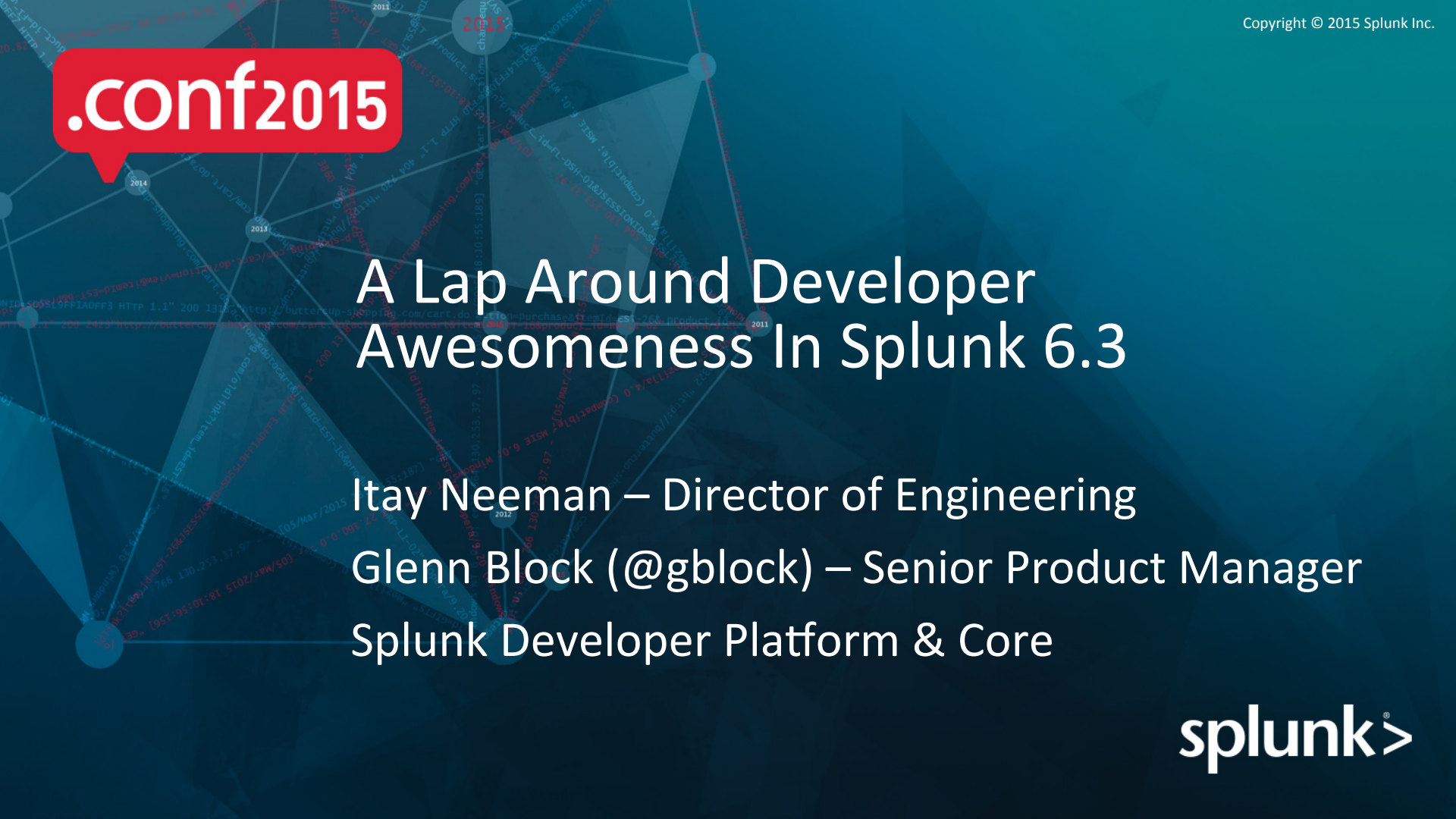


Copyright © 2015 Splunk Inc.

.conf2015

A Lap Around Developer Awesomeness In Splunk 6.3

Itay Neeman – Director of Engineering

Glenn Block (@gblock) – Senior Product Manager

Splunk Developer Platform & Core

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.

