

splunk> .conf2017

Triggering Alerts with xMatters and Achieving Automated Recovery Actions from ITSI

Marty & Marty | Office of the CTO & ITOA Practitioner

9/27/2017 | Washington, DC

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. © 2017 Splunk Inc. All rights reserved.



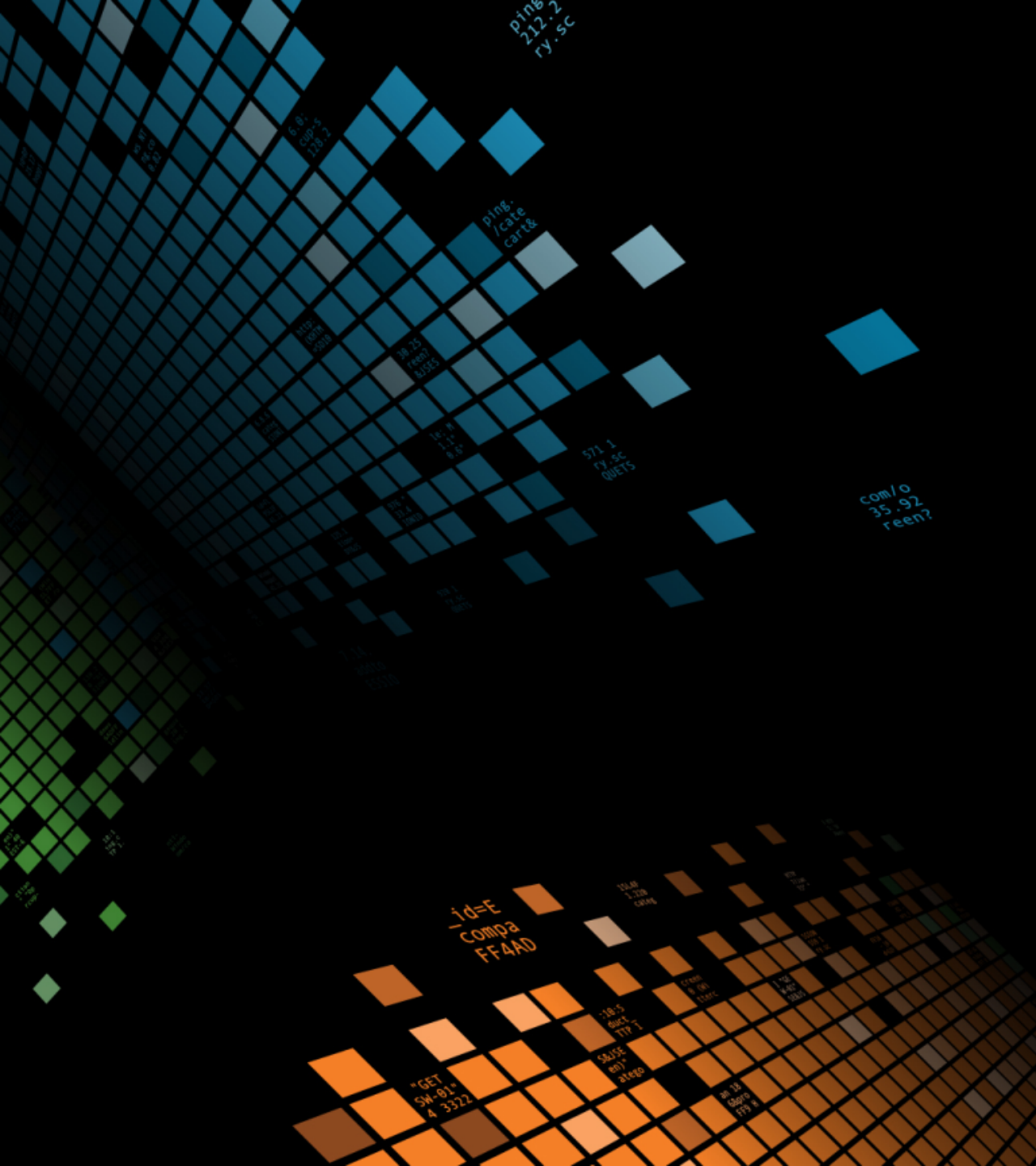
ITSI Alert Framework

Section subtitle goes here

Agenda

- ▶ What are Notable Event Alert Actions?
- ▶ Why do you need?
- ▶ How do you build them?
- ▶ Pitfalls & Gotchas

