Splunk Intelligence Management (TruSTAR) + Splunk ES Demo

In this video, you’ll learn how TruSTAR, now Splunk Intelligence Management, integrates with Splunk Enterprise and Splunk Enterprise Security deployments.

The capabilities offered by TruSTAR’s Unified app will depend on the Splunk offering you currently have, with Enterprise Security being the one that can take advantage of all available capabilities:

- **Detect**: Extract actionable insights from your Premium Intelligence. Create focused or broad searches and ingests into Splunk Kilo stores for improved detection. Select only indicator types that are relevant to you.
- **Triage**: Sift and prioritize actionable events in Splunk ES by making additional data about your incident sources within TruSTAR accessible. Using the “Final Likelihood” value, the severity of a threat event can be updated based on new information or insights from your incident response.
- **Disseminate**: Submit relevant threat events to TruSTAR to store and share information and learning for incidents captured during threat and investigation or to help step beyond data for the observation or case it applies again.

Additional resources

- Use Case: Configuration Video Path
- Docs: Unified App Installation Guide
- Docs: Unified App User Guide
- Docs: Unified App FAQs
- App: TruSTAR Unified

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.