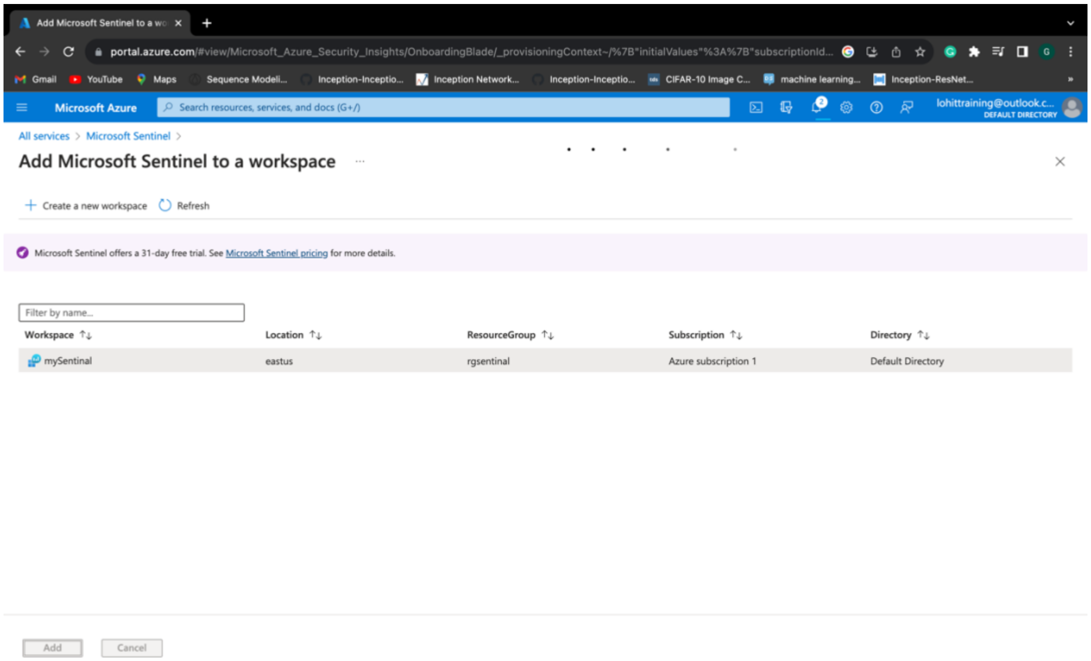
Configuring Microsoft Sentinel to Ingest data and Detect Threats

Step 1: I started by creating a log analytic workspace to add my in-Sentinel workspace



portal.azure.com/#view/Microsoft_Azure_Security_Insights/OnboardingBlade/_provisioningContext~/%7B"initialValues"%3A%7B"subscriptionId...

All services > Microsoft Sentinel >

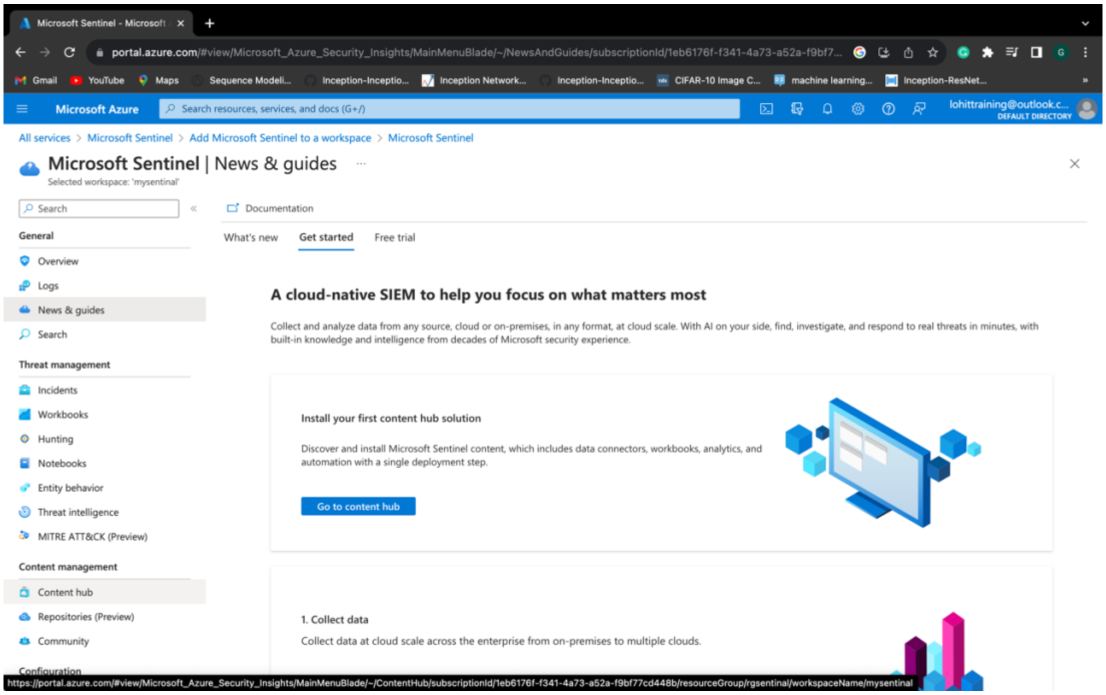
Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
mySentinal	eastus	rgsentinal	Azure subscription 1	Default Directory

Step 2: Install hub content solutions



portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/NewsAndGuides/subscriptionId/1eb6176f-f341-4a73-a52a-f9bf7...

All services > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | News & guides

Selected workspace: 'mysentinal'

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

Install your first content hub solution

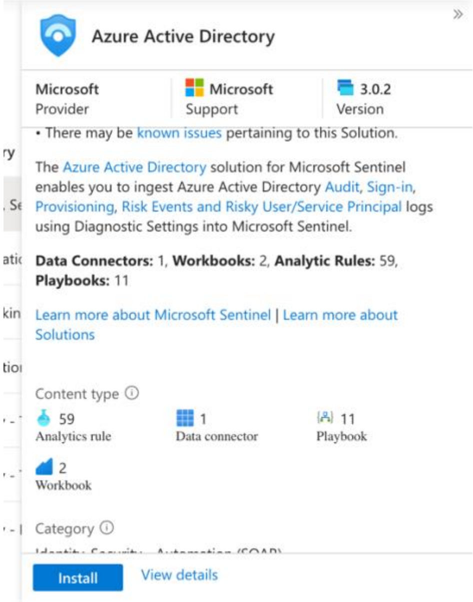
Discover and install Microsoft Sentinel content, which includes data connectors, workbooks, analytics, and automation with a single deployment step.

