Microsoft Security

Microsoft Sentinel

(SIEM+SOAR)

František Fait
Security and Compliance Technical Specialist

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Microsoft Sentinel

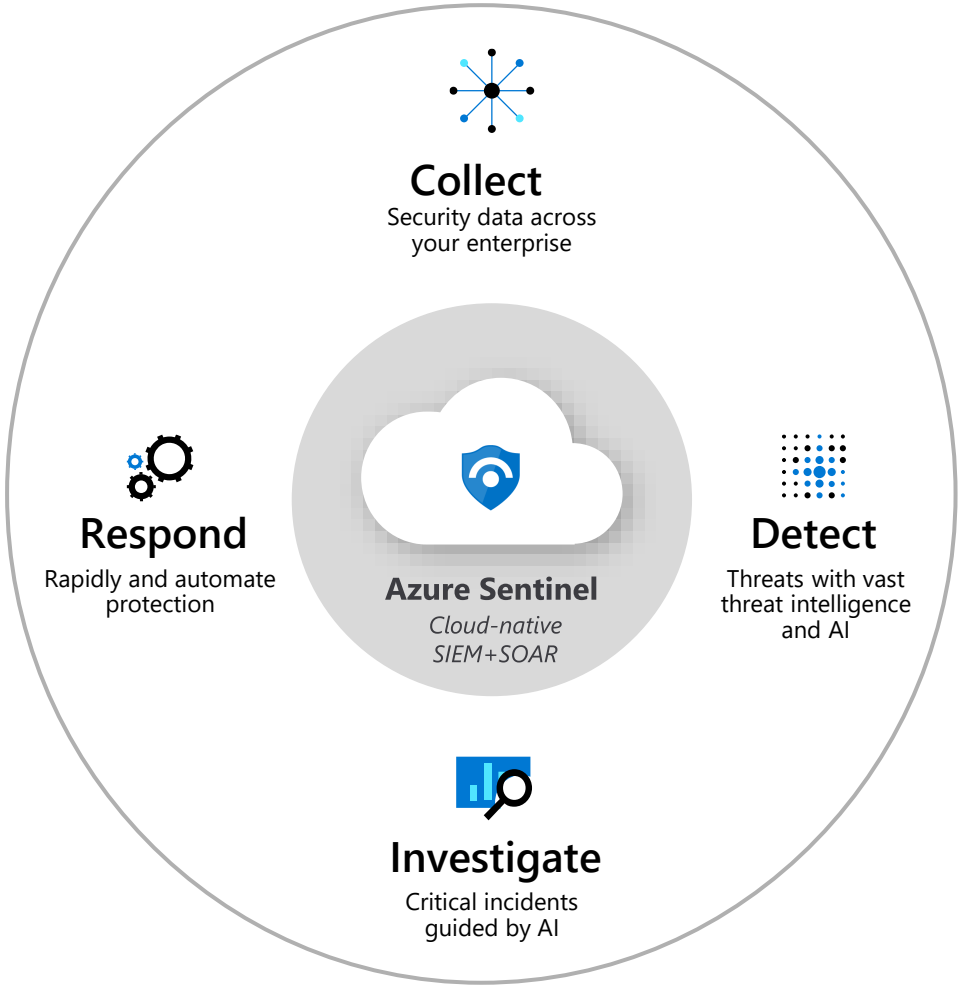
Cloud-native SIEM and SOAR for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

