

# Microsoft Sentinel Integration

**Microsoft Sentinel**, previously called Azure Sentinel, is a cloud-based **security information and event management (SIEM)** and **security orchestration automated response (SOAR)** platform offered by Microsoft and managed as an Azure resource. You can think of Sentinel as an additional layer for a mature **security operations center (SOC)**, where Microsoft 365 Defender telemetry, alerts, and incidents are combined with those from other services, such as other Microsoft data sources or third-party applications and appliances.

As Sentinel's use grows, it's important to learn about how it relates to and its integrations with Microsoft 365 Defender. So, in this chapter, you'll learn about the following:

- The relationship and differences between Sentinel and Microsoft 365 Defender
- The different types of integrations available and enabling them

Let's kick things off by reviewing how the two services differ and integrate.

## Understanding Microsoft 365 Defender's relationship with Sentinel

As explained in the introduction to this chapter, Sentinel allows for security response and incident management to many different services. This

is achieved using **data connectors**.

Included in the Microsoft 365 Defender connector are the main services of MDE, MDI, MDO, and MDA. You'll also find services not strictly under the Microsoft 365 Defender banner but that produce alerts there, such as Azure AD Identity Protection and Microsoft Purview DLP.

If you're a Sentinel customer, enabling these integrations means you can stick with Sentinel as the go-to interface for alert and incident response, rather than having to jump between it and Microsoft 365 Defender's queue. This improves your time to respond, as well as the benefits of a broader picture thanks to connectors. It also provides a means to improve your retention beyond Microsoft 365 Defender's limit of 30 days for advanced hunting or 180 days for other information.

The relationship between Sentinel and Microsoft 365 Defender is depicted visually in the following figure:

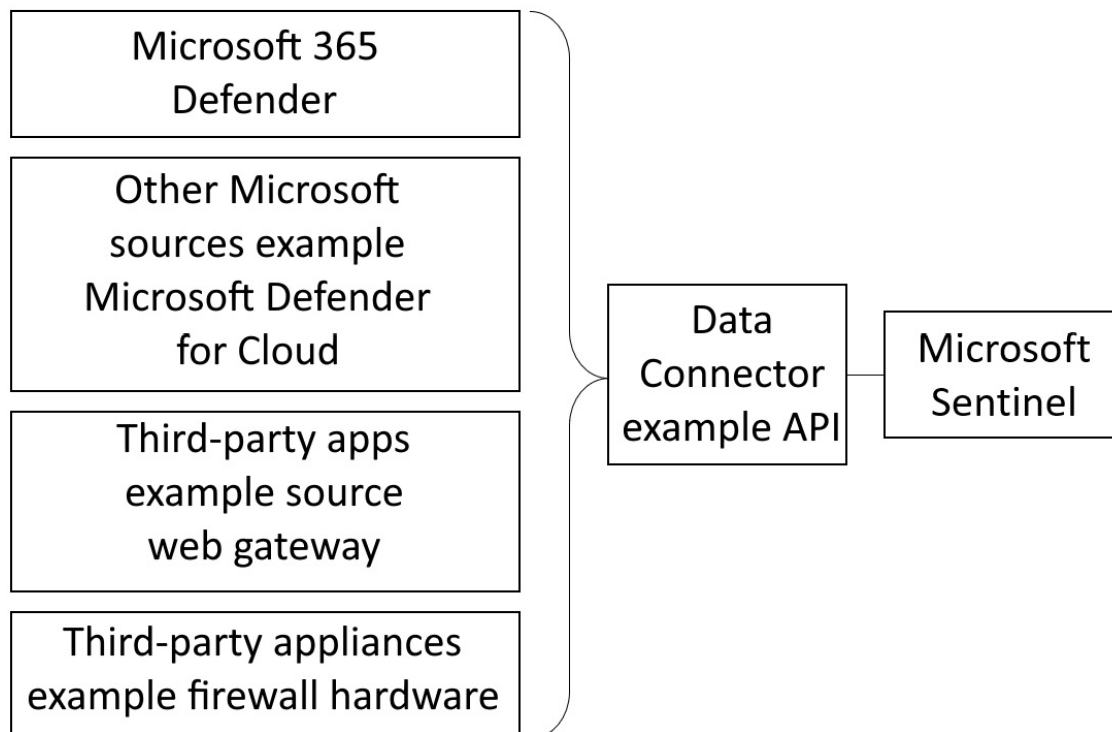


Figure 20.1 – Sentinel's relationship with Microsoft 365 Defender

*As you'd expect, a full overview and guide on Microsoft Sentinel are beyond the scope of this book. You can refer to the Further reading section of this chapter for some great Sentinel resources.*

