Soup to Nuts SRE:

How to leverage ITSI, VictorOps and Phantom to be a site reliability engineering super hero

Chris Crocco
Senior Sales Engineer | Splunk

splunk> .conf19

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.

What is SRE?

And why is my boss so excited about it?

.conf19
splunk>

Site Reliability Engineering is….

1. A set of core tenants adhered to by SRE teams to ensure the day to day operational requirements of their service are met.

2. Meant to ensure focus remains on engineering, not operations

3. A mechanism to maximize the pace of innovation and product stability

4. A way to ensure your resources and capacity are in line with scheduled deployments

5. Most importantly…..a little different for everyone!

Site Reliability Engineering should not be….

1. A catch all for the Dev teams deployment work
2. A strictly operational mindset
3. A single point of contact for all teams
4. ”In Charge” of DevOps team priorities
5. A “by the book” organization

Who should be Site Reliability Engineer?

1. Highly technical and top performing resources from your traditional ops team
2. Problem solvers
3. Curious and creative individuals
4. Self-directed and team focused

SRE and DevOps

Different roles with the same goals

How people think DevOps and SRE work together

I'm the SRE and you're doing it wrong!
Whatever, I'm in DevOps and I know my code is good.

How DevOps and SRE should work together

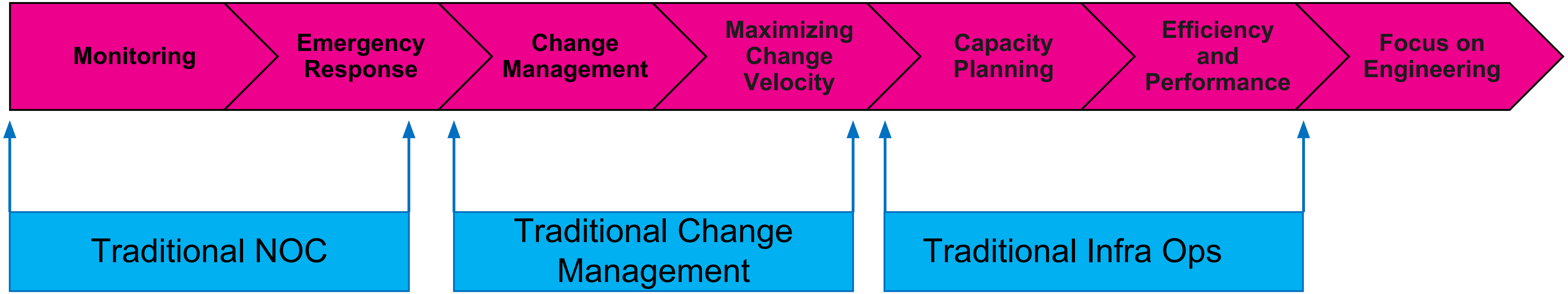
I'm the SRE and I found this as the root cause of that event, you might want to check it out.
Thanks man! I'm gonna do a bug fix for that since I'm DevOps

Tenants of SRE

The core of what your SRE team should be doing

Core Tenants

Building blocks for success



Monitoring

Emergency Response

Change Management

Maximizing Change Velocity

Capacity Planning

Efficiency and Performance

Focus on Engineering

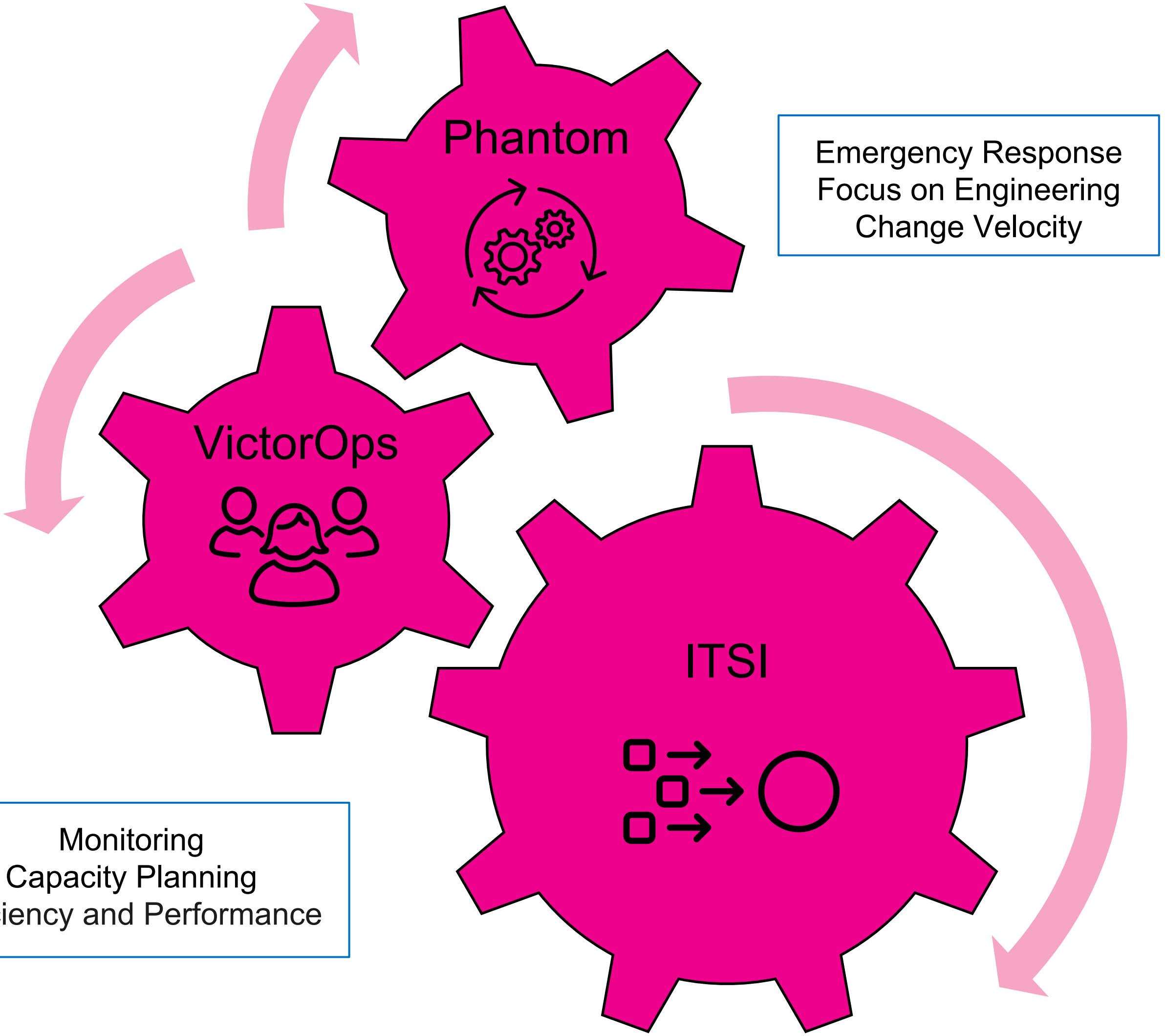
Traditional NOC

Traditional Change Management

Traditional Infra Ops

Core Tenants

Building blocks for success



Emergency Response
Focus on Engineering
Change Velocity

Emergency Response
Focus on Engineering
Change Management

Monitoring
Capacity Planning
Efficiency and Performance

Making Monitoring Matter

Alerting, ticketing, logging and so much more!