Faster threat protection with **AI by your side**



Reduce security and IT costs

No infrastructure costs or upfront commitment

Only **pay for what you use**

Bring your **Office 365 Data for free**

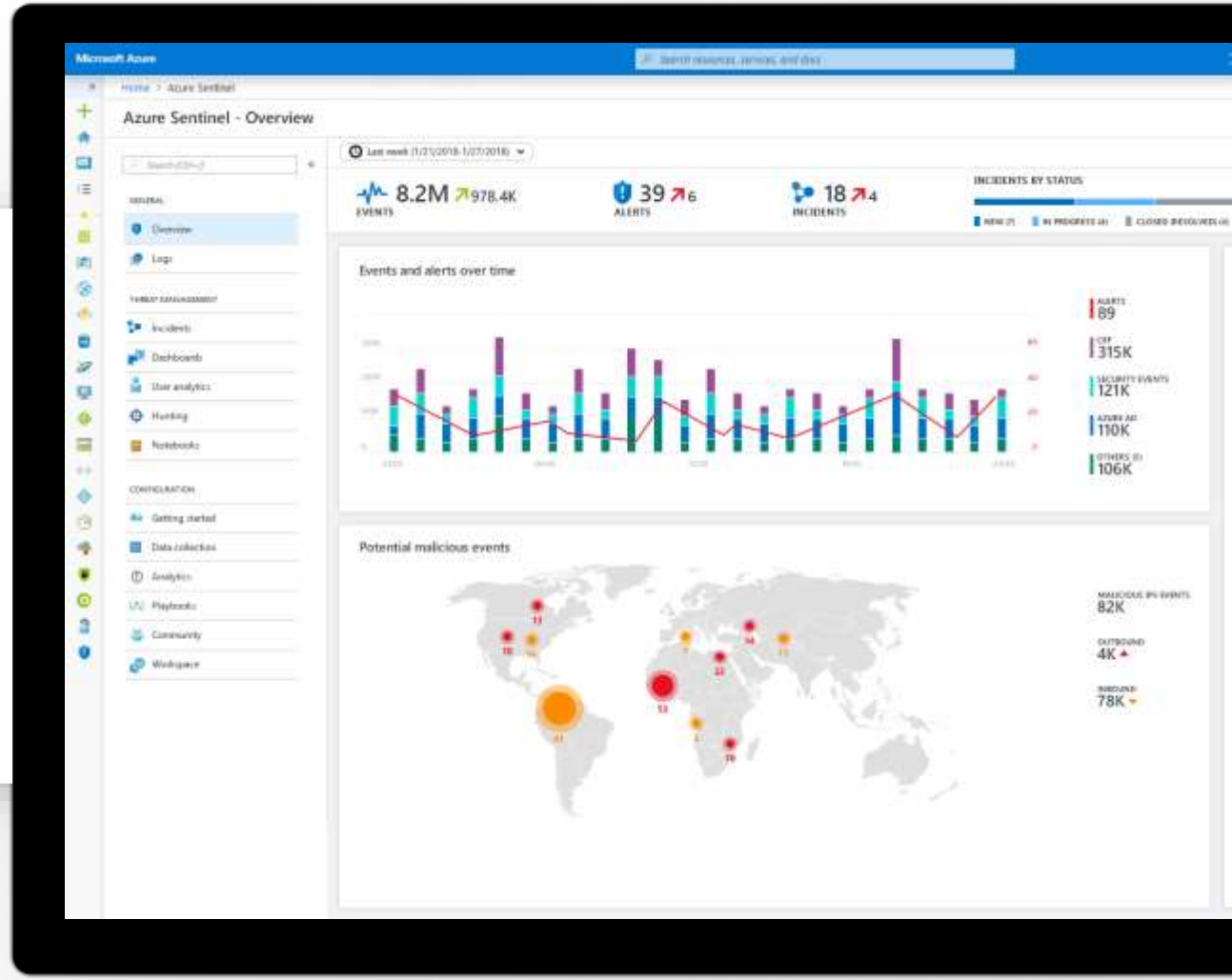
Cloud-native, scalable SIEM

Focus on security, unburden SecOps from IT tasks

