Guerrilla Marketing

How to sell Splunk internally to your Enterprise

Aaron Blythe

Knowledge Architect, Cerner Corporation

splunk>

Disclaimer

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 the 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.

Aaron Blythe

http://aaronblythe.org/

- Writing Code
- Answering questions

splunk>answers

freenode

- Running Meetups

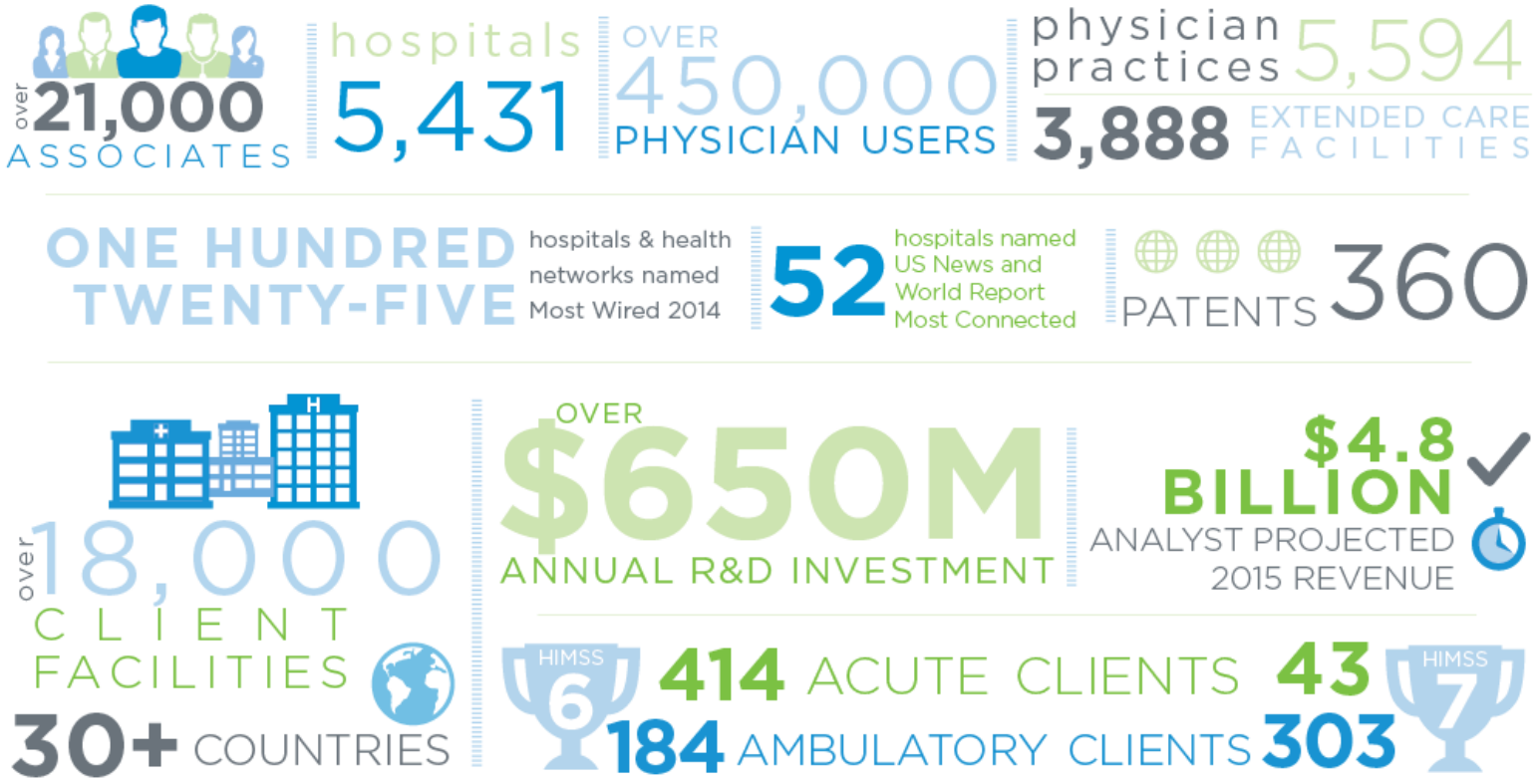
Meetup

Health care is too important to stay the same.™

Cerner™

The solution that started it all

Cerner today



Population health management

Connect

Empower

Facilitate

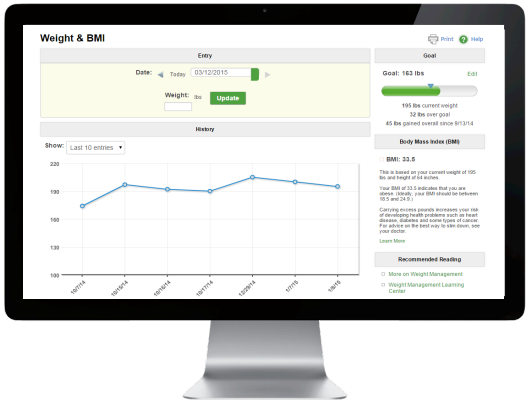
Move from reactive care to proactive health

