



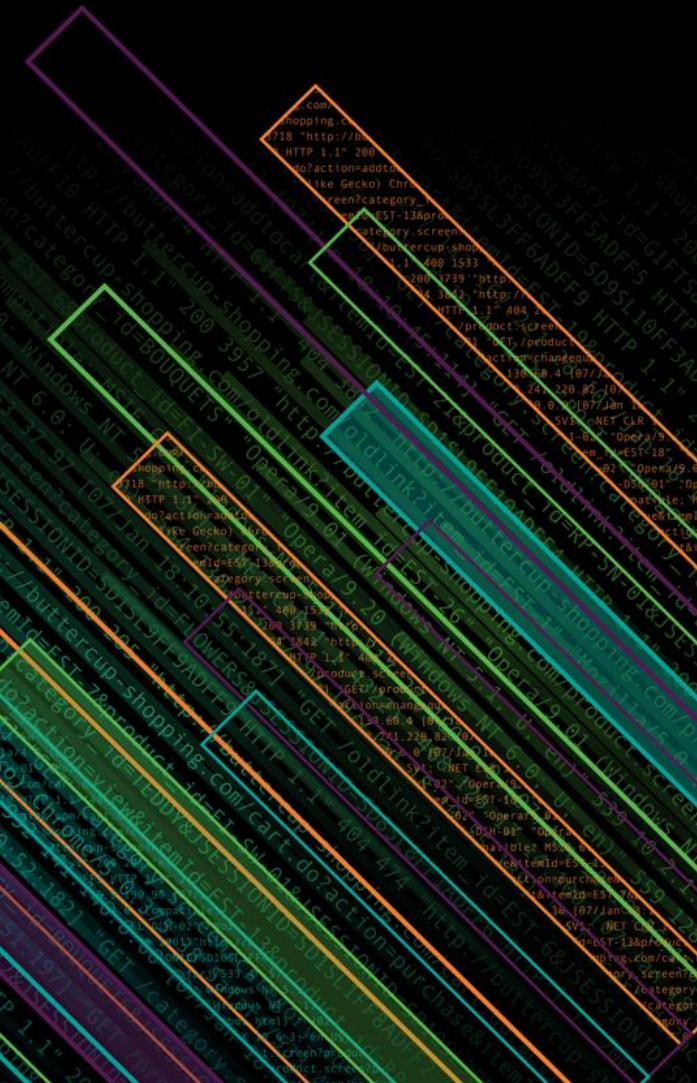
Splunk P30X: Become a lean, mean, Splunkin' machine in 30 days!