1. Collect data

Collect data at cloud scale across the enterprise from on-premises to multiple clouds.

https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/ContentHub/subscriptionId/1eb6176f-f341-4a73-a52a-f9bf77cd448b/resourceGroup/rgsentinal/workspaceName/mysentinal

In this step, I installed four Microsoft offered solutions which are mentioned below Starting with *Microsoft Azure Active Directory* for identity and access management data



Microsoft Provider	Microsoft Support	3.0.2 Version

• There may be known issues pertaining to this Solution.

The Azure Active Directory solution for Microsoft Sentinel enables you to ingest Azure Active Directory Audit, Sign-in, Provisioning, Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, **Workbooks:** 2, **Analytic Rules:** 59, **Playbooks:** 11

Learn more about Microsoft Sentinel | Learn more about Solutions

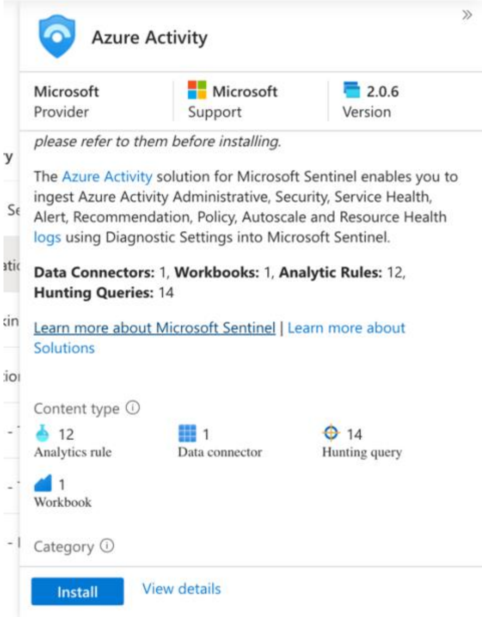
Content type

59 Analytics rule
1 Data connector
11 Playbook
2 Workbook

Category

Identity, Security - Automation (SOAR)

Then *Microsoft Azure Activity* for creating policy that should be followed



Microsoft Provider	Microsoft Support	2.0.6 Version

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

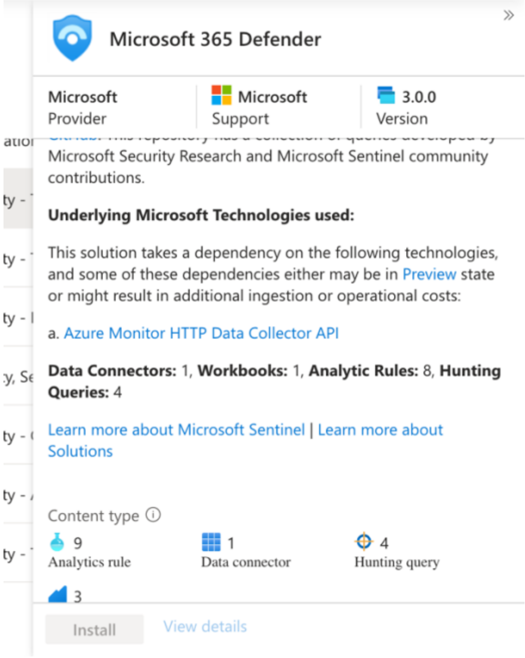
Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

12 Analytics rule
1 Data connector
14 Hunting query
1 Workbook

Category

Microsoft Defender 365



Microsoft 365 Defender

Microsoft Provider	Microsoft Support	3.0.0 Version

Microsoft Security Research and Microsoft Sentinel community contributions.

Underlying Microsoft Technologies used:

This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:

a. Azure Monitor HTTP Data Collector API

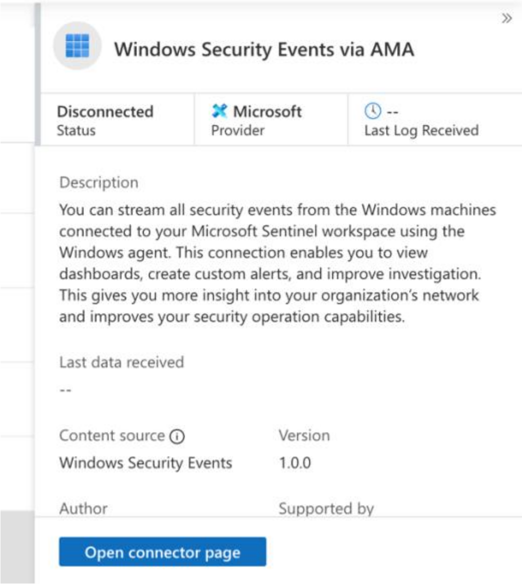
Data Connectors: 1, **Workbooks:** 1, **Analytic Rules:** 8, **Hunting Queries:** 4

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type ⓘ

9 Analytics rule	1 Data connector	4 Hunting query
3		

Windows Security Event.



Windows Security Events via AMA

Disconnected Status	Microsoft Provider	-- Last Log Received

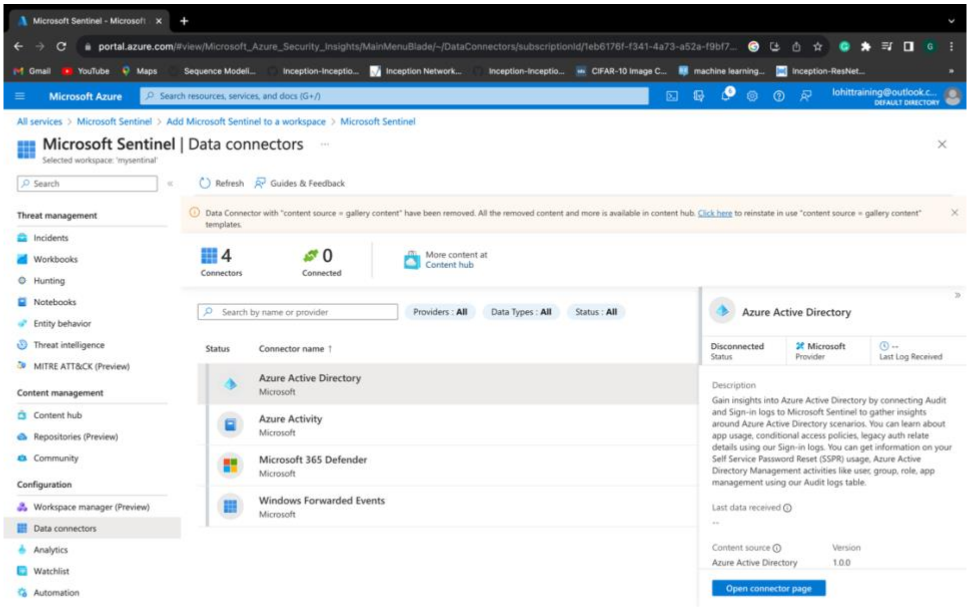
Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

