

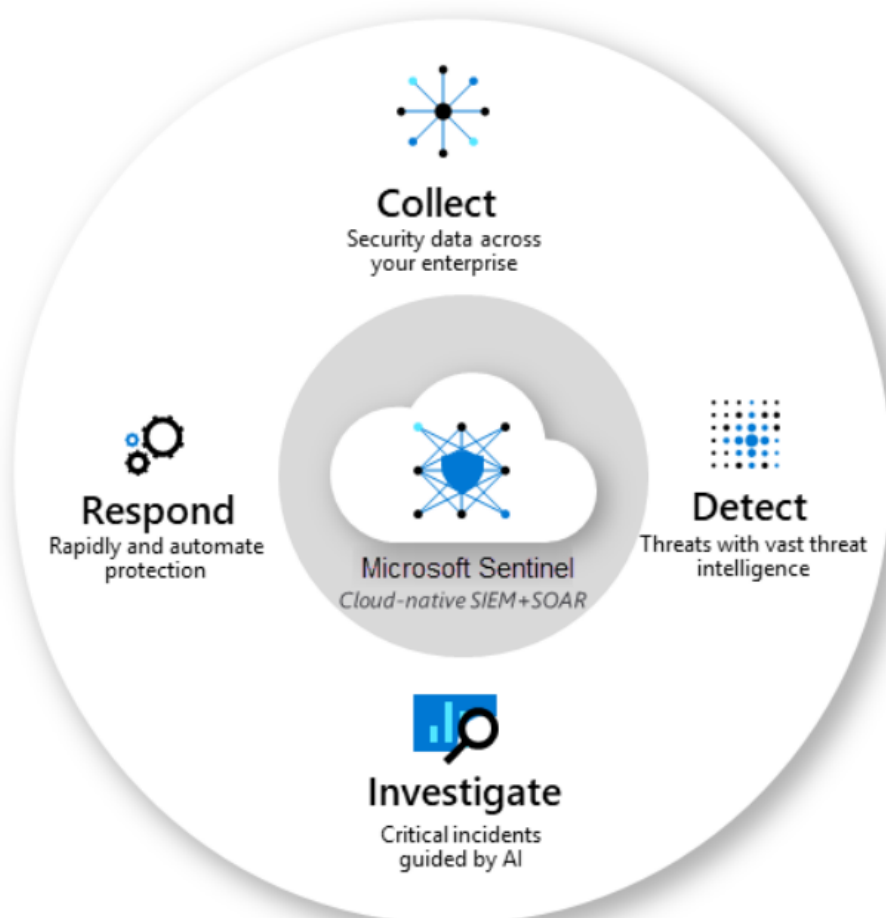
Log Analytical workspace and Microsoft sentinel

Microsoft sentinel

Sentinel will collect the logs along with that it will delivers intelligent security analytics and threat intelligence across the enterprise. it will keep eye on attacj detection, threat visibility, proactive hunting and threat response.

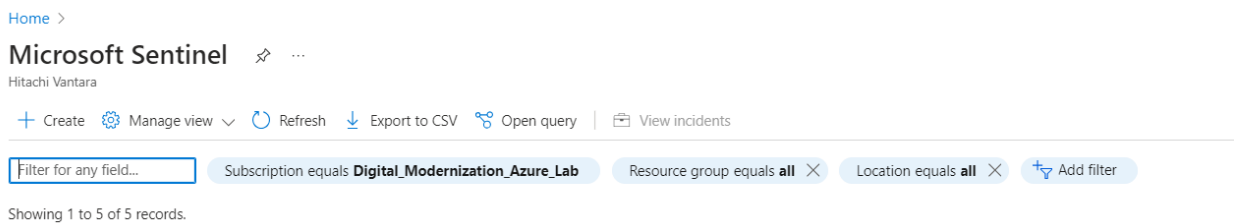
Microsoft Sentinel is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)



How to enable sentinel in Azure.

1. Search for Microsoft sentinel in console click on create



2. + create a new workspace

[Home](#) > [Microsoft Sentinel](#) > [Add Microsoft Sentinel to a workspace](#) >

Create Log Analytics workspace ...

