



splunk>

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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

“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

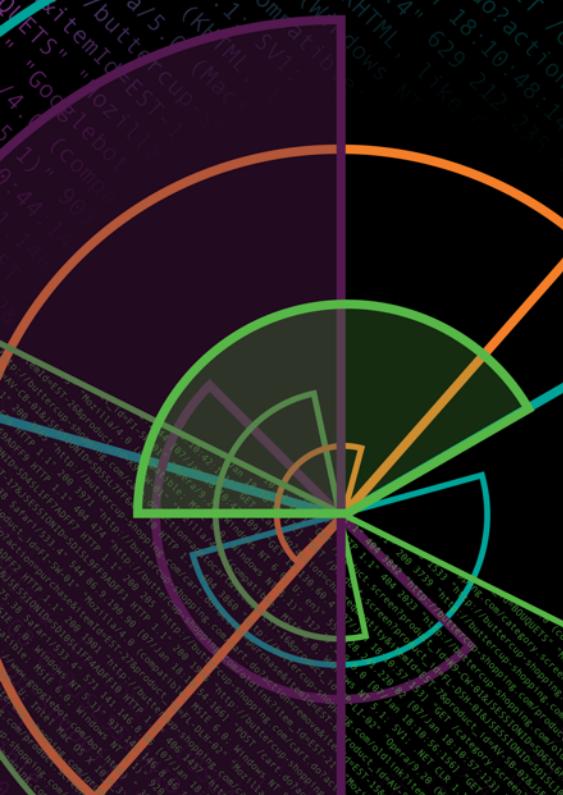
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

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

- ▶ Aho, Weinberger, and Kernighan
 - ▶ stream editor
 - ▶ practical extraction and report language
 - ▶ globally search a regular expression and print

Why are you focusing on regular expressions?

