Leveraging Splunk Analytics For Business Intelligence And Devops

Tim Watkins
Senior Consultant, MasterCard
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
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
Splunk Completes Your Analytics Ecosystems

IT Users | Analysts | Business Users
---|---|---
Ad Hoc Search | Monitor and Alert | Report/Analyze Custom Dashboards

ODBC SDK API

Splunk > Hunk

App/Devices | SaaS/Cloud | GPS/Cell | Hadoop
---|---|---|---
Social Media | Networks | Servers | Checkout

Data Warehouse

Structured Data Sources

CRM | ERP | HR | Billing | Product | Finance

DB Connect Look-ups
Analytics For Business Intelligence
Using Business Intelligence To Change

CUSTOMER EXPERIENCE

MARKETING TEAM

PRODUCT ANALYTICS

MACHINE DATA

127.0.0.1 - - [05/Jul/2016:11:24:02 -0500] GET /pc/dyn/offeredemption?locale=ru_RU &offerId=4b139d3b-e623-4g26-cdf1-1c71b34a829&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
Business Intelligence > Priceless.Com Reach

https://www.priceless.com
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=4b139d3b-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

Answering: Which Offer is Viewed Most? [Past 30 Minutes]
**Business Intelligence: ROI**

Answering: Which Offer Programs are Performing Best? [L24h]

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program_A</td>
<td>48588</td>
</tr>
<tr>
<td>Program_B</td>
<td>3708</td>
</tr>
<tr>
<td>Program_D</td>
<td>2391</td>
</tr>
<tr>
<td>Program_E</td>
<td>1267</td>
</tr>
<tr>
<td>Program_F</td>
<td>754</td>
</tr>
<tr>
<td>Program_G</td>
<td>287</td>
</tr>
<tr>
<td>Program_H</td>
<td>29</td>
</tr>
</tbody>
</table>
Analytics For Devops
Devops: Using Analytics To Change

CUSTOMER EXPERIENCE

SOFTWARE DEVELOPMENT

DEVOPS TEAM

PERFORMANCE ANALYTICS

MACHINE DATA

Devops: Portal API Load Per Cluster By Method

Search:

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

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

<table>
<thead>
<tr>
<th>deployment_artifact_version</th>
<th>Perf_S1</th>
<th>Perf_S2</th>
<th>S-Fix</th>
<th>Stage_S1</th>
<th>Stage_S2</th>
<th>UAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>r1.7.1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>r1.7.2</td>
<td>4</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>r1.7.3</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>16</td>
<td>12</td>
<td>4</td>
</tr>
</tbody>
</table>

#### Deployments by Version and Host L7Days - BarChart
New Visualizations In Splunk 6.4
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! See the Custom Visualization Documentation available: [http://docs.splunk.com/Documentation/CustomViz](http://docs.splunk.com/Documentation/CustomViz)
Reference Links

Tim Watkins: Contact Info

Tim.Watkins@mastercard.com

https://www.linkedin.com/in/timothywatkins
THANK YOU