

Leveraging Splunk Analytics For Business Intelligence And Devops

Tim Watkins

Senior Consultant, MasterCard

.conf2016

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. Additionally, I am speaking personally and not on behalf of my employer. The examples and comments are in the context of personal experience and should not be considered the official practices or positions of MasterCard nor its affiliates.

Agenda

- Why Splunk For Analytics
- The Power Of Partnership
- Analytics For Business Intelligence
- Analytics For Devops
- Visualization Enhancements In Splunk 6.4

Why Splunk For Analytics

.conf2016

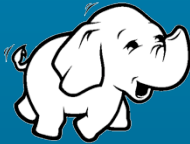
splunk >

Why Splunk For Business Intelligence

Splunk Complements Existing Business Intelligence Technologies



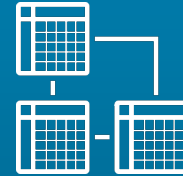
REAL-TIME
BUSINESS
INSIGHTS



FASTER INSIGHTS
FROM
HADOOP & NOSQL



TABLEAU, APT,
PENTAHO, LOOKER
& OTHERS



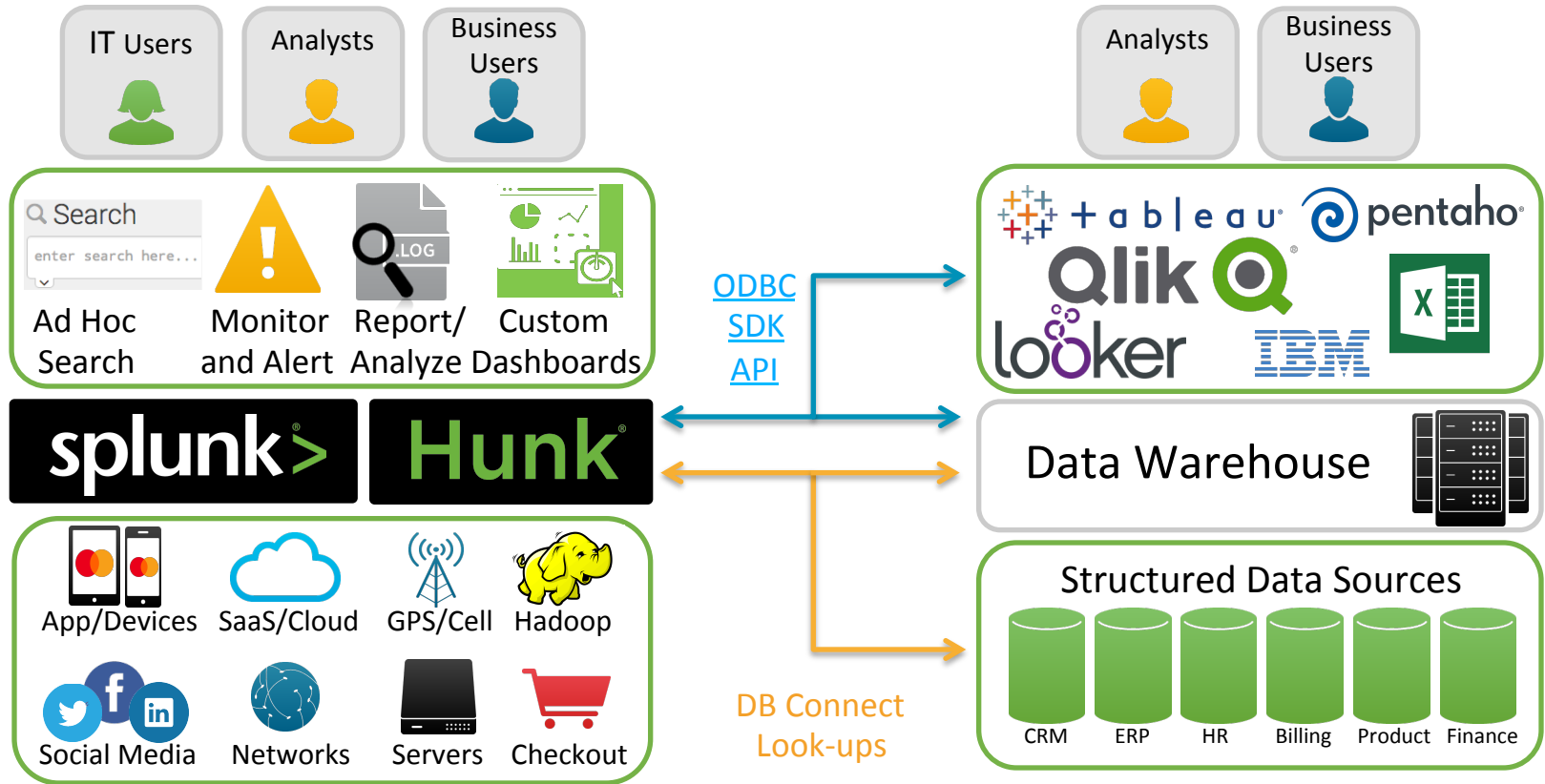
ENRICH MACHINE
DATA WITH
STRUCTURED DATA