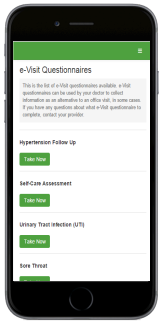
Member engagement across the spectrum

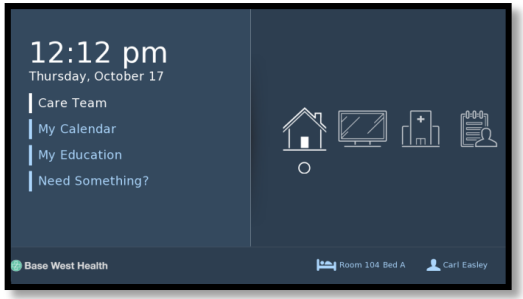
HOME

WORK

HOSPITAL







Cerner's success

#4

Top 100 Healthiest Workplaces in America

5-year results

- Lowered premium increases
  - 1.6% vs. 7-10% national average
- Decreased risk factors
- Improved biometric screening results

Agenda

- Know who you are
- Make things surprisingly easy
- Gather endorsements
- Be helpful in many mediums
- Promote your community
- Create champions
- When all else fails, hold a contest

"I'm referring to the soul and essence of guerrilla marketing which remain as always —

achieving conventional goals, such as profits and joy, with unconventional methods, such as investing energy instead of money."

.conf2015

Know Who You Are

splunk>

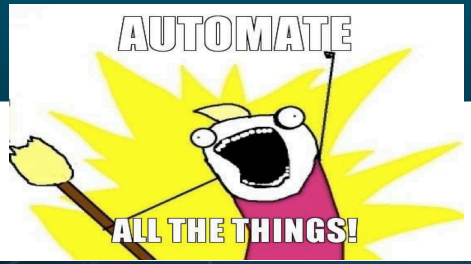
2015 we believe

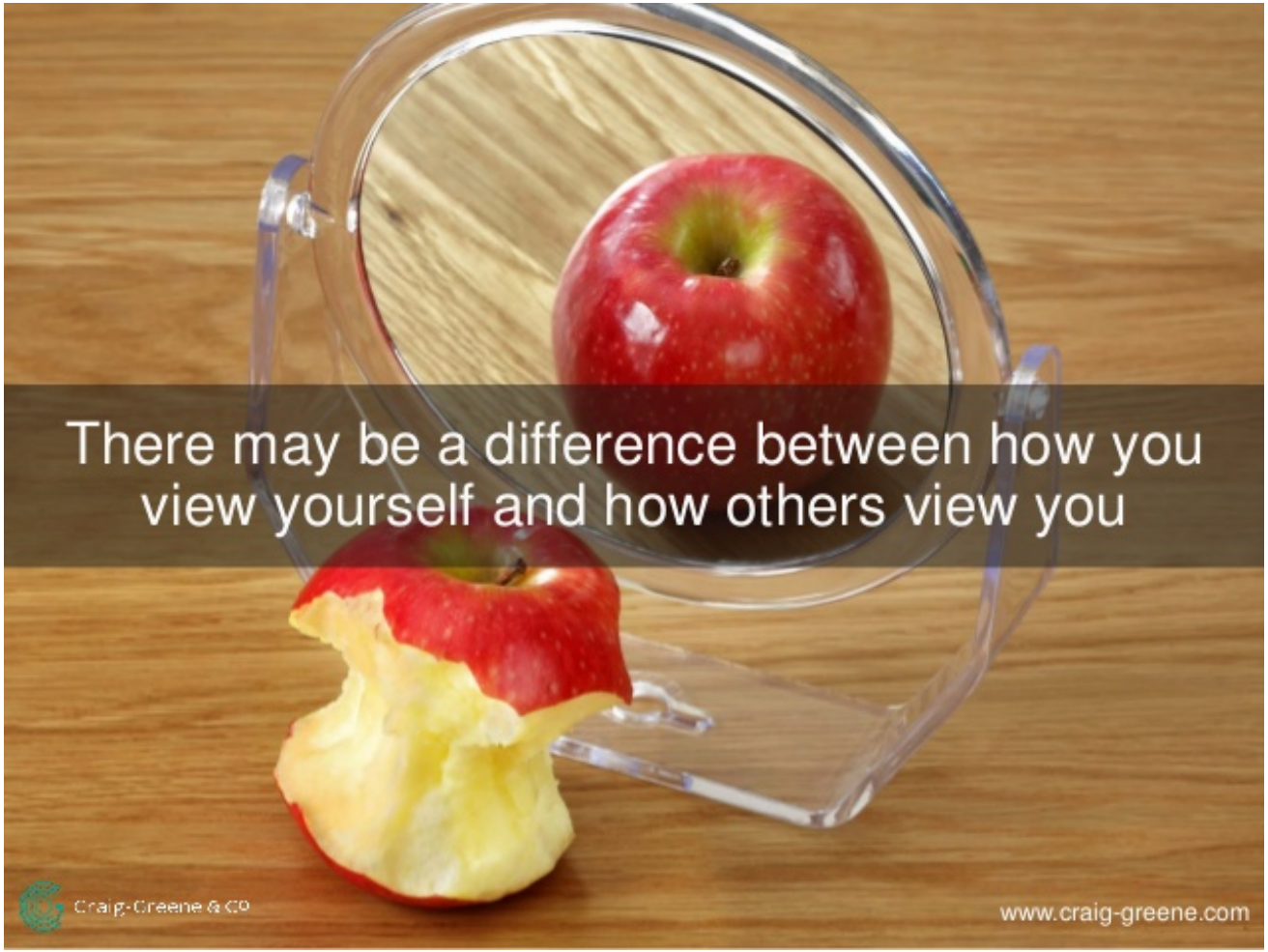
- Enable self services
- Transparency leads to better service
- Everything in source control

