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 Splunk Add-on to ingest the events logs data in Syslog format.

- Captures, indexes, and correlates in real time technical data within Splunk's searchable repository.
- Enables users to generate reports and visualizations, including graphs, alerts, and dashboards.
- Collect integrated data using REST-based API.
- Includes IOCs such as hashes, URLs, domains, as well as details related to malware families, mapping to the MITRE ATT&CK framework.

Sacumen developed the Splunk Add-on to ingest the events logs data in Syslog format.

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 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