The Power Of Partnership

.conf2016

splunk >

Splunk Completes Your Analytics Ecosystems

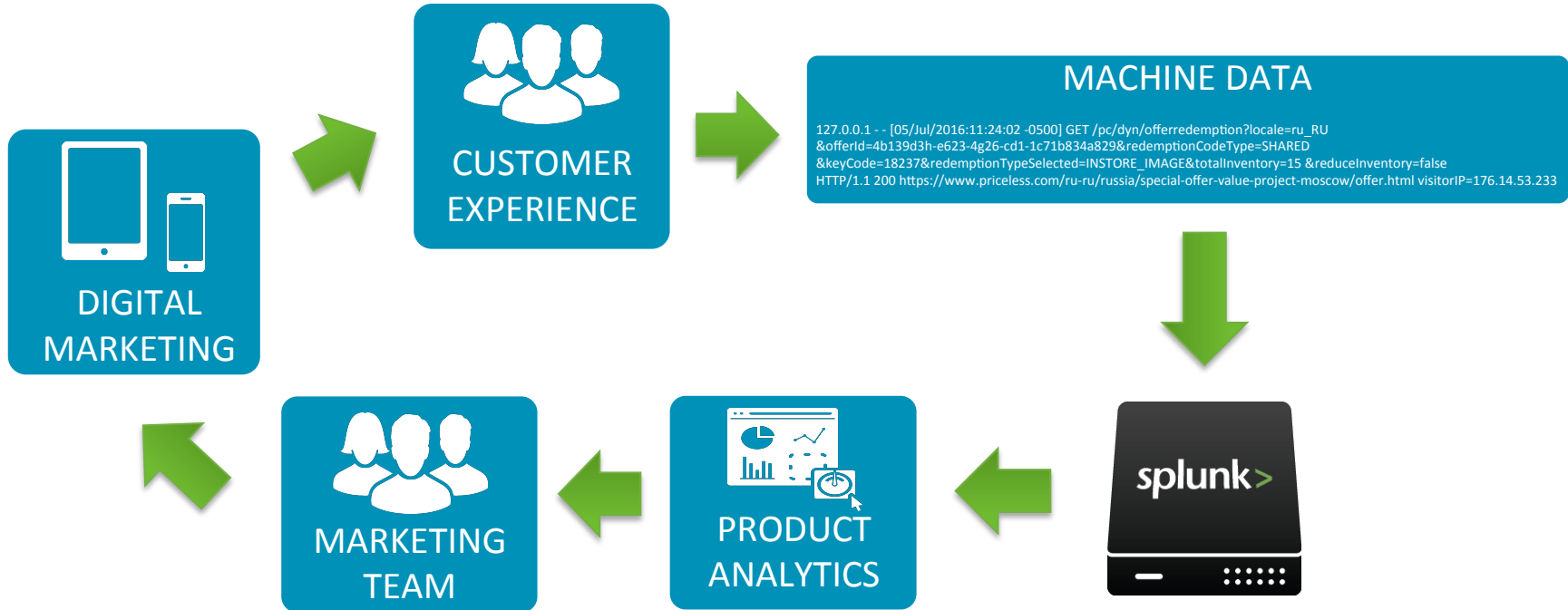


Analytics For Business Intelligence

.conf2016

splunk >

Using Business Intelligence To Change



Business Intelligence > Priceless.Com Reach



Machine Data: Where Does The Data Come From?

How is the Data Generated?

