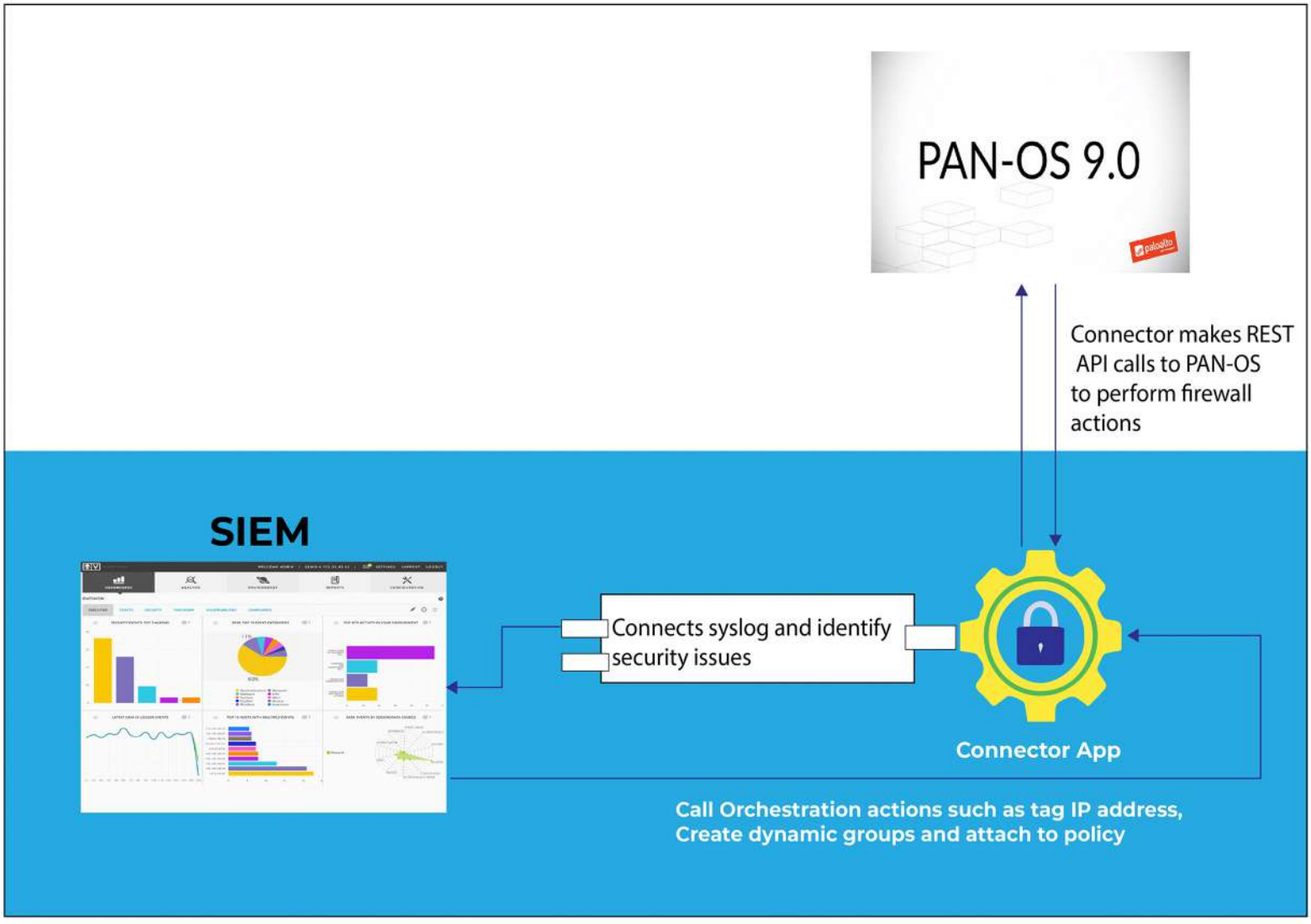
SIEM Integration with Palo Alto PAN-OS



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 Palo Alto Networks PAN-OS/Firewall to collect Syslog to present as event after normalization, and perform orchestration action to create dynamic address group attach IP address with tag so security policy can make use of it.

Technology Solution

PAN-OS is the software that runs all Palo Alto Networks® next-generation firewalls
Sacumen developed the Connector app to integrate Palo Alto Networks using java, and Apache REST.
The Connector app performs the following actions:

- Set up the prerequisites
  - Setup Palo Alto firewall
  - Create service account
- Set up the prerequisites
  - Sampling of the records to calculate estimated EPS.
  - Calculates bandwidth consumption.
  - Calculates Error rate.
  - Setup Palo Alto firewall
  - Perform the Orchestration action such as Create Tag to specific IP Address, create Dynamic Address Group.

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