Splunk Consulting Services

Splunk, www.splunk.com, is a leading platform for real-time operational intelligence. The application provides an easy, fast, and secure way to search, analyze, and visualize massive streams of machine data (i.e., big data). Sierra-Cedar is a Splunk partner. We are also a customer: Splunk is Sierra-Cedar's de facto SIEM application, and our security team utilizes the application for real-time security analytics.

Splunk's engine allows for easy searching and visualization of a vast array of machine data ranging from log files of application processes to streams of data from network devices. Splunk delivers powerful operational intelligence by providing real-time insight into the machine data collected in your information systems (whether onsite or in "the Cloud") through dashboards, charts, reports, and alerts. And it can collect and index information without connectors, databases, or limits.

With Spunk's access to so much raw (or big) data and the ability to translate and present it in meaningful ways, robust use cases are rapidly evolving—spanning industries as well as functional, compliance, security, and auditing domains.

Maturity Model

Organizations often acquire Splunk for its ability to be used as a **Search and Investigate** tool. These initial-use cases typically result in reduced escalations, reduced mean time to repair (MTTR), and reduced mean time to identification (MTTI). Following this initial success, organizations often choose to expand internal uses cases to include **Proactive Monitoring,** which often results in increased uptime and a further reduction in MTTR and MTTI incidents. The third rung in the use case maturity model is **Operational Visibility,** including monitoring key performance indicators (KPIs) and service level agreements (SLAs). At full maturity the model includes using Splunk for **Business Insights** and real-time behavior reporting.

Is Splunk a Good Fit for Your Organization?

Sierra-Cedar can help you decide. Our experienced consultants have worked with PeopleSoft clients to evaluate the use of Splunk for resolving audit findings related to application access, granting of application security, and failed login attempts.

Additionally, Sierra-Cedar has assisted organizations with mining data from existing PeopleSoft environments via Splunk to provide better insight and to provide detail for audit compliance into questions such as: Where do users log in from? Where are failed login attempts coming from? Where are users going within the PeopleSoft application? What changes are being made to application security?

Many organizations and institutions have similar compliance requirements. To answer these questions Sierra-Cedar is using different sources of machine data including default logging from PeopleSoft, database level auditing, and PeopleSoft Performance Monitor.

Sierra-Cedar is also exploring other ways for our clients to leverage Splunk to meet their PeopleSoft, auditing, and infrastructure needs.

Services

Whether an organization is new to Splunk or wants to elevate its use maturity, Sierra-Cedar can assist with the project. Our Splunk service offerings include the following:

- Assessment
- Installation
- Initial Configuration
- Report and Dashboard Creation
- Use Case Extension