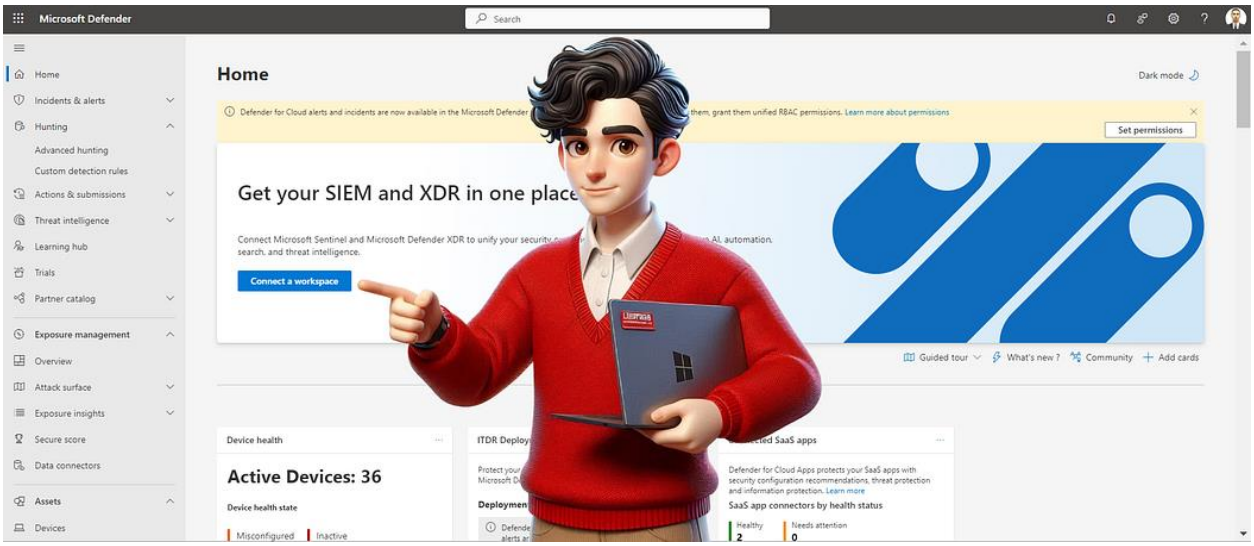
Unified Security Operations Platform — Connect Microsoft Sentinel to Microsoft Defender XDR