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name * ⓘ ✓

Region * ⓘ

Review + Create

« Previous

Next : Tags >

Click on Create

Data Retention

Once the sentinel is created decide how long data needs to be in sync. remember more data retention will leads to more cost. for better price you can choose the commitment tier as per your need.

Note: for this article, im choosing pay as you go tier

Go to Sentinel → <your sentinel> → Settings → Workspace settings (this will open log analytics workspace)

The screenshot shows the 'kavya-low' Log Analytics workspace in the Azure portal. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, Linked storage accounts, Properties, Locks, Classic, Legacy agents management, Legacy activity log connector, and Legacy storage account logs. The 'Settings' section is expanded, showing 'Workspace settings'. A notification at the top states: 'The Log Analytics agents (MMA,OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent'. The 'Essentials' section displays workspace details: Resource group (kavya-sentinel), Status (Active), Location (East US), Subscription (Digital), Subscription ID, and Tags. On the right, it shows Workspace Name (kavya-low), Workspace ID, Pricing tier (Pay-as-you-go), Access control mode (Use resource or workspace), and Operational issues (OK). Below this, the 'Get started with Log Analytics' section provides three steps: 1. Connect a data source, 2. Configure monitoring solutions, and 3. Monitor workspace health. A 'Useful' link is also present.

Go to → Usage and estimated cost → Data retention → select the number of days → click on ok

cap
Data Retention
Help

g tier for this workspace can be changed in the [how to change the Sentinel pricing tier](#).

Usage Charts

Billable data ingestion by table (last 31 days)

Data ingested by table (last 90 days)

Table
No data

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be [configured individually for specific data types](#).

Data Retention (Days)

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](#).

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the [Tables](#) page of this workspace.

OK

Provide Permission to Resource group

Giving permission to a resource group will help to manage automation and analytics rules in a resource group.

Go to Settings in sentinel → settings → Playbook permission → configure permission



Microsoft Sentinel | Settings

Selected workspace: 'kavya-low'

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

Analytics

Watchlist

Automation

Settings

Workspace usage report

Pricing

Settings

Workspace settings >

Entity behavior analytics

What is it?

Microsoft Sentinel's user and entity behavior analytics (UEBA) creates comprehensive profiles of users' and entities' behavior within your organization to create the context for determining anomalies from selected data sources. [Learn more about identifying threat](#)

How to enable it

To turn on Microsoft Sentinel's UEBA in just a few easy steps, follow the steps to enable providers and data sources. See [Enable User and Entity Behavior Analytics](#)

