



.conf2015

Splunk Apptitude II

Corey Marshall

Director, Splunk for Good

Monzy Merza

Minister of Defense



splunk®

Splunk Community

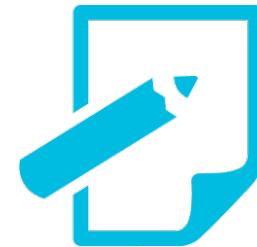
Splunk is at its best when we engage our community



Reinforce engagement
among core users



Create opportunities for
new users and
developers



New use cases and
applications

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



splunk>



- App development contest to engage our community
- Enhance visibility and create energy for the Splunk development ecosystem
- Raise the visibility of customer identified needs
- Reward innovative ideas

Splunk Apptitude II

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



splunk>

\$150,000 in cash prizes



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)



Social Impact

Grand Prize:
\$30,000 (US)



Innovation

Grand Prize:
\$20,000 (US)

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



splunk>

Develop Splunk apps to anticipate, predict and identify malicious user activity, fraud, insider threats, and more.



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)

- What are we looking for?
 - **Insider Threat:** Malicious insiders stealing intellectual property or company data
 - **Fraud Detection:** Financially benefitting from co-opting resources or processes
 - **Anomaly Detection:** Anomalies in application usage by humans or automated processes

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>

Develop open data apps for social impact with Splunk – a platform that matches the scale of our biggest challenges.



Social Impact

Grand Prize:
\$30,000 (US)

- What are we looking for?
 - **Open Data:** Innovative uses of public data sets that can change the game
 - **Public Benefit:** Help improve public services, enhance transparency, and make government more accessible
 - **Splunk4Good:** Use Splunk to help identify new insights and approaches to old problems, analyze disparate datasets and reveal hidden patterns in public data

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>

Your choice, your solution: Pick a problem and design your most innovative approach using Splunk software.



Innovation

Grand Prize:
\$20,000 (US)

- What are we looking for?
 - **Share:** We want our customers, partners, and developers to share the amazing things that are hiding behind the firewall.
 - **Your choice:** Pick a problem and design your most innovative app using Splunk software. You pick the data; you design the solution.
 - **Innovate:** Splunk is built on tireless, shameless innovation. We want you to impress us with your off-the-wall ideas and crazy applications of Splunk!

The Winners!!!

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)

Develop Splunk apps to anticipate, predict and identify malicious user activity, fraud, insider threats, and more.

Winner: Hyperthreat

Team: Mika Borner, Harun Kuessner,
Christoph Dittman, Simon Balz

Country: Switzerland



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



splunk>



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)

Risk Overview

Time Range: All time Risk Object Type: All Risk Object: All Alert Search: All

Risk Objects: 721 Average Risk Score: 4 Total Risk Score: 7815 Alert Searches: 38

Current Risk Objects - Top 10

Risk Object Type	Risk Object	Risk Score
user	CSF2712	32
user	ab4f62461cdaed77280740320545277177e7812390a	28
user	KXK1005	14
user	3608d6e60e1f61a720770e7a0d203195962295fa4777e7812390a	14
user	ab4f62461cdaed77280740320545277177e7812390a	14
user	LFR1463	12
user	CSF2712	12
user	VXR0344	12

Current Risk Events - Top 10

Risk Object Type	Risk Object	Event	Count
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-21 upload web	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 upload file	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 upload first time	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 download	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 device disconnect	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 file copy	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 logon	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 logoff	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 device disconnect	2
user	ab4f62461cdaed77280740320545277177e7812390a	encrypted_it_3-1-10 file copy	1

Risk Details (Decrypted)

Date	User	User Hash	File
2011-08-06 07:21	user	ab4f62461cdaed77280740320545277177e7812390a	(AES) Y703000-5400JZP5,01/08/2011 06:07:21,CSF2712PC-3343,VLAUPON.pdf/fileOpen?value=True,FF

Risk Manager

Risk Analyzer

Risk Score over Time

Risk Events over Time

Risk Details (Decrypted)

Date	User	User Hash	File
2011-08-06 07:21	CSF2712	ab4f62461cdaed77280740320545277177e7812390a	(AES) Y703000-5400JZP5,01/08/2011 06:07:21,CSF2712PC-3343,VLAUPON.pdf/fileOpen?value=True,FF

- Developed analytics and risk scoring framework to detect fraud and insider threats
- Developed a privacy feature to mask sensitive data in search results



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>



Social Impact

Grand Prize:
\$30,000 (US)

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>



Social Impact

Grand Prize:
\$30,000 (US)

Develop open data apps for social impact with Splunk – a platform that matches the scale of our biggest challenges.

Winner: Energy Scan

Team: Khyati Majmudar

Country: India



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud

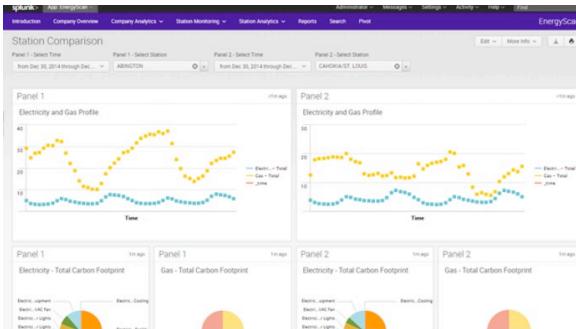


Social Impact

splunk>

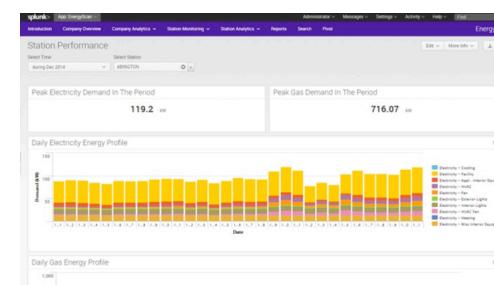
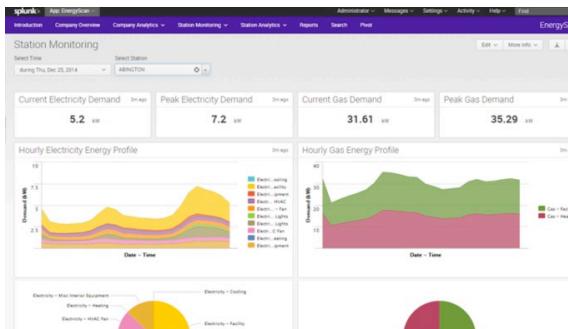
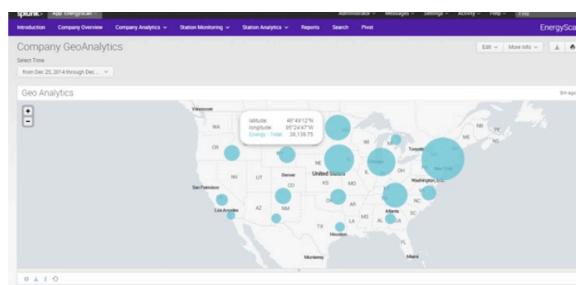


Innovation



Social Impact

Grand Prize:
\$30,000 (US)



.conf2015

2013
2014
2015

15

splunk>

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation



Innovation

Grand Prize:
\$20,000 (US)

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>



Innovation

Grand Prize:
\$20,000 (US)

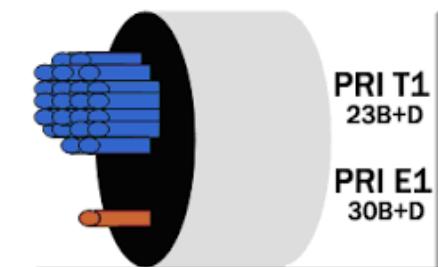
Pick a problem and design your most innovative approach using Splunk software.

Winner: PRI Capacity

Team: Frank Darrigo

AAA Western and Central New York

Country: US



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



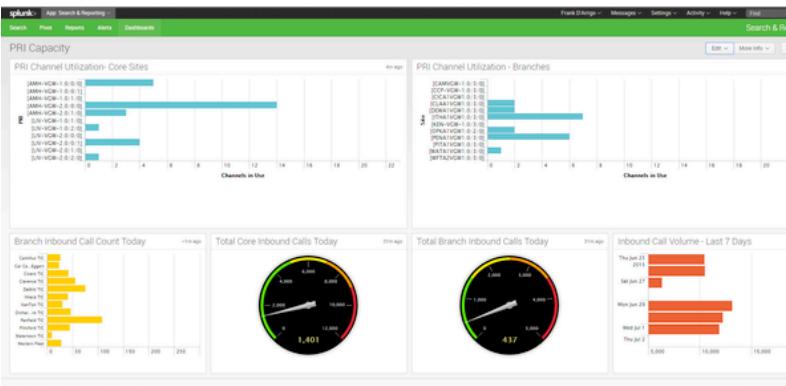
Innovation

splunk>



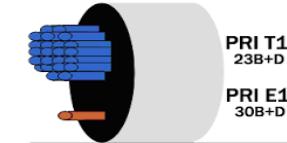
Innovation

Grand Prize:
\$20,000 (US)



```
#AMI VCL X
ACTIVATION_CUS: not applicable
Layer 3 status:
  Layer 3 Layer 3 MAC()
Active dsl 4 CCBs = 0
    Total Allotted ISDN CCBs = 8
    Total Active ISDN CCBs = 0
    No available CCBs to activate
K module input detected at '+' marker.

amn-voc-1<-->isdn-service
PRI channel statistics
ISDN Channel Statistics [1-1]
Configured ISDN Interface (dsl) 0
    Channel 1 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Service state (0=Inservice 1=Maint 2=Outofservice 8=WaitPend 9=HospD)
    Current : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Desired : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Idle : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    IdleStat : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Configured ISDN Interface (dsl) 1
    Channel 1 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Service state (0=Inservice 1=Maint 2=Outofservice 8=WaitPend 9=HospD)
    Current : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Desired : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Idle : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    IdleStat : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Configured ISDN Interface (dsl) 2
    Channel 1 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Service state (0=Inservice 1=Maint 2=Outofservice 8=WaitPend 9=HospD)
    Current : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Desired : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    Idle : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    IdleStat : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
AMN-VOC>: config
Enter configuration commands, one per line. End with CNTL/Z.
isdn-voc-1>conf-1<-->dial-peer
amn-voc-1>conf-1>#dial-peer voice 20072326 pots
amn-voc-1>conf-1>#description 10626326
amn-voc-1>conf-1>#dial-peer x incoming called-number 710626326
amn-voc-1>conf-1>#dial-peer x connect inuse-dial
amn-voc-1>conf-1>#dial-peer x/2
```



PRI T1
23B+D
PRI E1
30B+D

.conf2015



Runner Ups

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>

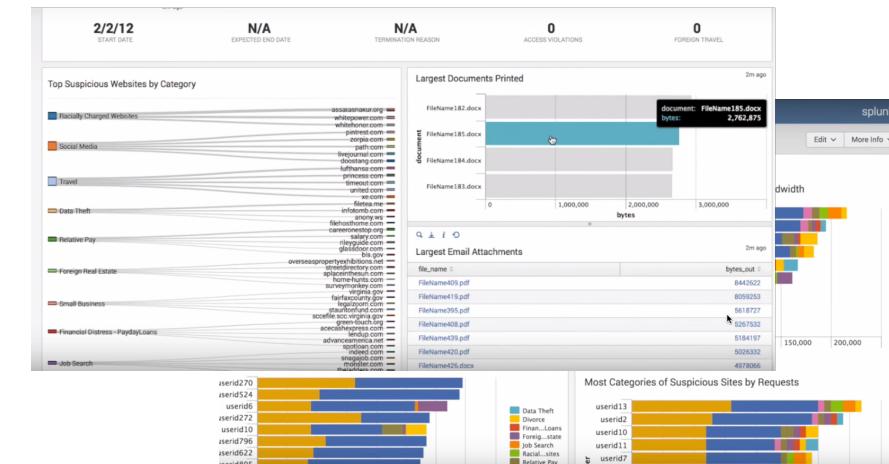
Runner Up: Qmulos, Q-trip



Fraud/Insider Threats

Grand Prize:
\$100,000 (US)

Insider threat focused
Visual analytics
Nice demo



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>

Runner Up: openFDA for Splunk



Social Impact

**Grand Prize:
\$30,000 (US)**

Team: Jeff Schumacher

Country: USA

**Public safety & health
API integrations
User friendly forms**

The screenshot displays the openFDA for Splunk application interface. It features several cards and charts. One card shows 'Food Recalls by Location' with a table of data:

country	state	city	count
US	NC	Goldsboro	85
US	WA	Shooshish	79
US	WA	Spokane Valley	67
US	CA	City Of Industry	65
US	WA	Seattle	61
US	TX	Austin	57
US	WA	Port Townsend	49
US	WI	Sullivan	35
US	GA	Atlanta	34
US	PA	Pittsburgh	33

Another card shows 'Food Recalls by Date' with a line chart of counts over time. A third card shows a pie chart of 'Food Recalls by Manufacturer'. Other cards include 'Device Events by Date' and 'Device Recalls by Date'.

Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more than just bragging rights. We'll give you \$150,000 cash.*



Insider Threat
and Fraud



Social Impact



Innovation

splunk>

Runner Up: OctopusDeploy



Innovation

Grand Prize:
\$20,000 (US)

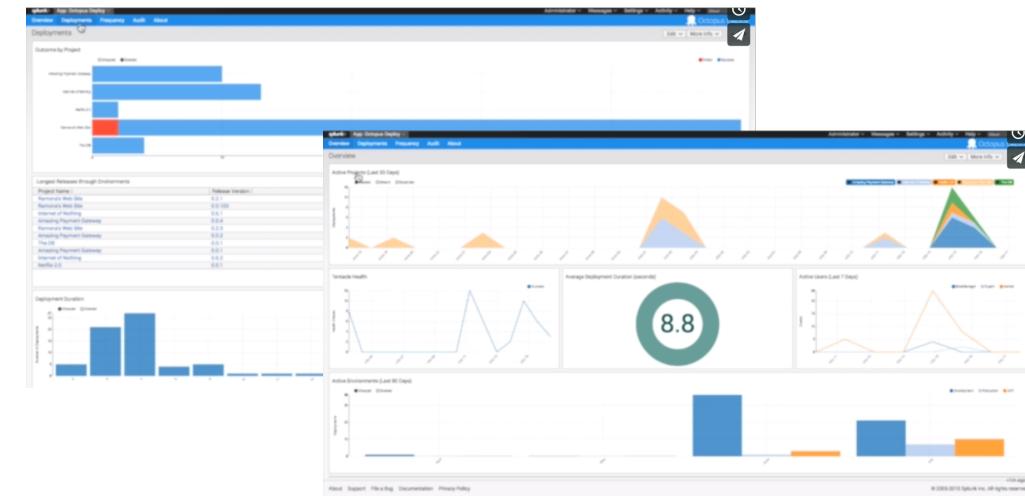
Team: Matthew Erbs

Country: Australia

DevOps

API integrations

Visual Analytics



Splunk Apptitude. Do you have it?

We want your big ideas...and we will give you more

than just bragging rights. We'll give you \$150,000 cash.*



splunk>

Insider Threat
and Fraud

Social Impact

Innovation

Learn More!

Check out the submissions!

<http://splunkapptitude2.devpost.com/>



.conf2015

2015

THANK YOU

splunk®