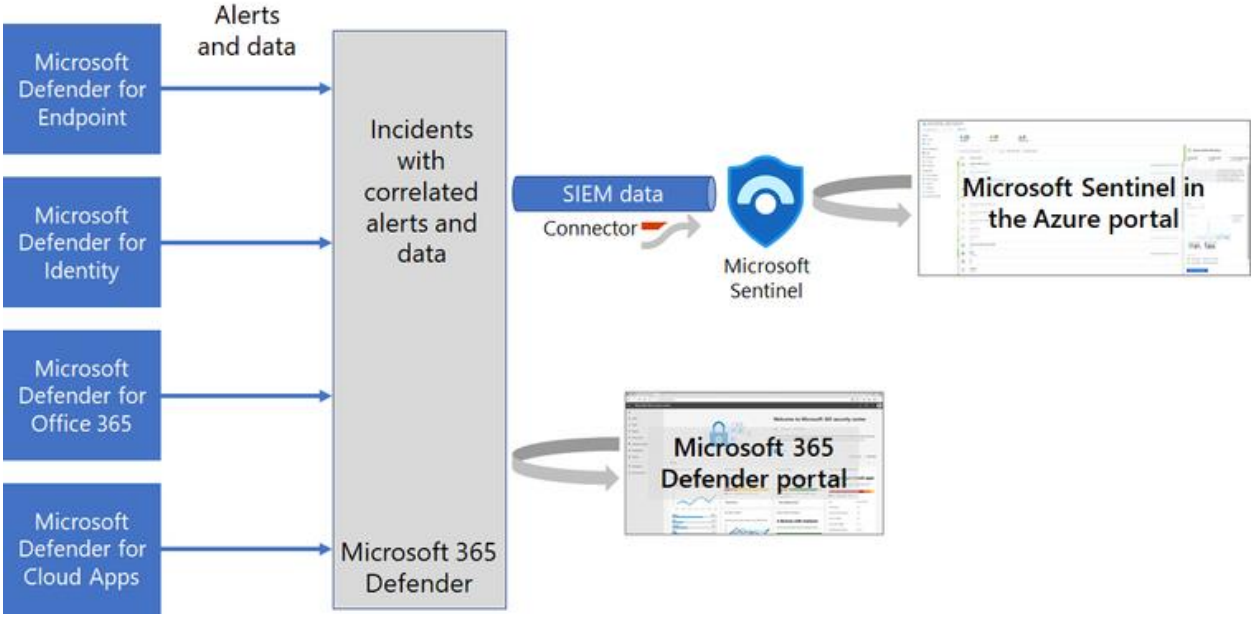


I am delighted to share that Microsoft has released the Unified Security Operations Platform.

As someone who took part in the preview phase of the platform and participated in the tests, I had the opportunity to examine its functionality in detail and provide feedback. It seamlessly integrates all the features from the leading cloud-based security information and event management (SIEM) system, a comprehensive extended detection and response (XDR) platform, and artificial intelligence

designed specifically for cybersecurity. This combination of capabilities delivers a truly unified experience for analysts in the security operations center (SOC) and saves effort.

Security teams are burdened with more responsibilities than ever before, and the complexity of today's security tools environment does not make their jobs easier, but on the contrary, more complex environments are expected to be managed. They must sift through large amounts of data from a variety of sources, which can lead to slower response and resolution of threats, increased time spent learning new technologies, greater integration, and less comprehensive insights. Additionally, managing the costs associated with data processing remains a significant challenge.
Microsoft is committed to empowering these teams by combining the multitude of tools needed to protect their digital data into a single, effective solution powered by artificial intelligence and automation.



So how will we gain advantages?

Integrated into the Unified Portal, advanced hunting lets you access and query data from a single platform, including all data in Microsoft Defender XDR, as well as information from various Microsoft security services, Microsoft Sentinel, and non-Microsoft products. You will also have the opportunity to quickly analyze your system with the queries that will run. It increases productivity and improves the quality of investigations by seamlessly querying data in both **Microsoft Sentinel** and **Microsoft Defender** . This integrated approach facilitates the hunting process by ensuring effective correlation of information.

Analyzing data from various tables in Microsoft Sentinel becomes easier with Advanced Hunting, considering the time and effort of IT staff. Accessing all tables in Sentinel in the Microsoft Defender portal simplifies the query process, saving time and effort. In this way, XDR customers benefit from greater flexibility in reporting, distribution automations and deeper insights across data sources. Likewise, SIEM customers can focus on proactive threat mitigation and new threat detection, gaining more out-of-the-box value.

Now if we examine the installation processes and phases;

Azure Portal Access

The first step is to access the Azure Portal. You must have owner authority on the relevant subscription and RG in the Azure portal, or your needs must be met according to the authorizations in the link. (Link1 , Link2)

Creating and Configuring Microsoft Sentinel

Microsoft Sentinel needs to be created and configured. You can review our previous articles on this subject, " Microsoft Sentinel — The Ultimate Blog Series Part 1 ".

Data Connectors Configuration

In Microsoft Sentinel, the relevant connectors must be activated by going to the "Data connectors" section.

Connecting Connectors

After configuring your Defender for Endpoint connector in Sentinel, you will follow the steps to integrate Sentinel with Microsoft Defender XDR.

Testing Data Flow

After configuring the connection, test the data flow between Sentinel and Defender XDR. This ensures that it is configured correctly and data is transferred smoothly.

Monitoring the Rules and Their Observations

After establishing the connection, create and monitor the necessary rules and observations in Sentinel. This allows you to analyze data from Defender XDR and detect potential threats.

By following these steps, you can successfully connect Microsoft Sentinel to Microsoft Defender XDR using Unified Security Operations Platform. This integration is a critical step in enabling your organization's cybersecurity operations and quickly detecting threats.

