
# Developing Splunk Apps

Luke Harris @skywalka

# Splunk ftw

How to develop Splunk apps efficiently
and get paid to $plunk for a living!

Luke Harris
Splunk App Developer
Sydney, Australia

# Introduction

A long time ago in a galaxy far,
far away....

# A New Hope

"I'm Luke Skywalker, I'm here to rescue you."

# Riviera Harris → admin / changeme

# The Force is strong with this one

# My Splunk Apps

Splunk for **Nagios**

Splunk for **Isilon**

Splunk for **Symmetrix**

Splunk for **Postfix**

Splunk for **SAP -** collab with Shaun Butler & Jim Cooke

(Combined total of over 10,000 downloads)

# Punch it, Chewie!

- Tools
- Deployment Procedure
- Big Data ftw
- Sideview Utils
- Examples
- Splunk for Nagios Demo
- Tips & Tricks
- Q&A

# Tools

## Virtualization:

- Ganeti
  http://code.google.com/p/ganeti

## Operating Systems:

- Ubuntu
- CentOS/RHEL

## Configuration Management:

- Puppet

# Puppet

"Puppet is IT automation software that helps system administrators manage infrastructure throughout its lifecycle"

http://puppetlabs.com

Splunk Puppet module:

https://github.com/tfhartmann/puppet-splunk

# Chef

Chef (forked from Puppet)

http://www.opscode.com

# Ansible

Orchestration engine over SSH

http://www.ansibleworks.com

# RHN Satellite

If we travelled back in time...

# Version Control

- Git is a free and open source distributed version control system

  Powerful features include:

  - Branching and Merging
  - Distributed
  - Fast
  - Created by Linus Torvalds

Reference:
http://git-scm.com

# Semantic Versioning

Example:

Splunk for Nagios version 3.0.1

Given a version number MAJOR.MINOR.PATCH, increment the:

MAJOR version when you make incompatible API changes,

MINOR version when you add functionality in a backwards-compatible manner,

PATCH version when you make backwards-compatible bug fixes.

Additional labels for pre-release and build metadata are available as extensions to the MAJOR.MINOR.PATCH format."

Reference:

