Joint Solution

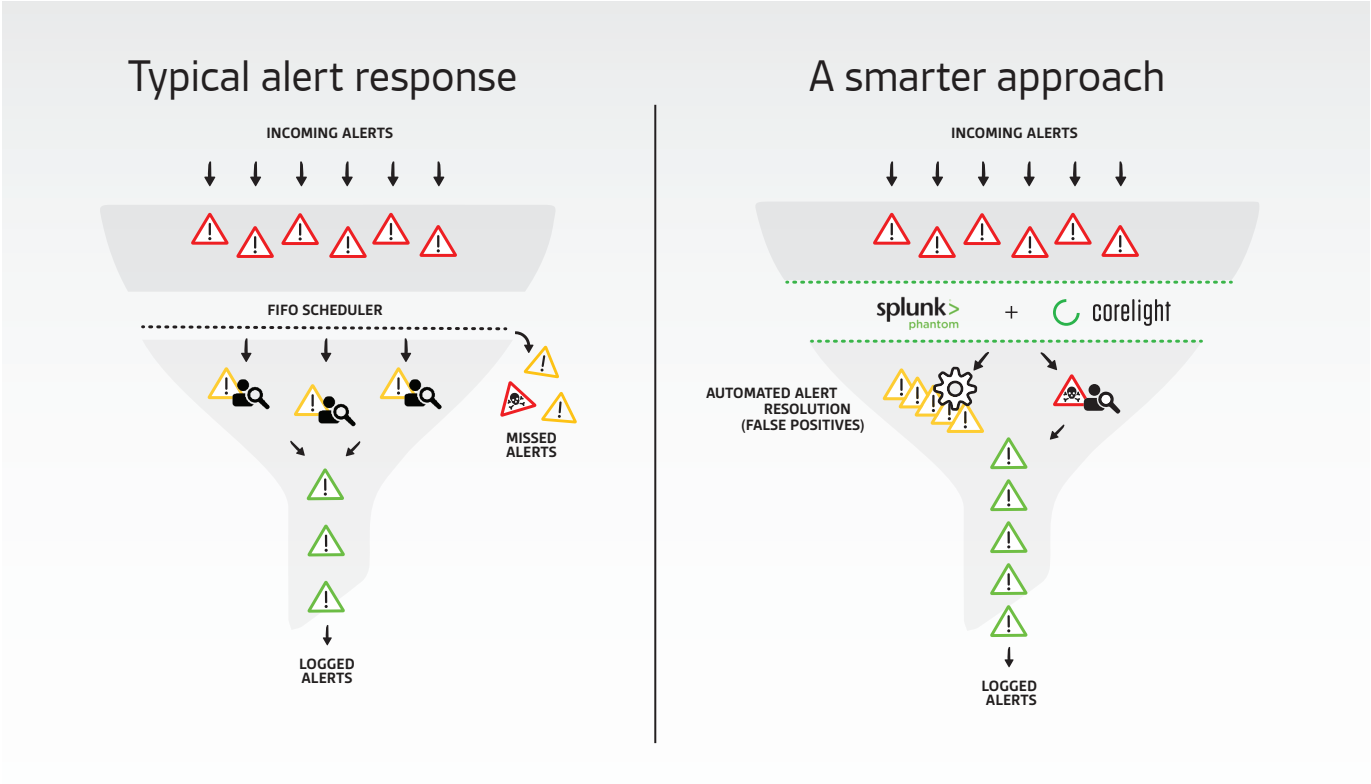
splunk> | corelight

Corelight SOC playbooks for Splunk® Phantom

The alert avalanche, solved.

Alert fatigue is one of the most widespread and broadly damaging problems in cybersecurity. It extracts an enormous toll in time and money when critical events are missed, or when the backlog grows impossibly large. What's more, alert fatigue impacts tier-one analysts, and the SOC team as a whole, by eroding morale and stifling advancement.

To solve this challenge, Corelight and Splunk® Phantom have created evidence-based playbooks by combining alerts, Zeek metadata, and tradecraft. The playbook automates and closes false positives, leaving behind only prioritized alerts. Analysts can then review these critical alerts in seconds while maintaining auditor-quality control. Together, Splunk's query language, Corelight's fusion of alert and context, and Phantom's automation framework can dramatically shift your SOC's efficiency and effectiveness.



