

DETECTING INSIDER THREATS

How Splunk Software is Used to Safeguard Financial Data

Use Cases

- Fortifying Internal Security
- Streamlining Internal Processes

Executive Summary

Financial institutions increasingly rely on outside contractors to program and maintain applications, manage projects, and perform analyses and assessments. Unfortunately, whether intentionally or not, these contract employees can pose a serious insider threat. How can organizations effectively monitor contract employees to detect potential security breaches before they can impact the confidentiality of customers' data?

The security teams at a major North American bank struggled with just this issue. Application developers approaching the end of their contracts were data flight risks and threatened the bank's intellectual property. Monitoring the activities of all these contractors using commercial tools, however, was far too costly and resource intensive. The bank also had no way to correlate data from its various monitoring tools to assign risk levels to contractors and it lacked an automated methodology to respond quickly to risky behavior.

To resolve these challenges, the bank turned to Splunk® Enterprise. The software rapidly integrated data from the bank's various monitoring systems to provide graphical, holistic views of its threat assessment environment. With this insight, the financial institution assigned risk levels to contract employees based on their roles at the bank and the expiration of their contracts. When a risk level is exceeded, the Splunk platform issues alerts and enables the security team to take timely and appropriate actions.

With the Splunk software capturing and displaying all relevant security data, the bank cost-effectively monitors its contract employees and safeguards its assets from both intentional and inadvertent wrongdoing.

- **Integrate disparate data sources into holistic views.** The bank's monitoring systems provided data about risky sites and malware and tracked which websites contractors visited, but these solutions were compartmentalized. Piecing together a threat matrix was far too manual and time consuming. The Splunk platform collects, indexes, and visualizes these unstructured data streams, offering managers coherent views of such questionable behaviors as improper site visits or downloads.
- **Identify high-risk behavior.** Managers were unable to correlate multiple data sources that contained indicators of high-risk behaviors with employee role data to identify which contract workers posed legitimate security risks. Deploying more granular monitoring tools was prohibitively expensive. Splunk software correlates threat data with contractors' role data to identify workers more likely to pose hazards to the bank.
- **Automated targeted responses.** The bank's costly monitoring tools were unable to automatically target contract employees who exceed predefined

Business Benefits at a Glance

Challenges	How Value Is Measured	Business Impact
Needed to correlate multiple data sources to identify high-risk behaviors by employees and contractors	<ul style="list-style-type: none"> • Elimination of data silos • Integrated, holistic views of data from multiple tools 	<ul style="list-style-type: none"> • Critical bank source code and data are protected • Visibility into potentially damaging employee behavior
Wanted trigger alerts on individuals with high-risk behaviors	<ul style="list-style-type: none"> • Flexibly align high-risk activities with security policies 	<ul style="list-style-type: none"> • Proactive enforcement of security policies
Needed to deploy more focused monitoring or loss prevention measures	<ul style="list-style-type: none"> • Rapid response to identified risks 	<ul style="list-style-type: none"> • Intellectual assets and financial data safeguarded from temporary employees • Reduced cost of monitoring

risk ratings and pose a security threat. The Splunk platform coheres all threat and employee data, so when workers exceed risk ratings, alerts notify managers of potential breaches and restrictive actions are triggered to defuse the threat. The bank preserves its security cost-effectively and neutralizes potential threats presented by employees identified as “high-risk.”

Data Flight: Much More Than a Financial Concern

Banks run on money and software. They require hundreds, sometimes thousands, of contract application developers, project managers, systems analysts and other technical staff to deliver functionality to customers across all banking services. In addition, banks must adhere to stringent security mandates to safeguard highly confidential financial data. Yet, in spite of considerable security measures, the threat of data flight is significant and difficult to proactively identify. As contractors approach the end of their terms, they typically attempt three things:

- Securing their next contract
- Obtaining a copy of the source code that they’ve written for their portfolios and subsequent jobs
- Getting enough sample data to exercise that code

Unfortunately, these activities can result in significant financial and legal impacts for any employer, but particularly for financial institutions. While employees’ motives for copying source code, process information or data might not be ill-intentioned, their actions can place the enterprise in peril and be in violation of multiple federal laws.