--

Content source ⓘ	Version
Windows Security Events	1.0.0
Author	Supported by



Microsoft Sentinel | Data connectors

Selected workspace: 'mysentinal'

Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.

4 Connectors | 0 Connected | More content at Content hub

Search by name or provider | Providers : All | Data Types : All | Status : All

Status	Connector name ↑
	Azure Active Directory Microsoft
	Azure Activity Microsoft
	Microsoft 365 Defender Microsoft
	Windows Forwarded Events Microsoft

Azure Active Directory

Disconnected Status | Microsoft Provider | -- Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

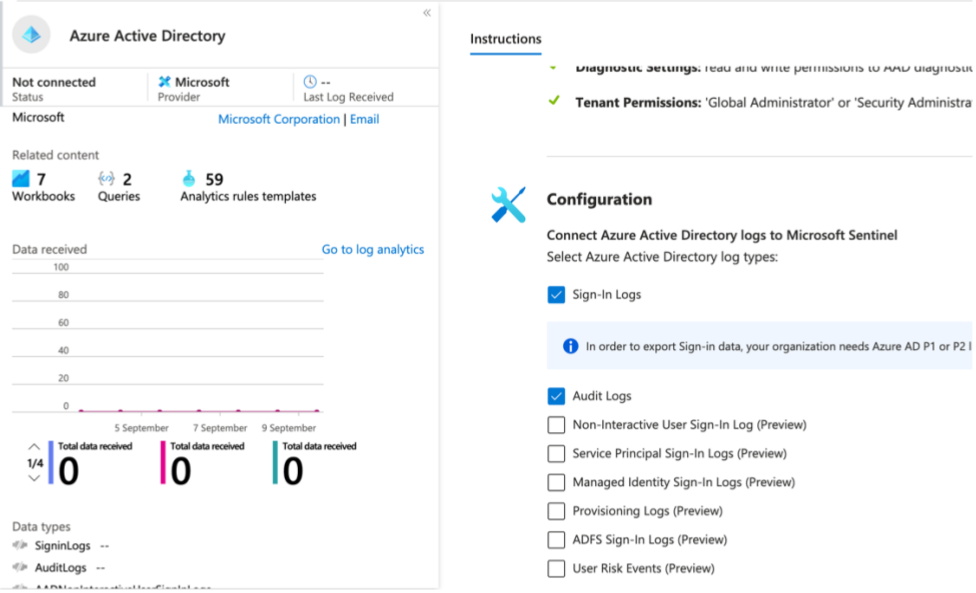
Last data received

--

Content source: Azure Active Directory

Version: 1.0.0

Step 3: I explored for a little while and then I started configuring data connectors, starting with Active directory, which enables a check box configuration. Here I get to choose the types of data I want ingested.



Azure Active Directory

Not connected Status | Microsoft Provider | -- Last Log Received

Microsoft | Microsoft Corporation | Email

Related content

7 Workbooks | 2 Queries | 59 Analytics rules templates

Data received

Total data received 0 | Total data received 0 | Total data received 0

Data types

SigninLogs --

AuditLogs --

Diagnostic Settings: read and write permissions to AAD diagnostic

✓ Tenant Permissions: 'Global Administrator' or 'Security Administra

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel

Select Azure Active Directory log types:

☑ Sign-In Logs

In order to export Sign-in data, your organization needs Azure AD P1 or P2 l

☑ Audit Logs

□ Non-Interactive User Sign-In Log (Preview)

□ Service Principal Sign-In Logs (Preview)

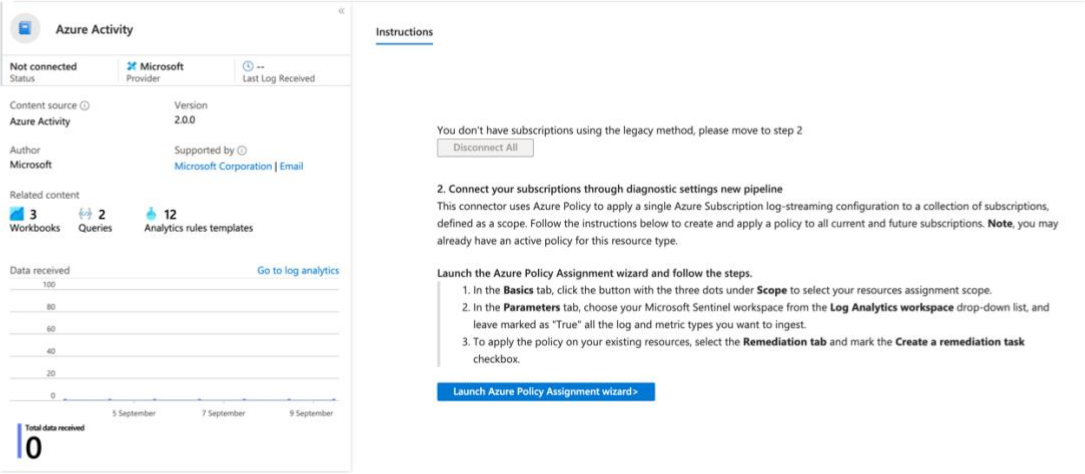
□ Managed Identity Sign-In Logs (Preview)

□ Provisioning Logs (Preview)

□ ADFS Sign-In Logs (Preview)

□ User Risk Events (Preview)

Next, I moved on to Azure activity, which is a little different from the connectors. For this, I needed to create a policy that the organization must comply to.



