Connecting the Dots Between "The Business" and IT with Splunk

Steve Baturin | Business Application Technology Mgr Raytheon Global Business Services

Forward-Looking Statements

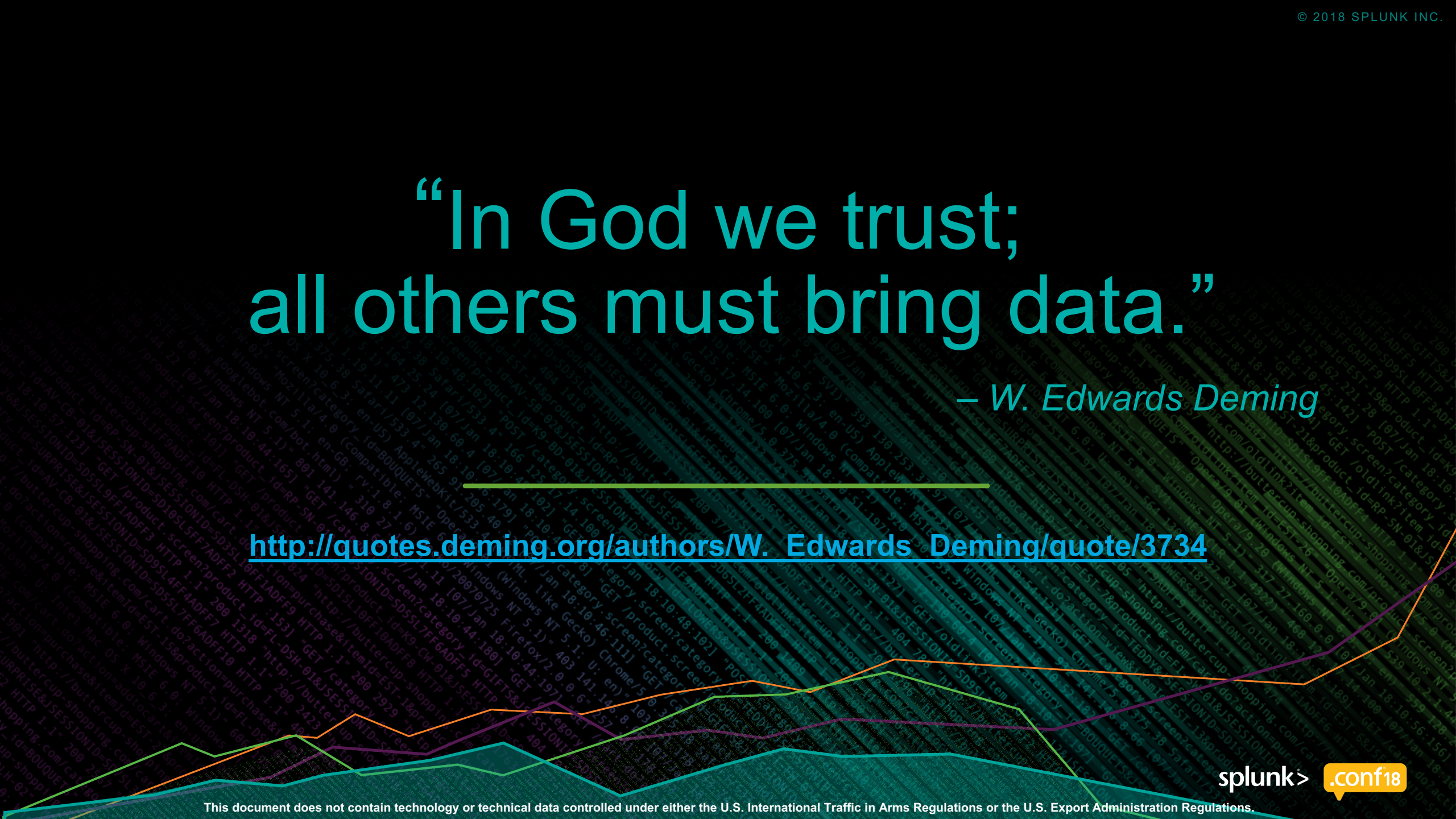
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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 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.

“In God we trust; all others must bring data.”

– W. Edwards Deming

http://quotes.deming.org/authors/W._Edwards_Deming/quote/3734



Overview

- Data correlation
- Data visualization
- Data depiction

Start your journey and discover where you want to go

Definitions

- Business – a profit seeking enterprise engaged in goods or services
- Business value – the assigned worth to goods or services
- ITIL – aligns IT services and “your Business’” needs
- Splunk facilitates ITIL alignment

Connect with “your Business” and increase its value

Correlation

Text Processing

- **A**ho, **W**einberger, and **K**ernighan
- **s**tream **ed**itor
- **p**ractical **e**xtraction and **r**eport **l**anguage
- **g**lobally search a **r**egular **e**xpression and **p**rint

Why are you focusing on regular expressions?

