Onboarding E3/E5 Data Sources into Microsoft Sentinel

April 2022

Queensland Government Customer and Digital Group

Queensland Government

Summary

It is recommended that Agencies at a minimum ingest the following data/logs into their agency Microsoft Sentinel Instances before they are onboarded onto the Sentinel of Sentinel QGCDG (Queensland Government Customer and Digital Group) instance.

Data Sources

FREE- TIER DATA SOURCES

Name	Connector	License
Azure activity Logs	Azure Activity Connector	E5
Office 365 Audit Logs	Office 365 Connector	E3/E5
Alerts from Microsoft Defender for Cloud	Microsoft Defender for Cloud Connector	E5
Alerts from Microsoft 365 Defender	Microsoft 365 Defender (Preview) Connector	E5
Alerts from Microsoft 365 Defender for Office 365	Microsoft 365 Defender (Preview) Connector	E5
Alerts from Microsoft Defender for Identity	Microsoft 365 Defender (Preview) Connector	E5
Alerts from Microsoft Defender for Endpoint	Microsoft 365 Defender (Preview) Connector	E5
Alerts from Microsoft Defender for Cloud Apps	Microsoft 365 Defender (Preview) Connector	E5

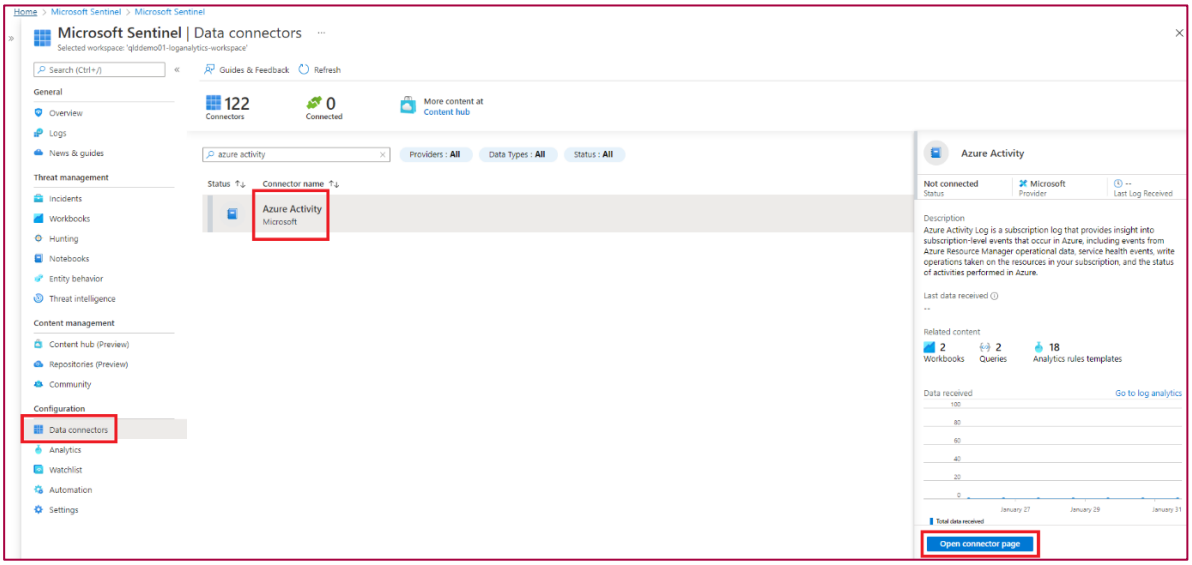
OTHER OPTIONAL DATA SOURCES OF INTEREST

Name	Connector	License
Message trace logs	See page 7	E3 or E5

This document is a guide that can be used to enable the minimum expected logs stated above.

Getting Azure Activity Logs into Sentinel

1. In Microsoft Sentinel, select Data connectors from the navigation menu.
2. From the data connectors gallery, select **Azure Activity**, and select **Open connector** page in the details pane.