A single log event within your HTTP server may look something like this:

```
127.0.0.1 - - [05/Jul/2016:11:24:02 -0500] GET /pc/dyn/offeredemption?locale=ru_RU
&offerId=4b139d3h-e623-4g26-cd1-1c71b834a829&redemptionCodeType=SHARED
&keyCode=18237&redemptionTypeSelected=INSTORE_IMAGE&totalInventory=15 &reduceInventory=false
HTTP/1.1 200 https://www.priceless.com/ru-ru/russia/special-offer-value-project-moscow/offer.html visitorIP=176.14.53.233
```

Q: How does Splunk use this Data to transform it into Meaningful BI Analytics?

Splunk can transform the IP Addresses using the search commands [iplocation](#)^[4] and [geostats](#)^[5] which correlate data to display geographic data and summarize on an actual world map.

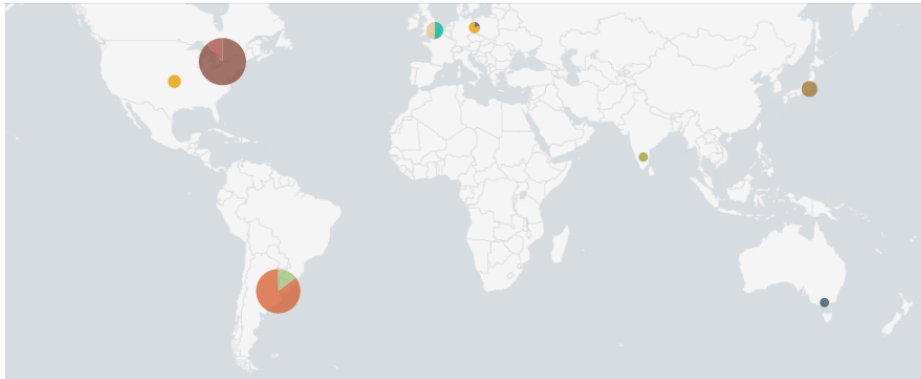
Business Intelligence: Global Awareness

Leveraging the Splunk Processing Language (SPL) in a search :

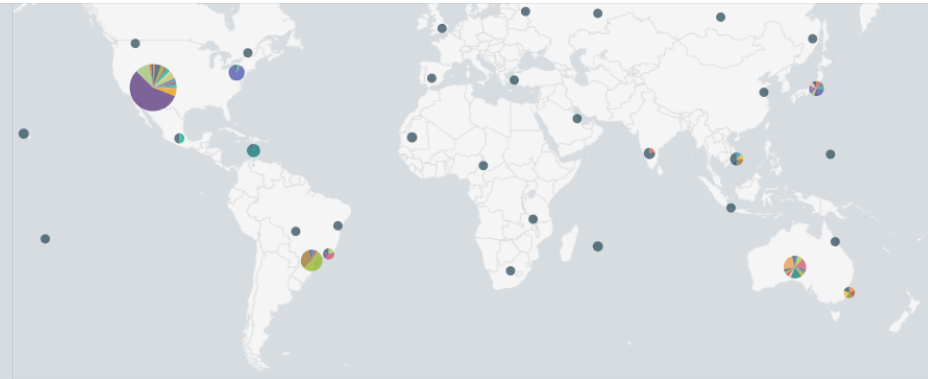
```
index="webindex" sourcetype="apache:access" priceless.com offerId | iplocation visitorIP | geostats count by visitorIP
```

Based on this search, Splunk is pinning visitorIP addresses to their origin on a map which allows us to achieve a global snapshot of visitor traffic by their region/market.

Offer Creators using the Admin Portal:



Card holders consuming Offers:



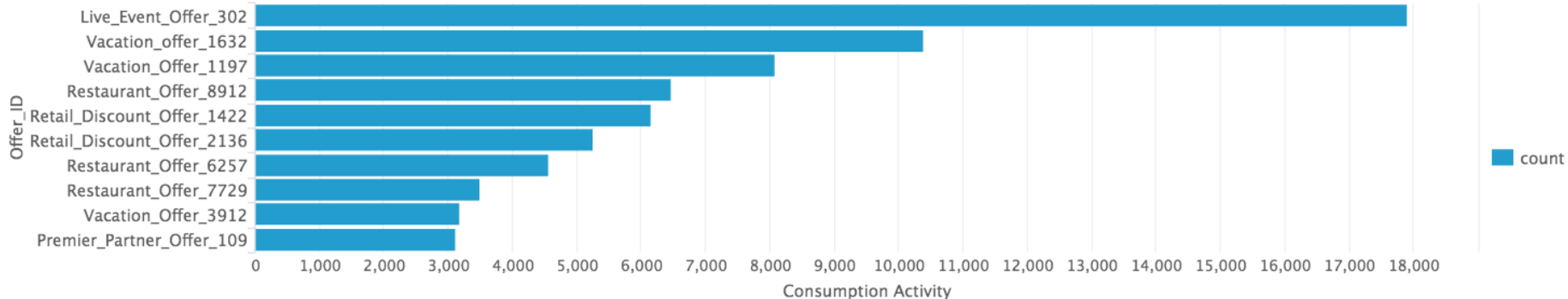
Business Intelligence: ROI

Offer and Program popularity in the market through recent or even real-time analysis. This helps illustrate Return on Investment (ROI) for specific marketing campaigns. Splunk uses machine data for analytics & this Business Intelligence easily:

```
index="webindex" sourcetype="apache:access" priceless.com offerId earliest=-30m | stats count by offerId | sort limit=10 -count
```

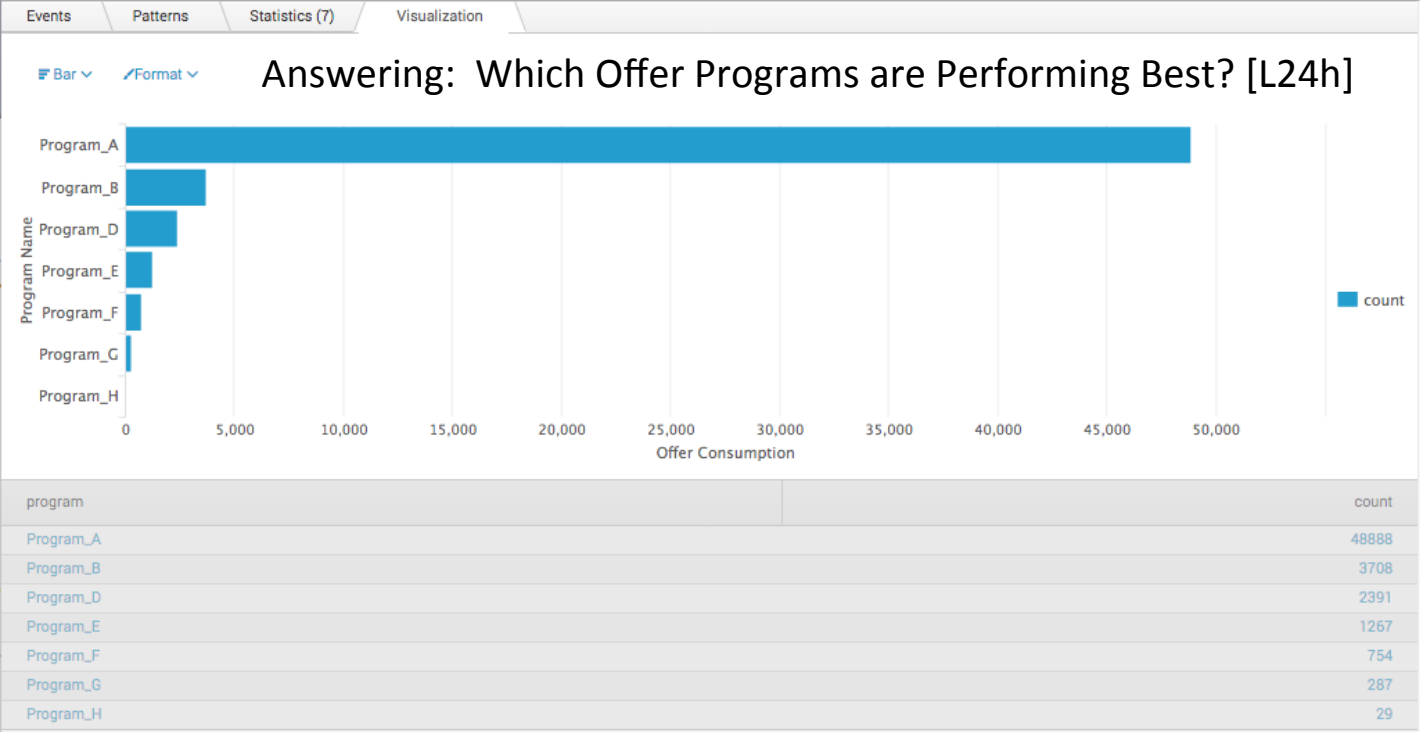
Top_10_Offers

Answering: Which Offer is Viewed Most? [Past 30 Minutes]



