Microsoft Security

Cloud-Native SIEM: Quick Start Guide to Azure Sentinel

Contents

Digital and cloud transformation continue to reshape IT. Information security leaders face growing complexity, diverse attack surfaces, alerts growing by orders of magnitude, as well as increasingly sophisticated and difficult-to-detect cyber assaults, including insider threats—all in the context of exponential growth in data volume. At the same time, they need to find ways to make systems and processes more efficient, control costs, and manage resources.

As IT becomes more strategic, the importance of security grows daily

A compromised digital business loses trust, customers, and revenue. Cyber defense will not suffice. Only a proactive approach to risk answers the call. Organizations need the ability to connect and collect data from all systems, whether in the cloud or on premises, commercial or homegrown.

Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks. Costly to operate and slow to scale, resource-heavy SIEM infrastructure and tools can easily become obstacles to digital transformation. Ever-growing volumes of data strain the limits of on-premises systems. Managing those same systems creates a huge operational burden that takes time away from strategic activities. Alert fatigue is reaching all-time highs, yet few organizations want to throw more money at the problem.

Traditional approaches simply can't handle the pace of change, and IT departments don't have more money to throw at the problem.

That's why Microsoft developed Azure Sentinel, a fully cloud-native SIEM designed to serve all four aspects of security operations.

- **Collect** data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.
- **Investigate** threats with AI and proactively hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks.

Built on Microsoft Azure, a leading public cloud platform, Azure Sentinel eliminates infrastructure and management complexity. It scales readily to meet dynamic needs. It maximizes the skills of your entire team with intelligent, role-based tools. And, it empowers you with insights from Microsoft's global security operations.

Why Azure Sentinel?

Azure Sentinel offers tools for all members of your security team

Improve threat protection with AI on your side: Intelligent correlation helps reduce false positives and alert fatigue by up to 90 percent and can detect complex, multi-stage attacks giving you the power to focus on what matters. Built-in intelligence helps automate and orchestrate up to 80 percent of common tasks, simplifying operations, and accelerate threat response.

Secure your entire enterprise: Integrate with existing tools, whether business applications, other security products, or home-grown software. Analyze data from users, applications, and infrastructure, both on-premises and multi-cloud. Get started fast and grow as needed with a broad range of connectors and industry-standard data formats.

Invest in security, not servers: Powered by the Microsoft cloud platform, Azure Sentinel delivers near-limitless speed and scale without the operational hassle of server-based SIEM. Proven, scalable log analytics get you insights in seconds. That means lower cost, more agility, and more time to focus on real security issues.

Free storage and analysis for Office 365 data: To help you maximize security effectiveness across your enterprise, Azure Sentinel empowers you to bring in data from Microsoft Office 365 for analysis and retain it for free, all in just a few clicks.

Build on Microsoft's investment: In security, knowledge is power. With Azure Sentinel, you gain the power of Microsoft's decades of experience managing security at a massive global scale. Microsoft solutions share insights gained from unparalleled threat intelligence that is informed from analyzing trillions of signals every day. Our security experts support proactive threat hunting with prebuilt queries based on years of security experience.

The role of Log Analytics

Azure Sentinel is built on the highly scalable, high performance Azure Monitor Log Analytics platform. Log Analytics is a proven analytics platform designed to store and analyze massive amounts of data in seconds.

Log Analytics uses Kusto query language (KQL), a rich language designed to be easy to read and author. It allows you to join data from multiple tables, aggregate large sets of data, and perform complex operations with minimal code. Virtually any question can be answered quickly and analysis performed as long as the supporting data has been collected.

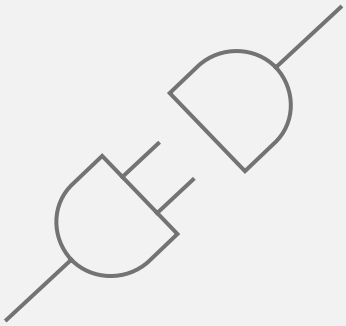
Meeting the needs of security roles

Azure Sentinel offers tools for all members of your security team. For example, security operations professionals can get alerts, investigate incidents, and remediate using automated tools. Security analysts and researchers employ its easy-to-learn query language for proactive threat hunting. Decision makers instantly view data across the enterprise using interactive dashboards. Each toolset saves time and helps people contribute maximum value in their roles.

Getting started with Azure Sentinel

Step 1

Access Azure Sentinel



Azure Sentinel is built on the Azure platform. It provides a fully integrated experience in the Azure portal to augment other Azure services, such as Azure Security Center and Azure Machine Learning. If you don't already have one, the first step is to create an **Azure free account**. (Please refer to the **pricing page** to learn about total costs for Azure Sentinel.)

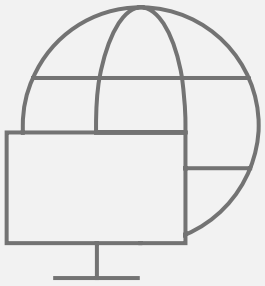
Once you have an Azure account, simply search for Azure Sentinel in the Azure portal and click +Add to add it to your portal.

Note you will also need the following:

- A Log Analytics workspace. Learn how to create a **Log Analytics workspace**.
- Contributor permissions to the subscription in which the Azure Sentinel workspace resides.
- Contributor or reader permissions on the resource group that the workspace belongs to.
- Additional permissions may be needed to connect specific data sources. Data ingestion pricing may differ among services. For more information, see the **Azure Sentinel pricing page**.