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

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

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Correlating Logs

HTTP Access Logs

JEE Server Logs

RDBMS Server Logs

Correlating Logs

HTTP Access Logs
JEE Server Logs
RDBMS Server Logs

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Focus on the Search

Text Processing

- ▶ Correlate log data from servers
 - ▶ Search it

Splunk – creates initial correlation

- ## ► Search it

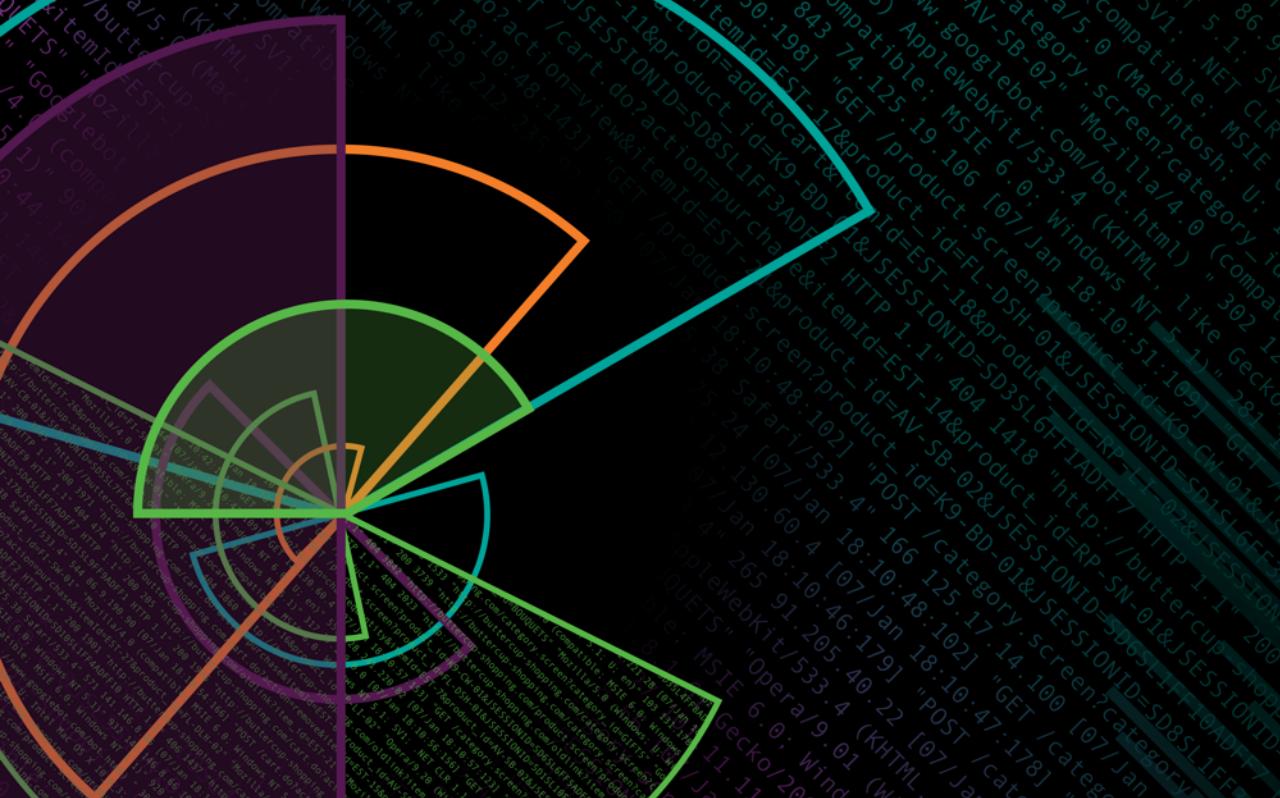
Wastes time correlating

Improves searching time

Get notified when errors occur and reduce your outage time

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

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?

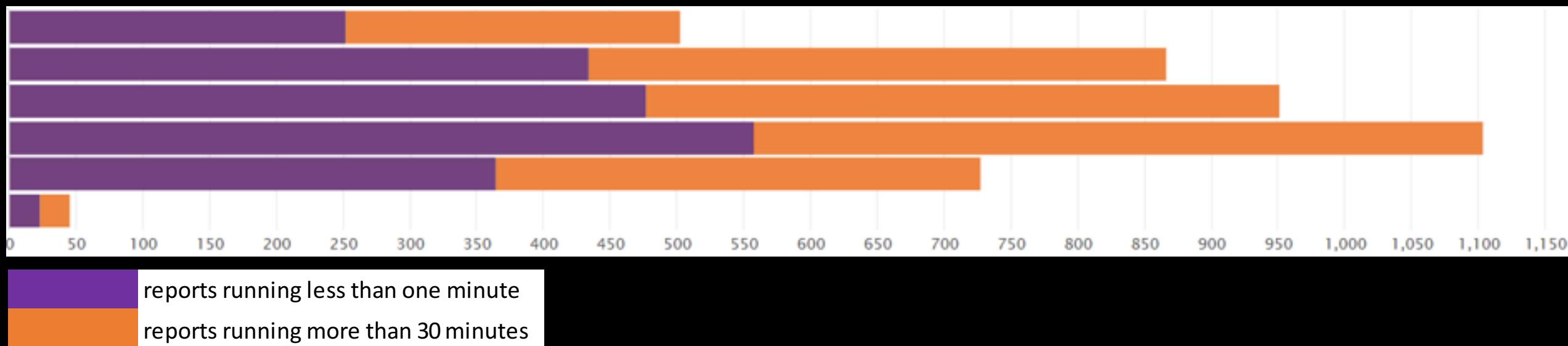
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

