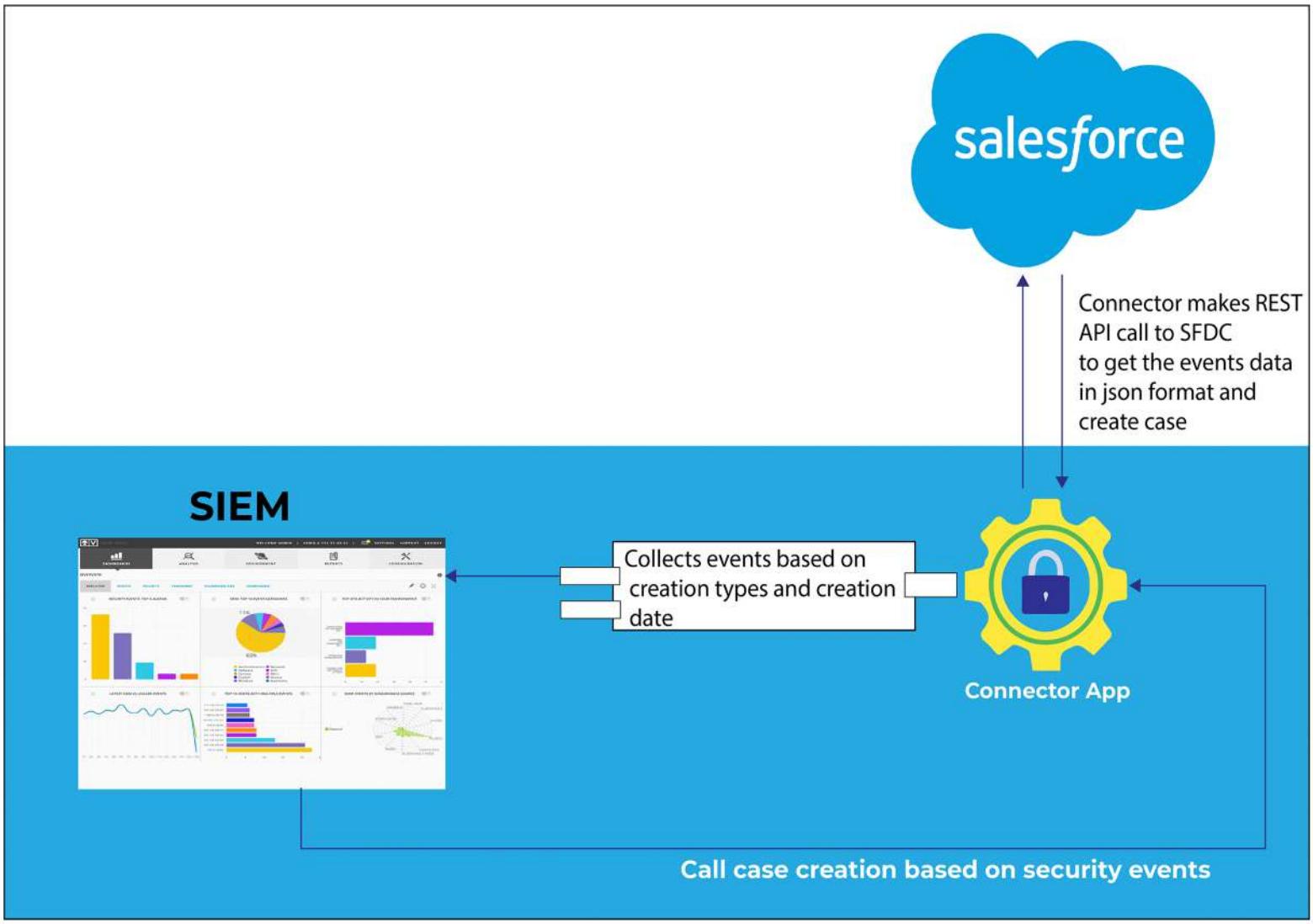
SIEM Integration with Salesforce



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 app to integrate their platform with Salesforce Event Monitoring to collect events, and perform orchestration action to create case based on security alert.

Technology Solution

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

- Set up the prerequisites
  - Setup Salesforce Developer login
  - Or Connect App credential

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

- Collect the events
- Collect event based on filter like event type, event creation date
- Calculates estimated EPS.
- Calculates bandwidth consumption.
- If EPS goes beyond the limit, then throttle the extra events to maintain performance of the app.
- Perform orchestration action like create cases in Salesforce.

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