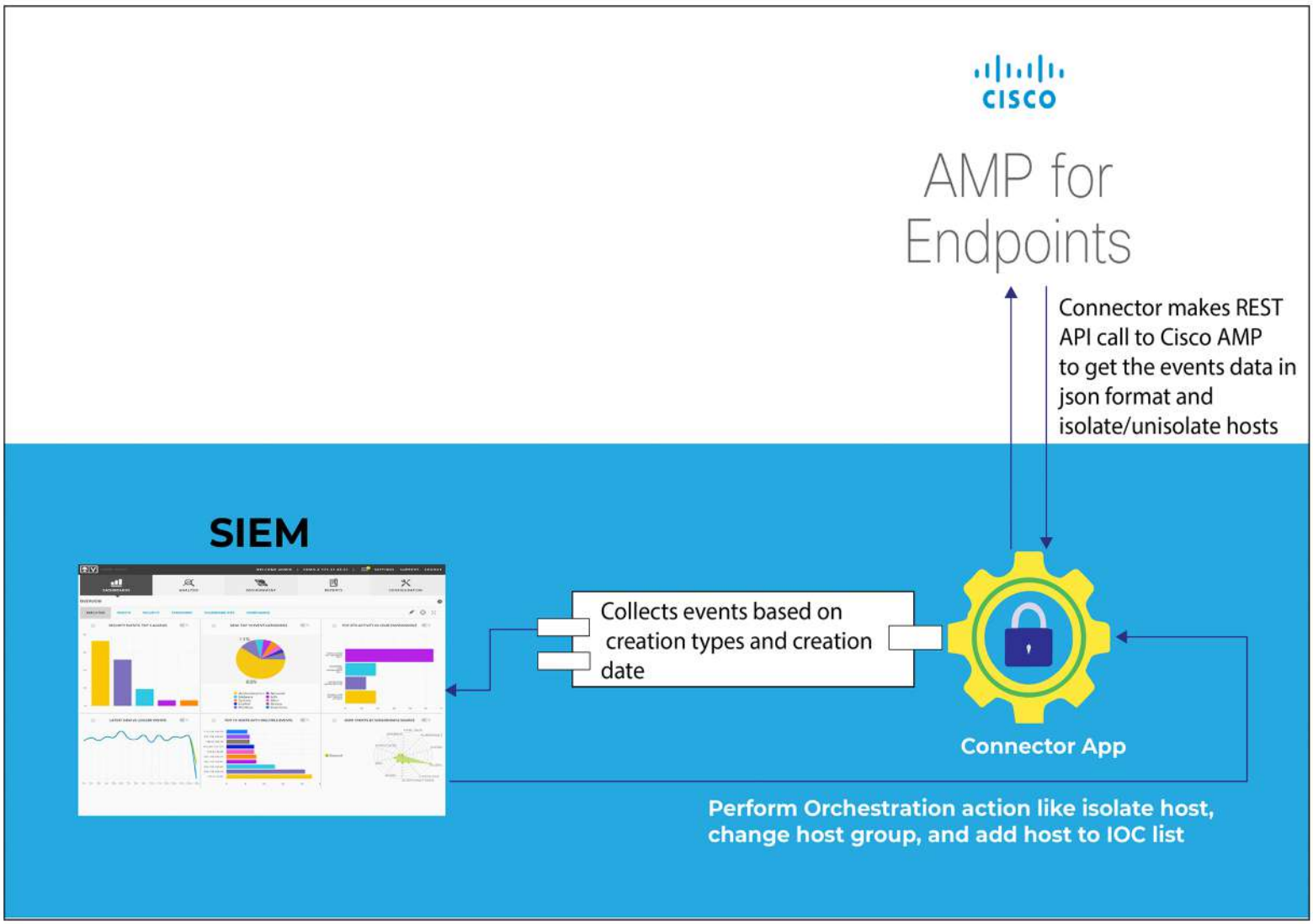
SIEM Integration with Cisco AMP



Customer

Customer is a leading SIEM solution provider.
They provide a platform for companies to aggregate and act upon Threat Intelligence.

Requirement

Customer requested to build a Connector to integrate their platform with Cisco AMP End Event Monitoring to collect events and perform orchestration action like isolation, unisolation based on file hash, IP address, change host group, and add IOC list based on security alert or event.

Technology Solution

Sacumen developed the Connector to integrate Cisco AMP using java, and Apache REST. The Connector performs the following actions:

- Set up the prerequisites
  - Login Cisco AMP Endpoint
  - Setup the Connect App

Authenticate using API (REST) with Basic OAuth , the access using API Key and Client ID.

- Collect the events
- Collect event based on filter like event type, event creation date
- Sampling of the records to calculate estimated EPS.
- Calculate error rate.
- Calculate bandwidth consumption.
- Perform orchestration action like isolate host, change host group, and add host to IOC list

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