Security Information and Event Management (SIEM) and Security Orchestration Automated Response (SOAR)

SIEM

A tool that an org uses to collect data across the entire realm - infra, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts/incidents.

SOAR

A system that takes alerts from many systems (such as an SIEM system). It then triggers action driven automated workfrlows and processes to run security tasks that mitigate the issue.

MS Sentinel Integrated threat management

MS Sentinel is a scalable, cloud native SIEM/SOAR solution providing intelligent security analytics and threat intelligence.

Collect: data at cloud scale across all users, devices, applicatoins, and infrastructure (both on-prem and cloud)

Detect: previously uncovered threats and minimise false positives using analytics and threat intelligence

Investigate: threats with AI and hunt suspicious activity at scale

Respond: t oincidents rapidly with built-in orchestration and automation of common security tasks

Sentinel helps enable E2E secops in SOC.

Key features of Sentinel

Connect Sentinel to your data

Sentinel comes with many connectors for MS solutions out of the box such as Office 365 and Azure AD. There are also community-built data connectors listed in the Microsoft Sentinel GH repo.

Workbooks

After connecting data sources you can monitor the data using Azure Monitor Workbooks (custom, or from template).

Analytics

Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that create an actionable possible threat you can investigate and resolve. You can use bulit-in correlation rules as is or use them as a basis for building your own.

Manage incidents

Incident management allows you to manage the lifecycle of the incident. View all related alarts that are aggregated into an incident - where you can then triage and investigate.

Security automation and orchestration

Use Sentinel to automate some secops and make your SOC more productive. Sentinel integrates with Azure Logic Apps allowing you to create automated workflows or playbooks in response to events.

Playbooks work beset with single repeatable tasks and don't require coding.

Investigation

In preview, Sentinel's investigation tools help understand the scope of potential sec threat and find root cause.

Hunting

Powerful search-and-query toos based on MITRE framework proactively hunt for sec threats across org data sources before an alert is triggered.

Notebooks

Sentinel supports Jupyter notebooks so you can extend the scope of what you can do with Sentinel data for example create custom data visualisations (timelines, process trees).

Community

The community is a powerful resource for threat detection and atuomation. MS Security analysts constantly create and add new workbooks, playbooks, and hunting queries.

Sentinel Costs

Capacity Reservations

Billed a fixed fee based on selected tier, giving a predictable TCO

Pay-As-You-Go: billed per GB for volume of data ingested for analysis in Sentinel and stored in Azure Monitor Log Analytics workspace.