.conf19

splunk>

Changing what and why you monitor

Stop fighting fires.

Traditional Monitoring

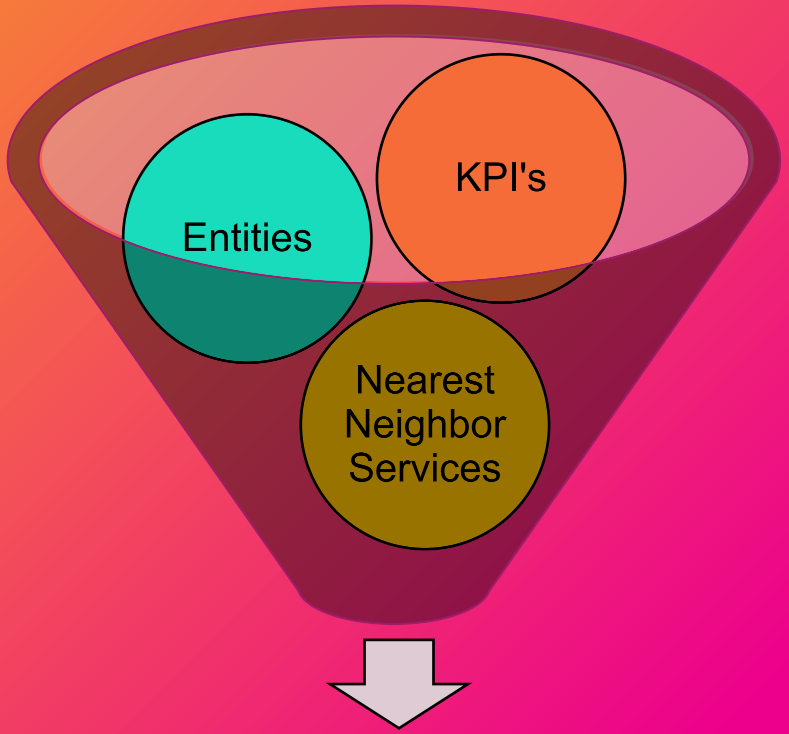
- Waiting for specific conditions to occur, minimal correlation
- Alert interpretation and decisions requires human interaction
- Dedicated people for taking action on alert conditions
- Manual ticketing, logging of events
- Silo'd RCA and problem resolution

Monitoring in SRE

- Automation of condition interpretation and correlation
- Humans only engaged when manual action is required
- Ticketing, logging and alert tuning are also automated
- Neighbor/dependent services are intelligently associated
- Symptom events are informed only if self-recovery doesn't occur

