Connecting Microsoft services to Microsoft Sentinel

The three Microsoft/azure related services we can connect are:

* First the **Office 365 connector**. The Configuration option allows for the sending of Exchange, SharePoint, and Teams data. Based on your organization's specific needs, you can decide which data to ingest. The Data types show that all the data will reside in the **OfficeActivity** table.
* The second is **Azure Active Directory**, which has two options for **Sign-on logs** and **Audit logs**.
* Third is **Azure Active Directory Identity Protection**. This connector will send data to the **SecurityAlert** table. The SecurityAlert table will hold the alert data only without the underlying data that caused the alert. A second option is to Create Incidents, which is Recommended! This process will automatically create an Incident based on and connected to the alert ingested to the SecurityAlert table from Azure Active Directory Identity Protection. You can also activate the incident creation rule on the Analytics page.

Tenant Permissions require **“Global Administrator”** or **“Security Administrator”** on the workspace’s tenant.

Azure AD Identity Protection requires Azure AD Premium P2.

# Office 365 Connector

Gives us insight into ongoing user activities. Details of operations such as file downloads, access requests sent, changes to group events, set-mailbox and details of the user who performed the actions.

# Azure Active Directory

Gain insights into Azure AD by connecting audit and sign in logs to Microsoft sentinel to gather insights around Azure AD scenarios. Sign in logs give details related to app usage, conditional access policies and legacy auth. Audit logs gives information on Self-service password reset usage and AAD management activities like user, group, role and app management.

# Azure AD Identity Protection

Azure ADIP provides a consolidated view of at-risk users, risk events and vulnerabilities, with the ability to remediate risk immediately and set policies to auto-remediate future events.