- ▶ **xMatters Deep Dive**



<Demo>

Section subtitle goes here

I Love ITSI's Notable Events


- ▶ But Management makes me forward events to <insert legacy manager here>
 - Sync back to OMI, Netcool/Omnibus, BPPM/Truesight, SCOM, ...
- ▶ But our incident police make us create incidents as well
 - Avoid having to swivel chair/manually open incidents in Service-Now, BMC/Remedy, ...
- ▶ But our notifications are managed in an alerting solution
 - You manage complex alerting/spoc/on call rules in xMatters, VictorOps, PagerDuty
- ▶ But I want to apply automated remediation actions like service restarts
 - You have a run book solution and workflows that you want to automatically initiate in <insert your run book solution here>





Mod Alerts and Notable Events


- ▶ Notable Event Actions build on top of Mod Alerts
- ▶ Mod Alerts are best kept in custom apps


- modular_alert_example/
 - metadata/
 - default.meta
 - default/
 - app.conf
 - alert_actions.conf
 - data/
 - ui/
 - alerts/
 - make_a_log_message.html
 - README/
 - alert_actions.conf.spec
 - appserver/
 - static/
 - applcon.png
 - bin/
 - modular_alert_example_app/
 - init .py
 - modular_alert.py


-  **Log Event**
Send log event to Splunk receiver endpoint

-  **Ping host**
Given one or more ITSI Notable Event, ping the 'host' in it.

-  **Run a script**
Invoke a custom script

-  **Send email**
Send an email notification to specified recipients

-  **Service Now Incident Integration**

-  **Webhook**
Generic HTTP POST to a specified URL

```

130.60.4 -- [07/Jan 18:10:57:153] "GET /ca
128.241.220.82 - - [07/Jan 18:10:57:123] "
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 1
itemId=EST-16&product_id=RP-LI-02" "0-
ofaction=purchase&is.com/rl
opping.com/category:screen?category_id=FLOWERS&SESSIONID=5D55LFFADFFC
category:screen?category_id=FLOWERS&SESSIONID=5D55LFFADFFC HTTP 1.1" 200 3885
link?item_id=EST-6&SESSIONID=5D55LFFADFFC HTTP 1.1" 200 3885 "http://butte
ngequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D55LFFADFFC HTTP
IFFAADF7 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category:screen?category_id=FI-SW-01"
ig.com/cart.do?action=purchase&itemId=EST-208&product_id=KQ-CW-01" "http://
'cup-shopping.com/category:screen?category_id=GIPTS" "http://
ipng.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"

```

ITSI Notable Events Add On

- ▶ Configured via notable_event_actions.conf
- ▶ What does notable event actions add?
 - Disabled = 0
 - Enabling/Disabling Actions for ITSI
 - Is the Action bulk compatible?
 - How often should it execute per group?



What Can You Do With The SDK?

- ▶ Get the event_id or any event field
 - Try that with your legacy Manager
- ▶ Get Configuration Setting
- ▶ CUD URL/Ticket Info
 - Add Knowledge Article/Instructions Link to Event or Event Group
 - Add link to Ticket or Notification/Outage Board/External App
- ▶ CRUD Comments
- ▶ RU Status
- ▶ CRUD Owner
- ▶ Log to _internal



Sir Spikensons

.conf Example – Trello Outage Board

- <https://github.com/mwiser/itsi-trello-board.conf>



```

event_id = payload['result']['event_id']
session_key = payload['session_key']
myboard="4978c0fb1d5db6908f3e618e"
urlstring = "https://api.trello.com/1/lists/"+myboard+"/cards"
logger.info("Session Key:"+session_key+" event id:"+event_id)
title=payload['result']['title']
description=payload['result']['description']
mykey = 'f1b83a540065a0aa7d4e1b2c0199c3e8'
mytoken='14ac1c8ac6950f0d666cf8f6db7c59ffb92c49412f55cf6942f5368d7ab05936'
payload = {'descData': 'MyDescData', 'dueComplete': 'true', 'due': '2017-04-07T21:26:00.365Z', 'name': title, 'desc': description, 'key': mykey}
r = requests.post(urlstring, data=payload)
event = Event(session_key, logger)
event.create_comment(event_id, "Trello Message has been created")