Step 2

Connect your data

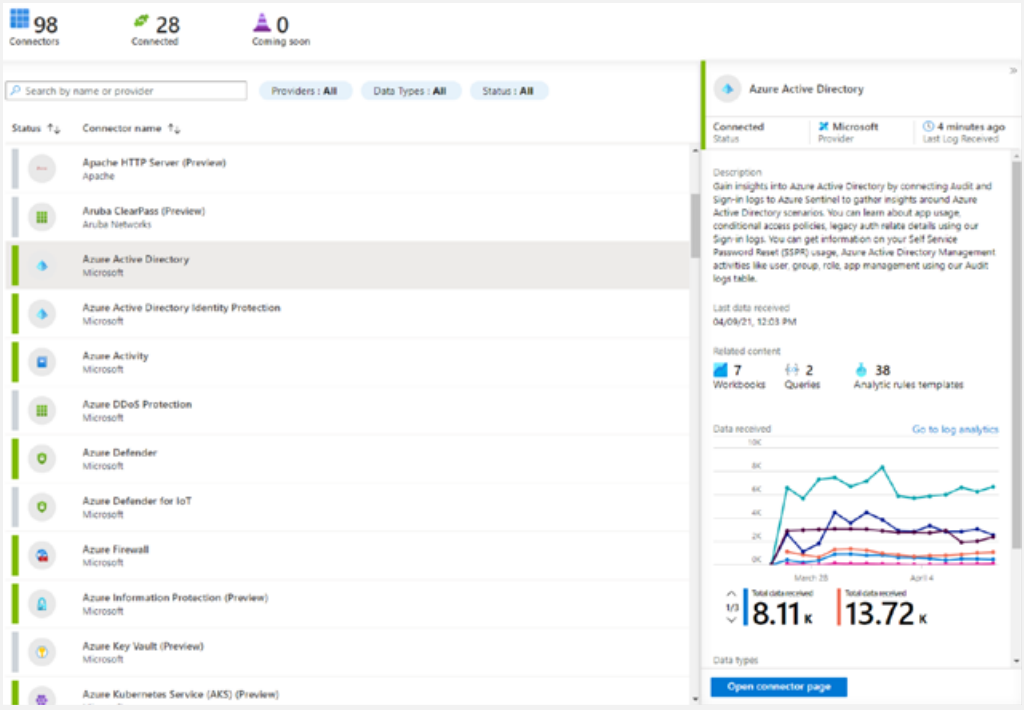


Azure Sentinel includes connectors providing real-time integration with many industry solutions. It enables easy connections to a variety of Microsoft services, such as Office 365, Azure Active Directory, Azure Advanced Threat Protection, and Microsoft Cloud App Security. You can also collect data from existing security solutions such as firewalls, routers, endpoint security, and many more using built-in connectors. Plus, you can use Common Event Format (CEF), Syslog, or REST-API to connect any compliant data source to Azure Sentinel.

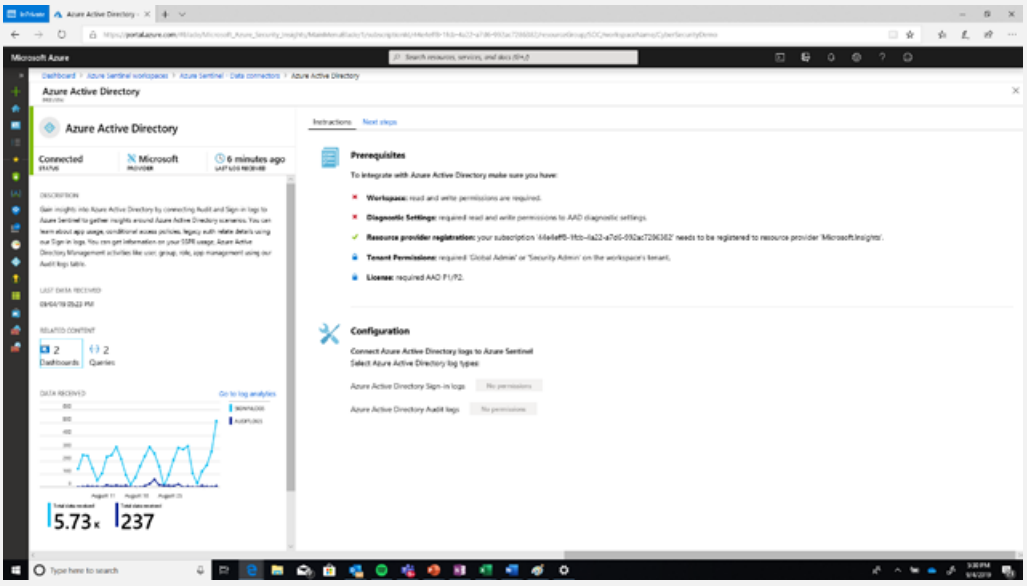
To connect to a data source:

1. Sign in to Azure with account credentials. Navigate to Azure Sentinel.
2. Click **Data connectors**.
3. Click the row for the data source you wish to connect.
4. Click the **Open connector** page to see the configuration steps for connecting the data source.

After your data sources are connected, your data starts streaming into Azure Sentinel and is ready for you to use. For information about data connectors, see **Connect Data Sources**.