http://semver.org

# Deployment Procedure

* SFTP Transfer Server
* Splunk Deployment Server

Execute Order 66

# Social Coding

Google Code

GitHub

https://github.com/skywalka

Twitter

@skywalka

Blog

http://verypowerful.info

Splunk Answers

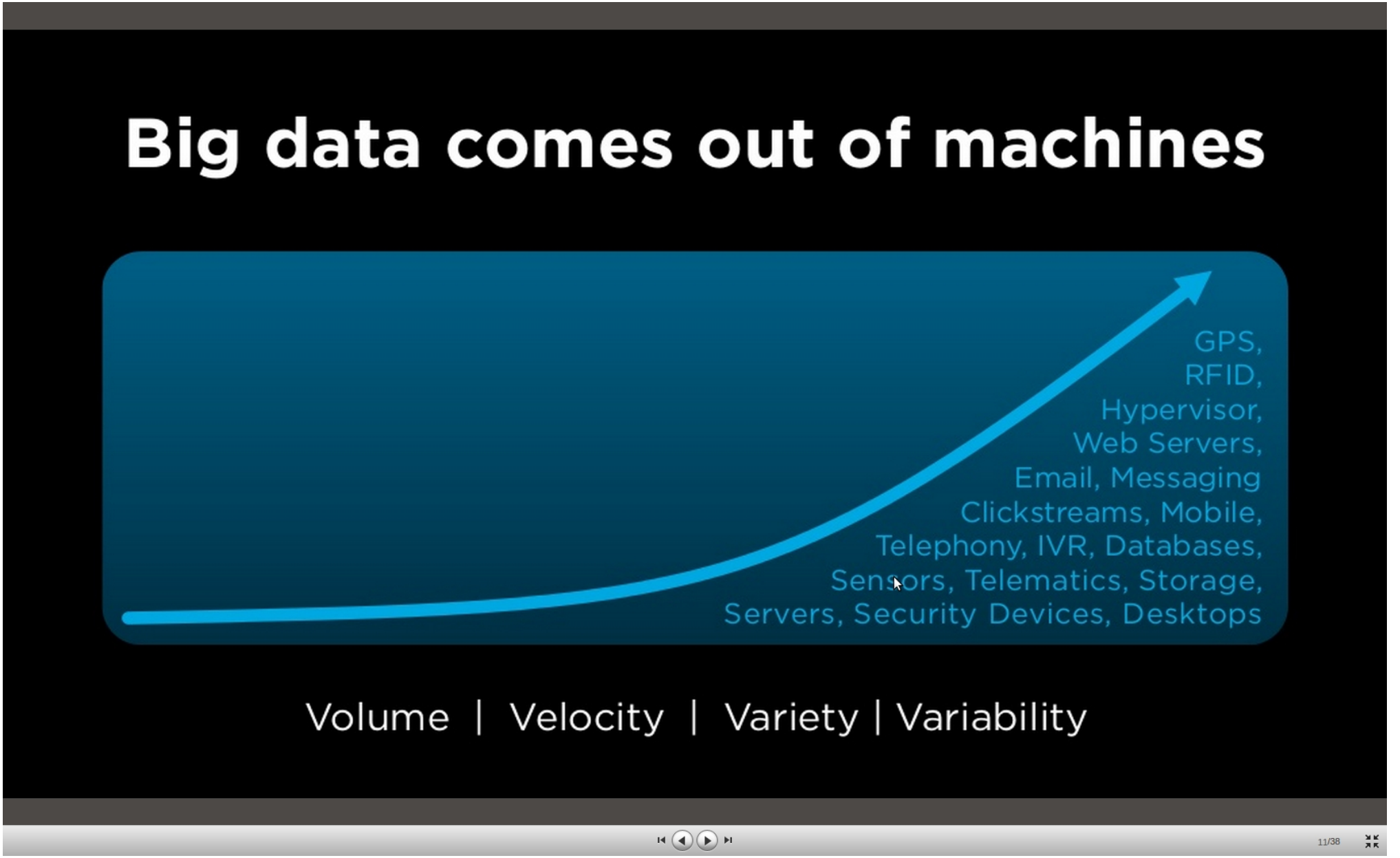
http://answers.splunk.com

# Buzz Words!!1!!!!111!!!

## Big Data

Small Data

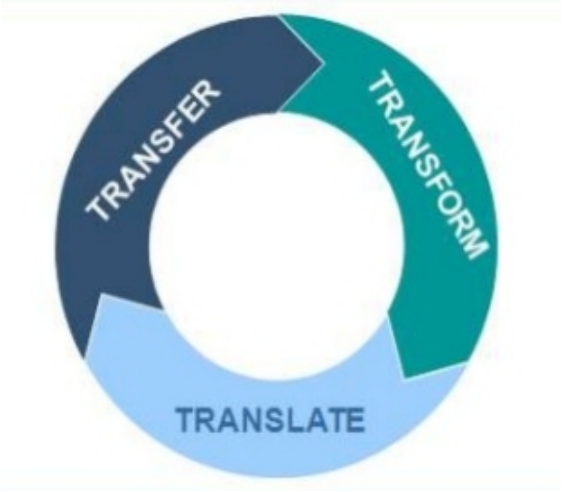
# Big Data


Big data comes out of machines
GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops
Volume | Velocity | Variety | Variability
11/38