```

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CU-01"
ows NT 5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"

```



Practical Use Cases

Section subtitle goes here

Service Management

This is where the subtitle goes

▶ Service-Now

- <https://splunkbase.splunk.com/app/1928/>
- ~5k Downloads – one directional

▶ BMC-Remedy

- <https://splunkbase.splunk.com/app/3087/>
- ~ 600 Downloads – one directional

▶ Bi-Directional:

- Field Developed Guide email: mwiser@splunk.com

▶ CMDB Enrichment Out of the box

- Support Group
- Location, Region, DC
- Class of Service/Dependency

▶ CMDB Enrichment via DBConnect or input-lookups/Rest Calls



Event Management Integrations

- ▶ Common Capability across Every Event Management solution
 - SNMP Traps
- ▶ HP Openview/OMI
 - opcmmsg – Make sure you open the OMI interface policy for the ITSI Server
- ▶ IBM Netcool
 - Omnibus Nco_postmsg or TEC – poste(is)msg or postzmsg
- ▶ BMC BPPM/Truesight
 - msend/mposter
- ▶ Microsoft SCOM
 - set-scomalert (Updates) & OMTestTool.msi



Run Book Automation Frameworks

- ▶ Common Across Most Run Book Solutions
 - Web Service Endpoints (Rest/Soap) and http post triggers
- ▶ Resolve Systems
 - <https://splunkbase.splunk.com/app/3331/>
- ▶ BMC Atrium Orchestrator
 - Rest/Soap/http
- ▶ HP Operations Orchestration
 - Rest/Soap



Pitfalls and Gotchas

► For Splunk Cloud customers

- Data Transfer has to be encrypted
- Alert Action has to go through certification process

► UI Based Backups

- Splunk ITSI Backups (UI/kvstore2json) do back up the KV store
- BACKUPS DO NOT BACKUP ALERT CONFIGURATION (file system backup)

► Including Splunk SDK for more advanced use cases

- If you want to enrich the data after the fact – look up support groups for handoff or more robust ML – have email notifications outside of the standard template

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-189"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-188"