There is some latency between alerts and incidents appearing in Microsoft 365 Defender and then appearing in Sentinel: expect up to 10 minutes. When a Microsoft 365 Defender incident appears in Sentinel, a bi-directional connection is maintained. This keeps the two in sync so that if the status or owner changes in one place, it's reflected in the other.

If the incident continues to generate information in Microsoft 365 Defender, this too continues to sync to Sentinel. This includes merging one incident into another. For example, you'll see new entities in the Sentinel incident if Microsoft 365 Defender connects them to the incident. Incident changes, unlike the original link from Microsoft 365 Defender to Sentinel of up to 10 minutes, are lower latency and should happen almost immediately.

One caveat of syncing incidents is, at the time of writing, Sentinel's limit of 150 alerts per incident. This isn't the case in Microsoft 365 Defender, so what you'll see in Sentinel if there are more than 150 alerts in an incident is a hyperlink to the Microsoft 365 Defender portal.

Now that we've explained the *why* and *what* of Microsoft 365 Defender's connection with Sentinel, let's review the *how*.

## Connecting Microsoft 365 Defender to Sentinel

To establish the connection between Microsoft 365 Defender and Sentinel, you need to complete some actions in Sentinel, which you can do in the Azure portal. You should be a Global or Security Administrator to complete these processes.

There are three types of integrations you can configure:

- Incidents and alerts
- Advanced hunting events
- **User and Entity Behavior Analytics (UEBA)**, based on MDI

Of these, incidents and alerts do not have an additional cost. These are the **SecurityIncident** and **SecurityAlert** data types, respectively.

Advanced hunting and UEBA have a cost based on the amount of data and analysis, the details of which you should review independently, including using the pricing information provided in the *Further reading* section in this chapter.

We'll begin the discussion on how to connect Microsoft 365 Defender to Sentinel with incidents and alerts.

## Using incidents and alerts

In this section, we're going to follow some simple steps to start syncing Microsoft 365 Defender incidents and alerts to Sentinel:

1. In your Sentinel workspace, head to **Configuration | Data connectors**.
2. Search for and select **Microsoft 365 Defender | Open connector page**, which will look similar to the following screenshot:

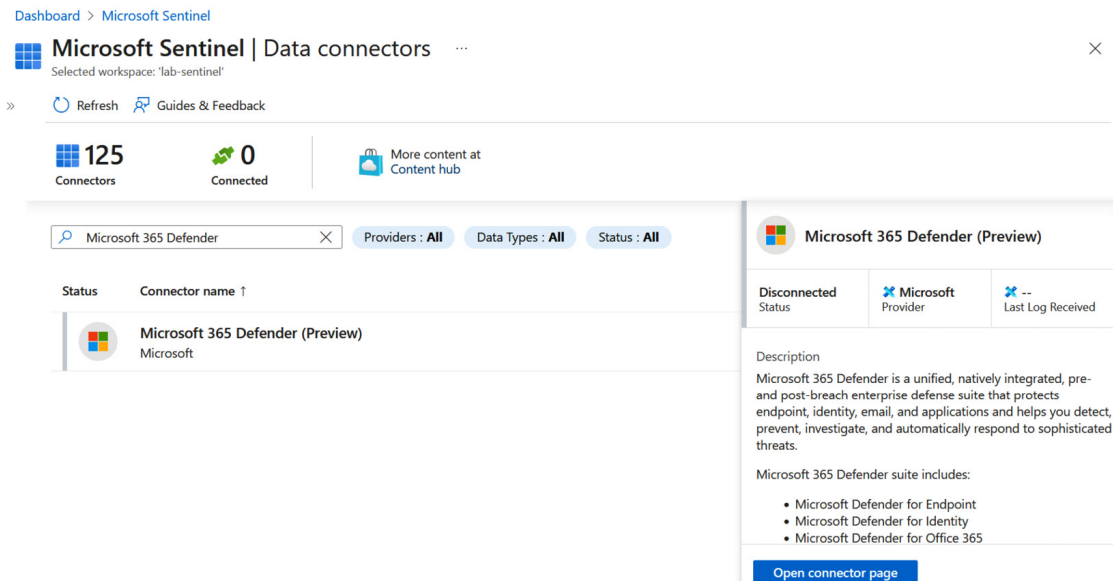


Figure 20.2 – Finding the Microsoft 365 Defender connector page

- Under **Configuration**, make sure that **Turn off all Microsoft incident creation rules for these products** is selected. This prevents duplicates from being created so that rather than having both the Microsoft Sentinel and Microsoft 365 Defender “engines” create incidents, only Microsoft 365 Defender does (then propagates them to Sentinel).
- Click the **Connect incidents & alerts** button to enable the connector:

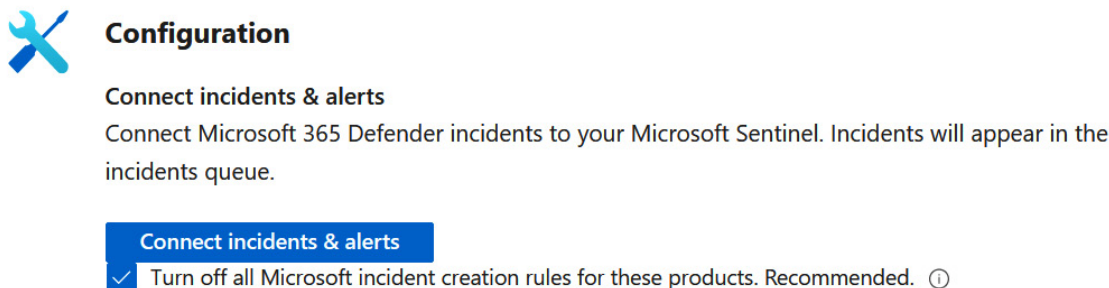


Figure 20.3 – Connecting incidents and alerts from Microsoft 365 Defender to Sentinel

- A validation process will take place, followed by a success confirmation. You’ll see the **Connect incidents & alerts** button transform into a **Disconnect** button.
- Returning to **Configuration | Data connectors**, you’ll find that not just Microsoft 365 Defender has been enabled as a connector. You’ll see that connectors for other Microsoft 365 Defender services have been enabled too:

1. Azure Active Directory Identity Protection
2. Microsoft Defender for Cloud Apps (in addition to **Alerts**, which are on by default, you can click on this one to enable **Cloud Discovery Logs**)
3. Microsoft Defender for Endpoint
4. Microsoft Defender for Identity
5. Microsoft Defender for Office 365

From now on, incidents in Microsoft 365 Defender will appear as incidents in Sentinel with bi-directional sync. You'll know it's a Microsoft 365 Defender incident because the product name referenced (**ProviderName** in KQL) is **Microsoft 365 Defender**, and there will be a hyperlink labeled **Investigate in Microsoft 365 Defender**:

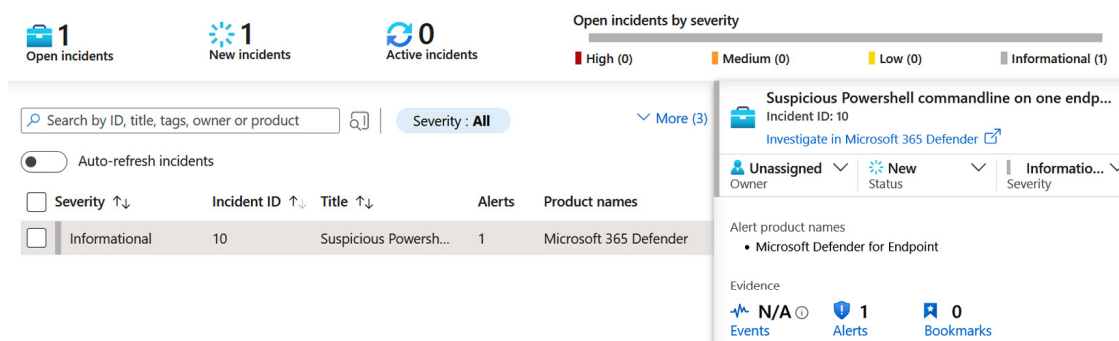


Figure 20.4 – A Microsoft 365 Defender incident in Sentinel

Now that we know how to sync incidents with Sentinel, let's look at how to ingest advanced hunting data too.

