Alert Fidelity Accelerator

Situation

SecOps teams are in a tough spot, trying to gain visibility across hybrid cloud and on-premises for both OT and IT environments, being flooded with overwhelming amounts of data from different business sources.

It's not just about chasing down every security hiccup, but reducing exposure and mitigating threats before they cause material damage.

Challenges

Rapid Technological Change Is Expanding the Attack Surface

Security teams are monitoring sprawling hybrid, cloud, and on-premises environment technology stacks that are often reliant on third-party applications and services.

This volume increases costs and even worse:

- Complexity – as it creates a larger attack surface
- Blurs visibility for defenders that can't detect what they can't see

Blind spots hinder rapid contextual understanding and the ability to detect, understand and resolve security incidents efficiently due to:

- Overwhelmed by data volume, alert storms, and manual tasks
- A shortage in security talent and skills is impacting the ability to find experienced staff

Implications

52%

of organizations report suffering a recent data breach

9

weeks is the average dwell time after a bad actor penetrates an organization's system - average MTTD is about 2.24 months

49%

of SOCs lack the staff to manually handle the increasing volume of security events

88%

of organizations report that they are experiencing talent challenges- costing them the ability to manage their security operations programs

Solutions

Alert Fidelity Accelerator

Unique to Splunk is a methodology called Risk-Based Alerting (RBA) which drastically reduces alert volumes.

RBA users see anywhere from a 50% to 90% reduction in alerts, with the remaining alerts being easier to investigate.

Splunk Alert Fidelity Accelerator is designed to jumpstart your ability to successfully deploy, adopt RBA to realize value faster.

Enhance the adoption and engagement to reduce the number of overall alerts while increasing the fidelity of alerts that do arise.

Successful Implementation of RBA Can Yield the Following Results

Significantly reduce alert volume

Greatly minimize false positives

Reduce mean time to detection (MTTD) / recovery (MTTR)

Splunk Enterprise Security capabilities enable you to realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency.

Key Benefits

- Leverage best practices to de-risk and optimize your environment
- Tap into our implementation experience so your team can stay focused on high-value initiatives to strengthen your security posture
- Accelerate results while building deep technical expertise on your team
- Drive the right outcomes with tailored roadmap guidance from Splunk experts

Alert Fidelity Accelerator Services Datasheet

Learn more

1 The Splunk Guide to Risk-Based Alerting