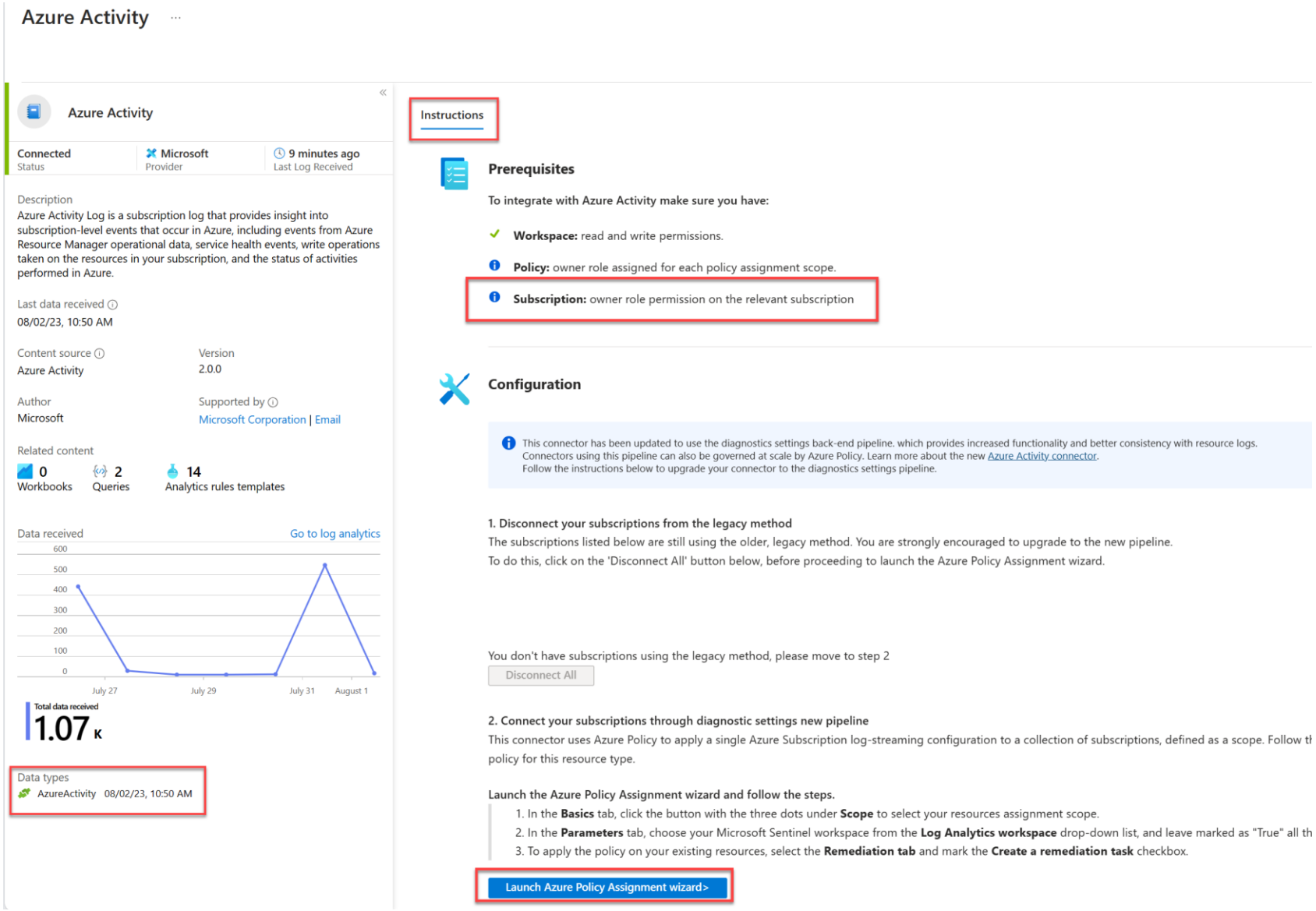
To view the connector page, do these steps:

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**.