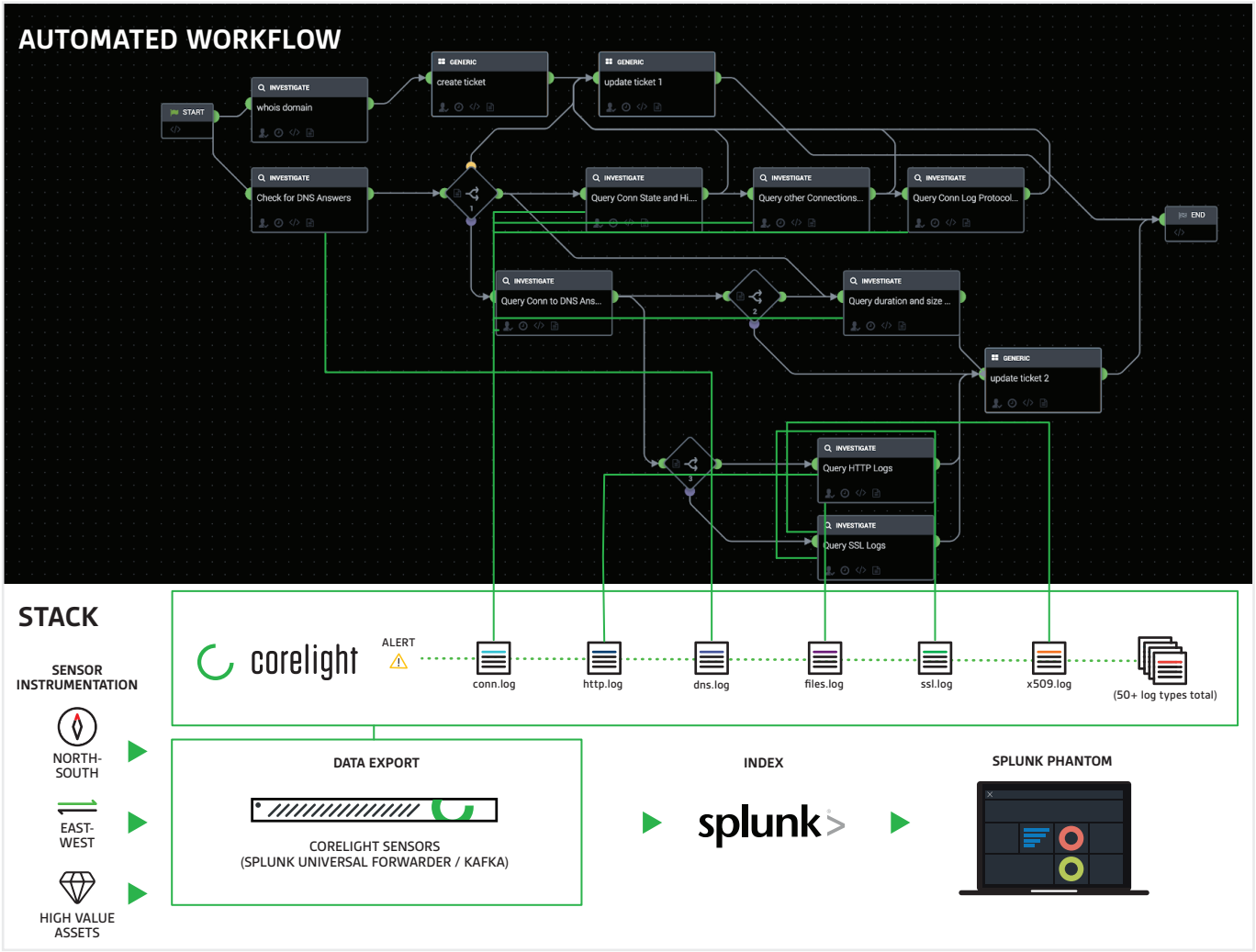
Focusing on real alerts means response is faster, cheaper, and free of drops.

Why Corelight + Splunk® Phantom

Proper instrumentation: The "right data" changes depending on location. At the ingress/egress point, integrated IDS fuses each alert with Zeek metadata, a pre-association crucial for later processing and disposition. For East-West traffic, correlating network services helps verify connections, enforcement, etc. All this is enabled by the field-proven Corelight sensor and Splunk's bulk data SKUs.

Tradecraft: Just getting the right data isn't enough; it takes experience and imagination to design a workflow that acts like an advanced practitioner. A quarter century of innovating alongside massive organizations gave Corelight experience with elite SOC teams. These playbooks reflect that knowledge—distilled and ready out-of-the-box.

Partnership: What makes this joint solution so powerful? First, it allows you to build your own tradecraft. Splunk, Corelight, and/or your staff can create and operationalize new playbooks, try them out, and improve or delete them as needed. Second, analysts already know the Splunk interface, so no 3rd party tool or UI (or training) is required.



info@corelight.com
888-547-9497
corelight.com