Session ID: 1611

Alan Ivarson – Splunk Staff Cloud Architect

Matt Portnoy – Splunk Senior Systems Engineer

October 2018 | Version 3.0



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

ALAN IVARSON

Staff Cloud Architect



MATT PORTNOY

Senior Sales Engineer



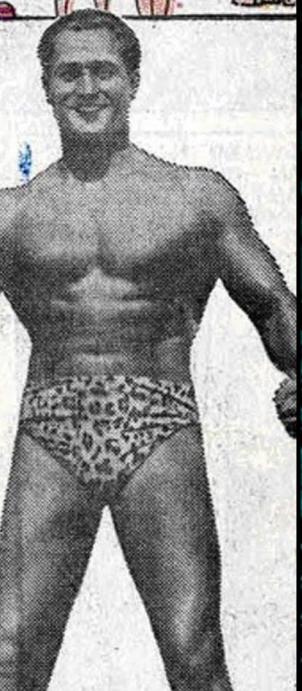
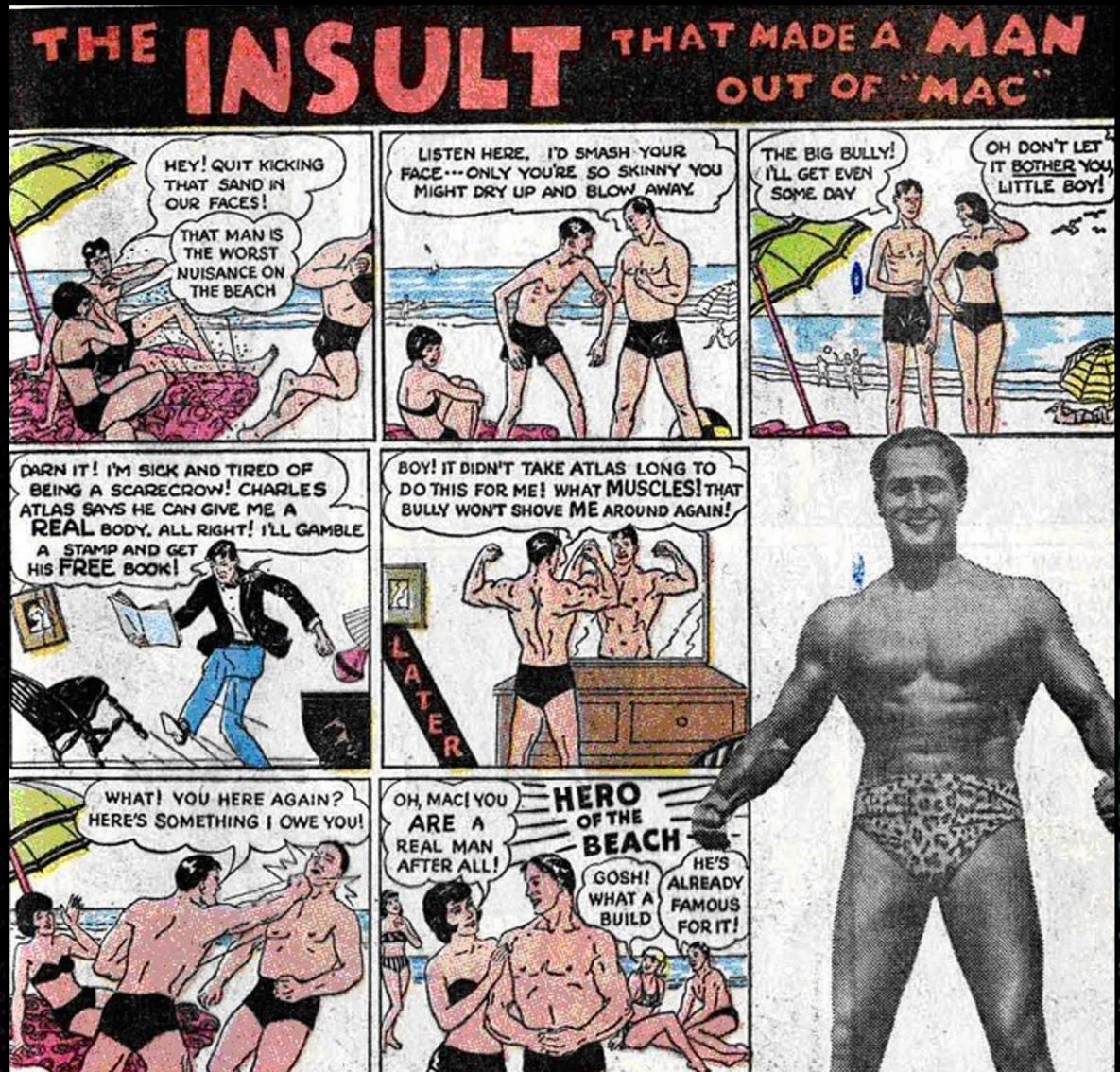


Results

The 30 Day Plan

Your Journey to Become a Lean, Mean, Splunkin' Machine

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	Splunk Install and Profile Configuration	Initial Config and Data Onboarding	Apps, Add-ons, and Sourcetype planning	Data Onboarding – Network Sourcetypes	Data Onboarding – Windows Data	
	Search and Reporting – Basic Search	Alerts	Dashboards	Loading Apps and Add-ons	Search and Reporting – Searching II	
	Splunk Fundamentals I Class – Modules 1 - 6	Splunk Fundamentals I Class – Modules 7 - 12	Knowledge Objects	Apps and Add-ons - II	Apps and Add-ons - III	Splunk your Car
	Dashboards - II	Alerts - II	Search and Reporting – Searching III	Create a Simple App	Dashboards - III	Splunk Your Thermostat
	Review Fundamentals I material	Splunk Core Certified User Test				



QuickStart

Everything you need to get started

Get a Splunk.com Account

Alan

Secure | https://www.splunk.com

Training Support Pricing Splunk Sites User

splunk > PRODUCTS SOLUTIONS CUSTOMERS PARTNERS RESOURCES ABOUT US

Free Splunk

Turn Machine Data Into Answers

Real-Time
Splunk gives you the real-time answers you need to meet customer expectations and business goals.
[See How Zillow is Taking Advantage](#)

Machine Data
Use Splunk to connect your machine data and gain insights into opportunities and risks for your business.
[Gain Answers With Machine Data](#)