# 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.



# Knowledge check

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

- ☐ OfficeActivity
- ☐ SigninLogs
- ☐ SecurityAlert

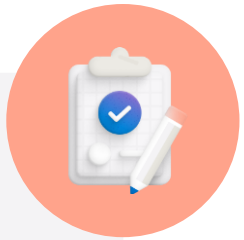
**2** **Which table (data type) would you query for the Microsoft 365 data?**

- ☐ 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 autocreate 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 Windows devices using the provided to the Microsoft Sentinel data connectors. The connectors offers 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

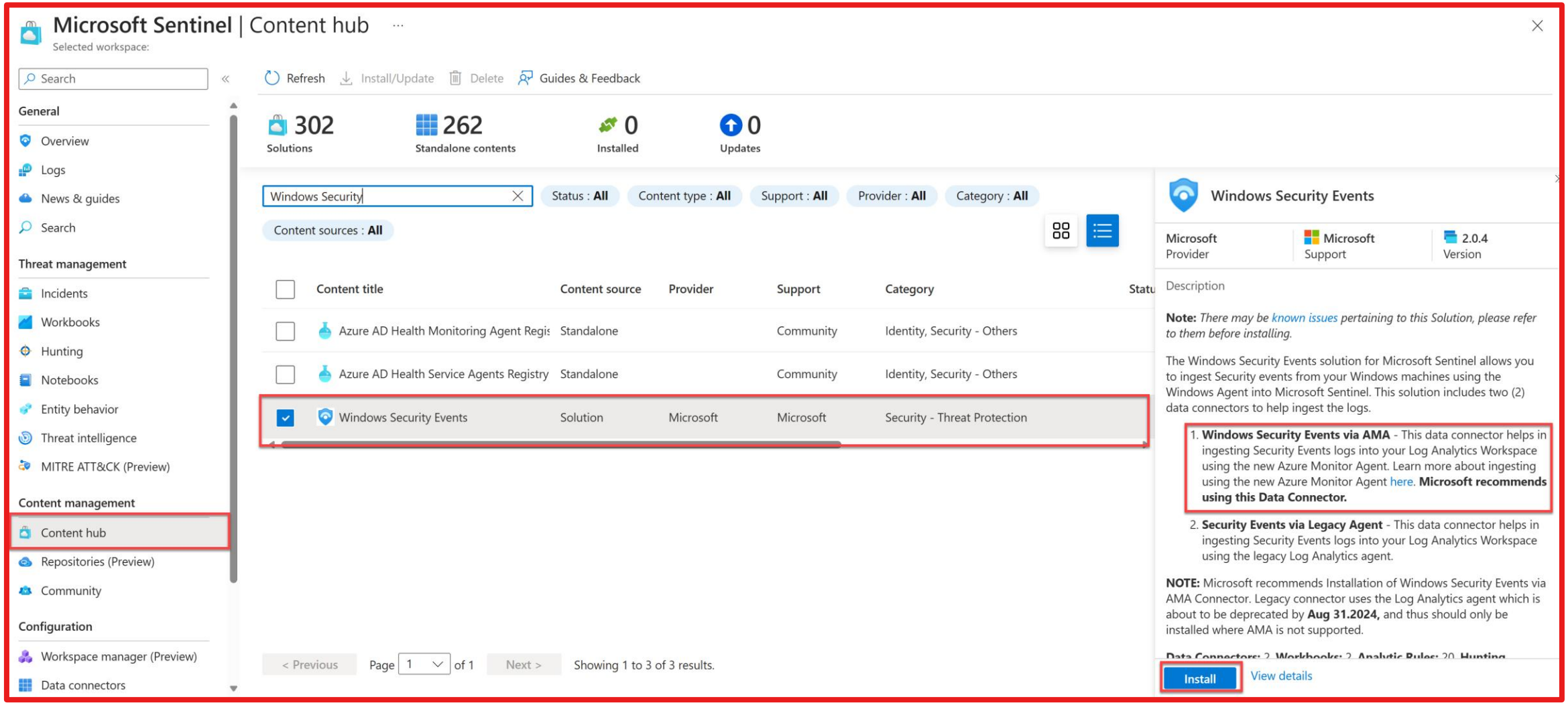
**Limitations:**

- 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

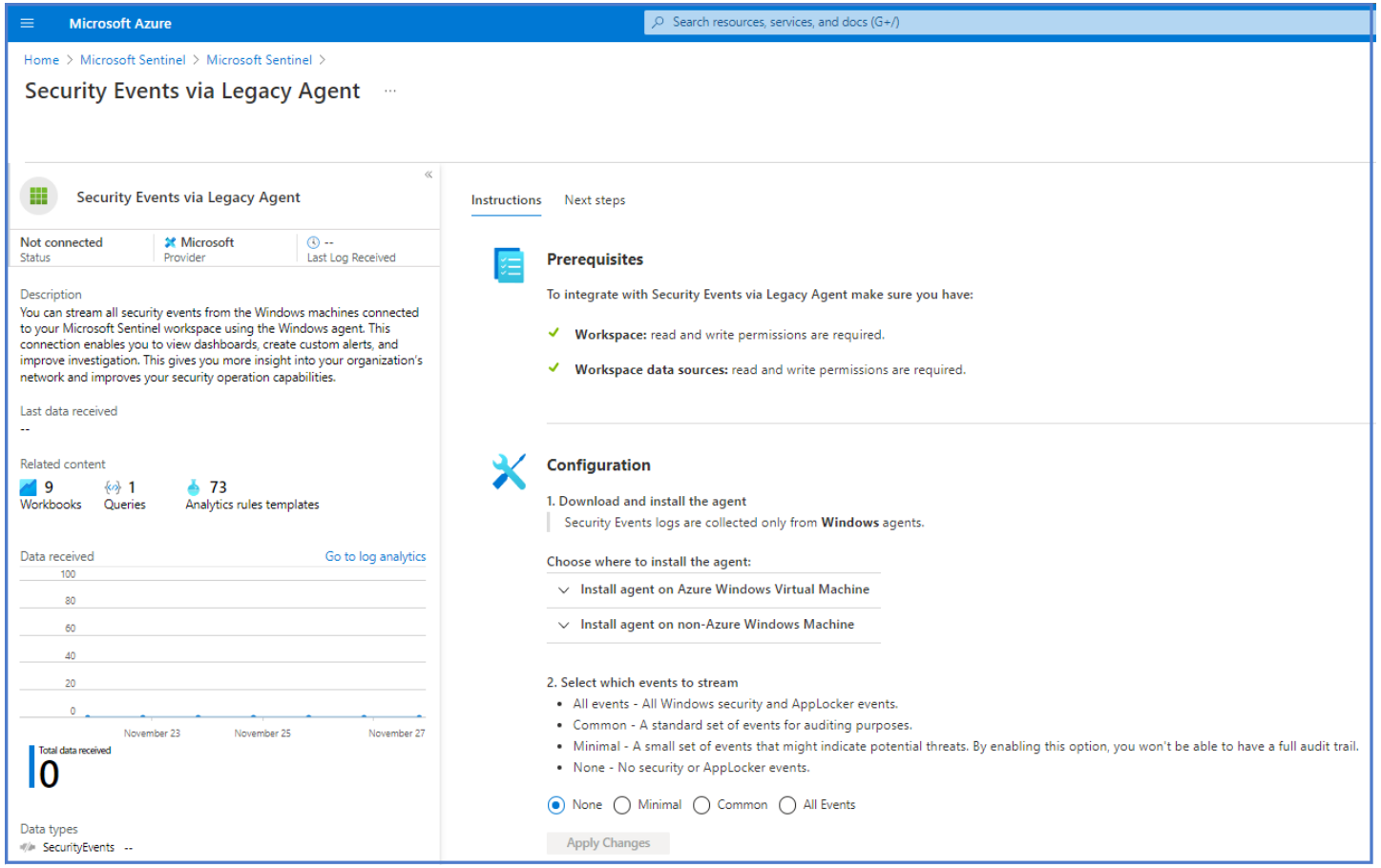


# Connect using the Security Events via Legacy Agent Connector

**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:

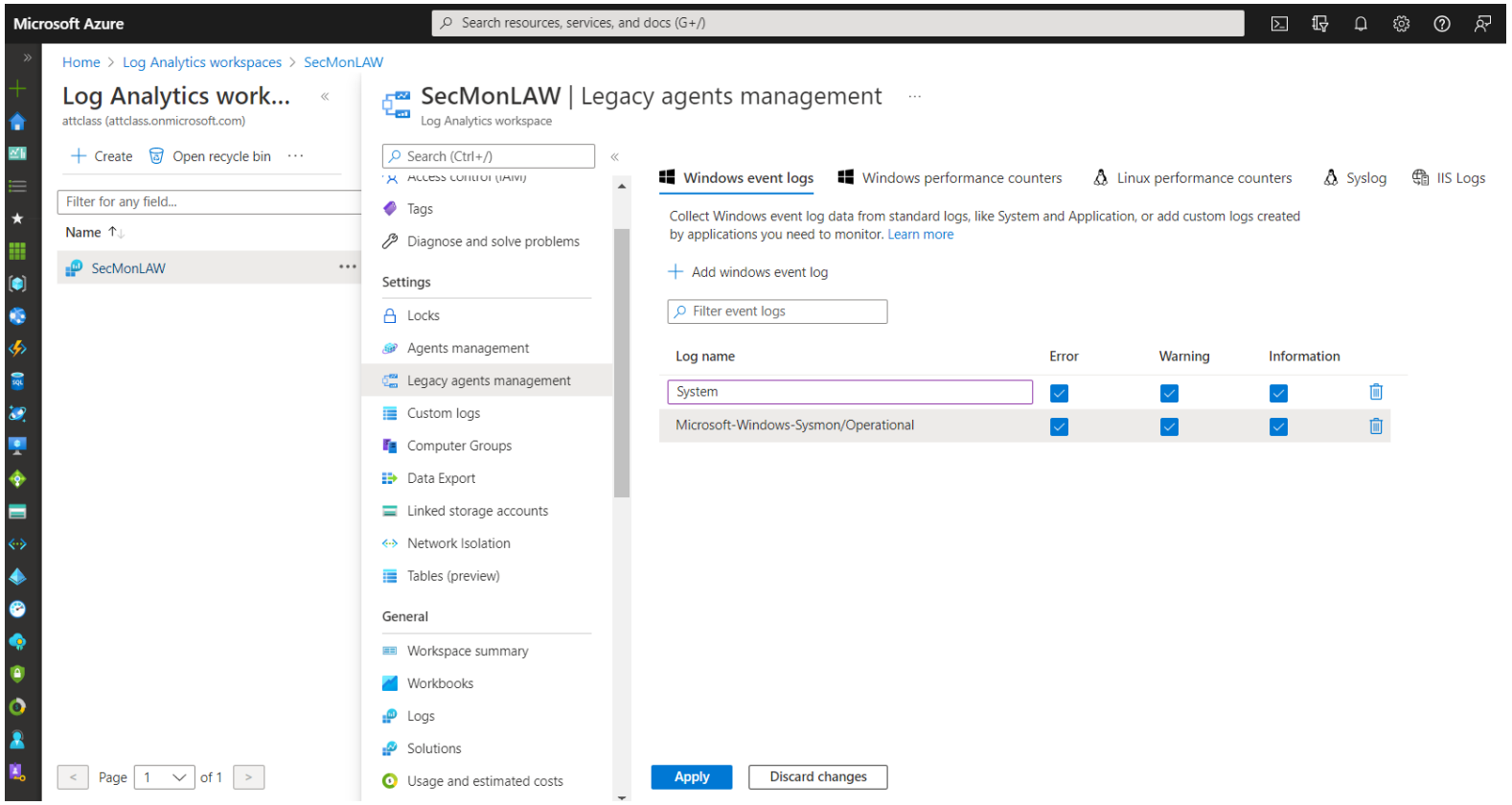
- All events
- Common
- Minimal
- None



# 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.



# Knowledge check

**1** **Which connector do you use to collect Windows security events?**

- ☐ Windows Security Events via AMA
- ☐ Common Event Format
- ☐ Syslog

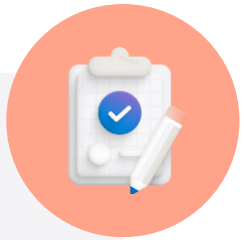
**2** **To collect Sysmon events with the Security Events via Legacy Agent connector, what is the log name used to collect it in advanced settings?**

