splunk>

CASE STUDY

# Splunk® at Sierra-Cedar: Managing Operational Risk for Maximum Reward


## The Business

Sierra-Cedar provides consulting, technical and managed services for the deployment, management and optimization of enterprise applications and technology. Founded in 1981, the Atlanta, Georgia-based firm serves as a trusted advisor to clients in commercial, energy, healthcare, higher education and public sectors.

## Challenges

Increasingly, Sierra-Cedar is helping clients refocus their business resources on core profit-generating activities by providing complete outsourcing services for ERP and other major enterprise applications.

Managed services hosting operations at Sierra-Cedar supports upwards of 700 Oracle/PeopleSoft ERP environments with the accompanying 700 Oracle database instances. In addition, the firm supports multiple versions of each software suite. This large variety of configurations and environments made it difficult to implement and leverage conventional SIEM solutions.

"We discovered that it was almost impossible to get our Oracle/PeopleSoft logging data into a traditional SIEM and then parse and correlate that data," notes Dan Frye, Sierra-Cedar associate vice president of corporate security. "Our SIEM did not provide us with any context—the who, what, where, when and why. If you ask a SIEM vendor to provide 30 different Oracle/PeopleSoft pattern files, they will say, 'Sure. We'll sell you the professional services to do it, but it will be a year-long engagement and cost you a couple hundred thousand dollars'."

## Enter Splunk

In 2009, Frye downloaded the free Splunk software trial and quickly discovered Splunk could be used to collect, index and harness unstructured security data from any source. He also learned that Sierra-Cedar's UNIX and networking groups were already using the Splunk trial version independently for more "traditional" IT operational uses.

Throughout 2010, the firm conducted proof of concept trials of leading SIEM solutions, as well as Splunk. The short list came down to RSA enVision, ArcSight, NitroSecurity and Splunk. "We looked at all of the deal breakers from our first experience with SIEM systems," Frye explains. "For example, our first SIEM assumed that everybody shares the same domain and therefore they designed the product to only support one set of authentication credentials. That's fine, but to support our varied list of clients we have multiple domains with different requirements in each."

### Industry

- Managed Services Provider and ERP

### Splunk Use Cases

- Security Intelligence
- Operational Intelligence
- Compliance Management
- Reporting and Analysis
- Asset Discovery

### Business Impact

- Saving $200,000+ in SIEM consulting and custom connector development services
- Avoiding $20,000+ in vulnerability management system licensing costs
- Converging operational and security data to provide continuous real-time views of the environment
- Avoiding ongoing costs and inflexibility of appliance-based SIEM solutions
- Reducing frequency and duration of downtime

### Data Sources

- Application logs: PeopleSoft, EBS, Exchange, SharePoint
- Database logs: Oracle
- Security data: Nessus, Secunia, OSSEC, Identity Finder, Blue Coat, Cisco, Juniper
- System logs: Linux/UNIX syslog, Windows, Solaris

### Splunk Products

- Splunk Enterprise

Says Frye, "The degree of flexibility we get with Splunk Enterprise is what really drove us toward choosing them as our solution. It gives us the ability to make Splunk into what we needed, rather than us having to adapt to a limited set of rules with very little ability to build upon them."

## Breakthroughs

### Operational risk management

Sierra-Cedar deployed Splunk Enterprise and the Splunk App for Enterprise Security, which adds traditional SIEM functionality to monitor for traditional known threats identified from security data sources, as well as the capabilities to identify unknown threats and perform comprehensive security investigations.

"We chose Splunk, in part, because it wasn't a traditional SIEM," Frye observes. "Yes, the Splunk App for Enterprise Security adds SIEM-like features, but in combination with Splunk Enterprise, it becomes a far more powerful and flexible environment."

Splunk is now Sierra-Cedar's central monitoring, alerting and reporting solution. "For vulnerability analysis, we pump in most of our vulnerability data and intrusion detection information then run custom searches on that data to correlate matching data points. This is allowing us to hold off buying a much larger vulnerability management system, saving tens of thousands of dollars," said Frye.

### Real-time threat analysis

Sierra-Cedar relies on Splunk software and the Enterprise Security app to proactively monitor large amounts of user activity in real time to identify abnormal behavior patterns.

In one case, students accessing the PeopleSoft campus registration module wrote a script that would repeatedly attempt to sign up for classes that were full—to automatically register if any new openings appeared. This resulted in thousands of concurrent connections.

---

**"Until we found Splunk, there hasn't been a tool that was flexible enough to allow us to develop our own level of technology to address our unique requirements. We tried a traditional SIEM system and it didn't work for us."**

**Dan Frye**
**Associate Vice President, Corporate Security, Sierra-Cedar, Inc.**

Sierra-Cedar used Splunk to set up an alert to identify when concurrent connections were occurring on the same user ID and same IP address and performance started to decrease past a certain threshold. The alert goes in real time to administrators on the help desk and they kill the sessions. It's very quick and prevents downtime in major campus applications.

### Asset discovery

With thousands of servers, network switches, multiple operating systems and complex application suites running in its environment, Sierra-Cedar needed a way to identify and monitor its information assets.

Sierra-Cedar downloaded the free Splunk Asset Discovery app from Splunkbase.com and uses it in conjunction with the open source NMAP security scanner to port scan network assets. The firm uses Splunk Asset Discovery to alert it to any new ports that open in its firewalls, which is then used to validate its network changes and ensure proper change control procedures are followed.

### Compliance management

Sierra-Cedar must meet the compliance needs of its clients, be it SOX, PCI or other mandates. Splunk is helping the firm achieve this with role-based access and automatic encryption of sensitive data. Splunk is also making it easier for the company to retain logs and audit trails for as long as necessary—and enable searches as required. In addition, the ability to save only the required logs saves the firm disk space costs.

### Custom dashboards

With the Splunk App for Enterprise Security, any search result can be incorporated into a dashboard or table. To enforce compliance with corporate security policies relating to mobile device use, the Sierra-Cedar security team is pulling data from Secunia's PSI and CSI products and other scanning systems and compiling a management dashboard in Splunk.

"Splunk is helping us converge security and operational data to provide a continuous, accurate and real-time view of our environment," Frye concludes. "Splunk is an awesome tool that is helping the security team manage its own IT resources and, increasingly, used for more operational use cases as well."