



Avalon + Splunk

# A Perfect Union

With the new Avalon Add-on for Splunk, security and intelligence teams can seamlessly move observed alert and log data from Splunk to Avalon for visualization and enrichment with OSINT and third-party threat intelligence, then easily ingest data back into Splunk to take action. Avalon helps security analysts streamline the investigation process - combining link analysis, visualization, collaboration and reporting in a single, interactive workspace.



## Integration Highlights



### Integrate Diverse Data Sources

Conduct investigations efficiently by seamlessly integrating threat data from Splunk and other sources into a single Avalon workspace.



### Interact in Real-Time

Enable real-time, secure collaboration across teams - or across your industry - to eliminate silos and increase analysis efficiency.



### Visualize Threats and Connections

Quickly visualize and enrich threat data from Splunk to easily discover and understand data relationships.



### Deliver Results

Move data directly from Splunk to Avalon to visualize, investigate, and create reporting, then export back to Splunk to take corrective action.



### Preserve Investigations

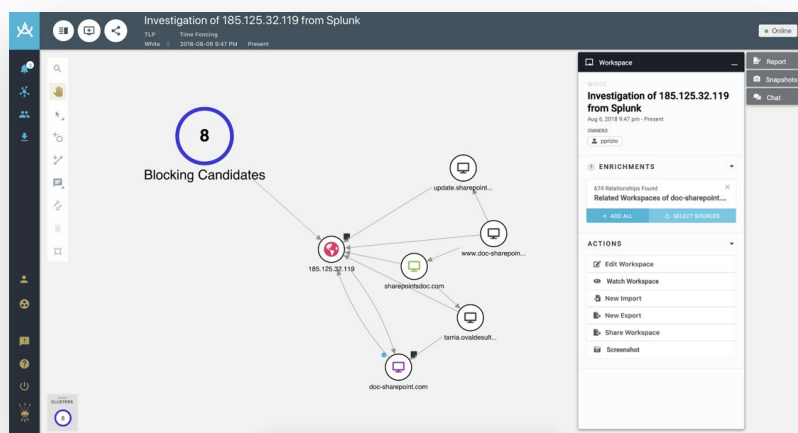
Create a centralized knowledge repository to maintain the latest investigative intelligence that can be utilized for future investigations.

## Integration Benefits

- Seamlessly pivot from Splunk to Avalon and back again to streamline investigations and operationalize intelligence
- Quickly visualize Splunk data in an easy-to-use link-analysis platform
- Easily integrate both internal and external threat data to gain full context
- Collaborate in real-time across teams to uncover context, relevance, and take action
- Preserve past analyses to enrich future investigations

## Streamline the Security Investigation Process

Avalon is the first enterprise platform built specifically to integrate link analysis, collaboration and reporting into a single, interactive platform. This helps security teams spend less time on manual, time-consuming administrative tasks and more time on security.



splunk >



- TicketingOrchestration Systems
- Collaborative Reporting
- Key Stakeholders
- splunk >

## King and Union

King and Union enables security teams to easily create and deliver the right intelligence to the right person across all levels of their organization by unifying data from multiple tools and results from investigations into a single cyber analysis delivery platform. With our platform, Avalon, security teams can quickly visualize threat data and investigate together in real time, and once complete, efficiently create and deliver the finished intelligence required to key stakeholders. Avalon reduces the time on manual, administrative tasks, leaving analysts more time to focus on security, and empowers organizations to take full advantage of the security investments they've made - in people, information and technology.

## Splunk

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and [try Splunk for free today](#). To learn more please visit [Splunk.com](#).



[kingandunion.com](http://kingandunion.com)  
 102 S. Union St.  
 Alexandria, VA 22314  
[info@kingandunion.com](mailto:info@kingandunion.com)

splunk >  
[splunk.com](http://splunk.com)

270 Brannan St.  
 San Francisco, CA 94107  
 1866-438-7758