- ☐ 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

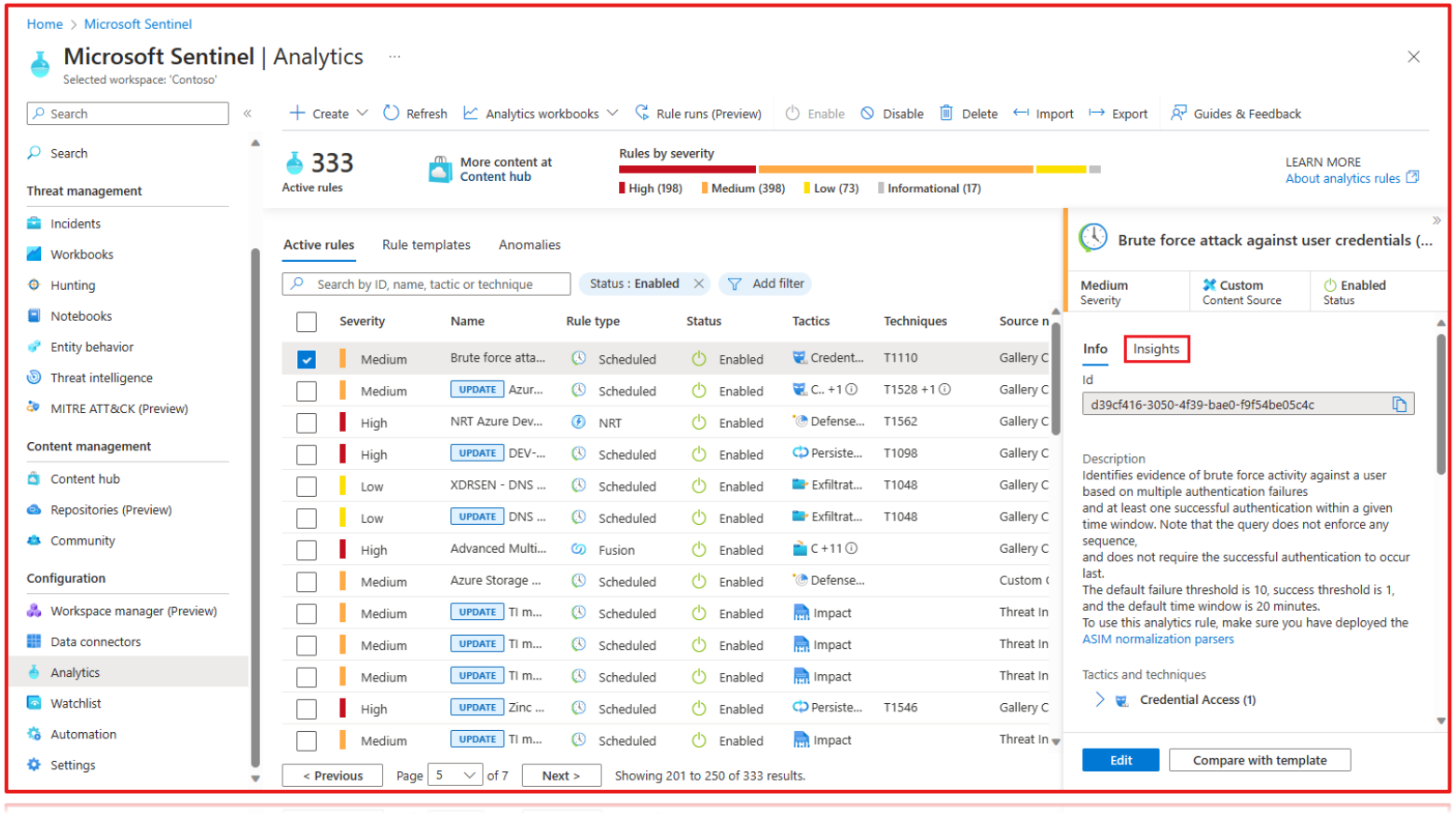
- Microsoft Sentinel Analytics provides an intelligent solution that you can use to detect potential threats and vulnerabilities in your organizations.
- In this module, you'll understand the importance of using Microsoft Sentinel Analytics, create, and