# Big Data 2: Electric Boogaloo

The 3 T's :-

* Transfer
* Transform
* Translate





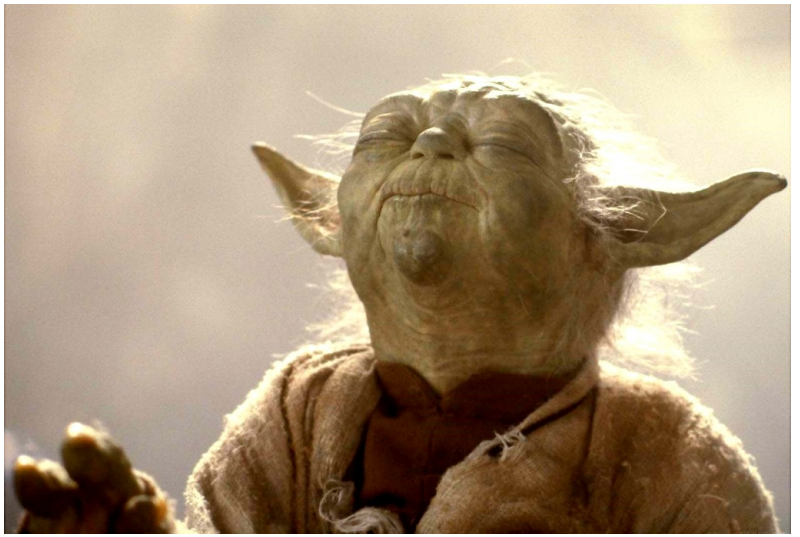
Reference:

http://www.datanami.com/datanami/2013-08-12/the_three_t_s_of_hadoop:_an_enterprise_big_data_pattern.html

# Sideview Utils

Sideview Utils is perfect for technical domain experts like you, and me!

http://sideviewapps.com



You don't have to know ANY programming languages and can get started immediately using the built-in examples in the app.

**10,000 Hour Rule (aka Myth)**

“The 10,000 hour rule made famous by Malcolm Gladwell’s book “Outliers” has become quite pervasive, but people were using it just to mean that practice was important, that’s it. That’s not what the theory says. The researcher behind it, Anders Ericsson said Gladwell misconstrued his work. His words, not mine.”

http://www.outsideonline.com/outdoor-adventure/media/books/How-Athletes-Get-Great.html

# How to Build Very Powerful Dashboards

## Use Sideview Utils.

- Guided Examples
- Features:
  - HTML
  - Search
  - PostProcess
  - Pulldowns
  - Checkboxes
  - URLLoader
  - Lookup Updater