Business Intelligence: ROI

```
index="offersPlatform" service="OfferDisplayService" earliest=-24h | stats count by program | sort limit=10 -count
```

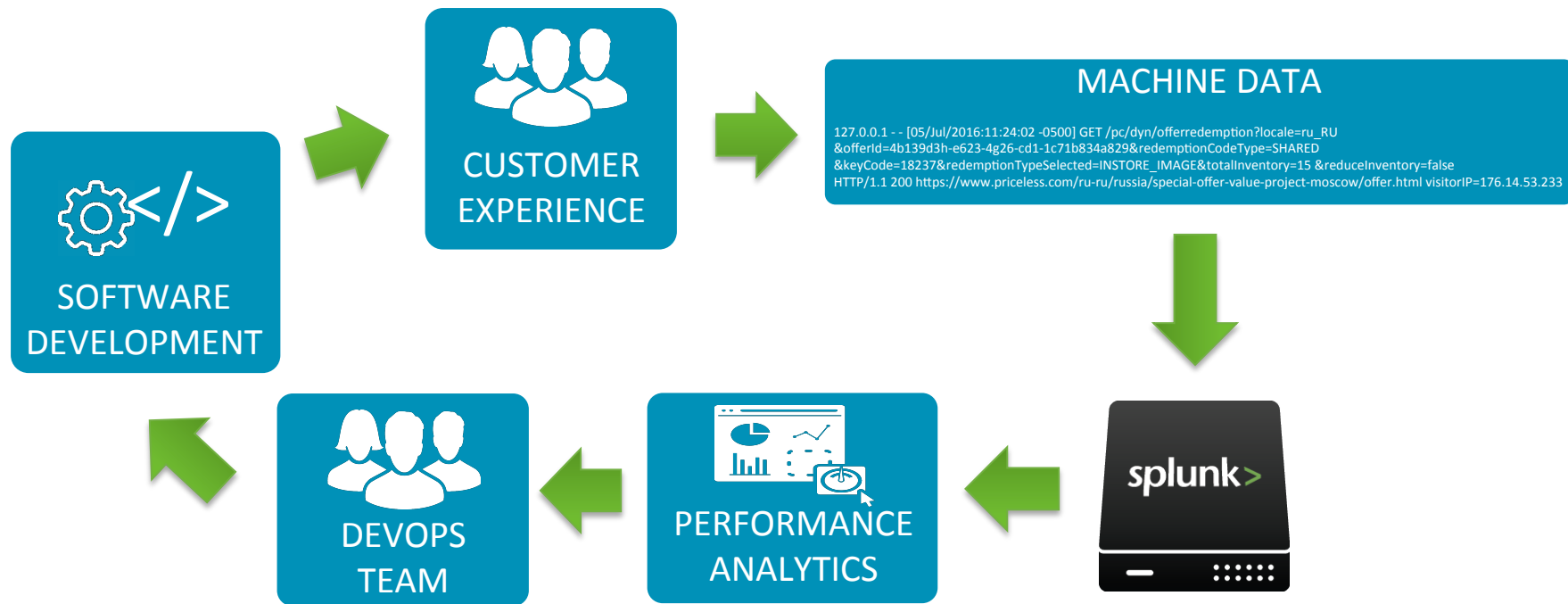


Analytics For Devops

.conf2016

splunk >

Devops: Using Analytics To Change

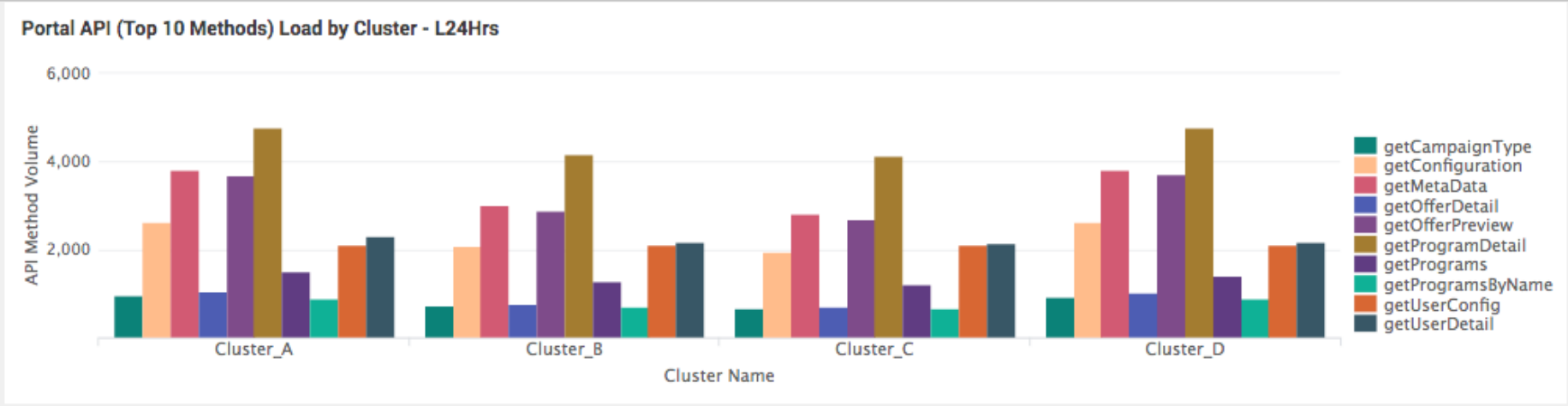


Devops: Portal API Load Per Cluster By Method

Search:

```
