Risk-Based Alerting

Reduce alert volume and enhance security operations

Improve detection of sophisticated threats like low-and-slow attacks that traditional SIEMs miss

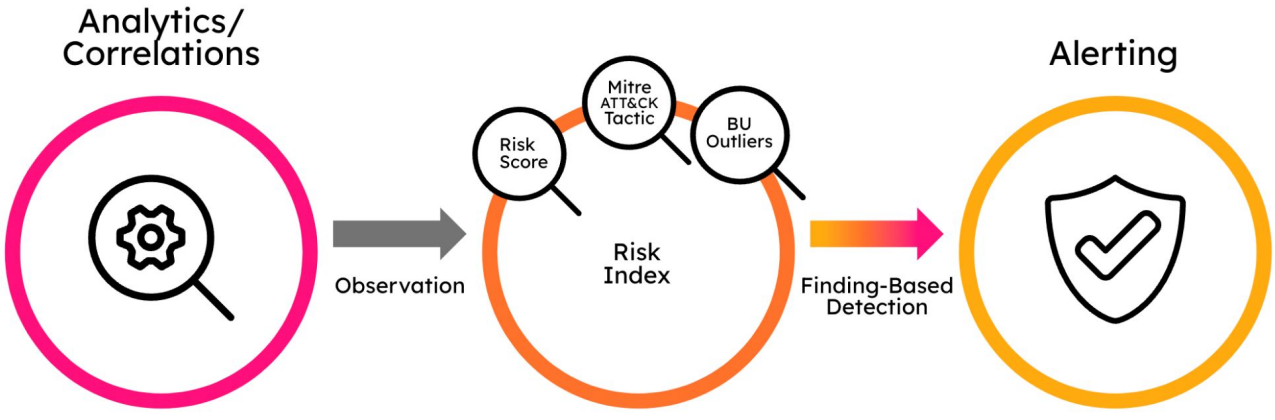
Seamlessly align to cybersecurity frameworks like MITRE ATT&CK, Kill Chain, CIS 20 and NIST

Scale analyst resources to optimize SOC productivity and efficiency

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 ignored. In hopes of remedying this, teams pour resources into perfecting their detections, 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.

As a feature of Splunk® Enterprise Security, risk-based alerting (RBA) drastically reduces alert volume, allowing users to increase their productivity with high-fidelity threat detection. Analysts create risk attributions for entities (e.g., users or systems) when something suspicious occurs. Instead of triggering an alert for each attribution, 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 their predetermined threshold, a finding gets triggered, providing analysts with valuable context at the onset of their investigative process to expedite the neutralization of threats.

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.



Operationalize cybersecurity 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. 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.

Address complex threat detection

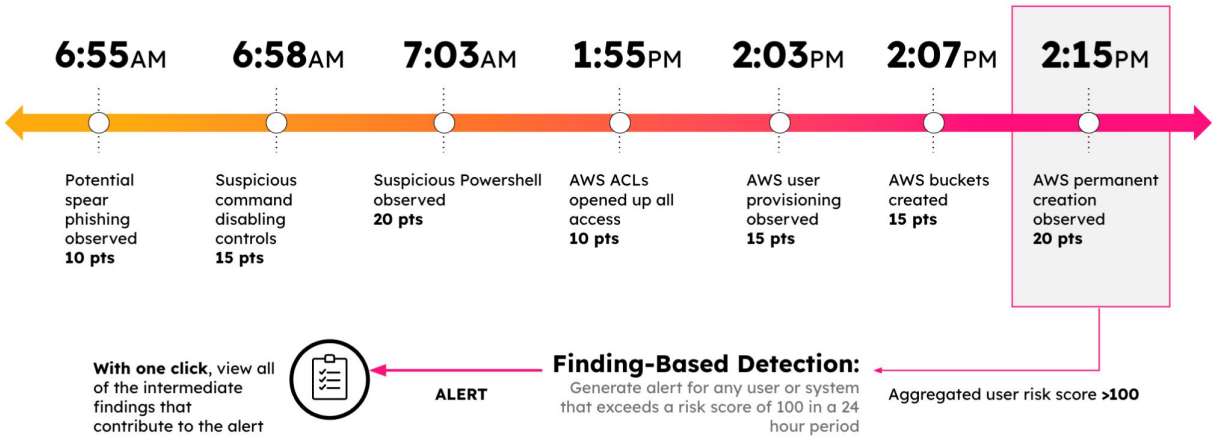
Historically, complex threat detection has posed a challenge for traditional SIEMs. The volume of disparate alerts makes it difficult to surface attacks like low-and-slow where it's hard to distinguish generated traffic from normal traffic. By building a comprehensive collection of attributions, it's easier to build detections spanning longer periods of time and detect anomalies, subtle attacker behavior, or insider threats. By expanding coverage and threading events together across your entire attack surface, you can detect far more elusive threats.

Streamline investigation and remediation

With Splunk® SOAR's* automation capabilities natively integrated in Splunk Enterprise Security, analysts reduce time spent on security incident triage activities, and provide better context for the investigative process. SOCs can seamlessly share high-fidelity findings, including indicators of compromise (IOCs), from Splunk Enterprise Security to Splunk SOAR. Splunk SOAR 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



*Splunk SOAR subscription required

splunk>

Contact us: splunk.com/asksales

splunk.com