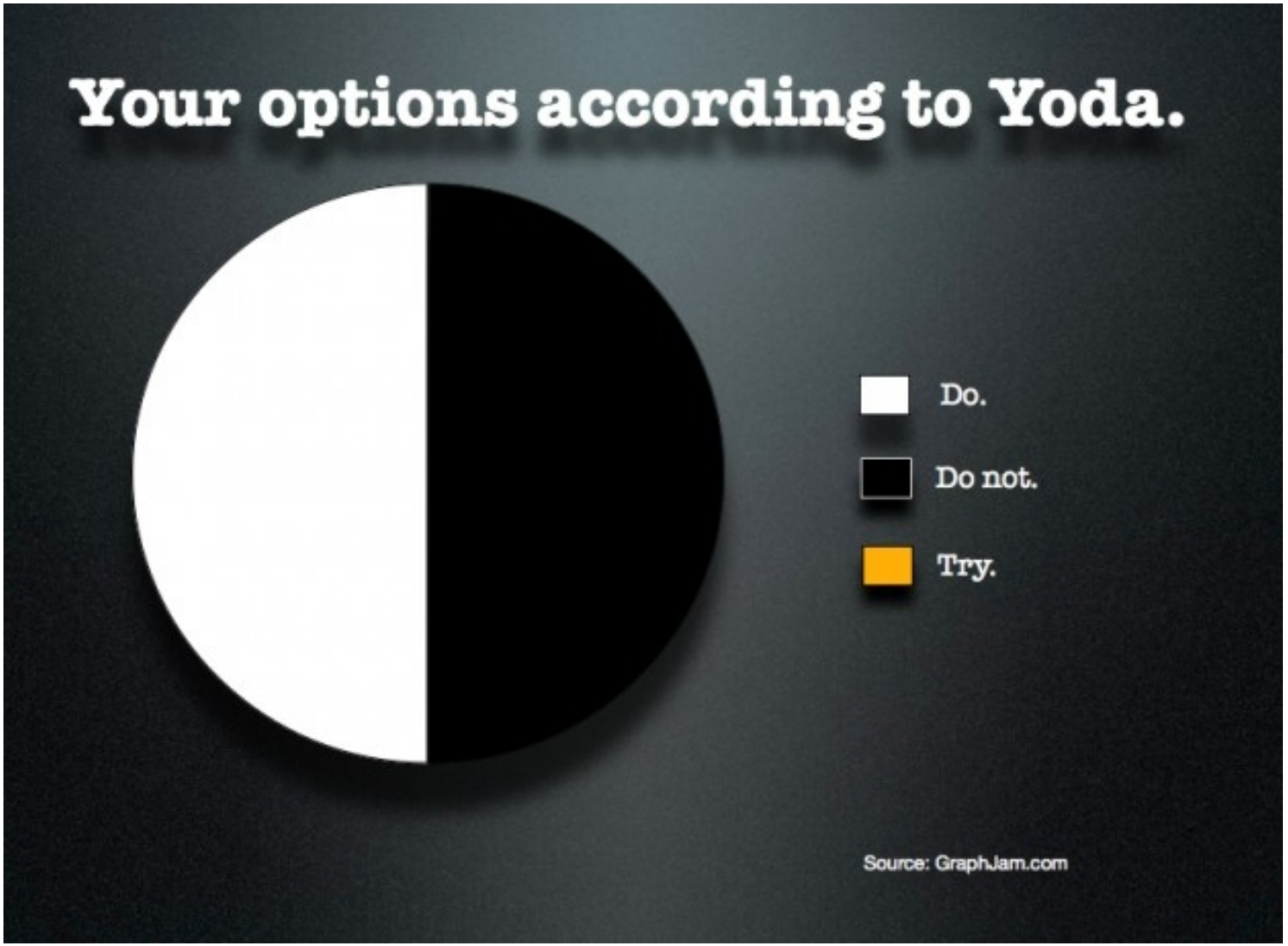
# Screenshots

Screenshots removed for general availability

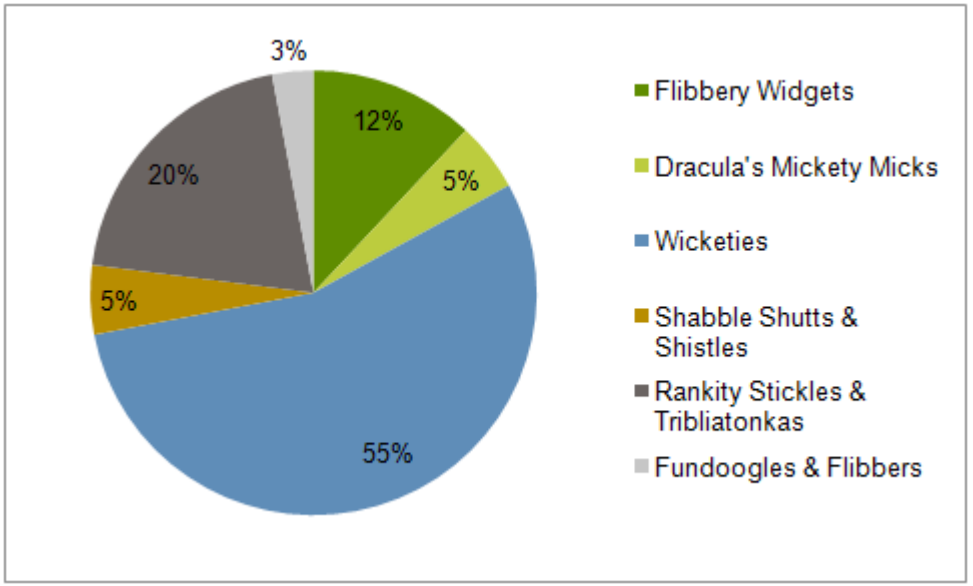
# Splunk for Nagios Demo

# How can you become a Splunk App Developer?!

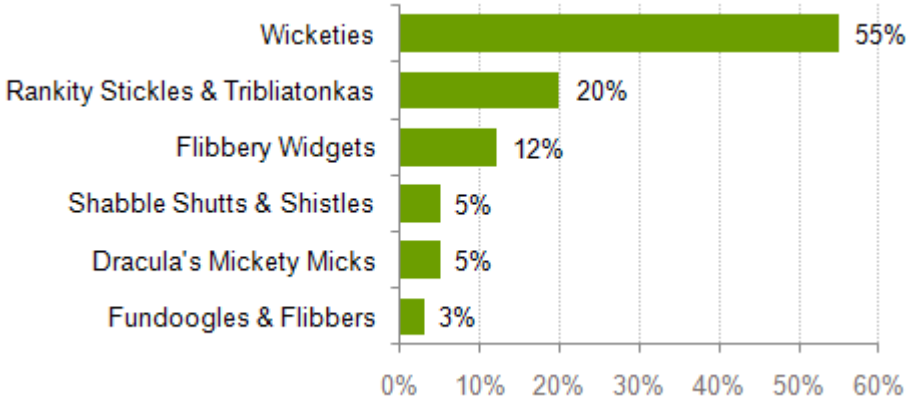
# Yoda's quote represented as a Chart



# Pie Charts are Evil




"Very Good"




"Excellent"

3 conditions must be met before using a Pie Chart :-

* Exactly 2 or 3 categories that make up the "whole"
* A fairly significant difference in % makeup for each of the categories
* Plenty of space available to present the information

Reference:
http://www.gilliganondata.com/index.php/2009/12/02/how-succinctly-can-i-explain-why-pie-charts-are-evil/