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

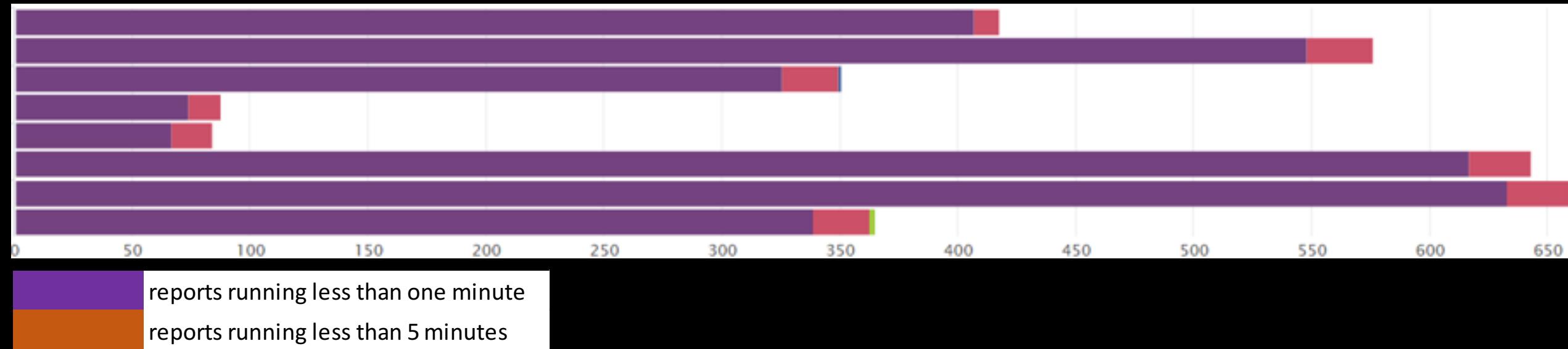
Visualize all of your data all at once

Initial Report Performance



This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

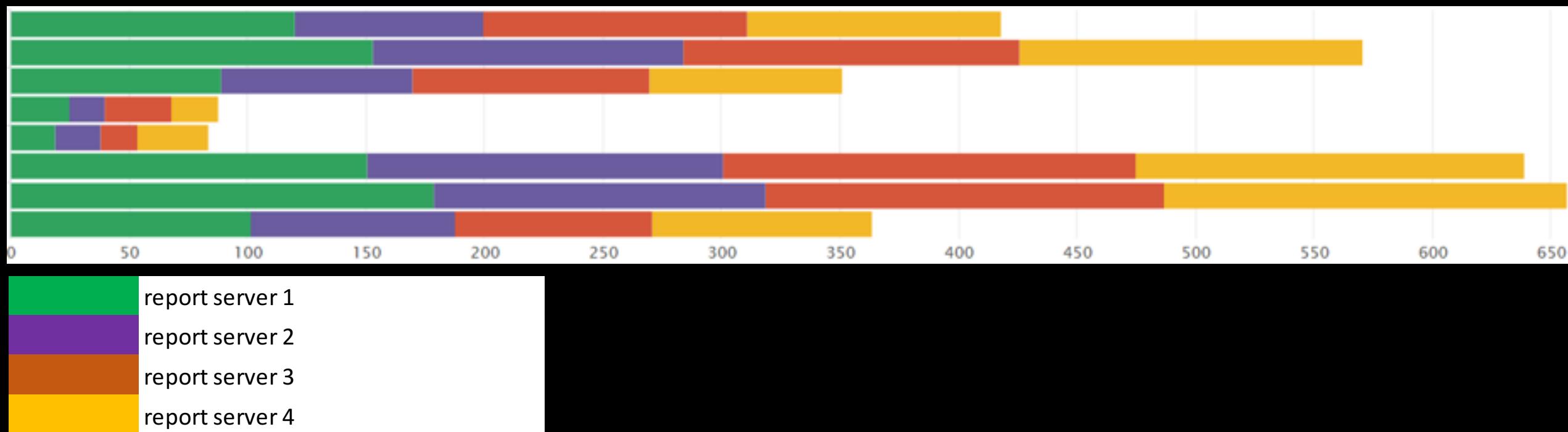
Improved Report Performance



reports running less than one minute
reports running less than 5 minutes

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Report Server Performance



The document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Focus on the Visualization