Connecting to Microsoft Defender XDR from Microsoft Sentinel

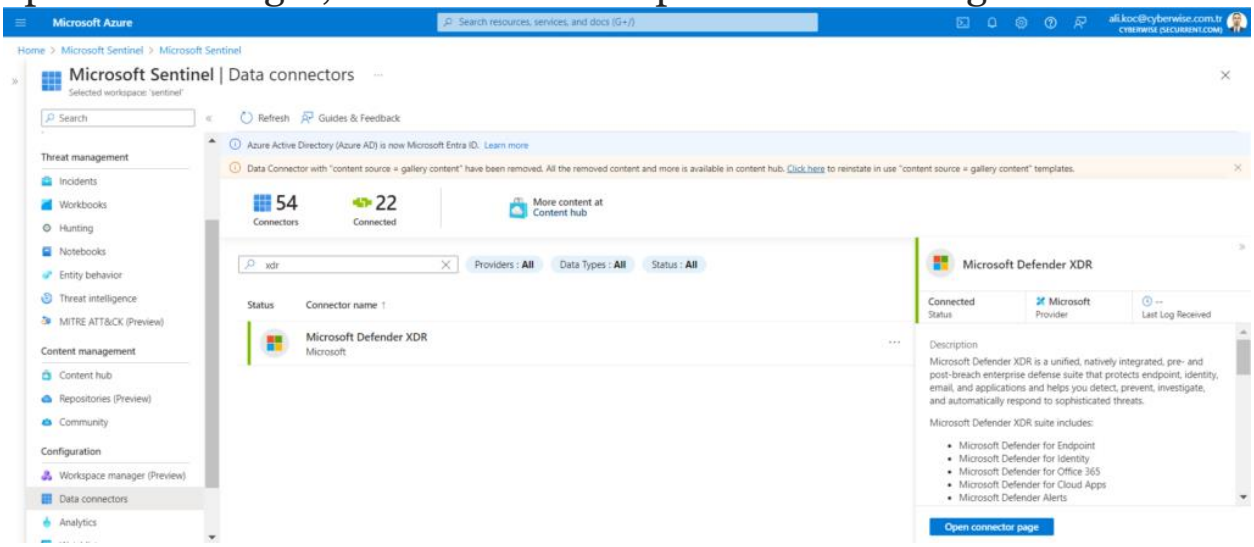
Prerequisites

- **Workspace:** read and write permissions.
- **Connector Access Control** : The user who will apply changes to the Connector must be a user of the tenant to which the Workspace belongs.
- **Tenant Permissions:** The tenant where the Workspace is located must have ' **Global Administrator** ' or ' **Security Administrator ' roles.**
- **License:** M365 E5, M365 A5 or any Microsoft Defender XDR must have a license suitable for use.

setup

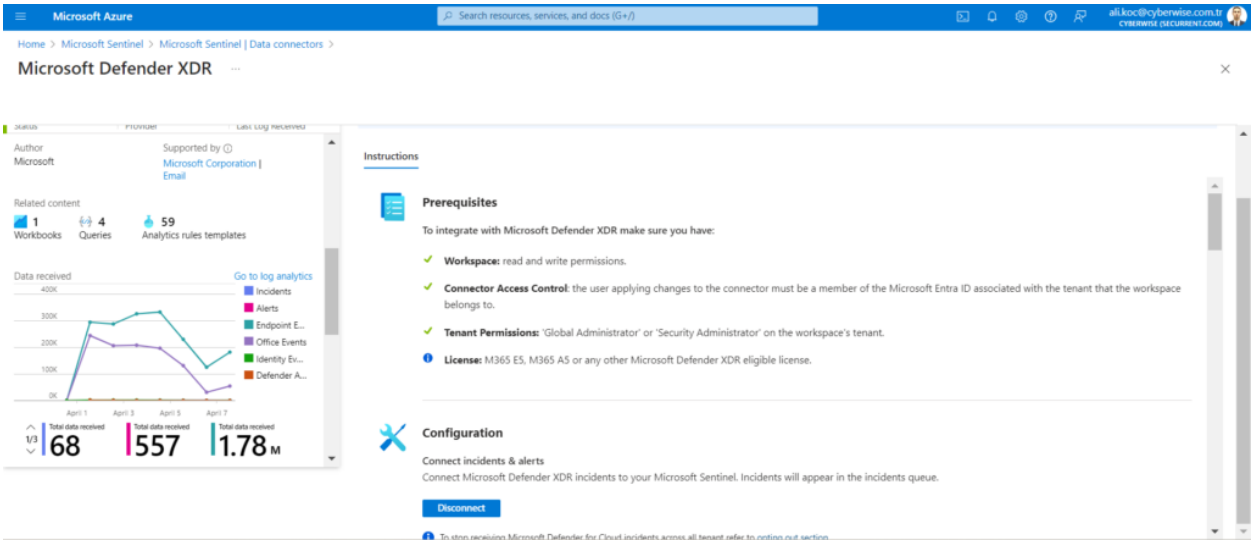
[We go to portal.azure.com](portal.azure.com) > **Microsoft Sentinal** .