Set UEBA

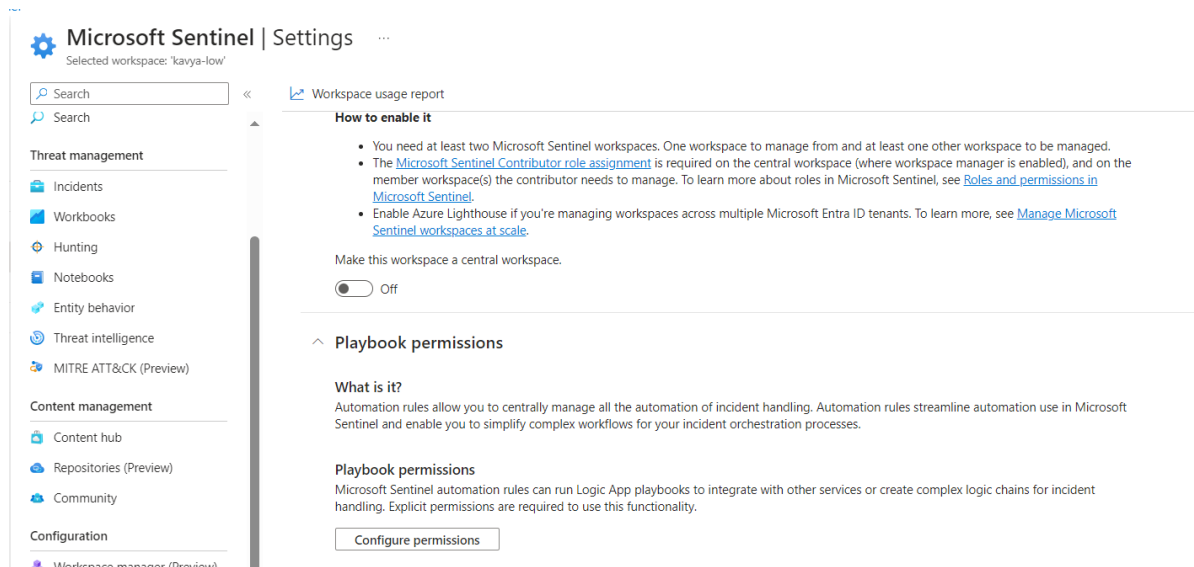
Anomalies

Microsoft Sentinel provides a rich set of behavior analytics Anomalies table in your workspace. You can use them in your investigations and also customize the parameters of the machine learning (ML) models to train the ML models. This data is cached and

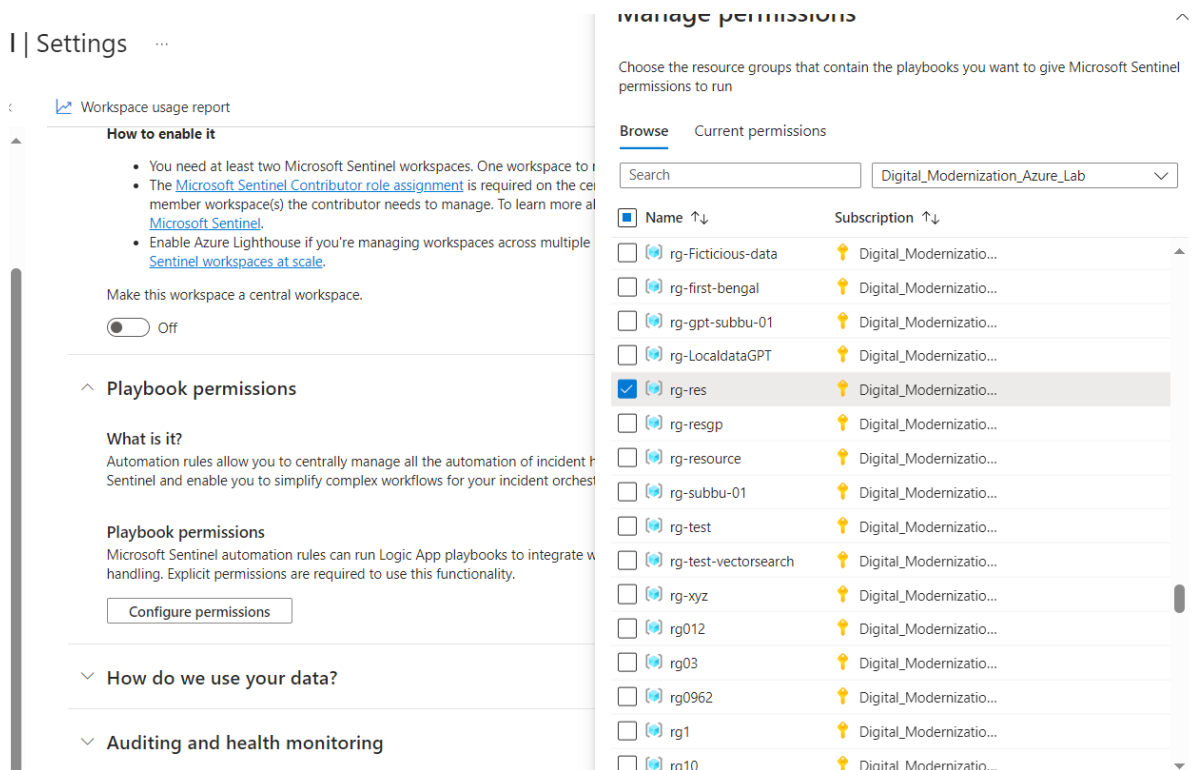
Only a Global Administrator or a Security Administrator can enable UEBA anomalies.

