What's New: Enhanced Search Assistance

Jesse Miller
Sales Engineer, Splunk

Agenda – Enhanced Search Assistance

- Syntax Highlighting
- Compact Assistant
- Demo
- Questions

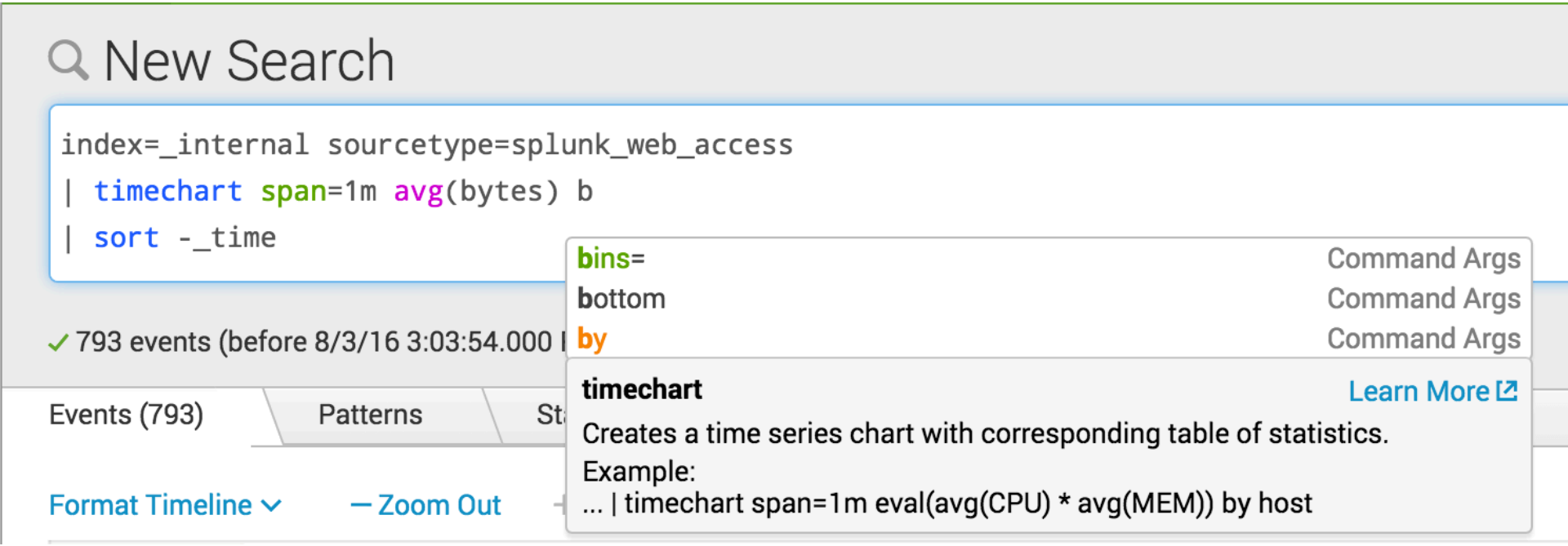
Disclaimer

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.