We go to the Data Connector section on the left panel and find the **Microsoft Defender XDR** data connector. In the window that opens on the right, we click on the “Open Connector Page” button.



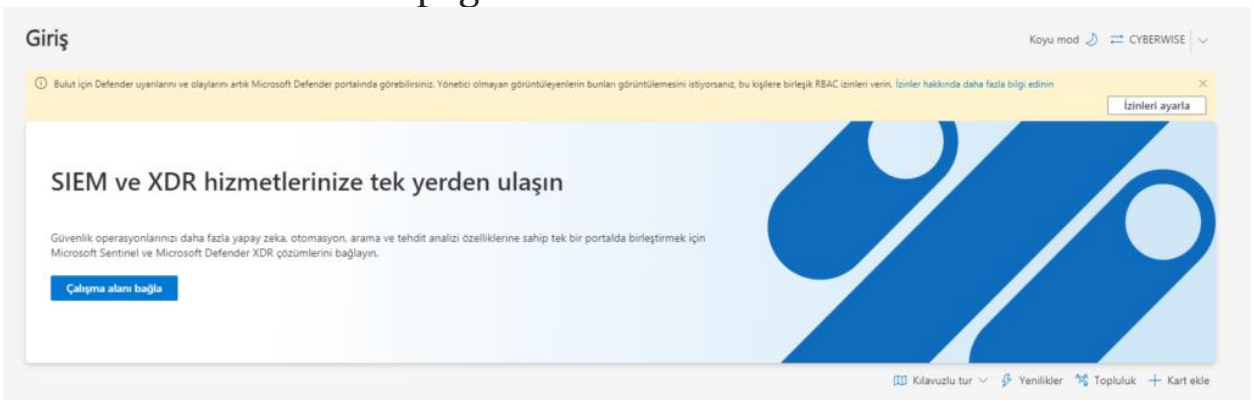
- **Connect events and alerts:** This provides basic integration by synchronizing events and alerts between both platforms.
- **Connect entities:** This integrates on-premises Active Directory user identities with Microsoft Sentinel via Microsoft Defender for Identity.
- **Connect events:** This enables the collection of raw advanced hunting events from Defender components for in-depth analysis.

Important Note: To disable a specific component's connector, the Microsoft Defender XDR connector must first be disconnected.

