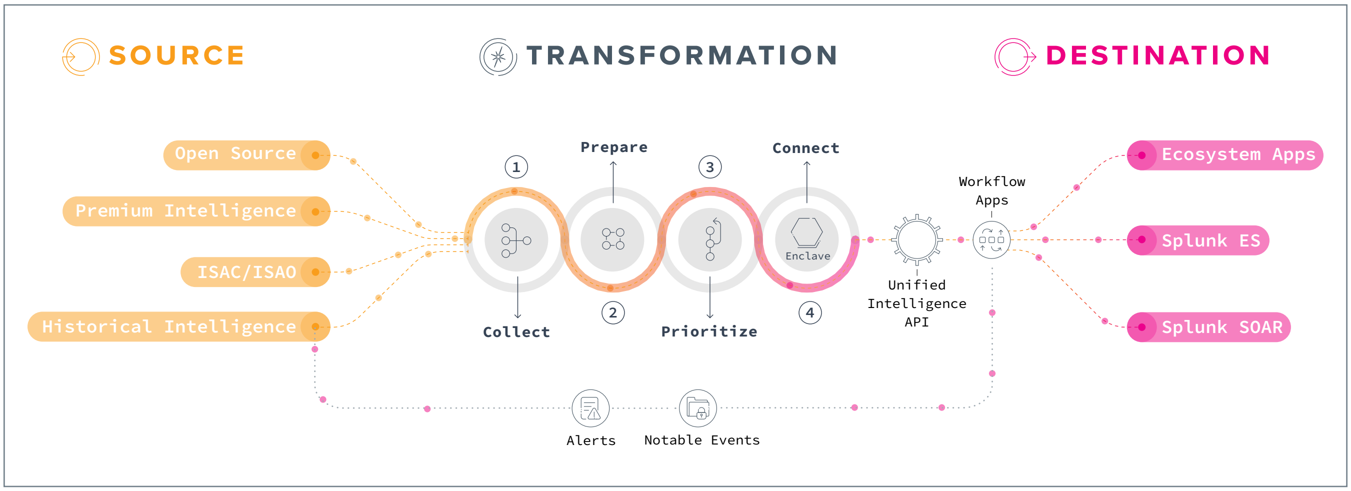
splunk> turn data into doing

PRODUCT BRIEF

Splunk Intelligence Management

Intelligence management for informed, actionable automation across your ecosystem of teams, tools and partners

- **Prepare, transform and prioritize intelligence** upstream from your core detection and response applications.
- **Normalize scores** from different intel sources, events and observables to surface the highest fidelity signal for action.
- **Facilitate intelligence exchange and collaboration** with peers, partners and ISACs/ISAOs.
- **Operationalize internal and external data sources** with leading SIEM, SOAR and case management integrations.



Transform, automate and operationalize intelligence for faster detection and response

Security analysts are overwhelmed with alerts and repetitive, manual tasks. SOC teams have added people, tools and external threat intelligence sources in an effort to alleviate these burdens, but security leaders struggle to integrate and automate to capitalize on their investments and keep up with alerts. The combination of tool sprawl and disparate data sources for enrichment causes fragmented silos and requires skilled professionals to wrangle data through manual curation.

