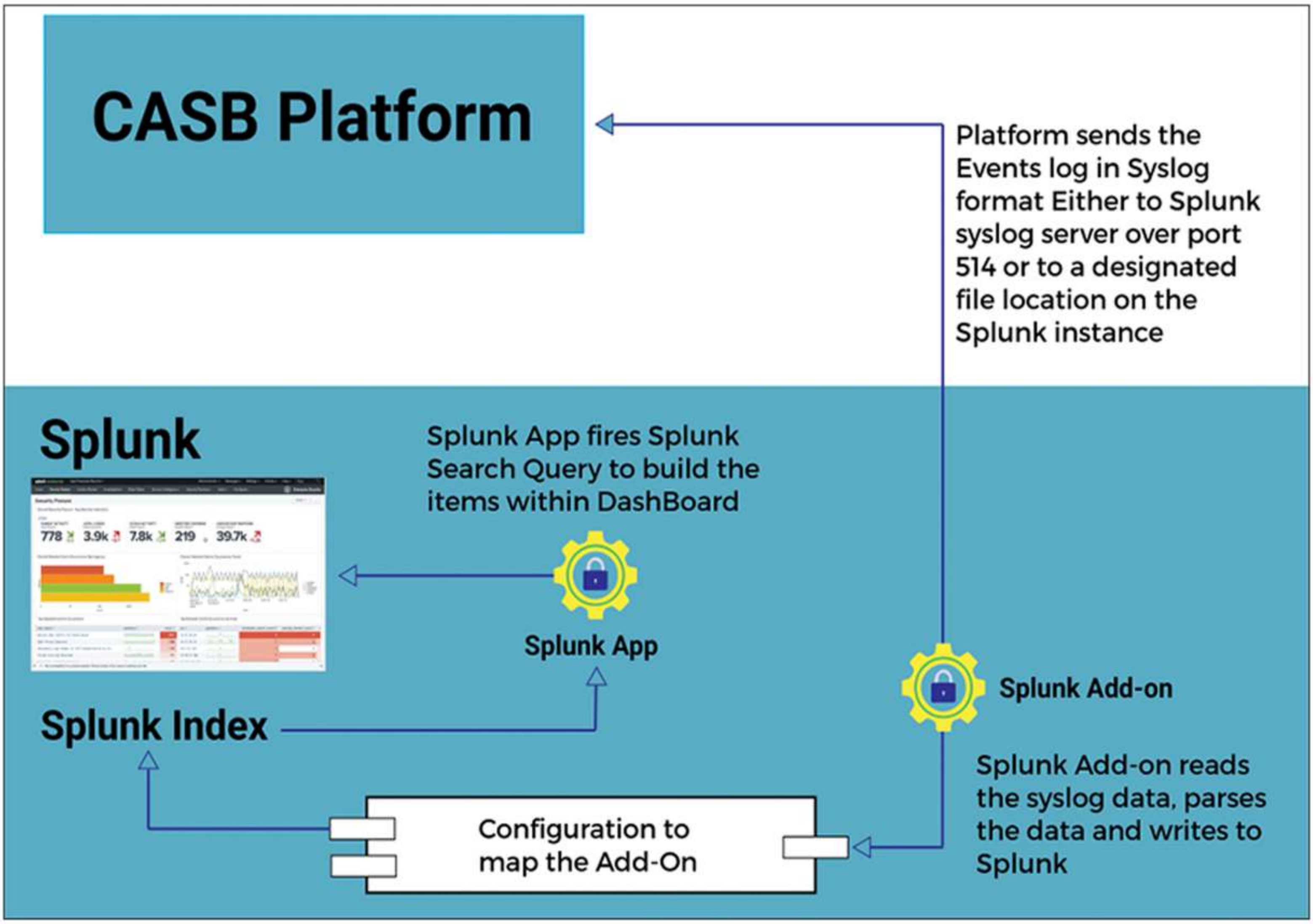
SACUMEN
Security Execution Partner

CASE STUDY

CASB Platform integration (Add-on and App) with Splunk



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 App fires Splunk Search Query to build the items within DashBoard

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

Configuration to map the Add-On

Customer

Customer is a leading CASB Solution Provider

The CASB solution provider delivers cloud visibility, security and anomaly detection for hybrid enterprises.

Requirement

Customer requested the development of Splunk Add-on and App to integrate with its CASB platform.

Technology Solution

Add-on

- Sacumen developed the Splunk Add-on to ingest the events logs data in Syslog format.
- Around 20 log events are supported by the add-on.
- Support for CIM 4.0

Add-on

- Sacumen developed the Splunk app containing 1 Dashboard. This Dashboard consists of 10 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.

Both Splunk app and add-on support Splunk Enterprise (version 7.3)

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