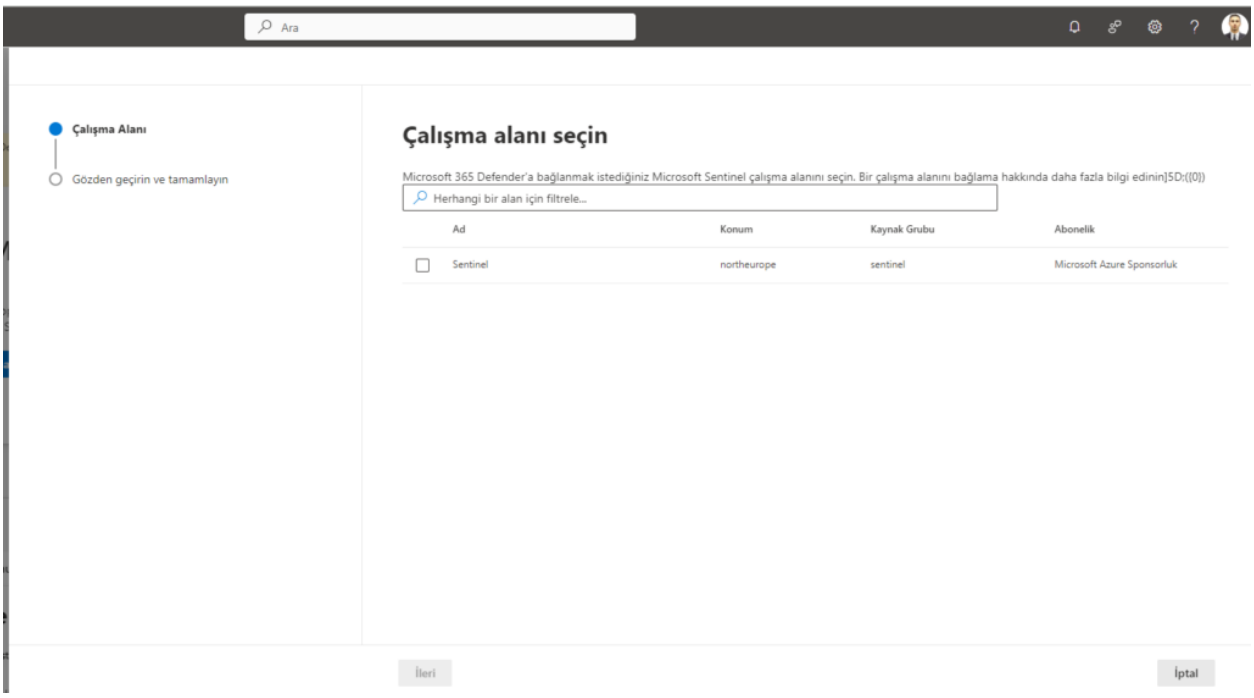


Now we can make the connection in Defeder XDR .

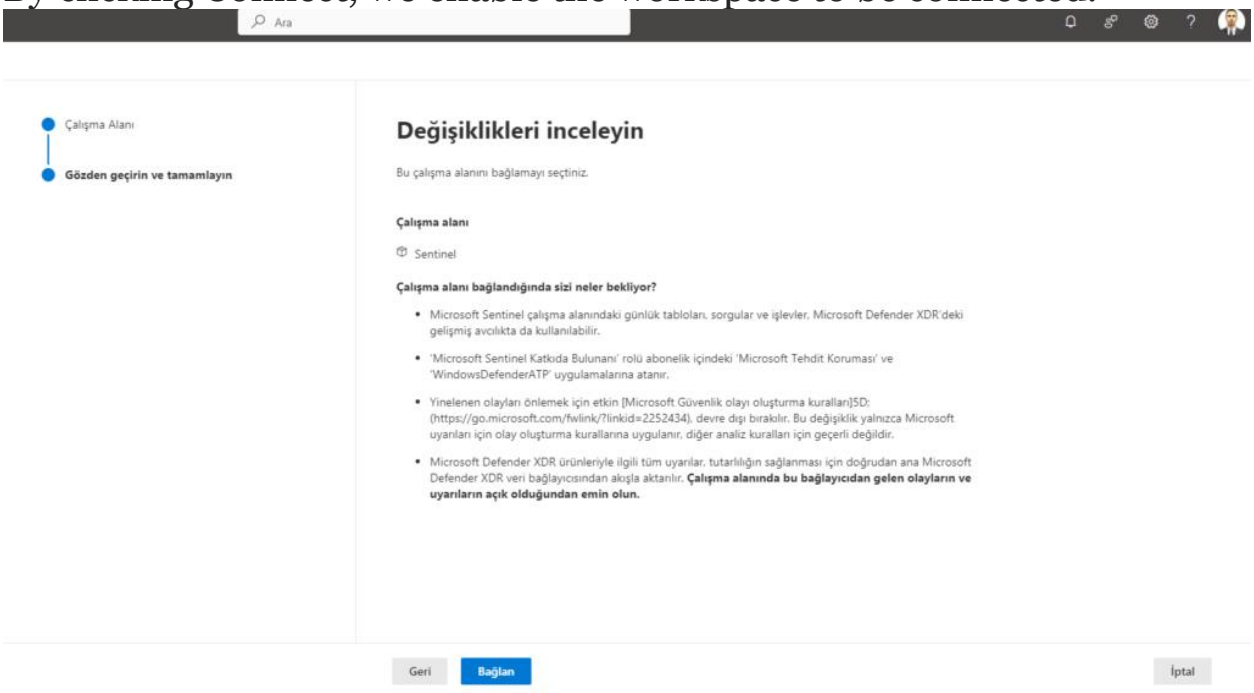
When we log in to security.microsoft.com, we will see a guide for the connector on the home page.