```



Operational Status

BUSINESS

Sales

●

Shipping

●

Support

●

APPLICATIONS



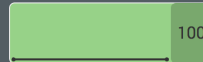
Customer Facing

- Web Store
- Mobile App



Corporate

- Email
- Intranet



Engineering

- Release Status
- Bugs



OVERSIGHT



SLAs

- Time to Respond
- Time to Resolve



Compliance

- AD Edits
- Regulatory



Incidents

- P1
- New



Security

- Malware
- Firewall Events

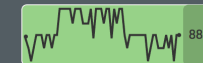


INFRASTRUCTURE



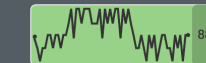
Compute

- Servers
- Storage



Network

- WAN
- LAN



Identity Services

- Active Directory
- PKI



Data Centers

- US1
- US2



Cloud

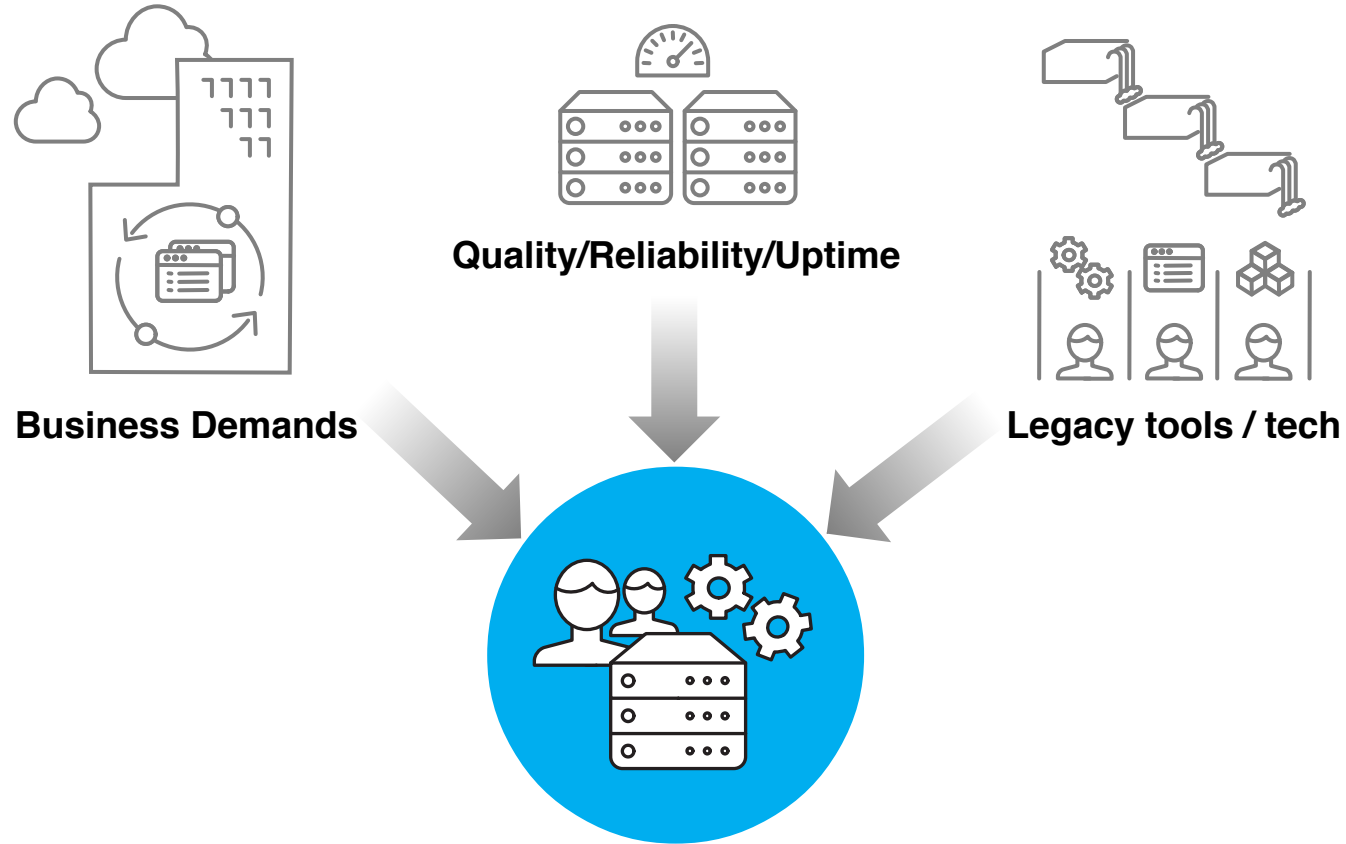
- US East
- US West

**As Martin
Mentioned**

The Value of ITSI
data...but how do we
leverage that value?