Excel Processing

- ▶ Correlate log data from servers
 - ▶ Visualize it

Splunk – creates initial correlation

- ## ► Visualize it

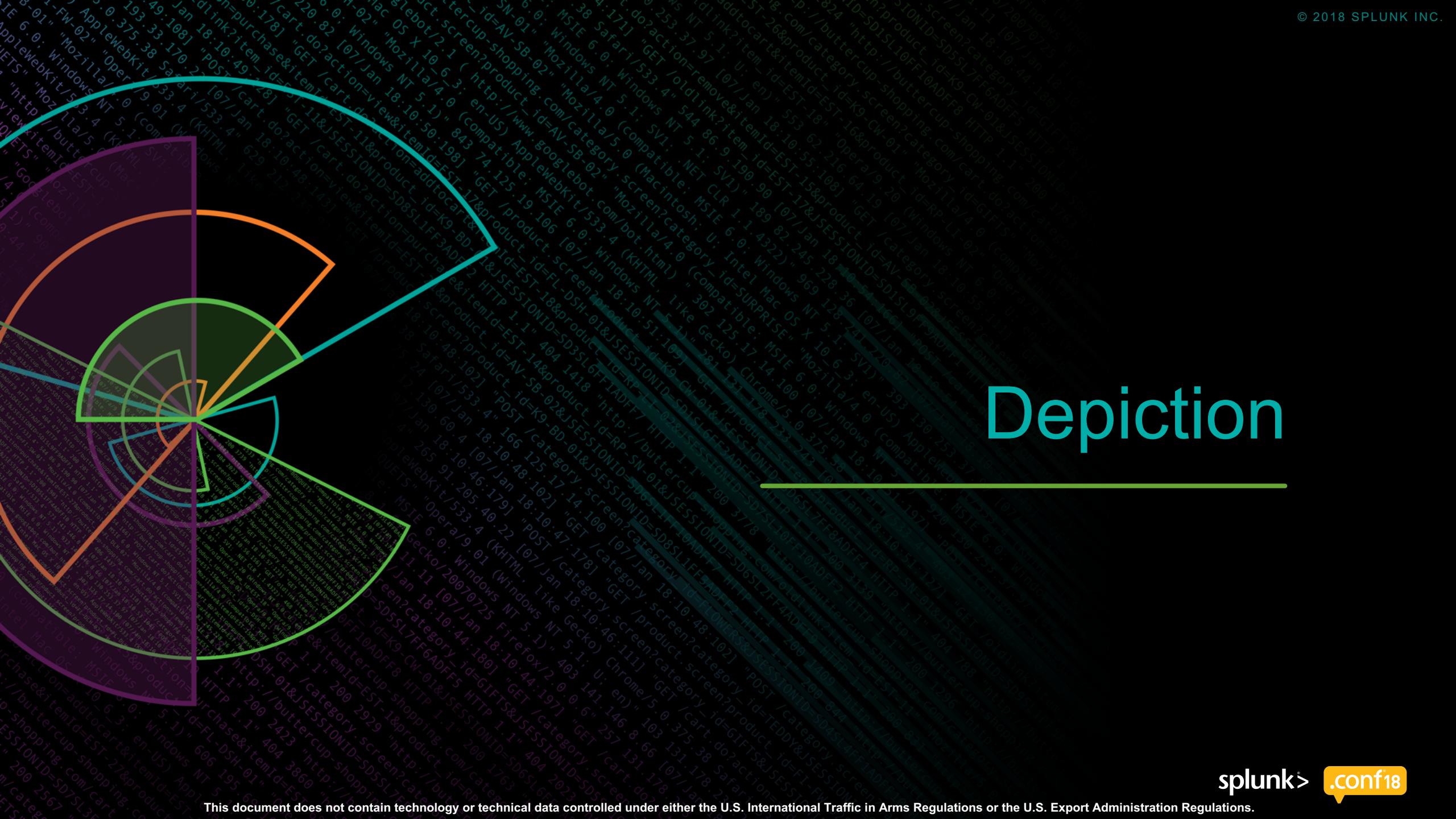
Wastes time correlating

Improves visualization time

Get visual confirmation when your performance changes

138.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?categoryId=EST_6&productScreenId=F2-SW-04" 200 3322
128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&jSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&productScreenId=F2-SW-04"
317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /product.screen?category_id=GIFTS&jSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
ows NT 5.1: SV1; .NET CLR 1.1.4322" 468 125.17.14.128 "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
kitemid=EST_16&product_id=RP-LI-02" "0-125.17.14.128" "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
://buttercup-shopping.com/purchase&item_id=EST_16&product_id=RP-LI-02" "0-125.17.14.128" "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
opping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
10?action=purchase&item_id=EST_16&product_id=RP-LI-02" "0-125.17.14.128" "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST_26&productScreenId=F2-SW-04"
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Depiction



User Psychology

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

Why are you engaging in your users' paradigm?

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

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

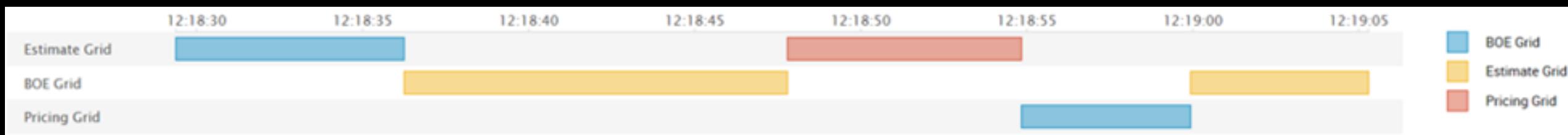
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