Azure Activity

Not connected
Status

Microsoft
Provider

--
Last Log Received

Content source
Azure Activity

Version
2.0.0

Author
Microsoft

Supported by
Microsoft Corporation | Email

Related content
3 Workbooks
2 Queries
12 Analytics rules templates

Data received

Total data received
0

Instructions

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

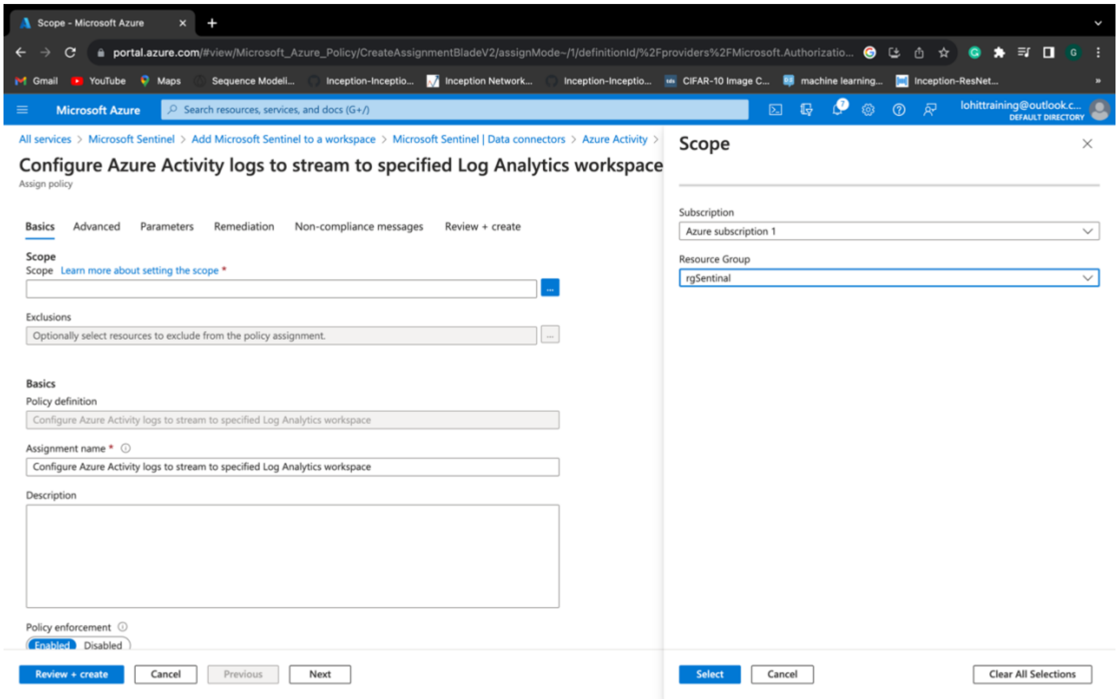
2. Connect your subscriptions through diagnostic settings new pipeline

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 instructions below to create and apply a policy to all current and future subscriptions. **Note**, you may already have an active policy for this resource type.

Launch the Azure Policy Assignment wizard and follow the steps.

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

Once redirected, I had to figure out the scope and parameters of the policy which can be done by selecting the respected resource group



Scope - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Policy/CreateAssignmentBladeV2/assignMode~/1/definitionId/%2Fproviders%2FMicrosoft.Authorizatio...

All services > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Scope

Scope Learn more about setting the scope *

Exclusions: Optionally select resources to exclude from the policy assignment.

Basics

Policy definition: Configure Azure Activity logs to stream to specified Log Analytics workspace

Assignment name *: Configure Azure Activity logs to stream to specified Log Analytics workspace

Description

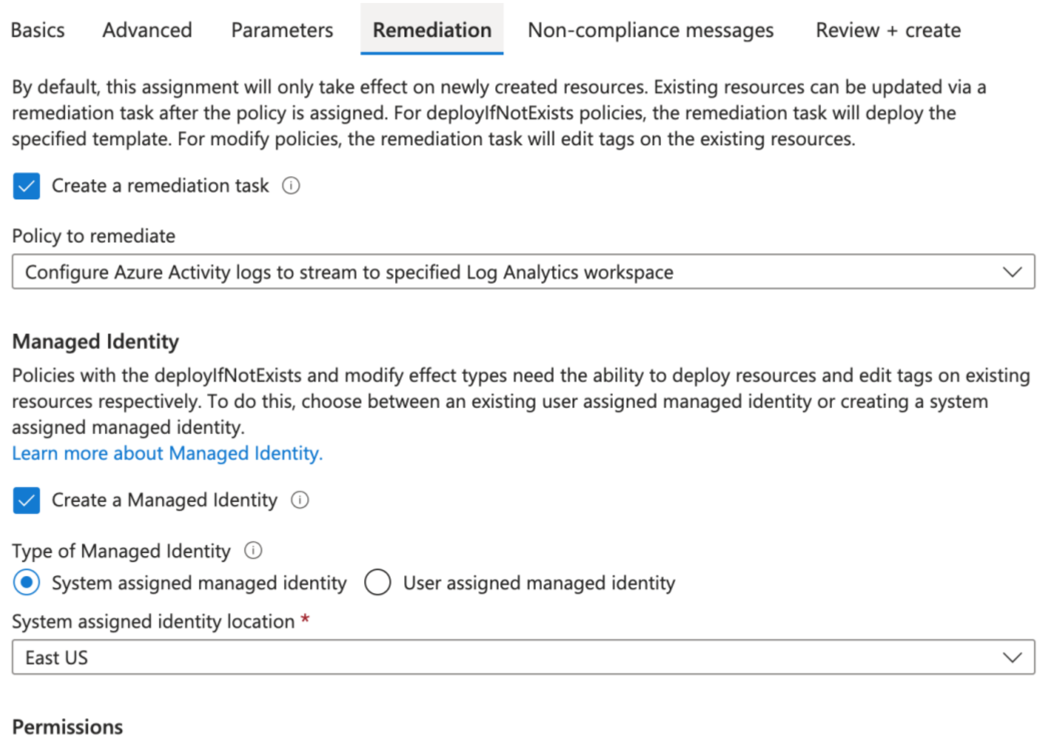
Policy enforcement: Enabled Disabled

Scope

Subscription: Azure subscription 1

Resource Group: rgSentinal

One of the most important settings here was remediation. Meaning if you want to implement this policy starting with the new devices or for all the previously existing devices as well. Remediation allows to include previous devices into the policy which by default would not be included.