- Cerner OpsInfra Team

2014 we believe…

- A minimal number of associates need to directly touch nodes (approaching zero)
- These tools matter – improve the lives of our users
- Tools should be hardened - so that we can find the root cause and drive corrective action




There may be a difference between how you view yourself and how others view you
Craig-Greene & Co
www.craig-greene.com

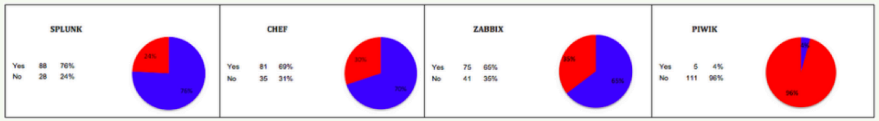
Surveys

- Use Google Docs FTW!!!

Be transparent

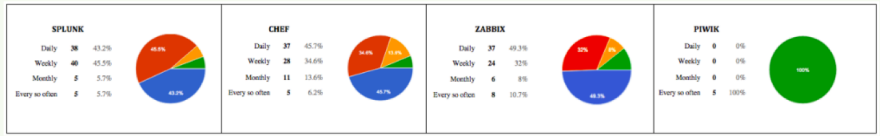
Of the responders, 44% identified themselves as Developers, 34.5% identified themselves as Operations, 4.3% identified themselves as neither and 17.2% identified themselves

Active Users:



Experience Levels:

Usage:



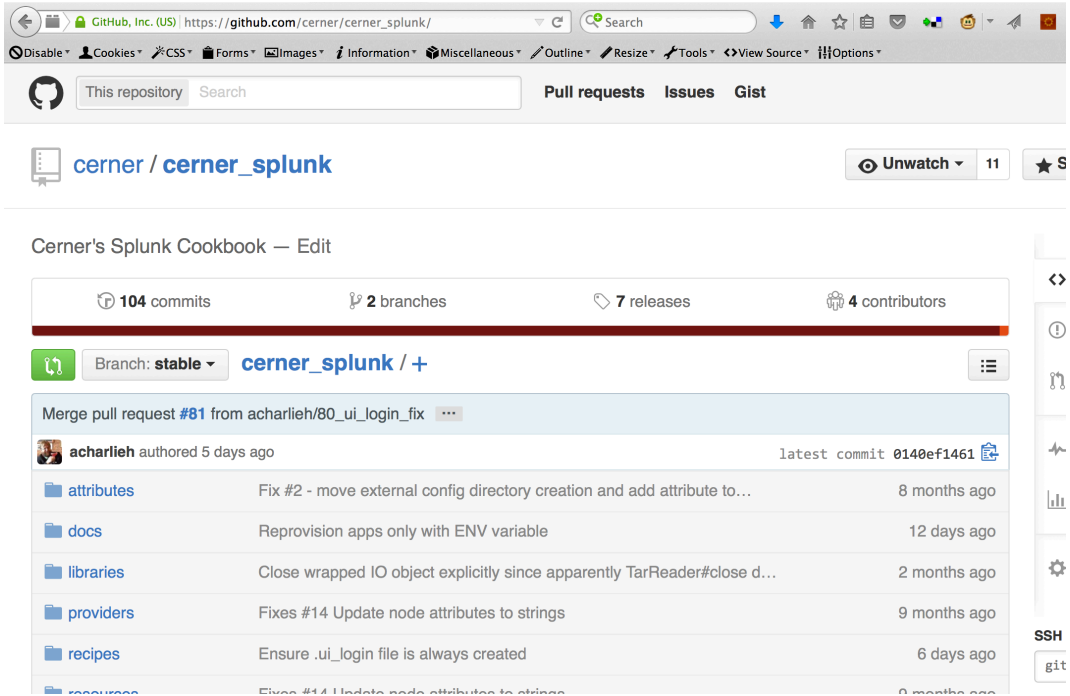
General Impressions:

.conf2015

Make Things Surprisingly Easy

splunk>

Chef cookbook



What we need

- 1 hour meeting
- Person in the room with:
  - troubleshooting knowledge of application (which logs are valuable)
  - root access to the node (so we can bootstrap Chef)
  - knowledge of Splunk and Chef (someone from my team)

Steps

- Bootstrap nodes to Chef with Cerner_Splunk role on run list
- Run chef-client on nodes