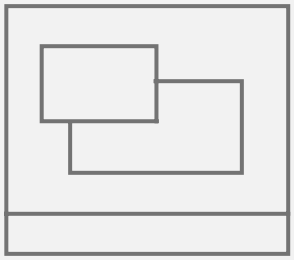
Click the row for the data source you wish to connect.



After you have clicked **Open connector**, you will see the configuration steps for connecting the data source you selected.

Step 3

Use overview dashboard and workbooks to get visibility across enterprise



You can use workbooks to view data, or create a new dashboard, either from scratch or based on an existing one. These are based on **Azure Monitor Workbooks** which enable rich, interactive reports for the data you have collected.

Overview dashboard

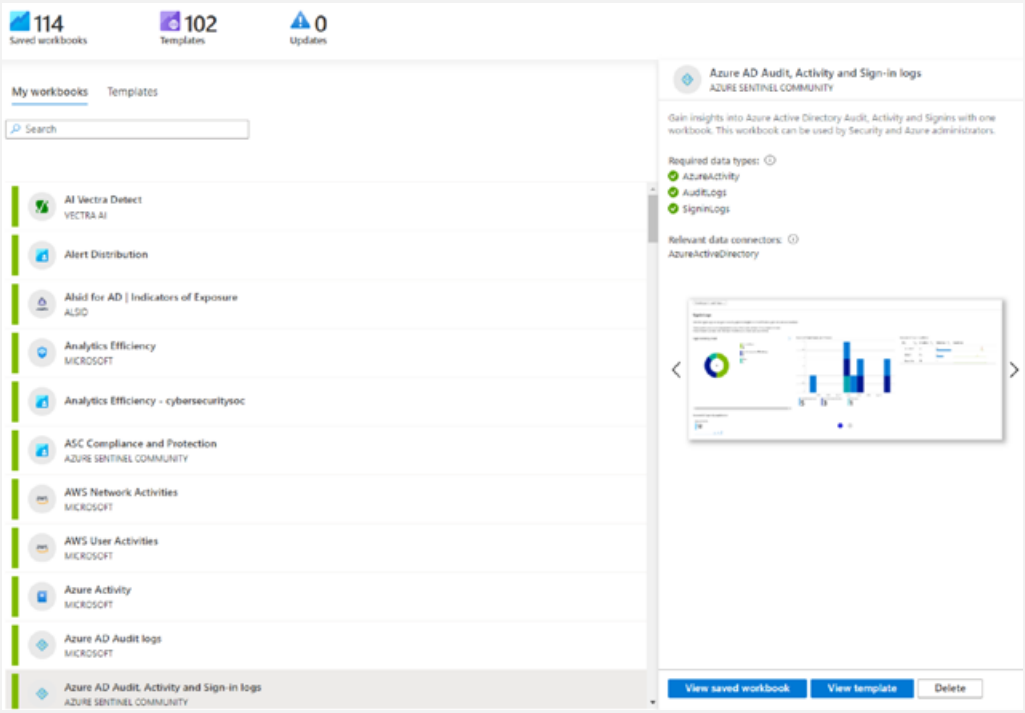
Start with the **Overview** dashboard, which provides insight at a glance into the security status of your workspace:

- **Events and alerts over time:** View the number of events and how many alerts were created from those events.
- **Potential malicious events:** Receive alerts when traffic is detected from sources that are known to be malicious.
- **Recent incidents:** View your most recent incidents, their severity, and the number of alerts associated with each incident.
- **Data source anomalies:** Use models created by Microsoft's data analysts to search your data sources for anomalies.

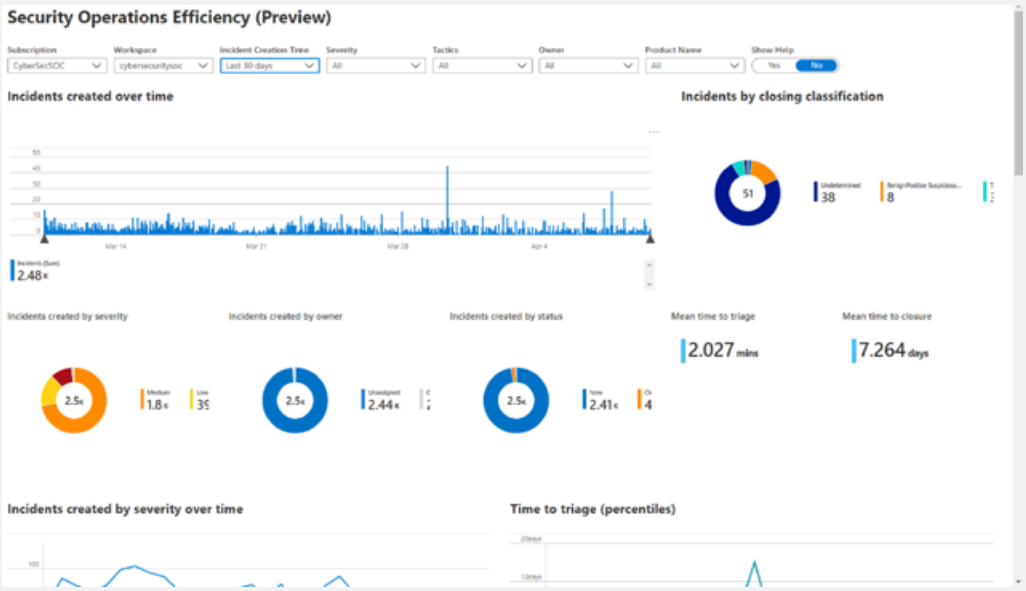
The **Overview** dashboard provides insight into the security status of your workspace.

