BlackLynx for Splunk Dashboard Descriptions

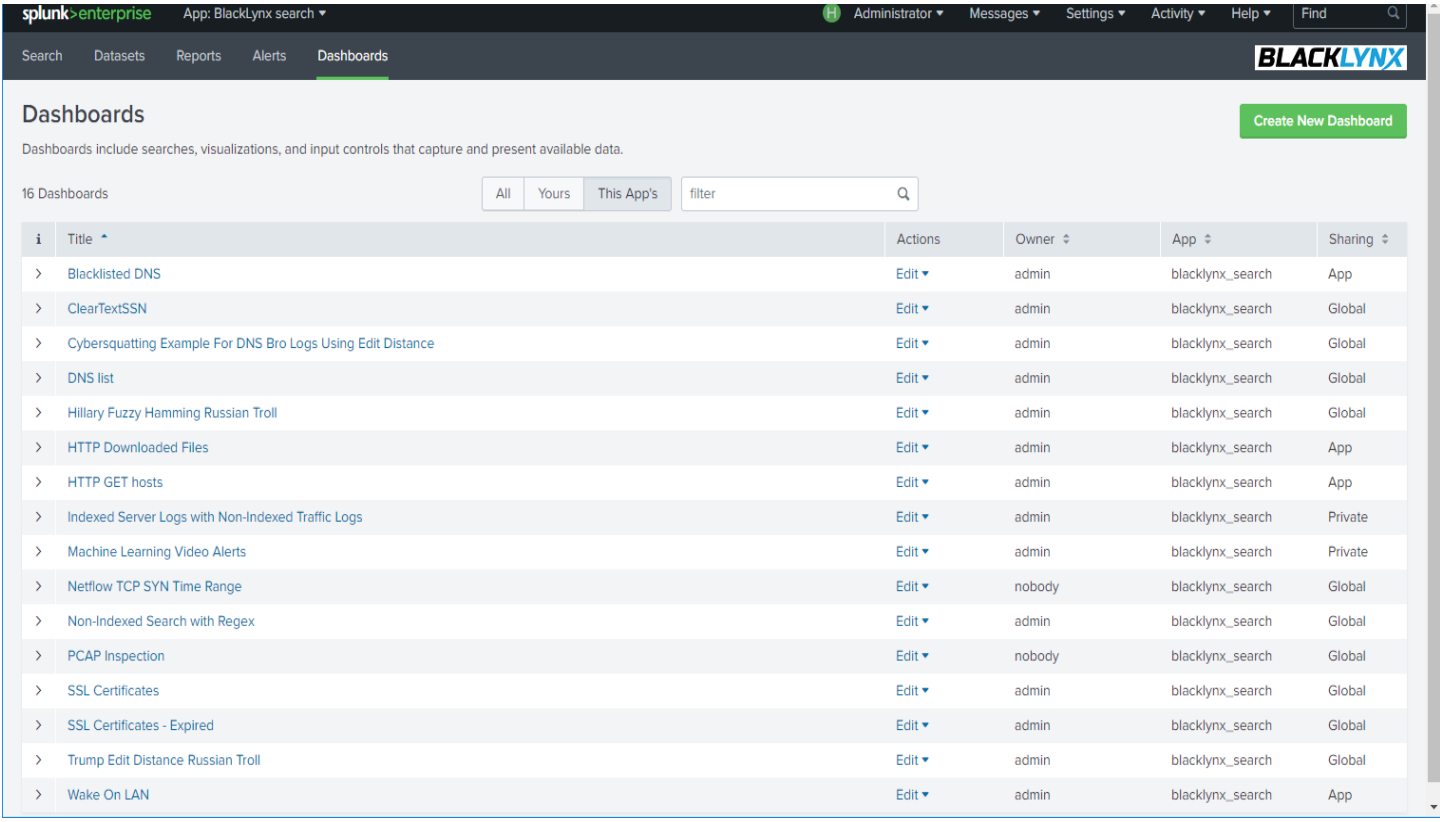
BlackLynx technology combines high performance heterogeneous computing (accelerated CPUs, GPUs, and FPGAs) with standard applications and protocols to achieve high performance analytics

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.