Hide everything but the details

Chef Role

```
name 'ipfactory_jira_logs'

description 'Forwards Jira log files to splunk'

run_list 'recipe[cerner_splunk]'

# Monitors the Chef Server logs for many concerns.
# Update accordingly if those attributes are overridden.

default_attributes(
  splunk: {
    monitors: [
      {
        path: '/jira/install/latest/logs/catalina.out',
        sourcetype: 'log4j'
      },
      {
        path: '/jira/install/latest/logs/access_log.*',
        sourcetype: 'access_combined'
      }
    ]
  }
)
```

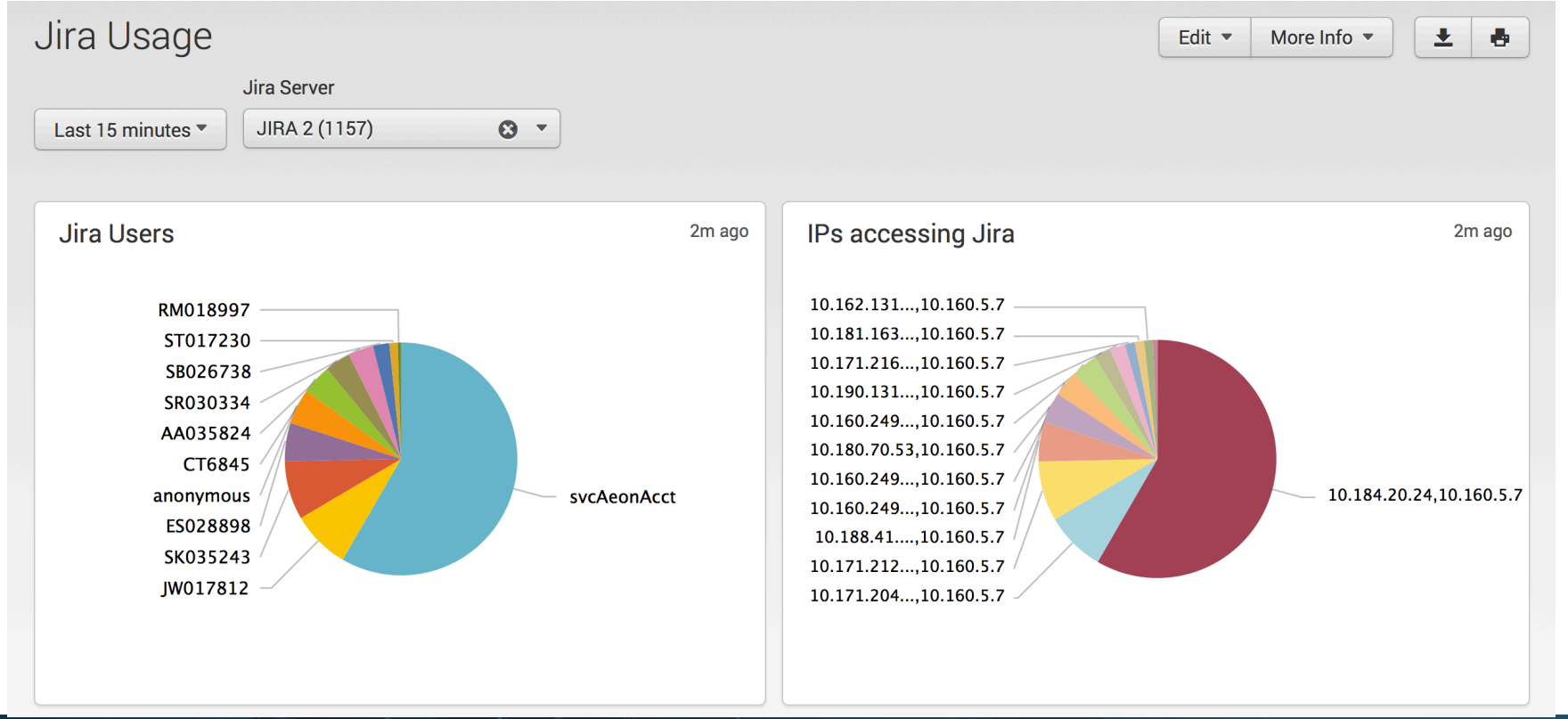
Chef Environment

```
name 'ipfactory_corporate'
description 'IP Factory for the Development (Corporate) Environment'

cookbook_versions( {
  cerner_splunk: '>= 1.0.0'
} )

default_attributes(
  # Splunk
  splunk: {
    config: {
      clusters: [
        'cerner_splunk/corporate_tools_cluster'
      ]
    },
    main_project_index: 'ipfactory',
    package: {
      base_url: 'http://repo.release.cerner.corp/nexus/content/sites/splunk/releases'
    }
  }
)
```

