



Outsmart cyber threats



splunk>



Specified automated ingestion within the Splunk app



Real-time threat detection in your environment



Automated event log enrichment



Instant true-positive incident details tied directly to threat intelligence

Intelligence-driven automation reducing manual work and empowering analysts.

The Analyst1 platform, integrated with Splunk, streamlines cybersecurity operations by centralizing the management of indicators such as IP addresses, domain names, URLs, file hashes, and more. These indicators, drawn from various sources and evidence records, are automatically correlated with threat actors, malware, and tactics, techniques, and procedures (TTPs), enhancing their intelligence value and reducing analysts' workloads. With Splunk's network telemetry, Analyst1 auto-discovers and tracks indicator hits within network endpoints, providing immediate insights into active threats within the Analyst1 platform. This integration also allows Analyst1 to enrich Splunk event logs with advanced threat intelligence and offers automated ingestion and correlation features based on predefined criteria such as actor and malware associations. This seamless interaction between Analyst1 and Splunk via a bi-directional data feed ensures high-level correlation and context for indicators, aiding in swift investigation, dissemination, and triage through both user interface and API interactions.



Outsmart cyber threats



Intelligence-driven
automation reducing
manual work and
empowering analysts.



Real time threat monitoring



Advanced data collection and analysis



Collaboration and info sharing



Threat hunting capabilities



Customizable and scalable



Threat intelligence reporting