Scale
Splunk scales to meet modern data needs — embrace the complexity, get the answers.
[Splunk Scales With Your Data](#)

AI and Machine Learning
Leverage artificial intelligence (AI) powered by machine learning for actionable and predictive insights.
[Learn About the Must Have Technology](#)

Contact Sales

Trusted by 89 of the Fortune 100

Zillow Coca-Cola AAA HYATT More Customers

New Account OR Login

The image shows a laptop displaying the Splunk website. The main content area features three sections: "Real-Time" (represented by a clock icon), "Machine Data" (represented by a gear icon), and "Scale" (represented by a bar chart icon). Below these sections, there are links to "See How Zillow is Taking Advantage" and "Gain Answers With Machine Data". At the bottom, a banner states "Trusted by 89 of the Fortune 100" and lists logos for Zillow, Coca-Cola, AAA, and others. To the right of the main content, a modal window titled "Get Started With Splunk OR" is open. It contains fields for "First Name", "Last Name", "Job Title", "Email Address", "Phone Number", "Company", a dropdown menu for "United States", a field for "Zip/Postal Code", and a field for "Username". A red arrow points to the "Login" button inside the modal. The top navigation bar includes links for PRODUCTS, SOLUTIONS, CUSTOMERS, PARTNERS, RESOURCES, and ABOUT US. The URL in the address bar is https://www.splunk.com.

Get Started With Splunk OR

Already Have a Splunk Account? [Login](#)

First Name

Last Name

Job Title

Email Address

Phone Number

Company

United States

Zip/Postal Code

Username

Alan

Secure | https://www.splunk.com

splunk > PRODUCTS SOLUTIONS CUSTOMERS PARTNERS RESOURCES ABOUT US

Turn Machine Data Into Answers

Real-Time

Machine Data

Scale

See How Zillow is Taking Advantage

Gain Answers With Machine Data

Splunk Scales With Your

Trusted by 89 of the Fortune 100

Zillow Coca-Cola AAA

www.splunk.com/download

The screenshot shows a laptop displaying the Splunk website at https://www.splunk.com/en_us/download.html. The page is titled "Splunk Platform Products" and features four product offerings: Splunk Enterprise, Splunk Cloud, Splunk Light, and Splunk Free. Each product has a brief description and a call-to-action button. A large red button labeled "easy" is prominently displayed in the center of the page.

Secure | https://www.splunk.com/en_us/download.html

Training Support Pricing Splunk Sites Alan

splunk > PRODUCTS SOLUTIONS CUSTOMERS PARTNERS RESOURCES ABOUT US

Free Splunk

Splunk Platform Products

Download the free trials of our core Splunk® solutions and see first-hand the benefits it can bring to your organization

 **Splunk Enterprise**
The fastest way to aggregate, analyze and get answers from your machine data

[Download Free 60-Day Trial](#)

 **Splunk Cloud**
No infrastructure, no problem —aggregate, analyze and get answers from your machine data

[Access Free 15-Day Trial](#)

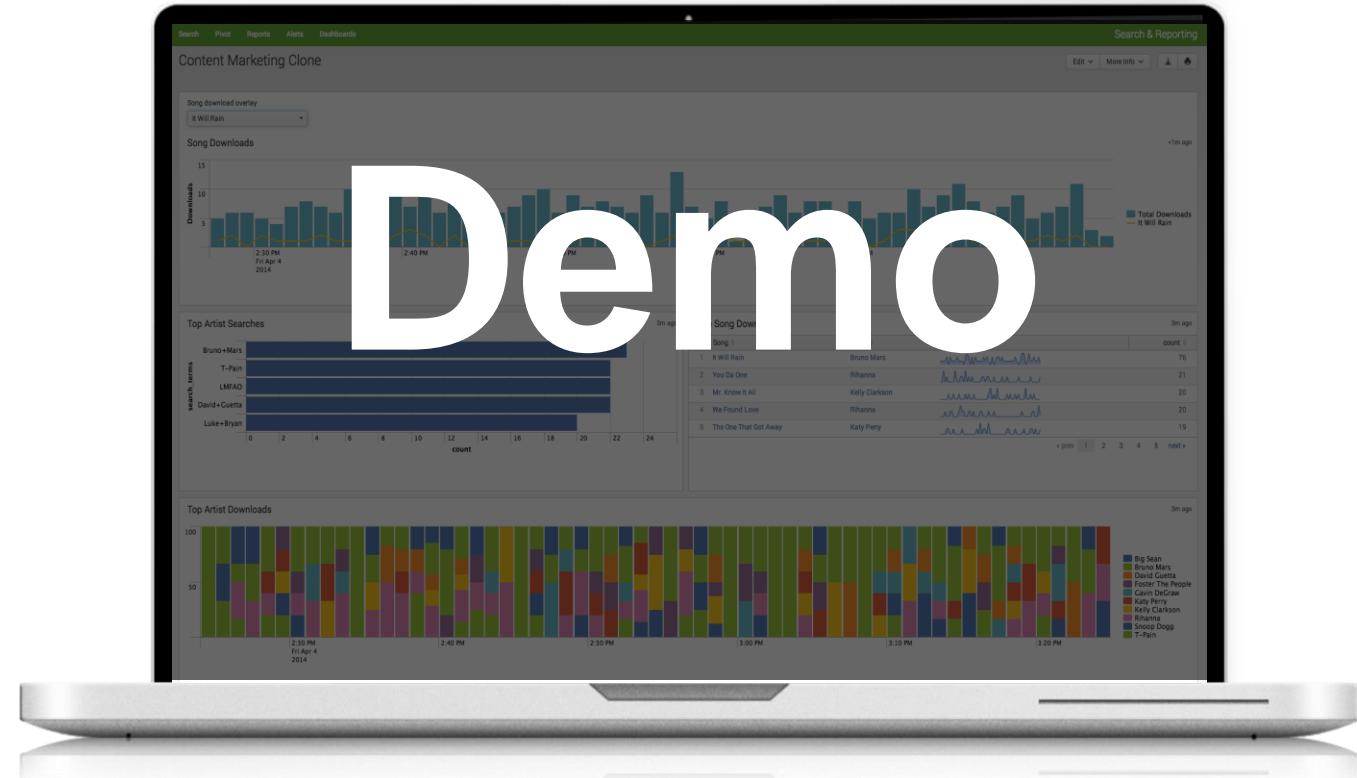
 **Splunk Light**
Search, report and alert on all your log data in real time from one place

[Download Free 30-Day Trial](#)

 **Splunk Free**
A free sample of our core enterprise platform

[Download](#)

easy



Demo



Warm Up!

Settings, Add Data

The screenshot shows the Splunk Enterprise web interface. On the left, there's a sidebar titled "splunk>enterprise" with a "Apps" section containing various icons and names like "Search & Reporting", "Splunk Dashboard Examples", etc. In the center, there's a "Explore Splunk Enterprise" section with a "Product Tours" icon and a "New to Splunk? Take a tour to help you on your way." message. To the right, there's a navigation bar with "Administrator", "Messages", "Settings" (which is highlighted with a red box), "Activity", "Help", and a search bar. Below the navigation bar is a large menu with sections like "KNOWLEDGE", "DATA", "DISTRIBUTED ENVIRONMENT", "SYSTEM", and "USERS AND AUTHENTICATION". Under "DATA", there are links for "Data inputs", "Forwarding and receiving", "Indexes", etc. Under "KNOWLEDGE", there are links for "Searches, reports, and alerts", "Data models", "Event types", etc. A red box highlights the "Add Data" link under the "DATA" section. Another red box highlights the "Add Data" link in the main menu. The word "OR" is placed between the two highlighted "Add Data" links. Below the menu, there's a "Monitoring Console" section and a "Choose a home dashboard" section with a chart icon.

Upload

splunk>enterprise Apps ▾

H Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data

How do you want to add data?



Upload
files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data ↗](#)



Monitor
files and ports on this Splunk indexer

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward
data from Splunk forwarder

Files - TCP/UDP - Scripts

Splunk can index any machine data. Common data sources are:

 STRUCTURED DATA	 MICROSOFT INFRASTRUCTURE	 NETWORK & SECURITY
CSV	Exchange	Syslog & SNMP
JSON	Active Directory	Cisco Devices
XML	Sharepoint	Snort

 WEB SERVICES	 DATABASE SERVICES	 CLOUD
Apache	Oracle	AWS Cloudtrail
IIS	MySQL	Amazon S3
	Microsoft SQL Server	Azure

 IT OPERATIONS	 VIRTUALIZATION	 APPLICATION SERVICES
Nagios	VMWare	JMX & JMS
NetApp	Xen Decider	WebLogic

Featured apps

Many Splunk apps and add-ons will add data for you
[See more Splunk Apps ↗](#)


***nix**


WIN


DB


REST


JMX


CISCO

Did you know?