index="devops" sourcetype="offers:apiMetrics" server="Portal" | chart count by cluster, method useother=f
```

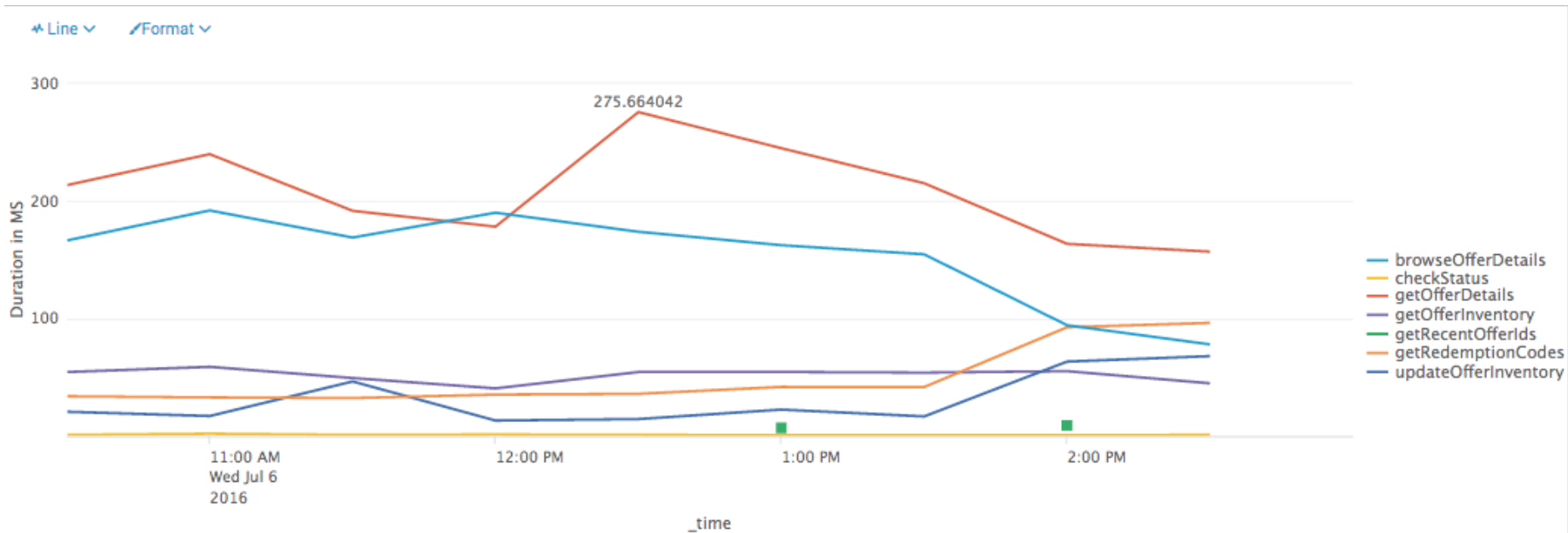
cluster	getCampaignType	getConfiguration	getMetaData	getOfferDetail	getOfferPreview	getProgramDetail	getPrograms	getProgramsByName
Cluster_A	948	2626	3809	1047	3696	4788	1500	903
Cluster_B	724	2076	3031	786	2901	4185	1282	710
Cluster_C	681	1951	2825	706	2684	4141	1223	659
Cluster_D	934	2641	3804	1028	3726	4774	1424	903