Use built-in workbook templates to get interactive dashboards for specific data sources

For additional visibility on specific data sources, you can use built-in templates. These workbooks provide contextual insights for the data collected and analyzed from specific sources, including information on data collected from Office 365, Azure Active Directory, Palo Alto Networks, Symantec, AWS, and many other sources.



My workbooks houses the workbooks you have saved or created.



Each workbook provides contextual insights for data collected and analyzed from specific sources.

In the Azure Sentinel menu under **Threat management** select **Workbooks**.

1. You can see the built-in dashboard templates under the **Templates** tab. Click the row for the template source you wish to view, make sure you have the relevant data types, and click **View workbook** to see the template.

If you're using Azure AD, we recommend that you view the following dashboards:

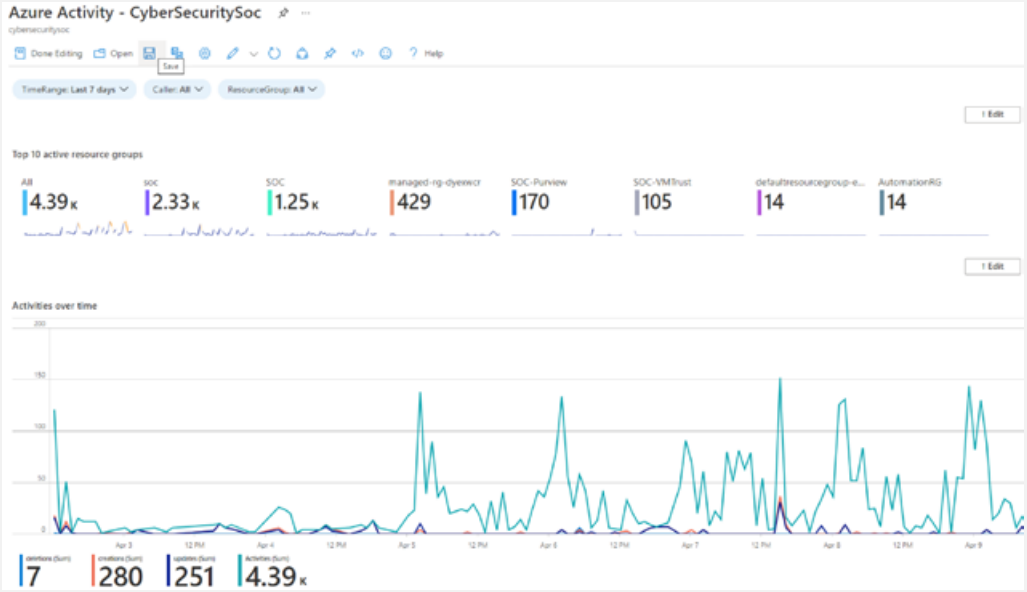
- **Azure AD sign-ins** analyzes sign-ins over time to see if there are anomalies.
- **Azure AD audit logs** analyzes admin activities, such as changes in users, group creation, and modifications.

2. Under the **My workbooks** tab, you will be able to see the workbooks that you have saved or created.

Get custom views and insights across different data sources

Customize an existing workbook template:

1. Click the row for the template source you wish to edit, then click **Save**.
2. Select a location where you want to save this workbook. This saves the workbook template and not the data.
3. Click **View workbook**.
4. Click **Edit**.



To customize an existing template, click the row for the template source you wish to edit, then click **Save**.

Create a new workbook to get a customized dashboard:

1. Click +**Add Workbook** to create a new workbook.

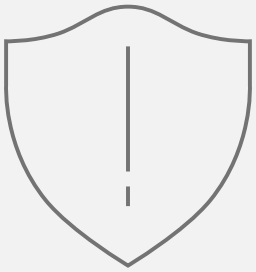
2. Save the workbook using the save button; make sure to save it under your Azure Sentinel Subscription and Resource Group.

3. Edit the workbook using the Edit button. Make sure to save again after changing the workbook.

More information and guidelines on how to create visualizations in Azure Sentinel can be found in the "**Create interactive reports with Azure Monitor Workbooks**" documentation.