The First Aha Moment

- Proposal System is a mission-critical application spread across multiple servers
- IT has no account access on production servers
- Splunk is a distributed grep

Access, search, and correlate all of your data all at once

Correlating Logs

HTTP Access Logs

JEE Server Logs

RDBMS Server Logs

Correlating Logs

HTTP Access Logs

JEE Server Logs

RDBMS Server Logs

Focus on the Search

Text Processing

- Correlate log data from servers
- Search it

Splunk – creates initial correlation

- Search it

Wastes time correlating

Improves searching time

Get notified when errors occur and reduce your outage time

Visualization

Performance

- ‘the Business’: “The system is too slow.”
- IT: “How fast should it be?”
- ‘the Business’: “As fast as possible!”

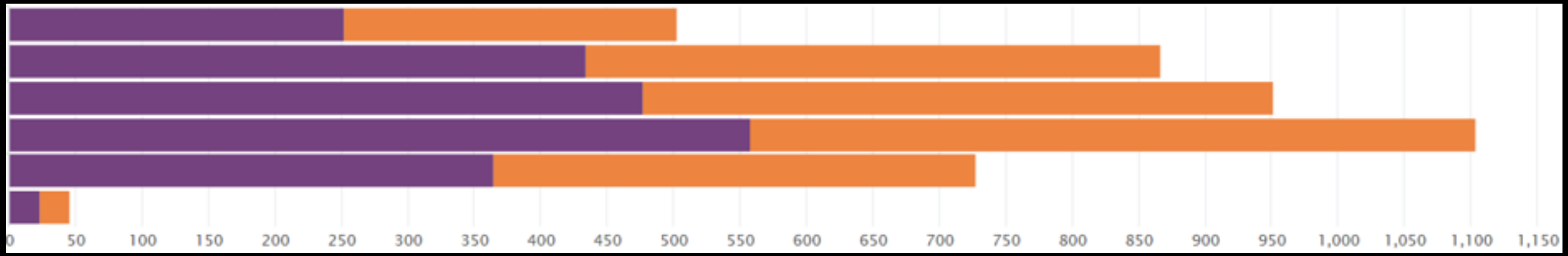
Why are you defining system performance?

The Second Aha Moment

- Proposal System contains a reporting system spread across multiple servers
- IT has no performance tools on production servers
- Splunk is a 4GL GUI

