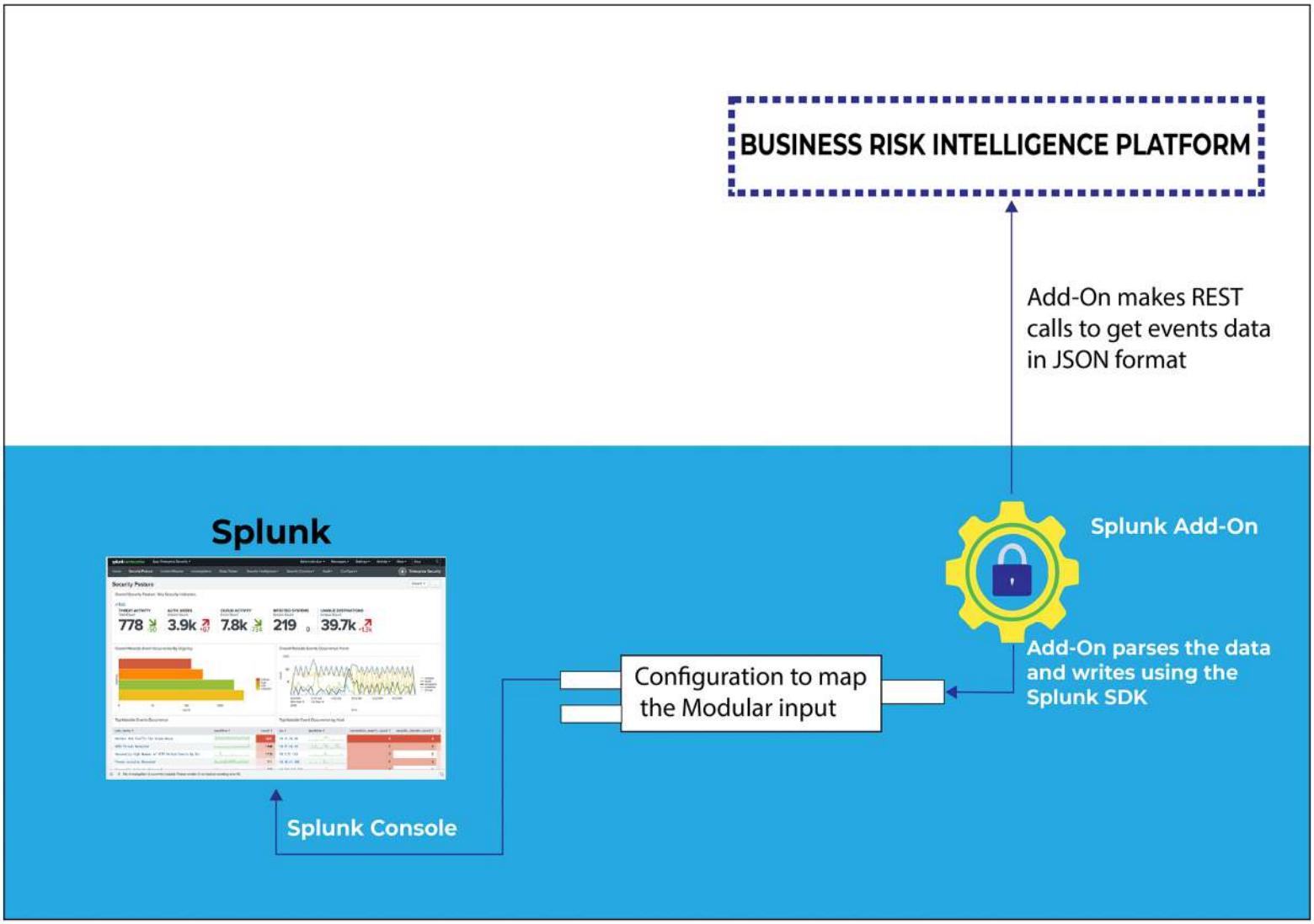
Business Risk Intelligence Platform integration (Add-on) with Splunk



Customer

Customer delivers converged intelligence and risk solutions to private and public sector organizations worldwide

It provides meaningful intelligence to assist organizations in combating threats and adversaries.

Requirement

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

Technology Solution

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

- Correlate Exposures and Behavior data to internal events tracked in Splunk.
- Create custom reporting, dashboards, and visualizations.
- Gain context for IPs, Exposures, and Risky Flows observed on your network perimeter
- Add-on for Splunk allows you to consume and access Events, Assets, and Behavior data through Splunk. You can configure your data as a Splunk data input, configure the add-on to use a proxy, search your data through the Splunk UI using Splunk data queries, and more.
- 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.
- 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