IT Is Challenged To Operate With More Agility And Velocity

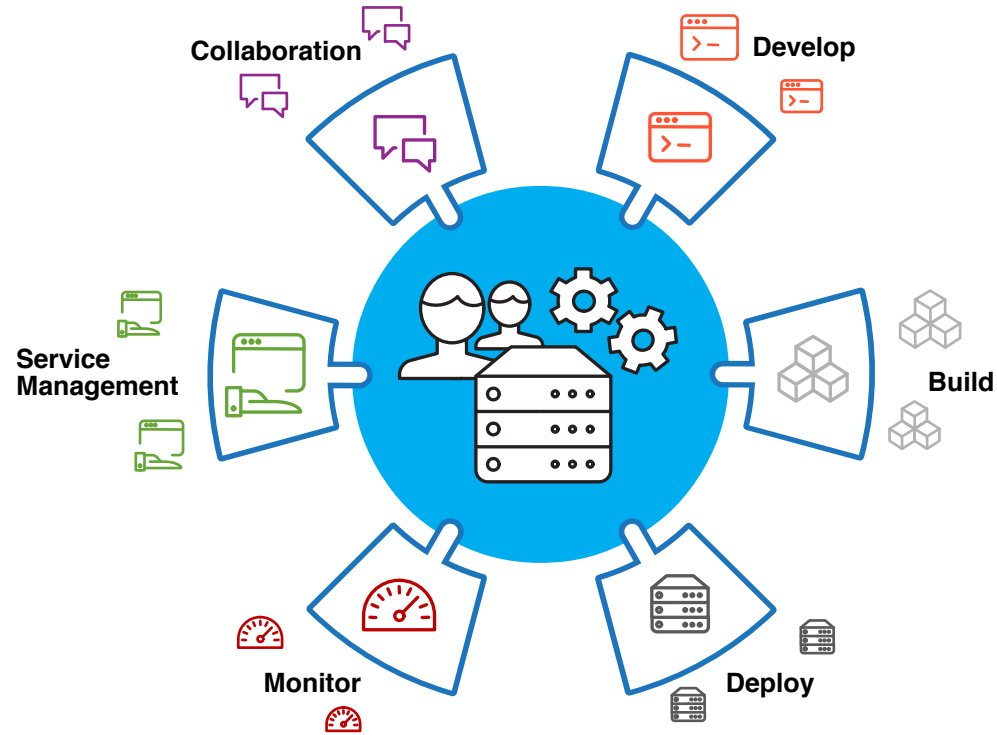


Confidential and Proprietary

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CU-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
```

IT Organizations Have Been Taking Steps To Evolve

... by adopting new tools and processes

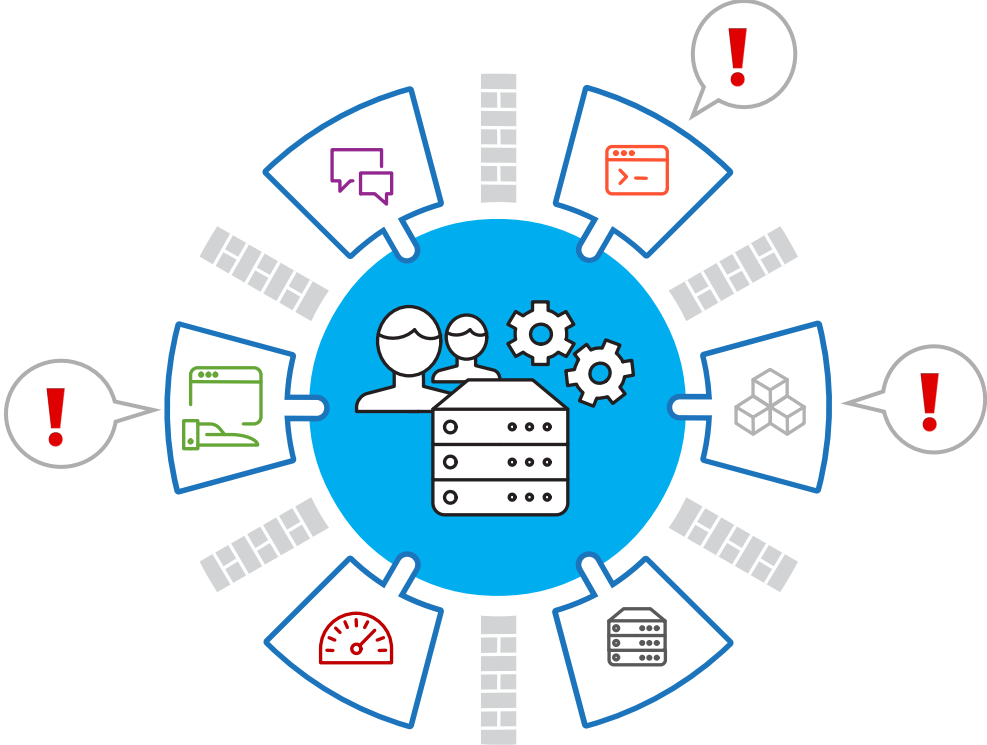


130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" Moz/1.12.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" Moz/1.12.0
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" Moz/1.12.0
10.0.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" Moz/1.12.0
10.0.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" Moz/1.12.0
10.0.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" Moz/1.12.0

Confidential and Proprietary

Barriers Still Exist That Prevent Agility

... due to lack of integration and automation

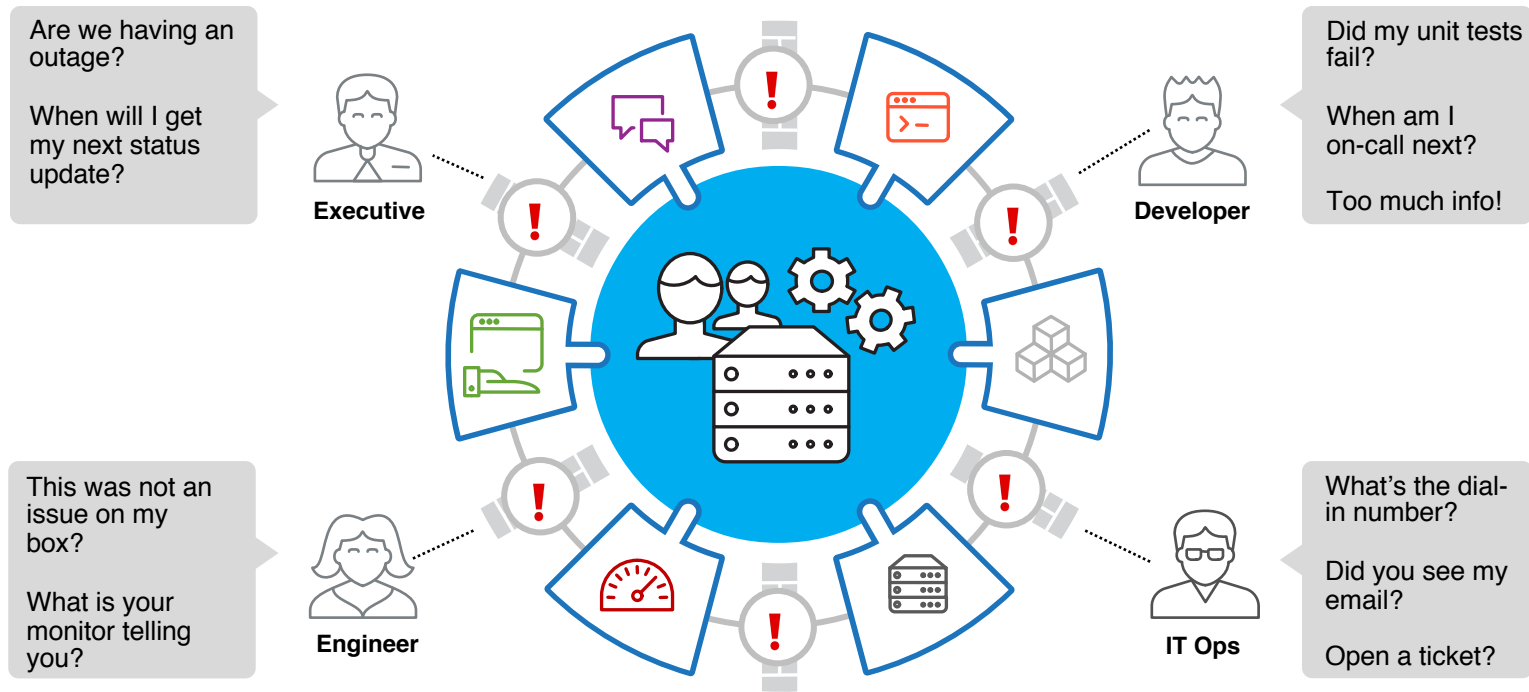


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17.14.11 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
... [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
... [07/Jan 18:10:57:123] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17.14.11 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
```