☒ On

UEBA anomalies will be enabled after 5 minutes. [Go to analytics in order to configure the anomalies](#)



Select the Resource group from the required subscription and apply.



To make sentinel to Inject the data, we need to complete below 3 configuration changes.

1. connect to data sources via content hub
2. Deploy analytic rules
3. Configure Hunting rule with workbooks.

Inject data into the workspace.

To onboard the sentinel, first you need to connect to your data sources via content hub with below steps

Go to content hub → search for Azure activity → install

Once installed click on manage.

The screenshot shows the Microsoft Sentinel Content Hub interface. On the left, there is a navigation pane with sections: Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), Content management (Content hub, Repositories (Preview), Community), and Configuration (Workspace manager (Preview), Data connectors, Analytics, Watchlist, Automation, Settings). The 'Content hub' section is active. The main area displays a list of solutions with filters for Status (All), Content type (All), and Support (All). The list includes solutions like Amazon Web Services, Analytics Health & Audit, Azure Active Directory, Azure Activity (selected), Cisco Umbrella, DNS Essentials, and Google Cloud Platform IAM. The 'Azure Activity' solution is highlighted, showing it is a 'Solution' from 'Microsoft' with 'Microsoft' support. On the right, a detailed view of the 'Azure Activity' solution is shown, including a description, a note about potential issues, and statistics: 12 Analytics rules, 1 Data connector, 14 Hunting queries, and 1 Workbook. A 'Manage' button is visible at the bottom of the details pane.

Manage will open new page → select the content type as data connector → open connector page

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub >

Azure Activity

Refresh Delete Reinstall Actions (Preview)

28 Installed content items 12 Configuration needed

Azure Activity

Microsoft Provider Microsoft Support 2.0.6 Version

Description

Note: 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

12 Analytics rule 1 Data connector 14 Hunting query 1 Workbook

Category

Manage Actions View details

Search...

Content name	Created content	Content type
<input checked="" type="checkbox"/> Azure Activity IN USE	1 item	Data connector
NRT Azure Active Directory Hybrid Health AD FS New Server	--	Analytics rule
New CloudShell User	--	Analytics rule
Creation of expensive computes in Azure	--	Analytics rule
Rare subscription-level operations in Azure	--	Analytics rule
Suspicious Resource deployment	--	Analytics rule
NRT Creation of expensive computes in Azure	--	Analytics rule
Azure Active Directory Hybrid Health AD FS Suspicious Application	--	Analytics rule
Suspicious number of resource creation or deployment activities	--	Analytics rule
Azure Active Directory Hybrid Health AD FS New Server	--	Analytics rule
Azure Active Directory Hybrid Health AD FS Service Delete	--	Analytics rule

Azure Activity

Connected Status Microsoft Provider Last Log Received

Last data received --

Content source Azure Activity Version 2.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Data received

Go to log analytics

Open connector page

in order to connect with the data connector, you need to assign azure policy with owner role assigned to azure activity.

scroll to Launch Azure Policy Assignment wizard>

Azure Activity

Checking... Status Microsoft Provider 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 --

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

Go to log analytics

Instructions

- 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 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.

- 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 log and metric types you want to ingest.
- 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>

This will open assign policy wizard →

in the basic section select Scope → to you subscription.

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Azure Activity > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Advanced Parameters Remediation Non-compliance messages Review + create

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

Assigned by

[Review + create](#) [Cancel](#) [Previous](#) [Next](#)

Scope

Subscription
Please choose a Subscription

Resource Group
Optionally choose a Resource Group

[Select](#) [Cancel](#) [Clear All Selections](#)

In Parameter section select primary log analytics workspace

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Content hub](#) > [Azure Activity](#) > [Azure Activity](#) >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

[Basics](#) [Advanced](#) [Parameters](#) [Remediation](#) [Non-compliance messages](#) [Review + create](#)

Search by parameter name

☒ Only show parameters that need input or review

Primary Log Analytics workspace * ⓘ

kavya-low

[Review + create](#)

[Cancel](#)

[Previous](#)

[Next](#)

leave rest as it is, click on Review and create


Once the policy is assigned, it will take couple of hours to reflect.