Moreover, temporary employees often spend company time searching for their next contracts, at the expense of their current work and productivity. Additionally, contractors who download code can inadvertently introduce malware to the corporate network. While the great majority of contract employees are trustworthy, it only takes one to cause significant illegal, financial and publicized problems.

This major bank confronted these challenges as contract employees’ termination dates neared. Although lost

productivity from contractors seeking new assignments was problematic, the bank’s chief concern was data exfiltration. Many contractors had access to application source code that revealed how the bank’s underwriting and loan applications systems worked. Such knowledge, if leaked to competitors or identity thieves, could cause severe financial losses and damage the bank’s reputation.

The financial institution maintained a robust security posture, but it was vulnerable to these internal threats. It required a way to identify potentially risky employee behavior and respond automatically with appropriate measures, such as deploying more granular monitoring tools.

How to Extract Value From Available Data?

The bank considered available solutions, including a leading security information and event management (SIEM) solution that proved unable to scale effectively to the institution’s needs. However, the information needed to identify potentially risky behavior was already available in the bank’s existing machine-generated data. The data simply needed to be integrated for a complete picture. There were, however, substantial challenges:

- **The data needed to identify high-risk behaviors was spread across multiple systems.** Microsoft® Active Directory provided detailed information about each employee’s business roles and contract terms. BlueCoat listed potentially risky websites, recorded when and which contract employee visited them, and even identified specific job listings accessed by the contractor. FireEye provided threat intelligence about malware and questionable sites. While these disparate systems continually issued logs that tracked internal activities, unfortunately there was no system in place to cohere the data streams to draw timely conclusions.
- **Once risky behavior was identified, deploying more invasive tools to monitor or restrict the target employees was time-consuming and complex.** The bank was unable to automate this process with existing tools, so even if triggering behaviors were noticed, the bank took days to deploy the appropriate monitoring.

- **The bank could not efficiently and selectively monitor based on risk.** Deploying tools like keystroke monitoring to watch employees at a more granular level would have been extremely costly. The bank would need to monitor every contract employee constantly to determine whether any engaged in questionable behavior, which would incur substantial licensing costs. Moreover, keystroke monitoring would consume network resources like CPU cycles, slowing down computing performance across the enterprise.

Enter Splunk

Looking for a solution, the bank downloaded a copy of Splunk Enterprise and discovered that the software can capture and index unstructured, machine-generated data. Splunk Enterprise could monitor and analyze logs from disparate application servers at a scale that the bank required and their current SIEM could not deliver. The Splunk Search Processing Language (SPL) enabled the bank's security team to quickly query the data and graphically display the findings in dashboards in real time.

Since its deployment, Splunk Enterprise has allowed the bank to harness its existing data to proactively identify employees who warrant additional monitoring. The software correlates the data about user behaviors coming from BlueCoat with the FireEye information about potentially risky sites, and then ties it all together with employee information from Active Directory. This allows the bank

to define a risk rating and identify employees who surpass it. The risk rating takes into account employees' roles at the company and contract end dates from their Active Directory profiles. For example, employees working on multiple code projects (such as project managers) have access to more data than those working on single projects. Splunk software also can identify high risk behaviors such as data downloads, which might contain malware, as well as external website visits after working hours.

Using the correlated data, Splunk Enterprise triggers an alert whenever an employee exceeds a predefined risk rating. As part of the alert firing, Splunk Enterprise is configured to take action automatically based on the data. For example, depending on the severity of the alert, Splunk Enterprise can do one or more of the following: turn on keylogging, block or track USB storage devices, and/or send a warning email to the contractor's manager. Other actions include setting a flag in the user's profile that blocks access to such online storage services as Dropbox, Yahoo! email, Amazon S3 or iCloud.

