Threat Intelligence Management

Accelerate investigations with integrated intelligence enrichment

Gain more context around threats with a full breadth of embedded intelligence.

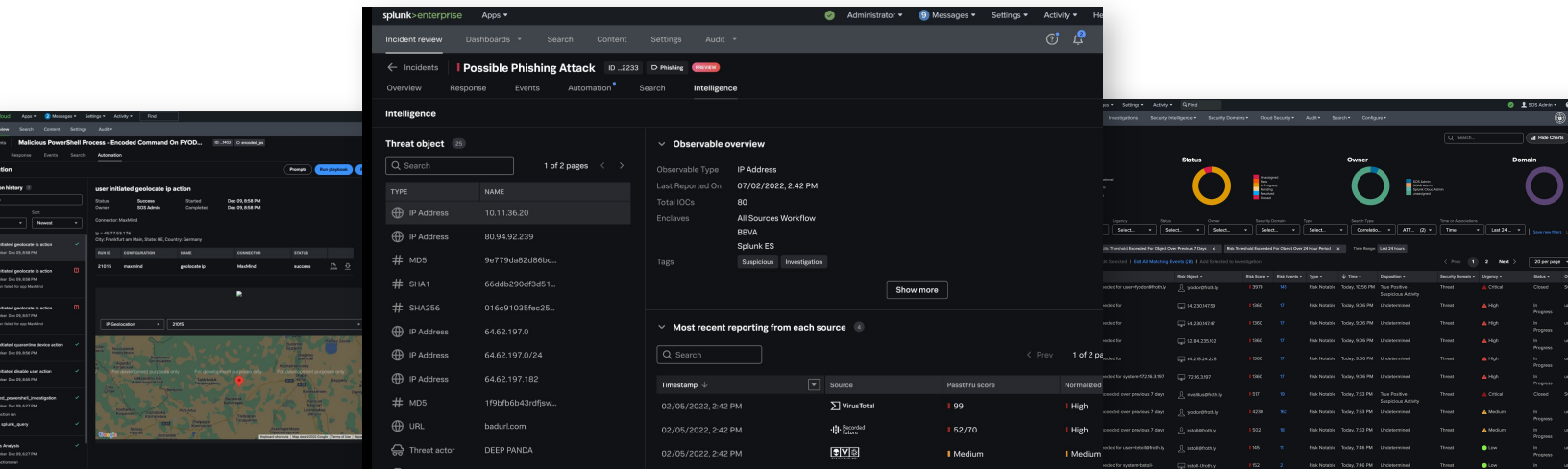
Reduce noise and surface the highest fidelity intelligence for action.

Simplify security workflows by accessing intelligence within Splunk Enterprise Security.

Security analysts are constantly overwhelmed by alerts and repetitive, manual tasks — negatively impacting their ability to triage and investigate critical security events. Analysts don't have the time to sift through multiple data feeds spanning countless sources, making it difficult to identify and synthesize intelligence related to an incident. The security operations center (SOC) requires seamless access to relevant threat intelligence along with a normalized scoring of data sources to have an objective view into critical events, as well as a comprehensive view into the potential risk to the enterprise.

Embedding threat intelligence into the operational framework of the SOC's detection, investigation and response workflows reduces mean time to detect (MTTD) and mean time to respond (MTTR), allowing analysts to manage events from a single console.

Threat Intelligence Management — a feature of Splunk® Enterprise Security — helps analysts to fully investigate security events by providing relevant and normalized intelligence to better understand threat context and accelerate time to triage. Analysts can manage security events and leverage threat intelligence feeds directly within Splunk Enterprise Security without pivoting to other tools, ultimately reducing time to investigate. This ensures informed, timely and actionable intelligence across the SOC's ecosystem of teams, tools and partners.



Informed, timely and actionable intelligence across the SOC's ecosystem of teams, tools and partners

Threat Intelligence Management reduces the number of alerts to investigate by filtering out intelligence that isn't relevant to the organization, allowing analysts to monitor for intelligence related to specific use cases. By synthesizing intelligence into a single, normalized view, Splunk is making it even easier for analysts to understand threat context and take action.

Monitor against curated IOC lists to reduce alert volume and speed up detections

The Intelligence Workflows allow analysts to create indicator of compromise (IOC) lists in order to receive relevant alerts that align to specific detection use cases. This reduces alert fatigue by detecting IOCs relevant to an analyst's environment and accessing pertinent intelligence.

Access integrated intelligence within events to reduce time to investigate

Threat Intelligence Management integrates directly with the Splunk Enterprise Security Risk-based alerting (RBA) framework so analysts can detect sophisticated threats and reduce alert fatigue. RBA attributes risk to users and systems and generates an alert in the form of Splunk Enterprise Security Risk Notable Event, when risk and behavioral thresholds are exceeded.

Having Threat Intelligence Management integrated into Risk Notable Events provides analysts with an integrated intelligence solution to support the investigation of critical events. Threat Intelligence Management empowers analysts to conduct a full investigation of a Risk Notable Event by centralizing, normalizing and prioritizing intelligence into the investigation management user interface.