implement analytics rules from existing templates, 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.**

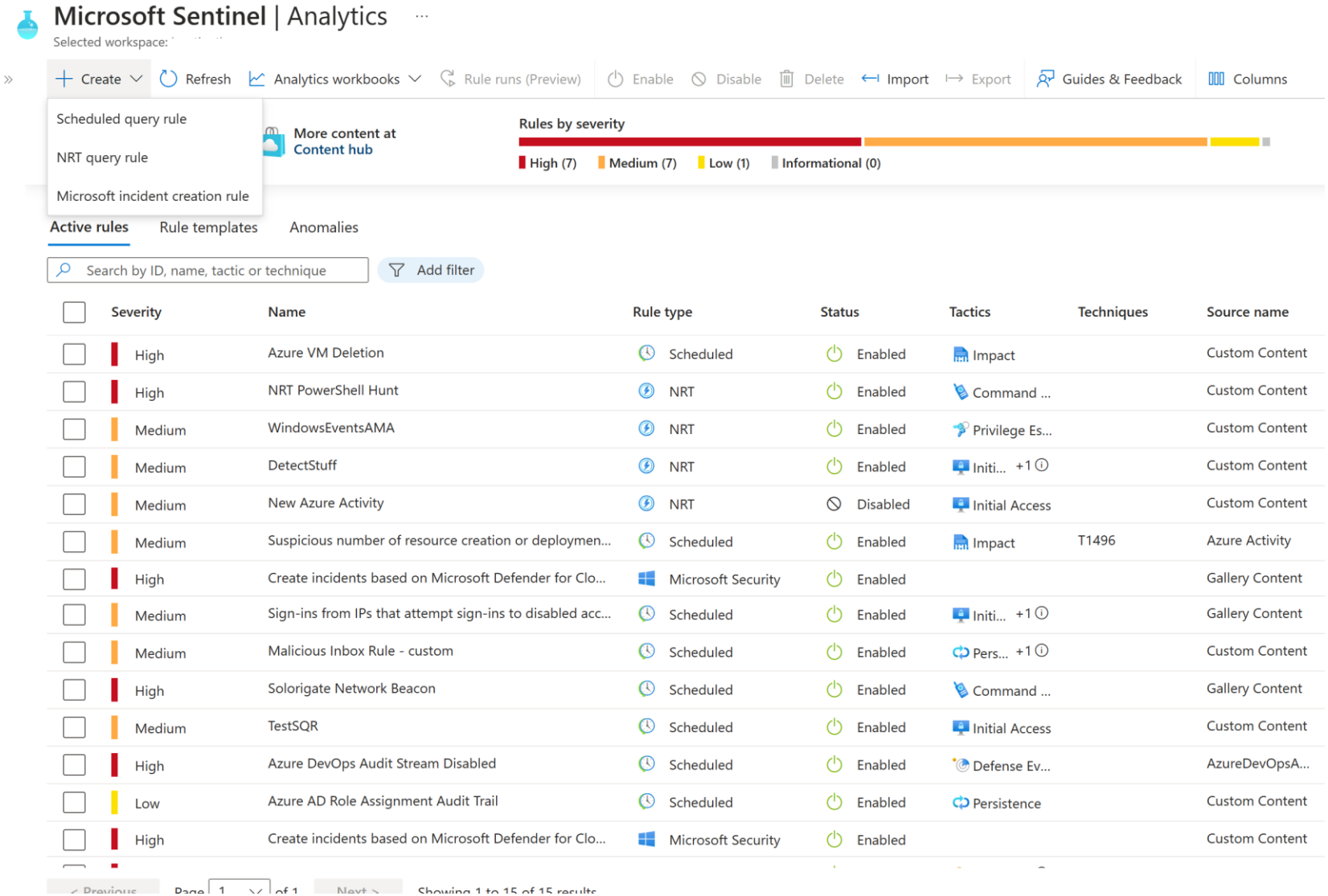
**With the proper analytics rule, you can get insights into where an attack originated from, what resources were compromised, potential data lost, along with the timeline for the incident.**