You can index just about anything with Splunk.
[Learn More ↗](#)

Having trouble finding data you added in Splunk?

Upload tutorialdata.zip file

splunk>enterprise Apps ▾

H Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data

Select Source Input Settings Review Done

< Back Next >

Select Source

Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

⚠ Preview is not supported for this archive file, but it can still be indexed.

Selected File: **tutorialdata.zip** 

Select File

Drop your data file here

The maximum file upload size is 500 Mb

FAQ

- › What kinds of files can Splunk index?
- › What is a source?
- › How do I get remote data onto my Splunk instance?

Input settings according to documentation

The screenshot shows the Splunk Enterprise interface with the title "Input settings according to documentation". The top navigation bar includes "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", and "Help". Below the title, a progress bar shows "Add Data" with four steps: "Select Source" (green dot), "Input Settings" (green dot), "Review" (white circle), and "Done" (white circle). A red box highlights the "Review >" button. The main content area is titled "Input Settings" and contains the following sections:

- Source type**: Describes the source type as a default field assigned by Splunk. It explains that it tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. A red box highlights the "Automatic" button.
- Host**: Describes how each event receives a "host" value. It states that the host value should be the name of the machine from which the event originates. A red box highlights the "Segment in path" radio button and the "Segment number?" input field, which contains the value "1".
- Index**: Describes how Splunk stores incoming data as events in the selected index. It suggests using a "sandbox" index as a destination if you have problems determining a source type for your data. A red box highlights the "Index" dropdown set to "Default" and the "Create a new index" link.