By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

☑ Create a remediation task

Policy to remediate: Configure Azure Activity logs to stream to specified Log Analytics workspace

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity.
Learn more about Managed Identity.

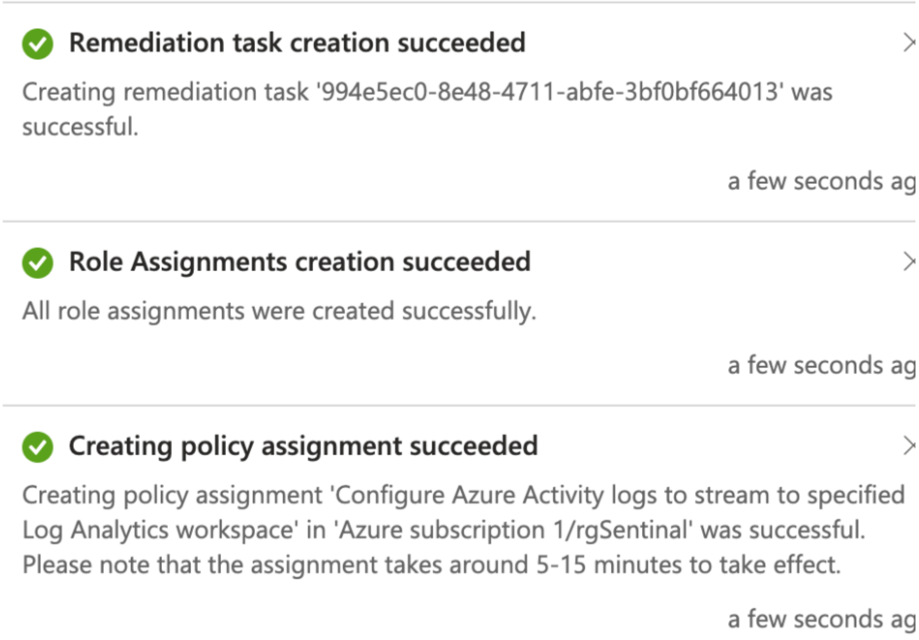
☑ Create a Managed Identity

Type of Managed Identity
● System assigned managed identity ○ User assigned managed identity

System assigned identity location *: East US

Permissions

Once all the setting we configured, I then submitted my configurations. It took some time, but I got the successful creation message.



Remediation task creation succeeded

Creating remediation task '994e5ec0-8e48-4711-abfe-3bf0bf664013' was successful.

a few seconds ag

Role Assignments creation succeeded

All role assignments were created successfully.

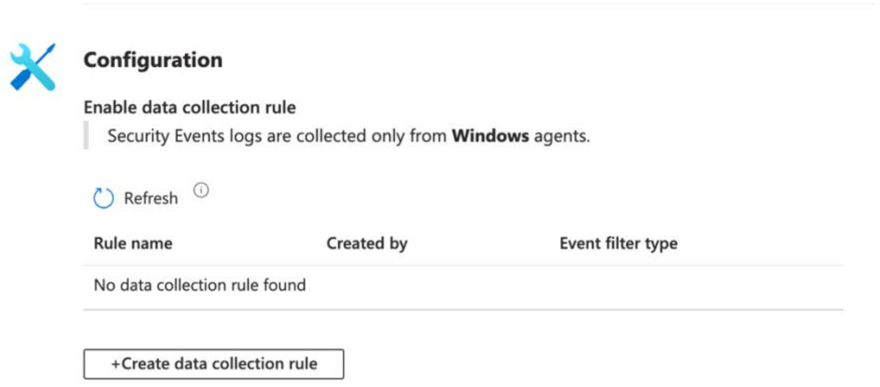
a few seconds ag

Creating policy assignment succeeded

Creating policy assignment 'Configure Azure Activity logs to stream to specified Log Analytics workspace' in 'Azure subscription 1/rgSentinal' was successful. Please note that the assignment takes around 5-15 minutes to take effect.

a few seconds ag

Finally, I moved to configure the Windows security events uses *Data collection rules* to collect data. So I had to create a DCR. Here I had an option to choose what kinds of data I wanted to send across which includes all data, alert data or custom.



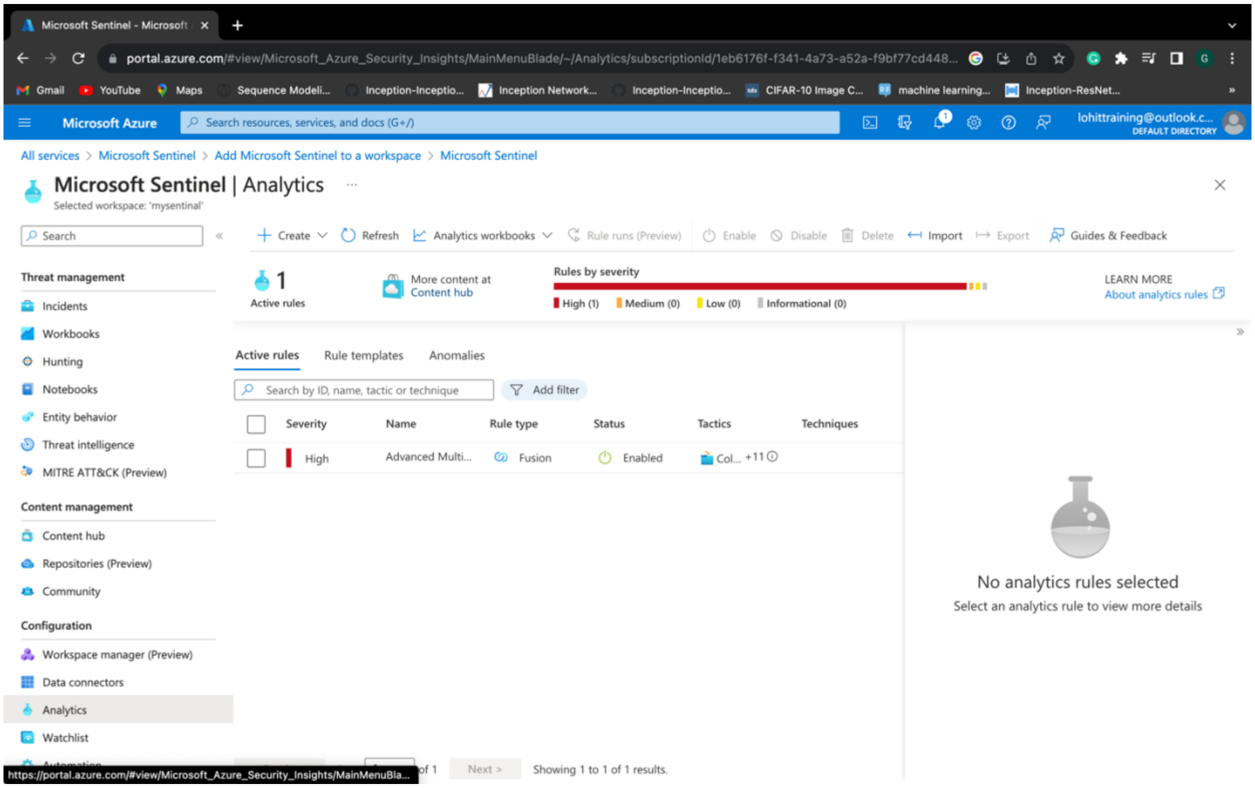
Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Event filter type
No data collection rule found		