# Jabba says NO to Pie Charts

# Splunk 101

- 10GB Developers License
  http://dev.splunk.com

- Semantic logging:
  - purposefully logging specific data that exposes the state of business processes
  - use clear key-value pairs, eg.
    **father="yes"**
    **jedis=2**

- Event Generator:
  https://github.com/coccyx/eventgen

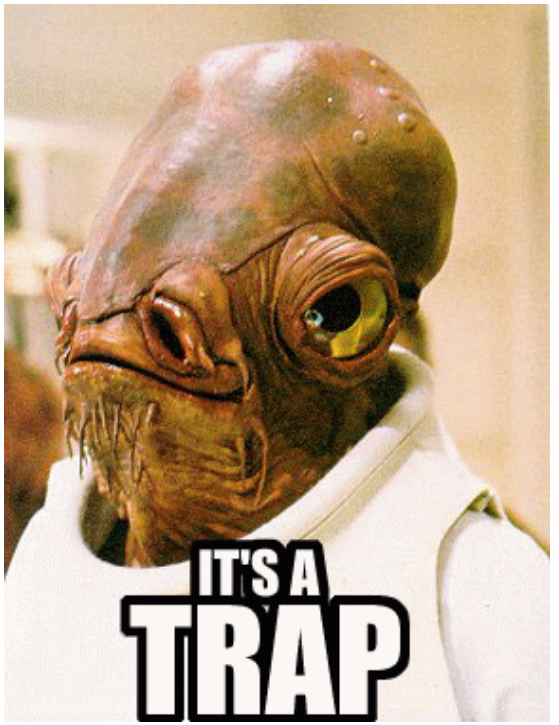
- Field Extractions:
  http://regexr.com

# Han Shot First!

Hindsight is a wonderful thing :-
http://wiki.splunk.com/Things_I_wish_I_knew_then

```
-Create a test splunk index
 Wipe entire index when testing is finished:
 # splunk clean eventdata -index <name>
```