Monitoring services in ITSI

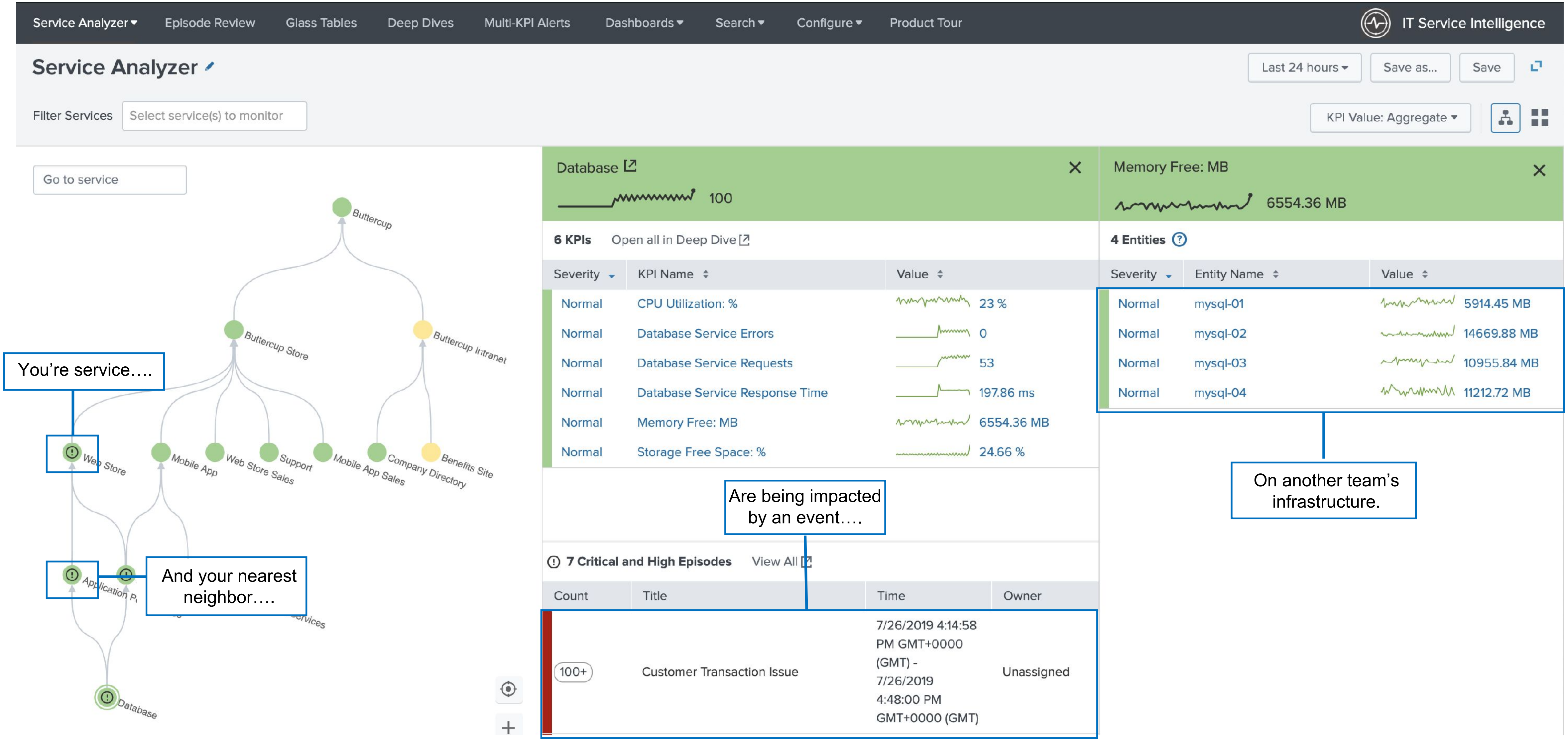
Building blocks for success



ITSI Service

- Decompose your service first
- Know what “Healthy” means
- Know who your neighbors are
- Have a process for all 3 component

Monitoring Services with ITSI



Database 100

6 KPIs Open all in Deep Dive

Severity	KPI Name	Value
Normal	CPU Utilization: %	23 %
Normal	Database Service Errors	0
Normal	Database Service Requests	53
Normal	Database Service Response Time	197.86 ms
Normal	Memory Free: MB	6554.36 MB
Normal	Storage Free Space: %	24.66 %

Memory Free: MB 6554.36 MB

4 Entities

Severity	Entity Name	Value
Normal	mysql-01	5914.45 MB
Normal	mysql-02	14669.88 MB
Normal	mysql-03	10955.84 MB
Normal	mysql-04	11212.72 MB

7 Critical and High Episodes View All

Count	Title	Time	Owner
100+	Customer Transaction Issue	7/26/2019 4:14:58 PM GMT+0000 (GMT) - 7/26/2019 4:48:00 PM GMT+0000 (GMT)	Unassigned

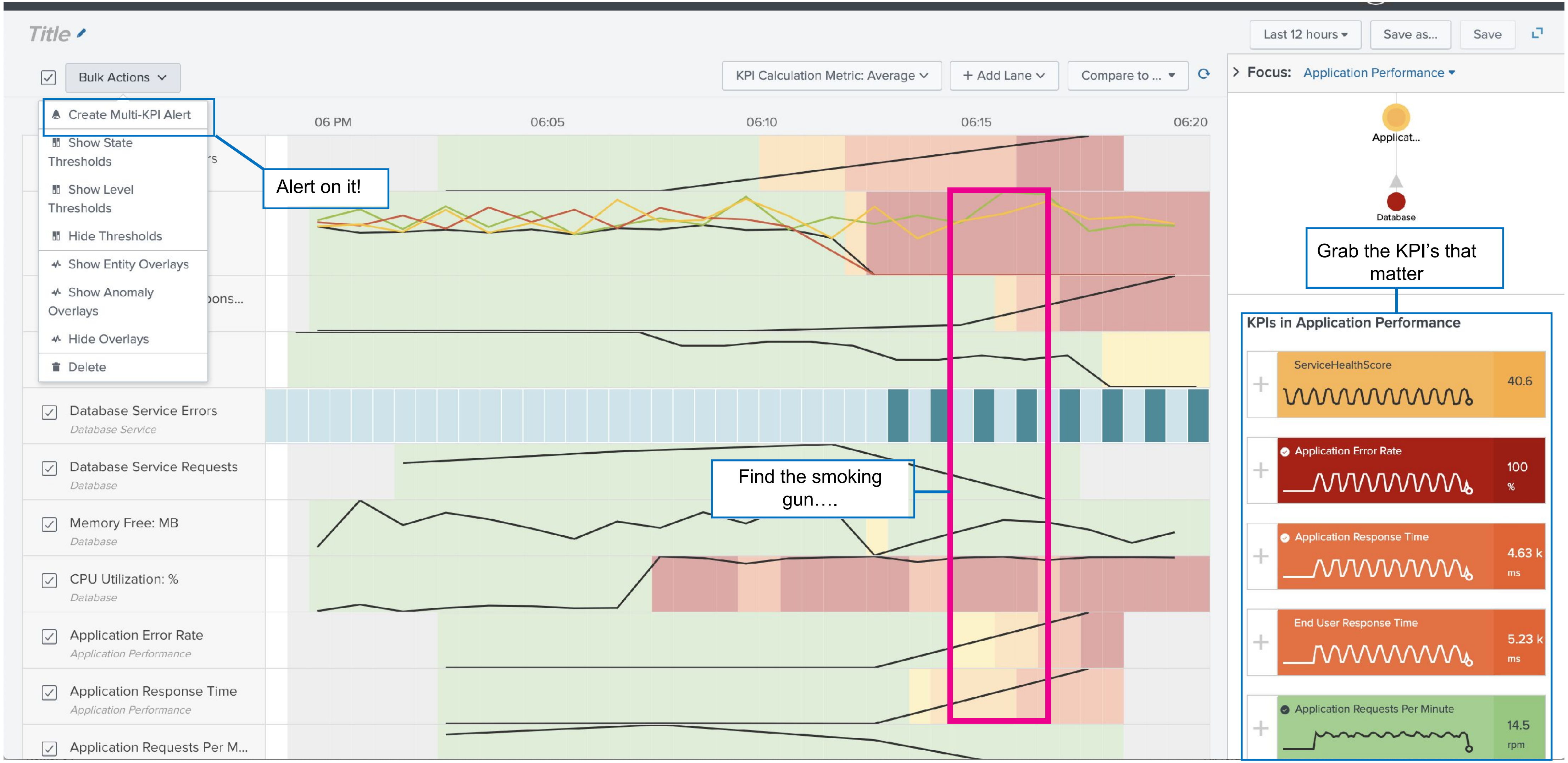
You're service….

And your nearest neighbor….

Are being impacted by an event….

On another team's infrastructure.

Monitoring Services with ITSI



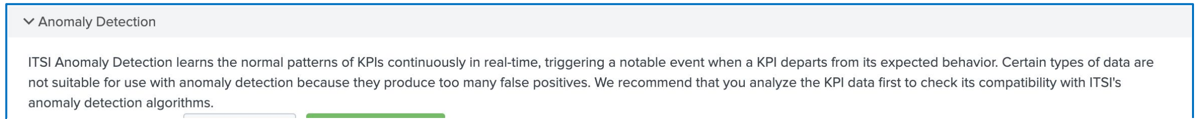
Alert on it!