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



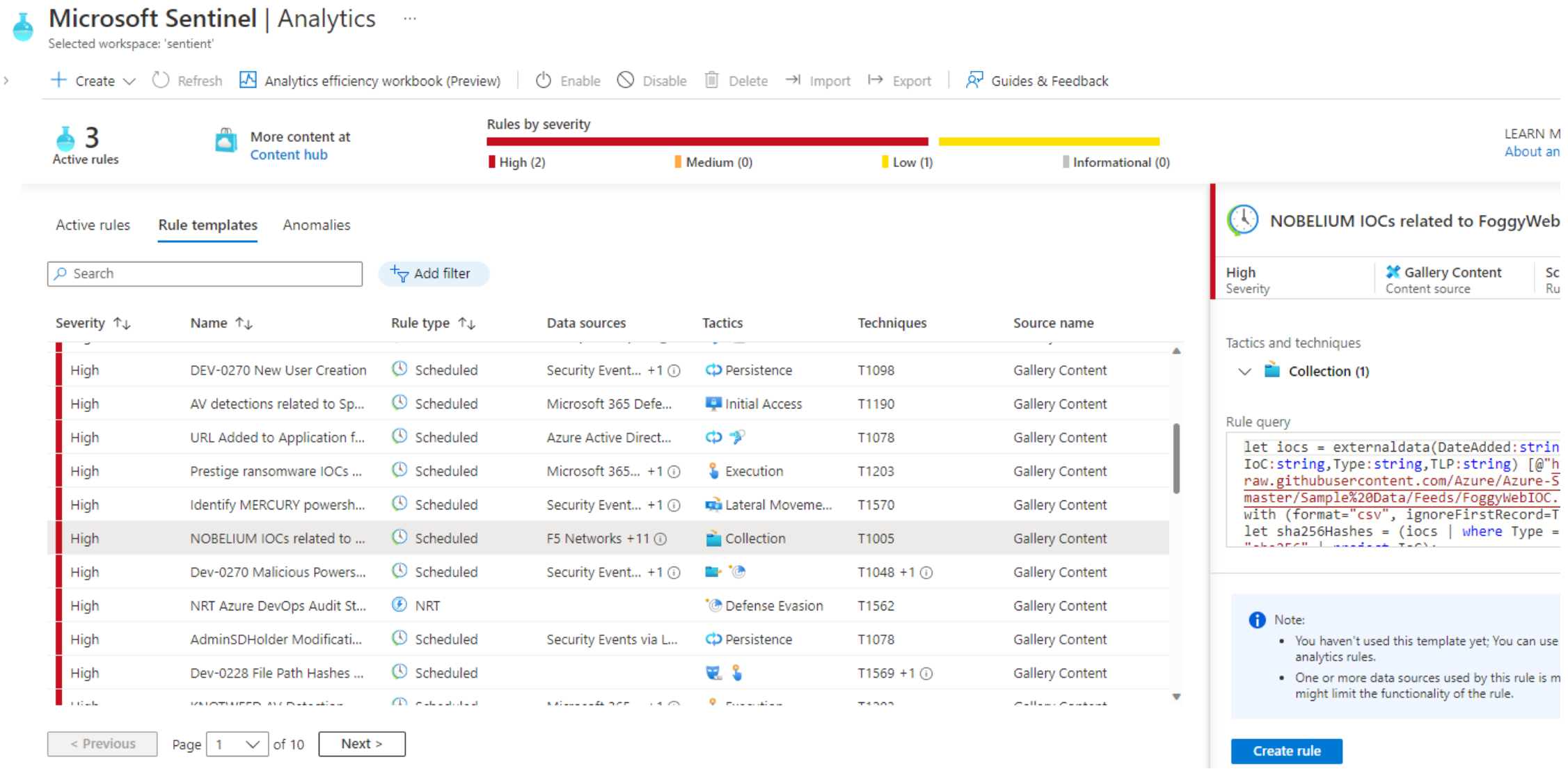
# Types of analytics rules

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



# Create an analytics rule from a template: Gallery Content rules

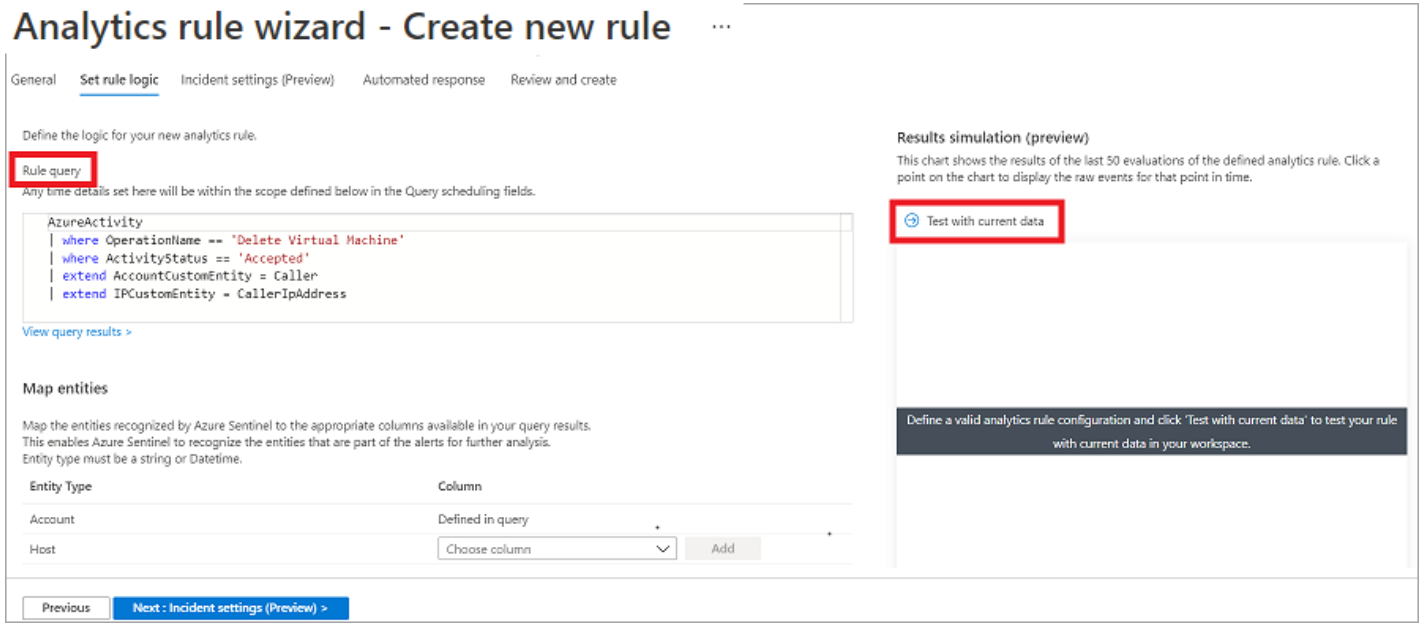
## Note: many Content Hub Solutions install analytic rule templates



