Splunk User Groups: More than Pints and Pizza

Tony Reinke, Nebraska User Group
Lead Systems Engineer, National Research Corporation

Aleem Cummins, London User Group
Data Analytics CTO, Computacenter

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.

Agenda

1. The Wonder of User Groups - We will be exploring the value of user groups, being a great citizen, how everyone wins, how we can join forces and what is next for user groups

2. User Group Creation and Management - We will be showing exactly what is involved in creating and operating successful User Groups. Everything you could imagine from emails to venues to YouTube to Agendas Section

3. Q&A

Splunk> Splunking the Cornhusker State

splunk> User Group London

Why Community Matters

- Communities Build Shared Memory *
- Communities Build Trust *
- Shared Memory and Trust Lead to Helpful Community Members *

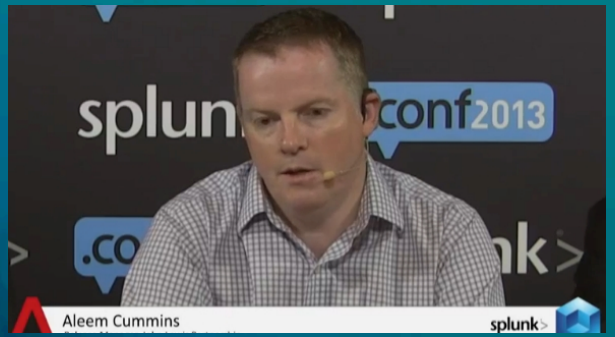
- Communities **care**
- Communities **nurture**
- Communities have **identity**
- Communities have **culture**
- Communities have **values**
- Communities **grow** together
- Communities **inspire**

** Wendell Berry "What are people for?"*

The Wonder of User Groups

splunk>

.conf2015



Aleem Cummins

London User Group

Data Analytics CTO, Computacenter

Computacenter
Services & Solutions

splunk>

London Story

Founded:	November 2013 following .conf
Meets:	Every month face to face
Membership:	300+
Organizations:	120+
Average attendance:	40+
Meeting organized:	20+
Special Guests:	15+

splunk> User Group London

Positive Intentions

- Establish a genuine community
- Create and maintain a safe environment
- Zero cost for members
- Foster Social Justice in the digital world
- Raise bar for IT
- Surface value and credibility
- Defining and modelling Success & Best Practice
- Personal & Professional Development
- Public Speaking
- Collaboration & Discussion
- Splunk Roadmap Insight
- Therapy
- Entertain, Empower and Inspire

splunk> User Group London

Familiar Special Guests












Helping Culture and Ethos

- Chatham House rules apply
- No selling
- No hiring
- Everyone is welcome
- No pressure to attend or speak
- Progressive
- Collegiate
- All voices are equal
- Community front and center
- Learn together

Lessons of World Community

- Share materials with other groups
- Share success stories
- Collaborate
- Speak at different groups
- Share effort
- Share guests
- Beta Programmes
- Vacations
- Fresh thinking
- Identity

User Group Creation and Management

splunk>

.conf2015

Tony Reinke

Nebraska User Group

Lead Systems Engineer - National Research Corporation

splunk>

Happy Birthday Hannah

Miss you - Love You

Why Community Matters

OSSEC and Splunk

July 27th, 2009 | Author: Tony Reinke

I have been playing with OSSEC and Splunk. OSSEC is a Host based Intrusion Detection System (HIDS). Splunk is a log archiving and searching system. OSSEC is open source and is multiple platform. You can run it on Linux/Unix and Windows. I am using OSSEC to forward Windows Event Logs to Splunk. Splunk makes the searching and correlation. Splunk can do WMI. This would be great since no agent would need to be installed. The problems is that if you have more than 30-50 systems, the amount time and traffic would cause issues. Using the OSSEC agent, I am able to push the event logs to the OSSEC server. From there the OSSEC server will upload to the Splunk server via Syslog.

Right now I have the servers all talking but I do need to adjust a few things. Right now Splunk sees all the hosts as the OSSEC server. I believe I just need to tweak the fields. The question is how.

