splunk> turn data into doing

SOLUTION GUIDE

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.

The Solution

The Splunk Intelligence Management (formerly 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 Splunk Intelligence Management, 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 Intelligence Flows to easily select intelligence sources, apply priority scores, Safelists, and filters based on Indicator type or attributes, and submit prepared data into Enclaves for Splunk to ingest.

Load Indicators from Splunk Intelligence Management into Splunk KV Stores

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

Update notable event urgency in Splunk ES based on normalized scores from Splunk Intelligence Management.

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

Use Cases

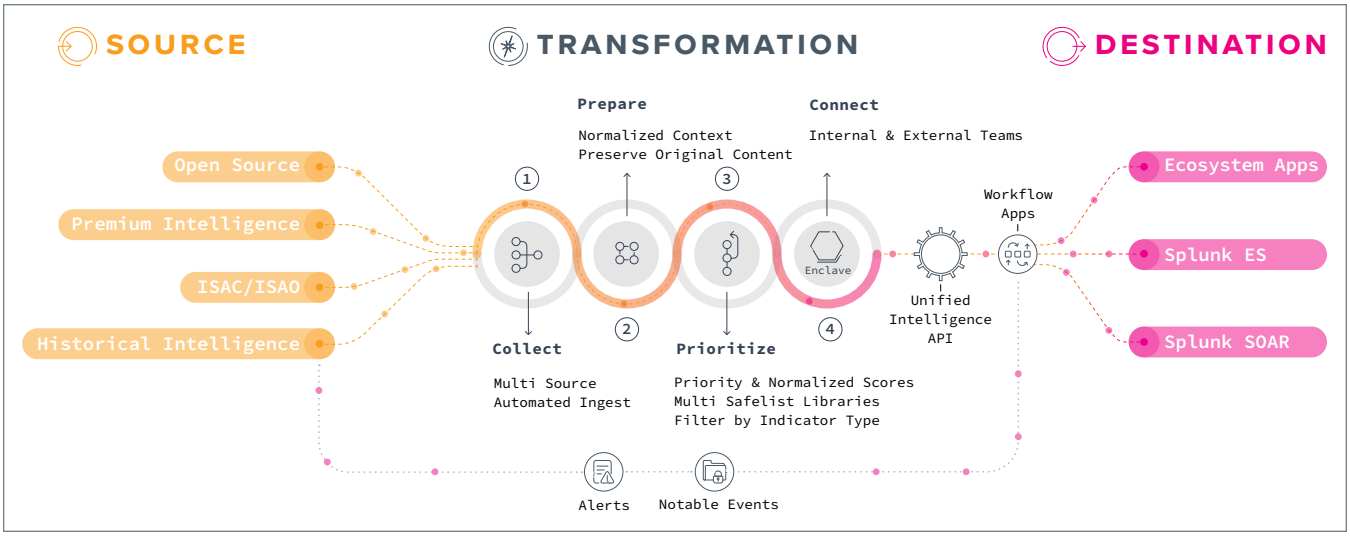
Detect
Automatically download observables from Premium Intelligence, Open Source, or Sharing Groups into Splunk KV Stores for use in searching or to alert against internal log events.

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 Enclaves for further enrichment and correlation with historical data to triage alerts based on context and severity.

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



Requirements

- Access to both Splunk and TruSTAR
- Download the TruSTAR Unified App from Splunkbase and find install instructions in the Product Learning Guides for Intelligence Management.

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

splunk>

www.splunk.com

22-19521-Splunk-IntelligenceManagementforSplunkEnterprise-SG-103