Step 4: Now, I started working on enabling and creating analytic rules.



Microsoft Sentinel - Microsoft
portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Analytics/subscriptionId/1eb6176f-f341-4a73-a52a-f9bf77cd448...
Gmail
YouTube
Maps
Sequence Modeli...
Inception-Inceptio...
Inception Network...
Inception-Inceptio...
CIFAR-10 Image C...
machine learning...
Inception-ResNet...
Microsoft Azure
Search resources, services, and docs (G+/)
lohittraining@outlook.c...
DEFAULT DIRECTORY
All services > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'mysentinal'

1 Active rules

More content at Content hub

Rules by severity: High (1) Medium (0) Low (0) Informational (0)

	Severity	Name	Rule type	Status	Tactics	Techniques
□	High	Advanced Multi...	Fusion	Enabled	Col... +11	

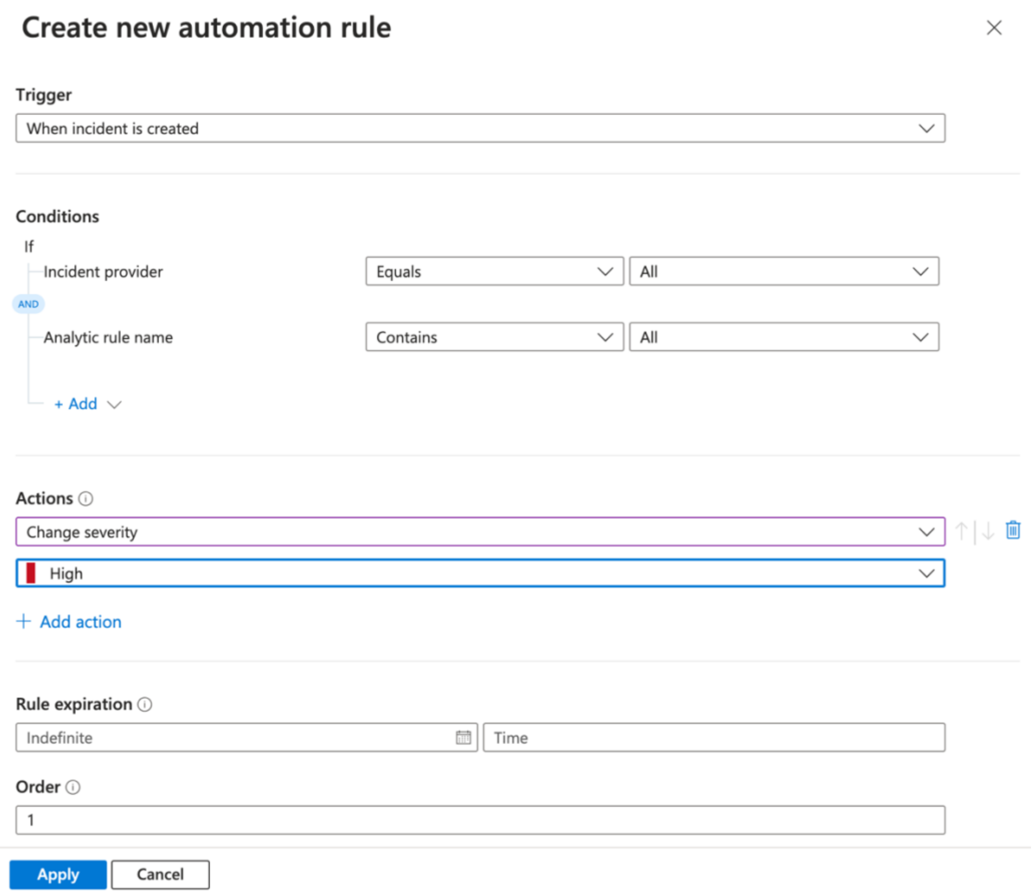
No analytics rules selected

Select an analytics rule to view more details

of 1
Next >
Showing 1 to 1 of 1 results.
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBla...

Here I have had access to a couple of pre-defined templated which were helpful in for the first time in creating these rules. These analytic rules co-relates the data collected from your data connectors and compares them to the rules create to determine its alert based on which incidents are reported.

Step 5: I also wanted to automate a few processes for which I used automation rules. This can also be done while creating analytic rules, but I wanted to do this separately to document.