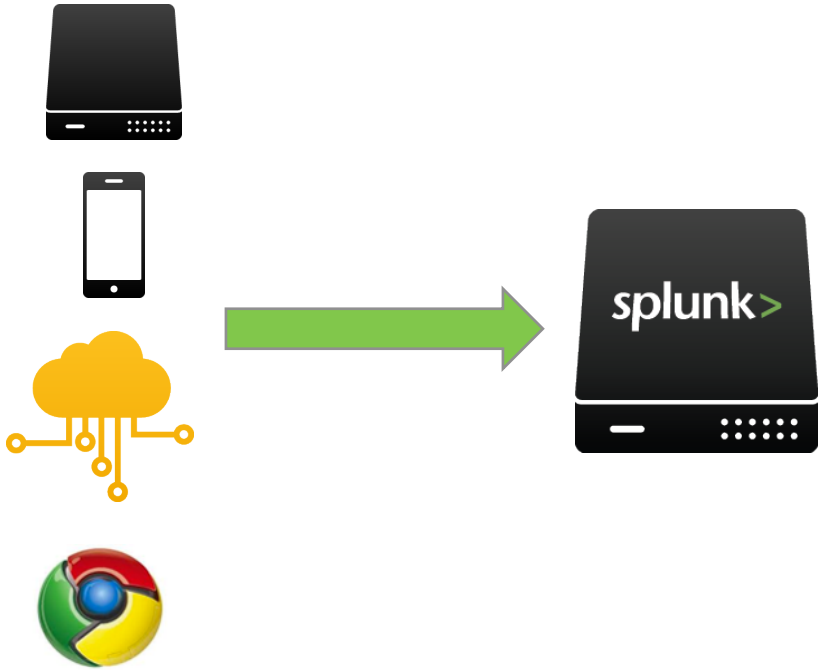
Splunk 6.3 is *filled* with Developer Awesomeness!

HTTP Event Collector

- A new token-based JSON API for events
- Send events ***directly*** from anywhere (servers, mobile devices, IOT)
- Easy to configure / works out of the box.
- Easy to secure
- Highly performant, scalable and available

Sessions to Learn more:

- Liberate your Application Logging!
- Accelerating your Solution Development with Splunk Reference Apps
- Throw Your Future Self a Lifeline with a Little DevOps Data



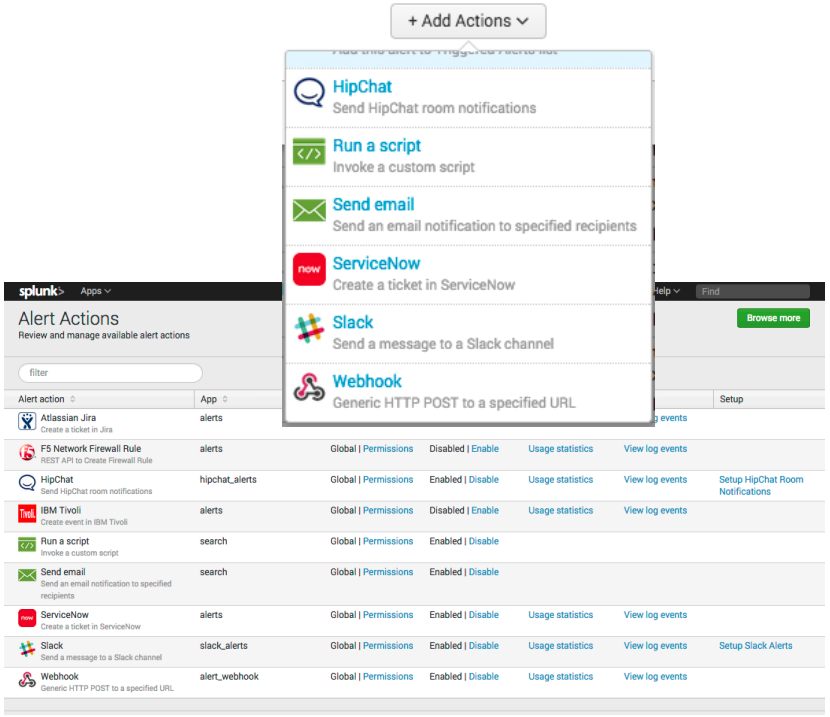
Demo

HTTP Event Collector

splunk>

Custom Alert Actions

- Build reusable alert hooks into Splunk
- Integrated into the Splunk UI
- Packaged in Splunk apps
- Similar to authoring Modular Inputs
- Very developer friendly:
  - Simple code interface
  - Easily hook into UI
  - Easy way to test your alert from a search



Sessions to Learn more:

- Creating and Using Custom Alert Actions
- Accelerating your Solution Development with Splunk Reference Apps

Demo

Custom Alert Actions

splunk>

Custom Search Commands

- Create new commands that can run in your search:
  - For example, “index=myindex | my_awesome_command some_field | stats count
- New in 6.3 - significantly improved protocol, drastically improved performance
  - Single process per search-invocation
  - Reduced serialization/deserialization
  - Increased flexibility and reliability
- New Python SDK release supports both v1 (6.2 and below) and v2 (6.3+) of the protocol

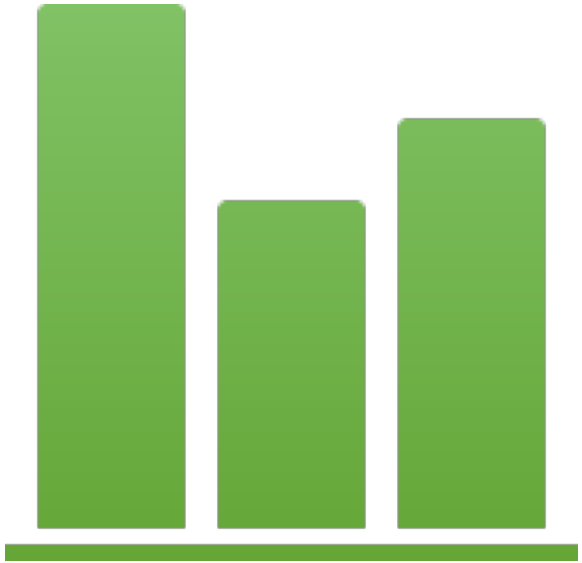
Demo

Custom Search Commands

splunk>

SimpleXml Enhancements

- Eval Tokens
  - Set tokens to an eval expression
- Search events
  - Tap into various stages of the search pipeline and update tokens based on job properties .



