



Microsoft Sentinel

examlabpractice.com

SOURCE: <https://learn.microsoft.com/en-us/azure/sentinel/overview>





What is Microsoft Sentinel?

- Microsoft Sentinel is a scalable, cloud based, security information event management (SIEM) and security orchestration automated response (SOAR) product.
- Sentinel delivers intelligent security analytics and threat intelligence solution, providing a centralized point for alert detection, threat visibility, proactive hunting, and threat response.

Purposes of Sentinel

Microsoft Sentinel offers a cloud-based, scalable approach, serving as:

- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

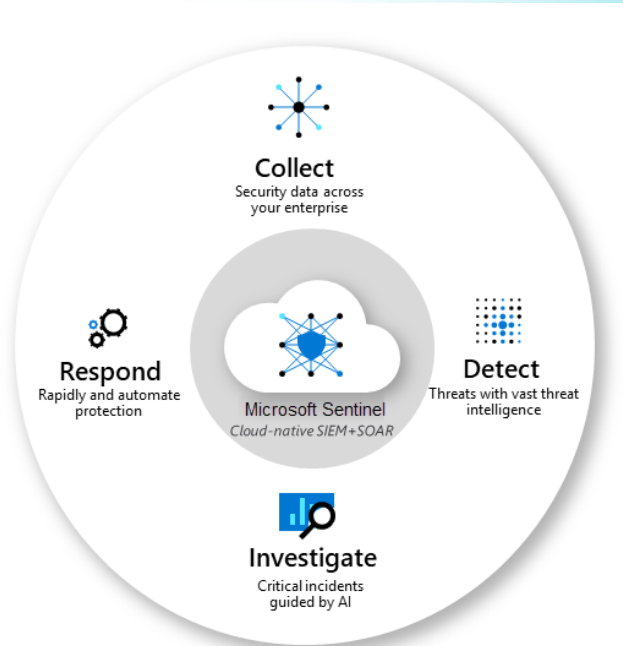
This solution brings advanced security analytics and threat intelligence throughout the enterprise. Microsoft Sentinel equips you with a unified platform for identifying attacks, enhancing threat perception, active pursuit, and responding to threats.

As your enterprise-wide watchtower, Microsoft Sentinel eases the burden of complex attacks, a growing number of alerts, and extended time to resolve incidents.



Cycle of Protection

- Aggregate data comprehensively from every user, device, app, and infrastructure, both onsite and across various clouds
- Uncover hidden threats while reducing false alarms through Microsoft's advanced analytics and unmatched threat intelligence.
- Employ artificial intelligence to probe into threats and methodically scour for dubious behavior, leveraging Microsoft's extensive cybersecurity experience.
- Swiftly tackle incidents with automated workflows and pre-programmed actions for routine tasks.



Collect data by using data connectors

Microsoft Sentinel offers a host of pre-configured connectors for seamless, immediate integration with various Microsoft tools, including:

- Microsoft platforms such as Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT, among others.
- Azure-based services like Microsoft Entra ID, Azure Activities, Azure Storage, Azure Key Vault, Azure Kubernetes Service, and more.

Additionally, Microsoft Sentinel features native connectors for a wide array of security assets and applications beyond the Microsoft ecosystem. Data integration with Microsoft Sentinel can also be accomplished through common event formats, Syslog, or REST-API for other data sources.

The screenshot shows the Microsoft Sentinel 'Data connectors' page. The left sidebar contains navigation links: Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), Content management (Content hub, Repositories, Community), Configuration (Workspace manager, Data connectors, Analytics, Watchlist, Automation). The main content area shows 137 connectors, with 12 connected. A table lists the following connectors:

Status	Connector name	Providers	Data Types	Status
Connected	Azure Active Directory	Microsoft		
Connected	Azure Active Directory Identity Protection	Microsoft		
Connected	Azure Activity	Microsoft		
Connected	Azure Data Lake Storage Gen1	Microsoft		

On the right, the 'Azure Active Directory' connector details are shown, including a description: 'Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app'. A button labeled 'Open connector page' is at the bottom.



Correlate alerts into incidents by using analytics rules

- Microsoft Sentinel consolidates alerts to lessen noise with:
 - Analytics that combine alerts into incidents.
 - Incidents that signify a potential threat for action.
- Utilize default correlation rules or customize them.
- Leverages machine learning to identify network behavior deviations.
- Analytics link low-level alerts to form high-confidence incidents.

The screenshot displays the Microsoft Sentinel 'Incidents' page. The top navigation bar includes 'Home > Microsoft Sentinel' and 'Selected workspace: Contoso'. Below this, there's a search bar and a set of filters: 'Refresh', 'Last 24 hours', 'Actions', 'Security efficiency workbook', 'Columns', and 'Guides & Feedback'. The main content area shows a summary of incidents: 403 Open incidents, 400 New incidents, and 3 Active incidents. A severity bar indicates 82 High, 95 Medium, and 207 Low incidents. The incident list table has columns for Severity, Status, Incident ID, Title, Alerts, Product names, and Created time. The selected incident, 'Authentication Methods Changed for Privileged Account' (ID: 203443), is shown in detail on the right. Its description states: 'Identifies authentication methods being changed for a privileged account. This could be an indication of an attacker adding an auth method to the account so they can have continued access. Ref: https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-account-changes-to-monitor-1'. The incident is assigned to 'Unassigned' with a status of 'New' and a severity of 'High'. It shows 1 event, 1 alert, and 0 bookmarks. The last update time is 05/11/22, 12:50 PM, and the creation time is 05/11/22, 12:49 PM. The entities list includes 'ghames@contoso...' and '192.168.65.82'. The tactics and techniques section is also visible at the bottom.