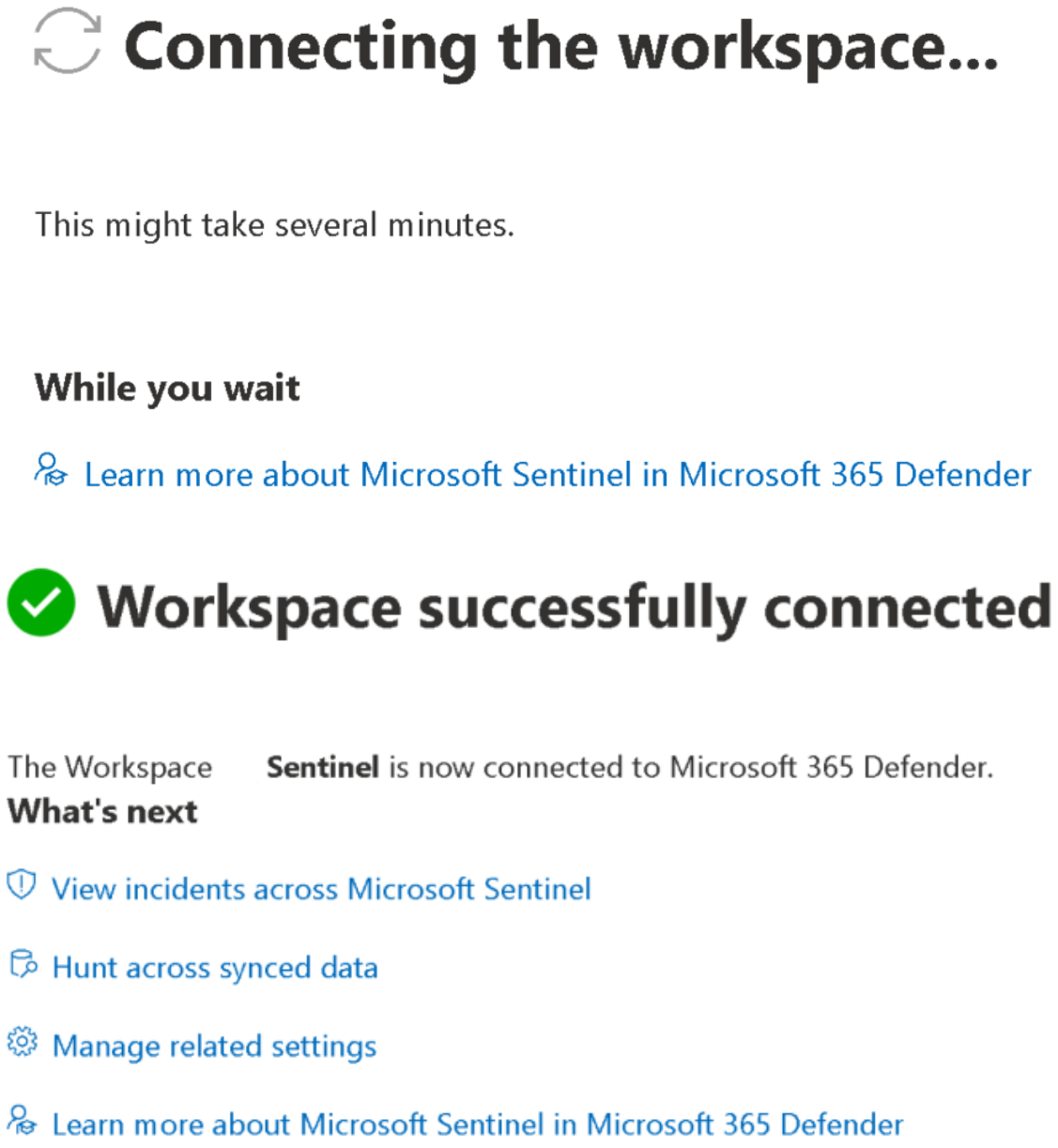


In the window that opens after the Connect Workspace option, we select the relevant Sentinel Workload and click "next".

