Intelligence Management for Splunk SOAR

Accelerated response through priority scoring

The Problem

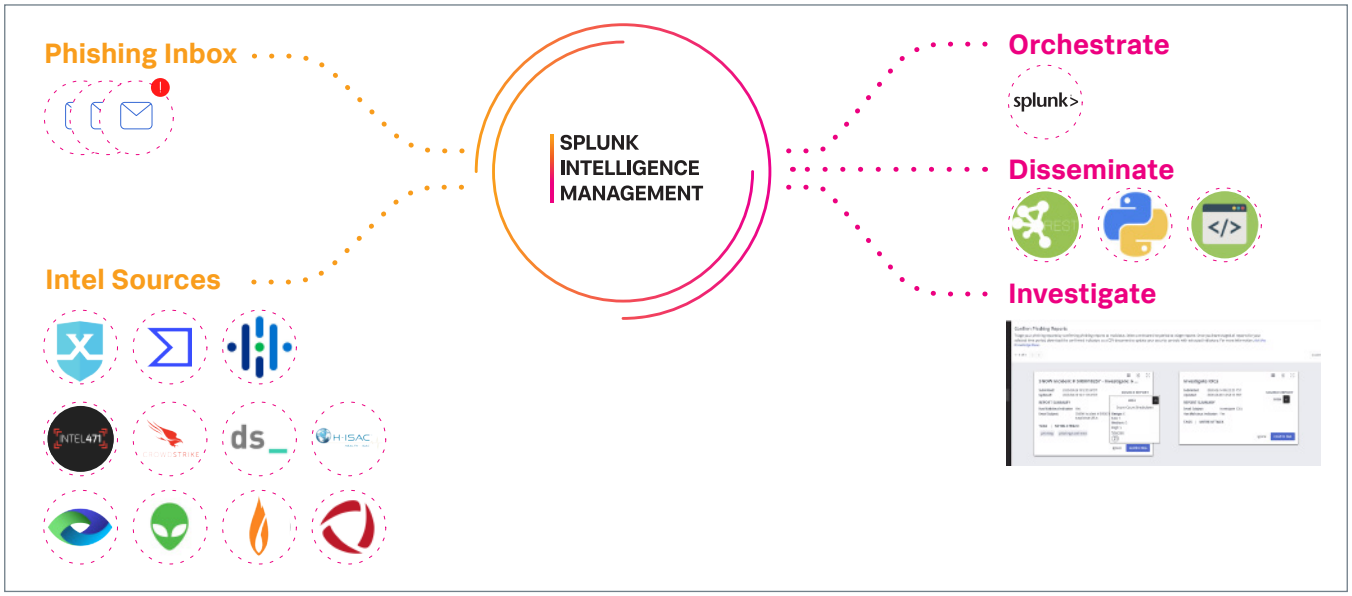
Analysts are burdened with an onslaught of security alerts, disparate data scoring and too many repetitive, manual security tasks. Phishing continues to be one of the most pervasive threats that organizations face and was present in 36% of breaches (compared to 25% last year). As a result, much of an analyst's time is spent manually reviewing and triaging phishing emails and other events, which takes time away from priority alerts and mission-critical objectives.

Splunk Intelligence Management for Splunk SOAR

Splunk SOAR automatically analyzes and responds to security use cases using automated playbooks. But Splunk SOAR playbooks become even more powerful with the addition of Splunk Intelligence Management (formerly TruSTAR). With Splunk Intelligence Management, you can take advantage of the following capabilities to bolster your automation and response within Splunk SOAR.