Find the smoking gun….

Grab the KPI's that matter

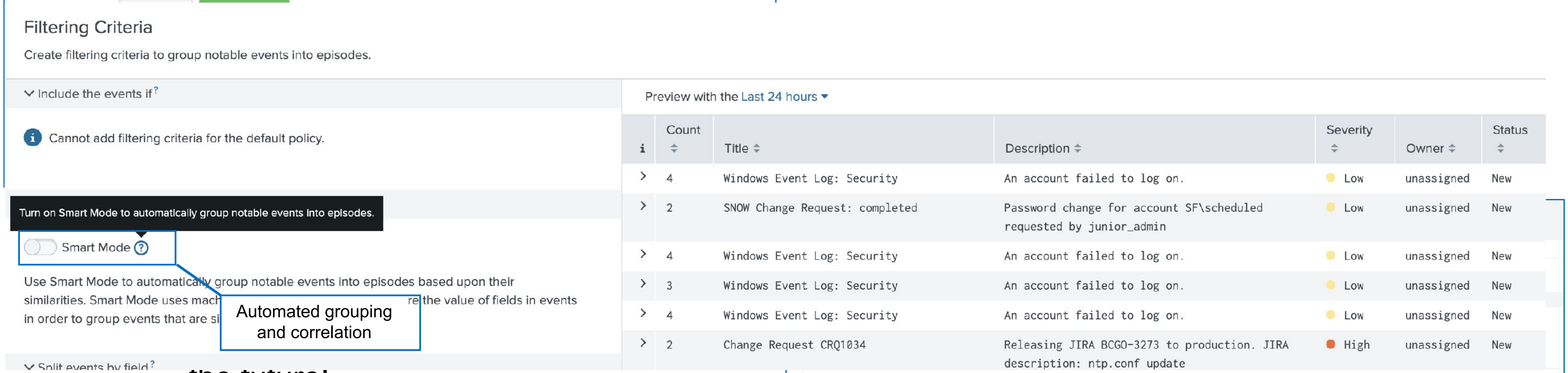
Monitoring Services with ITSI

Machine learning to the rescue!



Anomaly Detection

ITSI Anomaly Detection learns the normal patterns of KPIs continuously in real-time, triggering a notable event when a KPI departs from its expected behavior. Certain types of data are not suitable for use with anomaly detection because they produce too many false positives. We recommend that you analyze the KPI data first to check its compatibility with ITSI's anomaly detection algorithms.



Filtering Criteria

Create filtering criteria to group notable events into episodes.

Include the events if?

Cannot add filtering criteria for the default policy.

Turn on Smart Mode to automatically group notable events into episodes.

Smart Mode ?

Use Smart Mode to automatically group notable events into episodes based upon their similarities. Smart Mode uses mach… re the value of fields in events in order to group events that are si…

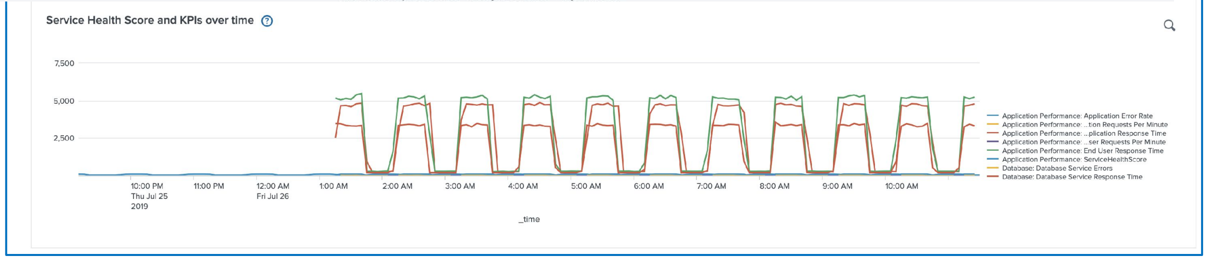
Automated grouping and correlation

Split events by field?

Preview with the Last 24 hours

i	Count	Title	Description	Severity	Owner	Status
›	4	Windows Event Log: Security	An account failed to log on.	● Low	unassigned	New
›	2	SNOW Change Request: completed	Password change for account SF\scheduled requested by junior_admin	● Low	unassigned	New
›	4	Windows Event Log: Security	An account failed to log on.	● Low	unassigned	New
›	3	Windows Event Log: Security	An account failed to log on.	● Low	unassigned	New
›	4	Windows Event Log: Security	An account failed to log on.	● Low	unassigned	New
›	2	Change Request CRQ1034	Releasing JIRA BCGO-3273 to production. JIRA description: ntp.conf update	● High	unassigned	New

the future!



Service Health Score and KPIs over time

Now….get the right hands on keyboards

For things unknown….