Visualize all of your data all at once

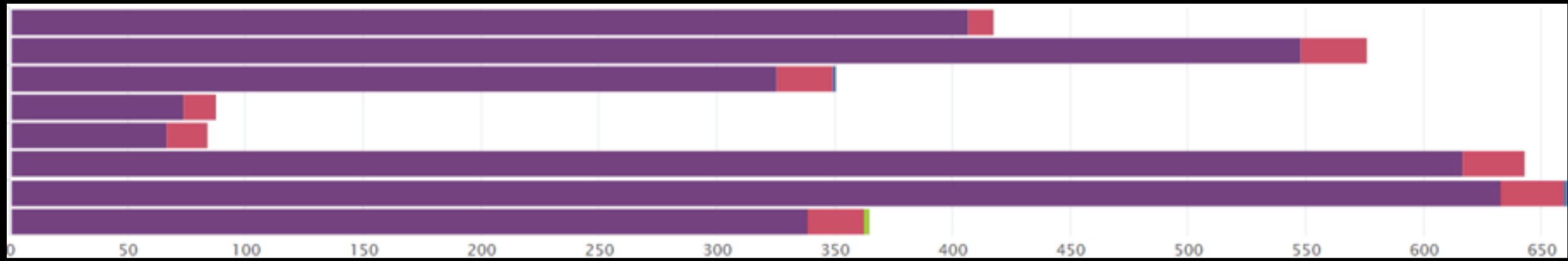
Initial Report Performance



reports running less than one minute

reports running more than 30 minutes

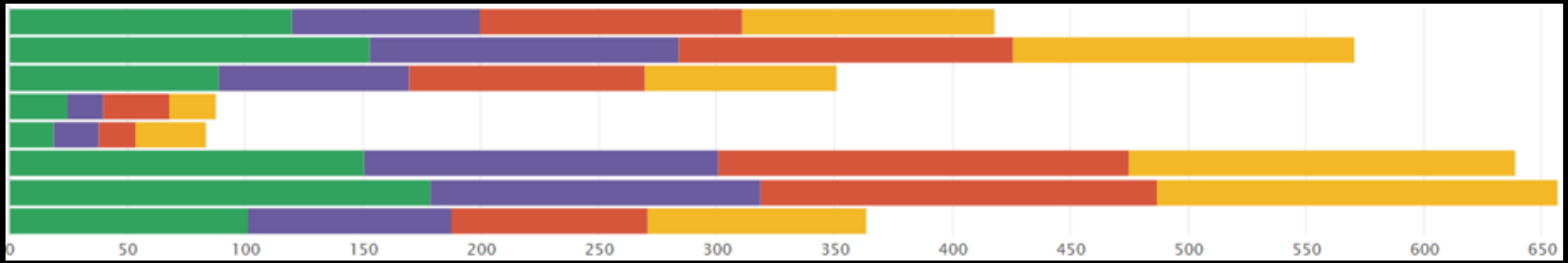
Improved Report Performance



reports running less than one minute

reports running less than 5 minutes

Report Server Performance



Focus on the Visualization

Excel Processing

- Correlate log data from servers
- Visualize it

Splunk – creates initial correlation

- Visualize it

Wastes time correlating

Improves visualization time

Get visual confirmation when your performance changes

Depiction

User Psychology

- ‘the Business’: “It’s always been done this way.”

Why are you engaging in your users’ paradigm?

The Third Aha Moment

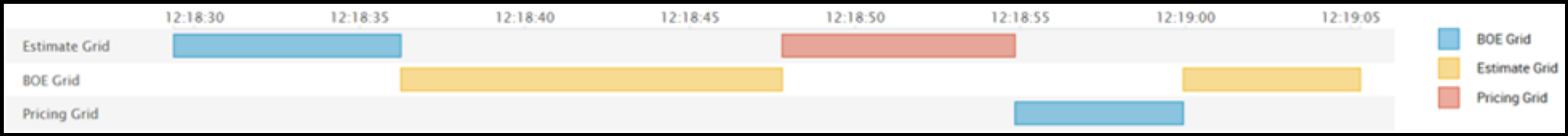
- Proposal System user base continually changes
- “the Business” has no time to continually survey user sentiment
- Splunk depicts user behavior

With timelines, depict all of your data all at once

One Business Does not Use the New Page

Pricing grid is new page

One Business Uses the New Page

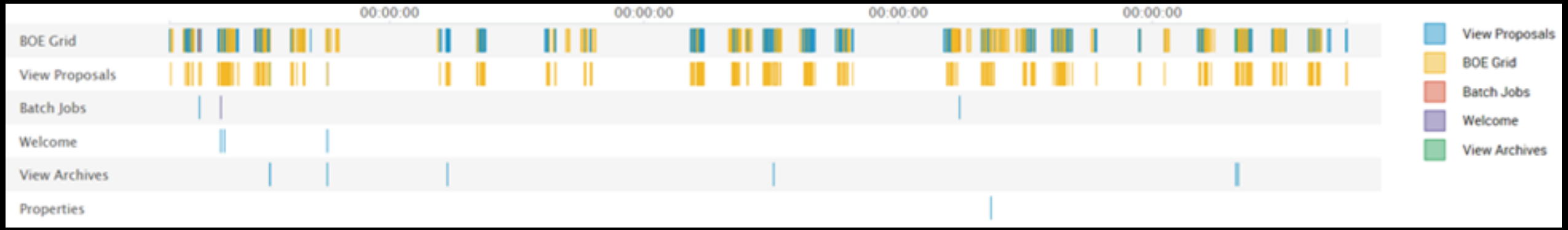


Pricing grid is new page

One Business Barely Uses a Key Role

A&D proposal role is key role

One Business Heavily Uses a Key Role



A&D proposal role is key role

One Business Does not Use a New Role

Business supervisor is new role

One Business Uses a New Role

Business supervisor is new role

Focus on the Depiction

Excel Processing

- Correlate log data from servers
- Depict it

Splunk – creates initial correlation

- Depict it

Wastes time correlating

Improves depiction time

Get predictive confirmation when your user behavior changes

Connecting the Dots

Start Your Journey

Agile Test-driven Development

Improves your TCO

Splunk Log-driven Development

Improves your Business Value

Connect with “Your Business”

Access, search, and **correlate** all of your data all at once

Get notified when errors occur and reduce your outage time

Visualize all of your data all at once

Get visual confirmation when your performance changes

With timelines, **depict** all of your data all at once

Get predictive confirmation when your user behavior changes

Discover Where You Want to Go

IT: “How can I increase ‘my Business’ value?”

Q&A

Thank You

Don't forget to rate this session in the .conf18 mobile app