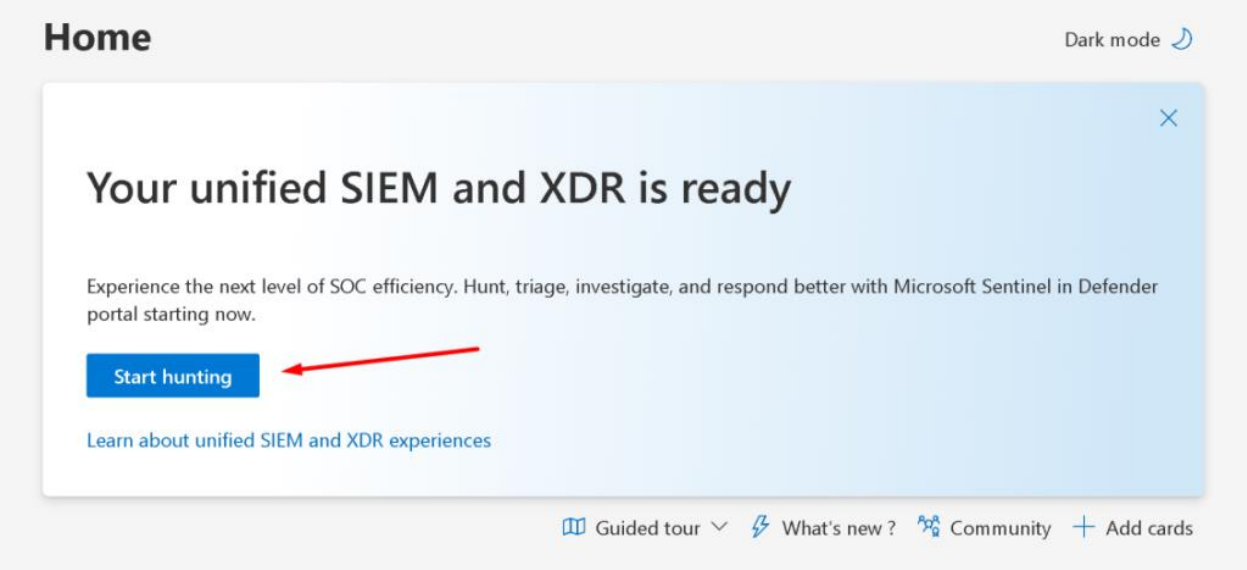


By clicking Connect, we enable the workspace to be connected.