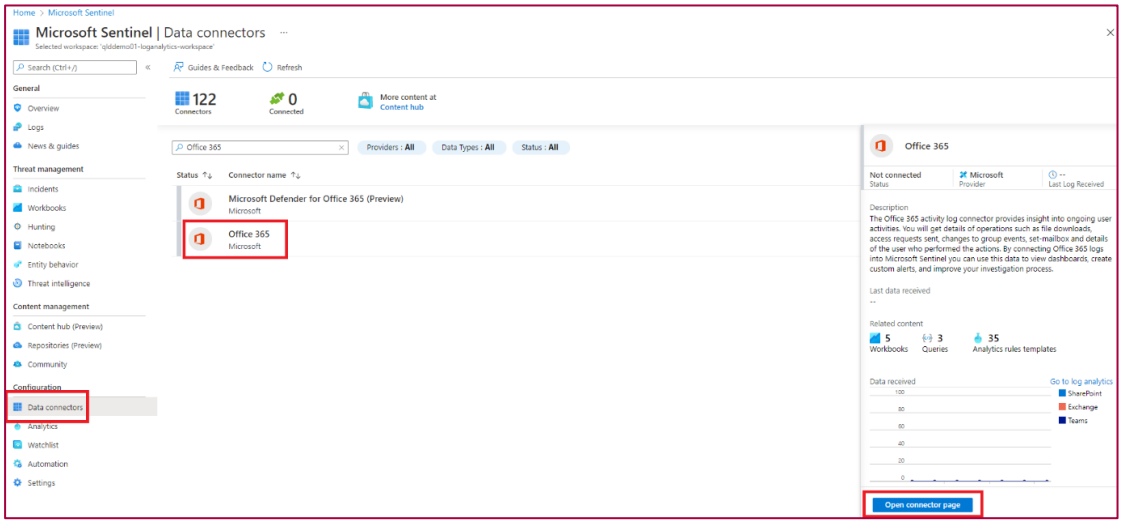


3. Click **Launch Azure Policy Assignment wizard** button to launch the Policy creation wizard.
4. Select the Scope (Subscription and Resource group) to which this policy will be applied using the ellipses to open a panel to make the selection.
5. Again, using the ellipses, select the Log Analytics workspace to which this new policy will be applied. The Log Analytics Contributor role is required to create this policy.
6. Enable the Remediation task to ensure that this policy can be applied to existing resources, otherwise it will only take effect on newly created resources.
7. A non-compliance message isn't necessary.
8. Select Create to save this new policy.
9. Use the following query to verify the data ingestion.

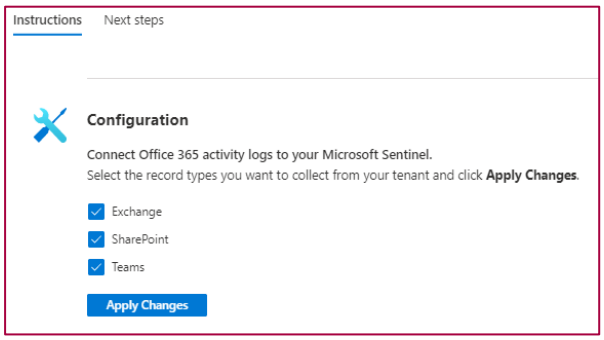
```
AzureActivity
| take 1000
```

Getting Office 365 Audit Logs into MS Sentinel

10. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
11. From the data connectors gallery, select **Office 365**, and select **Open connector** page in the details pane.



12. Check all the below boxes and hit **Apply Changes** to complete. The data source are free.

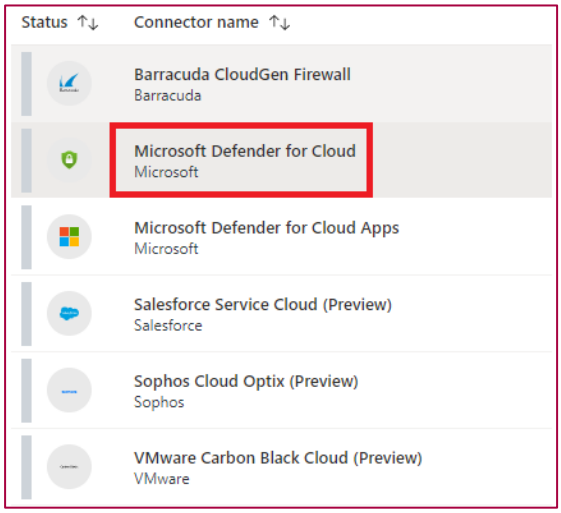


13. After you connect, you see a summary of the data in the Data received graph, and the connectivity status of the data types.
14. You can also verify the activities using the following query.

```
OfficeActivity
| where OfficeWorkload == "SharePoint" or OfficeWorkload == "OneDrive" or
OfficeWorkload == "Exchange" or OfficeWorkload == "MicrosoftTeams"
| sort by TimeGenerated
```