To check whether data connector is connected go to sentinel → content hub → installed → azure activity → manage → in content type select data connector → open.

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Content hub](#) > [Azure Activity](#) >


Data connectors

[Refresh](#) [Guides & Feedback](#)

 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.

 **1**
Connectors

 **0**
Connected

 More content at
Content hub

Providers : **All**

Data Types : **All**

Status : **All**

Status Connector name ↑




Azure Activity
Microsoft


if it is connected you will see green line below status.


[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Content hub](#) > [Azure Activity](#) >


Data connectors

[Refresh](#) [Guides & Feedback](#)

 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.


 **1**
Connectors

 **1**
Connected

 More content at
Content hub

Providers : **All** Data Types : **All** Status : **All**

Status Connector name ↑

 **Azure Activity**
Microsoft

Azure Activity

Connected

Status


Microsoft


Provider

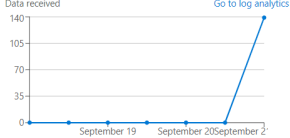
9 Minutes Ago

Last Log Received


Related content

 **3**
Workbooks

 **2**
Queries

 **12**
Analytics rules templates

Data received



Go to log analytics

AzureActivity

Open connector page

Deploy Analytic rules

Analytic rule is a detection that will allow you to detect the suspicious activity. To configure any rule follow the below steps.

Go to sentinal → content-hub → search for “azure activity” → manage → select any analytic rule of your choice → configuration.

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Azure Activity

Azure Activity

Refresh Delete Reinstall Actions (Preview)

28 Installed content items 12 Configuration needed

Azure Activity

Microsoft Provider Microsoft Support 2.0.6 Version

Description

Note: 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

12 Analytics rule 1 Data connector 14 Hunting query

1 Workbook

Category

Manage Actions View details

Search...

Content name	Created content	Content type
Azure Activity	1 item	Data connector
NRT Azure Active Directory Hybrid Health AD FS New Server	--	Analytics rule
New CloudShell User	--	Analytics rule
Creation of expensive computes in Azure	--	Analytics rule
Rare subscription-level operations in Azure	--	Analytics rule
Suspicious Resource deployment	--	Analytics rule
NRT Creation of expensive computes in Azure	--	Analytics rule
Azure Active Directory Hybrid Health AD FS Suspicious Application	--	Analytics rule
Suspicious number of resource creation or deployment activities	--	Analytics rule
Azure Active Directory Hybrid Health AD FS New Server	--	Analytics rule
Azure Active Directory Hybrid Health AD FS Service Delete	--	Analytics rule

NRT Azure Active Directory Hybrid Health AD FS Ne

Medium Severity Content Hub Content Source NRT Rule Type

Description

This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid Health AD FS service.

A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-premises AD FS server.

This can be done programmatically via HTTP requests to Azure. More information in this blog: <https://o365blog.com/post/hybridhealthagent/>

Tactics and techniques

Defense Evasion (1)

Rule query

AzureActivity | where CategoryValue == 'Administrative'

Note:

- You used this template to create analytics rules and can use it to create additional rules.

Configuration

Select the rule template → create rule

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Azure Activity > Analytics Rules

Create Refresh Analytics workbooks Enable Disable Delete Import Export Guides & Feedback

1 Active rules

More content at Content hub

Rules by severity

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

Active rules Rule templates Anomalies

ec491363-5fe7-4eff-b68e-442dc769c6f6 Add filter

Severity	Name	Rule type	Data sources	Tactics	Techniques	Source name
Medium	NRT Azure Active Directory Hybrid ...	NRT	Azure Activity	Defense Evasion	T1578	Azure Activity

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

NRT Azure Active Directory Hybrid Health AD FS Ne

Medium Severity Content hub Content Source NRT Rule Type

Description

This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid Health AD FS service.

A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-premises AD FS server.

This can be done programmatically via HTTP requests to Azure. More information in this blog: <https://o365blog.com/post/hybridhealthagent/>

Data sources

Azure Activity

AzureActivity 9/26/2023, 4:19:15 PM

Tactics and techniques

Defense Evasion (1)

Note:

- You haven't used this template yet; You can use it to create analytics rules.

