

Onboard Microsoft Sentinel and XDR

1. Prerequisites

- Representative with Global Administrator role access
- Representative with permissions required to create a Sentinel workspace and connect required data sources (Owner of the relevant subscriptions).
- Correct licenses in place.

2. General information

- The subscription should reside within the tenant where the Azure services to be monitored are placed. In the special cases where no Azure services are to be connected the location is more flexible.
- It is important for Defender for Identity to have the MDI sensor installed on all of your Domain Controllers and if applicable also on your ADFS machines and CA servers.

3. Tasks

3.1. Create Sentinel workspace

- Browse to <https://portal.azure.com>
- Use the search function to find "Microsoft Sentinel"
- Go to the Microsoft Sentinel pane and click "+ Create"
- Click "+ Create a new workspace"
 - This will create a new Log Analytics workspace
- Select subscription
- Create a new resource group
 - Select a name that follow the organizations naming convention. Truesec recommend that the name contain at least one of the following words: sentinel, soc or siem.
- Select a name for the instance
 - Truesec recommend putting a company name in the beginning of the name (e.g. "companyname-sentinel")
- Select region
 - Truesec recommend "West Europe".
- Click "Review + Create" and then "Create"
 - Use "Refresh" if the newly created workspace does not show.
- Select the workspace and click "Add".

3.2. Set data retention period

- Go to the Microsoft Sentinel pane and click on the Sentinel workspace.

- Click “Settings” → “Workspace settings >”
- Click “Usage and estimated costs” under “General” in the menu to the left
- Click “Data retention” on the top of the page.
- Set the data retention period to 90 days and click OK

3.3. Connect data sources

The data sources will bring in alert information and sometimes log from other services.

Note that it sometimes takes a while before the status is reported as connected after activating a data connector.

This is a common baseline of services and data types to connect.


- Go to the Microsoft Sentinel pane and click on the Sentinel workspace.
- Click “Content Hub”.
- Search for each connector and click “Install”. When installed, select the connector and click manage.
 - **Azure Activity** (Recommended but Optional Connector)
 - To enable this connector, Subscription Owner is required for all relevant Subscriptions
 - Click “Launch Azure Policy Assignment wizard”
 - Select the subscription under “Scope”
 - On the “Parameters” tab, select the Log Analytics workspace to use.
 - On the “Remediation” tab, change region of the “System assigned identity location” to “West Europe”.
 - Click “Review + Create” and “Create”
 - **Microsoft Entra ID**
 - Select “Sign in” and “Audit” -logs (free with E5)
 - **Microsoft Defender XDR**
 - Click “Connect incidents & alerts”
 - Enable “DeviceInfo” and all “Microsoft Defender for Office 365” events.
 - Click “Apply Changes”
 - This will activate several different 365 Defender suite connectors:
 - Entra Identity Protection
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Identity
 - Microsoft Defender for Office 365

3.4. Configure Cloud Apps Connector in Defender

- Go to security.microsoft.com

- Under “Settings” -> “Cloud apps”, click “App Connectors”.
- Make sure that “Microsoft 365” and “Microsoft Azure” are connected and that both are receiving data.

[+ Connect an app](#) ▼


App ▼	Status ▼
 Microsoft 365 Collaboration	 Connected
 Microsoft Azure Cloud computing platform	 Connected







- Edit settings for the Microsoft 365 connector and select all available data sources.

- ☒ Select Office 365 components
- ☐ Great, Office 365 is connected

Select Office 365 components

Connect as Microsoft Azure administrator to gain full visibility and control.

 To connect this app, provide your access credentials. We secure your data as described in the [privacy statement](#) | [Terms](#)

- ☒ Azure AD Users and groups 
- ☒ Azure AD Management events 
- ☒ Azure AD Sign-in events 
- ☒ Azure AD Apps 
- ☒ Office 365 activities 
- ☒ Office 365 files 

Enable file monitoring before enabling Office 365 files.

3.5. Configure Entra ID Protection alert service in Defender

- Go to security.microsoft.com
- Under “Settings” -> “Microsoft Defender XDR”, click “Alert service settings”.
- Make sure that “All alerts” is selected.

Microsoft Defender XDR

General

Account

Email notifications

Alert service settings

Permissions and roles

Streaming API

Multi-tenant content source

Alert service settings

You can turn off alerts from the listed services. When you turn them off, alerts from the service no longer appear within incidents or in the alerts queue.

Microsoft Entra ID Protection

Choose which identity protection alerts will appear in the alerts and incidents pages.

☒ **High-impact alerts only (Default)**
Show only alerts about known malicious or highly suspicious activities that might require attention.

☒ **All alerts**
Show all alerts, including activity that might not constitute unwanted or malicious activity.