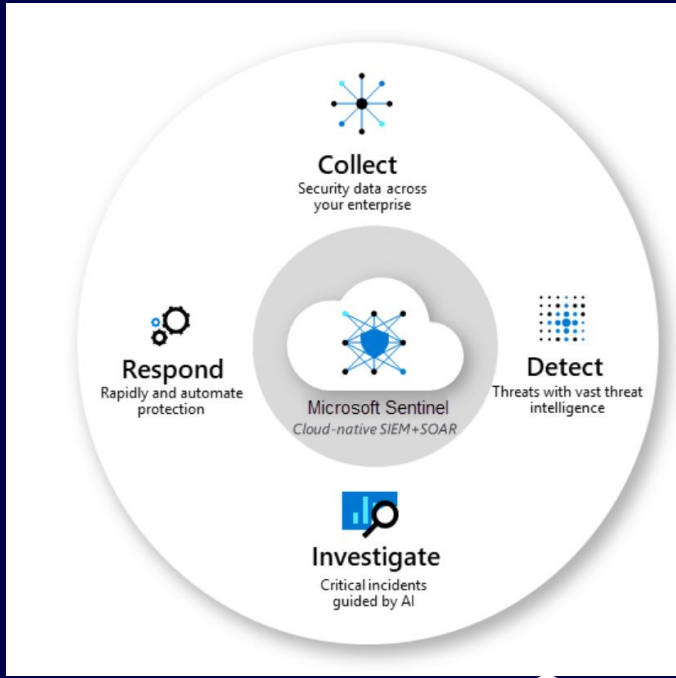
Defend Against Threats

Microsoft Sentinel is a scalable, cloud-native solution that provides Security information and event management (SIEM) and Security orchestration, automation, and response (SOAR).

Microsoft Sentinel's automation and orchestration solution provides a highly extensible architecture that enables scalable automation as new technologies and threats emerge.

Business Focused Outcomes

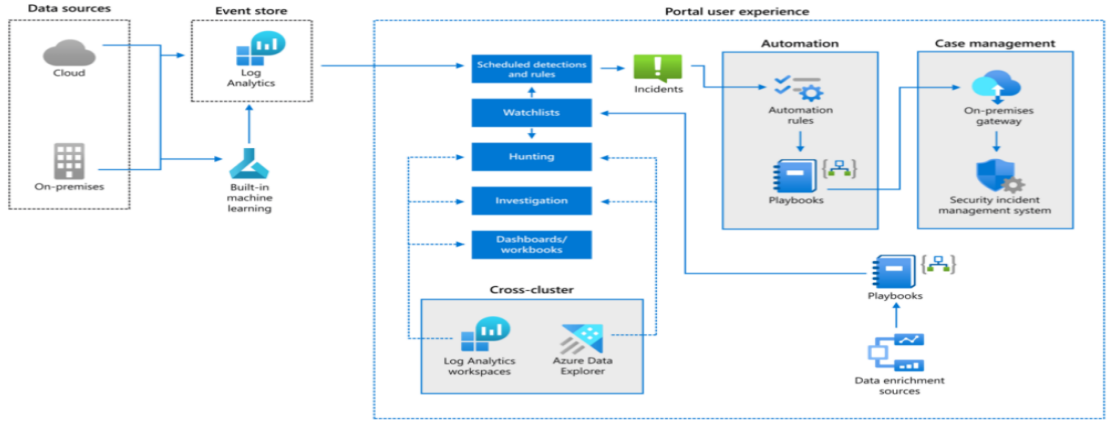
- Comprehensive security to Get end-to-end visibility across your resources, including users, devices, applications, and infrastructure.
- Integrated threat protection with SIEM and XDR
- Investigate prioritized incidents, Surface critical incidents and hunt suspicious activities at scale.
- Enable efficient and effective response incidents rapidly with built-in orchestration and automation of common tasks.
- Build next-generation security operations Uncover sophisticated threats and respond decisively with an easy and powerful security information and event management (SIEM) solution, powered by the cloud and AI.



> **Every company will need to be a technology company.**
>
> **Satya Nadella**

Microsoft Business Group

Architecture for the new SIEM solution using Microsoft Azure Sentinel



Phase 1 – Plan Architecture

Determine which data sources needed and the data size requirements to help accurately on deployment's budget and timeline. Design Microsoft Sentinel workspace and Make sure that data ingestion for both Microsoft Sentinel and Azure Log Analytics, any playbooks that will be deployed.

Phase 2 – Collect data

Enable a data connector to perform real-time log streaming. Classify and analyze data using entities

Phase 3 – Integrate Threat Intelligence

Integrate threat intelligence (TI) into Microsoft Sentinel and Import threat intelligence with data connectors

Phase 4 – Detect, Investigate data and Automate responses

Use tasks to manage incidents in Microsoft Sentinel and Create required Workflows. Create Automation rules and playbooks

cognizant