Severity	Status	Incident ID	Title	Alerts	Product names	Created time
High	New	203444	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:52 PM
High	New	203443	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 12:49 PM
High	New	203440	User login from different coun...	1	Microsoft Sentinel	05/11/22, 12:41 PM
High	New	203437	Preview: User and IP address rec...	2	Microsoft Defender fo...	05/11/22, 12:25 PM
High	New	203436	Preview: Suspicious PowerShell c...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203435	Preview: Network intrusion deta...	2	Microsoft Defender fo...	05/11/22, 12:23 PM
High	New	203426	Preview: Multiple alerts possibl...	5	Microsoft Defender fo...	05/11/22, 11:52 AM
High	New	203425	Preview: Multiple alerts possibl...	11	Microsoft Cloud App ...	05/11/22, 11:52 AM
High	New	203424	Preview: Crypto-mining activity f...	2	Azure Defender, Azur...	05/11/22, 11:52 AM
High	New	203423	Impossible travel to atypical loca...	2	Azure Active Directory...	05/11/22, 11:52 AM
High	New	203421	Preview: Suspicious PowerShell c...	2	Azure Active Directory...	05/11/22, 11:51 AM
High	New	203422	Preview: Multiple alerts possibl...	16	Microsoft Defender fo...	05/11/22, 11:51 AM
High	New	203420	Preview: Connection to web pag...	2	Azure Defender, Micr...	05/11/22, 11:48 AM
High	New	203419	Authentication Methods Change...	1	Microsoft Sentinel	05/11/22, 11:30 AM

Automate and Orchestrate

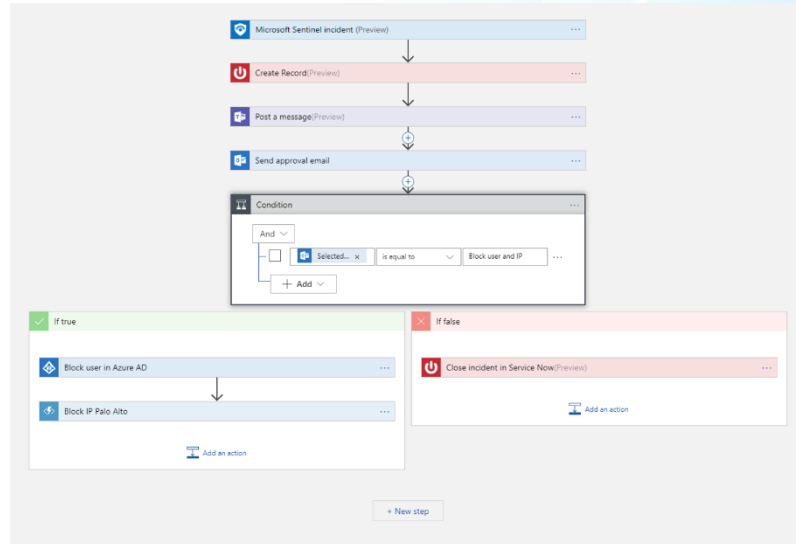
Streamline task automation and security management using playbooks compatible with Azure and other tools.

Sentinel offers a scalable automation system adaptable to new tech and threats.

Use Azure Logic Apps to create playbooks with a vast selection of connectors for different services, allowing custom workflow logic.

These connectors allow you to apply any custom logic in your workflow, for example:

- ServiceNow
- Jira
- Zendesk
- HTTP requests
- Microsoft Teams
- Slack
- Microsoft Entra ID
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud Apps



Investigate the scope and root cause of security threats

Microsoft Sentinel's advanced investigation features assist you in unraveling the extent and origin of a potential security issue. By selecting an entity on the dynamic graph, you can probe further into that entity's details and its links to uncover the underlying cause of the threat.

The screenshot displays the Microsoft Sentinel Investigation interface. At the top, the breadcrumb navigation shows 'Home > Microsoft Sentinel > Microsoft Sentinel > Incident'. The main header area includes the title 'Investigation' and a close button. Below this, there are filters for 'Incident' (ADFS DKM Master Key Export), 'Severity' (High), 'Status' (New), 'Owner' (Unassigned), and a timestamp '5/3/2021, 12:14:42 PM' with a note 'Last incident update time'. The central part of the interface features a dynamic graph with nodes representing entities and their relationships. On the right side, a 'Timeline' panel is open, showing a list of incidents. The first incident is 'ADFS DKM Master Key Export' dated '4/4/2021, 12:10:00 PM' with the description 'Identifies an export of the ADFS DKM Mast...'. The second incident is also 'ADFS DKM Master Key Export' dated '5/2/2021, 12:10:01 PM' with the description 'Identifies an export of the ADFS DKM Mast...'. A sidebar on the right contains navigation links: 'Timeline' (highlighted), 'Info', 'Entities', 'Insights', and 'Help'. The background of the slide features a large blue gear and a cloud containing various icons like a play button, a picture, a document, a person, and a folder.