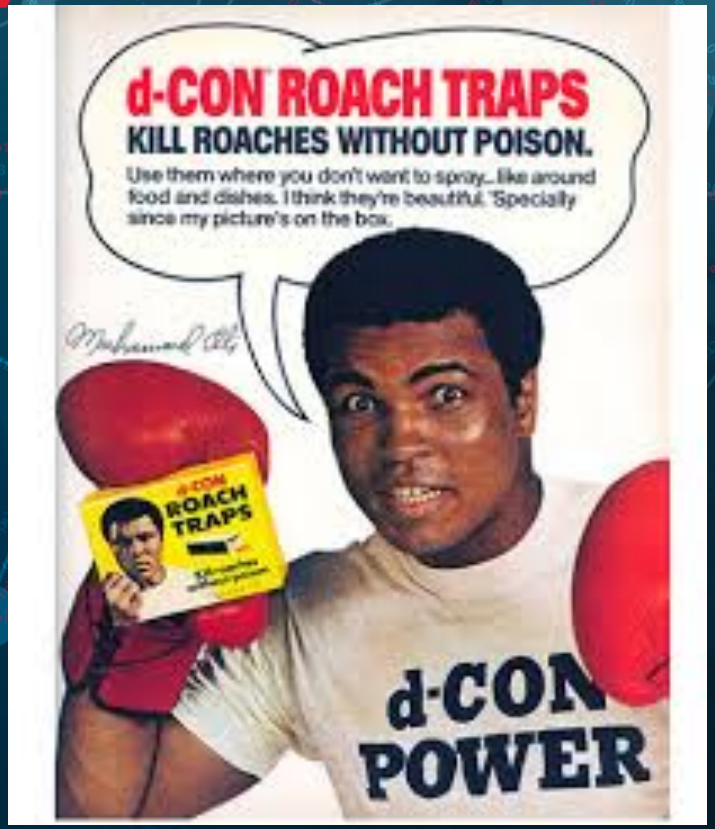
Jira usage


Jira Usage
Edit
More Info
Jira Server
Last 15 minutes
JIRA 2 (1157)
Jira Users
2m ago
RM018997
ST017230
SB026738
SR030334
AA035824
CT6845
anonymous
ES028898
SK035243
JW017812
svcAeonAcct
IPs accessing Jira
2m ago
10.162.131...,10.160.5.7
10.181.163...,10.160.5.7
10.171.216...,10.160.5.7
10.190.131...,10.160.5.7
10.160.249...,10.160.5.7
10.180.70.53,10.160.5.7
10.160.249...,10.160.5.7
10.160.249...,10.160.5.7
10.188.41....,10.160.5.7
10.171.212...,10.160.5.7
10.171.204...,10.160.5.7
10.184.20.24,10.160.5.7

Not top down

- Is this the right thing to do?
- Will it take very much index?

.conf2015



Gather Endorsements

splunk>

Creating allies

Splunk has played a vital role in stabilizing our **Jira** environments. In what would have taken weeks of manual correlation and analysis can be summarized in Splunk in matter of minutes.

For example we were able to identify a server was excessively calling our server, then moving straight from that to the URI's that the server was accessing. We were able to contact the team that was abusing our service and they were able to scale back their web calls correcting our slowness issue. **Without Splunk I feel that this process would have taken weeks to discover, if at all.** This is saving my team time in investigation, not to mention the time of all other associates by resolving this slowness issue quicker.

Joe Hostler
System Engineer, CWx Emerging Technology Services

Document the nice things

Splunk Endorsements

Last edited by Thomas,Leslie on Apr 30, 2015 (view change)

- Splunk User Endorsements
  - Population Health
  - IP Development - Cloud Application Dev
  - DeviceWorks
  - IP Factory - JIRA
  - Millennium Backend
  - Revenue Cycle Development
  - Member Portal
  - RevWorks

Splunk User Endorsements

Population Health

> *I'm generally very conservative in talking about tooling that solves problems in magically ways, especially in the context of leadership meetings and the like, but I've always found the results of Splunks usage counter-intuitive. Without drilling into the details of the drivers, Splunk is pretty close to the ultimate Cerner tool in my estimation — if you have a system that can produce text files (e.g. Logs) or just have text files, it can be ingested into Splunk in an automated fashion and Splunk makes it browseable, parsable and computable in a myriad of ways with very little work. For better or worse, it is a universal tool that can be finessed to do just about anything. I would put it on par with other associate favorites like Excel and PowerPoint.*
>
> *Nathan Beyer*
> *Distinguished Engineer & Senior Principal Architect, Population Health Dev*

