



## Okta integration with Threat Intelligence **Platform**



Connector uses the Okta System Log API to fetch the events data from Okta system

## **Threat Intelligence Console**



Client's agent will read this syslog data and feed into Client's platform for display



Connector

Connector app parses JSON response data and writes to LEEF syslog format

SACUMEN



Customer is a leading Threat Intelligence solution provider.

They provide a platform for companies to aggregate and act upon Threat Intelligence.

Customer requested for the integration of their product with the Okta Audit logs



Requirement



## **Technology Solution**

- Connector uses the Okta System Log API to fetch the events data from Okta system
- The Connector receives the events data and parses response data and writes in the LEEF format
- API Test methods and Selenium automation scripts were used to generate the Okta audit events for testing



**Learn More**: www.sacumen.com/services/connector-development

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,

www.sacumen.com