Step 4

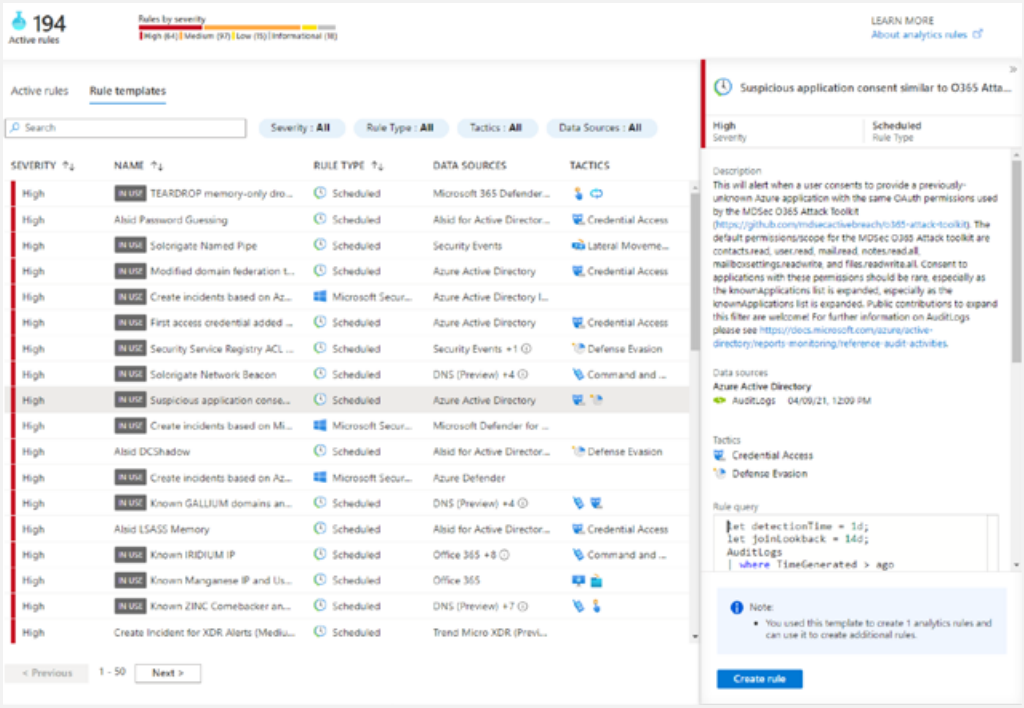
Detect threats



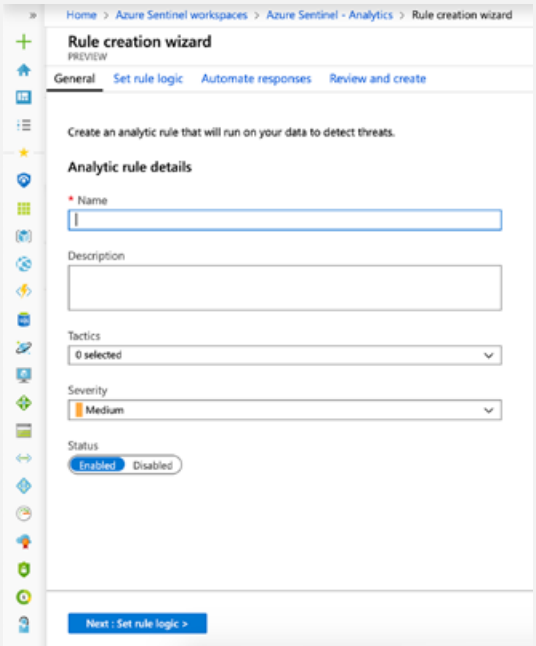
After you connect data sources to Azure Sentinel, the next step is to identify suspicious activities and threats.

Azure Sentinel provides built-in templates to enable you to do this and get notified of such threats.

These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. After you enable these templates, they will automatically search for suspicious activity across your environment. Many of them can be customized to search for, or filter out, activities according to your needs. To enable out-of-the-box detections, go to **Rule templates**.



Find out-of-the-box detection templates created by Microsoft's team of security experts and analysts in **Rule templates**.



Rule creation wizard allows you to create custom analytic rules.

You can also create custom analytic rules tailored to your data and environment:

1. In the Azure portal under Azure Sentinel, select **Analytics**.

2. In the top menu bar, click +Add analytic rule and select **Custom rule**.

3. In the **General** tab, provide a descriptive name and a description. Set the Alert severity as necessary. When you create the rule you can enable it, which will cause it to run immediately. Alternatively, you can create it as disabled, in which case the rule will be added to your Active rules tab and you can enable it from there when you need it.

4. In the **Settings** tab, you can either write a query directly, or create the query in Log Analytics, and then paste it into the **Search** query field. As you change and configure your query, Azure Sentinel simulates the query results in the results preview window on the right. This enables you to understand how much data will be generated over a specific interval for the alert you created. This will depend on how you set up the **Run** query and **Lookup** data. If you see that your alert will be triggered too frequently, you can set the number of results higher so that it's above your average baseline.

5. Under **Query scheduling**:

   Set the **Run** query every field to set the **Frequency** for how often the query is run—as frequently as every five minutes or as infrequently as once a day.

   Set the **Lookup data** from the last field to control the time window for how much data the query runs on. For example, it can run every hour across 60 minutes of data.

   You can set Azure Sentinel to **Stop** running the query after an alert is generated if you only want to get an alert once after it occurs. You must set the amount of time to stop running the query, up to 24 hours.

6. Under **Entity mapping**, you can map the columns in your query to entity fields recognized by Azure Sentinel. For each field, map the relevant column in the query you created in Log Analytics to the appropriate entity field. Each entity includes multiple fields, for example SID, GUID, etc. You can map the entity according to any of the fields, not just the upper-level entity.

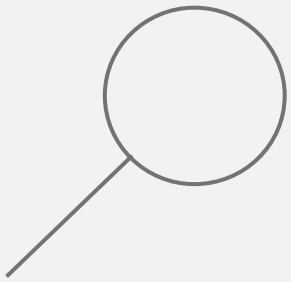
7. In the **Response automation** tab, select any playbooks you want to run automatically when an alert is generated by the custom rule. For more information on creating and automating playbooks, see the section "Respond to threats."

