splunk> + TRUSTAR

PRODUCT BRIEF

TruSTAR Intelligence Management for Splunk SOAR

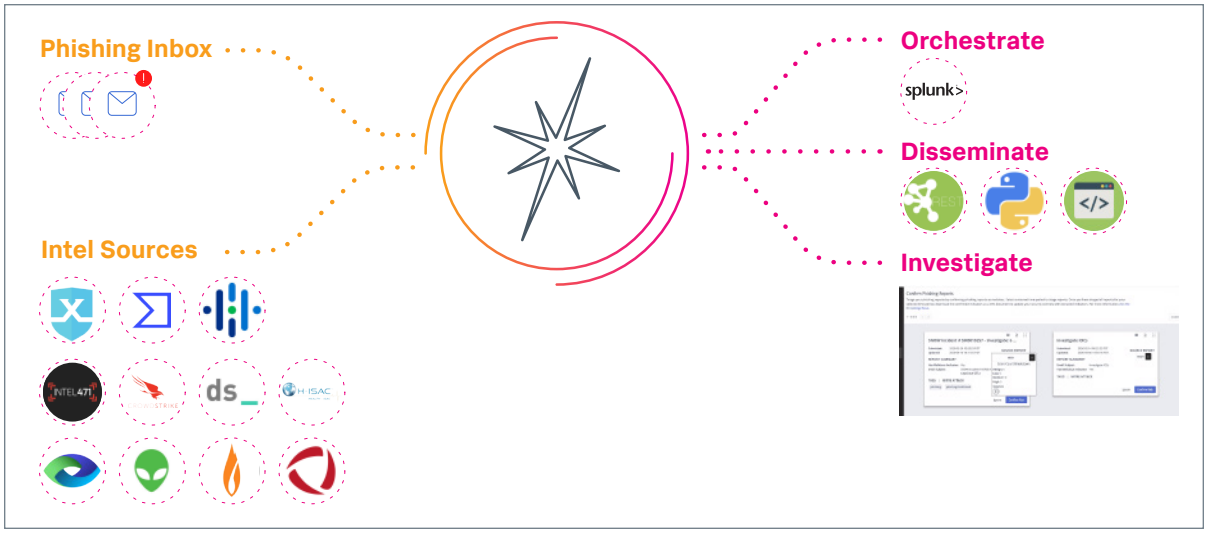
Accelerated phishing response through priority scoring

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 emails, which takes time away from priority alerts and mission-critical objectives.

TruSTAR and Splunk SOAR

Splunk SOAR automatically analyzes and responds to phishing attacks using automated playbooks. But Splunk SOAR playbooks become even more powerful with the addition of TruSTAR Intelligence Management. TruSTAR ingests user-reported suspicious emails, extracts observables and enriches them with open source, commercial intelligence feeds, and internal historical data. TruSTAR then calculates a normalized score for each Indicator and applies a priority score to each email for automated response.



Feature Highlights

- Accelerate automation by setting up playbooks that utilize the context of TruSTAR's Intelligence Reports and Indicators.
- Obtain prepared and normalized intelligence for faster triage and more streamlined playbooks.
- Use Indicator Normalized Scores, attributes and properties aggregated by TruSTAR in Splunk SOAR playbooks.
- Send observables from Splunk SOAR to TruSTAR whitelist and TruSTAR will automatically remove them from your security information event management (SIEM) tool.

Use Cases

- **Detect**
  Feed observables from Splunk SOAR investigations into SIEM tools. Automatically remove whitelisted observables from SIEM tools.
- **Triage**
  Prioritize investigations in Splunk SOAR using TruSTAR normalized scores.
- **Investigate**
  Enrich events with prepared and normalized data from intelligence sources.
- **Disseminate**
  Share SOAR investigations with ISACs/ISAOs.

Outcomes

Simplified enrichment playbooks

By managing all of your intelligence sources and preparing your data in a single platform, TruSTAR 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 TruSTAR by providing a single unified API for enrichment based on normalized intelligence.

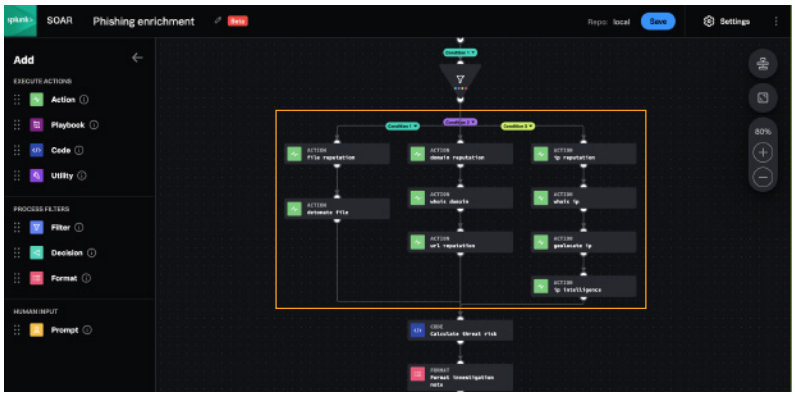


Figure A: Playbooks without TruSTAR.

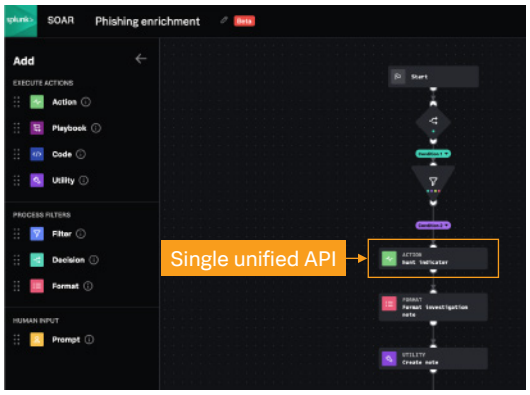


Figure B: Playbooks with TruSTAR.

Operationalized investigation results in SIEM tools

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

Metrics that Matter

Spend less time wrangling data, and more time catching bad guys.

Reduction in Mean-Time-to-Detect
"How long does it take me to find something is bad?"

Reduction in Mean-Time-to-Respond
"How long does it take me to stop it?"

Hours Saved Per Analyst Per Day
"How long does it take me to manually enrich investigations"

Requirements

- Access to both Splunk SOAR and TruSTAR
- Configure the TruSTAR app in Splunk SOAR
- Enable Phishing Triage on your TruSTAR company

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

splunk> + TRUSTAR

www.splunk.com