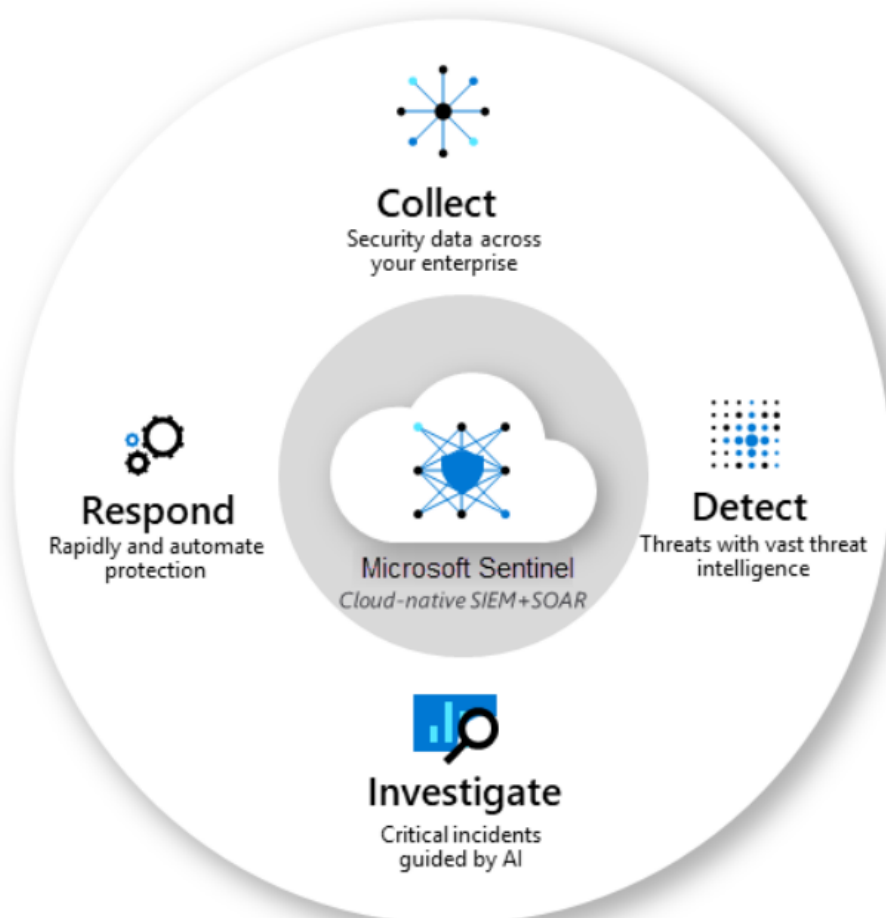# Log Analytical workspace and Microsoft sentinel

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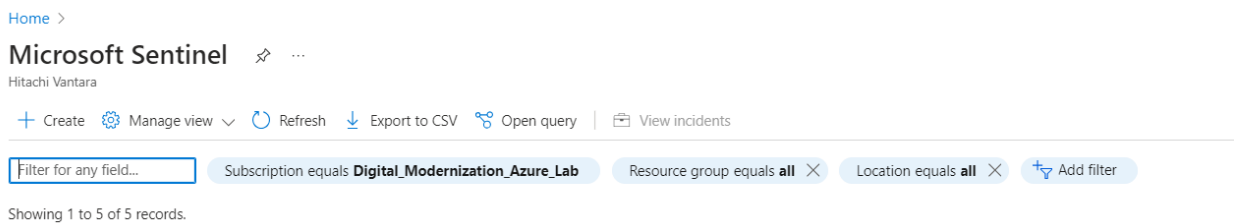
Microsoft Sentinel is a scalable, cloud-native solution that provides:

- 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

Create Log Analytics workspace ...

Basics   Tags   Review + Create

ⓘ 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 * ⓘ   Digital_Modernization_Azure_Lab   ⌄

  Resource group * ⓘ   kavya-sentinal   ⌄
                          Create new

Instance details

Name * ⓘ   sentinal-workspace   ✓

Region * ⓘ   East US   ⌄

[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)

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
l 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)

[slider] 31

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 sentinal → settings → Playbook permission —> configure permission

⚙ Microsoft Sentinel | Settings ...
Selected workspace: 'kavya-low'

Search
≪

🔍 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 (UEE
It creates comprehensive profiles of users' and entities' beh
organization) to create the context for determining anoma
selected data sources. Learn more about identifying threat

How to enable it

To turn on Microsoft Sentinel's UEBA in just a few easy step
providers and data sources. See Enable User and Entity Beh

[Set UEBA]

∧ **Anomalies**

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

```
Only a Global Administrator or a Security Administrat
```