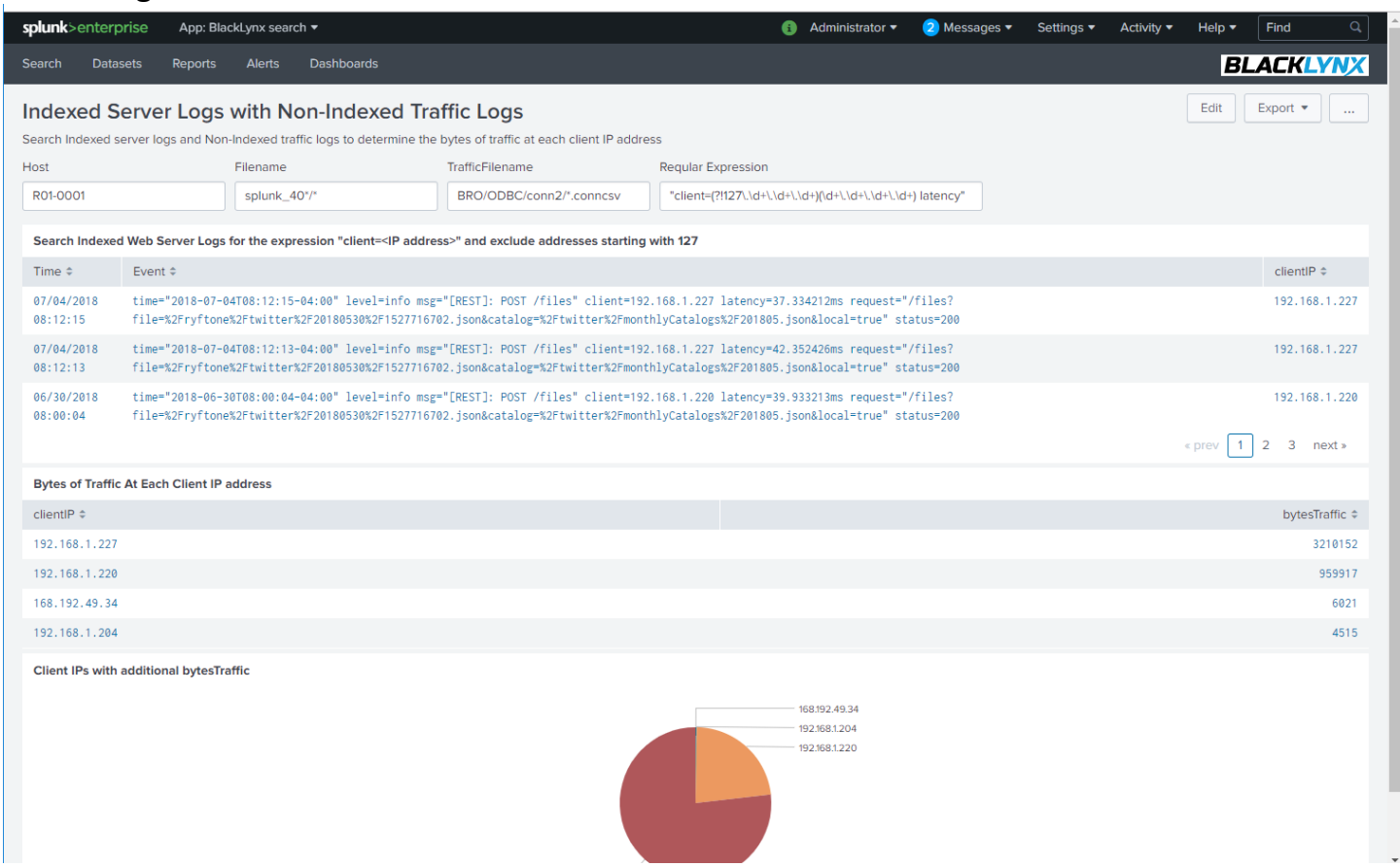
BlackLynx for Splunk Dashboards

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.



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