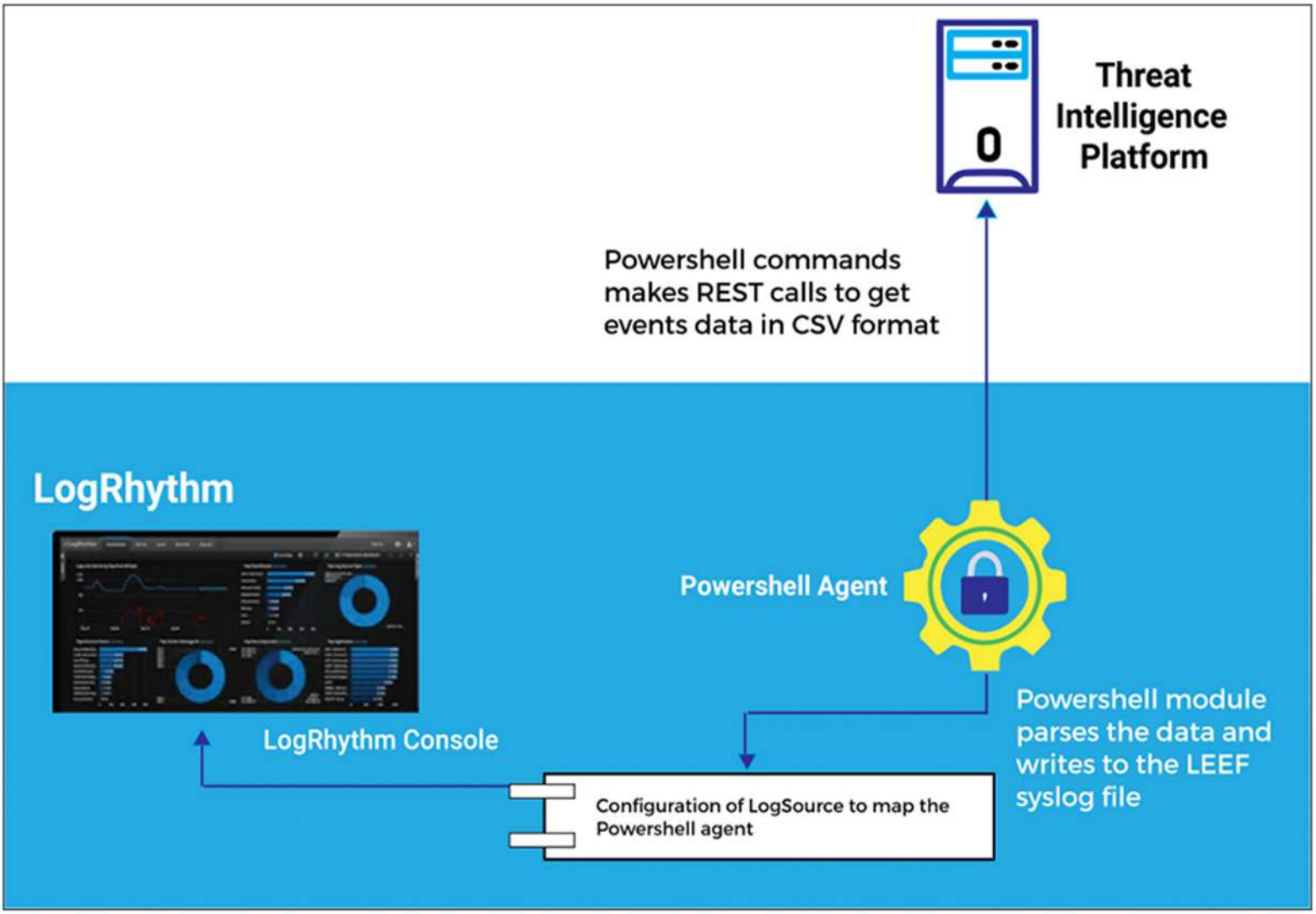
Threat Intelligence Platform integration with LogRhythm



Customer

Customer's Threat Intelligence platform enriches every stage of your security operations workflow from your trusted and relevant data sources.

Requirement

The Client requested for the integration of their Threat Intelligence platform with the LogRhythm so that their clients can view the Indicators of Compromise (IOC) data in LogRhythm's console

Technology Solution

- Sacumen developed the Powershell based agent app
- Powershell Agent used a configuration file in the Agent's config folder to configure the Client's URL, API Key and other required configuration parameters.
- Powershell Agent made REST calls to Client's platform to retrieve events data in CSV format.
- Powershell Agent parsed the data and write in LEEF format
- Events mapping was done against the LogRhythm field and custom events were defined

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