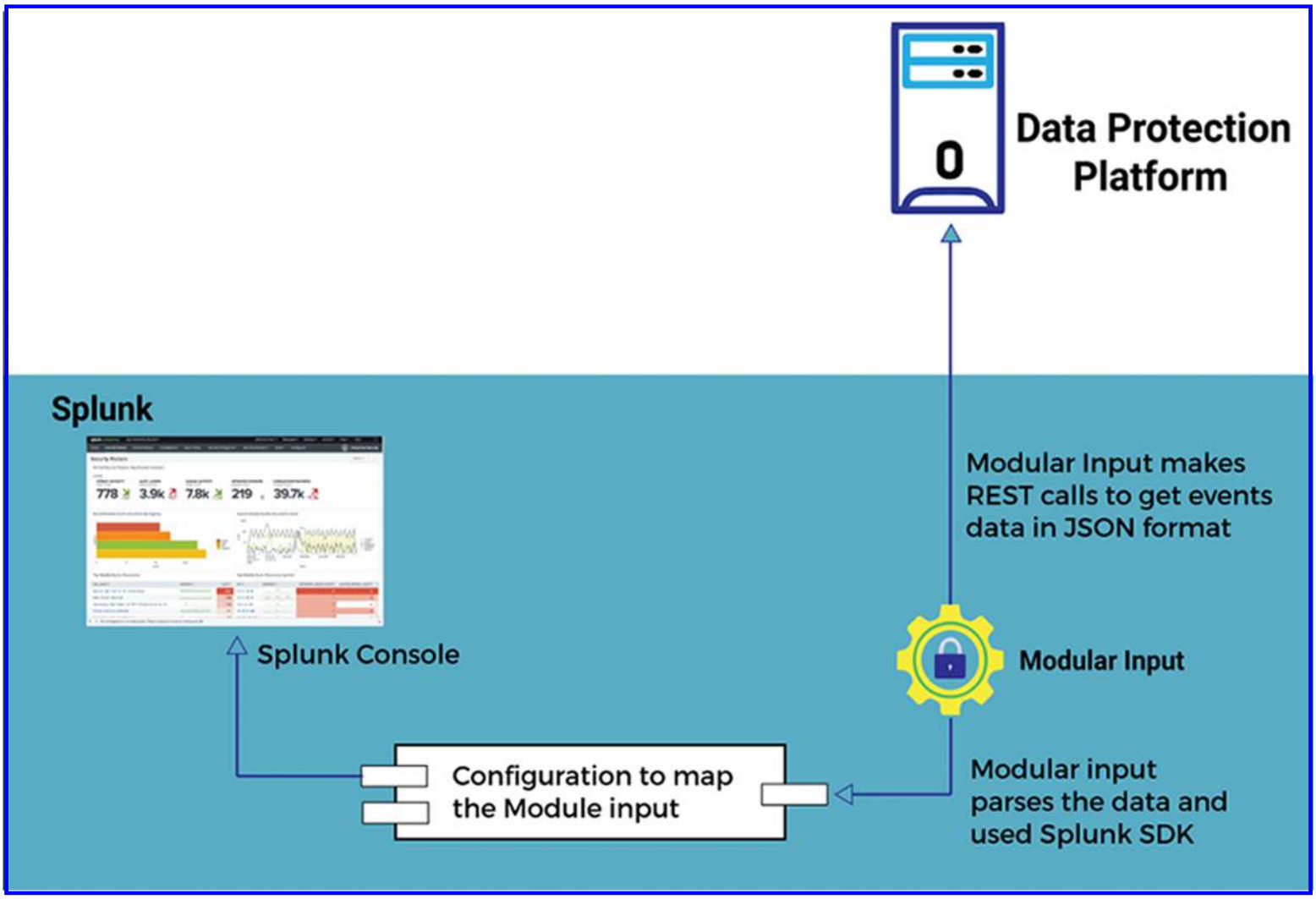
Data Protection Platform integration(Add-on) with Splunk



Customer

Customer is a leading Data Protection solution provider.

It has security software platform to let organizations track, visualize, analyze and protect their structured and unstructured data

Requirement

Customer requested the integration of their Data protection platform with the Splunk so that their clients can view the threat data in Splunk console.

Technology Solution

- Sacumen developed the Splunk Modular Input app that polls events data in JSON format from the Data protection platform through REST APIs
- Modular Input had configuration file to configure the Client's URL, API Key and other required configuration parameters.
- Modular Input parsed the data and used Splunk SDK
- Events mapping was done against the Splunk field and custom events were defined
- Splunk Modular Input app was developed for Splunk version 6.5 and above

SACUMEN
Security Execution Partner

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