DevOps: API Method Response Times

Search:

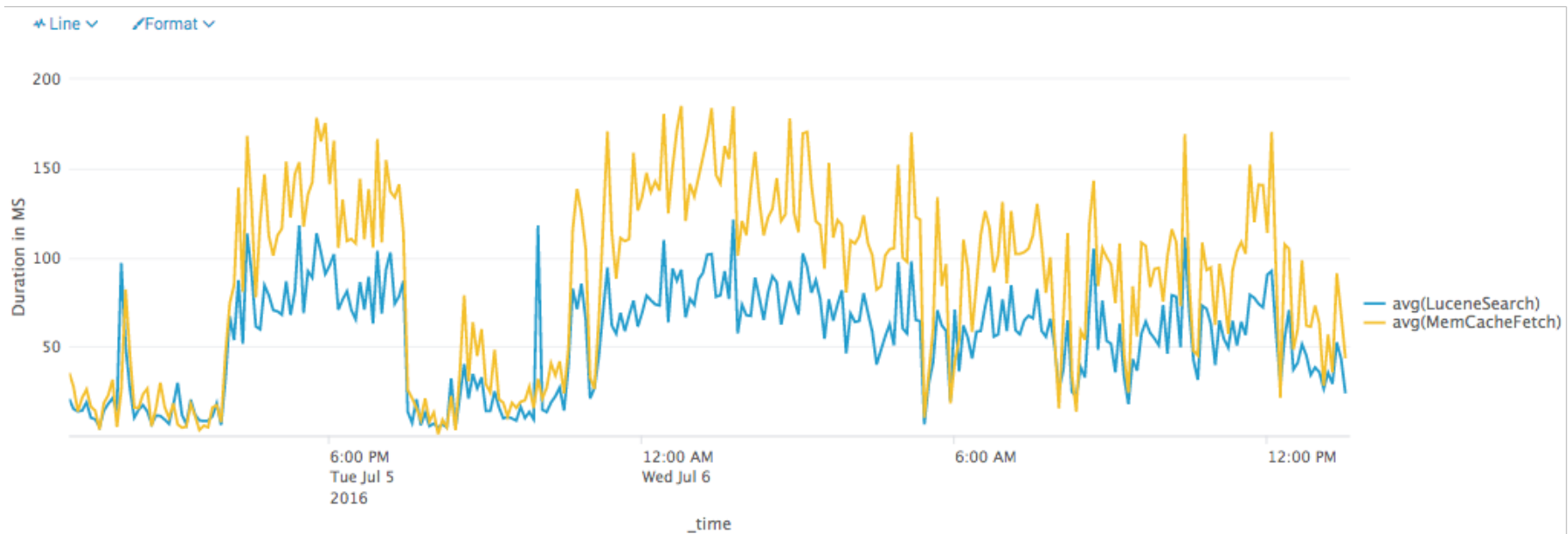
```
index="devops" sourcetype="offers:apiMetrics" server="Consumer" type="ServerResponse"  
| timechart span=1m eval(avg(totalTime)) by method
```



DevOps: Caching Technology Performance

Search:

```
index="devops" sourcetype="offers:caching" | eval LuceneSearch=LuceneSearchTime | eval MemCacheFetch=memcacheFetchTime | timechart span=5m avg(LuceneSearch), avg(MemCacheFetch)
```



DevOps: Deployment Activity Analytics

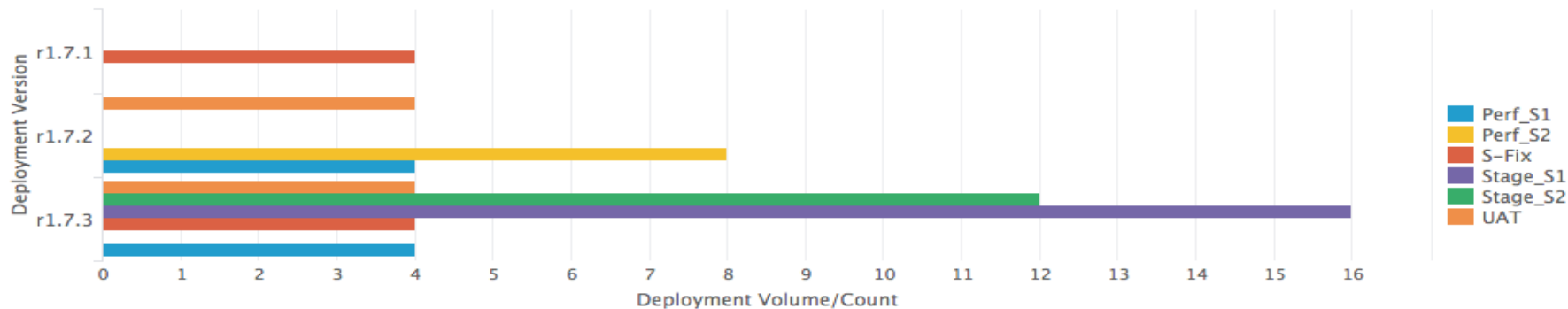
Search:

```
index="devops" sourcetype="offers:deployments" | chart count by deployment_artifact_version, host
```