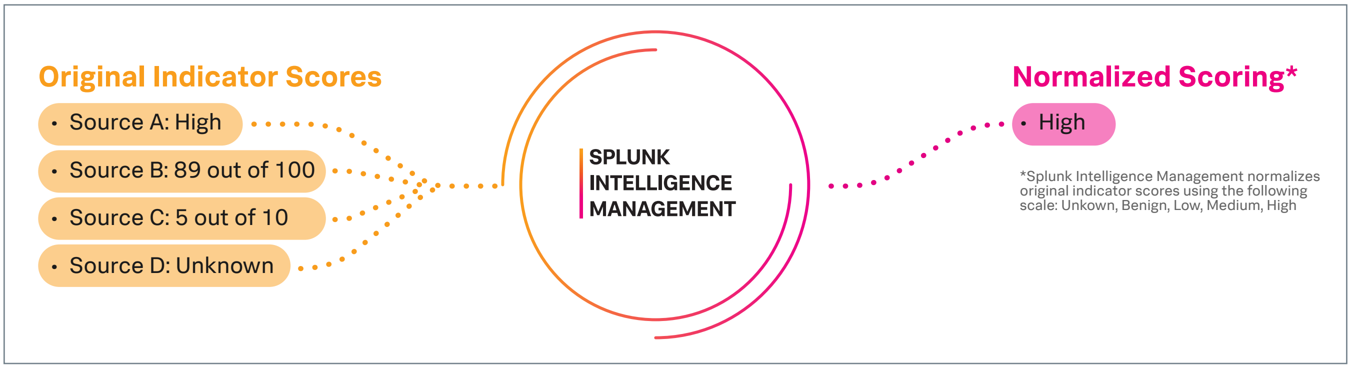
Stop wrangling data and start managing it for automation. Splunk Intelligence Management (formerly TruSTAR) transforms internal and external intelligence for actionable automation across detection, triage, investigation and dissemination use cases to reduce mean time to detection and mean time to response. Splunk Intelligence Management ingests intelligence from over 70 sources, normalizes, prioritizes and prepares it to be disseminated into the tools already used by teams to improve the efficiency of security operations and help eliminate integration debt. Manage intelligence upstream from core detection and response applications in order to customize and control the flow of data, validate and share intelligence and reduce mean time to detect and mean time to respond.

Enrichment when and where it's needed for improved investigations

Splunk Intelligence Management combines and enriches multiple data sources to provide more context around security events. Advanced search and filtering options across indicators and reports give rapid access to intel within the web interface. Splunk Intelligence Management enrichment also allows for operationalizing data within ecosystems of tools. Enriched data can be displayed directly in workflow applications to aid detection and response. Deeper link analysis is also available with one-click access back to the Splunk Intelligence Management web interface.

Spend time investigating what matters most

Data from multiple sources comes in different structures and formats, and teams have to rely on tedious, time-consuming collection, data cleaning and manual curation techniques. As tools start generating alerts from that data, analysts spend valuable time investigating unnecessary alerts that could have been prevented if the intelligence had been professionally curated. Splunk Intelligence Management normalizes data from multiple sources into a single data model and schema. When data is submitted to Splunk Intelligence Management, observables are extracted and enriched with intelligence sources and then normalized with a single normalized indicator score that can be used by analysts to prioritize investigation and triage.



*Splunk Intelligence Management normalizes original indicator scores using the following scale: Unkown, Benign, Low, Medium, High

Eliminate manual curation to accelerate automation and detect threats confidently

Without proper curation, open and premium external data sources create more false positives than true detections and overwhelm SOC teams. Splunk Intelligence Management aggregates, enriches, normalizes, and prioritizes intelligence from multiple sources, including open source, premium intelligence and internal historical intelligence, eliminating the need for manual curation.

Splunk Intelligence Management uses a no-code setup for intelligence pipelines that enables multi source collection of data, normalization, enrichment, scoring and prioritization of indicators. With Intelligence Flows, you can customize source weights to influence indicator priority scores and create multiple data flows tailored to a team's specific use cases and destination tools. Prepared and prioritized intelligence makes teams faster and more efficient at making security decisions.

Disseminate data seamlessly

Splunk Intelligence Management uses dynamic, cloud-based intelligence repositories known as Enclaves to manage user permissions and control proprietary flows of intelligence to tools and teams. Enclaves are flexible and customizable to meet an organization's unique data analysis, sharing and access control needs. Create private Enclaves to validate intelligence and seamlessly share intelligence with internal or external teams or tools by using tags or other attributes. The redaction feature protects the privacy of sources to effortlessly exchange intelligence and collaborate with peers, partners and industry group ISACs and ISAOs.

Get started at www.trustar.co/contact-sales or learn more about how Splunk Intelligence Management delivers insights directly into Splunk Enterprise Security and Splunk SOAR.