**Different on Windows
Follow docs!**

Validate Settings

splunk>enterprise Apps ▾

H Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

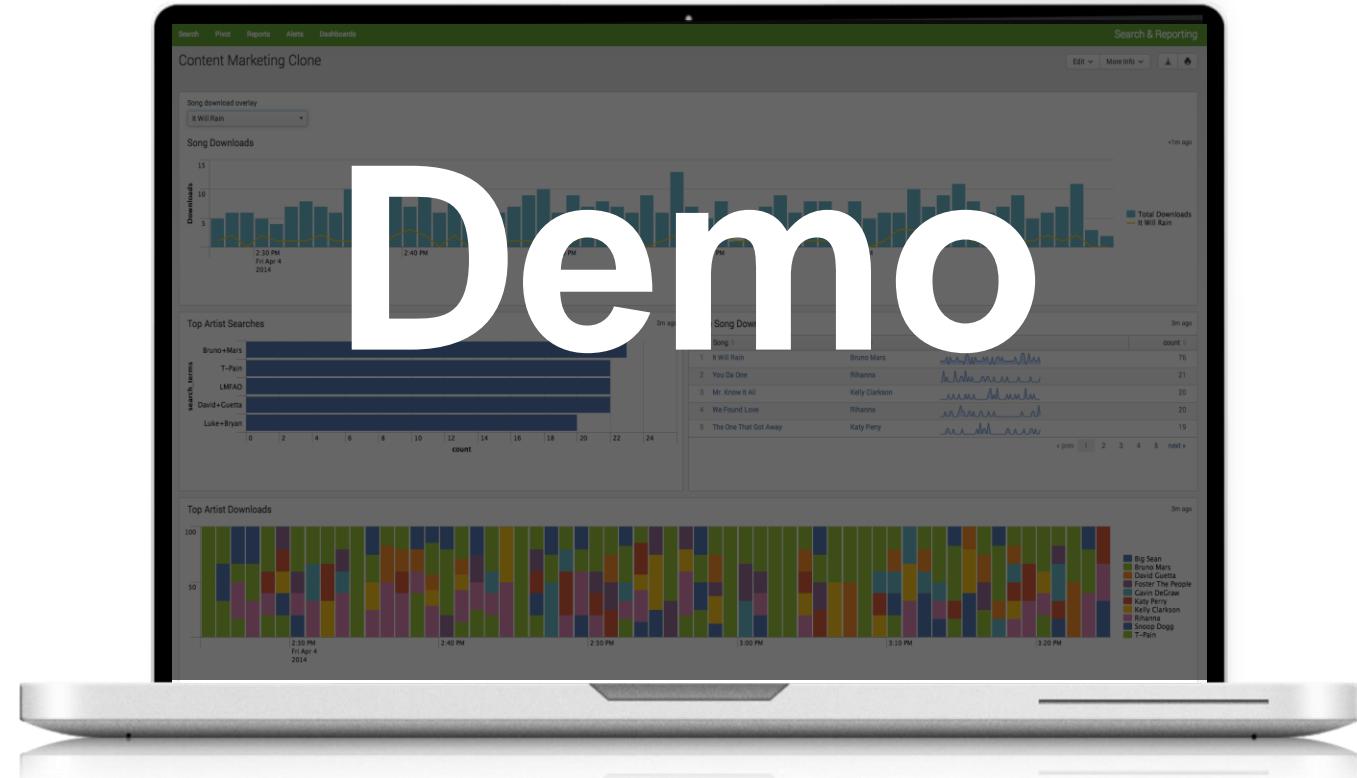
Add Data

Select Source Input Settings Review Done

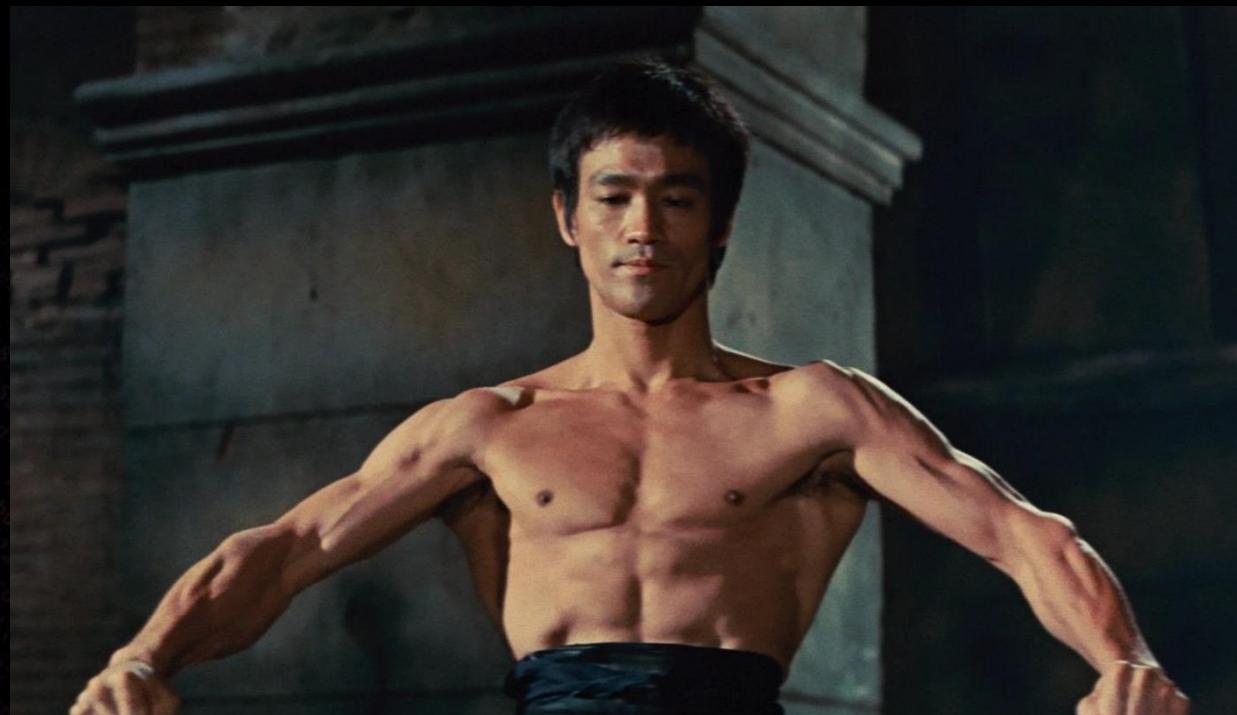
Submit >

Review

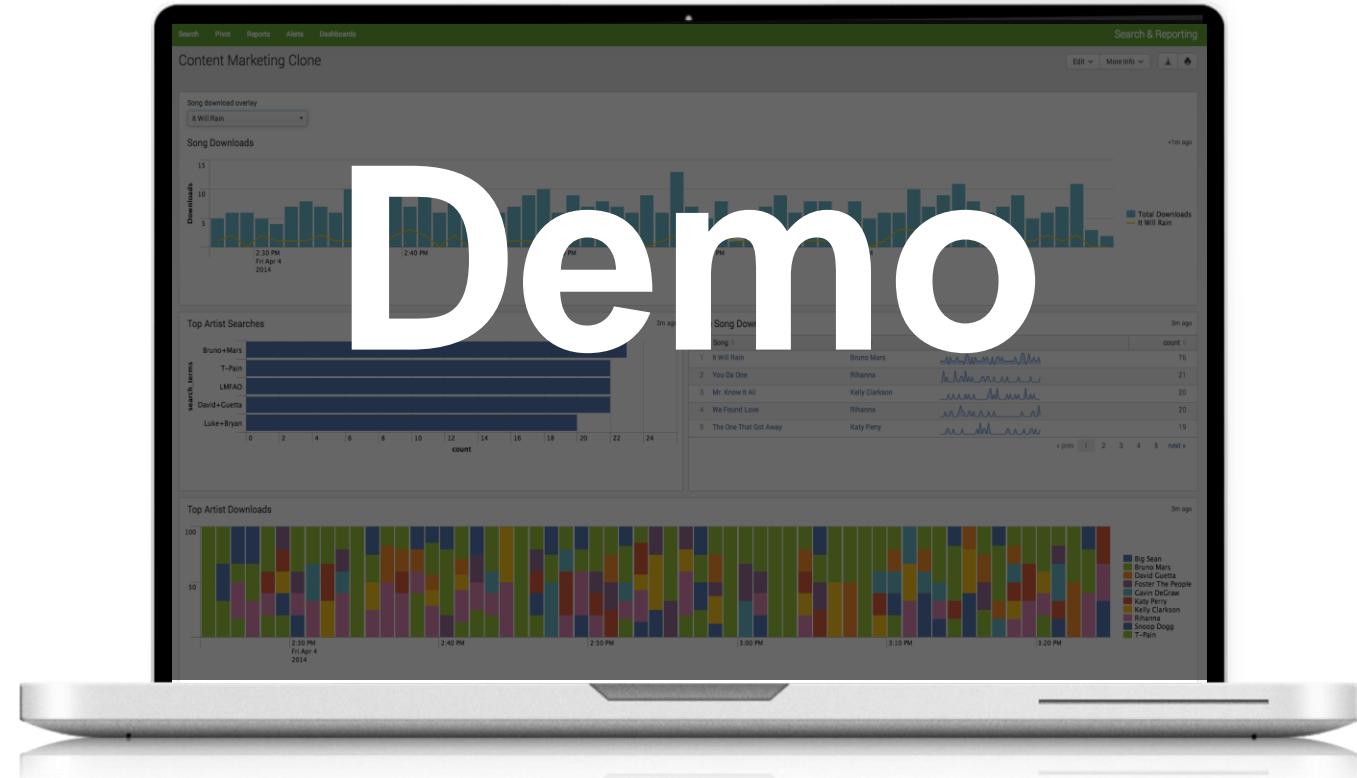
Input Type Uploaded File
File Name tutorialdata.zip
Source Type Automatic
Host Source path segment number: 1
Index Default



Demo



Exercise Set #1



Demo



Exercise Set #2

The Splunk Data Onboarding

splunk>enterprise

splunk>cloud™

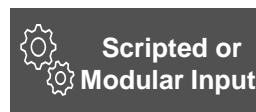
splunk® Platform for Operational Intelligence



