



Set Up Microsoft Sentinel + Log Analytics

Security Starts with Visibility

Deploy Microsoft Sentinel using a Log Analytics Workspace to start collecting security data across Azure, Entra ID, and beyond. This is the foundation of modern threat detection and response.



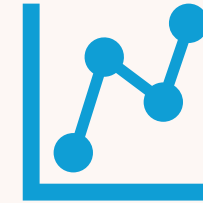
What is Microsoft Sentinel?



Microsoft Sentinel is a **cloud-native SIEM (Security Information and Event Management)** and **SOAR (Security Orchestration, Automation, and Response)** solution.

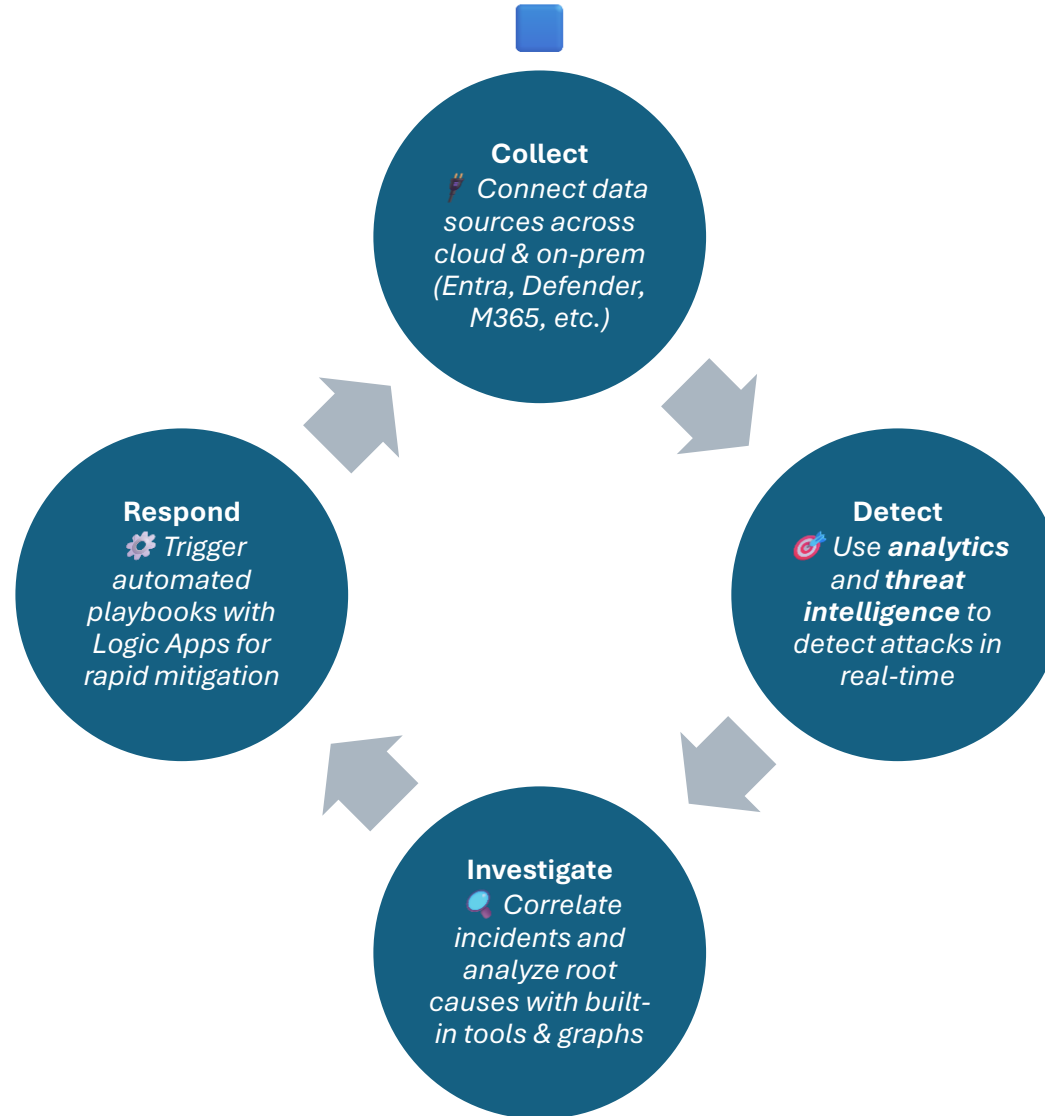


It provides **intelligent security analytics** and **threat intelligence** across the entire enterprise.



Sentinel uses **Log Analytics Workspaces** to collect and correlate data from multiple sources.

Sentinel's Cycle of Protection



[Home](#) > [Perparims Cloud Solutions](#) >

Perparims Cloud Solutions ...



What Powers Microsoft Sentinel?

Visualize threats. Automate detection. Investigate faster.



1. Data Connectors



Enable Sentinel to pull in logs and telemetry from Entra ID, Defender, M365, on-prem firewalls, and third-party tools.



2. Analytics Rules



Use built-in or custom logic to detect threats by correlating signals from connected sources.



3. Workbooks



Interactive dashboards for visualizing insights, such as failed logins, MFA challenges, or geographic sign-in trends.


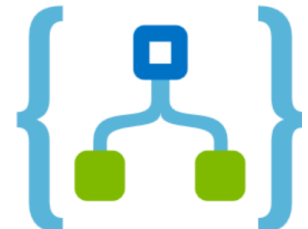








4. Incidents & Investigation



Group alerts into incidents, review the root cause with graphs, timelines, and investigate attacker activity.






Automate Response with Sentinel Playbooks

-  **What Are Playbooks?**
 - Built on **Azure Logic Apps**
 - Automate actions when threats are detected
 - Triggered by **analytics rules** or **incidents**
- 
-  **Common Use Cases:**
 -  **Send alerts to Microsoft Teams / Slack**
 -  **Notify SOC via email**
 -  **Auto-close false positives**
 -  **Disable risky user accounts**
 -  **Open tickets in ServiceNow or Jira**

Sentinel in Action: Detecting Suspicious Logins

- **Scenario:**







An attacker tries to log in to multiple user accounts from different countries within minutes.

-  **How Sentinel Helps:**
-  **Data Connector** pulls in sign-in logs from **Microsoft Entra ID**
-  **Analytics Rule** detects multiple failed logins + geolocation anomalies
-  **Incident** is automatically triggered
-  **Playbook** disables the user account + sends alert to SOC

This kind of real-time threat detection and response
used to take hours. Now it's automatic.







Watch the Costs: Log Analytics & Sentinel Tips

-  **Key Reminders:**
-  **Sentinel uses Log Analytics** – every query and log stored consumes **storage**
-  The **more connectors + analytics rules**, the more cost adds up
-  Use **Azure Pricing Calculator** to estimate your cost ahead of time
-  **Delete unused resource groups & workspaces** to avoid unnecessary charges
-  Enable **Retention Policies** to auto-delete old log data

Visibility is powerful. But visibility without control... is expensive

Wrap-Up: Start Strong with Microsoft Sentinel

Key Takeaways:

-  **Sentinel** connects to a **Log Analytics Workspace**
-  Built for advanced **cloud & hybrid threat detection**
-  Use **Workbooks**, **Analytics**, and **Hunting** to gain deep insights
-  Start small, monitor your **cost**, and expand as needed



Follow for more Microsoft Security projects! 

#PerparimLabs | #MicrosoftSentinel | #CloudSecurity | #SC300 |
#AzureSecurity