No infrastructure setup or maintenance

SIEM Service available in **Azure portal**

Scale automatically, put no limits
to compute or storage resources

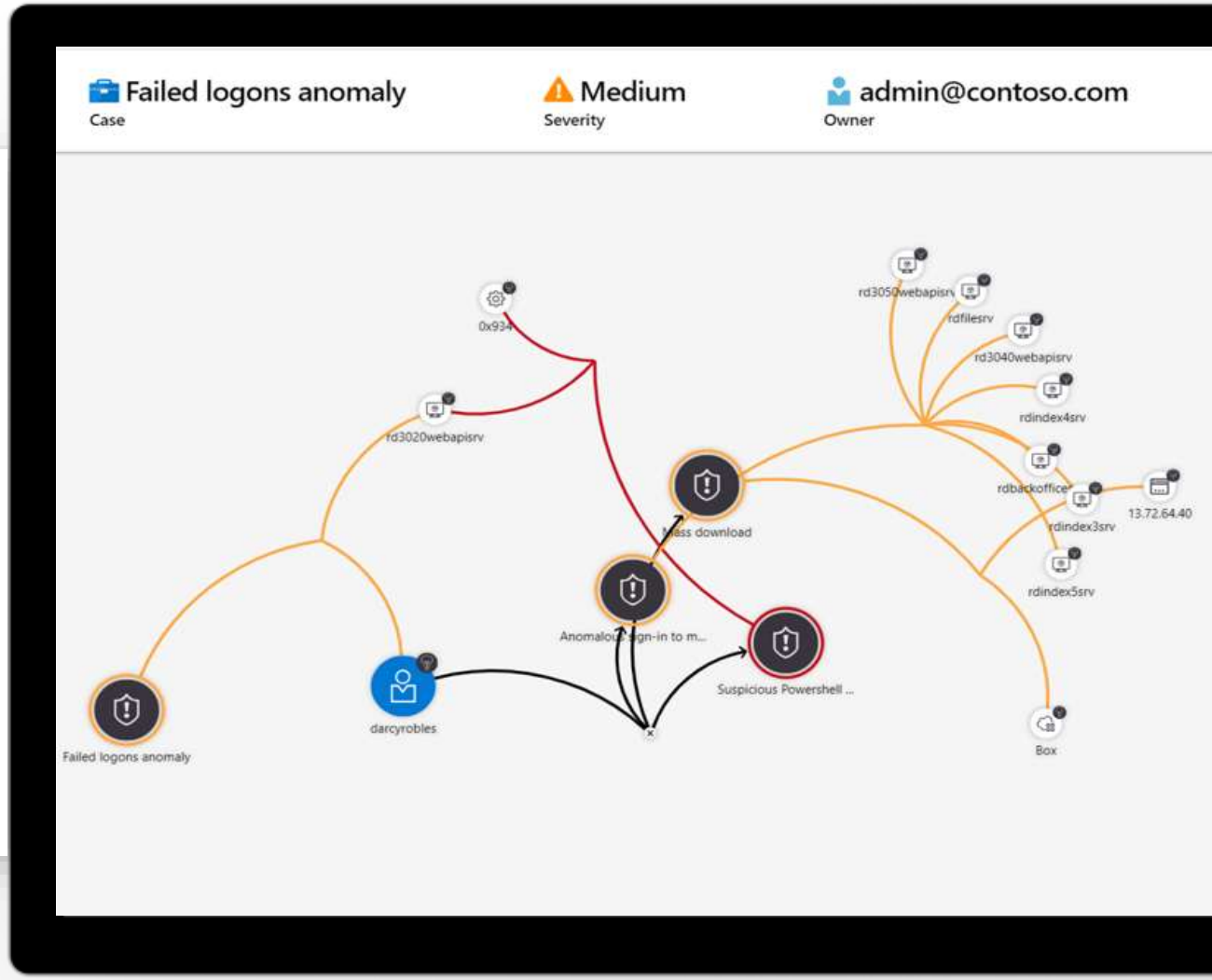


Investigate threats with AI and hunt suspicious activities at scale, tapping into years of cybersecurity work at Microsoft