# Create an analytics rule from a wizard

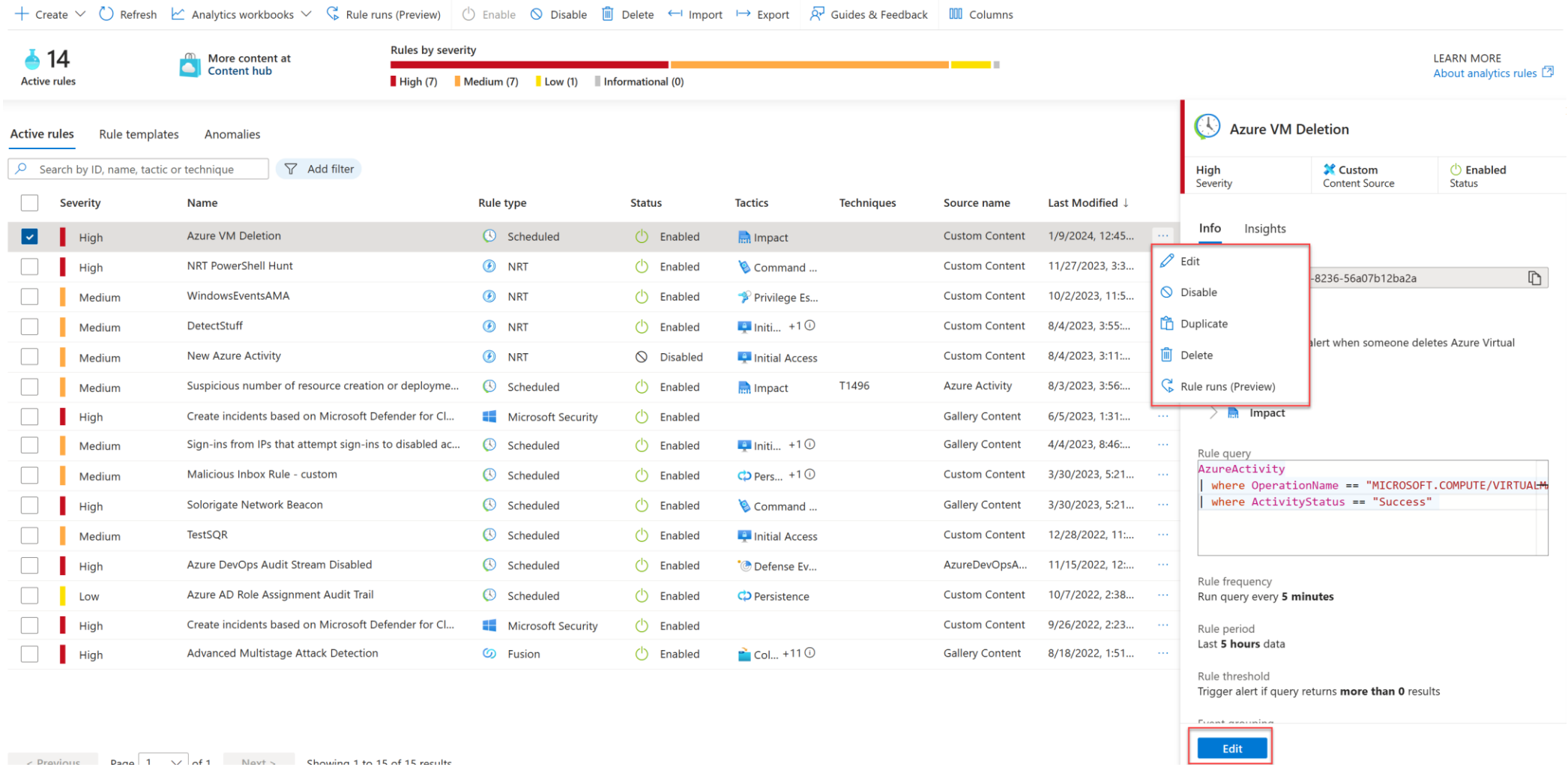
**Creating a custom rule from a scheduled query rule type provides you with the highest level of customization. You can define your own KQL code, set a schedule to run an alert, and provide an automated action by associating the rule with a Microsoft Sentinel Playbook.**

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**.



# 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.**



# 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.

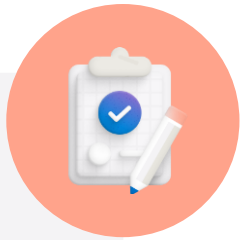
## Duplicate rules:

- 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

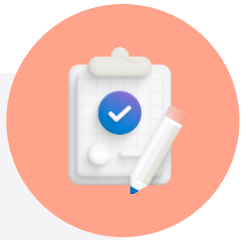
**2** **You use a Logic Apps to create a_?**

- ☐ 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

Microsoft

Swiss Post Cybersecurity

# Thank you.

Microsoft Solutions Partner
Security
Specialist
Threat Protection