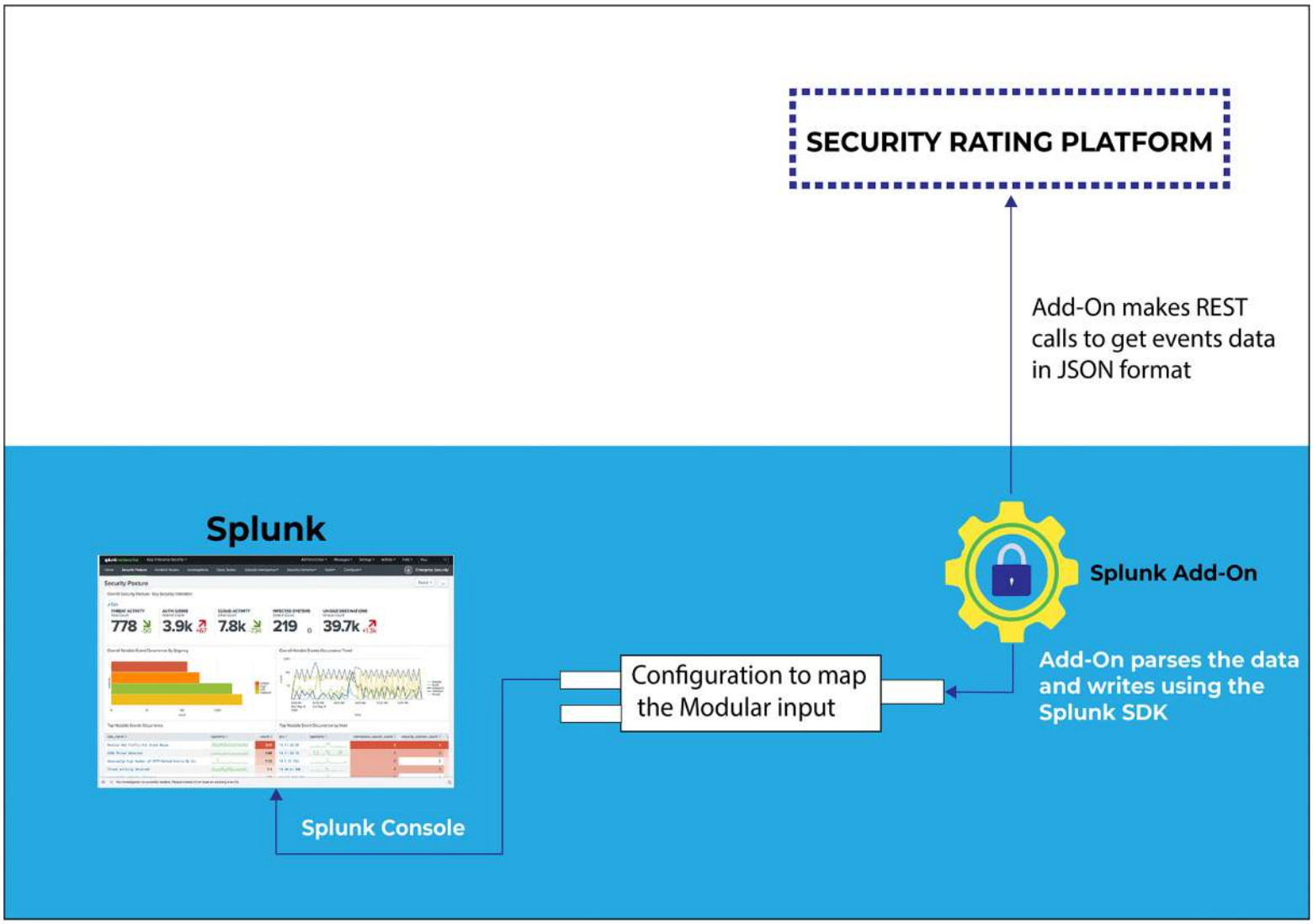
Security Rating Platform integration (Add-on) with Splunk



Customer

Customer is a leading Security Rating provider.

It rates Cybersecurity postures of corporate entities through the scored analysis of cyber threat intelligence signals for the purposes of third party management and IT risk management

Requirement

Customer requested for the development of the Certified Splunk Add-on to integrate its rating platform with Splunk

Technology Solution

Sacumen developed the Certified Splunk Add-on that performs the following:

- Fetch the Overall/Factors/Issues/ Issue findings data
- Application set-up (API key, Polling interval, Different flags to poll and filter data as per customer needs)

The Add-on was built using Splunk Add-on builder and modular input in python language was written

The Add-on supports Splunk version 7.x and 8.0

Complex logic to manage the date logic was implemented. This ensured that the data loss did not happen

Add-on supported Retry mechanism. It supported setting logging level and proxy support

Add-on supported CIM 4.x

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