

## SIEM PERSONAL PROJECT: MICROSOFT SENTINEL :

<https://medium.com/@hhv8051/microsoft-sentinel-siem-soar-setup-1bd1ea9c4b7c>

In this article we will go through the configuration of cloud native Microsoft sentinel as a SIEM & SOAR.

SIEM—Security information & event management & SOAR—Security Orchestration, Automation & Response.

Go login to microsoft azure portal, search microsoft sentinel, Go to azure sentinel in the azure portal, click on add button, if log analytic workspace exist, select it or create a new workspace.

Select existing resource group or create a new one, enter a unique name, which is globally unique, Login name and then select region and it should be same with azure resources.

Click on review + create , this might take a few minutes.

✓ **Deployment succeeded** ✕

Deployment 'henil' to resource group 'Henildemonstrate' was successful.


📌 Pin to dashboard

Go to resource group

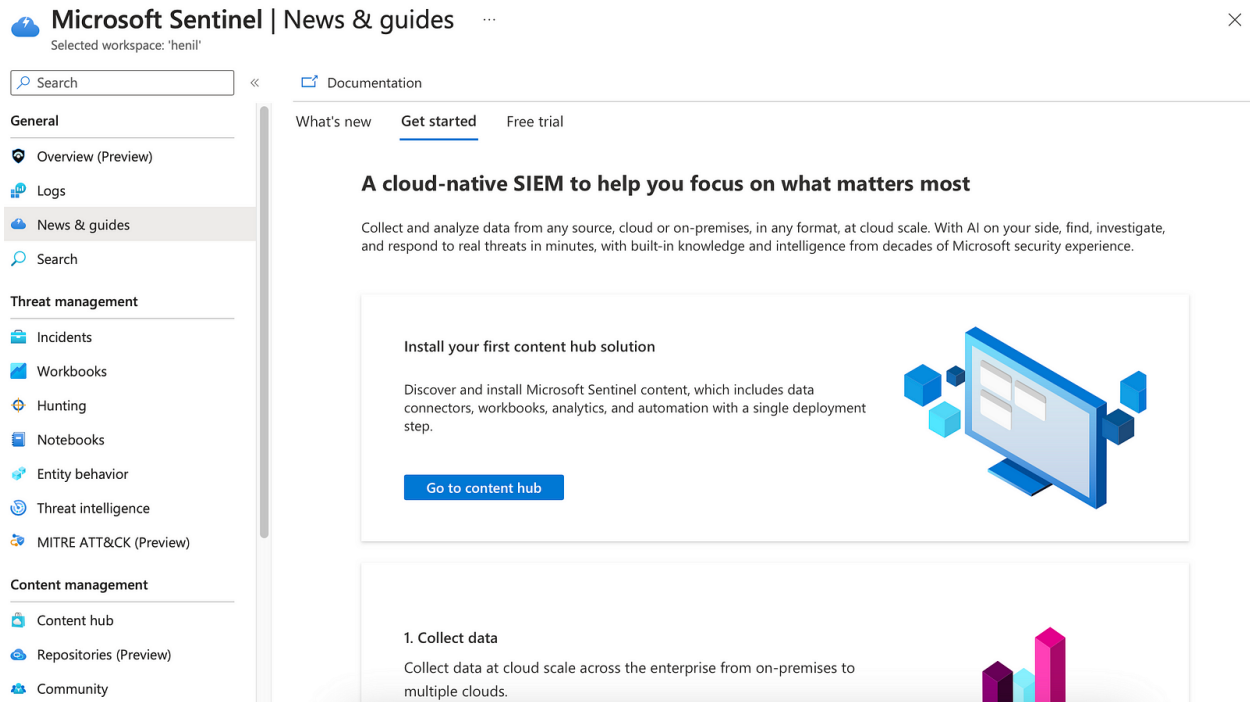
a few seconds ago

Then when validation has passed click create to create your new log analytics workspace, again give a few minutes for it to be created.

Then select the workspace, click add azure sentinel button.

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
 henil	eastus	henildemonstrate	Azure subscription 1	Default Directory

You are now in news and guides, a cloud native SIEM displays, this is your landing page once sentinel has loaded and on the left side is your sentinel workspace ( navigation menu) with options such as general/threat management/content management/ configuration.




Configure log analytics, select settings in navigation menu and then workspace in header menu bar.

