SailPoint and Splunk
An Integrated Approach to Identity Governance Monitoring and Auditing

In a world where digital transformation is evident, and traditional security does not cover all the bases, identity has never been more strategically important. Security Information Event Management tools (SIEM) are excellent in the detection and reporting of threats, vulnerabilities, and security events. Without the proper management and identification of compromised users or analytics of identity data, enterprises are at risk of a security breach. By combining these digital forensic tools with SailPoint's Identity Governance capabilities, enterprises can augment their identification and management of compromised users while lowering their risk of a security breach.

60% of digital businesses will suffer a major service interruption, according to Gartner, because their IT security teams will not know how to deal with one or more of the sophisticated cyber-threats related to identity.

The integration of identity governance, identity data, and context can provide SIEM solutions with the intelligence needed to make better, more informed security decisions and provide increased accuracy and precision with actionable results.

Using SailPoint Predictive Identity™ fine-grained visibility and control helps organizations more quickly identify risks, spot compliance issues, and make the right decisions to strengthen controls.

The combination of SailPoint, the leader in identity governance, and Splunk®, the enterprise Security Information and Event Management (SIEM) technology leader, provides a best in class integrated identity governance, monitoring, and auditing solution. The integration of SailPoint and Splunk enables enterprises to automate identity governance tasks with SIEM alerts and provides Splunk with an enhanced identity context.

By integrating SailPoint and Splunk, you can initiate identity, application, or entitlement-based certifications, automatically disable or remove access from identities, and even disable or remove access from identities without additional approval steps, allowing for automation of identity task.

- Enable more precise security analytics with identity context
- Consume security context to make identity policies more security-aware
- Automate workflows and or automate tasks in SailPoint in response to SIEM alerts
- Report and prioritize on non-governed application usage and access

How does the integration work?
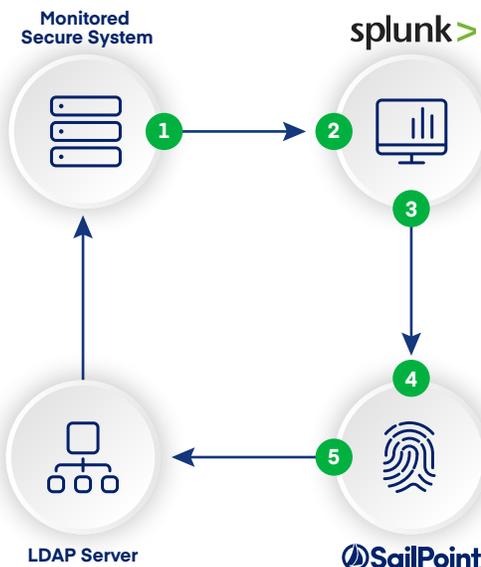
1. An out of band change occurs identifying a potential threat

2. The change detected and analyzed by Splunk

3. Splunk creates alert and sends to SailPoint

4. SailPoint analyzes alert from Splunk.

5. Action is then taken to certify, disable/remove access; all tracked for audit purposes.

Benefits of SailPoint and Splunk:

By combining the power of SailPoint Identity Governance and Splunk SIEM, you can gain the following benefits:

- **Context:** Enhance detection and investigation of potential threats and risky behavior. Leverage identity information with behavioral analysis to validate compromised/ rogue users.

- **Monitoring:** Integrate SailPoint system logs and audit events into the Splunk platform. Pre-built dashboards are available to provide Splunk administrators with an at-a-glance view into the health of the SailPoint deployment.

- **Productivity:** Significantly reduce noise for Security Operation Center analysts to focus on the highest value tasks. Gain insight through a centralized view of all access.

- **Automation:** Leverage Splunk to utilize enforcement and account automation capabilities of SailPoint.

Summary

Combining SailPoint and Splunk gives enterprises more precise security analytics through identity awareness and more elegant security enforcement with governance access controls. With stronger visibility, organizations are now able to mitigate risk derived from related cyber-security threats. Utilizing this integration gives enterprises active governance capabilities to mitigate risk and to continuously stay on top of their users and data.