8. Click **Review** to check the settings for your new alert rule, and then click **Create** to initialize it. After the alert is created, a custom rule is added to the table under **Active analytic rules**. There, you can also see the number of matches for each rule—the alerts triggered. From this list you can enable, disable, or delete each rule. You can also right-select the ellipsis (...) at the end of the row for each alert to edit, disable, clone, show matches, or delete a rule. The **Analytics** page is a gallery of all your active alert rules, including templates you enable and alert rules you create based on templates.

9. To view the results of the alert rules you create, go to the Incidents page, where you can triage, investigate incidents, and remediate the threats.

Step 5

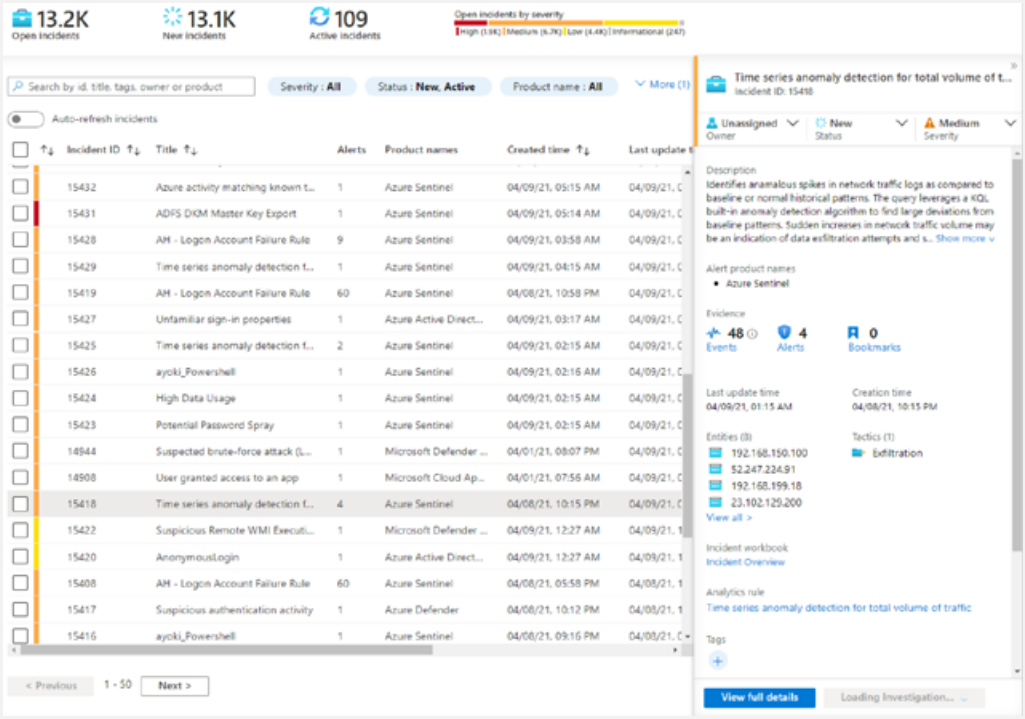
Investigate incidents



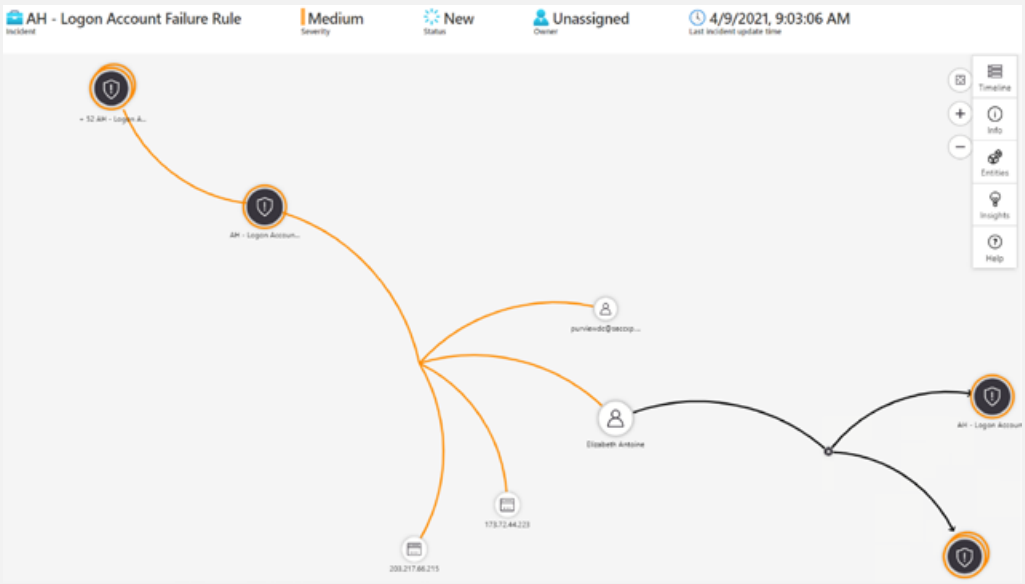
An incident is an aggregation of all the relevant evidence for a specific investigation. Incidents are created based on alerts you have defined in the **Analytics** page. The properties related to the alerts, such as severity and status, are set at the incident level.

Now you can easily investigate the detected threats and the entire incident.