.conf19

splunk>

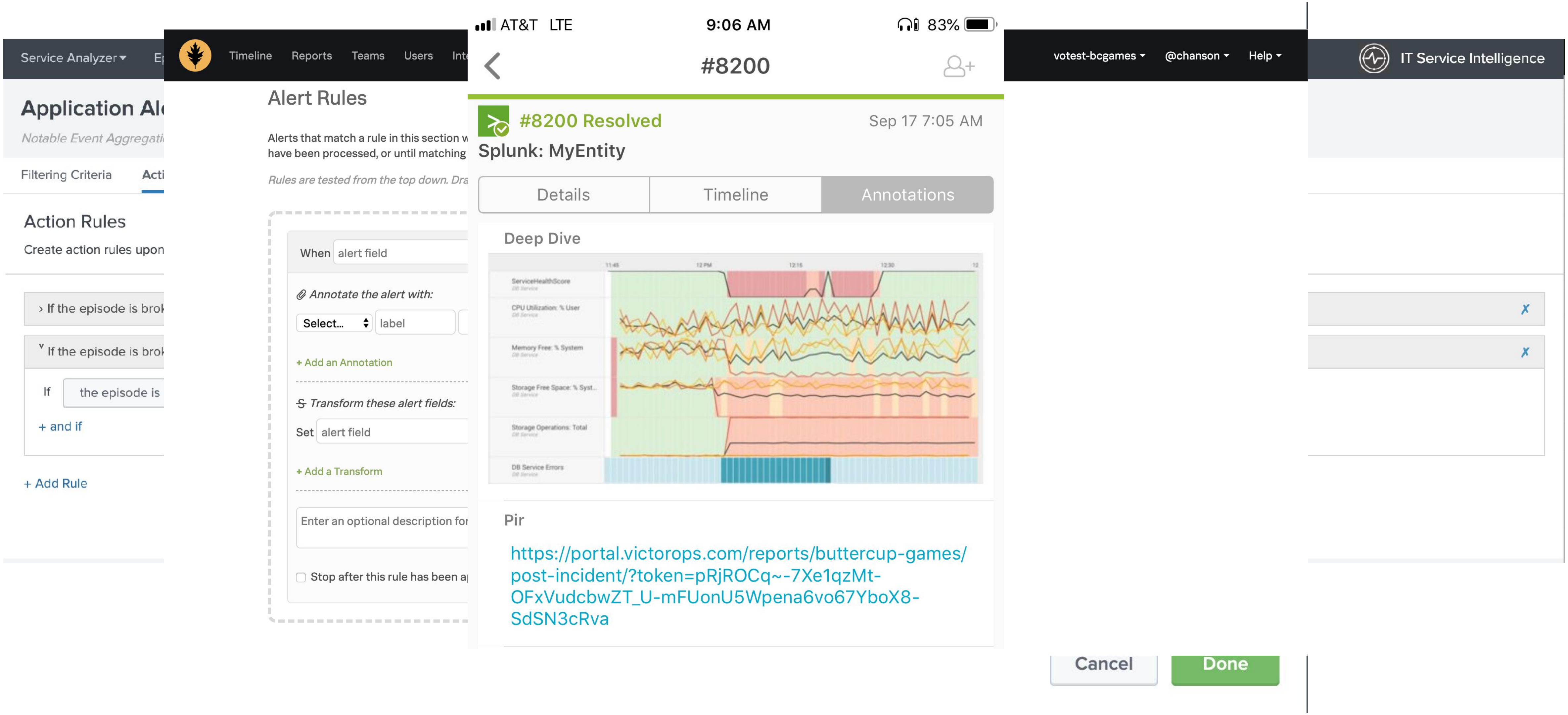
Alerting in the SRE Age

Show the pain, make it painless

1. Alerts should be rare, significant and immediately impacting to the business
2. ITSI should have already interpreted and correlated the data
3. Unknown and complex issues should take priority
4. Triage is not the sole responsibility of the SRE or DevOps teams
5. Ensure that Incident administration is automated up to the RCA process

Intelligent routing of Episodes

Episodes to teams with no in between



Service Analyzer ▾ Ep

Application Al

Notable Event Aggregati

Filtering Criteria Acti

Action Rules

Create action rules upon

› If the episode is brok

˅ If the episode is brok

If the episode is

+ and if

+ Add Rule

IT Service Intelligence

✗

✗

Cancel Done

Timeline Reports Teams Users Int

votest-bcgames ▾ @chanson ▾ Help ▾

Alert Rules

Alerts that match a rule in this section w have been processed, or until matching

Rules are tested from the top down. Dra

When alert field

Annotate the alert with:

Select... label

+ Add an Annotation

Transform these alert fields:

Set alert field

+ Add a Transform

Enter an optional description for

□ Stop after this rule has been a

AT&T LTE 9:06 AM 83%

#8200

#8200 Resolved Sep 17 7:05 AM

Splunk: MyEntity

Details | Timeline | Annotations

Deep Dive

Pir

https://portal.victorops.com/reports/buttercup-games/post-incident/?token=pRjROCq~-7Xe1qzMt-OFxVudcbwZT_U-mFUonU5Wpena6vo67YboX8-SdSN3cRva

Orchestration to the rescue!

For the things that are known…

.conf19
splunk>

Automate the simple, orchestrate the complex

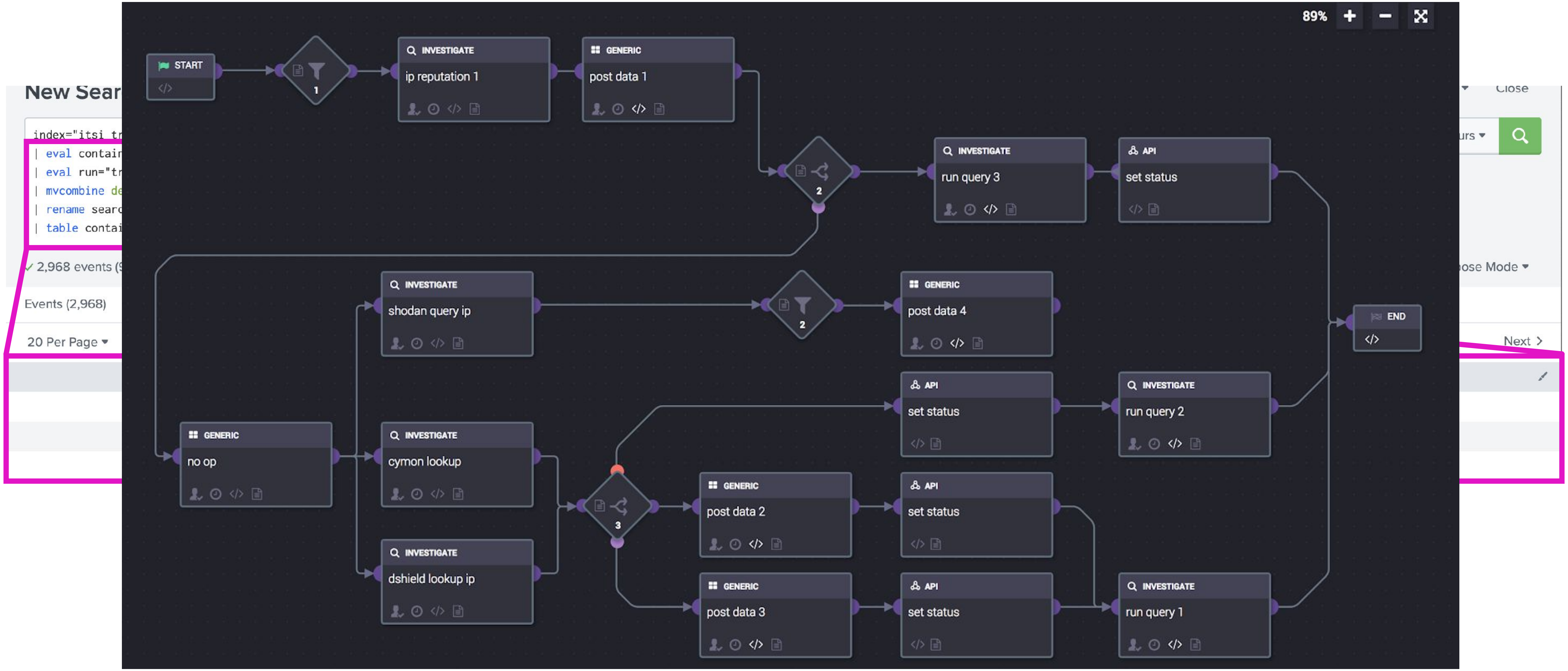
Know what kind of task you're dealing with