## Using advanced hunting data

By default, you won't find that the raw advanced hunting data has been transmitted to your Sentinel workspace. To enable this, head back to **Microsoft Sentinel | Configuration | Data connectors | Microsoft 365 Defender | Open connector page**.

You'll find a list of advanced hunting tables under the **Connect events** section. Simply check the boxes you need, then click on **Apply Changes**:

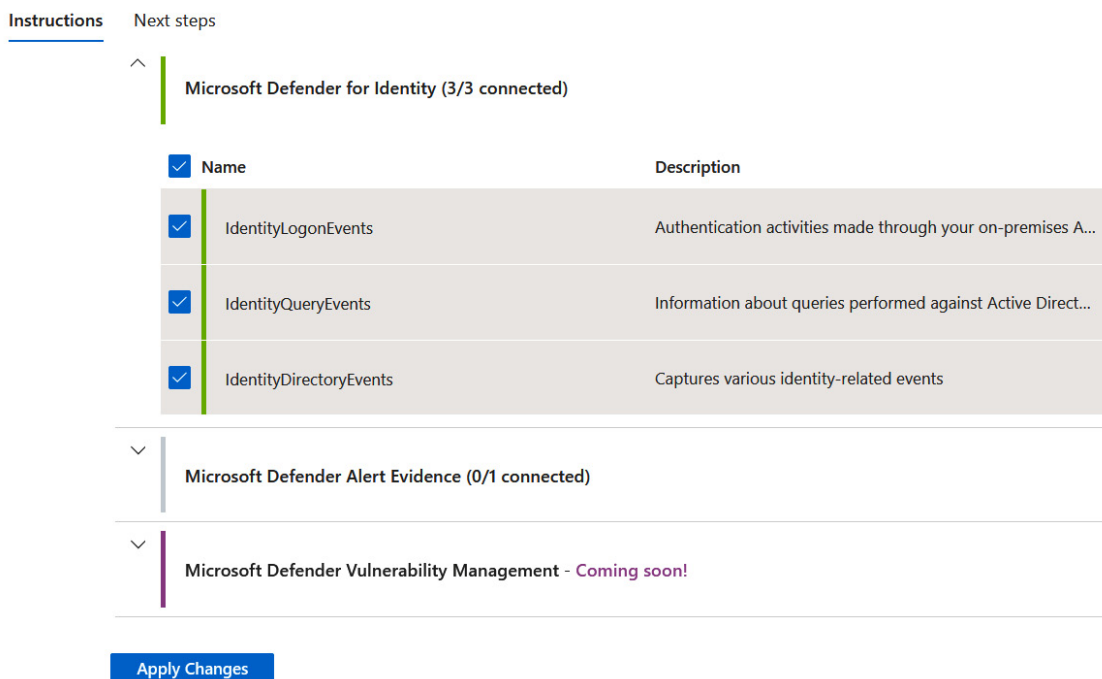


Figure 20.5 – Connecting events (advanced hunting) to Sentinel

Two connections down, one more type to look at: entities. We'll check it out in the next section.

## Enabling the UEBA feature

Sentinel has UEBA capabilities that were primarily based on Azure AD for user entities but now include Active Directory (on-premises). This is based on MDI telemetry, so as a prerequisite, you must have that deployed.

Here are the steps to add on-premises AD data to Sentinel's UEBA capabilities:

1. Head to **Microsoft Sentinel | Configuration | Data connectors | Microsoft 365 Defender | Open connector page**.
2. In the **Connect entities** section, choose **Go to UEBA configuration page**.
3. On the **Entity behavior configuration** page, you can choose **Turn on the UEBA feature** if you haven't done so already, and click the box to add **Active Directory** as a directory service:

[Dashboard](#) > [Microsoft Sentinel | Data connectors](#) > [Microsoft 365 Defender \(Preview\)](#) >

## Entity behavior configuration


### 1. Turn on the UEBA feature

You must complete step 2 for UEBA functionality to start.

