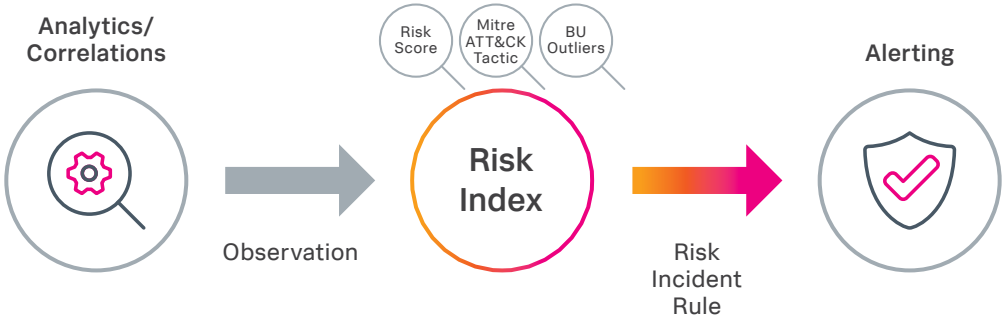
Embark on Your Risk-Based Alerting Journey With Splunk

Reduce alert volume and enhance security operations

Benefits

- **Improve detection** of sophisticated threats like low-and-slow attacks traditional SIEMs miss
- **Seamlessly align** to cyber security frameworks like MITRE ATT&CK, Kill Chain, CIS 20, and NIST
- **Scale analyst resources** to optimize SOC productivity and efficiency

How RBA Reduces Alert Volumes



Security Operations Centers (SOC) are incredibly noisy places. They experience tens of thousands of alerts daily and are constrained by limited resources. As a result, only the highest priority alerts are examined, and most are later determined to be false positives or are simply abandoned. Hoping to improve things, teams pour resources into "perfecting" their correlation searches, but doing so paradoxically creates even more noise. The other option isn't much better: teams inadvertently create blind spots in their security coverage through alert suppression, making it even more difficult to detect and investigate threats. There has to be a better way.

Splunk® Enterprise Security (ES) introduces new risk-based alerting functionality to SOC operations. This helps organizations address the elephant in the room: alert fatigue. Analysts create risk attributions for entities (e.g., users or systems) when something suspicious happens. Then, instead of triggering an alert, the attributions are sent to the risk index. Teams can enrich their risk attributions by appending relevant context, like annotating them against a relevant MITRE ATT&CK technique or applying a risk score. When an entity's risk score or behavioral pattern meets your predetermined threshold, then a notable event sets off, providing analysts with valuable context at the onset of their investigative process to expedite the neutralization of threats. The benefits of RBA extend well beyond these improvements.

A risk-based approach provides teams with a unique opportunity to pivot resources from traditionally reactive functions to proactive functions in the SOC. As alert fidelity and true positive rates increase, analysts' resources can be shifted to higher impact tasks like threat hunting or adversary simulation, empowering SOCs to build up the skill sets of their analysts and prepare them for any threats they might encounter in the wild. Let's create happier and more productive analysts by enabling them to conduct more security investigations.

Operationalize Cyber Security Frameworks

Splunk Enterprise Security provides out-of-the-box alignments to leading cybersecurity frameworks like MITRE ATT&CK, CIS 20, NIST Controls and more. By embedding the framework of your choice into your detections, your team can transform valuable security concepts into foundational cornerstones of your security operations. These frameworks form the base for proactive exercises like adversary simulation.

Also, teams can use their preferred framework to quantify gaps (e.g., which MITRE tactics detections are covering) in their security coverage and determine the additional data sources needed to enhance security.

Complex Threat Detection

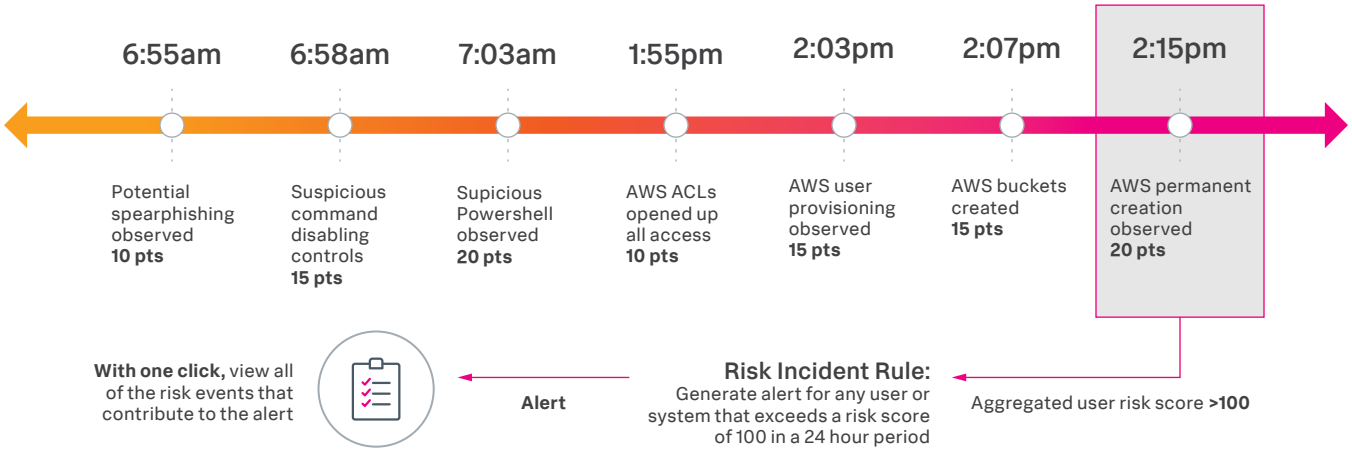
Historically, complex threat detection has posed a challenge for legacy SIEMs. The volume of disparate alerts makes it difficult to surface attacks like low-and-slow. It's hard to distinguish the generated traffic from normal traffic. Through building a comprehensive collection of attributions, it's easier to build detections spanning longer periods of time, making it very difficult for attackers to use low-and-slow tactics. For example, your team can configure alerts to fire when an entity's behavior spans three or more MITRE ATT&CK tactics over a two-week period, effectively expanding the coverage of your attack surface.

Streamline Investigation and Remediation

Splunk® Phantom's automation capabilities reduce time spent on security incident triage activities, and provide better context for the investigative process. SOCs can seamlessly share high fidelity notable events, including Indicators of Compromise (IOCs), from Splunk Enterprise Security to Splunk Phantom. Then, Phantom can automatically investigate all associated attributions simultaneously: IPs, domains, URLs, hashes, and more can be queued for automatic blocking. This ensures that risky devices or users present in your environment can be quarantined or disabled instantaneously, without the need for human interaction. This frees up time for your security team to focus on other high-value activities within the SOC.

How Does This Look in Practice?

With risk-based alerting, these events become context that informs high-fidelity alerts



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

21-16748-SPLK-EmbarkonYourRisk-BasedAlertingJourneyWithSplunk-108-SG