1. Automation is removing human intervention in singular tasks or functions
   - Ticket Creation
   - Adding a new cluster node
   - Incident Notification

2. Orchestration schedules, integrates and validates automation tasks
   - Network configuration
   - OS configuration changes
   - Container Orchestrations

Using Phantom for ITSI Episodes

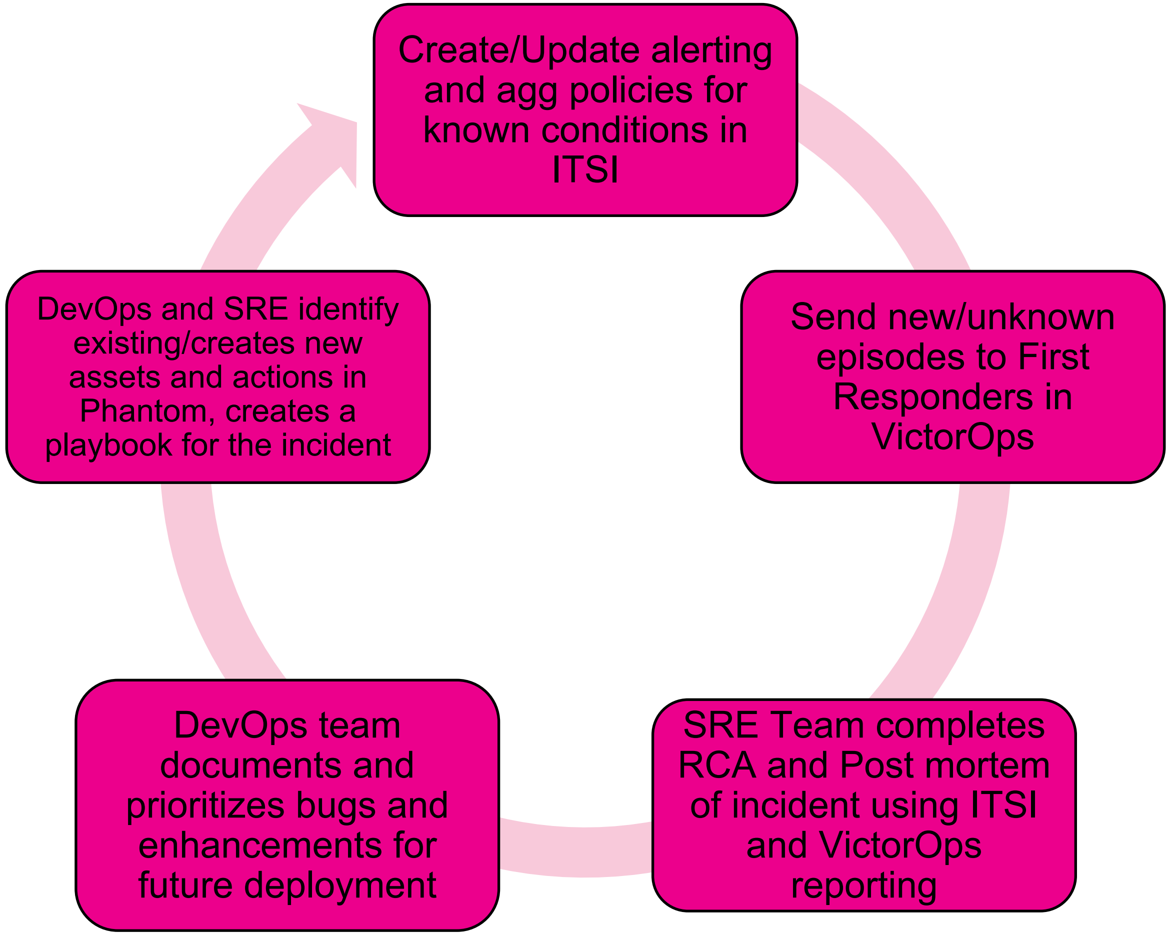
Getting under the hood for a minute…



```
index="itsi_tr
| eval contai
| eval run="tr
| mvcombine de
| rename searc
| table contai
```

Incident Automation Flow

Bridging the gap between Ops responsibility and Pipeline Priority



Create/Update alerting and agg policies for known conditions in ITSI

Send new/unknown episodes to First Responders in VictorOps

SRE Team completes RCA and Post mortem of incident using ITSI and VictorOps reporting

DevOps team documents and prioritizes bugs and enhancements for future deployment

DevOps and SRE identify existing/creates new assets and actions in Phantom, creates a playbook for the incident