.conf2015

Be Helpful in Many Mediums

splunk>

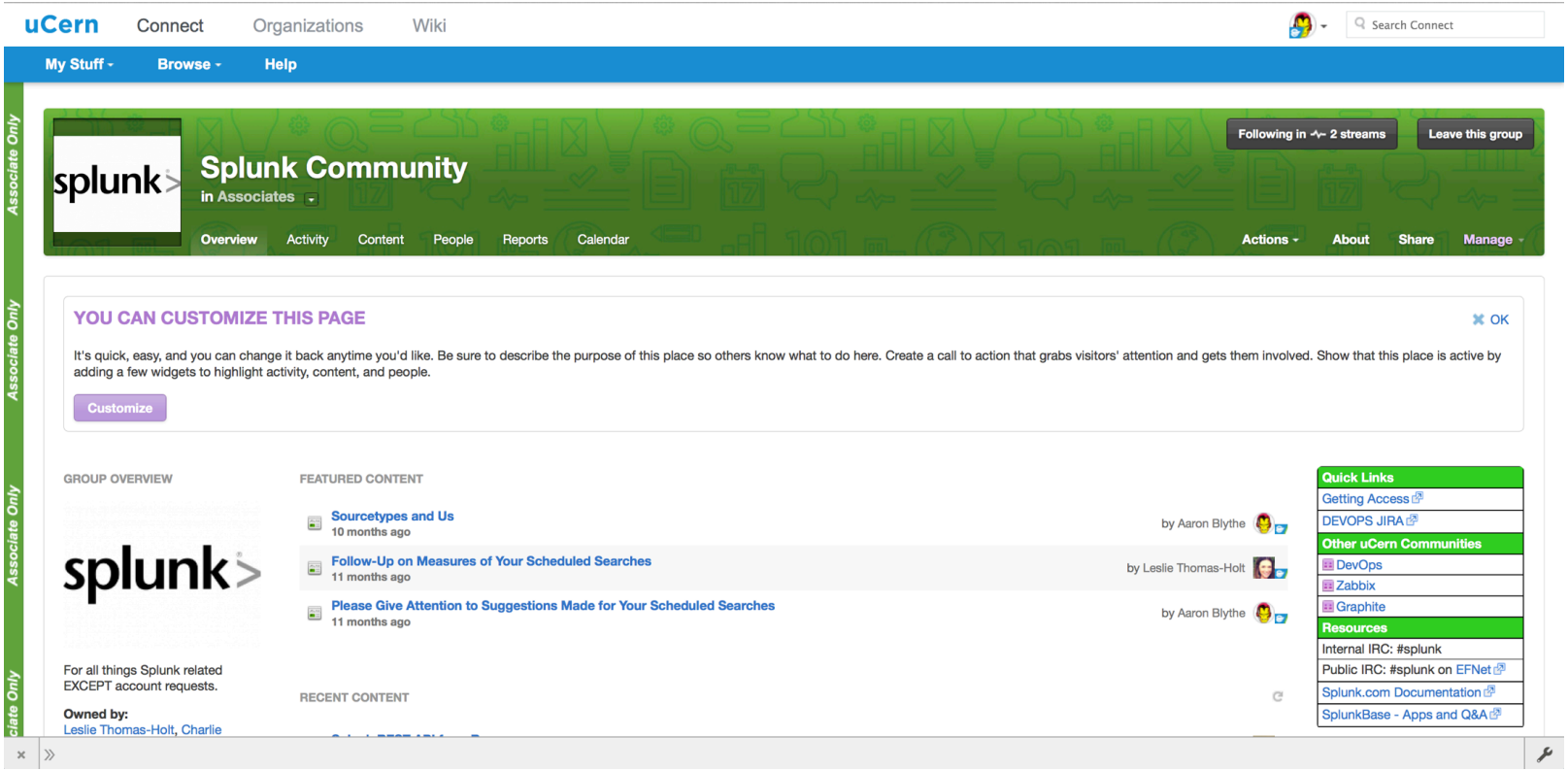
Go to where the users are asking questions

Internal logs in Splunk

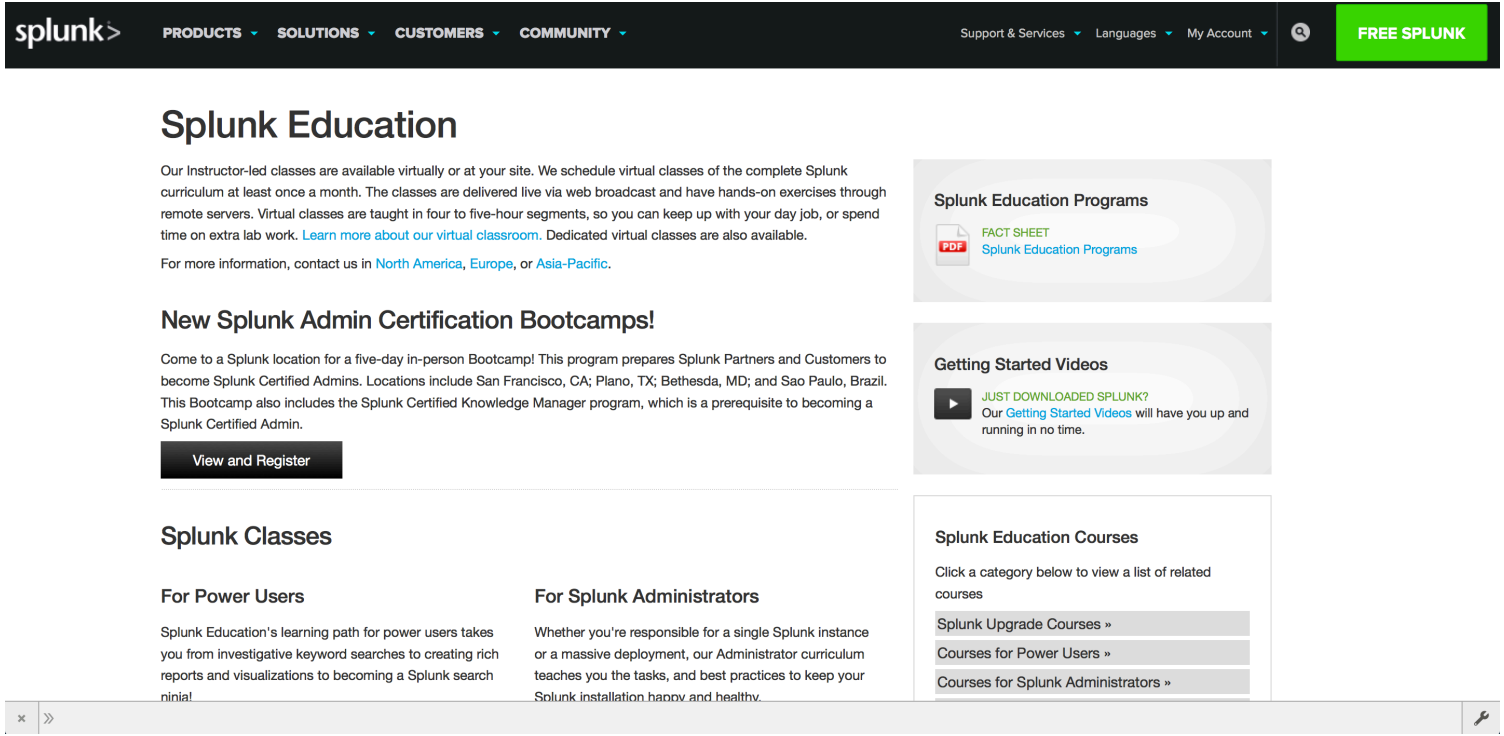
Internal logs not in Splunk

External

Provide a place to discuss



Provide education

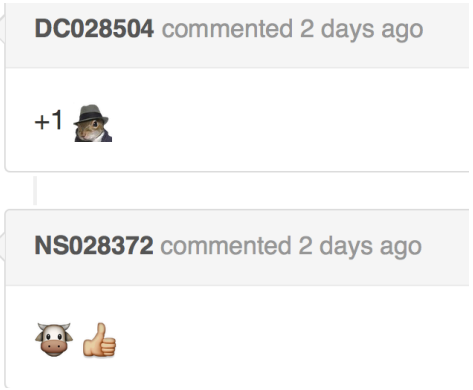


.conf2015

Promote your community

splunk>

Encourage



award points ·

Seize the Opportunity

- Meetups
- Conferences

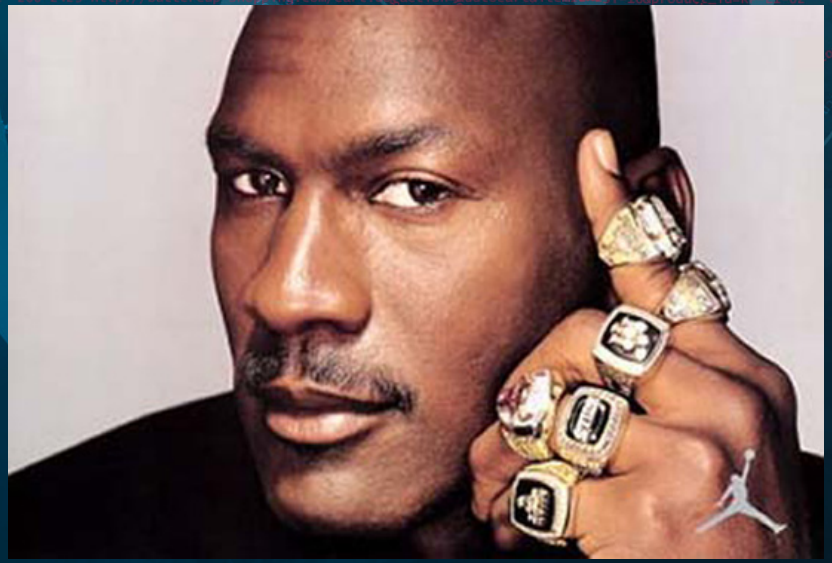
Internal Conferences

- DevCon 2012 – 1 talk
- DevCon 2013 – 0 talks on Splunk

- Started Opsinfra team

- DevCon 2014 - 1 talk from Opsinfra team
- DataCon 2014 – 1 talk from Opsinfra team
- DevCon 2015 – 3 talks (1 from Opsinfra team)
- DataCon 2015 - 3 talks (1 from Opsinfra team)

.conf2015



Create Champions

splunk>

Garry Polley

- Canadarm – Open Source Project
- Configurable JavaScript collection
- Send information back to Splunk

http://engineering.cerner.com/blog/javascript-logging-we-can-do-better/

Rima Poddar

- Defined and explained eventtype usage
- Prototyped first working alerting sub-system

http://engineering.cerner.com/blog/managing-30000-logging-events-per-day-with-splunk/

Mike Hemesath

- Defined and explained eventtype usage
- First major use of pivot tables
- Many internal presentations to other teams and leadership
- Push for standardization

http://engineering.cerner.com/blog/managing-30000-logging-events-per-day-with-splunk/

Hold a Contest

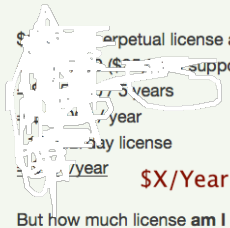
splunk>

Splunk Value Contest

Posted by Leslie Thomas-Holt in DevOps on Aug 10, 2015 12:09:20 PM

We've heard our users are finding value in Splunk, now's your chance to tell us about it!

On OpsInfra we are frequently asked by teams how much Splunk license they are consuming and the associated cost. After some rough estimating



But how much license **am I** using per day you might ask? We're excited to announce that we now have a dashboard available for you to determine h

- https://logs-license.cerner.com/en-US/app/search/usage_per_role

For more information on understanding and utilizing this dashboard see: Splunk Usage Per Role Dashboard Tutorial

Contest Guidelines: OpsInfra will be hosting a contest running from today, August 10, 2015 through August 14, 2015 in which we are asking Splun and multipliers. **The team(s) with the best cost/savings ratios will win!**

Please submit a doc with this information to the Splunk Value Competition uCern Group by 5:00PM on August 14, 2015.

- EXAMPLE: Splunk Value Contest Submission - HealtheLife (Personal Health)

What's in it for you?

- 1st Place will receive pizza for lunch for themselves and their team/coworkers (Limit 5 Large Pizzas)
- 2nd Place will receive donuts to share with their teams/coworkers (Limit 2 Dozen Donuts)
- 3rd Place will receive candy/chocolate to share (or not share!)
- All participants will receive some Splunk Swag!

279 Views Tags (edit):

Usage Per Role

Explore Splunk Usage per Role

Edit More Info

Select a role

Last 14 days | personal_health

Average personal_health Usage

<1m ago

1.355
GB/DAY

Assuming Same Average Usage, Estimated License Cost for personal_health

<1m ago

$
PER YEAR

Available License

1m ago

400
GB/DAY

Percentage used by all roles

1m ago

78.72%

Percentage used by personal_health

<1m ago

0.34%

Usage in GB/day for "personal_health" versus Everyone Else

<1m ago

personal_health Index Usage Breakdown

<1m ago

Index	Environments	Cost	Num Days	Average	Max	Min	90%	95%	Std. Dev

EXAMPLE: Splunk Value Contest Submission - HealtheLife (Personal Health)

Created by Leslie Thomas-Holt on Aug 7, 2015 12:04 PM. Last modified by Leslie Thomas-Holt on Aug 7, 2015 3:48 PM.

- Defects closed won't fix- 1 defect closed per quarter due to Splunk analysis. 2 engineering weeks per defect
  - 2 engineer months = 1/6 * [redacted]
- Faster SR Investigation - 200 SRs per month, 1 hour faster investigation per SR. 200 hours per month. 50 hours per week
  - 50 hours per week = 1.1 FTE [redacted]
- Faster Incident Investigation - 1 incident per quarter, 1-2 hour per incident faster resolution, 5 people per incident
  - 5 person hours per quarter [redacted] per person = [redacted]
- Executive and Engineering Data Analysis - 1 hour per week faster, 3 engineers/execs
  - 3 hours per week = 5% [redacted]

Total Savings: [redacted]

Total Estimated Cost/Year for Personal Health Role: [redacted]

- https://logs-license.cerner.com/en-US/app/search/usage_per_role?earliest=-30d%40d&latest=%40d&form.role=personal_health

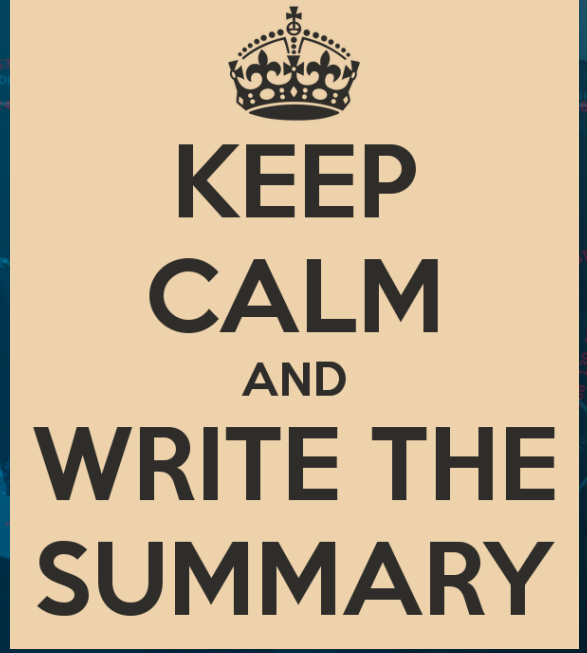
Savings/Cost Ratio: [redacted] = 127.28

124 Views Categories: Tags (edit):

Extend the Deadline

- We did this 3 times, got more submissions each time.

.conf2015



Review

splunk>

Summary

- Know who you are
- Make things surprisingly easy
- Gather endorsements
- Be helpful in many mediums
- Promote your community
- Create champions
- When all else fails, hold a contest

THANK YOU

splunk>