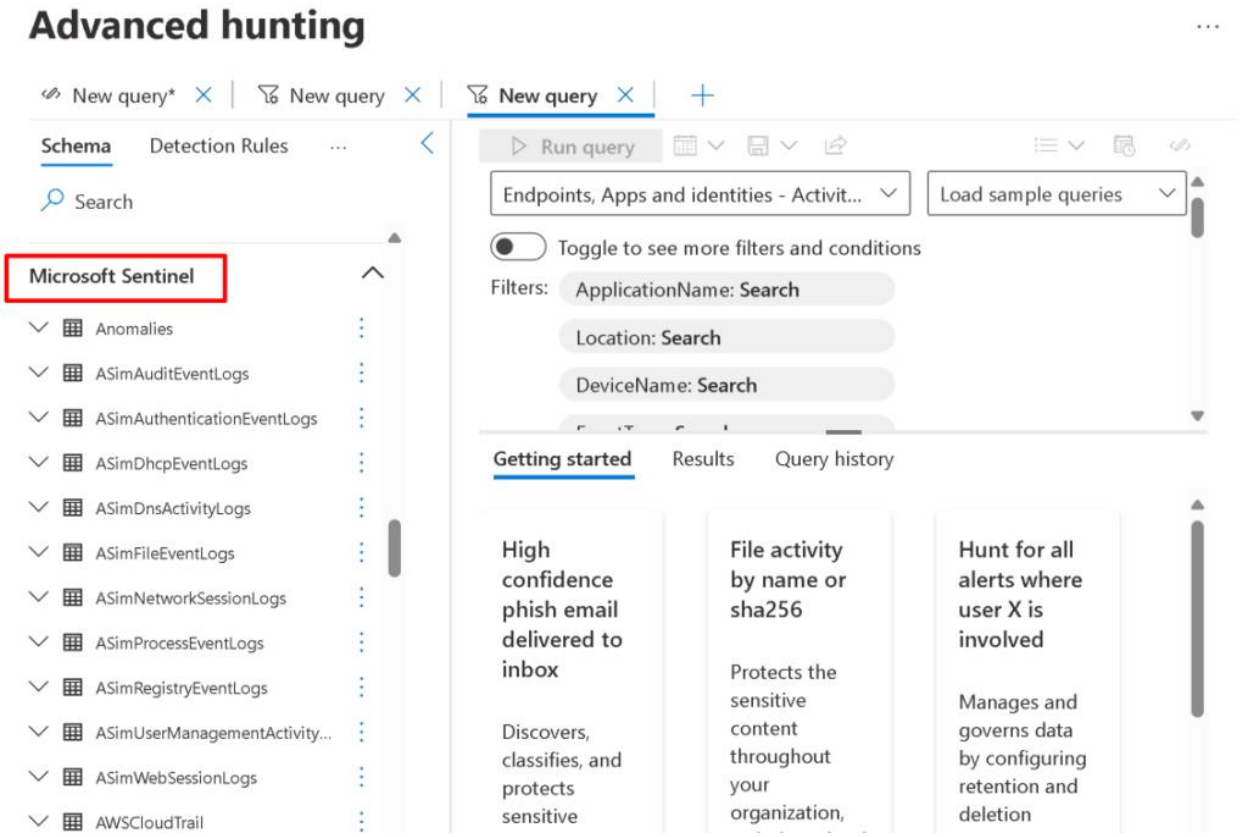




When we enter security.microsoft.com again, we will see the following screen.



We can now see the Sentinel tab in the Defender for Endpoint Advanced Hunting section.



You can use advanced hunting KQL queries to examine data from both Microsoft Defender XDR and Microsoft Sentinel. When you first access the advanced hunting page after connecting to Workspace, you can see your Sentinel tables categorized by solution under the Microsoft Defender XDR tables in the Schema tab.

To use a Sentinel function, go to **the Function** tab and find the function you want. Double-click the function name to add it to the query editor. Alternatively, click the ellipsis (⋮) next to the function and select “Insert to query” to insert it into a query.

You can use it to improve threat detection in your environment with the Custom Detection Rule (link). You can drill down to the rules applied to the data received via the connected Sentinel Workspace.

To briefly summarize the changes to be expected during the research process in Microsoft Sentinel and Microsoft Defender XDR:

Microsoft Defender XDR:

- Events from Sentinel can be seen in the events queue.
- You can filter events by selecting Microsoft Sentinel as the service source.
- Alerts originating from Microsoft Sentinel appear in the alert queue.

- Filtering options include selecting Microsoft Sentinel as the service or detection source.
- If you turn off events in Defender XDR it will also be turned off in Sentinel

Microsoft Sentinel:

- The reception of data is transferred to the XDR connector.
- Event creation rules are automatically disabled.
- Custom event titles are created for aggregated alerts.
- The default event provider is Microsoft Defender.
- Editing comments, adding/removing alerts, and tasks are not supported.
- Automation rules now contain detailed information about updates.
- If you turn off events in Sentinel, they are also turned off in Defender XDR.

Up to 150 alerts to events can be displayed in Sentinel. If a Defender XDR event exceeds the 150 alert threshold, Sentinel will display 150+ alerts and also provide an extra link to access the entire alert set in Defender

In conclusion, Microsoft is really making a serious effort to unify the different portals. It continued to support the Unified perspective, first by connecting it to the Defender portal for MDI and Cloud Applications, and now by connecting its Sentinel Workspace to it as well.
I can see that in the future, we will be able to reach all security stakeholders from a single page :)

Source: **Learn Microsoft , CCP , Sonne's Cloud**