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.

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>

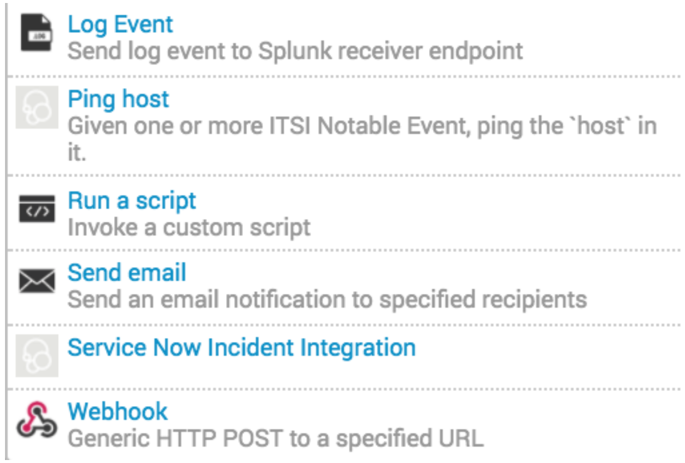
Section subtitle goes here

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/
                - appIcon.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

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?

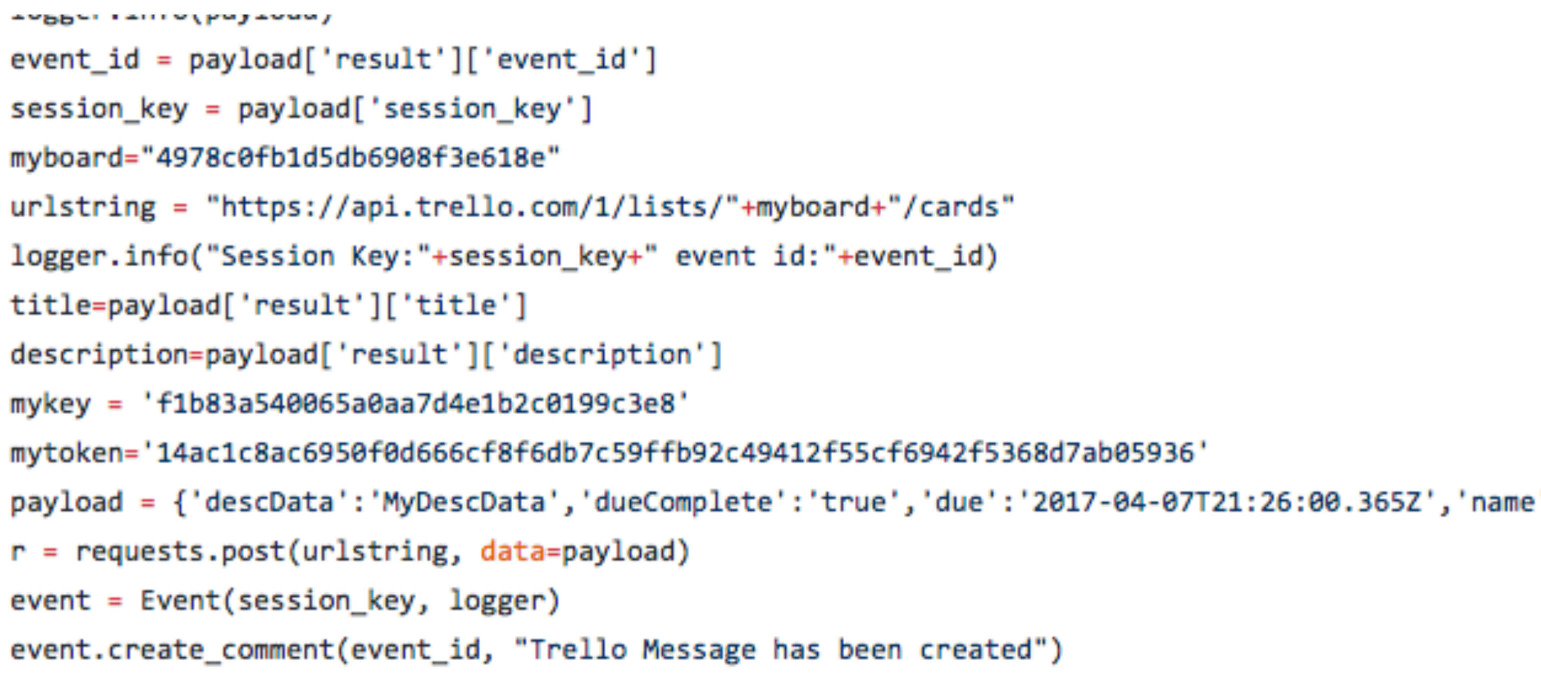
What Can You Do With The SDK?

- 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/Externa 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



```
logger.info(payload)
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':myke
r = requests.post(urlstring, data=payload)
event = Event(session_key, logger)
event.create_comment(event_id, "Trello Message has been created")
```

splunk> .conf2017

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
  - opcmsg – 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

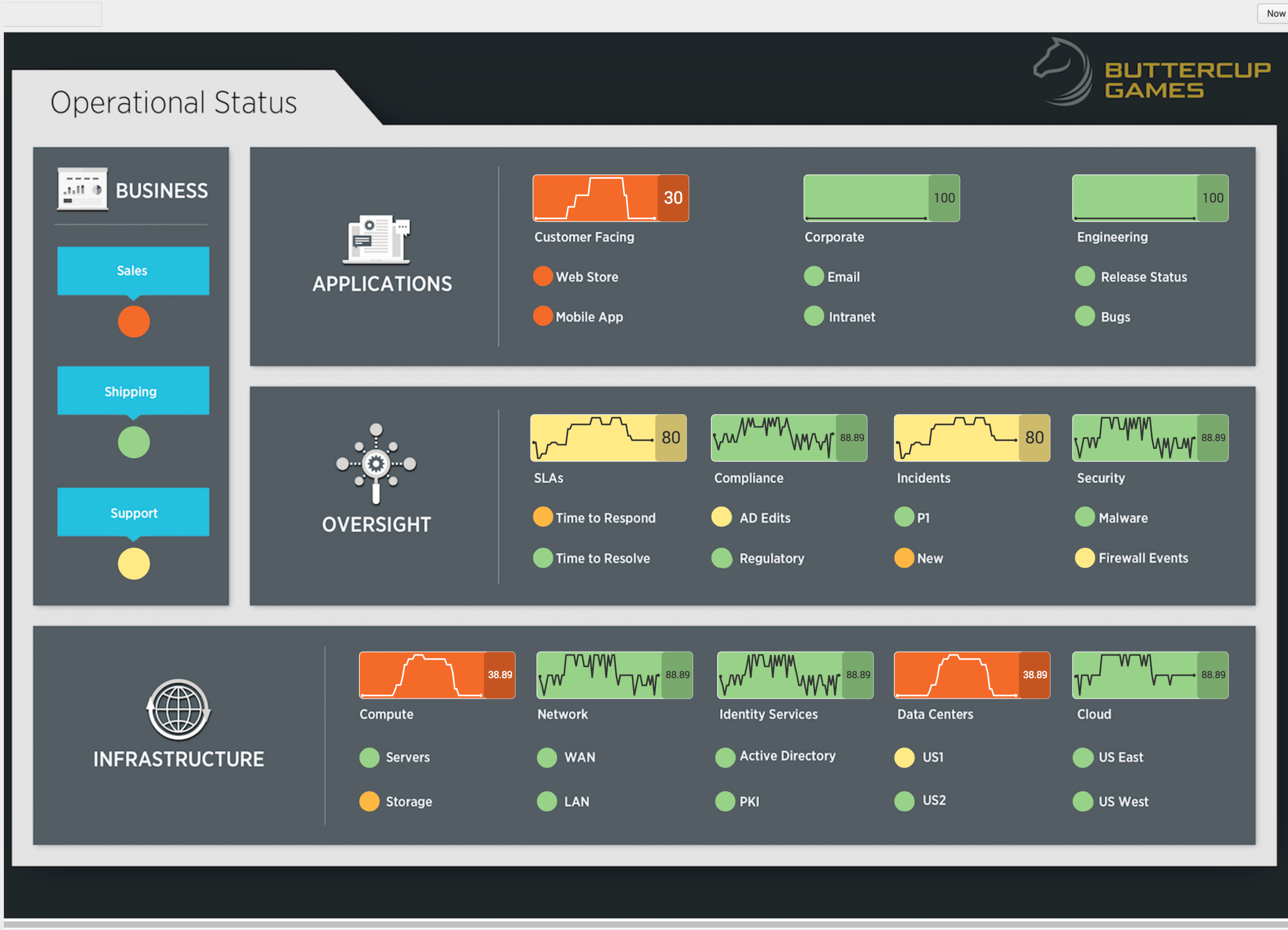
- Common Across Most Run Book Solutions
  - Web Service Endpoints (Rest/Soap) and http post triggers
- Resolve Systems
  - https://splunkbase.splunk.com/app/3331/
- BMC Atrium Orchestrator
  - Rest/Soap/http
- HP Operations Orchestration
  - Rest/Soap

Pitfalls and Gotchas

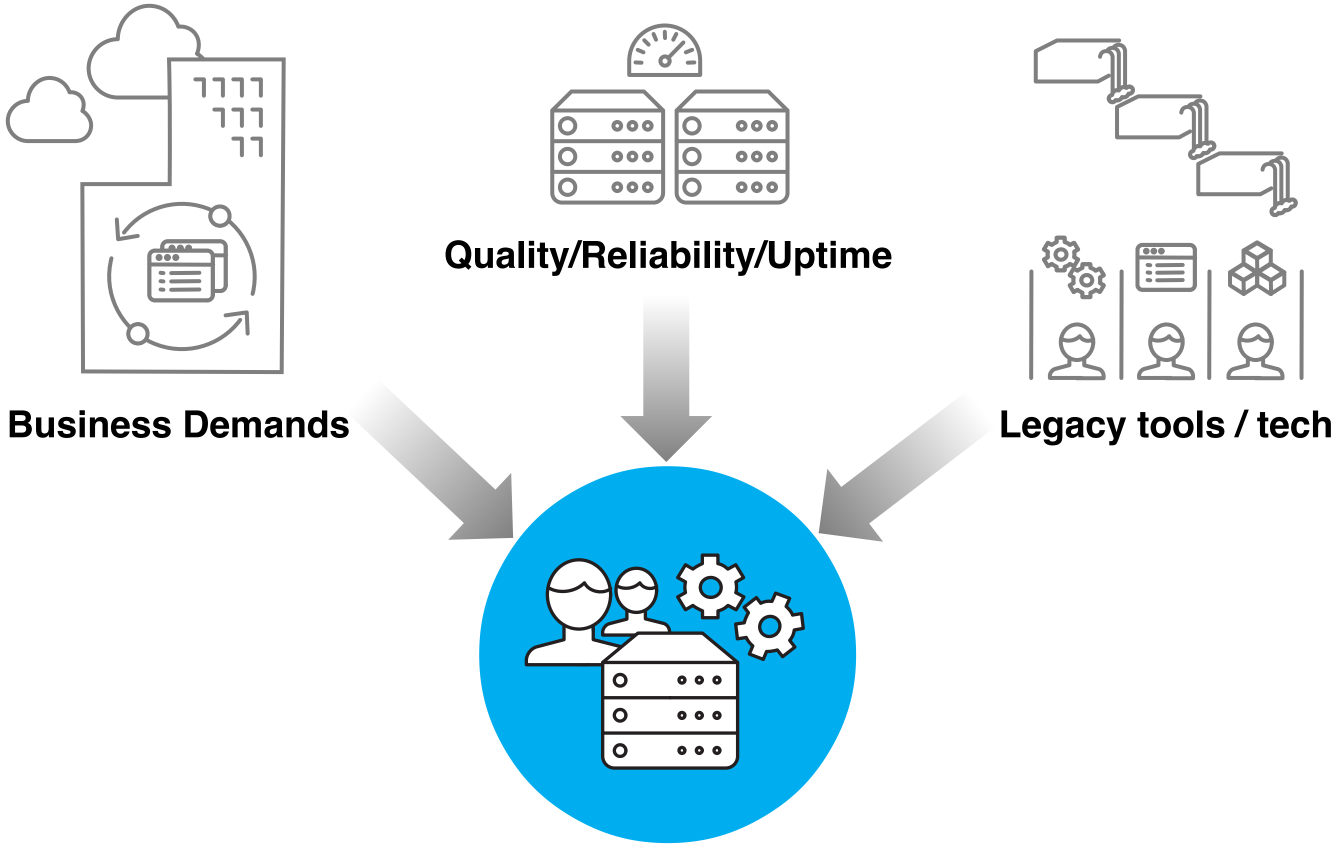
- For Splunk Cloud customers
  - Data Transfer has to be encrypted
  - Alert Action has to go through certification process
- UI Based Backups
  - Splunk ITSI Backups (UI/kvstore2json) do back up the KV store
  - BACKUPS DO NOT BACKUP ALERT CONFIGURATION (file system backup)
- Including Splunk SDK for 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

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



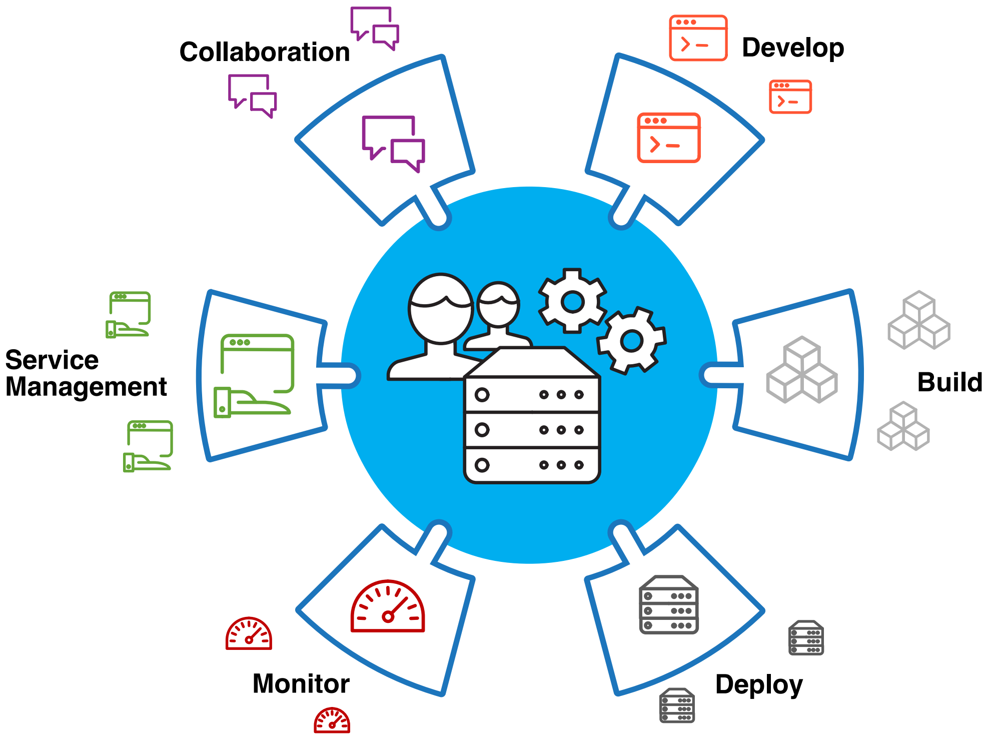
Quality/Reliability/Uptime

Business Demands

Legacy tools / tech

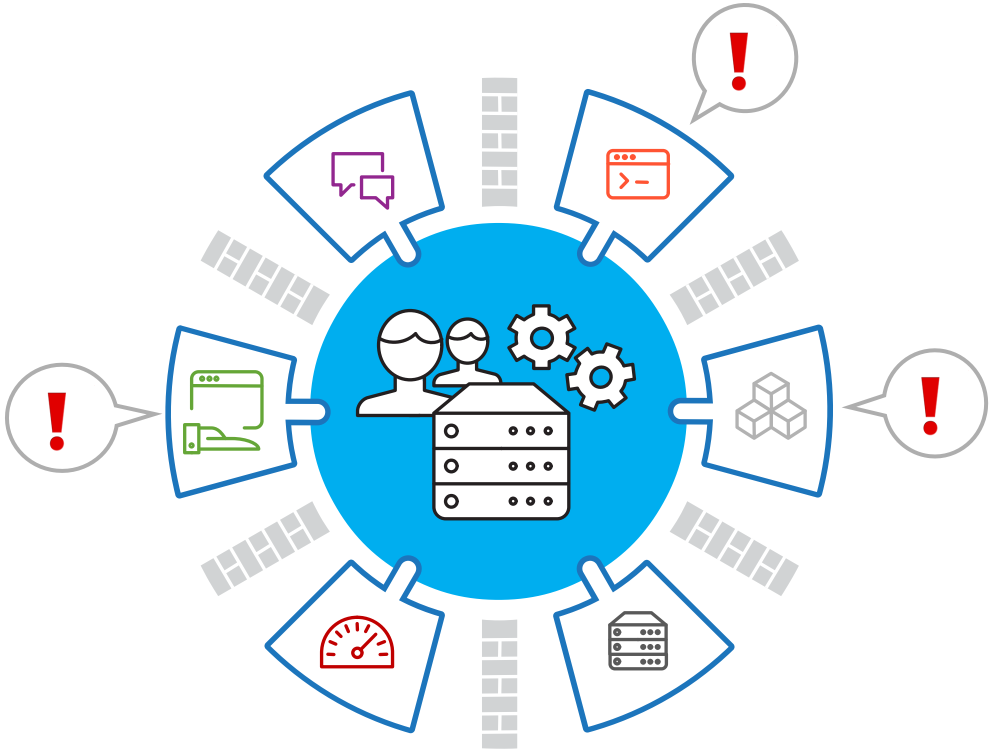
IT Organizations Have Been Taking Steps To Evolve

… by adopting new tools and processes



Barriers Still Exist That Prevent Agility

… due to lack of integration and automation



Add Disconnected Communication To The Equation

… and automation can become compromised

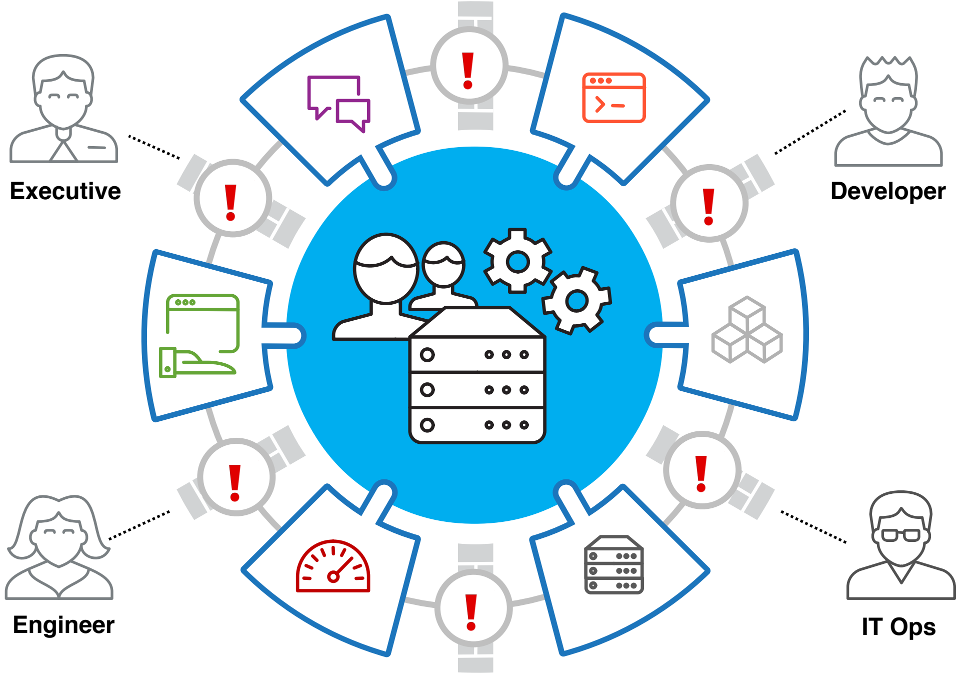
Are we having an outage?

When will I get my next status update?

Did my unit tests fail?

When am I on-call next?

Too much info!



This was not an issue on my box?

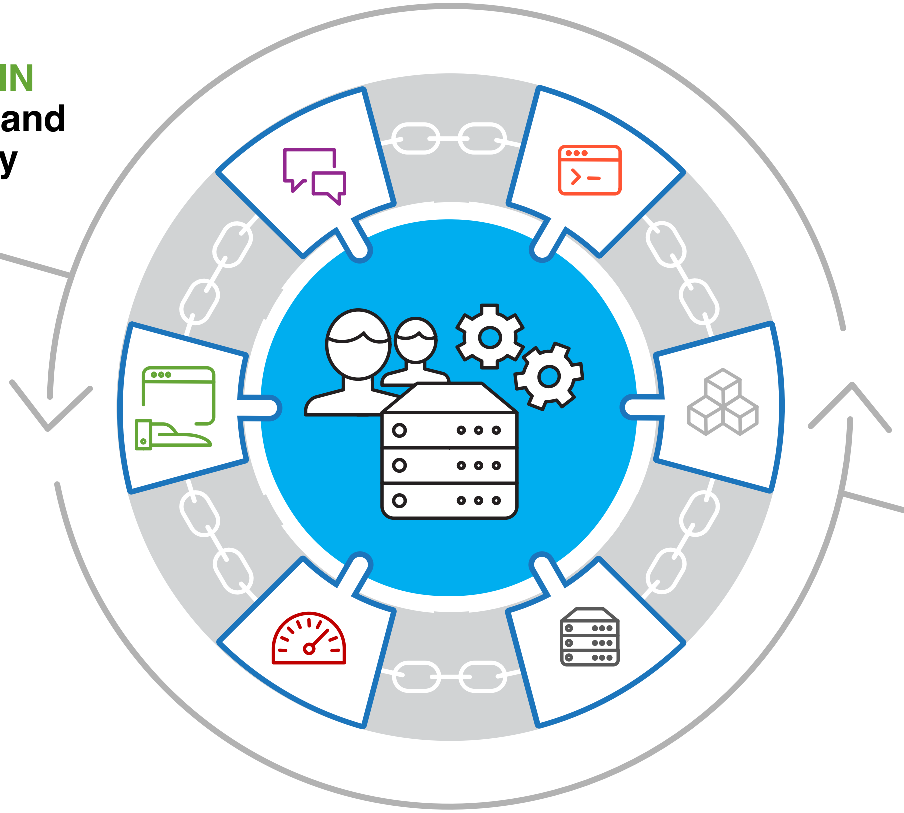
What is your monitor telling you?

What's the dial-in number?

Did you see my email?

Open a ticket?

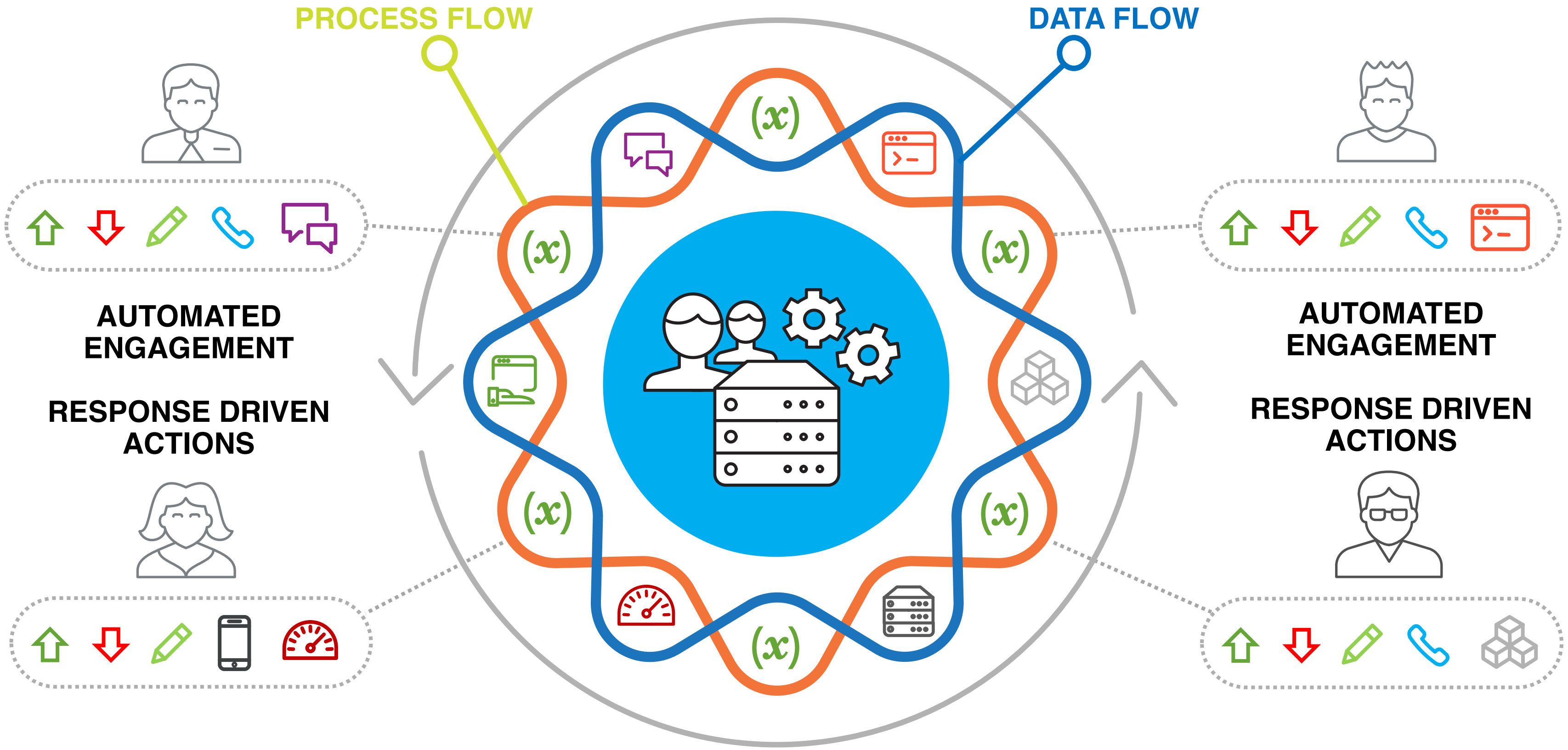
Toolchains Allow IT To Align Tools And Activities And Are Required To Deliver Agility



Connected TOOLCHAIN should enable IT agility and faster service delivery

TOOLCHAINS must automate hand-offs and address gaps between solutions

Enhance Your Toolchain Links With Xmatters Intelligent Communication



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

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"

splunk> .conf2017

Want more?

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

Visit us at booth #xxxx for more demo goodness

splunk> .conf2017

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, 201712:05 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, 20173:30 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, 201711:00 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

splunk> .conf2017