Get prioritized alerts and **automated expert guidance**

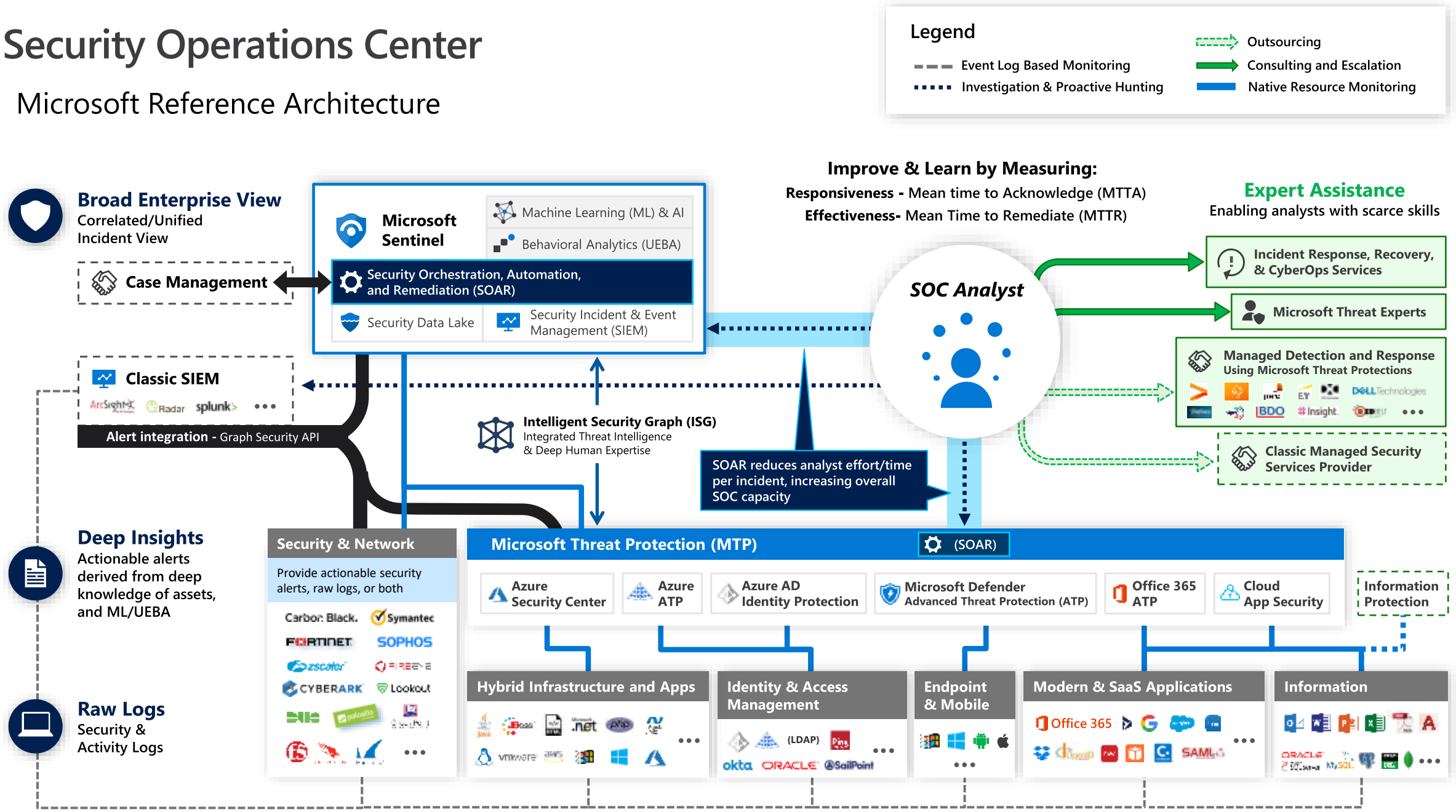
Visualize the entire attack and its impact

Hunt for suspicious activities using **pre-built queries and Azure Notebooks**



Security Operations Center

Microsoft Reference Architecture



Getting started with Microsoft Sentinel

Step 1: **Access Azure Sentinel**

Step 2: **Connect your data**

Step 3: **Use overview dashboard and workbooks to get visibility across enterprise**

Step 4: **Detect threats**

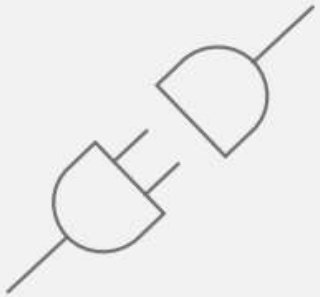
Step 5: **Investigate incidents**

Step 6: **Respond to threats**

Step 7: **Hunt for threats**

Step 1

Access 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

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**.

