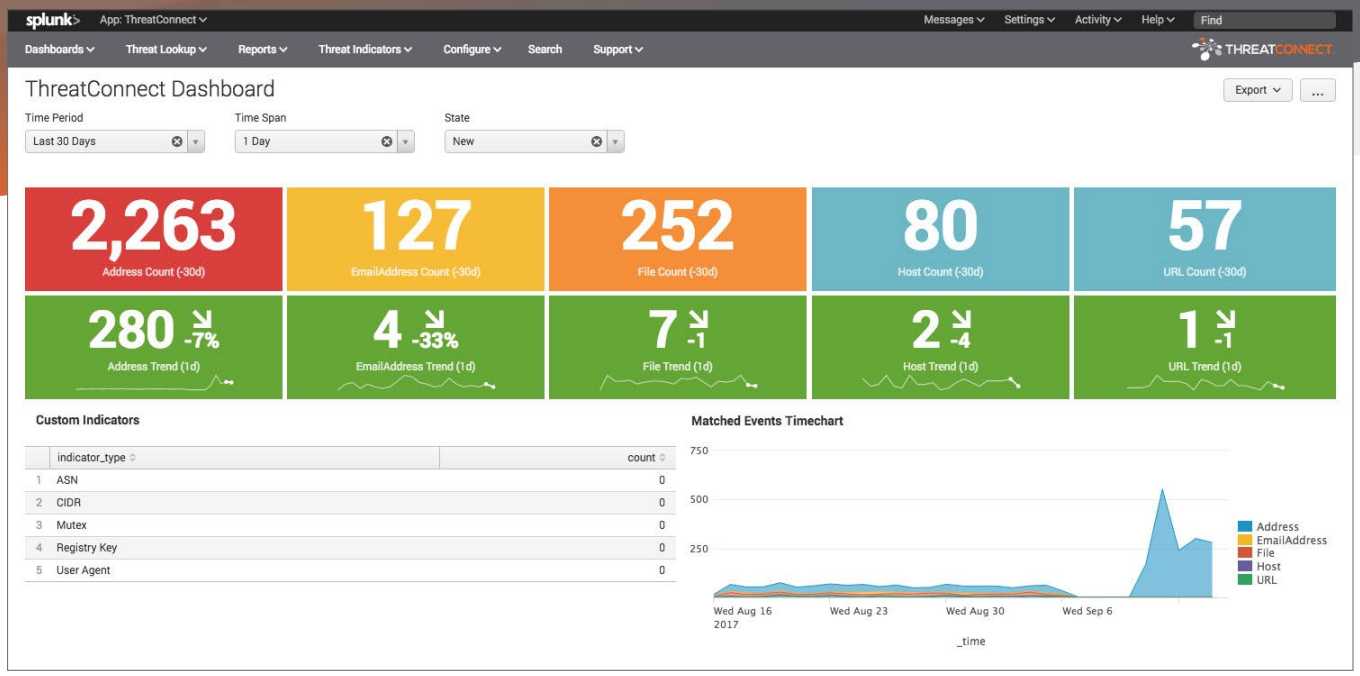
THREAT CONNECT

App for Splunk Enterprise

splunk>

Identify, Analyze, and Respond to Threats in Your Environment

ThreatConnect provides the ability to aggregate threat intelligence from multiple sources (i.e., open source, commercial, communities, and internally created), analyze and track identified adversary infrastructure and capabilities, and put that refined knowledge to work in Splunk, identifying threats targeting organizations. The **ThreatConnect® App for Splunk** provides Splunk users the ability to leverage customizable threat intelligence integrated into Splunk from their ThreatConnect accounts.



Automate the Detection of Advanced Threats in Your Environment

- Collect multi-source threat intelligence (open source, commercial, communities, internal research)
- Access insights on a threat's capability, infrastructure, and past incidents

Reduce False Positives to Save Time

- Leverage tailored, accurate, and timely threat intelligence
- Receive alerts on intel sourced from ThreatConnect communities and feeds matched against the logs and other machine data from a network within Splunk Enterprise