# Dashboards 101




- Use one search for a whole dashboard
- Use the Common Information Model
- lookups > tags
- Use macros or event types
- Splunk 5: Use Summary Indexing or Report Acceleration (some limitations)
- Splunk 6: Create a Data Model and tick 'Accelerate'
- Timechart: last field appears on top
- Brush Palettes: custom brush colours / sizes / dashes / dots

# autoRun


NOOOOOOOOOO!
I HAVE MORE THAN ONE AUTORUN IN MY DASHBOARD
memegenerator.net

# Advanced Splunkage

- Chart Overlays :-

  http://answers.splunk.com/answers/9053/example-of-chart-overlay

- transaction vs stats :-

  http://answers.splunk.com/answers/103/transaction-vs-stats-commands

- Client-Side Splunk :-

  http://blogs.splunk.com/2013/02/07/client-side-splunk/

- httpstatus by Nimish Doshi :-

  http://blogs.splunk.com/2011/07/18/real-time-status/

# Use the Force

- Predict :-

  http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Predict

- Compare Two Time Ranges in One Report :-

  http://blogs.splunk.com/2012/02/19/compare-two-time-ranges-in-one-report/

  - There is a disturbance in the force - everything is time shifted, all the data is crammed at the end of the chart... you need:

    | makecontinuous _time

    http://answers.splunk.com/answers/56907/how-to-create-a-week-over-week-chart-comparison-from-current-time

# Build a chart of multiple data series

Splunk's reporting commands do not support a direct way to define multiple data series in your charts (or timecharts). However, you CAN achieve this using a combination of the **stats** and **xyseries** commands

Reference:

http://docs.splunk.com/Documentation/Splunk/latest/Search/Chartmultipledataseries

# Solution: Combine Two Field Names into One

```
index=sw sourcetype=episode_iv
(hostname=wookie metric=Inbound_ethernet0_0) OR
(hostname=ewok metric=Inbound_ethernet2_1)
| dedup _raw
| eval metric=hostname.":".metric
| streamstats current=t global=f window=2 earliest(value) as curr latest(value) as next by metric
| eval delta=next-curr
| eval gigabits=(delta*8/1000/1000/1000)
| timechart span=5m per_second(gigabits) as Gbps useother=f limit=0 by metric
| addtotals *ethernet*
| fields + Total
```

# Splunk Education

- Follow the Splunk Tutorial :-

  http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/WelcometotheSearchTutorial

- Watch Splunk Videos :-

  http://www.splunk.com/videos

  http://www.splunk.com/view/education-videos/SP-CAAAGB6

- Download Sideview Utils :-

  http://sideviewapps.com

# Splunk Books

- “Exploring Splunk” by David Carasso :-
  http://www.splunk.com/goto/book
- “Implementing Splunk: Big Data Reporting and Development for Operational Intelligence” by Vincent Bumgarner :-
  http://www.amazon.com/Implementing-Splunk-Operational-Intelligence-ebook/dp/B00AO2VXA0/ref=tmm_kin_title_0
- “Big Data Analytics Using Splunk: Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources” by Peter Zadrozny & Raghu Kodali :-
  http://www.amazon.com/Big-Data-Analytics-Using-Splunk/dp/143025761X

# Free Splunk Apps

- All your base are belong to us :-
  http://apps.splunk.com
- Splunk DB Connect :-
  http://apps.splunk.com/app/958
- Splunk for Nagios :-
  http://apps.splunk.com/app/352/
- Splunk for Postfix :-
  http://apps.splunk.com/app/933/

# Web Developers

- Use the Web Framework :-

  http://dev.splunk.com
- Download the Web Framework Toolkit
- Splunk SDKs :-
  - Python
  - Java
  - JavaScript
  - PHP
  - Ruby
  - C#

# Q&A

1/ Do you think the average stormtrooper knows how to install a toilet main?

A. All they know is killing and white uniforms.

2/ Were the contractors working on the uncompleted Death Star innocent victims when the space station was destroyed by the rebels?

A. Any contractor willing to work on that Death Star knew the risks. If they were killed, it was their own fault.

3/ Any other questions?

A. These aren't the droids you're looking for.