Velocity, Capacity and staying Engineering Focused

Turn your pipelines into hyperloops

.conf19

splunk>

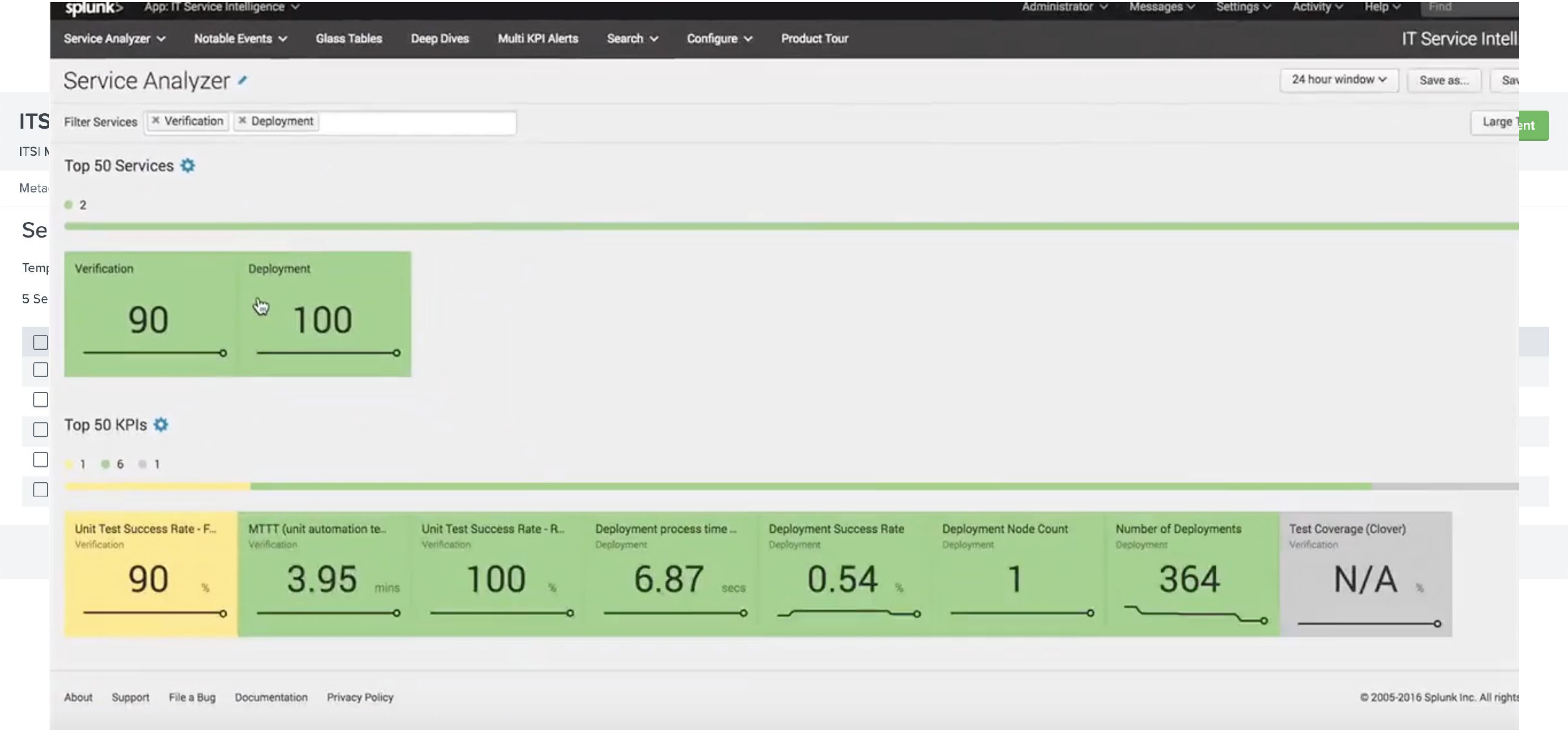
Pipelines are…complicated

Monitor the changes and change the monitoring

1. Most organizations will have multiple CICD pipelines based on business unit, stack, app, etc.
2. Not all pipelines will have the same capacity, velocity or success rate
3. There is likely to be a variety of deployment tools in use
4. What is being deployed directly impacts and is impacted by monitoring/alerting