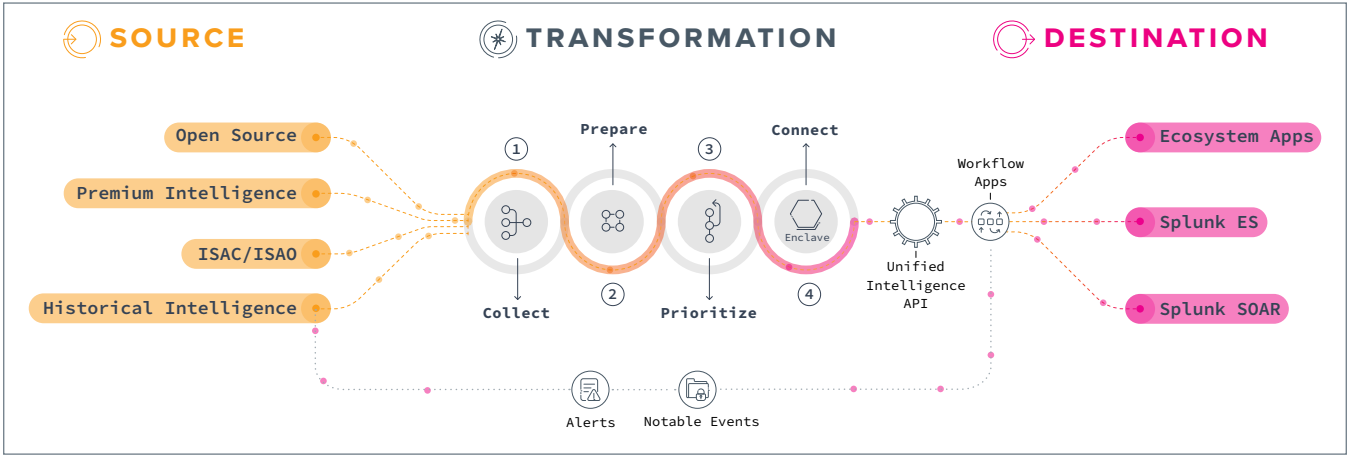
Enhanced phishing triage flows

Splunk Intelligence Management ingests user-reported suspicious emails, extracts observables and enriches them with open source, commercial intelligence feeds, and internal historical data. Splunk Intelligence Management then calculates a normalized score for each Indicator and applies a priority score to each email for automated or manual response within Splunk SOAR.



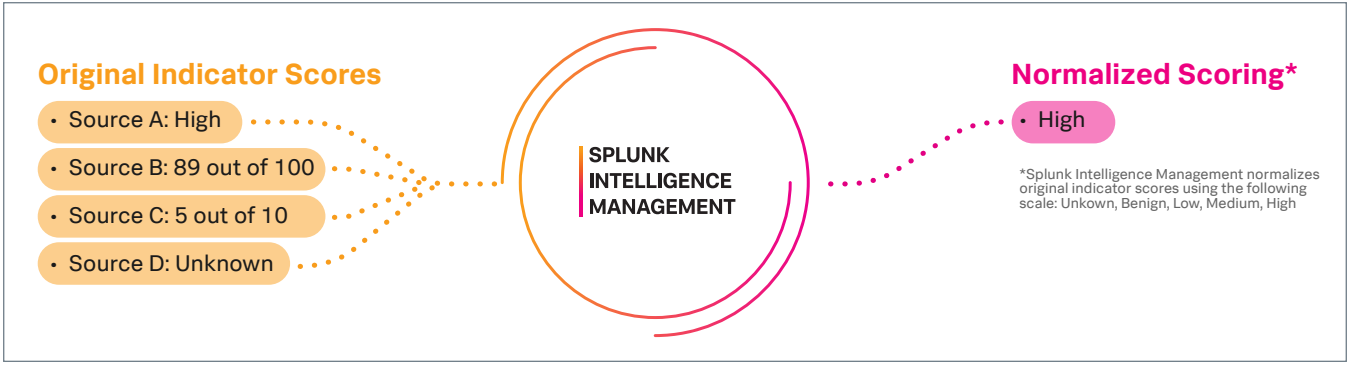
Investigation enrichment for rapid manual response

Splunk Intelligence Management enriches and scores indicators with open source, commercial intelligence feeds, and internal historical data to provide deeper context and intelligence. The Splunk SOAR Threat Investigate playbook natively incorporates Splunk Intelligence Management via the built-in TruSTAR Enrich Indicators playbook. Indicators are passed from Splunk SOAR to Splunk Intelligence Management for enrichment, which is then captured in the notes of a container. Within a single prompt, analysts can view indicator enrichment details and specify subsequent response actions directly in Splunk SOAR, eliminating the need to pivot between security tools.