Confidential and Proprietary

Add Disconnected Communication To The Equation

... and automation can become compromised



```

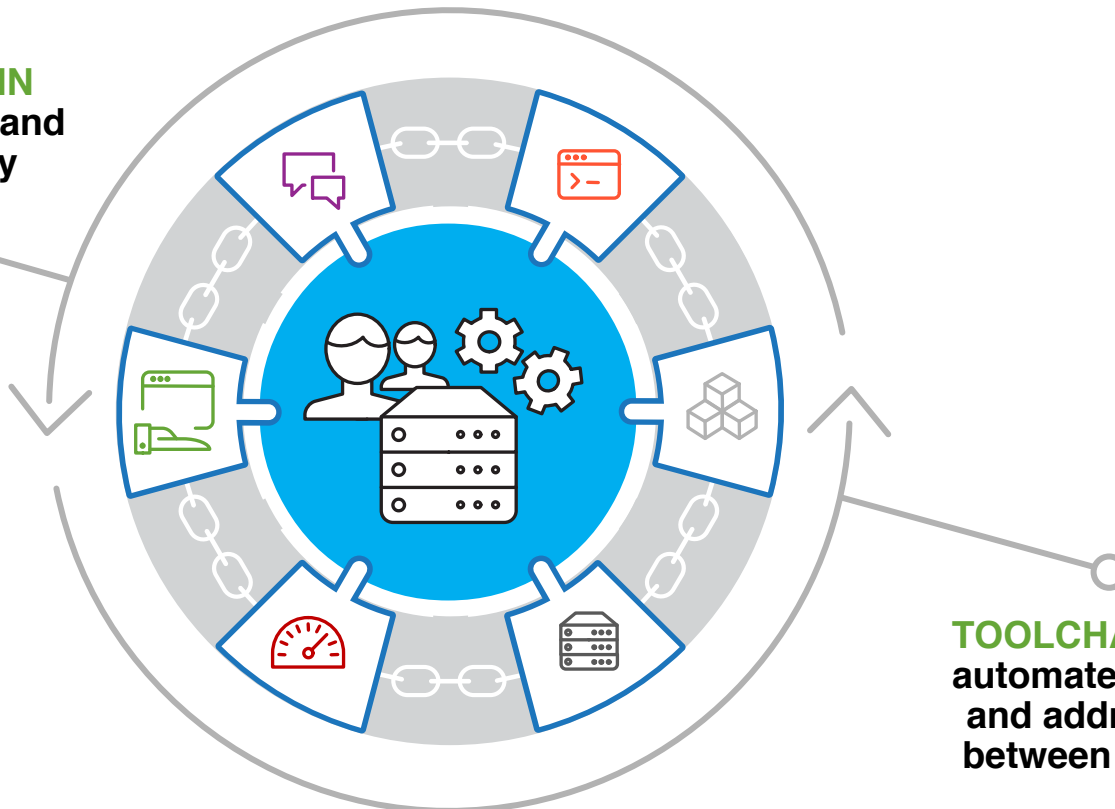
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" Moz/1.1.7.0 "comp11111"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CW-01" Moz/1.1.7.0 "comp11111"
ows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?category_id=FL-DSH-01&JSESSIONID=5D35L7FFGADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55LFF2ADFF3" Moz/1.1.7.0 "comp11111"
itemId=EST-16&product_id=RP-LI-02)" 468 125.17 14.1.1.189] "GET /cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D18SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CW-01" Moz/1.1.7.0 "comp11111"
do?action=purchase-shopping_id=RP-LI-02)" 468 125.17 14.1.1.189] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55LFF2ADFF3" Moz/1.1.7.0 "comp11111"
buttercup-shopping.com/oldlink?item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55LFF2ADFF3" Moz/1.1.7.0 "comp11111"
buttercup-shopping.com/oldlink?item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55LFF2ADFF3" Moz/1.1.7.0 "comp11111"

