Unified App for ES: Enrich and Submit Notable Events - Splunk Intelligence Management (TruSTAR)

In this video, we explain how you can take advantage of the enrich and submit actions available with the Splunk Intelligence Management Unified app and Splunk Enterprise Security. Learn also how a Notable Event urgency can be automatically updated based on your intelligence data and how to add shortcuts for these actions into your Notable Events.

Continue to the next section of the video path. Each step is explained in a short video:

- **Unified App: Use Case - Splunk Intelligence Management (TruSTAR)**
  Learn how a Security Analyst working with Splunk Enterprise Security can use the Splunk Intelligence Management (TruSTAR) Unified app to improve detection and triage.

- **Unified App: Initial Configuration - Splunk Intelligence Management (TruSTAR)**
  Learn about the initial configuration of the Splunk Intelligence Management Unified app for Splunk and Splunk Enterprise Security.

- **Unified App: Configure Inputs - Splunk Intelligence Management (TruSTAR)**
  Learn about the configurations that control how indicators are downloaded into Splunk with Intelligence Management Unified App inputs.

- **Unified App: Validate Download of Indicators - Splunk Intelligence Management (TruSTAR)**
  Learn to validate that your Unified App has successfully downloaded observables from Intelligence Management to Splunk and Splunk Enterprise Security KV Stores.

- **Unified App for ES: Enrich and Submit Notable Events - Splunk Intelligence Management (TruSTAR)**
  Learn to take advantage of the enrich and submit actions, as well as how a Notable Event urgency can be automatically updated based on your intelligence data.
Additional resources

- Video Demo: Splunk Intelligence Management + Splunk Enterprise Security Overview and Demo
- Docs: Unified App Installation Guide
- Docs: Unified App User Guide
- Docs: Unified App FAQs
- App: TruSTAR Unified