Getting MS Defender for Cloud data into MS Sentinel

1. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
2. From the data connectors gallery, select **Microsoft Defender for Cloud**, and select **Open connector** page in the details pane.



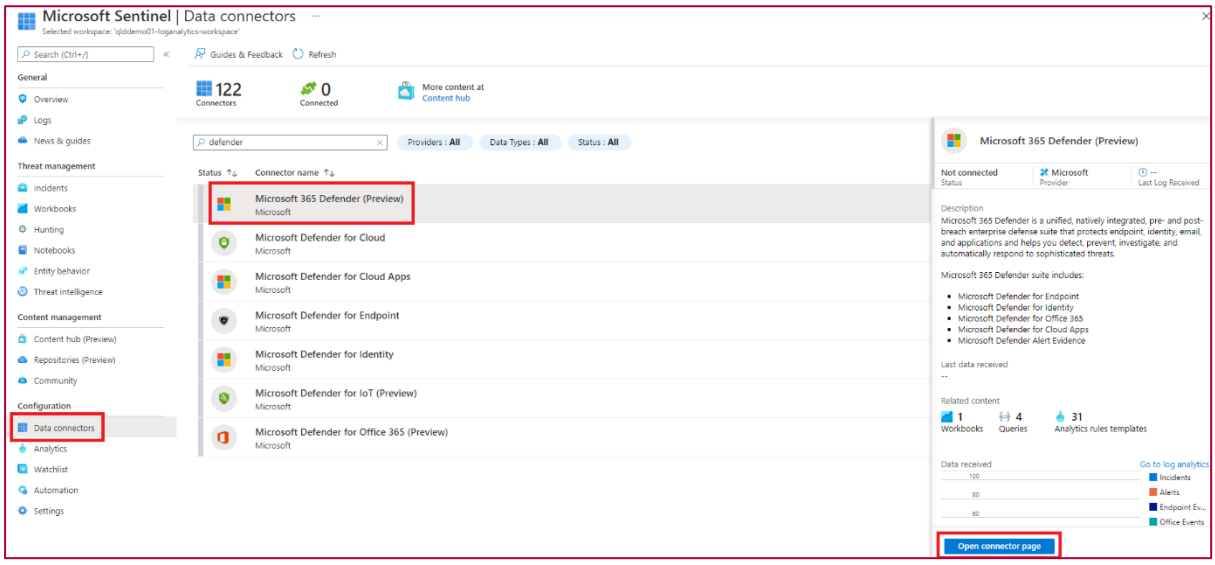
3. Under **Configuration**, you will see a list of the subscriptions in your tenant, and the status of their connection to Microsoft Defender for Cloud. Select the Status toggle next to each subscription whose alerts you want to stream into Microsoft Sentinel
4. Enabling **bi-directional sync** will automatically sync the status of original security alerts with that of the Microsoft Sentinel incidents that contain those alerts. So, for example, when a Microsoft Sentinel incident containing a security alerts is closed, the corresponding original alert will be closed in Microsoft Defender for Cloud automatically.
5. In Microsoft Sentinel, select **Logs** from the navigation menu and enter the following command

```
SecurityAlert | where ProductName == "Azure Security Center"
| sort by TimeGenerated
```

Getting Alerts from MS Defender (Office 365, Identity, Endpoint, Cloud App) into MS Sentinel

Microsoft 365 Defender connector allows you to stream all alerts from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Defender for Cloud Apps.

1. In Microsoft Sentinel, select **Data connectors**, select Microsoft 365 Defender (Preview) from the gallery and select **Open connector** page.