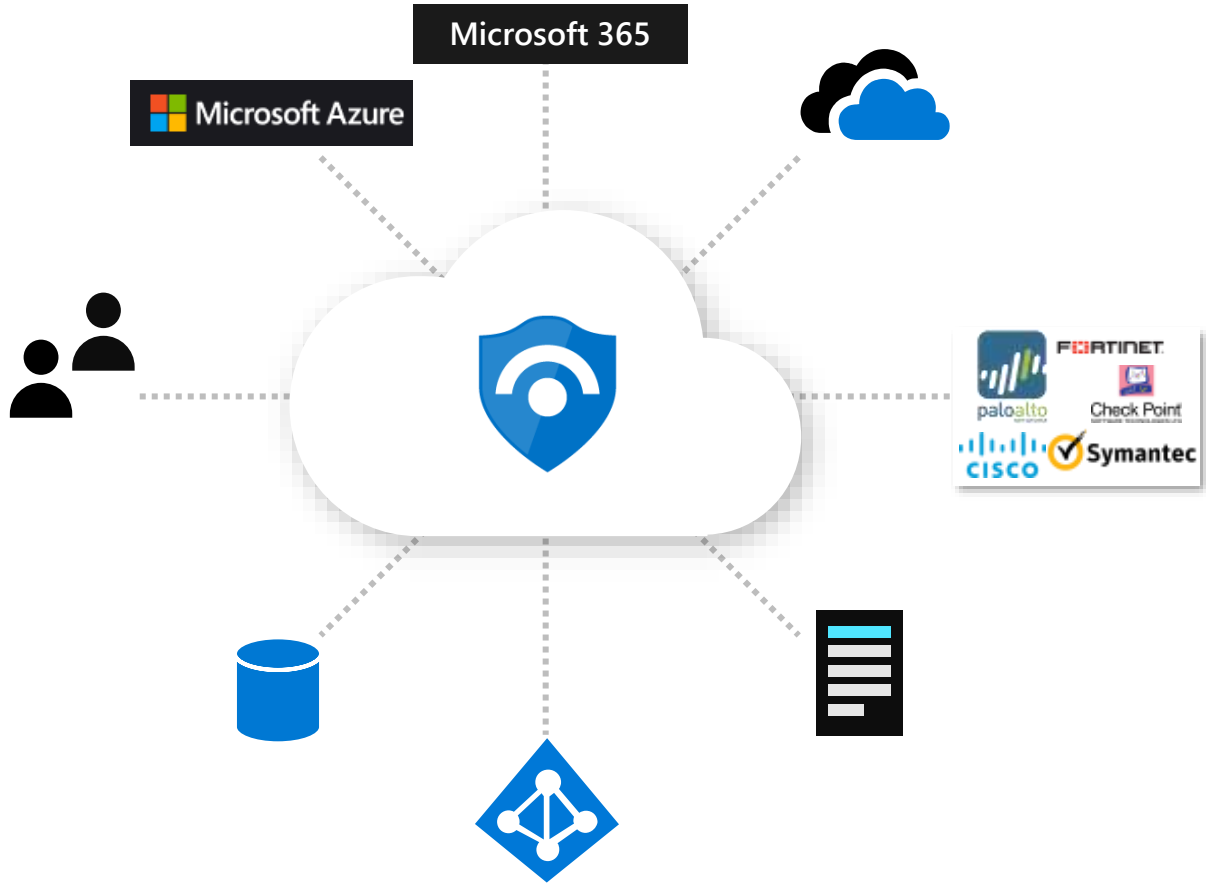
Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

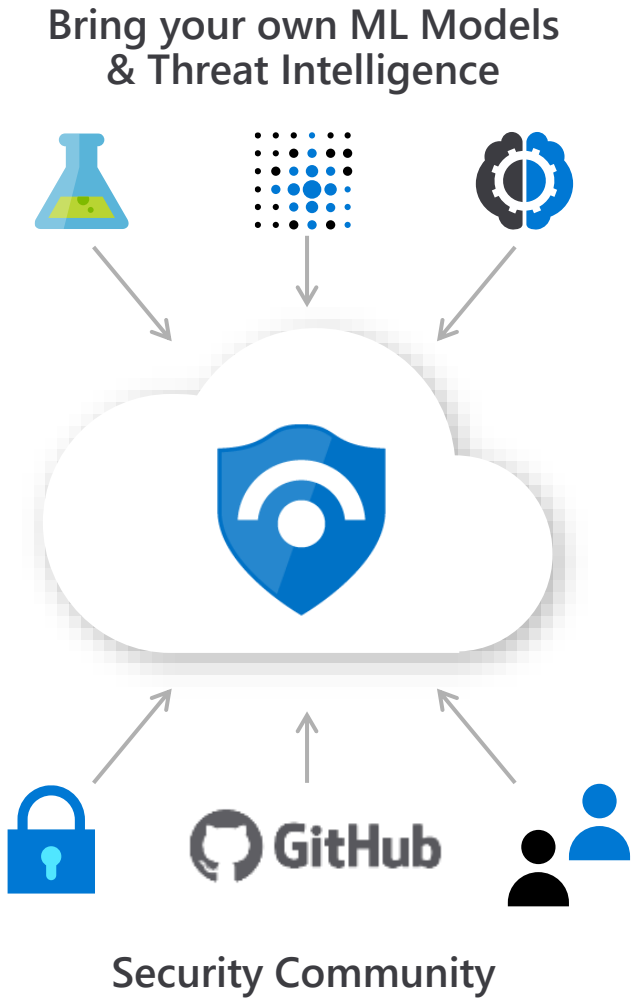
Proven log platform with **more than 10 petabytes** of daily ingestion



