![SACUMEN - Security Execution Partner]

ServiceNow integration with SIEM Platform

The Connector makes REST API calls to the ServiceNow end point to register an incident for various for alerts/events/vulnerabilities

SIEM

Connector app exposes interface to receive the data from SIEM process and parse as required

Connector App

Customer

Customer is a leading SIEM solution provider. They provide a platform for companies to aggregate and act upon Threat Intelligence.

Requirement

Customer requested for the integration of their product with the ServiceNow

Technology Solution

- Sacumen developed the Connector app that creates incident tickets in ServiceNow for the events, alerts and vulnerabilities reported by the SIEM platform

- Connector exposes the interface that gets invoked at various stages of the orchestration rule, and events or alarm creation to register an incident ticket in ServiceNow

- Connector app processes and maps the events data, perform Oauth verification, and makes the REST api calls to the appropriate ServiceNow end points to register an incident.