* 4 minutes

Security management on a large scale can benefit from a dedicated security information and event management (SIEM) system. A SIEM system aggregates security data from many different sources (as long as those sources support an open-standard logging format). It also provides capabilities for threat detection and response.

[Azure Sentinel](https://azure.microsoft.com/services/azure-sentinel/) is Microsoft’s cloud-based SIEM system. It uses intelligent security analytics and threat analysis.

## Azure Sentinel capabilities

Azure Sentinel enables you to:

* **Collect cloud data at scale** Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
* **Detect previously undetected threats** Minimize false positives by using Microsoft’s comprehensive analytics and threat intelligence.
* **Investigate threats with artificial intelligence** Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.
* **Respond to incidents rapidly** Use built-in orchestration and automation of common tasks.

## Connect your data sources

Tailwind Traders decides to explore the capabilities of Azure Sentinel. First, the company identifies and connects its data sources.

Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built-in connectors or industry-standard log formats and APIs.

* **Connect Microsoft solutions** Connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, and Windows Defender Firewall.
* **Connect other services and solutions** Connectors are available for common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud, and Okta SSO.
* **Connect industry-standard data sources** Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

## Detect threats

Tailwind Traders needs to be notified when something suspicious occurs. It decides to use both built-in analytics and custom rules to detect threats.

**Built in analytics** use templates designed by Microsoft’s team of security experts and analysts based on known threats, common attack vectors, and escalation chains for suspicious activity. These templates can be customized and search across the environment for any activity that looks suspicious. Some templates use machine learning behavioral analytics that are based on Microsoft proprietary algorithms.

**Custom analytics** are rules that you create to search for specific criteria within your environment. You can preview the number of results that the query would generate (based on past log events) and set a schedule for the query to run. You can also set an alert threshold.

## Investigate and respond

When Azure Sentinel detects suspicious events, Tailwind Traders can investigate specific alerts or *incidents* (a group of related alerts). With the investigation graph, the company can review information from entities directly connected to the alert, and see common exploration queries to help guide the investigation.

Here’s an example that shows what an investigation graph looks like in Azure Sentinel.

![An example incident investigation graph in Azure Sentinel.](data:image/png;base64;base64,)

An example incident investigation graph in Azure Sentinel.

The company will also use [Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/workbooks-overview/) to automate responses to threats. For example, it can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.
2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message includes two user option buttons: **Block** or **Ignore**.

When an admin chooses **Block**, the IP address is blocked in the firewall, and the user is disabled in Azure Active Directory. When an admin chooses **Ignore**, the alert is closed in Azure Sentinel, and the incident is closed in the IT ticketing system.

The workbook continues to run after it receives a response from the admins.

Workbooks can be run manually or automatically when a rule triggers an alert.

## Next unit: Store and manage secrets by using Azure Key Vault

[Continue](https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/4-manage-secrets-key-vault/)

Need help? See our [troubleshooting guide](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.3-detect-respond-threats-sentinel&documentId=a9c597b6-5928-280c-b983-54edbcfc65c0&versionIndependentDocumentId=dfa3e461-848e-8566-6a93-424b8fc7cdd2&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F3-detect-respond-threats-sentinel.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F3-detect-respond-threats-sentinel&author=rknapp) or provide specific feedback by [reporting an issue](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.3-detect-respond-threats-sentinel&documentId=a9c597b6-5928-280c-b983-54edbcfc65c0&versionIndependentDocumentId=dfa3e461-848e-8566-6a93-424b8fc7cdd2&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F3-detect-respond-threats-sentinel.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F3-detect-respond-threats-sentinel&author=rknapp#report-feedback).