Sessions to Learn more:

- Advanced Interactions using Simple XML

Demo

SimpleXml Enhancements

splunk>

Modular Inputs in Node.js

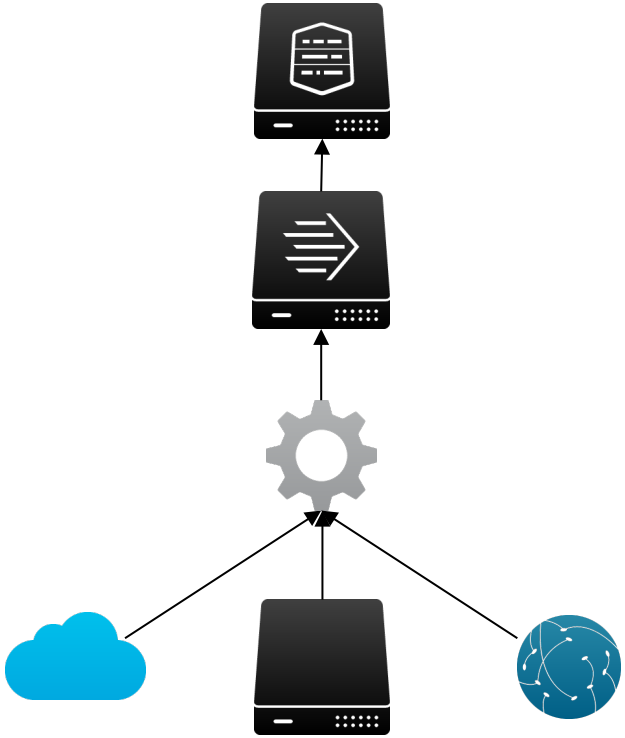
- Used to create new new types of reusable inputs in Splunk
- The Splunk SDK for Node.js has built-in support for writing Modular inputs:

Benefits:

- Easy to write
- No boilerplate
- Use NPM packages
- Cross-platform

Sessions to Learn more:

- Throw Your Future Self a Lifeline with a Little DevOps Data
- Modular Inputs - If You Build It, They Will Come



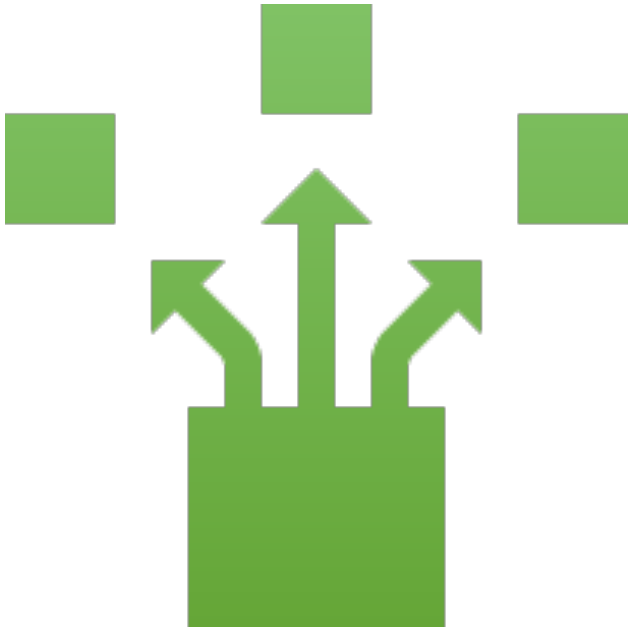
Demo:

Node.js Mod Inputs

splunk>

REST API/SDK Support for SHC

- Search Head Clustering allows you to have a scalable, redundant search tier with config synchronization
- SHC supports cookie-based authentication for cross-cluster authentication support
- Several SDKs now support SHC:
  - JavaScript SDK
  - C# SDK
  - Java SDK
  - Python SDK



SDK + SHC Demo!

splunk>

Next steps?

Related breakout sessions and activities…

Breakouts

- Creating and Using Custom Alert Actions
- The HTTP Event Collector, a New Way for Developers to Send Events to Splunk
- Accelerating Your Solution Development with Splunk Reference Apps
- Advanced Interactions using Simple XML

More information

- dev.splunk.com
- blogs.splunk.com/dev

Come by the Developer Booth and say hi / ask questions!

THANK YOU

splunk>