splunk>

CASE STUDY

Splunk® at a Global Retailer

Detecting Online Fraud With Visibility and Insight

"Our Splunk solution proves over and over that operational intelligence can combat malicious exploits like fraud on e-commerce sites. Fraudsters and cybercriminals may be getting savvier, but with the analytics enabled by our Splunk software, so are we."

Lead Application Security Engineer
Leading global retailer

OVERVIEW

INDUSTRY
- Retail / e-commerce

SPLUNK USE CASES
- Fraud investigation
- Fraud detection and prevention
- IT security
- Application management
- IT operations

BUSINESS IMPACT
- Reduced financial losses from fraud and chargebacks
- Reduced labor costs from fraud investigations
- Real-time detection of fraud and cyberattacks
- Reduced security vulnerabilities and an improved security posture

DATA SOURCES
- RSA Silver Tail
- Accertify
- Fox IT threat intelligence feed
- Firewalls
- Akamai Web Application Firewall and content delivery network
- OSSEC
- Riverbed Cascade network monitoring
- Custom tools and applications

The Business

This American department store chain operates globally and sells clothing, tools, appliances, automotive supplies and more. It sells via brick and mortar stores, mail-order catalogs and, more recently, online.

Challenges

With an online business featuring over 100 websites, the retailer faced online fraud ranging from customer account takeovers to abuse of new account activation incentives. The retailer's security team was tasked with supporting the company's online anti-fraud efforts. It had deployed a variety of tools to defend the enterprise, but was unable to aggregate, correlate and reveal data quickly from a myriad of systems and sources.

Of particular pain was the fraud investigation workflow process which involved multiple teams and a manual process of having to SSH into servers to gather relevant log files and then using grep, the command line utility, to search through the logs. The entire process was tedious, often requiring multiple people to work on the issue for over 90 minutes, which corresponded to 12 worker-hours. Worse, correlations across different log types was very difficult and sometimes log data was overwritten and thus lost, limiting investigations. Another issue facing the retailer was that fraudsters are relentlessly clever and devise new tactics that existing anti-fraud tools cannot detect.

To safeguard its global online business, the retailer required a single platform that could index all fraud and security-relevant machine data and more quickly present the information to the internal teams to identify, investigate and prevent fraud, as well as be useful for cybersecurity. The platform would also need to be flexible enough to quickly detect new fraud techniques.

Enter Splunk

The retailer considered traditional Security Information and Event Management (SIEM) products, but turned to Splunk Enterprise, which the firm's IT operations already deployed for operational and application management use cases. The retailer discovered that traditional SIEMs could not ingest the data sources it needed to index and were focused on rigid, fixed rules that would not catch creative fraudsters or cybercriminals.

The lead security engineer explains the decision: "Splunk Enterprise won because of its flexibility and ability to capture, index and visualize logs from any source. By pulling all of our logs into one tool through which we can easily search, we'd slash the time needed to investigate a suspect activity to just a few minutes."

Splunk Enterprise indexes machine data from sources like web fraud events from RSA Silver Tail, credit card fraud events from Accertify, firewalls, OSSEC intrusion detection and file integrity monitoring, custom tools and applications, and threat intelligence from Fox IT. The Splunk REST API is also used to integrate real-time data in Splunk Enterprise with a legacy portal used by all the security and loss prevention teams.

Breakthroughs

Rapidly investigate and detect fraud

With Splunk software, all relevant machine data from the retailer's e-commerce business is now in a single location for fast searching, correlations and reporting; no more tedious

use of SSH and grep to obtain and search logs. Teams can quickly research alerts by entering data like a suspicious IP address on the security portal and then having the Splunk solution show all the behavior associated with that address. Investigations now can be completed as rapidly as five to ten minutes or less—just 0.2 worker-hours—and are not hampered by missing log data. The result is substantially quicker identification and blocking of fraud before it undermines the bottom line or tarnishes the company's reputation, as well as reduced labor costs associated with fraud investigations.

Splunk Enterprise has proven particularly useful for large-scale fraud investigations, detecting fraud rings and advanced correlations. "We connect the dots faster with our Splunk system," explains the lead security engineer. "For example, we might see a transaction with an overseas IP address, a shipping address in New York and a billing address in California. We'll then immediately alert our fraud team."

With Splunk Enterprise, the retailer can also automate lookups against all the IPs connecting to their websites to quickly spot possible site traffic related to fraud. All IP addresses in Splunk Enterprise are crosschecked against both a list of known bad IPs from Fox IT as well as a custom blacklist of IPs previously involved in fraud against the retailer.

Splunk has also proven helpful in identifying fraudsters trying to hide their true location. By indexing log data from its Akamai content delivery network, the retailer can spot the true, originating IP address of visitors. With this, it has identified overseas fraudsters who used proxies with U.S. IP addresses to appear as though they were domestic users.

Prevent customer account takeovers and safeguard incentive programs

Splunk can also help identify account takeovers where a fraudster has obtained the online store credentials of legitimate customers via phishing or malware with the intent of accessing these accounts for nefarious purposes. The retailer can spot these account takeovers by looking for patterns such as a single IP or URL referrer string accessing an excessive number of customer accounts, or a single IP address attempting to log in using hundreds of different credentials.

Loyalty programs that offer financial incentives or redeemable points are a frequent target for e-commerce abuse. Using Splunk, administrators are able to detect fraudulent attempts to open and exploit multiple accounts with the sole intent of obtaining "account opening" financial incentives. For example, they determined that thousands of loyalty accounts had originated from one IP address and were opened by an automated bot.

Enterprise-wide integration and view into fraud

The security and loss prevention teams now have additional context and data integrated into their legacy portal for fraud investigations that can be shared by multiple teams. Splunk Enterprise also provides consolidated fraud reporting across multiple fraud tools to help break down the data silos that typically exist between point tools to show a broader, enterprise-wide view of fraud. Splunk dashboards show trending of fraud events, critical alerts from other fraud tools and spikes in alerts.

A single platform for fraud and IT security

The retailer is of the mindset that IT security and online fraud are related, so its security team handles both functions. Efficiencies are gained by using Splunk software because the machine data in Splunk is used for both IT security and anti-fraud use cases. The security team uses Splunk software to detect and defeat cyberattackers attempting to break into the network to compromise customer information, which can lead to downstream fraud.

Item#CS-Splunk-AnonRetailFraud-105