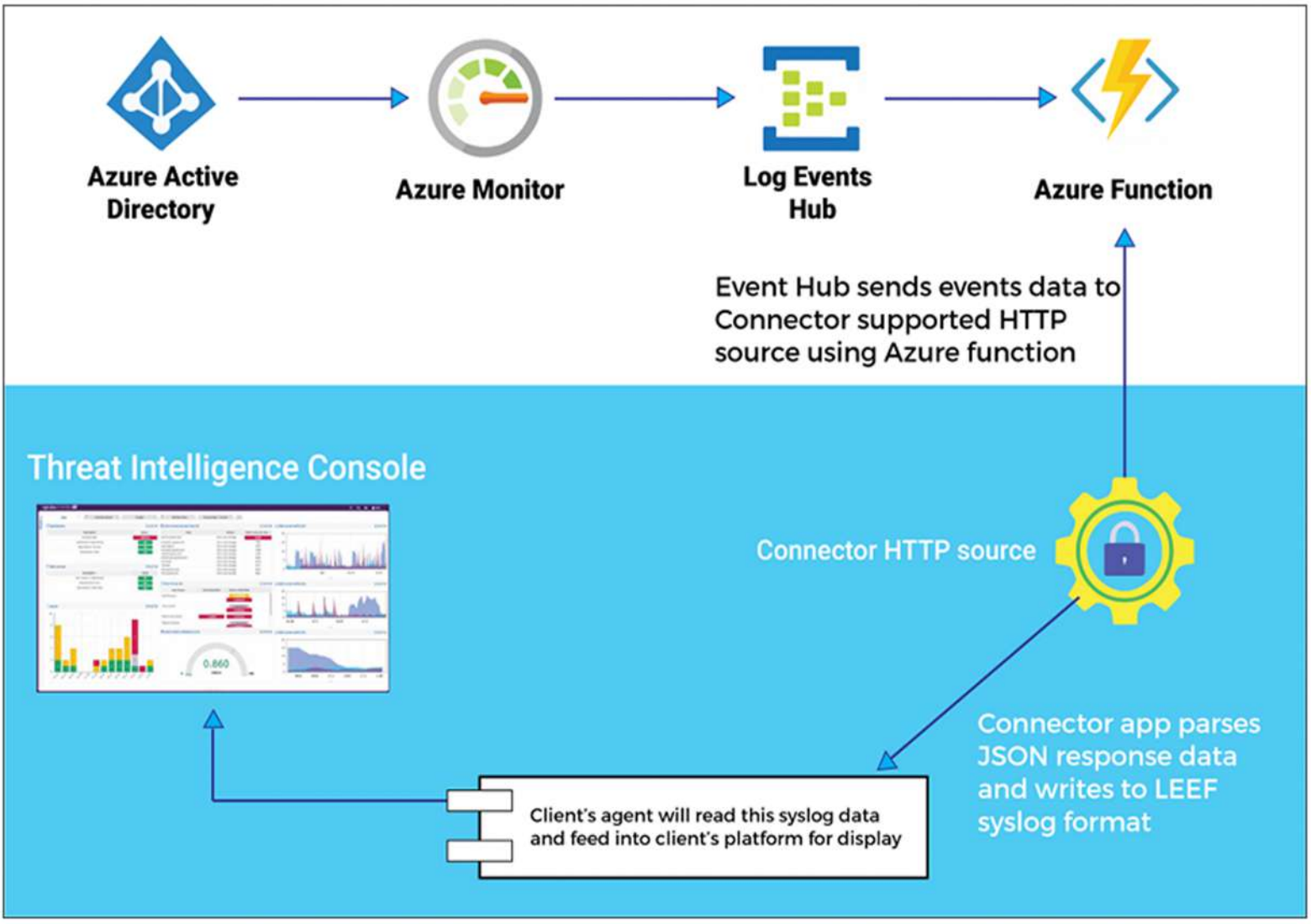
Azure Active Directory with Threat Intelligence Platform



Customer

Customer is a leading Threat Intelligence solution provider.

They provide a platform for companies to aggregate and act upon Threat Intelligence.

Requirement

Customer requested for the integration of their product with the Azure Active Directory logs

Technology Solution

- Azure Monitor collects logs for Azure Active Directory, and streams the data to an Azure Event Hub. The Event Hub streams the logs collected by Azure Monitor to the Connector supported HTTP Source through an Azure function
- The Connector receives the events data and parses response data and writes in the LEEF format
- API Test methods and Selenium automation scripts were used to generate the Azure Active Directory events for testing

SACUMEN Security Execution Partner

Learn More : *www.sacumen.com/services/connector-development*

www.sacumen.com

Sacumen is an award winning pure play security product development services company. We are engaged with 50+ security product companies such as Symantec, Palo Alto Networks, Varonis, AlienVault, IBM, CA Technologies, ThreatConnect, SecurityScorecard, ForgeRock, Code42, BigID, Flashpoint etc in the areas of Connector Development, Connector Support and Product Engineering.

info@sacumen.com

+1 408 585 9982