LOOKINGGLASS

LOOKINGGLASS™ SPLUNK INTEGRATION

Unify Threat Intelligence in Your SIEM

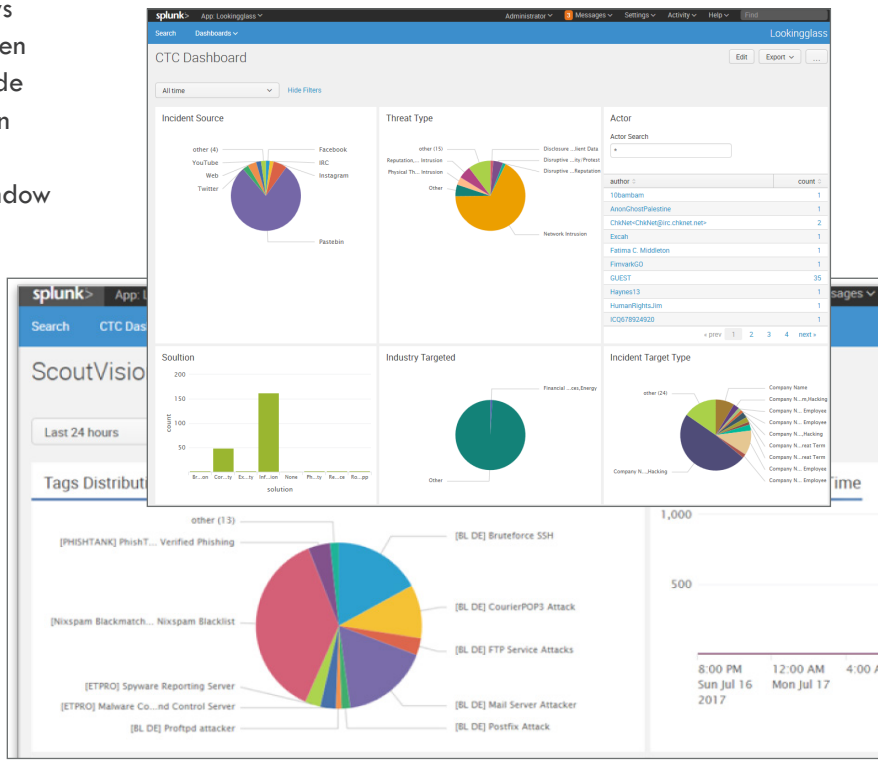
Making sense of threat intelligence data is a daunting task, but now it's made simpler by integrating Splunk with ScoutVision™. Teams monitoring an organization's landscape can be confident in the quality of their threat information and consequently, the decisions made while mitigating threats.

Ingesting data from firewalls, logs, command and control (C2) domains, infected machines, and other threat intelligence end points and network assets, ScoutVision correlates threat data with Global Border Gateway Protocol (BGP) Networking Data, allowing for footprinting of an organization's network.

ScoutVision's ability to search for IP addresses and fully qualified domain names (FQDN) in our collection of over 100 million registered domains powers Splunk. This allows analysts to receive and review information regarding open source threats and identified network elements living inside and outside ofan organization's infrastructure. ScoutVision categorizes threats given their criticality, threat type and actor, and time of incident allowing Splunk to open a window of additional threat data readily available to act upon.

The Splunk Integration for ScoutVision comes pre-packaged and contextualizes threat intelligence through various metrics, trends, and data visuals regarding projects and project tags. The Splunk Dashboard provides insight into the types, volume, and categories of open-source threat intelligence incidents that are collected.

It's finally here — the unified approach to visualizing threat intelligence, solved by LookingGlass' Splunk Application. Whether it's blocking bad network elements, or monitoring threats outside the walls of an organization, it is now possible to integrate threat data with Splunk, free of charge.



> Splunk users incorporate the power of ScoutVision directly into their SIEM infrastructure, leveraging the rules and processes that are part of their existing workflow, as well as receiving critical context to surrounding threats.

FEATURES	BENEFITS
Integrated Threat Intelligence	• Allows for analysis of ScoutVision network elements directly inside of Splunk • Centralization of security operations within Splunk • Threat intelligence correlation between intelligence provided by LookingGlass and SIEM customer specific log and event data • Increase in analyst productivity, while allowing for optimal decision-making • Additional metrics and charts are displayed in the ScoutVision project element and threats dashboard
High Quality Data Feeds	• Integration with ScoutVision allows for access to ScoutVision's high-quality threat intelligence feeds
Plug and Play	• The Splunk App for ScoutVision is free, quick, and easy to install and integrates out-of-the-box with Splunk

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass Cyber Solutions delivers unified threat protection against sophisticated cyber attacks to global enterprises and government agencies by operationalizing threat intelligence across its end-to-end portfolio. Scalable threat intelligence platforms and network-based threat response products consume our machine-readable data feeds to provide comprehensive threat-driven security. Augmenting the solutions portfolio is a worldwide team of security analysts who continuously enrich our data feeds and provide customers unprecedented understanding and response capability into cyber, physical, and third party risks. Prioritized, relevant, and timely insights enable customers to take action on threat intelligence across the different stages of the attack life cycle. Learn more at https://www.lookingglasscyber.com/.

Know More. Risk Less.