```

Confidential and Proprietary

Toolchains Allow IT To Align Tools And Activities And Are Required To Deliver Agility

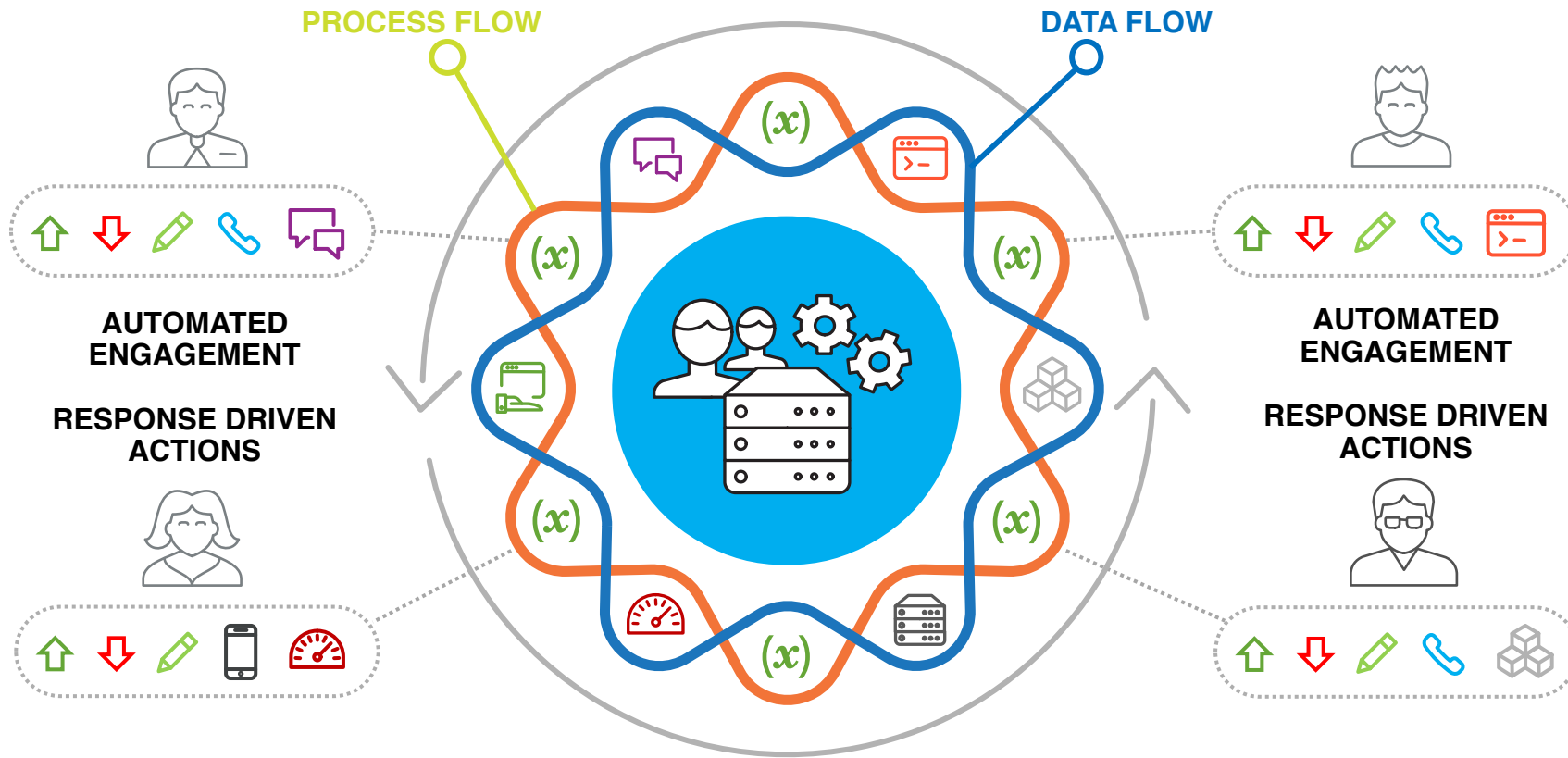
Connected **TOOLCHAIN** should enable IT agility and faster service delivery