☒ On  Only a Global Administrator or a Security Administrator in your Azure Active Directory can turn this feature on or off

### 2. Sync Microsoft Sentinel with at least one of the following directory services

This will create profiles for the users and entities in your organization and also creates data stores in Microsoft Sentinel

 Only tenants onboarded to Microsoft Defender for Identity can enable Active Directory syncing

<input checked="" type="checkbox"/>	Active Directory (Preview)
<input checked="" type="checkbox"/>	Azure Active Directory

Apply

Figure 20.6 – Adding AD for UEBA via MDI

You’ve now learned about the three types of connections you can make between Microsoft 365 Defender and Sentinel. Let’s head onto the summary to revisit and conclude this chapter.

## Summary

In this chapter, you learned that Microsoft Sentinel is a SIEM and SOAR solution that improves the *single-pane-of-glass* desire of SOC teams. Where Microsoft 365 Defender goes *deep* for the services it is scoped to (MDE, MDO, MDI, MDA, and MDVM), Sentinel goes *broad*.

If your team already uses Sentinel, you now know the advantages of creating the sync between it and Microsoft 365 Defender, as well as how that sync operates, with bi-directional integration for improved response times and incident management. We covered the steps for creating the three types of integration (incidents/alerts, advanced hunting data, and UEBA) so that you can maximize your investment in the platform.

Sentinel’s SOAR capabilities offer a means to automate security incident response. In the next chapter, we’ll look at the APIs that allow program-



matic access to Microsoft 365 Defender for additional automation and integration capabilities.

## Questions

To test your understanding of integrating Microsoft 365 Defender with Microsoft Sentinel, take a shot at the following questions:

1. A serious incident in your Microsoft 365 Defender portal is made up of 140 alerts. How would you expect Microsoft Sentinel to respond to this? Choose one.
  1. Sentinel will split the incident into two incidents
  2. Sentinel will have one incident with all alerts
  3. Sentinel will redirect you to Microsoft 365 Defender to see all the alerts
  4. Sentinel will hide alerts with a lower priority
2. Which of the following components would not fall into scope for Microsoft 365 Defender's connector to Sentinel? Choose all that apply.
  1. Azure Active Directory Identity Protection
  2. Microsoft Defender Vulnerability Management
  3. Microsoft Purview Data Loss Prevention
  4. Microsoft Defender for SQL
3. You are using Microsoft Sentinel to create queries for your SOC team. Which of the following tables would be most appropriate to find out the severity of an alert as determined by Microsoft 365 Defender? Choose one.
  1. **EmailUrlInfo**
  2. **AlertInfo**
  3. **IncidentInfo**
  4. **DeviceEvents**
4. True or false: incidents created by the Microsoft 365 Defender connector for Microsoft Sentinel must be closed separately.
  1. True
  2. False

5. True or false: Microsoft 365 Defender's retention period, as specified at [security.microsoft.com](https://security.microsoft.com) under **Settings**, sets the hard limit of Microsoft Sentinel's data retention for Microsoft 365 Defender advanced hunting events.
1. True
  2. False

## Further reading

There is a lot more to learn about general Microsoft Sentinel usage than we can cram into this book. Check out the following links for useful resources:

- Rod Trent of Microsoft has championed KQL more than anyone. You can find his Must Learn KQL repository on GitHub, including purchase options for a hard copy book of the same name, to help you master KQL: [github.com/rod-trent/MustLearnKQL](https://github.com/rod-trent/MustLearnKQL).
- Another must-visit GitHub repository is Matt Zorich's, which is home to a massive list of his custom queries and the #365daysofKQL series: [github.com/reprise99/Sentinel-Queries](https://github.com/reprise99/Sentinel-Queries).
- Want to join a community and learn, share, or practice the Sentinel query language? The KQL Café, run by Gianni Castaldi and Alex Verboon, hosts regular meetups to cover all things Kusto: [kqlcafe.github.io/website](https://kqlcafe.github.io/website).
- For the most comprehensive book on Microsoft Sentinel you'll find, check out *Microsoft Sentinel in Action – Second Edition*, from Packt Publishing: [packtpub.com/product/microsoft-sentinel-in-action-second-edition/9781801815536](https://packtpub.com/product/microsoft-sentinel-in-action-second-edition/9781801815536).
- The Microsoft Sentinel pricing page is useful for understanding and calculating the cost of Microsoft Sentinel for your environment: [azure.microsoft.com/en-gb/pricing/details/microsoft-sentinel](https://azure.microsoft.com/en-gb/pricing/details/microsoft-sentinel).