You can quickly view the status of each incidents and manage the full lifecycle of this event.



See how many incidents you have, how many are open, how many you've set to In progress, and how many are closed in one view.



The investigation graph uses raw data to illustrate connections.

Investigating an incident using the Investigation Graph

1. To begin an investigation, click on a specific incident. On the right, you can see detailed information for the incident including its severity and a summary of the number of entities involved (based on your mapping). Each incident has a unique ID. The severity of the incident is determined according to the most severe alert included in the incident.

2. To view more details about the alerts and entities in the incident, click on **View full details** on the incident page and review the relevant tabs that summarize the incident information. Full incident view consolidates all evidence in the alert, the associated alerts, and entities.

3. In the **Alerts** tab, review the alert itself—when it was triggered and by how much it exceeded the thresholds you set. You can see all relevant information about the alert—the query that triggered the alert, the number of results returned per query, and the ability to run playbooks on the alerts. To drill down even further into the incident, click on the number of events. This opens the query that generated the results and the results that triggered the alert in Log Analytics.

4. In the **Entities** tab, you can see all the entities that you mapped as part of the alert rule definition.

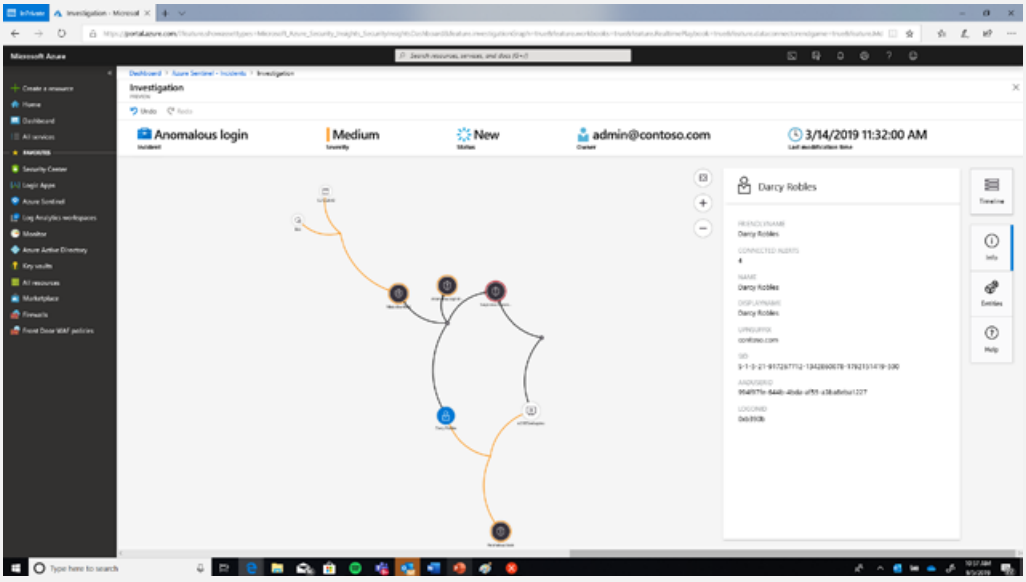
5. If you're actively investigating an incident, it's a good idea to set the incident status to **In progress** until you close it.

6. Incidents can be assigned to a specific user. For each incident you can assign an owner by setting the incident **owner** field. All incidents start as unassigned. You can go into the incidents and filter by your name to see all the incidents that you own. You can also add comments so that other administrators will be able to understand what you investigated and what your concerns are around the incident.

7. Click **Investigate** to view the investigation graph tool. The investigation graph helps you understand the scope and identify the root cause of a potential security threat by correlating relevant data with any involved entity. Azure Sentinel analyzes your raw data to find additional insights and connections on the entities extracted from your alerts. It will then surface those connections in the live investigation graph. You can dive deeper and investigate any entity presented in the graph by clicking on it and choosing between different expansion options.

8. Select each entity to open the **Entities** pane so you can review each entity.

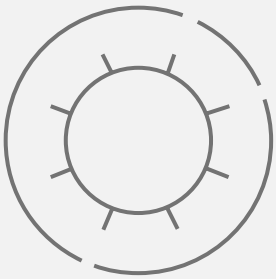
9. Expand your investigation by hovering over each entity to reveal a list of questions that was designed by our security experts and analysts per entity type to deepen your investigation. For example, on a computer you can request related alerts. The related alerts are added to the graph. For each entity, you can select the option to open the results in Log Analytics to see the raw data for the incidents. The graph provides you with a list of connections that you might not have known about, enabling you to reach full scope of the breach. It also gives you a timeline parallel to the graph. You can hover over the timeline to see which things on the graph occurred at what point in time.



Dive deeper into the data to investigate the full scope of a breach.

Step 6

Respond to threats



A security playbook is a collection of procedures that orchestrates a threat response. Playbooks can run manually or automatically. Security playbooks in Azure Sentinel are based on Azure Logic Apps, providing built-in templates you can customize. Note that Azure Logic Apps incur charges. View the **pricing page** for more details.

For example, if you're worried about malicious attackers accessing your network resources, you can set an alert that looks for malicious IP addresses accessing your network and trigger a playbook to stop the attack in real time.