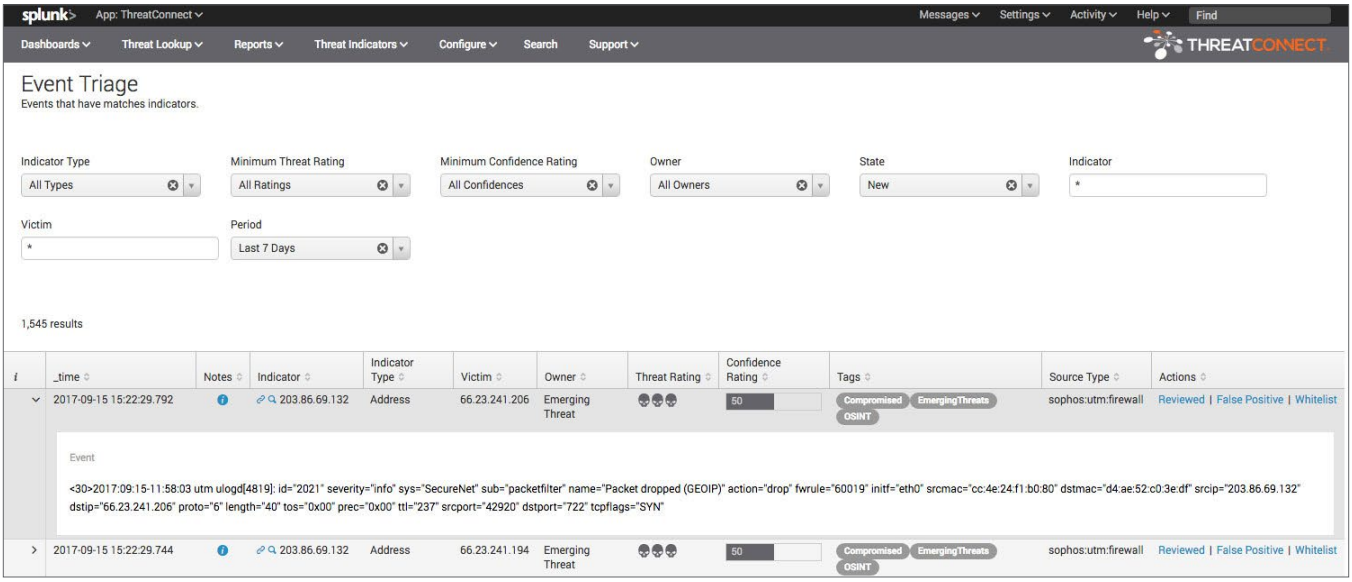
Prioritize Events and Respond to Threats as They Happen

- Sort by threat rating and confidence scores, relationships to known threat types and adversary groups, past incidents, and tags
- Triage events with context to quickly spot abnormal trends and patterns and act on them efficiently

www.ThreatConnect.com

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708

The ThreatConnect® App for Splunk takes your aggregated logs from Splunk and combines them with your threat intelligence in ThreatConnect. ThreatConnect provides context with the indicators, and enables your security team to easily spot abnormal trends and patterns to be able to act on them efficiently. Tie your data and intelligence to Playbooks, ThreatConnect's orchestration capability, to automate nearly any cybersecurity task and respond to threats faster.



Features and Benefits of ThreatConnect

- Apply tailored, relevant threat intelligence to your existing infrastructure
- Easily mark false positives
- Enrich and take action on your intel automatically
- Orchestrate security actions across your enterprise with Playbooks
- Receive alerts to block cyber threats and respond to incidents
- Correlate strategic and tactical threat intelligence with actionable machine-readable data
- Collect and share threat intelligence data from trusted communities
- Built-in dashboards and reports to expedite time to value

The ThreatConnect App for Splunk is available on splunkbase.com as a free download. Search for ThreatConnect.

ThreatConnect is available in the cloud, or as a dedicated cloud or on-premises deployment. We offer an always-free basic account. Visit **www.threatconnect.com** for details, and register for an account today.

About ThreatConnect®

ThreatConnect® arms organizations with a powerful defense against cyber threats and the confidence to make strategic business decisions. Built on the industry's only intelligence-driven, extensible security platform, ThreatConnect provides a suite of products designed to meet the threat intelligence aggregation, analysis and automation needs of security teams at any maturity level. More than 1,600 companies and agencies worldwide deploy the ThreatConnect platform to fully integrate their security technologies, teams, and processes with actionable threat intelligence resulting in reduced detection to response time and enhanced asset protection.

www.ThreatConnect.com

3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203
sales@threatconnect.com P: 1.800.965.2708