

BlackLynx for Splunk Dashboard Descriptions

BlackLynx technology combines high performance heterogeneous computing (accelerated CPUs, GPUs, and FPGAs) with standard applications and protocols to achieve high performance analytics



Prerequisites

Install Splunk BlackLynx App version 1.0.2

BlackLynx for Splunk brings the enhanced speed and search capabilities of the BlackLynx solution to the Splunk Search, Dashboard, and Alerts features. This is done using the BlackLynx Splunk Apps *blstructsearch* and *blunstructsearch*.

This document describes each dashboard, the corporate function it provides and details the methodology used by BlackLynx to demonstrate potential solutions to the problems.

Each of these dashboards are designed to highlight some aspect of BlackLynx's ability to rapidly search and process large data sets without the need to Extract, Transform, and Load (ETL) the data.

splunk > enterprise App: BlackLynx search Administrator Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards **BLACKLYNX**

Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data. [Create New Dashboard](#)

16 Dashboards

i	Title ^	Actions	Owner ↕	App ↕	Sharing ↕
>	Blacklisted DNS	Edit ▼	admin	blacklynx_search	App
>	ClearTextSSN	Edit ▼	admin	blacklynx_search	Global
>	Cybersquatting Example For DNS Bro Logs Using Edit Distance	Edit ▼	admin	blacklynx_search	Global
>	DNS list	Edit ▼	admin	blacklynx_search	Global
>	Hillary Fuzzy Hamming Russian Troll	Edit ▼	admin	blacklynx_search	Global
>	HTTP Downloaded Files	Edit ▼	admin	blacklynx_search	App
>	HTTP GET hosts	Edit ▼	admin	blacklynx_search	App
>	Indexed Server Logs with Non-Indexed Traffic Logs	Edit ▼	admin	blacklynx_search	Private
>	Machine Learning Video Alerts	Edit ▼	admin	blacklynx_search	Private
>	Netflix TCP SYN Time Range	Edit ▼	nobody	blacklynx_search	Global
>	Non-Indexed Search with Regex	Edit ▼	admin	blacklynx_search	Global
>	PCAP Inspection	Edit ▼	nobody	blacklynx_search	Global
>	SSL Certificates	Edit ▼	admin	blacklynx_search	Global
>	SSL Certificates - Expired	Edit ▼	admin	blacklynx_search	Global
>	Trump Edit Distance Russian Troll	Edit ▼	admin	blacklynx_search	Global
>	Wake On LAN	Edit ▼	admin	blacklynx_search	App

BlackLynx for Splunk Dashboards

BlackLynx for Splunk Dashboard Descriptions: Indexed Server Logs with Non-indexed Traffic Logs



Dashboard Solution Statement:

This dashboard searches Indexed server logs and non-Indexed traffic logs correlating the bytes of traffic at each client IP address. The non-indexed search is preformed on raw BRO logs.

Time	Event	clientIP
07/04/2018 08:12:15	time="2018-07-04T08:12:15-04:00" level=info msg="[REST]: POST /files" client=192.168.1.227 latency=37.334212ms request="/files?file=%2Fryftone%2Ftwitter%2F20180530%2F1527716702.json&catalog=%2Ftwitter%2FmonthlyCatalogs%2F201805.json&local=true" status=200	192.168.1.227
07/04/2018 08:12:13	time="2018-07-04T08:12:13-04:00" level=info msg="[REST]: POST /files" client=192.168.1.227 latency=42.352426ms request="/files?file=%2Fryftone%2Ftwitter%2F20180530%2F1527716702.json&catalog=%2Ftwitter%2FmonthlyCatalogs%2F201805.json&local=true" status=200	192.168.1.227
06/30/2018 08:00:04	time="2018-06-30T08:00:04-04:00" level=info msg="[REST]: POST /files" client=192.168.1.220 latency=39.933213ms request="/files?file=%2Fryftone%2Ftwitter%2F20180530%2F1527716702.json&catalog=%2Ftwitter%2FmonthlyCatalogs%2F201805.json&local=true" status=200	192.168.1.220

clientIP	bytesTraffic
192.168.1.227	3210152
192.168.1.220	959917
168.192.49.34	6021
192.168.1.204	4515

Indexed Servers with non-indexed Traffic Dashboard

Query Inputs:

Host – BlackLynx server hostname or IP Address

Filename – BRO log(s) to be searched relative to “/ryftone” directory

Query Expression – search criteria, in this case any connections that are not local

BlackLynx Capabilities:

- Search of native CSV files using PCRE2 search to exclude local connections
- Combination of indexed Splunk data and non-indexed raw CSV data
- Return of the results to Splunk in a JSON format