Unix, Linux, Mac
and Windows
Hosts,
web logs,
file monitoring



Syslog hosts and network devices



Shell Scripts and APIs



HTTP Event Collector



Splunk App for Stream



HEC and Web logs

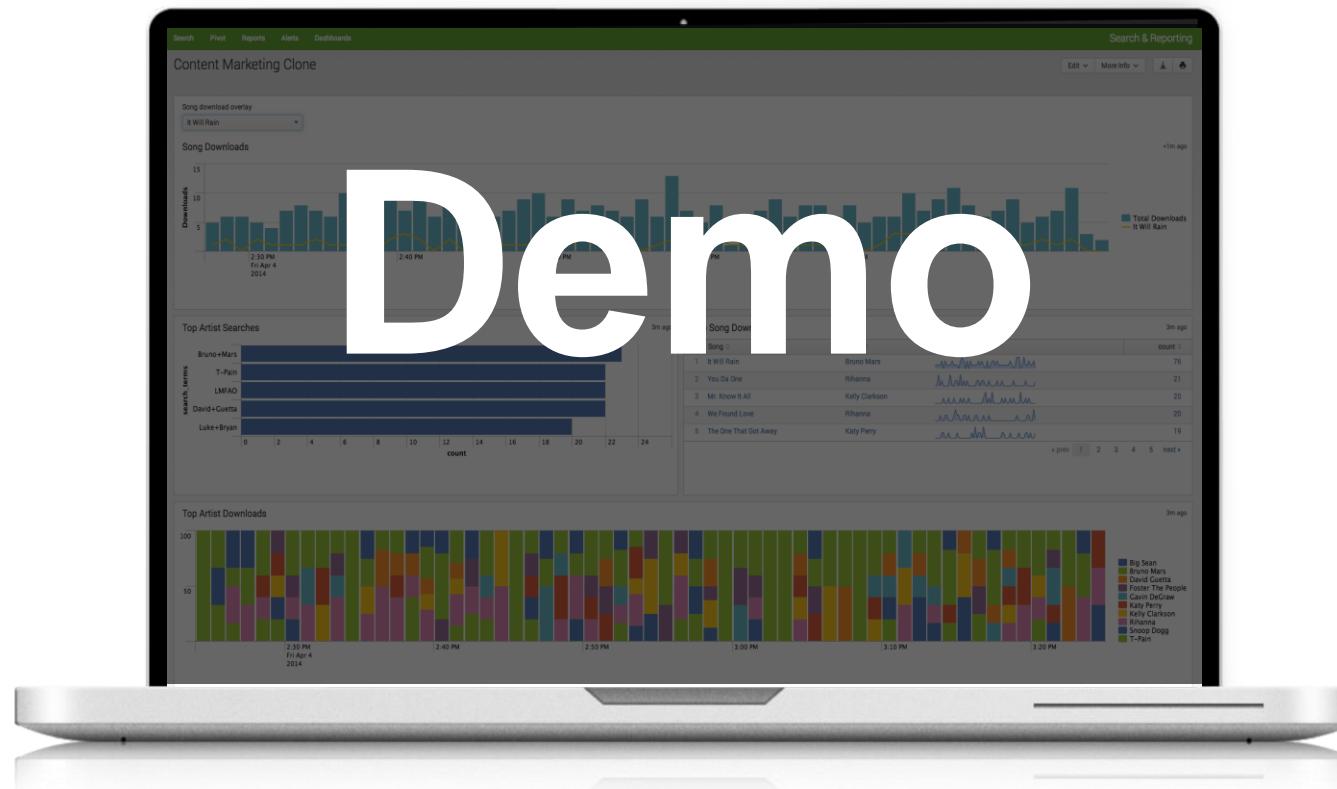


DB Connect



3rd party and File monitoring

Demo



Level Up and Cool Down!

What's next after you master this?



Next Steps

- ▶ Deployment Server
 - ▶ Distributed Architecture
 - ▶ Certifications
 - Splunk Core Certified User
 - Splunk Core Certified Power User
 - Splunk Enterprise Certified Admin
 - Splunk Enterprise Certified Architect (advanced)



References

GO TO ► <http://bit.ly/1611goodies>

- ▶ Splunk Documentation ([link](#))
 - ▶ Additional Sites
 - Go Splunk
 - Splunk Answers
 - REGEX101.com
 - Blog(s)
 - ▶ Reference document ([link](#))
 - ▶ Tutorial Data Exercise ([link](#))
 - ▶ SPL reference sheets ([link](#))
 - ▶ Dashboarding reference sheet ([link](#))
 - ▶ On-line book ([link](#))
 - ▶ The 30 day plan ([link](#))



The 30 Day Plan

Your Journey to Become a Lean, Mean, Splunkin' Machine

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	Splunk Install and Profile Configuration	Initial Config and Data Onboarding	Apps, Add-ons, and Sourcetype planning	Data Onboarding – Network Sourcetypes	Data Onboarding – Windows Data	
	Search and Reporting – Basic Search	Alerts	Dashboards	Loading Apps and Add-ons	Search and Reporting – Searching II	
	Splunk Fundamentals I Class – Modules 1 - 6	Splunk Fundamentals I Class – Modules 7 - 12	Knowledge Objects	Apps and Add-ons - II	Apps and Add-ons - III	Splunk your Car
	Dashboards - II	Alerts - II	Search and Reporting – Searching III	Create a Simple App	Dashboards - III	Splunk Your Thermostat
	Review Fundamentals I material	Splunk Core Certified User Test				

Q&A

Alan Ivarson | Splunk Staff Cloud Architect
Matt Portnoy | Splunk Senior Sales Engineer

Thanks!

Don't forget to rate this session
in the .conf18 mobile app

