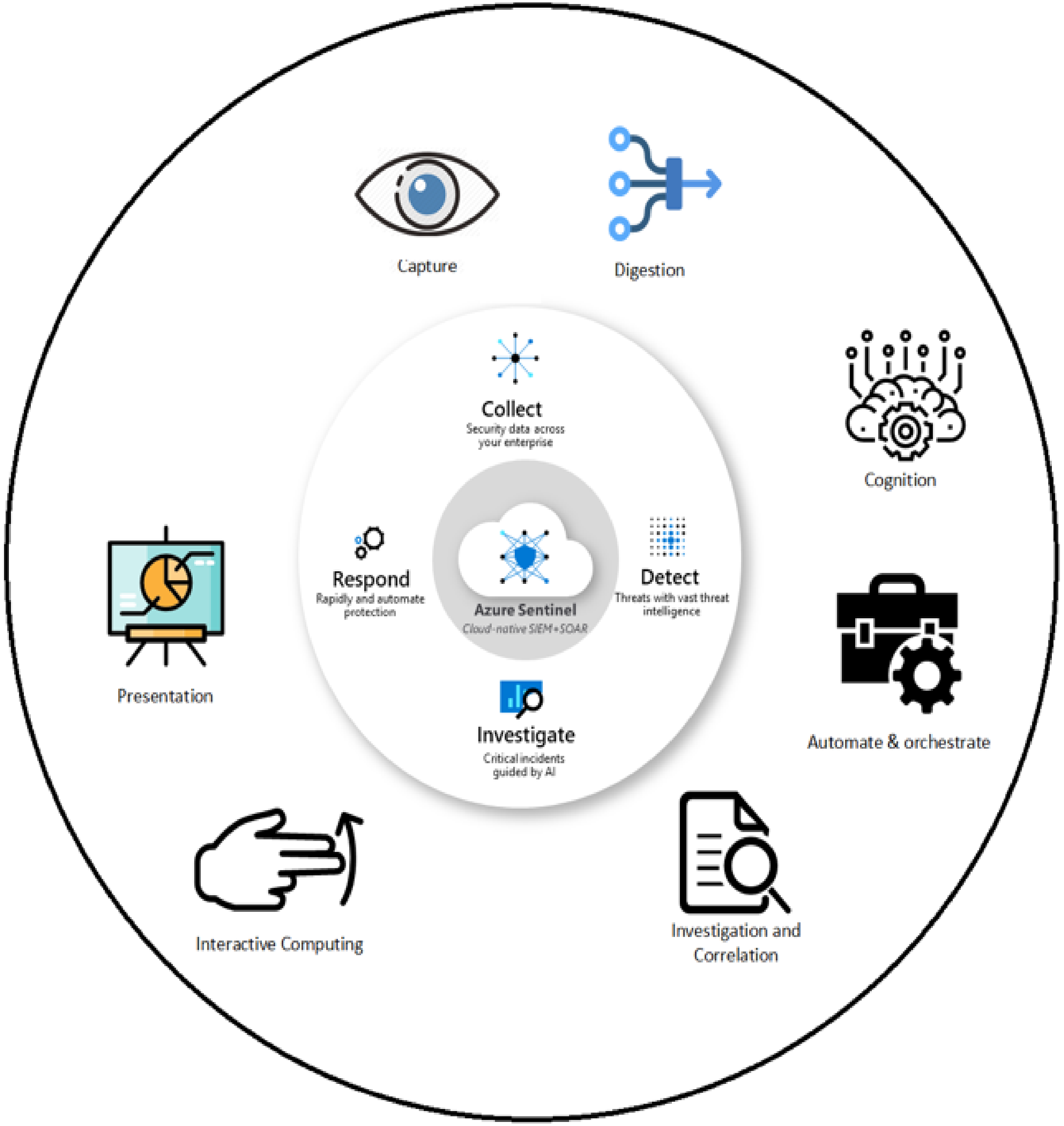
Global Brands Group

Security Hub Solution



Capture

Digestion

Cognition

Automate & orchestrate

Investigation and Correlation

Interactive Computing

Presentation

Collect
Security data across your enterprise

Detect
Threats with vast threat intelligence

Investigate
Critical incidents guided by AI

Respond
Rapidly and automate protection

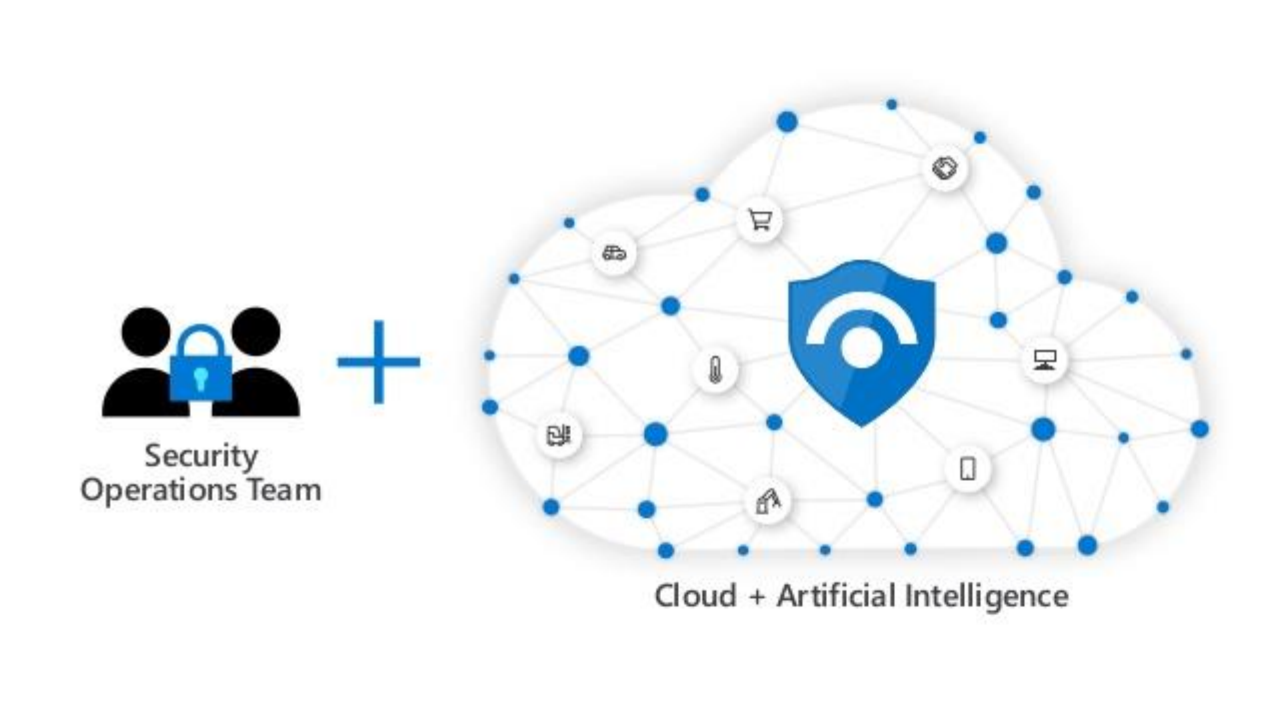
Azure Sentinel
Cloud-native SIEM+SOAR

Global Brands Group

Microsoft Gold Partner

We are Targeting all Cloud Customers

provides a comprehensive view of your security state in Azure and helps you check your compliance with the security industry standards and best practices. Security Hub Solution collects security data from across Azure, on-premises, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.



CHALLENGES

collect log information from any source, including other clouds and on-premises systems and to provide many ways of looking at the security situation with automatic response

IDEAL SOLUTION

We need one solution to collect all log info from any source (clouds , on-premises) and provide it with many ways and dashboards

DESIRED OUTCOMES

cloud based SIEM Solution with amazing scaling capabilities that not only protects Azure but also helps to protect other cloud services. It can analyze data from Office 365, cloud app security, etc.

With Automatic Response and easy installation

Global Brands Group

Security Hub

provides a comprehensive view of your security state in Azure and helps you check your compliance with the security industry standards and best practices. Security Hub Solution collects security data from across Azure, on-premises, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

Built-in AI: Security Hub includes built in AI to focus on real threats quickly with machine learning feature. It learns from the daily signals it gets based on trillions of analysis and track security breaches. With AI it can easily collect, detect, analyze and respond to threats.

Cloud SIEM: Security Hub Solution is purely cloud based with amazing scaling capabilities that not only protects Azure but also helps to protect other cloud services. It can analyze data from Office 365, cloud app security, etc.

