splunk> turn data into doing™

CASE STUDY

Fortune 100 Financial Institution Improves Detection and Investigative Capabilities With Risk-Based Alerting

Key Challenges

The volume of alerts generated at this premier financial institution required analysts to spend most of their time triaging alerts, consuming nearly all the organization's analyst resources.

Key Results

With Splunk, this financial services organization significantly decreased alert volume while increasing true positive rates and operationalizing MITRE ATT&CK.

Industry: Financial Services

Solutions: Security & Fraud, Enterprise Security

This Fortune 100 financial services organization, one of the largest banking institutions in the United States, knows a thing or two about managing risk responsibly.

Throughout the years, they have been early adopters of disruptive ideas — from launching online trading when the internet first emerged into the mainstream, to eliminating account fees for clients.

The security team at this multinational institution, responsible for safeguarding the company's security posture from unwanted intrusions, is always keeping an eye out for transformative technologies and processes to bolster their defenses. And at .conf18, they came across one topic that left a lasting impression: Risk-Based Alerting (RBA).

When the team returned home, they made the implementation of RBA their top priority. RBA augmented the organization's existing Splunk Enterprise Security solution to illustrate a different story: an attribution-based one. These seemingly subtle changes in mindset and processes empowered the team with a better way to collect pertinent security context and accelerate threat hunting.

It's Getting Loud in Here

Historically, Security Operations Centers (SOC) have been noisy places. The pursuit of the "perfect" correlation search intended to pinpoint the breach generates too many false positives and has not been an effective way to detect campaigns.

Data-Driven Outcomes

65%
reduction in alert volume

~2x
improvement in alert fidelity

Better
complex threat detection

"Out of 200 alerts in a day, only a fraction of those warrant further investigation, and most of them pertain to policy violations," says one of the organization's security engineers. The problem is, whenever a flood of alerts reaches the SOC today, security analysts have to sift through all of them and attempt to piece together what's happening. SOCs generally lack the mechanisms to efficiently decipher the story their data is trying to tell them. The team viewed RBA as an opportunity to improve upon widely accepted best practices within the SOC while improving their detections, investigations, and complex threat hunting.

Everyone Likes A Good Story

The relationship between security and the business could be more cohesive — and historically, language plays a big role in the disconnect. One of the early benefits of RBA for the team was how "Risk-Based Alerting allowed business and security to speak the same language," says the security engineer.

Security practitioners tend to speak in a highly technical manner that makes it challenging for most people outside the SOC to follow. Risk attributions, a central component of RBA, provide the common language needed to get the SOC and business on the same page. "Before, we were pivoting between a bunch of different places so the story got lost and overly technical," says the security engineer. "RBA centralizes all the risk attributions for a given user/object. We can now show teams outside the SOC how the various risky behaviors associated with a user/object weaves together into the security story."

> Many products check a box for business or compliance purposes, but don't really impact security operations. Risk-Based Alerting with Splunk Enterprise Security provides real security improvements while clearly demonstrating the value of security to the business."
>
> **Security Engineer,** Financial Institution

Using Frameworks as a Guide

Security analysts have disproportionately borne the brunt of alert fatigue. This has forced many analysts to adopt a security alert mindset that is singularly focused on triage-related activities. The attributions that drive notable events within RBA provide the context needed for security analysts to see the whole security story. Investigation-worthy attributions can be mapped against leading cybersecurity frameworks like MITRE ATT&CK, and analysts can now spend more time conducting security investigations into real threats. With the Splunk platform, the team at this premier institution has decreased its false positives while improving overall detection coverage.

Want to see how RBA can help enhance security operations at your organization? Watch this demo.

21-18016-Splunk-Tier2-Fortune100-FinServices-102-CS