One Business Does not Use the New Page

Pricing grid is new page

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

One Business Uses the New Page



Pricing grid is new page

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

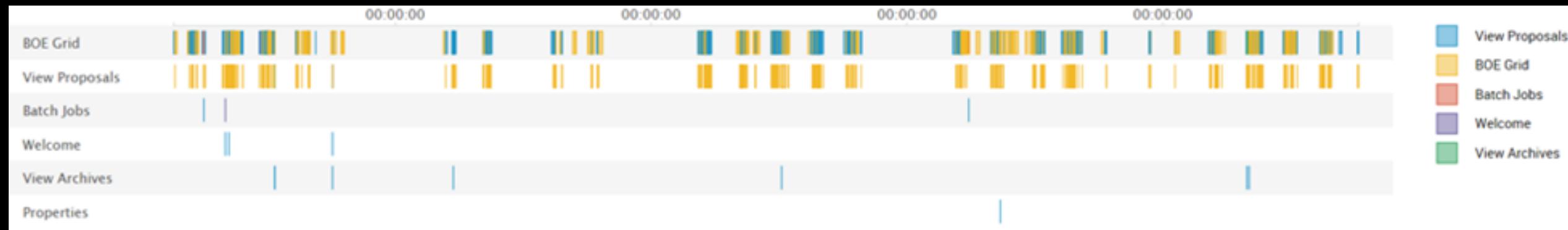
One Business Barely Uses a Key Role



A&D proposal role is key role

138,60,4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_6&product_name=BUTTERCUP GIFT SWAGGER" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
128,241,220,82 ~ [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&product_id=EST_6&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=print&screenId=EST_6&product_id=EST_6&product_name=BUTTERCUP GIFT SWAGGER" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
317,27,160,0,0 ~ [07/Jan 18:10:56:156] "GET /product.screen?category_id=GIFTS&product_id=EST_6&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=print&screenId=EST_6&product_id=EST_6&product_name=BUTTERCUP GIFT SWAGGER" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

One Business Heavily Uses a Key Role



A&D proposal role is key role

138,60,4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&productScreenId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
 128,241,220,82 ~ [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=printless&itemId=EST-26&productScreenId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
 317,27,160,0,0 ~ [07/Jan 18:10:56:156] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 2423 "http://buttercup-shopping.com/cart.do?action=print&itemId=EST-18&productScreenId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
 128,241,220,82 ~ [07/Jan 18:10:56:156] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 2423 "http://buttercup-shopping.com/cart.do?action=print&itemId=EST-18&productScreenId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125,17,14,109
 This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

One Business Does not Use a New Role

Business supervisor is new role

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations

One Business Uses a New Role



Business supervisor is new role

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Focus on the Depiction

Excel Processing

- ▶ Correlate log data from servers
- ▶ Depict it

Wastes time correlating

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F2-SW-B4" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=plusless&itemId=EST-26&product_id=F2-SW-B4" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
317.27.160.0.0 ~ [07/Jan 18:10:56:156] "GET /product.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADF10 HTTP 1.1" 404 2423 "http://buttercup-shopping.com/cart.do?action=plusless&itemId=EST-18&product_id=F2-SW-B4" "Opera/9.80 (Windows NT 5.1; U; en-US) AppleWebKit/525.27 (KHTML, like Gecko) Version/3.1.10.1342.1889" 468 125.17.14.109
/:/buttercup-shopping.com/purchase&item_id=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
opping.com/cart.do?action=remove&itemId=EST-16&product_id=F2-SW-B4" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Splunk – creates initial correlation

- ▶ Depict it

Improves depiction time

Get predictive confirmation when your user behavior changes

138.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?categoryId=EST_6&productScreenId=F2-Sw-8u" 200 3322 "-"
128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.screen?category_id=GIFTS&jSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "-"
317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /product.screen?category_id=GIFTS&jSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 322 "-"
ows NT 5.1: SV1; .NET CLR 1.1.4322" 468 125.17.14.102 "-"
kitemid=EST_16&product_id=RP-LI-02" "0-
://buttercup-shopping.com/cart.do?action=purchase&item_id=EST_16&product_id=EST_16&quantity=1&sessionid=EST_16&sessionid=SD10SLBFF2ADFF9_HU
j0?action=remove&item_id=EST_16&product_id=EST_16&sessionid=SD10SLBFF2ADFF9_HU
opping.com/cart.do?action=remove&item_id=EST_16&product_id=EST_16&sessionid=SD10SLBFF2ADFF9_HU
10-
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Connecting the Dots

splunk> .conf18

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Start Your Journey

Agile Test-driven Development

Splunk Log-driven Development

Improves your TCO

Improves your Business Value

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations

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?”

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations

Q&A

Thank You

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