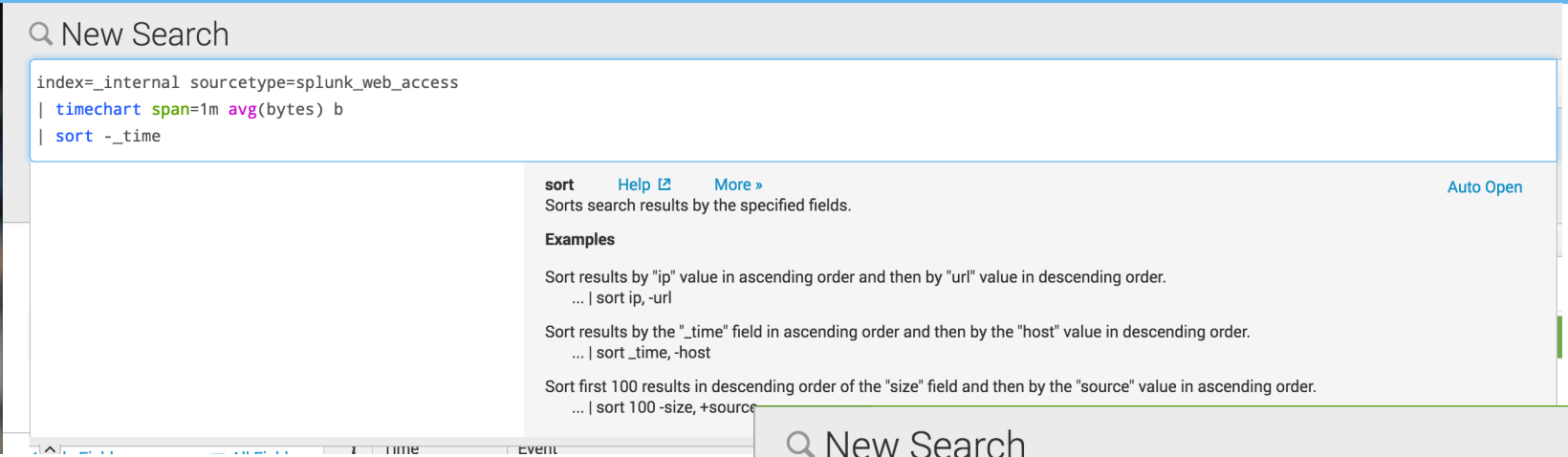
Syntax Highlighting

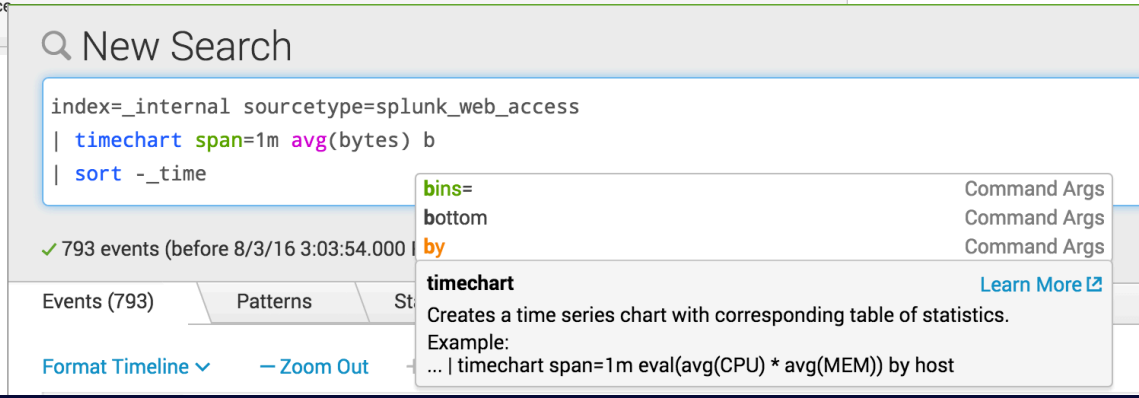
```
index=techmon sourcetype="techmon_hpom_messages_history"
| chart count over NODE_NAME by SEVERITY
| join NODE_NAME
    [ index=techmon sourcetype="technom_hpom_messages_history"
    | stats sparkline(count) by NODE_NAME]
| addtotals labelfield=SEVERITY label=Total
| sort -Total
| head 20
| stats count by series
| fields - count
| eval troublecount=mvindex(sourcetype_count,1)
| top toublecount limit=5 showperc=false
```

Compact Assistant

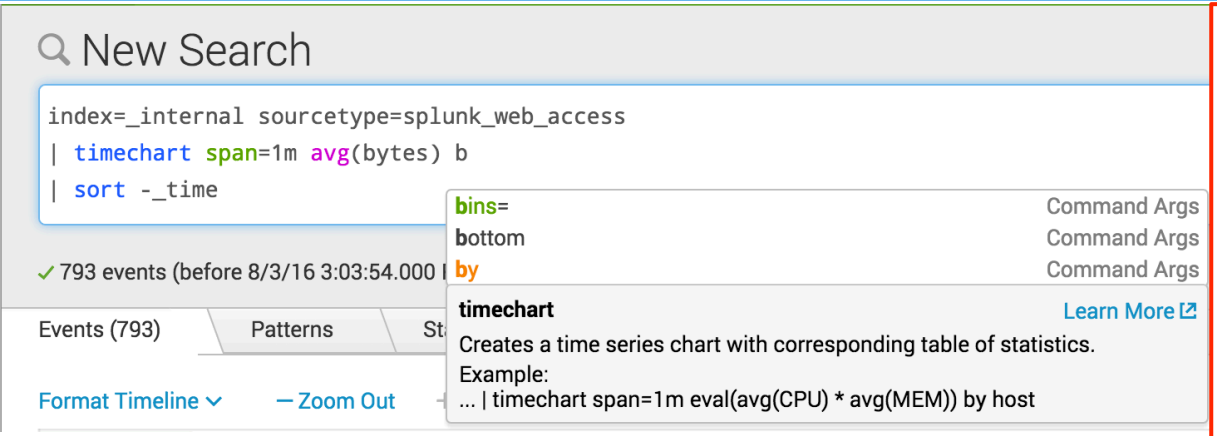


Compact vs. Full Assistant





Compact Assistant – Keyboard Shortcuts



Keyboard Shortcuts

Find-in-query: (CTRL+F)

Find & Replace: (CTRL+F)x2

Format Query: (CTRL+\)

Open Assistant: (CTRL+space)

Bonus: Bracket & Term Matching!

Key Takeaways

Syntax Highlighting

Improves readability and comprehension of queries with varied SPL syntax.

Can be disabled for individuals with color-vision deficiencies

Colors cannot be customized

Invalid arguments are shaded

Compact Assistant

Compact on-screen footprint, with a position relative to keyboard cursor

Assistance is contextual to keyboard cursor

Retains existing matching terms and search capabilities

Keyboard shortcuts

Configuration

Account Settings Page

User-Prefs.conf

Default: Compact Assistant

Default: Syntax Highlighting ON

Demo

Questions

THANK YOU

splunk>