TOOLCHAINS must automate hand-offs and address gaps between solutions

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0" "909499-20
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20
ows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20
://buttercup-16&product_id=RP-LI-02" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20
action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20
/shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20
/buttercup-16&product_id=RP-LI-02" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0" "508111-20

Enhance Your Toolchain Links With Xmatters Intelligent Communication



Confidential and Proprietary

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
 10 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
 10 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
 10 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
 10 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"

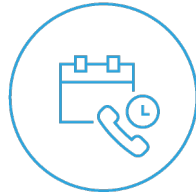
Features

ITSI value is extended with xMatters capabilities

Available Enterprise & Cloud



Dynamic Call Schedules



Intelligent Communications



Targeted Alerts & Notifications

Voice, Push, SMS, Email, Fax, etc.



Automated Work Flow and Closed Loop



Mobile Push with Actions



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.1 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.1 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.1 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0"
```

So, What's Possible?

Love your ITSI data? Share the LOVE



- 1 When Notable Events meet predetermined criteria, xMatters can automatically relay critical Splunk ITSI data to the correct people and systems - can also be manual
- 2 Create a service management ticket with Splunk ITSI insights
- 3 Invite people across multiple teams to a conference call with context from Splunk ITSI
- 4 Initiate a targeted chat room via Slack, HipChat or Hubot
- 5 Record chat room activity back into a service management ticket
- 6 Record assignee, severity, and status comments back to the Splunk Notable Events dashboard

“Live Demo”

Want more?

Download the integration at: <https://splunkbase.splunk.com/app/3598/>

Visit us at booth #xxxx for more demo goodness

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017

Want to Learn More About ITSI at .conf2017?

Tuesday
September
26th, 2017

- ▶ **Ready, Set, Go! Learn From Others - The First 30 Day Experiences of ITSI Customers:** Tuesday, September 26th, 2017 12:05 PM- 12:50 PM Room Salon C
- ▶ **Splunk ITSI Overview:** Tuesday, September 26th, 2017 1:10 PM-1:55 PM Room 147 AB
- ▶ **PWC: End-to-End Customer Experience:** Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room 143ABC
- ▶ **RSI: Operational Intelligence: How to go From Engineering to Operationalizing IT Service Intelligence Where the Rubber Meets the Road:** Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room147AB
- ▶ **Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI:** Tuesday, September 26th, 2017 3:30 PM-4:15 PM Room143ABC
- ▶ **ITSI in the Wild - Why Micron Chose ITSI and Lessons Learned From Real World Experiences:** Tuesday, September 26th, 2017 4:35 PM- 5:20 PM Room Salon C

Wednesday
September
27th, 2017

- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:** Wednesday, September 27th, 2017 11:00 AM-11:45 AM Ballroom C
- ▶ **Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI:** Wednesday, September 27th, 2017 1:10 PM- 1:55 PM Room Salon C
- ▶ **Leidos - Our Journey to ITSI:** Wednesday, September 27th, 2017 2:15 PM-3:00 PM Room147AB
- ▶ **How Rabobank's Monitoring Team Got a Seat at the Business Table by Securing Sustainability on Competitive Business Services Built on Splunk's ITSI:** Wednesday, September 27th, 2:15-3:00pm Room 147AB
- ▶ **Here Comes the Renaissance: Digital Transformation of the IT Management Approach:** Wednesday, September 27th, 2017 3:30 PM-4:15 PM Room Salon C

Thursday
September
28th, 2017

- ▶ **The ITSI 'Top 20' KPI's:** Thursday, September 28th, 2017 10:30 AM-11:15 AM Room Salon C
- ▶ **Automation of Event Correlation and Clustering with Machine Learning Algorithms – An ITSI Tool:** Thursday, September 28th, 2017 11:35 AM- 12:20 PM Room Salon C
- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:** Thursday, September 28th 11:35 AM - 12:20 PM in Ballroom B
- ▶ **IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI:** Thursday, September 28th, 2017 1:20 PM-2:05 PM Room Salon C