Head to log analytics page, go on azure virtual machines aswell as if the machine is connected to this or other workspace, the second option is connected sources these are the ones where logs are generated from and not connected to your azure, sysmon(on-premises and cloud).

If there is data that you want but not included use Syslog and CEF for these data providers that do not have a connector

Go to data connectors, add azure active directory since I made azure active directory account and then go to logs and you will see logs to add.


**Azure Active Directory**

Not connected

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

Author

Microsoft

Supported by

[Microsoft Corporation](#) | [Email](#)

Related content

7

Workbooks

2

Queries

59

Analytics rules templates

Instructions

✓

Sign-In Logs

?

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

✓

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)

✓







Service Principal Risk Events (Preview)

Apply Changes


Otherwise install from content creator section.

Status : **All**
Content type : **Data connector (253)**
Support : **All**


Provider : **All**
Category : **All**
Content sources : **All**


<input type="checkbox"/>	Content title	Content source	Provider	Support	Category
<input type="checkbox"/>	 Amazon Web Services <b>FEATURED</b>	Solution	Amazon Web Servi	Microsoft	Security - Cl
<input checked="" type="checkbox"/>	 Azure Active Directory <b>FEATURED</b>	Solution	Microsoft	Microsoft	Identity, Secu
<input type="checkbox"/>	 Azure Activity <b>FEATURED</b>	Solution	Microsoft	Microsoft	IT Operatio
<input type="checkbox"/>	 Cisco Umbrella <b>FEATURED</b>	Solution	Cisco	Microsoft	Security - Au
<input type="checkbox"/>	 Google Cloud Platform IAM <b>FEATURED</b>	Solution	Google	Microsoft	Cloud Provid
<input type="checkbox"/>	 Microsoft 365 Defender <b>FEATURED</b>	Solution	Microsoft	Microsoft	Security - Th

[< Previous](#)
Page  of 8
[Next >](#)
Showing 1 to 30 of 234 results.


**Azure Active Directory**

Microsoft Provider

 Microsoft Support

 3.0.0 Version

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.

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](#)

Install

View details

Then templates show in workbook templates. Go to workbooks in left, see templates, click templates and then save to add in saved workbooks.



## Microsoft Sentinel | Workbooks

Selected workspace: 'henil'

### General

- Overview (Preview)
- 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

Refresh + Add workbook

Saved workbooks

Templates

Updates

Content hub

My workbooks

**Templates**

Workbook name ↑↓

Content source ↑↓

	Azure Activity	Content hub AZURE ACTIVITY
	Azure AD Audit logs	Content hub AZURE ACTIVE DIRECTORY
	Azure AD Sign-in logs	Content hub AZURE ACTIVE DIRECTORY
	DNS Solution Workbook	Content hub DNS ESSENTIALS
	Log4j Impact Assessment	Content hub APACHE LOG4J VULNERABILITY DETECTION
	Log4j Post Compromise Hunting	Content hub APACHE LOG4J VULNERABILITY DETECTION

Rules are the key of azure, it detects security threats and generates alerts.

In workspace click on analytics in left-hand menu, select create to create a new rule, choose a template or create a blank rule, specify data source and conditions to trigger the rule.

# Analytics rule wizard - Create a new Microsoft Security rule

General Automated response Review and create

## Analytics rule details

Name rule\_henil1

Description

Status  Enabled

## Analytics rule logic

Microsoft security service Azure Active Directory Identity Protection

Filter by severity Any

Include by alert name(s) Any

Exclude by alert name(s) Any

## Automated response

Automation rules  rule1hhv

After custom rules are created refresh go in insights, if alerts they will be seen here, can create demo insight, can see more analytics in security efficiency workbook, review details and take appropriate action for your alert.

 2  
Active rules

 More content at  
Content hub


LEARN MORE  
[About analytics rules](#)






## Rules by severity

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

Active rules Rule templates Anomalies

 Search by ID, name, tactic or technique

 Add filter

<input type="checkbox"/>	Severity	Name	Rule type	Status	Tactics	Techniques	Source name
<input type="checkbox"/>	High	rule_henil1	 Microsoft S	 Enabled			Custom Content
<input type="checkbox"/>	High	Advanced Multist	 Fusion	 Enabled	 Collec +11		Gallery Content

Click on sentinel name, not resource group then after sentinel navigation bar go to workbook, add workbook, select workbook and save so it is custom workbook.

