SACUMEN
Security Execution Partner

Okta integration with Threat Intelligence Platform

okta

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

Threat Intelligence Console

Connector

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

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

Customer

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