Create new automation rule

Trigger

When incident is created

Conditions

If

Incident provider — Equals — All

AND

Analytic rule name — Contains — All

+ Add

Actions

Change severity

High

+ Add action

Rule expiration

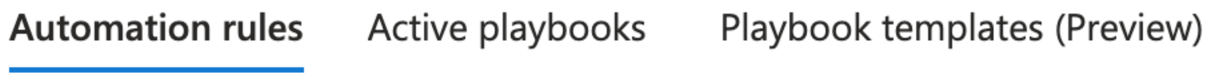
Indefinite — Time

Order

1

Apply Cancel

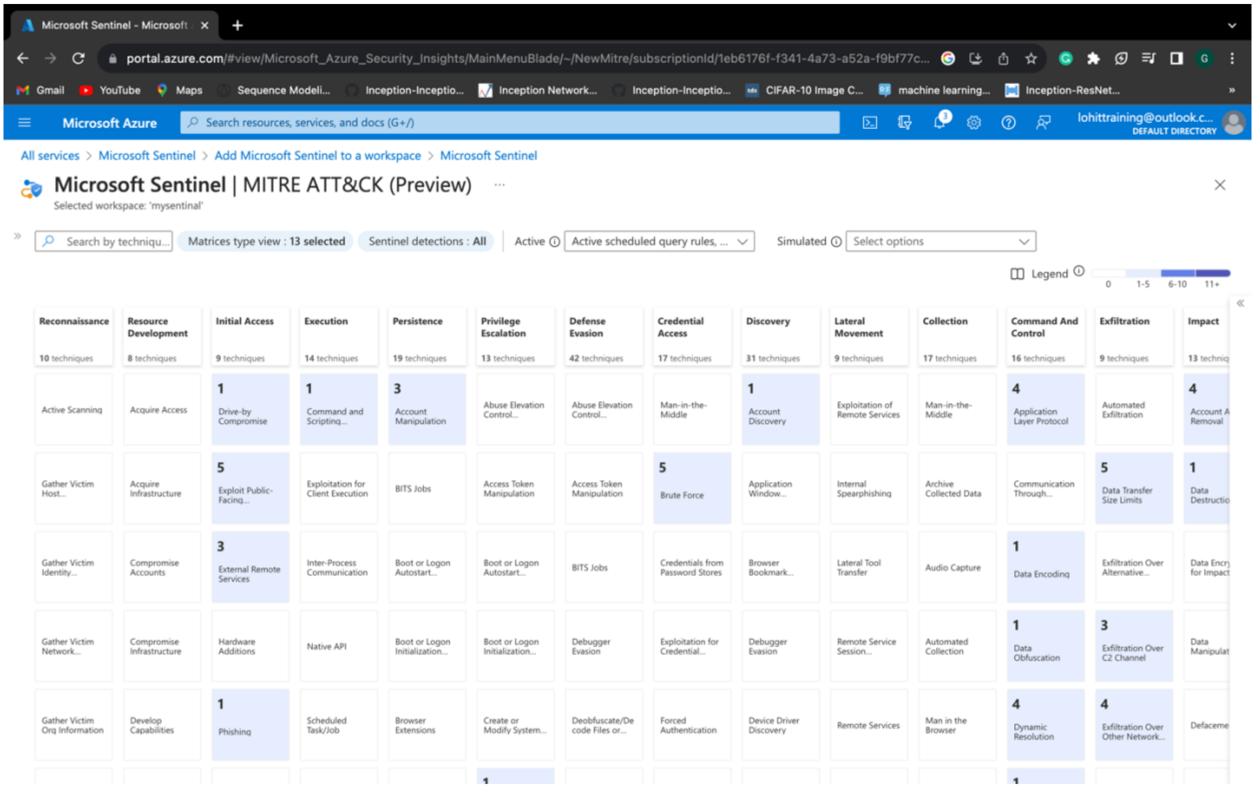
This rule takes the appropriate actions defined by me, based on the logic, which will also be decided by me. I also got to select the time for which this rule can be active.



Automation rules Active playbooks Playbook templates (Preview)

Analytics offers Automation rules and playbooks. Automation rules are easy tasks at management level whereas playbooks use azure logic to allow more control and function related to incident.

Step 6: Once, all that was done I wanted to see the coverage of my security. For this, sentinel has *MITRE ATT&CK*. This provides a cohesive look of your security posture based on the collection all the data from a non-profit organization.



portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/NewMitre/subscriptionId/1eb6176f-f341-4a73-a52a-f9bf77c...

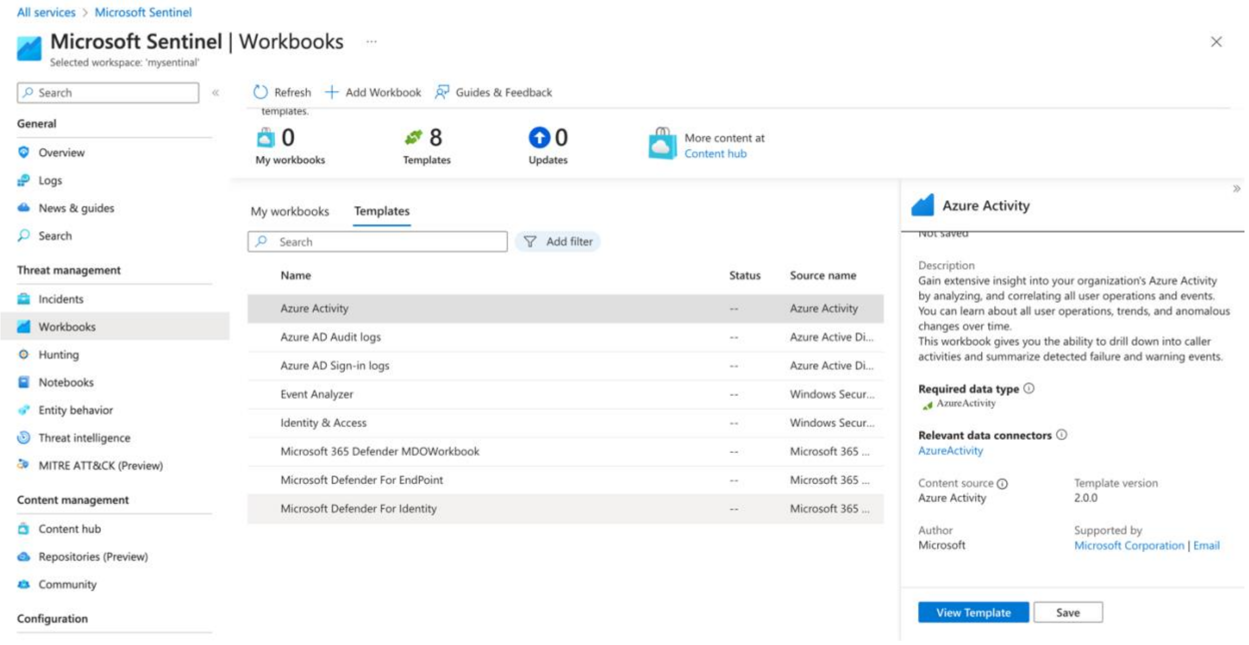
Microsoft Sentinel | MITRE ATT&CK (Preview)

Selected workspace: 'mysentinal'