2. Under Configuration in the Connect incidents & alerts section, select **the Connect incidents & alerts** button.
3. To avoid duplication of incidents, it is recommended to mark the check box labeled **Turn off all Microsoft incident creation rules for these products**.

> **Warning**
>
> You can collect advanced hunting events if you select the data types under Connect events, but it will incur additional cost. Please refer to **Appendix B** for more details

4. To query Microsoft 365 Defender incident data, use the following statement in the query window:

```
SecurityIncident
| where ProviderName == "Microsoft 365 Defender"
```

Getting Message Trace Logs with Azure Sentinel

Prerequisites
You need to have an Azure Subscription, ability to create an Azure Function App. You need to have an account with permissions to run get-messagetrace in Office 365. Use a dedicated account with a complex pwd stored in Azure Key Vault.

Create Account
To ingest the message trace logs a service account is required to be created with the ability to run the Get-MessageTrace command.

1. Log in to the Office 365 Admin center
2. Create an account called "messagetrace@"
3. Click on the account and select "Manage Roles"
4. Assign the Role: Admin Center Access -> Message Center Reader
5. Log in to the Exchange admin Center
6. Dashboard -> Admin Roles -> Create group called "Message Trace"
7. Assign the "Message Tracking Role" and "View-only Recipients"

Installing
The preferred way to ingest logs is to follow the guide written by Microsoft available at https://github.com/OfficeDev/O365-ActivityFeed-AzureFunction/tree/master/Sentinel/msgtrace an extract of which has been included here.

1. Create the Azure Function App with PowerShell. It works well with a consumption plan in most scenarios. The runtime stack should be PowerShell Core.
2. Create a new function that is timer based. Depending on your need, set it to run on a schedule like every 5 minutes. (For high load consider more often)
3. Paste the code from ingestmsgtrace.ps1 to the code window
4. Select Platform features, by clicking on the Function App name and click the Platform features tab at the top. Click Configuration under General Settings.
5. Provide the following values, if you want to add further protection store the pwd and key in Azure Key Vault. https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
    - expass (Exchange password)
    - exuser (User account with the right to run Get-messagetrace)
    - workspaceId (log analytics workspace)
    - workspaceKey (log analytics Key)
    - customLogName (table name in log analytics)
6. From the platform features open Console (CMD / Powershell), run the following command to initiate the file that will keep track of the runs (customize time). out-file d:\home\timetracker.log -InputObject "2020-04-02T10:22:13.962Z"

Appendix A

Data Connector Status

The following table displays the current status of the data connectors whether it is in Preview stage or not as of 04/02/2022.

Data Connector	Status
Microsoft 365 Defender	Preview
Microsoft Defender for Cloud	
Microsoft Defender for Cloud Apps	
Microsoft Defender for Endpoint	
Microsoft Defender for Identity	
Microsoft Defender for Office 365	Preview
Azure Activity	
Office 365	

Appendix B

Data Type and Cost

Microsoft Sentinel Data Connector	Data type	Free or paid
Azure Activity Logs	AzureActivity	Free
Azure AD Identity Protection	SecurityAlert (IPC)	Free
Office 365	OfficeActivity (SharePoint)	Free
	OfficeActivity (Exchange)	Free
	OfficeActivity (Teams)	Free
Microsoft Defender for Cloud	SecurityAlert (Defender for Cloud)	Free
Microsoft Defender for IoT	SecurityAlert (Defender for IoT)	Free
Microsoft 365 Defender	SecurityIncident	Free
	SecurityAlert	Free
	DeviceEvents	Paid
	DeviceFileEvents	Paid
	DeviceImageLoadEvents	Paid
	DeviceInfo	Paid
	DeviceLogonEvents	Paid
	DeviceNetworkEvents	Paid
	DeviceNetworkInfo	Paid
	DeviceProcessEvents	Paid
	DeviceRegistryEvents	Paid
	DeviceFileCertificateInfo	Paid
Microsoft Defender for Endpoint	SecurityAlert (MDATP)	Free
Microsoft Defender for Identity	SecurityAlert (AATP)	Free
Microsoft Defender for Cloud Apps	SecurityAlert (Defender for Cloud Apps)	Free
	MCASShadowITReporting	Paid