To Catch a Potential Data Thief

How does Splunk software perform the analysis? Data indexed from the BlueCoat Proxy can be searched (and alerted on) for suspicious activity. Figure 1 shows a contractor visiting sites such as dice.com and monster.com to search for "Big Data Hadoop Engineer jobs" during working hours.

```
2013-08-30 11:20:18 172.16.200.9 SG-SSL-Proxy-Service shaun 172.16.210.74 www.dice.com
74.115.248.15

443 http://www.dice.com/job/results?caller=basic&q=big+data&x=all&p= "Job_Search/Careers" 200
text/html "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:6.0) Gecko/20100101 Firefox/6.0" www.
dice.com 986 494 TUNNELED OBSERVED ICAP_NOT_SCANNED -

2013-08-30 11:20:18 172.16.200.9 SG-SSL-Proxy-Service shaun 172.16.210.74 www.dice.com
74.115.248.15

443 http://www.dice.com/job/result/10451979/268944?src=19&q=big%20data "Job_Search/Careers" 200
text/html "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:6.0) Gecko/20100101 Firefox/6.0" www.
dice.com 986 494 TUNNELED OBSERVED ICAP_NOT_SCANNED -

2013-09-02 15:10:45 172.16.200.9 SG-SSL-Proxy-Service greg 172.16.211.32 jobsearch.monster.com
208.71.195.72 443 http://jobsearch.monster.com/search/?q=big-data "Job_Search/Careers" 200 text/
html Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14) - 961 1516 TUNNELED OBSERVED
ICAP_NOT_SCANNED -

2013-09-02 15:10:45 172.16.200.9 SG-SSL-Proxy-Service greg 172.16.211.32 jobsearch.monster.com
208.71.195.72 443 http://jobview.monster.com/Big-Data-Hadoop-Engineer-Job-San-Jose-CA-124644251.
aspx "Job_Search/Careers" 200 text/xml;%20charset=utf-8 "Mozilla/5.0 (Windows; U; Windows NT
5.1; en-US; rv:1.8.1.14) - 961 1516 TUNNELED OBSERVED ICAP_NOT_SCANNED -
```

Figure 1. Data reveals a contractor searching for jobs on external sites.

To identify contractors who may warrant more monitoring, the bank's security team crafted Splunk searches like the one in *Figure 2*.

This search examines BlueCoat data to identify contractors accessing job search sites over a 24-hour period and displays the search terms used broken down by

```
Index="bluecoat" cs_host="*.dice.com" OR cs_host="jobsearch.monster.com" cs_username=* | rex "(FREE_TEXT|q)=(?<"Search-String">["\w\+\(\)\%\'\.\"]+)" | stats count by SearchString, cs_host, cs_username | rename cs_host AS "Web Site" cs_username AS "User Name" | sort _time
```

Figure 2. A Splunk search to help identify high-risk contractors.

contractor name and site, as shown in the bottom panel of *Figure 3*. Splunk's **rex** search command automatically extracts the search term (in this case, the type of jobs the person is searching). *Figure 3*'s top panel displays when the searches were made over this 24-hour period.

Results from this search are then enhanced with FireEye data and used to drive the automated deployment of additional monitoring to contractors with "risk rating" values above the defined level. In addition to

this example, the bank has over 200 other types of data collected from 11 other applications by over 3,000 Splunk forwarders linked to application servers and web devices. This information feeds close to 200 security dashboards and reports, which are images of static dashboards sent by email or PDF.

Clamping Down on Internal Threats

While companies typically invest heavily in technologies that protect them from external security threats, internal breaches are often the harder challenge. This problem is exacerbated when numerous temporary contractors are working on key projects and have access to sensitive systems and data. Individual device-level monitoring can be expensive, foster an atmosphere of distrust, and may be ineffective because they capture only a single facet of risky behavior, such as keystrokes. Companies need to leverage data sources from all IT systems and applications. Correlating across these data sources can provide insights to risky behavior that prefaces security breaches.

Splunk software analyzes and correlates data and helps customers understand the behavior of internal users. Specifically, the Splunk solution allowed this particular bank to engage in proactive enforcement of its security policies to protect its intellectual assets and potentially avoid multi-million dollar fines.