🔵 On   ⓘ UEBA anomalies will be enabled after s
Go to analytics in order to configure the anomalies>
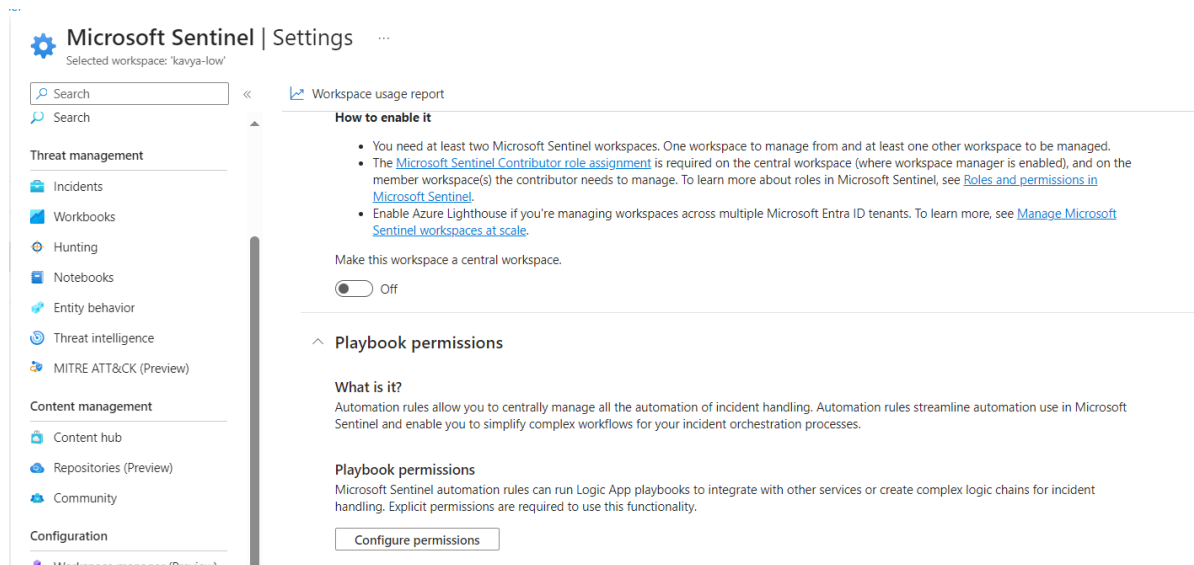
Select the Resource group from the required subscription and apply.
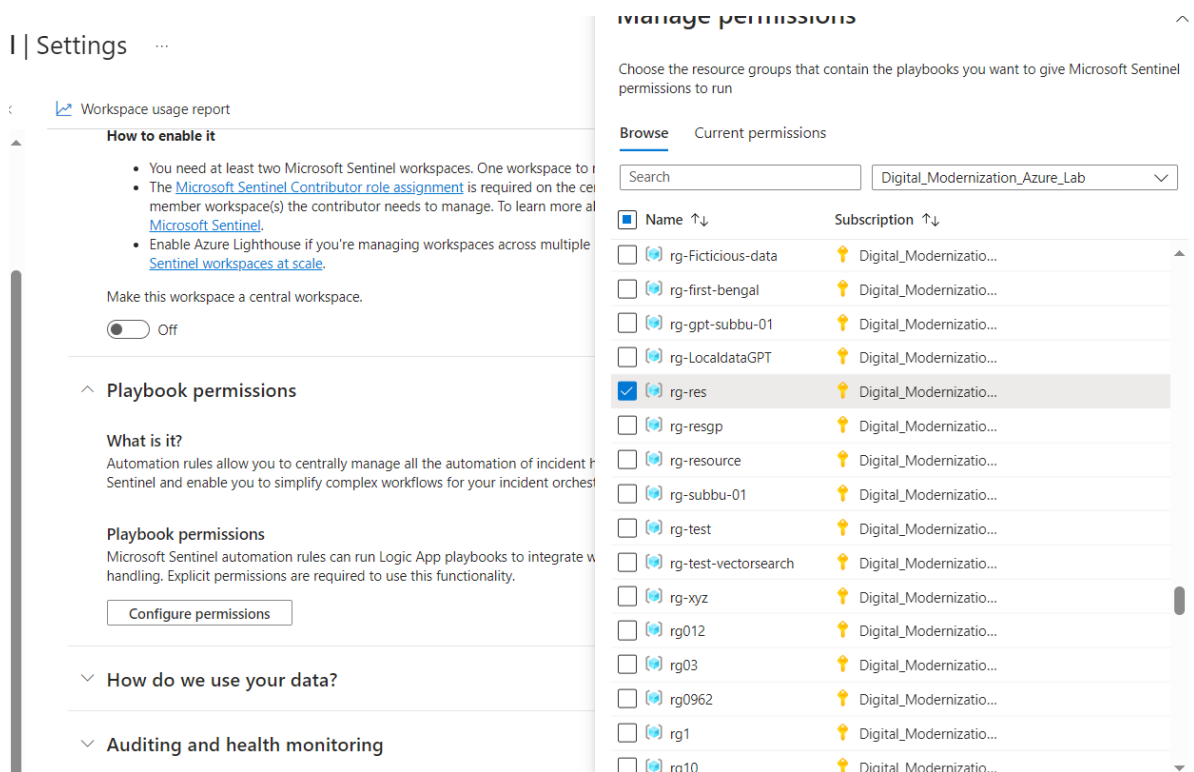
To make sentinel to Inject the data, we need to complete blolow 3 configuration changes.

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.

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

This will open assign policy wizard →

in the basic section select Scope → to you subscription.

In Parameter section select primary log analytics worspace

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 os connected go to sentinel → contect hub→ installed → azure activity → mange→ in content type select data connector → open.

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

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.

Select the rule template → 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

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

Create hunting rule.

hunting rule will proactivelu look for any anamolies 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 → sentnel → 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

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

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

Azure Activity - kavya-low
kavya-low

Edit Open 💾 🔄 ☁ 📌 😊 ? Help 🕐 Auto refresh: Off

TimeRange: Last 7 days ⌄   Caller: All ⌄   ResourceGroup: All ⌄

Top 10 active resource groups

All	MC_DEMO_DEVSECOPS...	MC_YASB_GROUP_KUBE...	MC_DASHBOARDASCO...	KAVYA-SENTINAL	SENTINAL-2023	SENTINAL-2023-PLAYG...	POLICYTEST_YASREEB	HV-DEVSECOPS-LAB
538	180	145	136	44	12	3	3	2

Activities over time