ThreatConnect

APP FOR SPLUNK ENTERPRISE

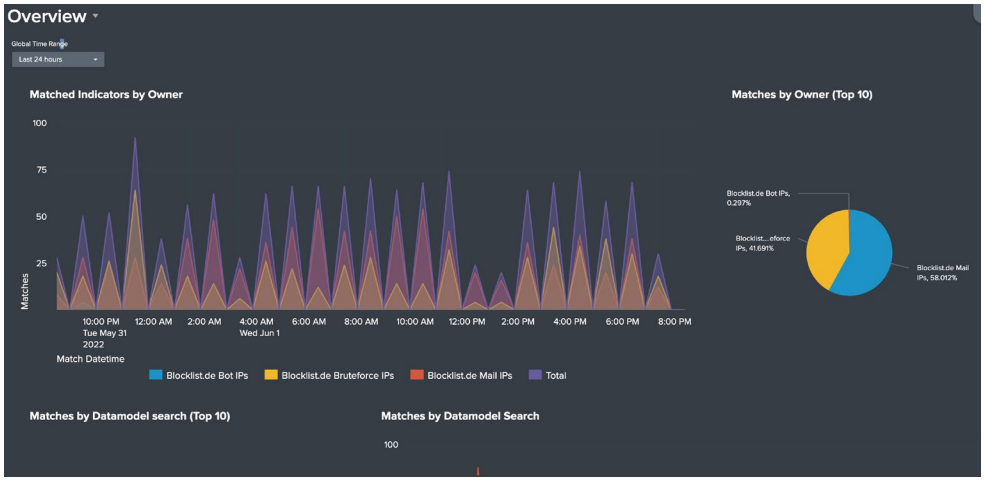
splunk>

ThreatConnect

Splunk Integration

Identify, Analyze, and take Action on Threats in your Environment

ThreatConnect™ provides the ability to aggregate and analyze threat intelligence from multiple sources - open source, commercial, community provided, or internally created. Users can centralize their intelligence, establish process consistency, scale operations, measure their effectiveness in one place, and use that refined knowledge in Splunk to identify threats targeting their organization. After the threat has been identified the user can take action to contain and remediate them with automated processes and workflows. The ThreatConnect App for Splunk provides Splunk users the ability to leverage customizable threat intelligence integrated into Splunk from their ThreatConnect accounts.



Automate Detection and Response in Your Environment

- Utilize ThreatConnect Query Language (TQL) to tailor the data imported into Splunk.
- Operationalize multi-source threat intelligence (open source, internal, commercial, etc) to enhance your detection capabilities.

Reduce False Positives to Save Time

- Leverage tailored, accurate, and timely threat intelligence refined and enriched from multiple sources, including our Collective Analytics Layer (CAL) to reduce False Positives.
- Take advantage of intel sourced from ThreatConnect communities and feeds against the logs and other machine data from a network within Splunk Enterprise.

Prioritize Events and Respond to Threats as They Happen

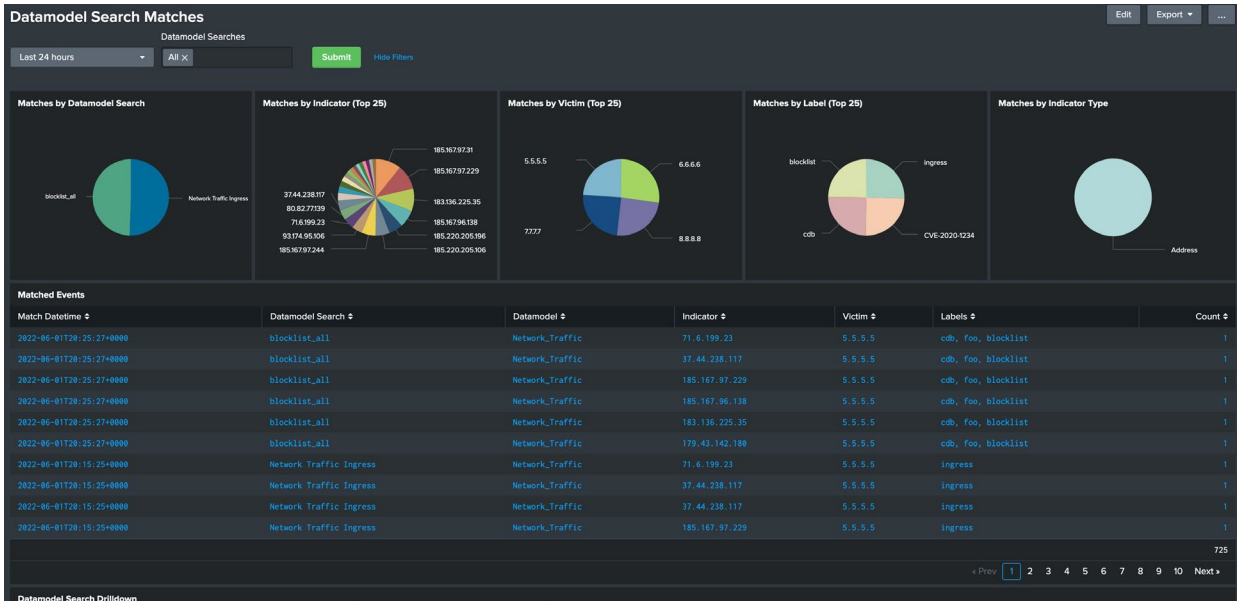
- Sort by threat rating and confidence scores, relationships to known threat types and adversary groups, past incidents, and tags.
- Complete dashboard overview of all matches from ThreatConnect by source of intelligence and data model search.
- Utilize drill down behavior to take a deep dive of the relevant information for matched events.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

The ThreatConnect Splunk Integration takes your aggregated logs from Splunk and combines them with your threat intelligence in ThreatConnect. Users can centralize their intelligence, establish process consistency, scale operations, measure their effectiveness in one place, and use that refined knowledge in Splunk to identify threats targeting their organization and take action to contain and remediate them with automated processes and workflows. 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.



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.

ThreatConnect app for Splunk and Technical Add-on (App)
ThreatConnect Threat Intel are both available on **splunkbase.com** as a free download.

Search for ThreatConnect .

ThreatConnect™

By operationalizing threat and cyber risk intelligence, The ThreatConnect Platform changes the security operations battlefield, giving your team the advantage over the attackers. It enables you to maximize the efficacy and value of your threat intelligence and human knowledge, leveraging the native machine intelligence in the ThreatConnect Platform. Your team will maximize their impact, efficiency, and collaboration to become a proactive force in protecting the enterprise.
Learn more at www.threatconnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708