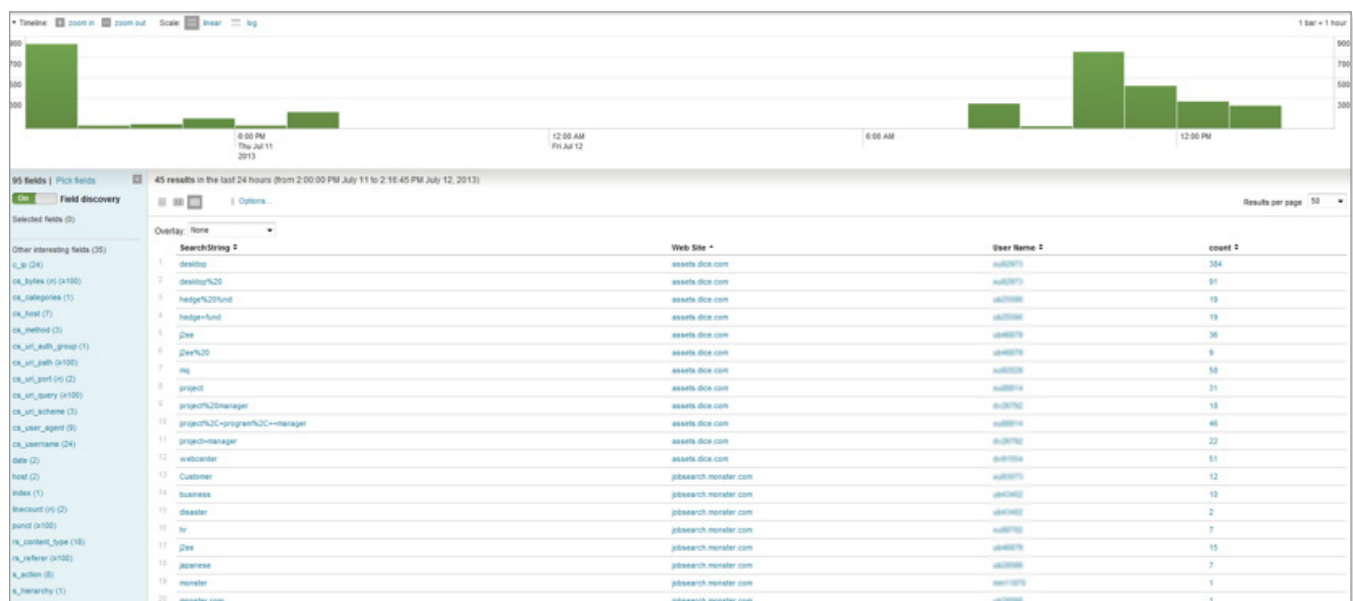


Figure 3. Contractors accessing job search sites over 24 hours (bottom) and the times when the searches were conducted (top).

With Splunk, They Are Safe and Secure

Enterprise data can reveal much to a business. This use case demonstrates how machine-generated data provides the knowledge to ensure the internal security of a financial institution. What is essential, however, is that data produced by many disparate systems is captured, integrated, and displayed. This use case demonstrated:

- **Elimination of data silos.** Because Splunk software indexes all kinds of data, the customer's siloed data no longer hinders its ability to obtain coherent views of potential security problems.
- **Correlations can bolster security.** Because Splunk software correlates different types of data, the customer links messages in the logs of multiple systems into useful evidence for potential issues.
- **Flexible analytics powered by a read-time schema.** Because Splunk Enterprise collects data in full fidelity without any filtering, the customer does not lose any potential value by making its data fit in a schema. The customer can engage in near real-time analysis of questionable employee behavior.
- **Significantly reduced manual intervention and labor cost.** Because the Splunk platform provides real-time visibility of online actions and can trigger alerts when thresholds are exceeded, appropriate responses are automated, providing very rapid measures to curb unwanted actions.

About Splunk

Splunk Inc. (NASDAQ: SPLK) is the pioneer in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk provides the enterprise machine data fabric that drives digital transformation. More than 12,000 customers in over 110 countries use Splunk in the cloud and on-premises. Join millions of passionate users by trying a [free trial of Splunk](#).