Detecting Insider Threat with Okta and Sumo Logic

Faster Incident Response - Detect, Contain, Eradicate

Organizations are adopting SaaS applications at an accelerating pace. User provisioning and activity monitoring for insider threat detection in the SaaS environment is complex. Traditional security solutions built for on-prem infrastructure are not effective in monitoring SaaS applications. Okta and Sumo Logic integration enables organization to detect insider threat by correlating authentication log from Okta with user activity logs from SaaS applications.

Business Challenges

Organizations are adopting SaaS applications at an accelerating pace. It is common for a company to have anywhere between 16-22 SaaS applications, and these business-critical applications hold sensitive and valuable company information. While SaaS applications provide the benefits of immediate time-to-value and are always accessible from anywhere, this ubiquitous access and lack of control, creates new challenges for security operations team. SaaS applications creates a new attack surface that represents substantial risk to the company. To reduce the risk without slowing SaaS adoption, companies have to address two main challenges. How to easily and securely provision and deprovision users across multiple SaaS applications? Second, how to monitor user activities across multiple SaaS applications and be able to detect insider threat and automate incident management process? Beyond those challenges, some of the compliance mandates such as PCI DSS 3.2 mandates companies to store log data for an year. Non compliance with PCI can result in a large fines, company disrepute and in certain cases not allowed to process credit card transactions.

The Solution

The Sumo Logic integration for Okta simplifies and automates the incident management process for SaaS applications and cloud workloads. Okta provides user authentication and activity, SaaS application provisioning, and policy data to Sumo Logic which can then be correlated with the actual user activity within external SaaS applications to detect anomalous and malicious user behavior. This integration enables organizations to quickly detect insider threats and contain or stop the attack with a variety of automated responses including but not limited to disabling the user in Okta, creating security incidents within a ServiceDesk, or triggering an automation platform.

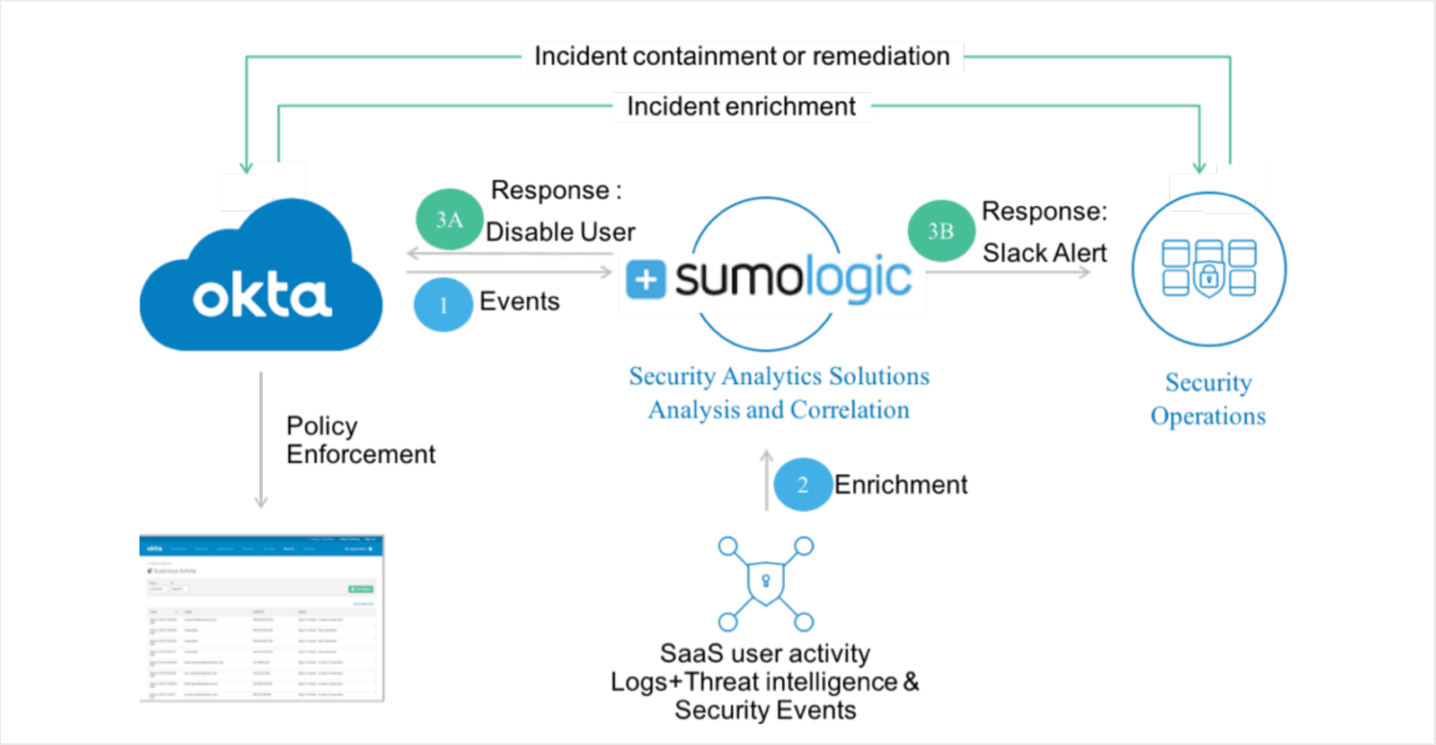
With this integration, customers can also discover long term trends from Okta, retain immutable logs for a year to satisfy PCI requirement 10. The Sumo Logic integration for Okta provides:

Benefits

Both CloudPassage Halo and Sumo Logic are delivered as SaaS applications, so they are on-demand, fast to deploy, fully automated, and work at any scale. Benefits of the joint integration include:

- **Insider threat detection**
  The first step from the attacker after exploiting the vulnerability is to steal employee's identity and move laterally in the organization. In that process, attacker's behavior will be considerably different from the regular user's behavior. It is critical that the entire incident response and management processes are automated for detection and containment of such attacks to minimize the potential damage or data leakage. The Okta and Sumo Logic integration provide better visibility and faster detection of insider threats, as Okta ensures that every user is uniquely identified across multiple SaaS applications. Sumo Logic can ingest authentication logs from Okta and be able to correlate with the user activities across multiple SaaS applications such as Salesforce, Box and Office 365. Sumo Logic with its advanced machine learning operators can detect outliers in the access pattern and can take variety of actions from opening the ServiceNow ticket to disabling the user in Okta. Correlations with automated response reduces the detection time and improves the response to quickly contain and eradicate the attacker before any data leakage.

- **Security visibility and insights**
  Okta combined with Sumo Logic provides visibility into top



Sumo Logic Dashboard for CloudPassage

applications, top users with failed authentication and users with deactivated multi-factor authentication (MFA). These checks are helpful for measuring basic hygiene for the security operations team.

- **Long term trends and compliance.**
  Log retention and immutability of logs are some of the core requirements of the most of the compliance mandates and regulations. For example, PCI DSS 3.2 requirement 10 specifically calls out 1 years of log retention (PCI DSS 10.7.a) and immutability of logs (PCI DSS 10.5.3). By sending Okta logs to Sumo Logic, organizations can easily implement longer retention policies and also be able to chart long term trends. Sumo Logic logs cannot be changed as public key cryptography ensure that logs are not altered and are encrypted.

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security protections. It integrates directly with an organization’s existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. Thousands of customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International and Western Union, trust Okta to help their organizations work faster, boost revenue, and stay secure.

About Sumo Logic

Sumo Logic is the leading cloud-native, machine data analytics platform that delivers continuous intelligence across the entire application lifecycle and stack. More than 1,500 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.