

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.

The screenshot shows the Splunk interface for the BlackLynx app. The top navigation bar includes 'splunk>enterprise', 'App: BlackLynx search', and user information. The main content area is titled 'Dashboards' and contains a list of 16 dashboards. The table below represents the data shown in the screenshot.

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
>	Netflow 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

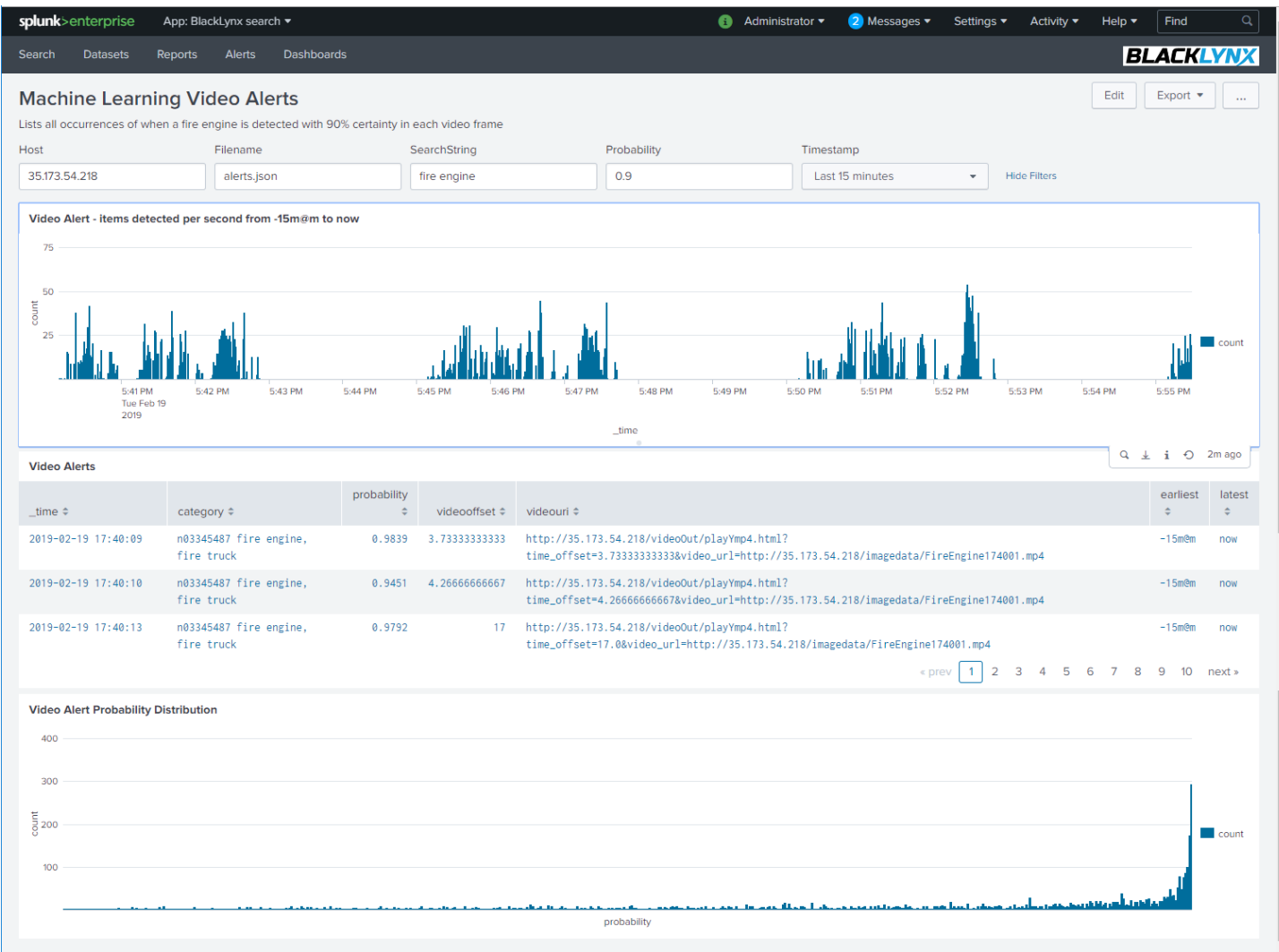
BlackLynx for Splunk Dashboards



Machine Learning Video Alerts

Dashboard Solution Statement:

The Machine Learning Video Alerts dashboard lists the alerts registered in the BlackLynx object detection demo, shows the time and probability distributions, and provides an interface into the alerts webpage. The raw data is the JSON output of the machine learning object detection and classification system. Clicking on the videouri entry



Machine Learning Video Alerts Dashboard



BlackLynx for Splunk Dashboard Descriptions: Machine Learning Video Alerts - continued



BLACKLYNX

Query Inputs:

Host – BlackLynx server hostname or IP Address

Filename – PCAP file(s) to be searched relative to “/ryftone” directory

Search Expression – the alert text used in the video demo

Probability – the detection probability used to generate the alert. The default is 90% certainty

Timestamp – Time range for the alerts to be displayed; may be absolute or relative

BlackLynx Capabilities:

- Search of native JSON files extracting alerts that meet the criteria (type, probability, and time)
- Return of the results to Splunk in a JSON format
- Demonstrate the ability to call up web pages based on the data in the Splunk table.

BLACKLYNX

Video Object Detection & Image Classification

Video Frame 0:03.73

Object Detection Frame Markup

truck, 29.7%

0.30 truck

Image Classification

0.98 - fire engine, fire truck
0.01 - tow truck, tow car, wrecker
0.01 - ambulance

Watchlist: fire engine, fire truck, Probability: 0.98, Alert Action: classes[* prob>0.9 & cat~fire engine i]

Alerts detected in this video: 1490

Alert Category:
fire engine, fire truck(1490)

fire engine, fire truck(0:03.73) fire engine, fire truck(0:04.27) fire engine, fire truck(0:16.80) fire engine, fire truck(0:17.00) fire engine, fire truck(0:17.47) fire engine, fire truck(0:17.53) fire engine, fire truck(0:17.67) fire engine, fire truck(0:17.87) fire engine, fire truck(0:17.93) fire engine, fire truck(0:18.13) fire engine, fire truck(0:18.27) fire engine, fire truck(0:18.53) fire engine, fire truck(0:18.73) fire engine, fire truck(0:18.80) fire engine, fire truck(0:18.87) fire engine, fire truck(0:18.93) fire engine, fire truck(0:19.00) fire engine, fire truck(0:19.07) fire engine, fire truck(0:19.13) fire engine, fire truck(0:19.20) fire engine, fire truck(0:19.27) fire engine, fire truck(0:19.33) fire engine, fire truck(0:19.40) fire engine, fire truck(0:19.47) fire engine, fire truck(0:19.53) fire engine, fire truck(0:19.60) fire engine, fire truck(0:19.73) fire engine, fire truck(0:20.33) fire engine, fire truck(0:20.40) fire engine, fire truck(0:20.47) fire engine, fire truck(0:20.53) fire engine, fire truck(0:20.67) fire engine, fire truck(0:21.07) fire engine, fire truck(0:27.53)

BlackLynx Video Object Detection and Classification Demo Page

