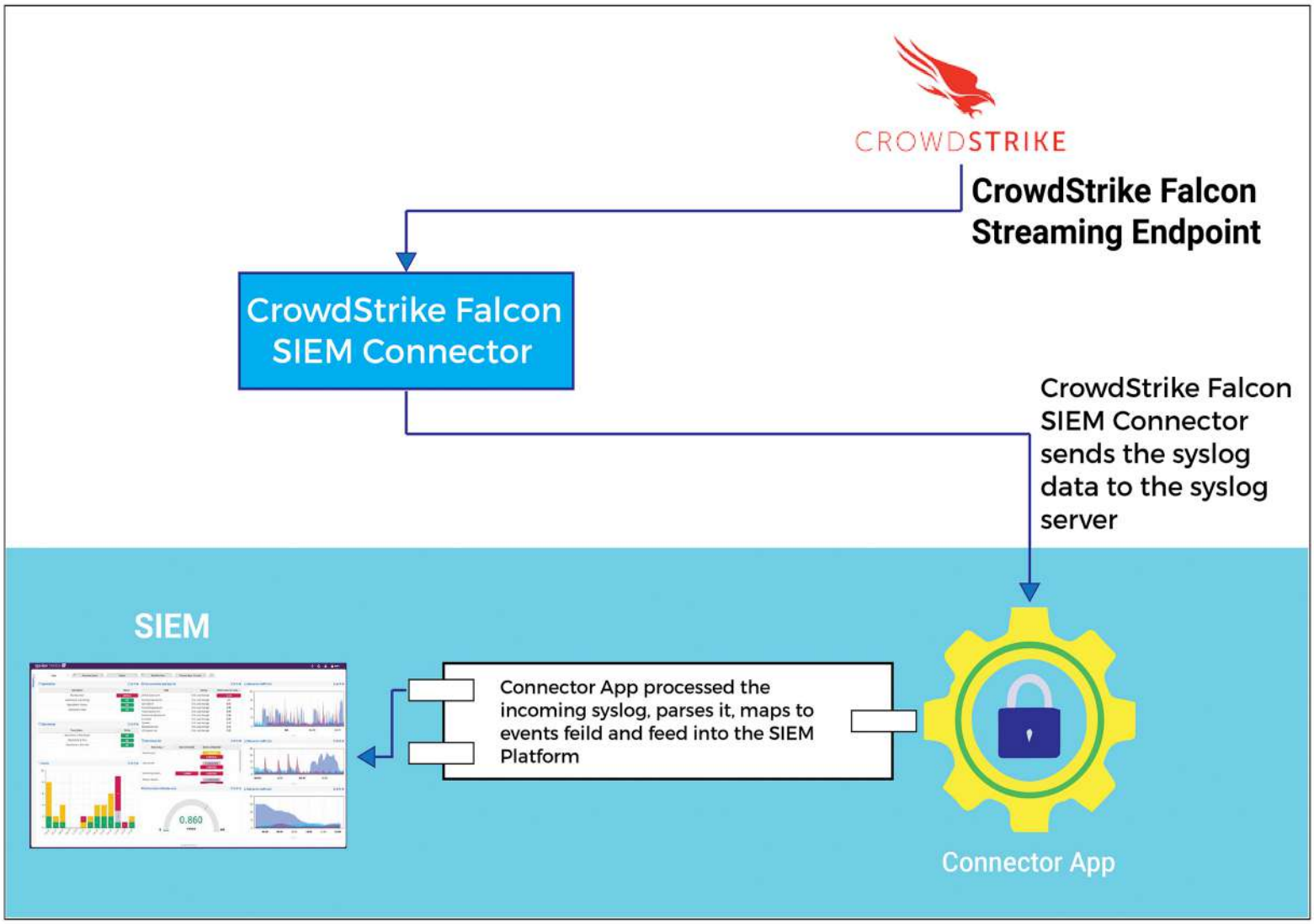
CrowdStrike Falcon integration with SIEM Platform



Customer

Customer is a leading SIEM 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 CrowdStrike Falcon

Technology Solution

- Sacumen developed the Connector app that collects and process logs from the CrowdStrike Falcon platform through CrowdStrike Falcon SIEM Connector
- CrowdStrike Falcon SIEM Connector collects the events data from CrowdStrike Falcon platform by making API calls to the CrowdStrike Falcon platform
- CrowdStrike Falcon SIEM Connector then pushes Syslog data to Syslog server
- Connector app processed the incoming Syslog, parses it, maps to events fields and feed into the SIEM Platform

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