Optimize for your needs

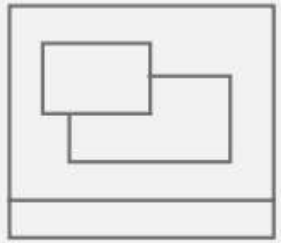
Bring your own insights, machine learning models, and threat intelligence

Tap into our **security community** to build on detections, threat intelligence, and response automation.



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.

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.

Step 4

Detect 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**.

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.

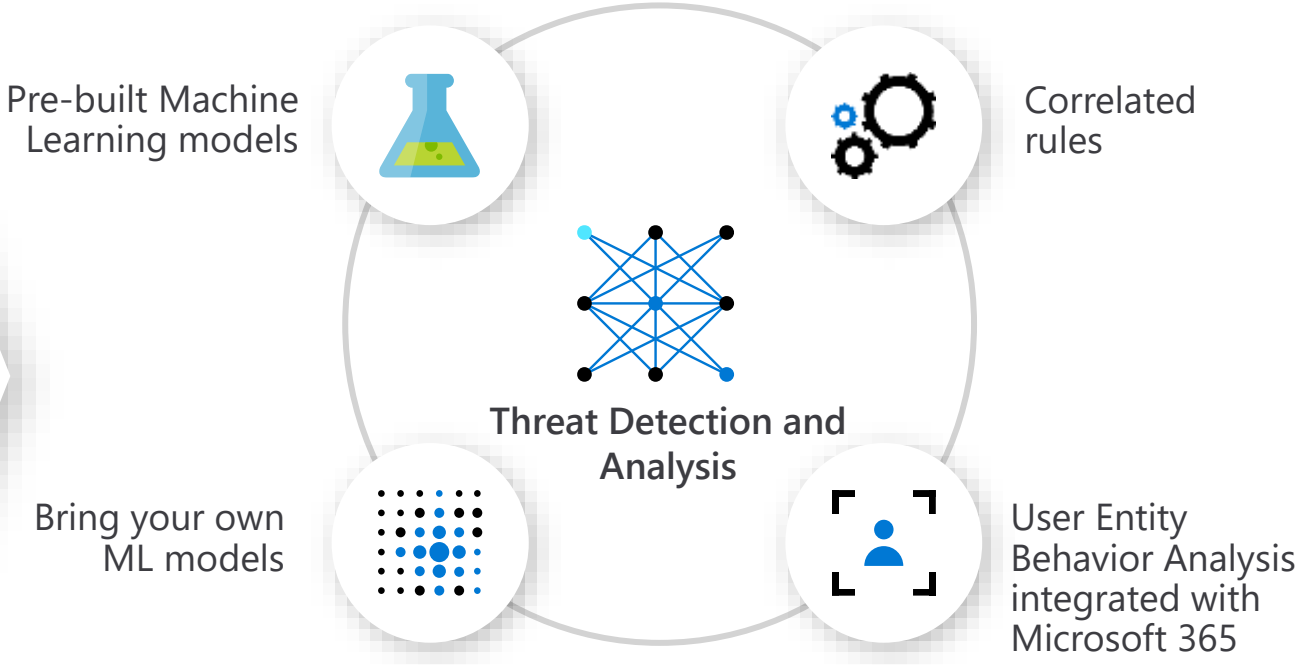
Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%



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.

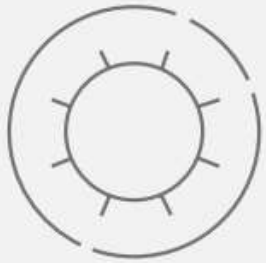
Now you can easily investigate the detected threats and the entire incident.

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

The investigation graph uses raw data to illustrate connections.

Step 6

Respond to threats



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**.

