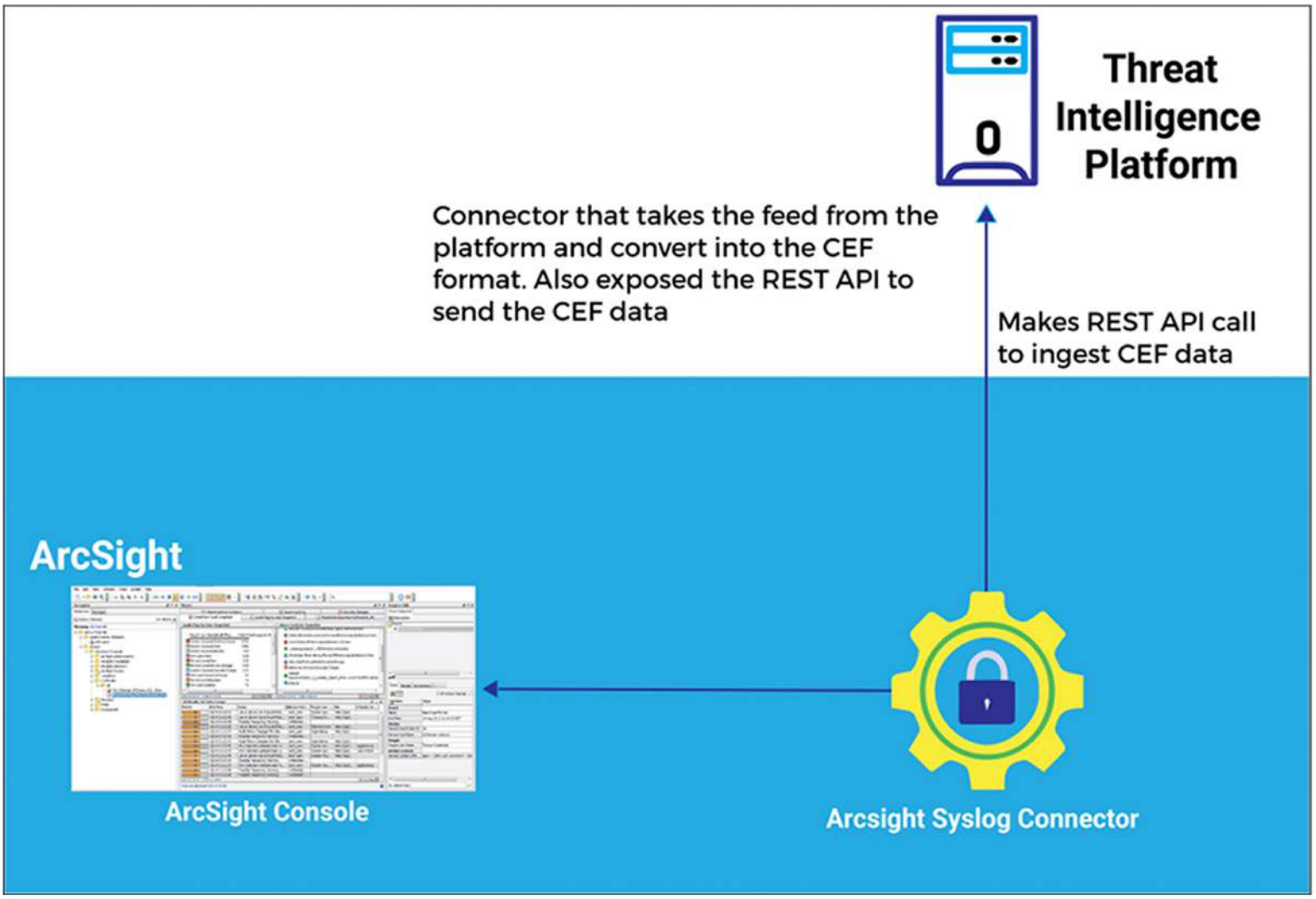
Threat Intelligence Platform integration with ArcSight



Customer

Customer is a leading Threat Intelligence platform, delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals around the globe.

Requirement

Client requested for the integration of their CASB product with the On-premise/Cloud based QRadar so that they can monitor the Cloud through one SIEM console

Technology Solution

- Sacumen developed the Connector for customer's Threat Intelligence Sproduct for integration with HP ArcSight ESM using CEF (Common Events Format)
- Threat Intelligence Connector (to provide REST interface) developed using JAVA to send the CEF Syslog data to HP Arcsight Syslog Connector
- Automatically correlate internal and external network events using prioritized real-time IP threat intelligence with contextual information to detect malicious IP threats for investigation
- IP Correlation component developed using HP ArcSight Console
- Built dashboards to display alerts and other relevant information. The nature of the reports and dashboards developed was in line with the model provided by HP ArcSight Console

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