Create rule

this will open new wizard.

go to Basic —> status → enabled → next: set rule logic

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Content hub](#) > [Azure Activity](#) > [Analytics Rules](#) >

Analytics rule wizard - Create a new NRT rule ...

NRT Azure Active Directory Hybrid Health AD FS New Server

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *

NRT Azure Active Directory Hybrid Health AD FS New Server

Description

This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid Health AD FS service.
A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof

Severity

Medium

Tactics and techniques (2)

Status



Enabled

[Next : Set rule logic >](#)

You can define the logic as per the need. For now i'm leaving to by default.

Review and create. —> save

Analytics rule wizard - Create a new NRT rule

NRT Azure Active Directory Hybrid Health AD FS New Server


Validation passed.

General Set rule logic Incident settings Automated response **Review + create**

Analytics rule details

Name NRT Azure Active Directory Hybrid Health AD FS New Server

Description This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid Health AD FS service. A threat actor can create a new AD Health AD FS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-premises AD FS server. This can be done programmatically via HTTP requests to Azure. More information in this blog: <https://o365blog.com/post/hybridhealthagent/>

Tactics and techniques  Defense Evasion
T1578 - Modify Cloud Compute Infrastructure

Severity  Medium

Status  Enabled

Analytics rule settings

Rule query AzureActivity | where CategoryValue == 'Administrative' | where ResourceProviderValue == 'Microsoft.ADHybridHealthService' | where _ResourceId has 'AdFederationService' | where OperationNameValue == 'Microsoft.ADHybridHealthService/services/servicemembers/action' | extend claimsjson = parse_json(Claims) | extend AppId = tostring(claimsjson.appid), AccountName = tostring(claimsjson.name), Name = tostring(split(Caller, '@')[0]), UPNSuffix = tostring(split(Caller, '@')[1][0]) | project-away claimsjson

Event grouping Group all events into a single alert

Suppression Not configured

Entity mapping

Entity 1: Account
Identifier: Name. Value: Name

[< Previous](#)

[Save](#)

We need to modify the alert query to get more accurate result.

Create hunting rule.

hunting rule will proactively look for any anomalies in the workspace. We can configure the hunting rule by using workbooks as well as logic app flows

in this article we will be configuring hunting rule using workbooks.

in order to configure go to → sentinel → content hub → search for “azure activity” → manage → in content name → scroll down to end → you will find workbook called “Azure Activity”

Select the workbook → configuration

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub >

Azure Activity

Refresh Delete Reinstall Actions (Preview)

28 Installed content items 11 Configuration needed

Azure Activity

Microsoft Provider Microsoft Support 2.0.6 Version

Description

Note: 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

12 Analytics rule 1 Data connector 14 Hunting query 1 Workbook

Category

Manage Actions View details

<https://portal.azure.com/#>

Content	Version	Category
Microsoft Sentinel Analytics Rules Administrative Operations	--	Hunting query
Anomalous Azure Operation Hunting Model	--	Hunting query
Rare Custom Script Extension	--	Hunting query
Azure Virtual Network Subnets Administrative Operations	--	Hunting query
Azure VM Run Command executed from Azure IP address	--	Hunting query
Granting permissions to account	--	Hunting query
Creation of an anomalous number of resources	--	Hunting query
Azure storage key enumeration	--	Hunting query
Microsoft Sentinel Workbooks Administrative Operations	--	Hunting query
AzureActivity Administration From VPS Providers	--	Hunting query
Microsoft Sentinel Connectors Administrative Operations	--	Hunting query
Common deployed resources	--	Hunting query
Azure Activity	--	Workbook

Azure Activity

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

[Configuration](#) [View Template](#)

this will open new wizard select on save → region → yes

Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Azure Activity >

Workbooks

Refresh Add Workbook Guides & Feedback

0 My workbooks 1 Templates 0 Updates More content at Content hub

My workbooks Templates

AzureActivityWorkbook

Add filter

Name	Status	Source name
Azure Activity	--	Azure Activity

Azure Activity

Status

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

[View Template](#) [Save](#)

It will take couple of minutes to reflect the data in workbook.