Deployments by Version and Host L7Days

deployment_artifact_version	Perf_S1	Perf_S2	S-Fix	Stage_S1	Stage_S2	UAT
r1.7.1	0	0	4	0	0	0
r1.7.2	4	8	0	0	0	4
r1.7.3	4	0	4	16	12	4

Deployments by Version and Host L7Days - BarChart



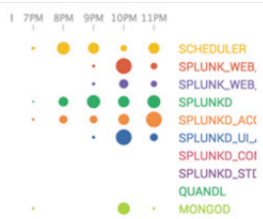
New Visualizations In Splunk 6.4

.conf2016

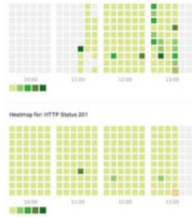
splunk >

New Advanced Visualization Options In 6.4

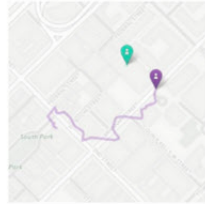
With the launch of 6.4 you have access to numerous new advanced visualizations that can be used in Search, on Dashboards, and in Reports!^[6]
See the Custom Visualization Documentation^[7] available: <http://docs.splunk.com/Documentation/CustomViz>



Punchcard



Calendar Heat Map



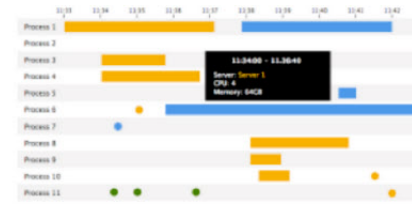
Location Tracker



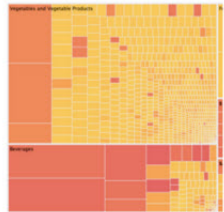
Sankey Diagram



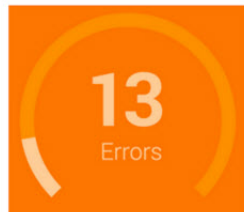
Bullet Graph



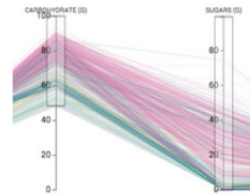
Timeline



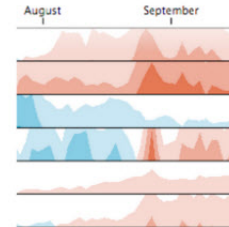
Treemap



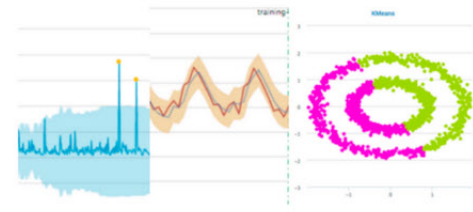
Horseshoe Meter



Parallel Coordinates



Horizon Chart



Machine Learning Charts

Q & A

.conf2016

Reference Links

1. http://www.splunk.com/en_us/solutions/solution-areas/business-analytics/odbc-driver.html
2. <http://dev.splunk.com/sdks>
3. <http://dev.splunk.com/restapi>
4. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/iplocation>
5. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/geostats>
6. <http://docs.splunk.com/Documentation/Splunk/6.4.1/AdvancedDev/CustomVizDevOverview>
7. <http://docs.splunk.com/Documentation/CustomViz>
8. https://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Business_Analytics.pdf

Tim Watkins: Contact Info



Tim.Watkins@mastercard.com



<https://www.linkedin.com/in/timothywatkins>

THANK YOU

.conf2016