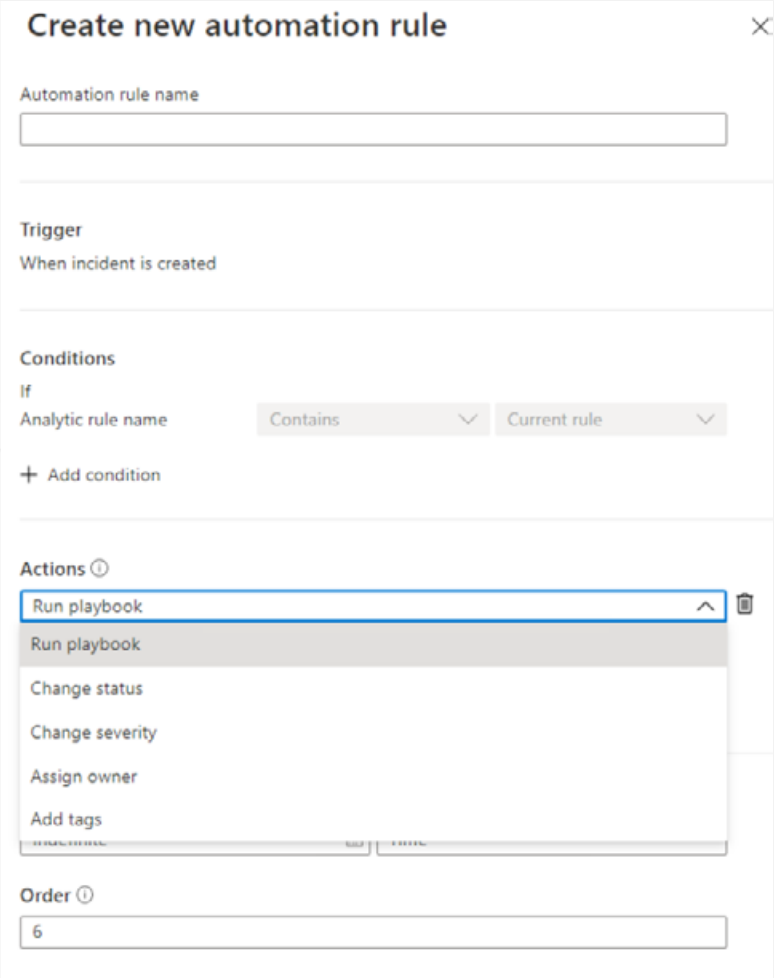
Create a security playbook

1. Open the **Azure Sentinel** dashboard.
2. Under **Management**, select **Playbooks**.
3. In the **Azure Sentinel — Playbooks (Preview)** page, click **Add** button.
4. In the **Create Logic app** page, type the requested information to create your new logic app, then click **Create**.
5. In the **Logic App Designer**, select the template you want to use. If you select a template that necessitates credentials, you will have to provide them. Alternatively, you can create a new blank playbook from scratch. Select **Blank Logic App**.
6. From here you can either build a new playbook or edit the template. Learn more about creating a playbook with **Logic Apps**.

Automate threat responses

Using real-time automation, response teams can significantly reduce their workload by fully automating routine responses to recurring types of alerts. Note that this requires setting the playbook trigger to **Azure Sentinel**.

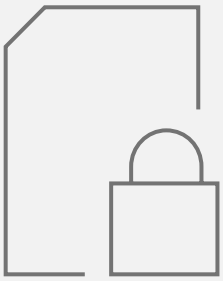
1. Choose the alert for which you want to automate the response.
2. From the Azure Sentinel workspace navigation menu, select **Analytics**.
3. Select the alert you want to automate.
4. In the **Edit alert rule** page, under **the Automate responses tab**, choose the **Triggered playbook** you want to run when this alert rule is matched.
5. Select **Next: Review**.



Reduce team workloads by automating routine responses to recurring types of alerts.

Step 7

Hunt for threats



Analysts need to proactively look for threats that may not have been discovered by security apps. Azure Sentinel includes built-in hunting queries that guide you to ask the right questions to find previously undiscovered threats.

With Azure Sentinel hunting, you can take advantage of the following capabilities:

- **Built-in queries:** A starting page provides preloaded query examples designed to get you started quickly and familiarize you with the tables and the query language. These built-in hunting queries are developed and fine-tuned by Microsoft security researchers and the GitHub community on a continuous basis to provide you with an entry point and help you start hunting for the beginnings of new attacks.
- **Powerful query language with IntelliSense:** Built on top of a query language, this gives you the flexibility you need to take hunting to the next level.

Azure Sentinel's built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network."

- **Create your own bookmarks:** Bookmarks let you save items for later so you can use them to create an incident for investigation. You can bookmark a row, promote it to an incident, and then investigate with an investigation graph.
- **Use notebooks to automate investigation:** Notebooks encapsulate all the hunting steps in a reusable playbook that can be shared with others in your organization.
- **Query the stored data:** The data is accessible in tables for you to query. For example, you can query process creation, DNS events, and many other event types.
- **Links to community:** Leverage the power of the greater community to find additional queries and data sources.

Try Azure Sentinel today

No infrastructure investment. Powerful AI built in. Tools for every role. Virtually unlimited scalability. All backed by Microsoft security research. If you're looking to improve the security posture of your enterprise while simplifying security operations, consider Azure Sentinel.

See how fast, easy, and inexpensive it is to get started.

Talk to an Azure Specialist about Azure Sentinel now >

Microsoft