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:

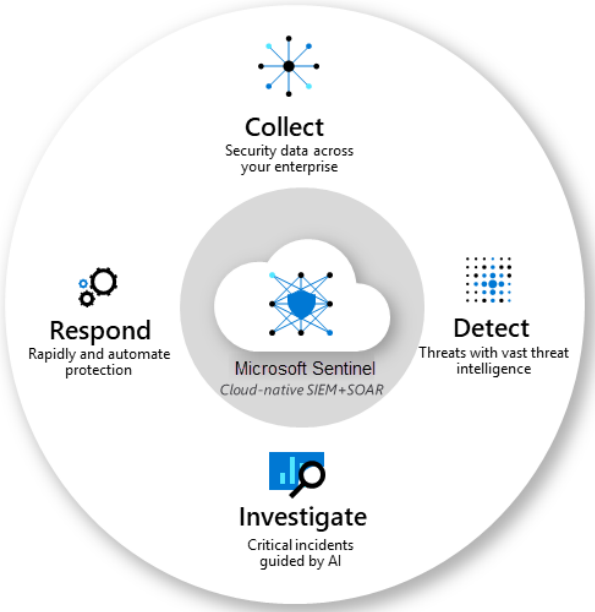
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

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.

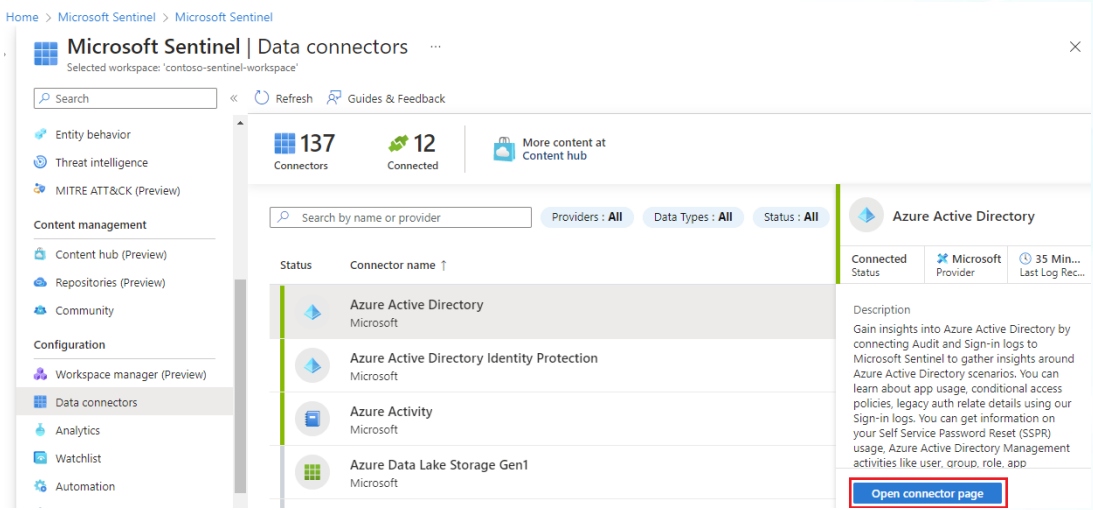


Collect data by using data connectors

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

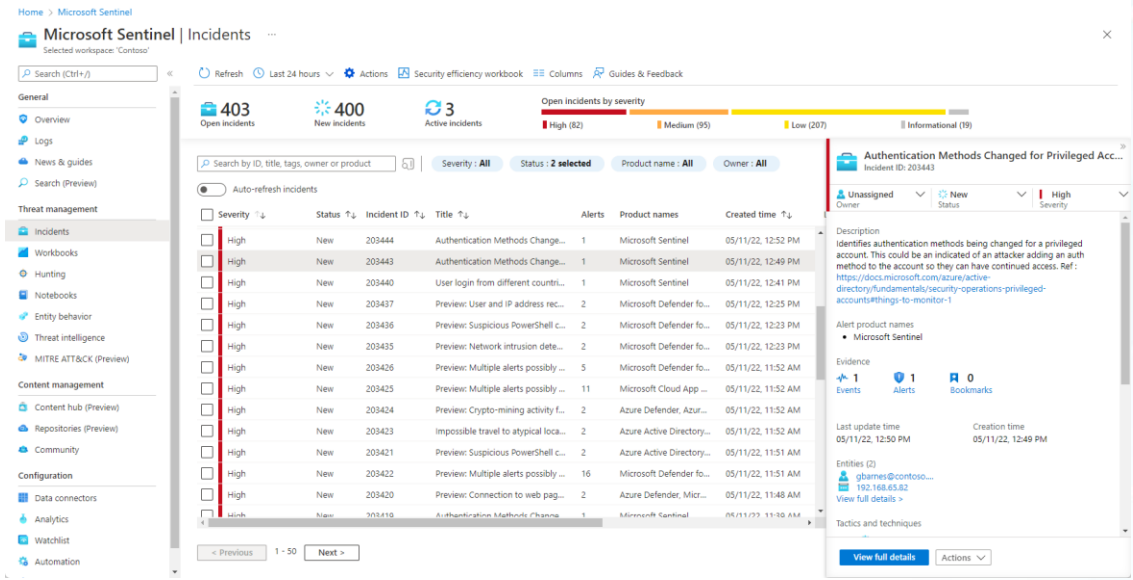
- Microsoft platforms such as Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT, among others.
- Azure-based services like Microsoft Entra ID, Azure Activities, Azure Storage, Azure Key Vault, Azure Kubernetes Service, and more.

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.



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.



Automate and Orchestrate

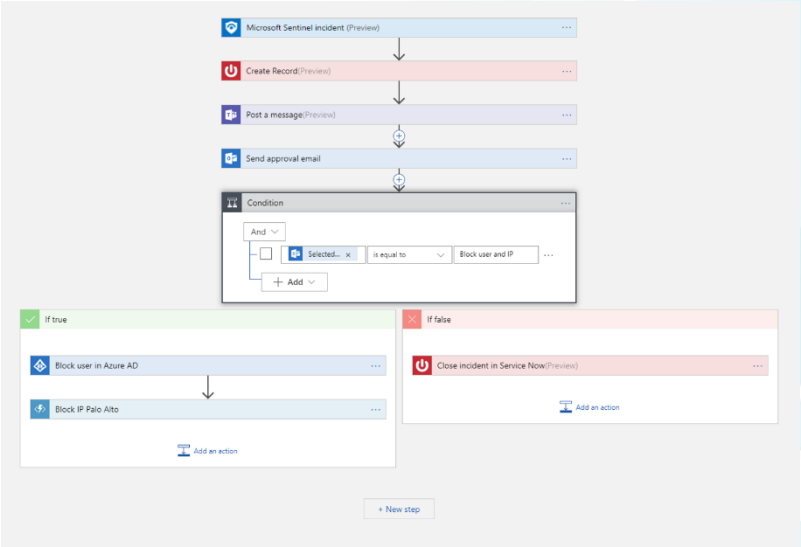
Streamline task automation and security management using playbooks compatible with Azure and other tools.

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.