Automatic Response: Security Hub features automatic detection and responses to the threats and keep your enterprise secure. Due to the automated response feature it is highly favorable choice.

Security Hub is fully integrated with Azure sentinel for the dashboards and automatic response

Global Brands

Security Hub + Azure Sentinel

is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.
Also collects security data from network devices, servers, domain controllers, and more. Security Hub stores, normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.

Dashboards:

From the administrator’s viewpoint, the epicenter of Sentinel is the dashboard. It provides many ways of looking at the security situation. The toolbar gives information about the number of events and alerts over a time period, as well as the number of new, investigated, and closed events.

Machine Learning:

Security Hub makes information more manageable with machine learning, including built-in ML and an optional module called Fusion. Third parties can add “build-your-own” ML. They recognize patterns which are especially suspicious, such as logging in from an unusual IP address followed by a massive file download.

Automation & Orchestration:

It supports automated threat responses in the form of “playbooks”. Playbooks, built on Azure Logic Apps, set up a series of procedures to run when the situation warrants it.

Customer success: WADI DEGLA CLUBS

It gives WADI DEGLA security teams live insight into network traffic through a variety of rich user displays and interactive dashboards. From there, analysts can attend to high-priority alerts with relevant context into the location of the activity, the type of threat detected, a timeline of events, and several other useful data points the team may need to successfully mitigate the threat.

Win Results

Automate common security tasks, such as event alerts, threat responses, and process workflows to streamline company security efforts from end to end

Integrates with a variety of native and 3rd party data sources, granting security teams the ability to collect and analyze massive amounts of network data across deployments, users, applications, and devices each second

Gives security teams a set of intelligent search and query tools their analysts can use to unearth threats and catch other suspicious behavior that may have passed under the radar.