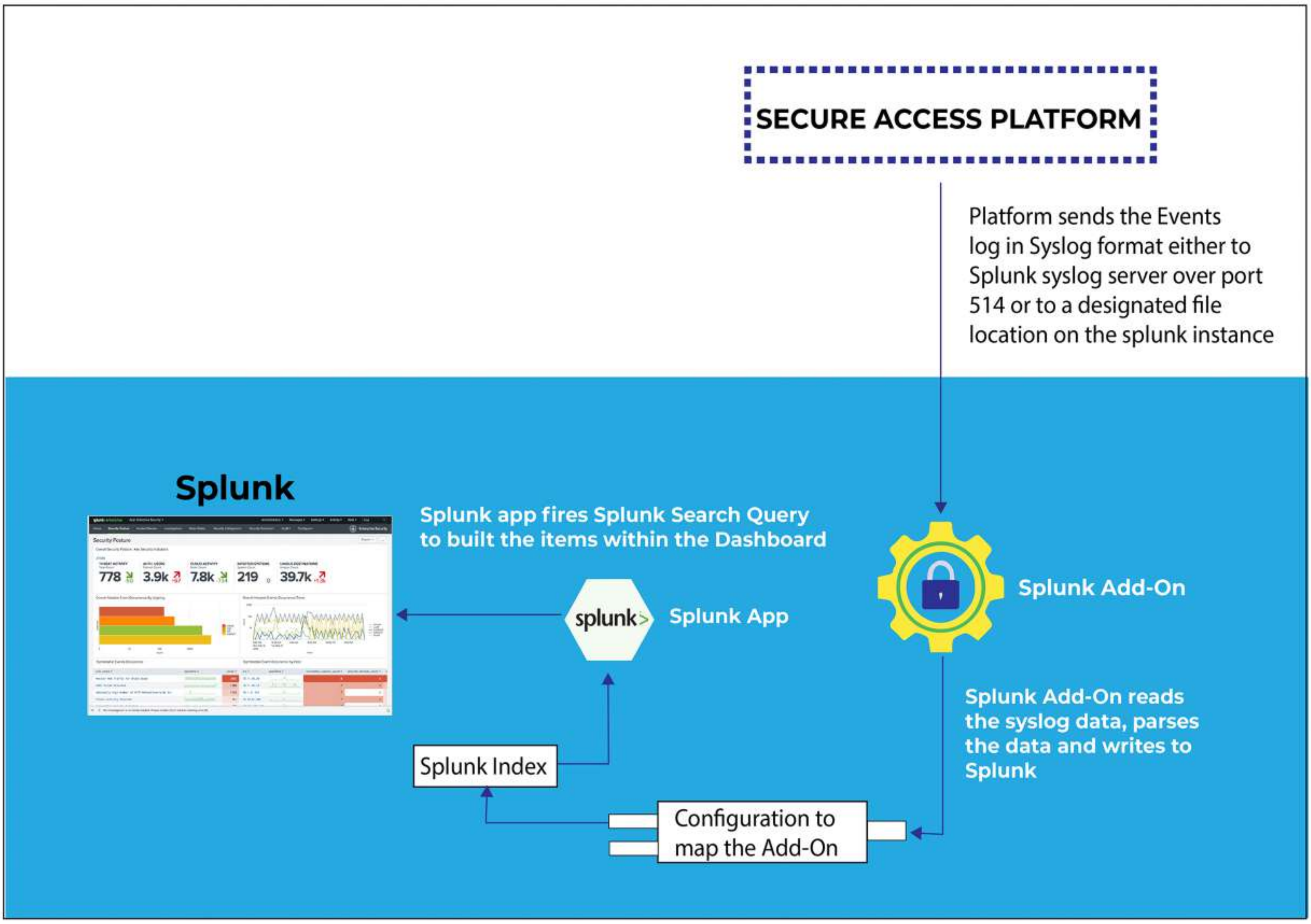
Secure Access Platform integration (Add-On and App) with Splunk



SECURE ACCESS PLATFORM

Platform sends the Events log in Syslog format either to Splunk syslog server over port 514 or to a designated file location on the splunk instance

Splunk

Splunk app fires Splunk Search Query to built the items within the Dashboard

Splunk App

Splunk Add-On

Splunk Add-On reads the syslog data, parses the data and writes to Splunk

Splunk Index

Configuration to map the Add-On

Customer

Customer is a leading provider of secure access solutions to both enterprises and service providers.

Requirement

Customer requested the development of Splunk Add-on to ingest data from its platform into Splunk and provide visualization.

Technology Solution

Add-On:

- Sacumen developed the Splunk Add-on to ingest the events logs data in Syslog format.
- Around 100 Log events are supported by the add-on
- Support for CIM 4.0

App:

- Sacumen developed the Splunk App containing 1 Dashboard. This Dashboard consists of 9 items. Splunk App fires the Splunk Search Query against the indexed data (data ingested into Splunk by the Splunk Add-on) and build the items in the Dashboard
- Reports were built against the indexed data (data ingested into Splunk by the Splunk Add-on)

Both Splunk App and Add-on support Splunk Enterprise (version 7.3)

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