splunk> + TRUSTAR

PRODUCT BRIEF

TruSTAR Intelligence Management for Splunk Enterprise and Enterprise Security

Accelerate investigations through automated data enrichment

The Problem

Manual vetting and data from multiple sources cause analysts to waste much of their time data wrangling, taking time away from alerts that matter the most. Analysts need the ability to normalize and enrich multiple data sources for an objective view of security events.

TruSTAR's Solution

The TruSTAR Unified App for Splunk Enterprise and Enterprise Security helps security professionals analyze notable events and leverage intelligence to quickly understand threat context and prioritize and accelerate triage. With TruSTAR and Splunk, intelligence analysts can leverage data in Splunk and enrich against threat intelligence feeds and case management data to gain insight into attack trends.

Feature Highlights

Leverage Indicator Prioritization Intel Workflows to easily select intelligence sources, apply priority scores, Safelists, and filters based on Indicator type or attributes, and submit prepared data into TruSTAR Enclaves for Splunk to ingest threat enrichment attributes to the indicators associated with security incidents

Load Indicators from TruSTAR into Splunk KV Stores

Enrich a notable event in Splunk ES using intel from TruSTAR Enclaves

Update notable event urgency in Splunk ES based on normalized scores from TruSTAR

Prioritize notable events using scores from intel sources normalized to a common scale

Use Cases

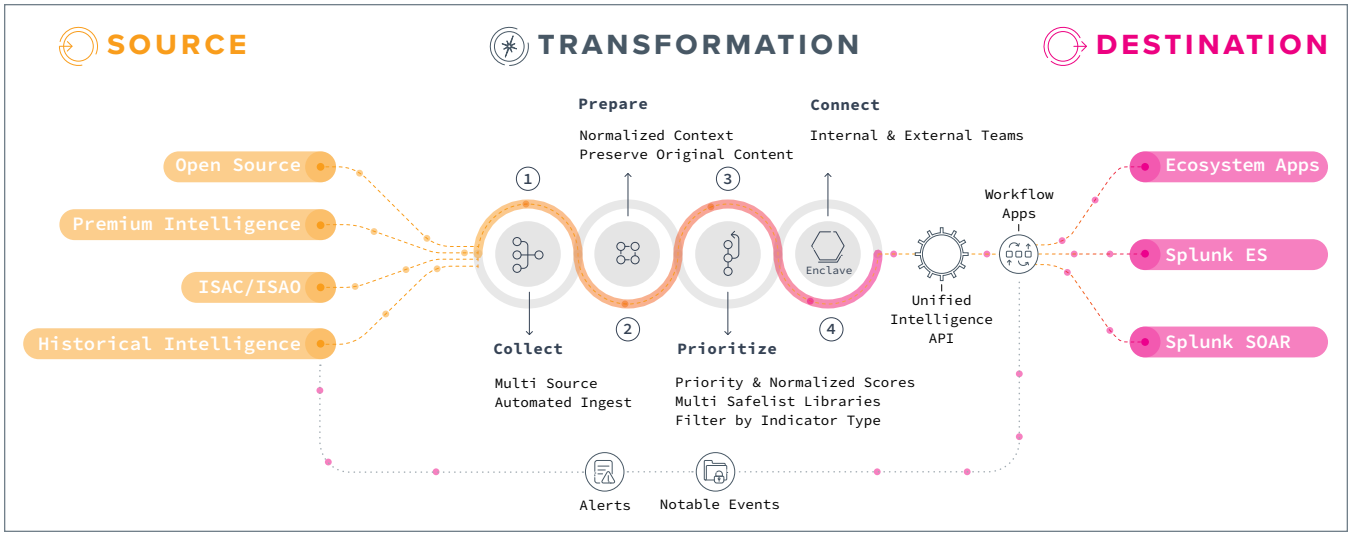
Detect
Automatically download observables from Premium Intelligence, Open Source, or Sharing Groups into Splunk KV Stores for use in searching or to alert against internal log events.

Triage
Enrich and prioritize notable events in Splunk Enterprise Security with multiple intelligence sources for accelerated investigations.

Optimize Workflows
Customize data ingest preference based on Indicator type, tags, and age of Indicator to cut down on data volume exchange between tools for better accuracy.

Investigate and Respond
Automatically submit notable events to TruSTAR Enclaves for further enrichment and correlation with historical data to triage alerts based on context and severity.

Prepare Data
TruSTAR allows companies to centralize, normalize, and prioritize cyber intelligence to help with investigation time and resources.



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 and TruSTAR
- Download the TruSTAR Unified App from Splunkbase and find install instructions at support.trustar.co

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

splunk> + TRUSTAR

www.splunk.com

21-19521-Splunk-Trustar for Enterprise Security-PB-101