Matrices type view : 13 selected
Sentinel detections : All
Active: Active scheduled query rules, ...
Simulated: Select options

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command And Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniq
Active Scanning	Acquire Access	1 Drive-by Compromise	1 Command and Scripting...	3 Account Manipulation	Abuse Elevation Control...	Abuse Elevation Control...	Man-in-the-Middle	1 Account Discovery	Exploitation of Remote Services	Man-in-the-Middle	4 Application Layer Protocol	Automated Exfiltration	4 Account A Removal
Gather Victim Host...	Acquire Infrastructure	5 Exploit Public-Facing...	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	5 Brute Force	Application Window...	Internal Spearphishing	Archive Collected Data	Communication Through...	5 Data Transfer Size Limits	1 Data Destructio
Gather Victim Identity...	Compromise Accounts	3 External Remote Services	Inter-Process Communication	Boot or Logon Autostart...	Boot or Logon Autostart...	BITS Jobs	Credentials from Password Stores	Browser Bookmark...	Lateral Tool Transfer	Audio Capture	1 Data Encoding	Exfiltration Over Alternative...	Data Encry for Impact
Gather Victim Network...	Compromise Infrastructure	Hardware Additions	Native API	Boot or Logon Initialization...	Boot or Logon Initialization...	Debugger Evasion	Exploitation for Credential...	Debugger Evasion	Remote Service Session...	Automated Collection	1 Data Obfuscation	3 Exfiltration Over C2 Channel	Data Manipulat
Gather Victim Org Information	Develop Capabilities	1 Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System...	Deobfuscate/Decode Files or...	Forced Authentication	Device Driver Discovery	Remote Services	Man in the Browser	4 Dynamic Resolution	4 Exfiltration Over Other Network...	Defaceme
					1						1		

Step 7:



Microsoft Sentinel | Workbooks

Selected workspace: 'mysentinal'

templates.

0 My workbooks | 8 Templates | 0 Updates

Name	Status	Source name
Azure Activity	--	Azure Activity
Azure AD Audit logs	--	Azure Active Di...
Azure AD Sign-in logs	--	Azure Active Di...
Event Analyzer	--	Windows Secur...
Identity & Access	--	Windows Secur...
Microsoft 365 Defender MDOWorkbook	--	Microsoft 365 ...
Microsoft Defender For EndPoint	--	Microsoft 365 ...
Microsoft Defender For Identity	--	Microsoft 365 ...

Azure Activity

Not saved

Description
Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events. You can learn about all user operations, trends, and anomalous changes over time.
This workbook gives you the ability to drill down into caller activities and summarize detected failure and warning events.

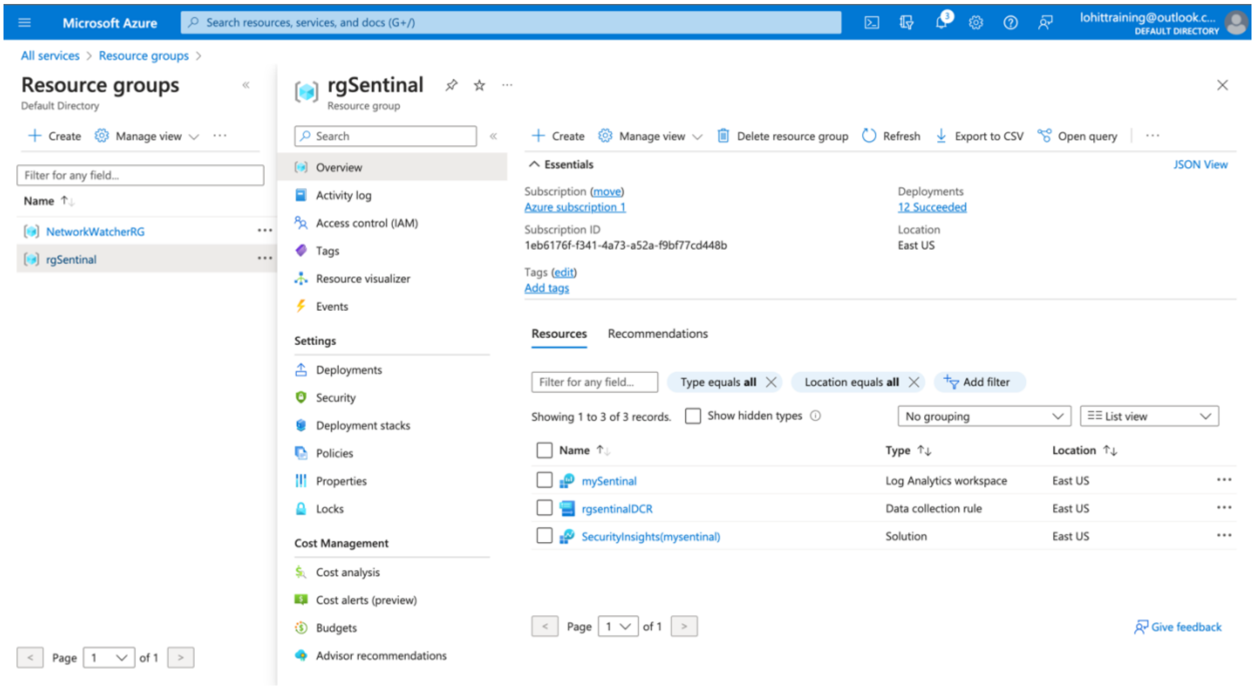
Required data type
AzureActivity

Relevant data connectors
AzureActivity

Content source: Azure Activity
Template version: 2.0.0

Author: Microsoft
Supported by: Microsoft Corporation | Email

I also want to see the data depected in a visual form which makes it easier for me and anyone else who looks at it. For which I create a workbook which is a graphical tool to analyze data.
Workbook has some predefined templets that can be used to create your workbook



Subscription (move)
Azure subscription 1

Subscription ID
1eb6176f-f341-4a73-a52a-f9bf77cd448b

Tags (edit)
Add tags

Deployments
12 Succeeded

Location
East US

Showing 1 to 3 of 3 records. □ Show hidden types

No grouping | List view

□ Name ↑↓	Type ↑↓	Location ↑↓
□ mySentinal	Log Analytics workspace	East US
□ rgsentinalDCR	Data collection rule	East US
□ SecurityInsights(mysentinal)	Solution	East US

All the resources and security we added is completely isolated under one resource group, which if need can be deleted with rest of your work.