Splunk
http://www.splunk.com

OSSEC
http://www.ossec.net

Michael Wilde says:
July 29, 2009 at 1:24 pm

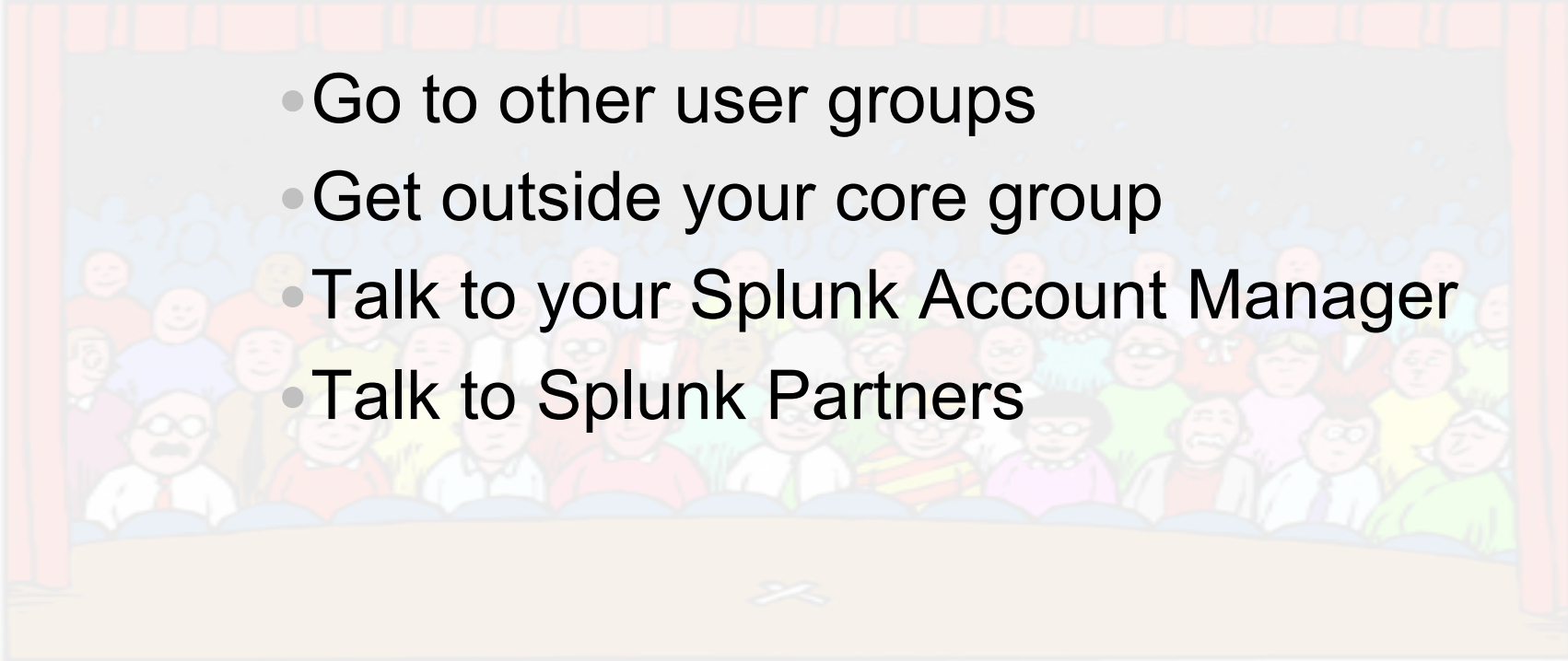
Anthony. Next to each event, right below the timestamp is an "Extract Fields" link. Its a nice little wizard that helps you pick out things you'd like to be fields and it writes the REGEX for you. You give it samples, it builds the field extraction.

Check it out. I'm a regex ninja and i don't need most of my skills anymore.

Michael Wilde
Splunk Ninja
twitter: @michaelwilde

Reply

Meeting Tools – Knowing Your Audience



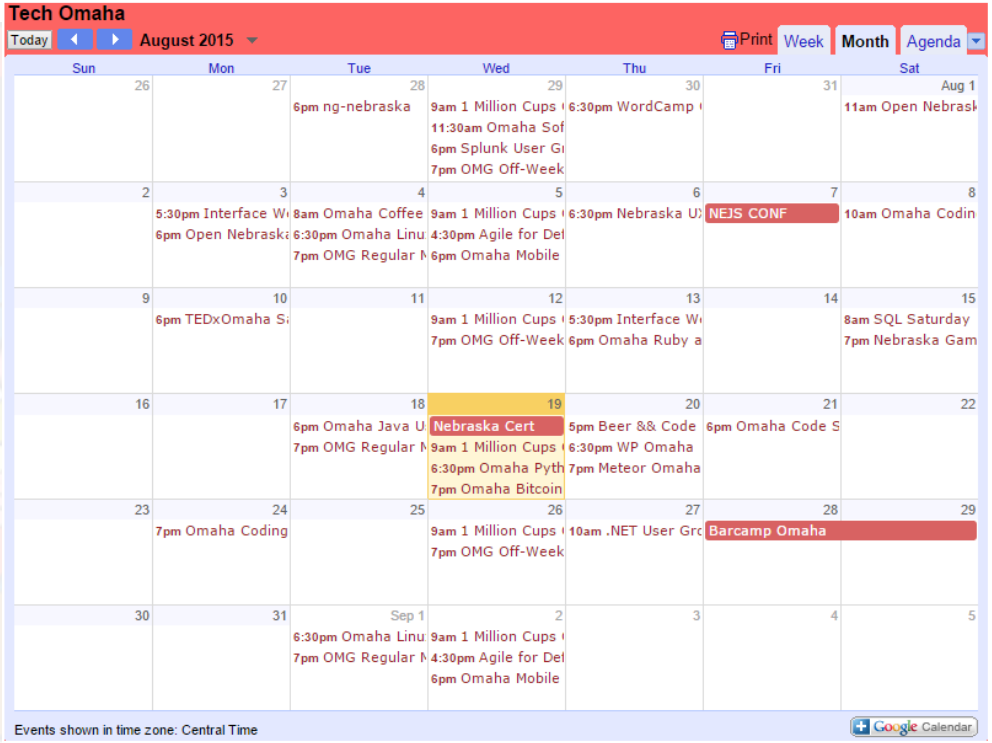
- Go to other user groups
- Get outside your core group
- Talk to your Splunk Account Manager
- Talk to Splunk Partners

Meeting Tools – Knowing Your Audience

Do your homework!

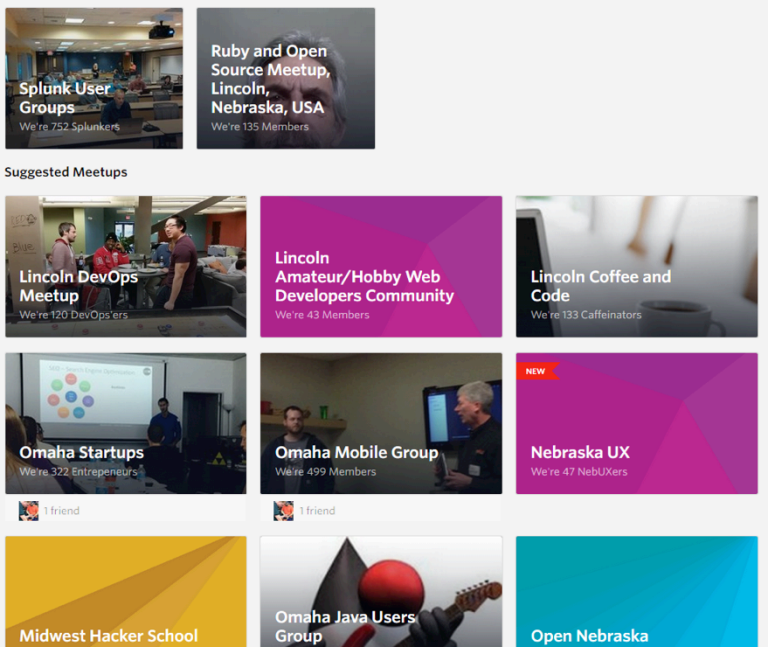
- Technical Group or Business Group?
- How often will you meet?
- What time works?
- What day of the week?

Meeting Tools – Knowing Your Audience



http://techomaha.com | @techomaha

Meeting Tools – Knowing Your Audience



http://www.meetup.com/
http://www.meetup.com/Splunk-Meetups/

Meeting Tools – Get The Ball Rolling

Rachel Perkins
Sr. Director, Community
aka PieBob
aka Your New Best Friend

Planning Your Meeting

- Meeting Day of the Week
- Meeting Time
- How Often to Meet
- Food
- Drinks
- Speakers
- Topics
- Vendors / Sponsors ?

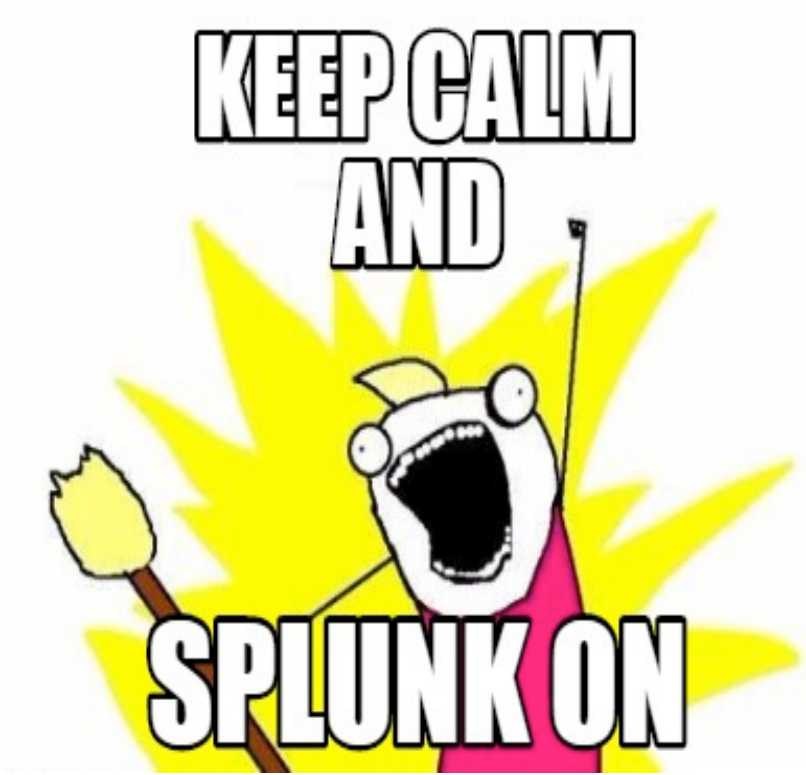
Vendor / Sponsor Talks

85% technical
10% sales
7% electricity
5% evaporation
3% butterscotch ripple

Getting the Word Out

- Social Media
- Your Splunk Account Manager
- Splunk Partners
- Friends
- Family
- Random person walking their dog

Running Your Meeting



Stay Calm
Welcome Everyone
Give a quick overview
Have a quick intro for each person
Make sure there is time for food
Networking
Enjoy Yourself

Sample Meeting Agenda

6:00pm – Start Meeting, Introductions and Welcomes

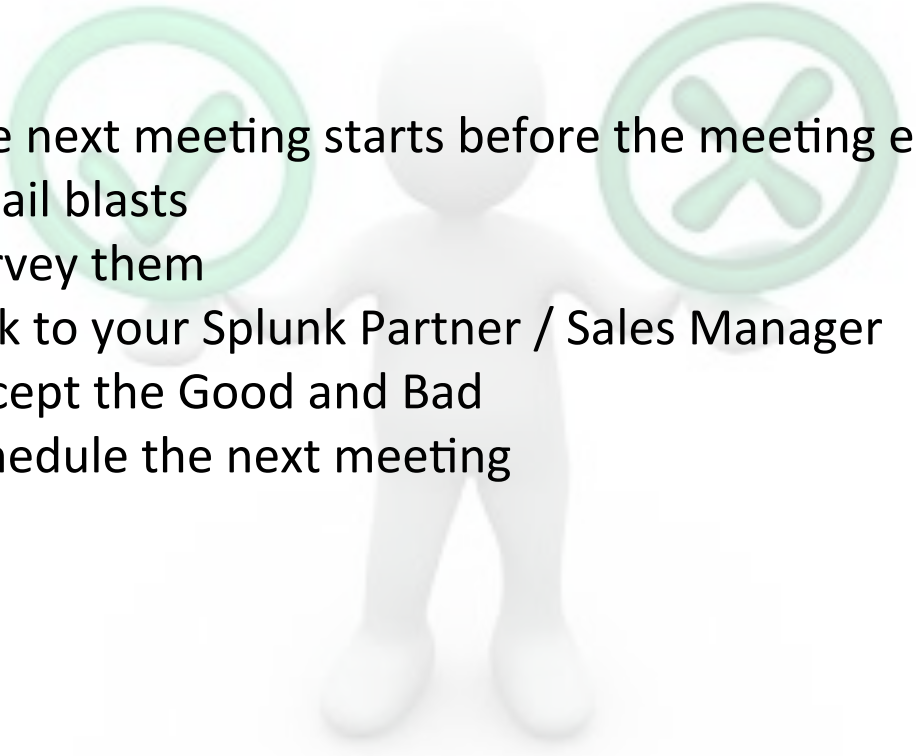
6:15pm – Customer Success Story

6:45pm – Technical Topic

7:30pm – Vendor / Guest Speaker

8:15pm – Networking

The Follow Up



The next meeting starts before the meeting ends
Email blasts
Survey them
Talk to your Splunk Partner / Sales Manager
Accept the Good and Bad
Schedule the next meeting

The Main Take Aways

Follow Your Passion

Have Fun

Don’t Go Alone

The Splunk402 Community

Tony Reinke
@tjreinke
contact@splunk402.com
www.splunk402.com

Aleem Cummins
@AleemCummins
Aleem@Cummins.me

splunk>

Q&A

splunk>