Indicator enrichment and priority scoring for improved automated response

Splunk Intelligence Management integrates with a number of premium intelligence sources as well as open source feeds. Each of those sources calculates scores for events and indicators in their own unique way. Splunk Intelligence Management aggregates, normalizes, and prioritizes intelligence across all of your subscribed sources by applying an indicator priority score. Splunk SOAR playbooks can be simplified by calling Splunk Intelligence Management for indicator enrichment from all of your intelligence sources. Instead of having to build a playbook that aggregates intelligence from all of your intelligence sources separately, the aggregated priority score from Splunk Intelligence Management can be used to automate actions.



Feature Highlights

- Accelerate automation by setting up playbooks that utilize the context of Intelligence Reports and Indicators from Splunk Intelligence Management.
- Obtain prepared and normalized intelligence in a single action for faster triage and more streamlined playbooks.
- Inform phishing triage playbooks with priority event scores for faster response
- Use Indicator normalized score, attributes and properties aggregated by Splunk Intelligence Management for more accurate automated response triggers in Splunk SOAR.
- Send observables from Splunk SOAR to Splunk Intelligence Management whitelist and Splunk Intelligence Management will automatically remove them from your security information event management (SIEM) tool.

Outcomes

Simplified enrichment playbooks

By managing all of your intelligence sources and preparing your data in a single platform, Splunk Intelligence Management increases the fidelity and usability of Splunk SOAR automated playbooks. The comparison of Figure A and Figure B shows how Splunk SOAR playbooks can be streamlined with Splunk Intelligence Management by providing a single unified API for enrichment based on normalized intelligence.

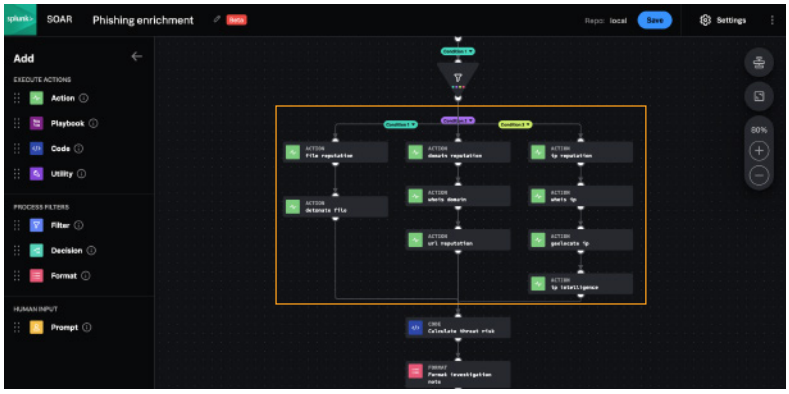


Figure A: Playbooks without TruSTAR.

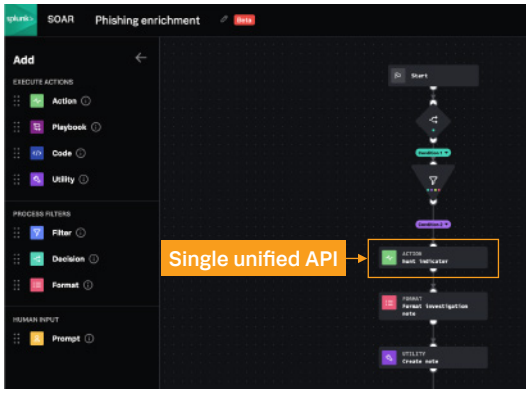


Figure B: Playbooks with TruSTAR.

Operationalized investigation results in SIEM tools

By sending Splunk SOAR investigations to your Enclave, Splunk Intelligence Management SIEM integrations will automatically add malicious observables to detection sets and remove whitelisted observables from detection sets.

Requirements

- Access to both Splunk SOAR and Splunk Intelligence Management.
- Splunk Intelligence Management (TruSTAR) app for Splunk SOAR.
- Enable Phishing Triage on your Splunk Intelligence Management (TruSTAR) account.
- Download the Splunk SOAR Threat Investigate playbook playbook from Splunk SOAR Community Playbooks.

Get started at www.trustar.co/contact-sales

splunk>

www.splunk.com