Pipeline monitoring done right

Modules and apps for the whole picture



Service Analyzer

Filter Services: × Verification × Deployment

Top 50 Services

● 2

Verification	Deployment
90	100

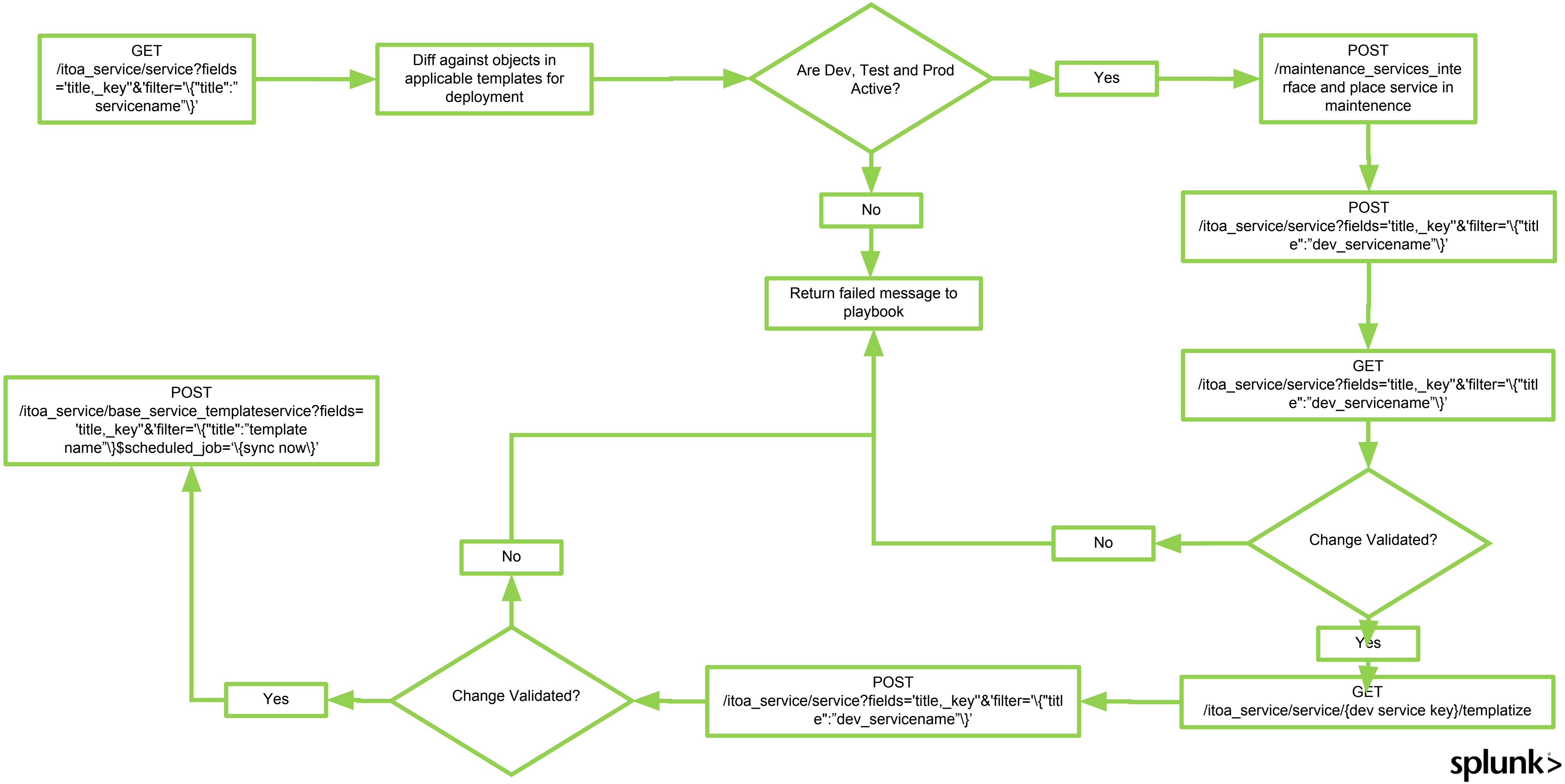
Top 50 KPIs

● 1 ● 6 ● 1

KPI	Service	Value
Unit Test Success Rate - F...	Verification	90 %
MTTT (unit automation te...	Verification	3.95 mins
Unit Test Success Rate - R...	Verification	100 %
Deployment process time ...	Deployment	6.87 secs
Deployment Success Rate	Deployment	0.54 %
Deployment Node Count	Deployment	1
Number of Deployments	Deployment	364
Test Coverage (Clover)	Verification	N/A %

Using your deployments to change ITSI

Adjusting existing ITSI services



GET
/itoa_service/service?fields
='title,_key"&'filter='\{"title":”
servicename”\}’

Diff against objects in
applicable templates for
deployment

Are Dev, Test and Prod
Active?

Yes

POST
/maintenance_services_inte
rface and place service in
maintenence

No

Return failed message to
playbook

POST
/itoa_service/service?fields='title,_key"&'filter='\{"titl
e":”dev_servicename”\}’

GET
/itoa_service/service?fields='title,_key"&'filter='\{"titl
e":”dev_servicename”\}’

Change Validated?

No

Yes

GET
/itoa_service/service/{dev service key}/templatize

POST
/itoa_service/service?fields='title,_key"&'filter='\{"titl
e":”dev_servicename”\}’

Change Validated?

No

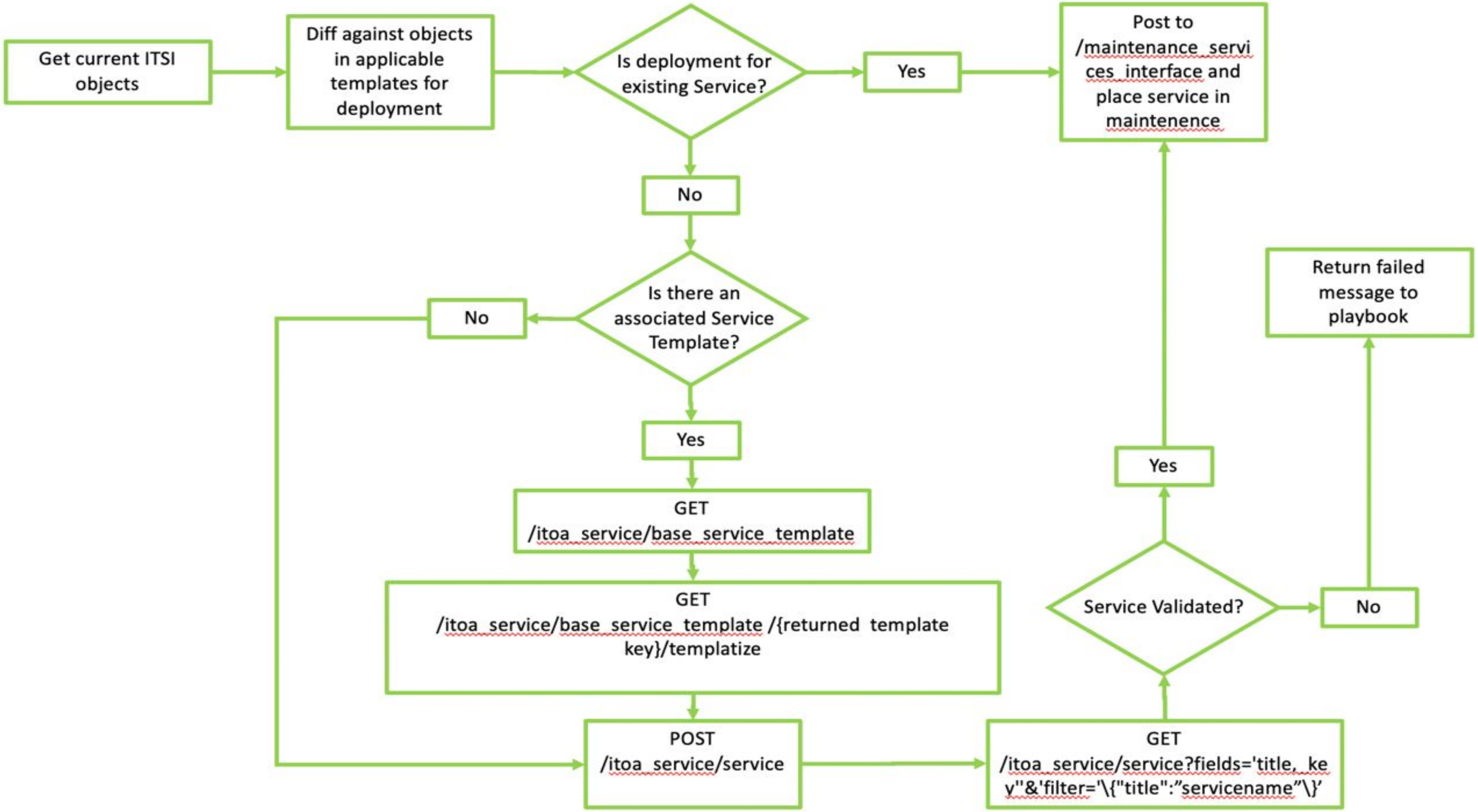
Yes

POST
/itoa_service/base_service_templateservice?fields=
'title,_key"&'filter='\{"title":”template
name”\}$scheduled_job=‘\{sync now\}’

splunk> .conf19

Using your deployments to change ITSI

Adjusting existing ITSI services



Get current ITSI objects

Diff against objects in applicable templates for deployment

Is deployment for existing Service?

Yes

Post to /maintenance_services_interface and place service in maintenence

No

Is there an associated Service Template?

No

Yes

GET /itoa_service/base_service_template

GET /itoa_service/base_service_template /{returned_template key}/templatize

POST /itoa_service/service

GET /itoa_service/service?fields='title,_key"&'filter='\{"title":”servicename”\}’

Service Validated?

Yes

No

Return failed message to playbook

Demo

Q&A

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION