Pulse Secure integration (Add-on) with Splunk

Pulse Secure

Add on makes REST calls to Pulse secure API to push Processed Alerts data in JSON format

Splunk

Splunk Alert Trigger will pass the Alerts data to the Alert action defined In Add-On

Splunk Add-On

Alert Action handler parses the data, retrieves the Alerts events data (based on CIM fields filter)

Customer

Customer is a leading provider of secure access solutions to both enterprises and service providers.

Requirement

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

Technology Solution

- Sacumen built Splunk TA(Technical Add-On) that retrieves the Splunk's Alerts data and feed into the PulseSecure PPS (Pulse Policy Secure) platform.
- The Add-on was developed in Python using Alert Action Handler
- Add-On has configuration parameters defined on the Alerts screen such as PulseSecure's REST API URL, API Token, and other required configuration parameters
- Splunk Alert Trigger passes the Alerts data to the Alert action defined in Add-on, on match of search query output defined as part of Alerts configuration
- The Add-on supports Splunk version 7.x a
- Add-on supported Retry mechanism
- 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