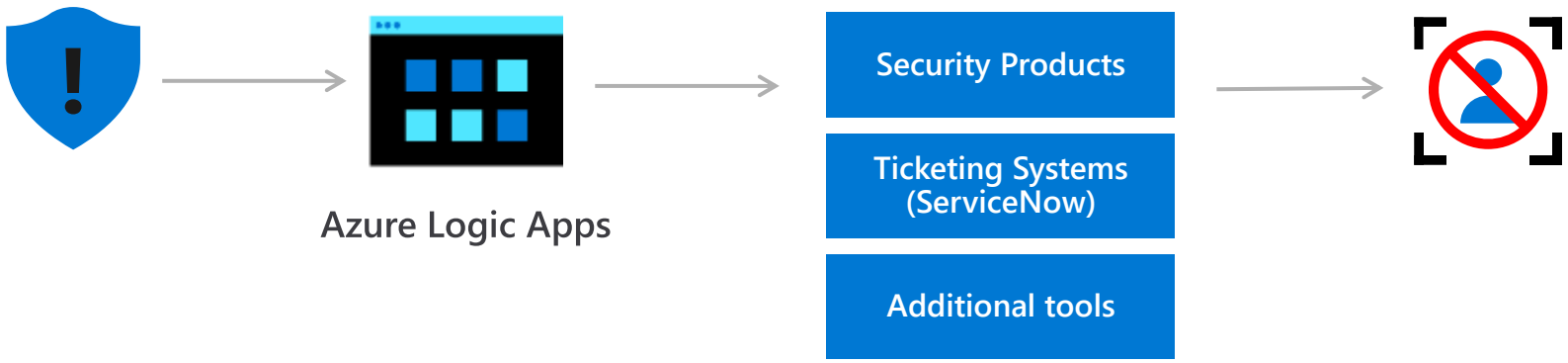
Automate threat responses

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**.

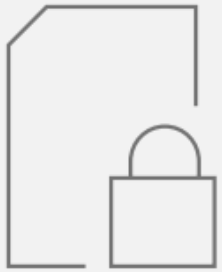
Respond rapidly with built-in orchestration and automation

Build automated and scalable playbooks that integrate across tools



Step 7

Hunt for threats



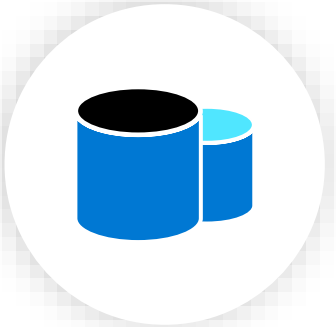
With Azure Sentinel hunting, you can take advantage of the following capabilities:

- **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.
- **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.

Take actions today- Get started with Azure Sentinel

Start
Microsoft Azure trial

Open Microsoft
Sentinel dashboard
in Azure Portal



Connect
data sources

To learn more, visit
https://aka.ms/AzureSentinel

https://www.microsoft.com/security/blog/2020/12/01/azure-sentinel-achieves-a-leader-placement-in-forrester-wave-with-top-ranking-in-strategy/

November 16, 2020 • 5 min read

Forrester TEI study: Azure Sentinel delivers 201 percent ROI over 3 years and a payback of less than 6 months

- A three-year 201 percent return on investment (ROI) with a payback period of less than six months.
- A 48 percent reduction in costs compared to legacy SIEM solutions, saving on expenses like licensing, storage, and infrastructure costs.
- A 79 percent reduction in false positives and 80 percent reduction in the amount of labor associated with investigation, reducing mean time to resolution (MTTR) over three years.
- A 67 percent decrease in time to deployment compared to legacy on-premises SIEMs.

https://www.microsoft.com/security/blog/2020/11/16/forrester-tei-study-azure-sentinel-delivers-201-percent-roi-over-3-years-and-a-payback-of-less-than-6-months/

July 8, 2021 • 3 min read

Microsoft named a Visionary in the 2021 Gartner Magic Quadrant for SIEM for Azure Sentinel

We're pleased to announce that in its first year of inclusion in the Gartner Magic Quadrant report, Microsoft Azure Sentinel has been named a Visionary, where we were recognized for our completeness of vision for SIEM.[1]

Gartner has said that "cloud SIEM will be the future of how many organizations consume technology."[2] We wholeheartedly agree! Today, security teams are constantly asked to do more with less. They need to protect expanding digital estates, detect increasingly advanced threats through huge amounts of noise, and keep up with a massive backlog of investigations.

Azure Sentinel is built from the ground up to be completely cloud-native, and it enables security teams to focus on protecting their organizations instead of maintaining infrastructure. It collects, correlates, and analyzes data at cloud scale across the entire organization, resulting in higher efficiency and more effective security analytics.