Every Minute Counts: Integrating Splunk and VictorOps to Accelerate Incident Response

.conf19

splunk>

Kirk Hanson | ITOA/Devops Specialist

Dylan Klausing | ITOA/ Devops Specialist

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.

Every Minute Counts: Integrating Splunk and VictorOps to Accelerate Incident Response

Kirk Hanson

ITOA/Devops Specialist

Dylan Klausing

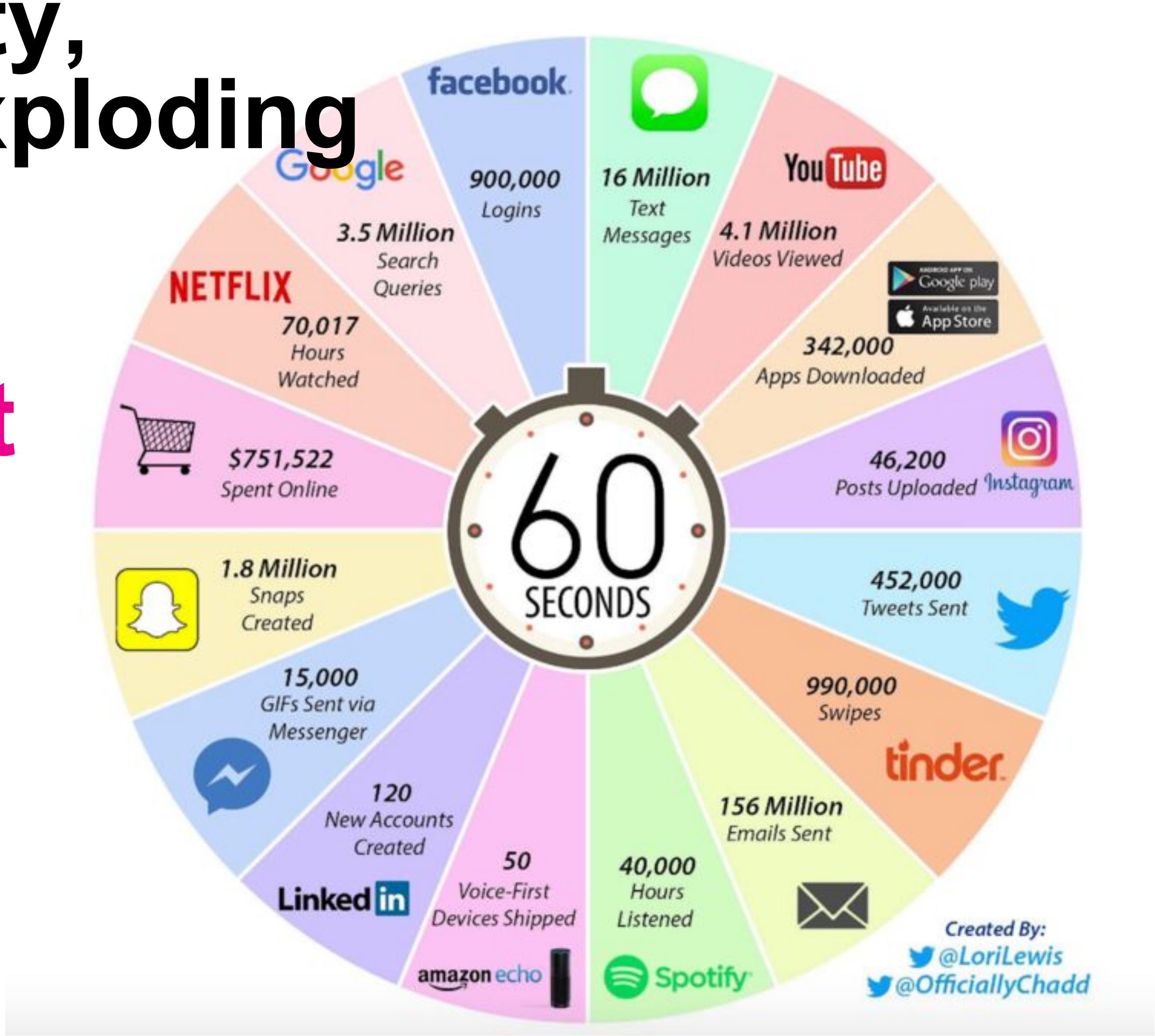
ITOA/ Devops Specialist

Agenda

1. Effects of Downtime
2. Benefits of ITSI+VictorOps
3. Product Presentation
4. Key Takeaways

The volume, velocity, variety of data is exploding

In an internet minute…



Lori Lewis and Chadd Callahan of [Cumulus Media](), via [http://www.businessinsider.com/everything-that-happens-in-one-minute-on-the-internet-2017-9]()

Most organizations are starting to realize that **downtime is inevitable**

but….

haven’t realized they **do control their preparation** for downtime.

IT Struggles to Identify, Investigate and Resolve Critical Service Issues

- Guesswork
- Reactive
- Unproductive

What Are the Impacts of Downtime?

Catchpoint surveyed 188 SREs and found that downtime meant:

36% Saw social media backlash

Brand

86% Saw a drop in customer satisfaction

Customers

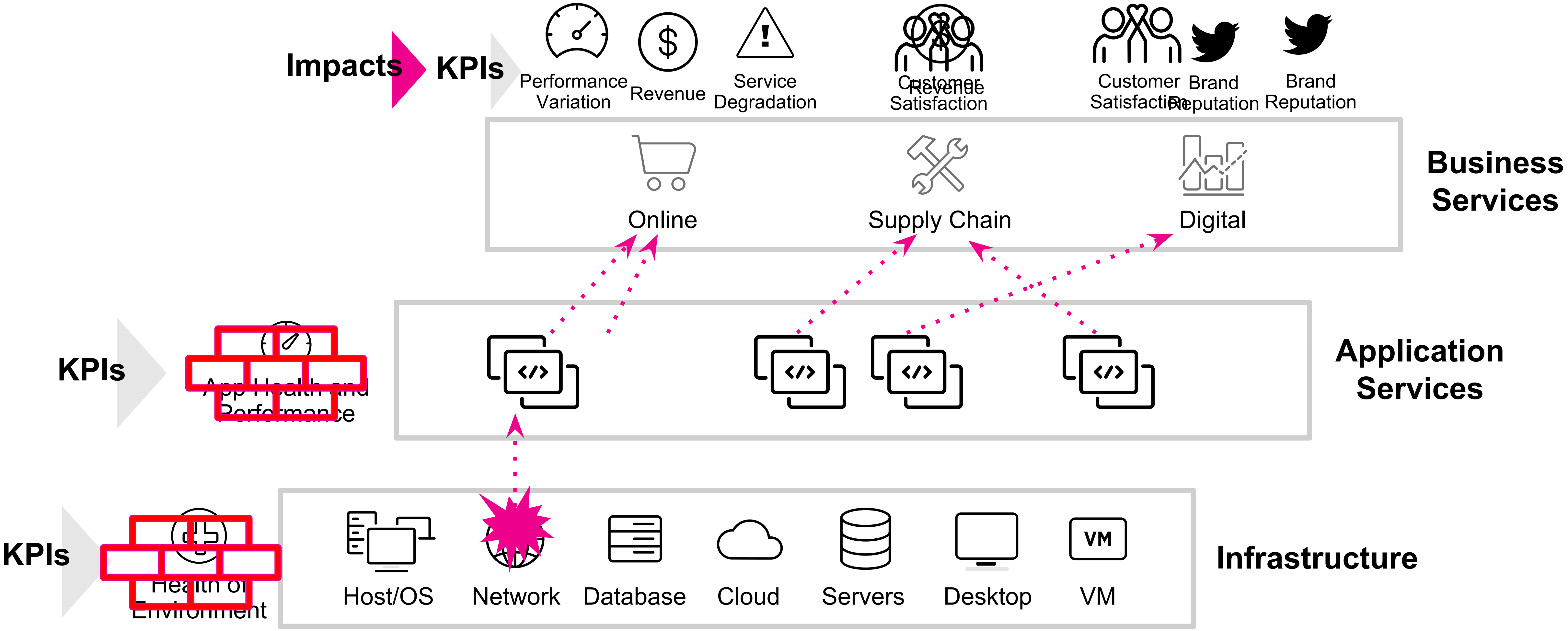
57% Reported decreased employee productivity

Team

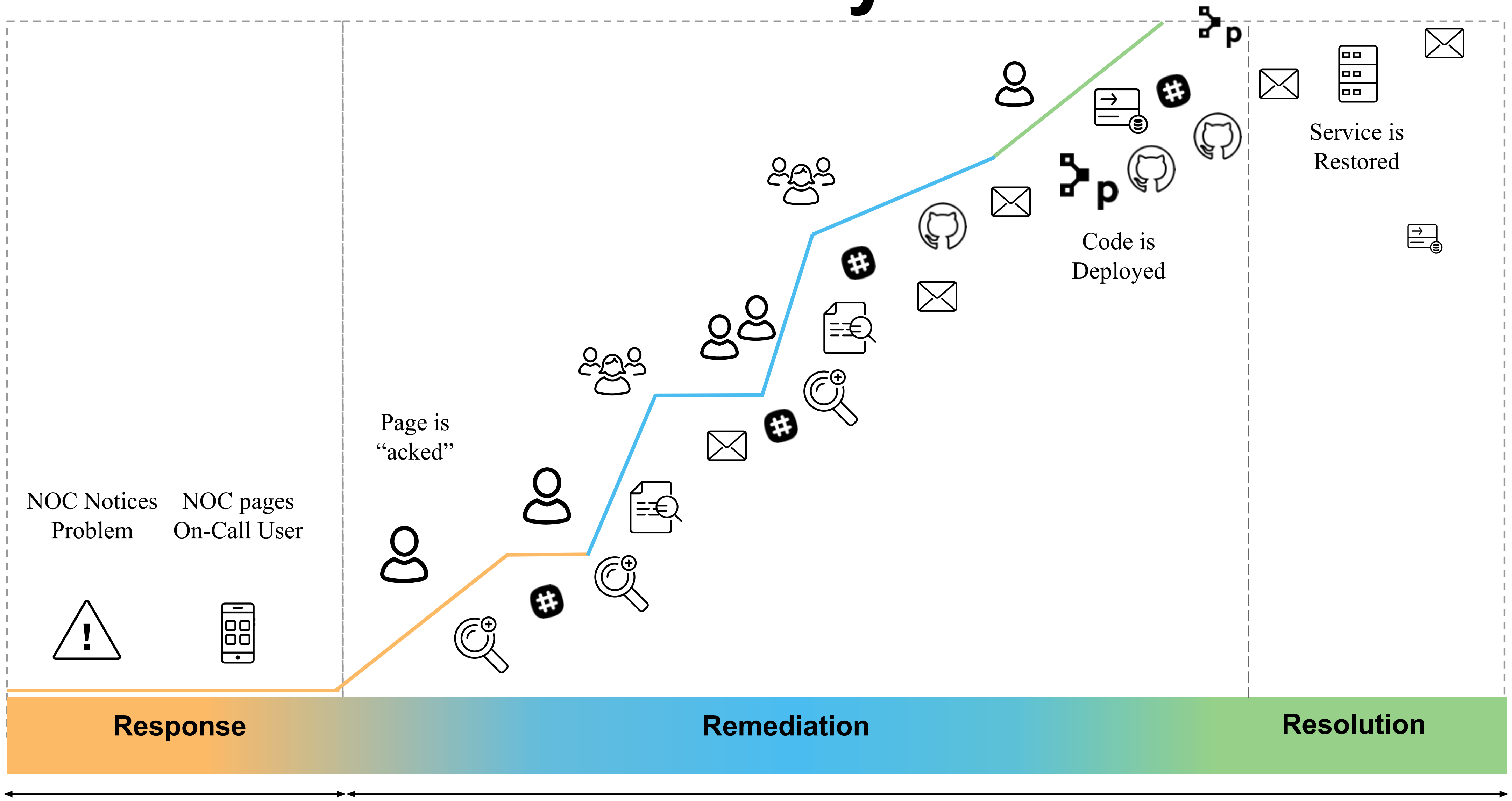
70% Experienced lost revenue

Revenue

IT Struggles to Identify, Investigate, and Resolve Critical Issues



Normal Incident Lifecycle - confusion



25-45 min

6 hours / 5 re-routes / 8 people

VictorOps & ITSI Solves

Preventing and Reducing Downtime

Visibility & Collaboration

On-Call Burnout

Lack of Continuous Improvement Culture and Process, and tools that support continuous improvement

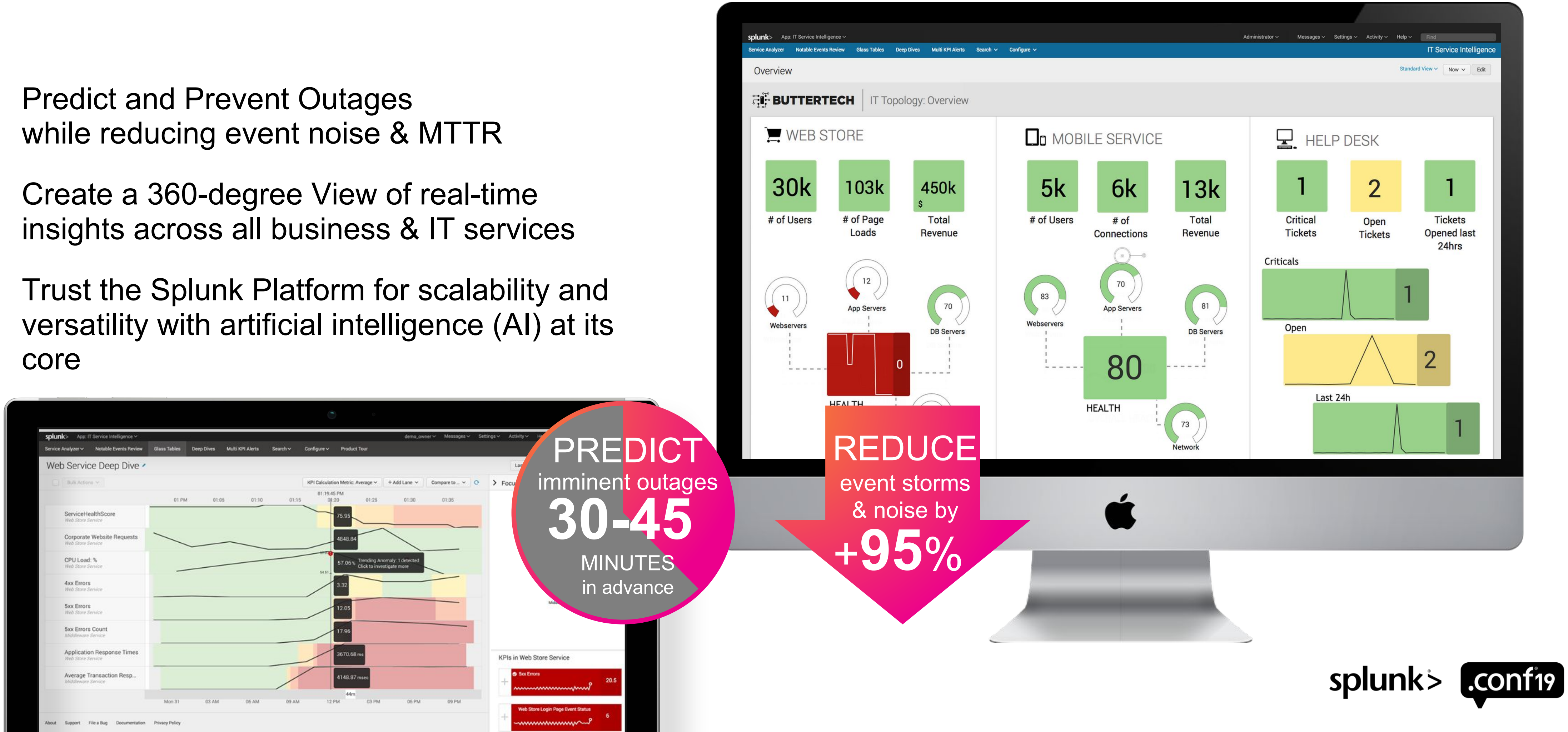
Splunk IT Service Intelligence (ITSI)

Predictive analytics for real-time insights, simplified operations and root cause isolation

Predict and Prevent Outages while reducing event noise & MTTR

Create a 360-degree View of real-time insights across all business & IT services

Trust the Splunk Platform for scalability and versatility with artificial intelligence (AI) at its core

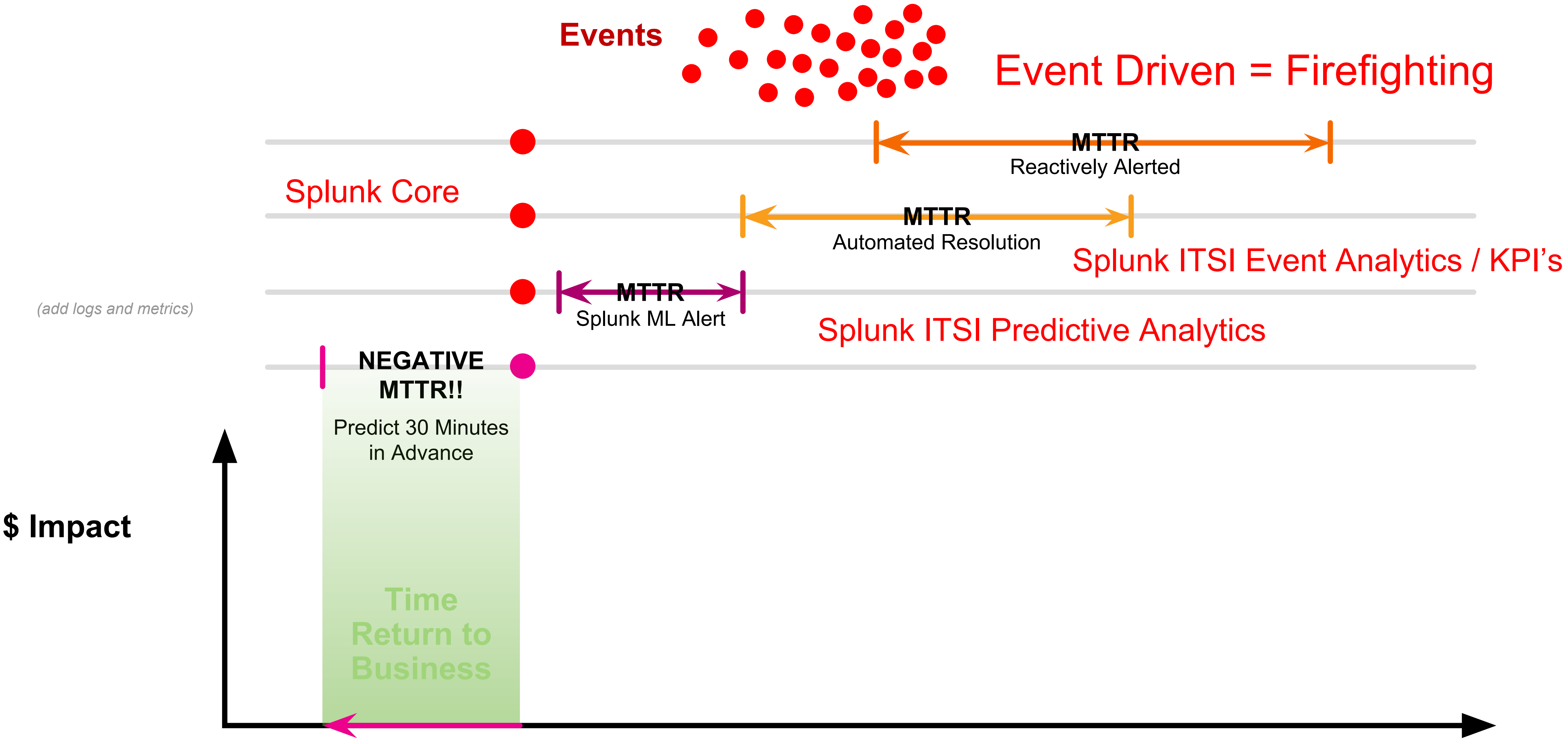


PREDICT imminent outages **30-45** MINUTES in advance

REDUCE event storms & noise by **+95%**

splunk> .conf19

Predict and Prevent Operational Issues With AI



Events

Event Driven = Firefighting

Splunk Core

MTTR
Reactively Alerted

MTTR
Automated Resolution

Splunk ITSI Event Analytics / KPI’s

MTTR
Splunk ML Alert

Splunk ITSI Predictive Analytics

(add logs and metrics)

NEGATIVE MTTR!!

Predict 30 Minutes in Advance

$ Impact

Time Return to Business

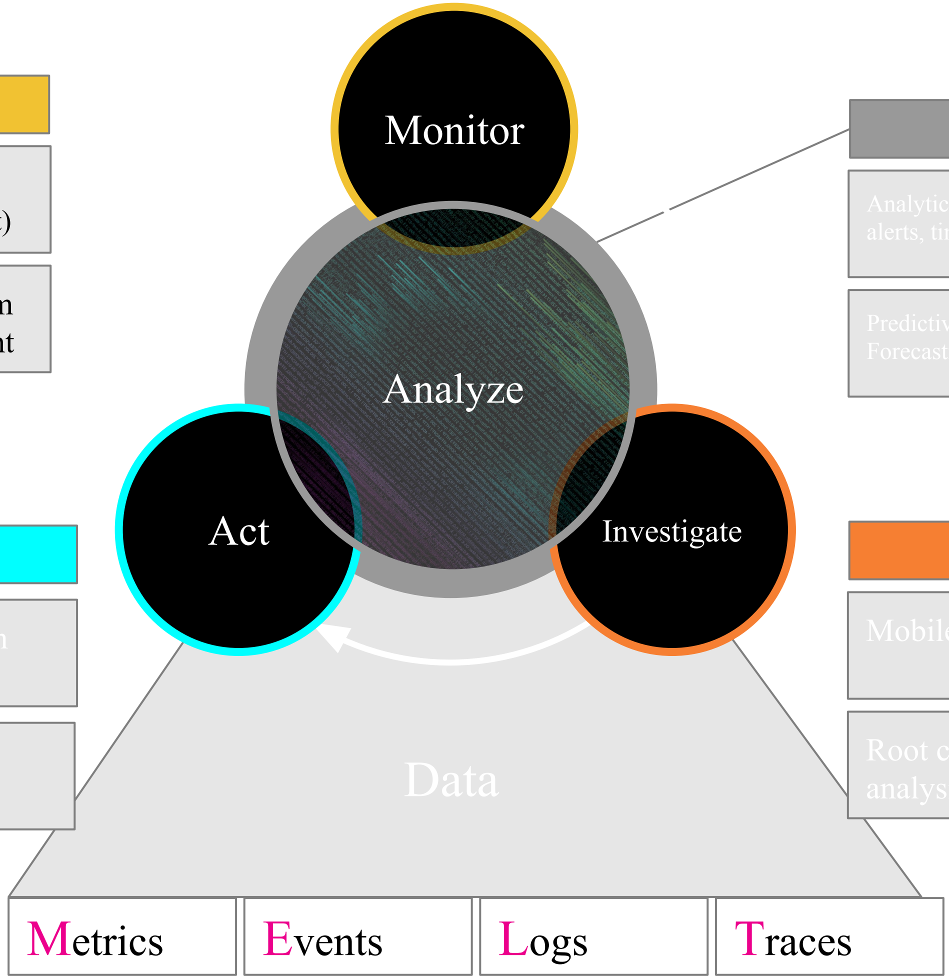
Splunk is the platform, ITSI is the Solution

Splunk's Vision for AIOps

Persona Based Workflows, Dashboards

Monitoring	
Infrastructure Monitoring	Service Mon (Internal + Ext)
Application Monitoring	Event/Alarm Management

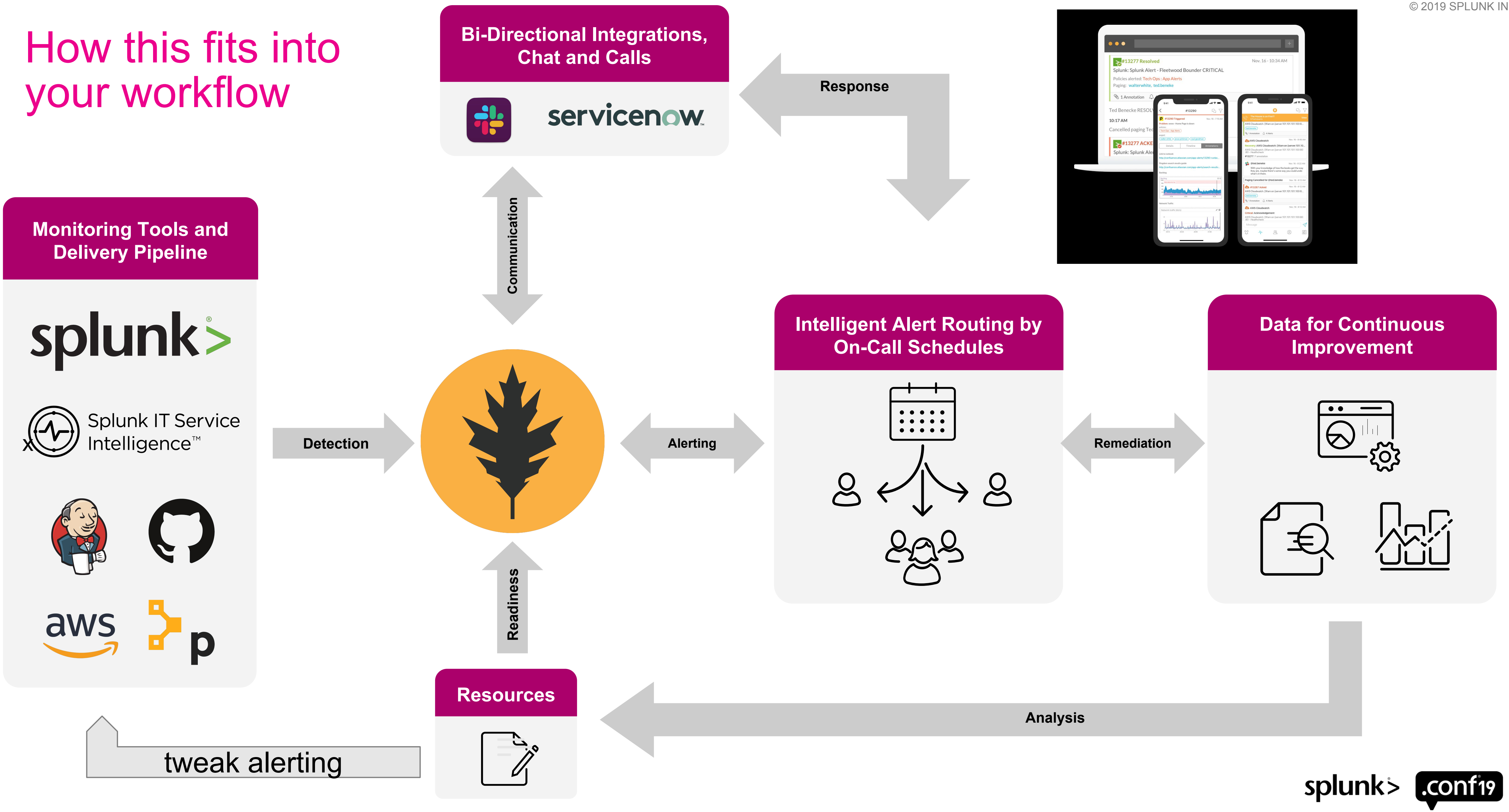
AI / ML + Analytics	
Analytics on events, alerts, timelines	Proactive Alerting
Predictive / Forecasting	Chatbots



Incident Remediation	
Identify and Test fixes	Plan production remediation
Run playbook/action	Rollback

Incident Response	
Mobile	Collaborative Troubleshooting
Root cause analysis	Stakeholder Mgmt

How this fits into your workflow



Bi-Directional Integrations, Chat and Calls

Monitoring Tools and Delivery Pipeline

Intelligent Alert Routing by On-Call Schedules

Data for Continuous Improvement

Resources

#13277 Resolved Nov. 16 - 10:34 AM
Splunk: Splunk Alert - Fleetwood Bounder CRITICAL
Policies alerted: Tech Ops : App Alerts
Paging: walterwhite, ted.beneke
1 Annotation

Ted Benecke RESOL
10:17 AM
Cancelled paging Tec

#13277 ACKE
Splunk: Splunk Aler

#13290
#13290 Triggered Nov. 16 - 7:15 AM
Problem: www - Home Page is down
policies: Tech Ops : App Alerts
paged: walter white, jesse pinkman, saul goodman
Details | Timeline | Annotations
Link to runbook
http://confluence.atlassian.com/app-alerts/13290-runbo...
Pingdom search results guide
http://confluence.atlassian.com/app-alerts/search-results...
Backlog

The House is on Fire!!! 6 Participants View
AWS Cloudwatch: [Warn on {server:101.101.101.100:8...
ted.beneke
1 Annotation 4 Alerts

AWS Cloudwatch Nov. 16 - 8:45 AM
Recovery: AWS Cloudwatch: [Warn on {server:101.10...
AWS Cloudwatch: [Warn on {server:101.101.101.100:80 :80 - Healthcheck
#13277 / 1 annotation

@ted.beneke Nov. 16 - 8:22 AM
With your knowledge of how the books got the way they are, maybe there's some way you could undo what's in there.

Paging Cancelled for @ted.beneke Nov. 16 - 8:12 AM

#13287 Acked Nov. 16 - 8:12 AM
AWS Cloudwatch: [Warn on {server:101.101.101.100:8...
ted.beneke
1 Annotation 4 Alerts

Splunk ITSI & VictorOps Sitting in a tree

Service Analyzer

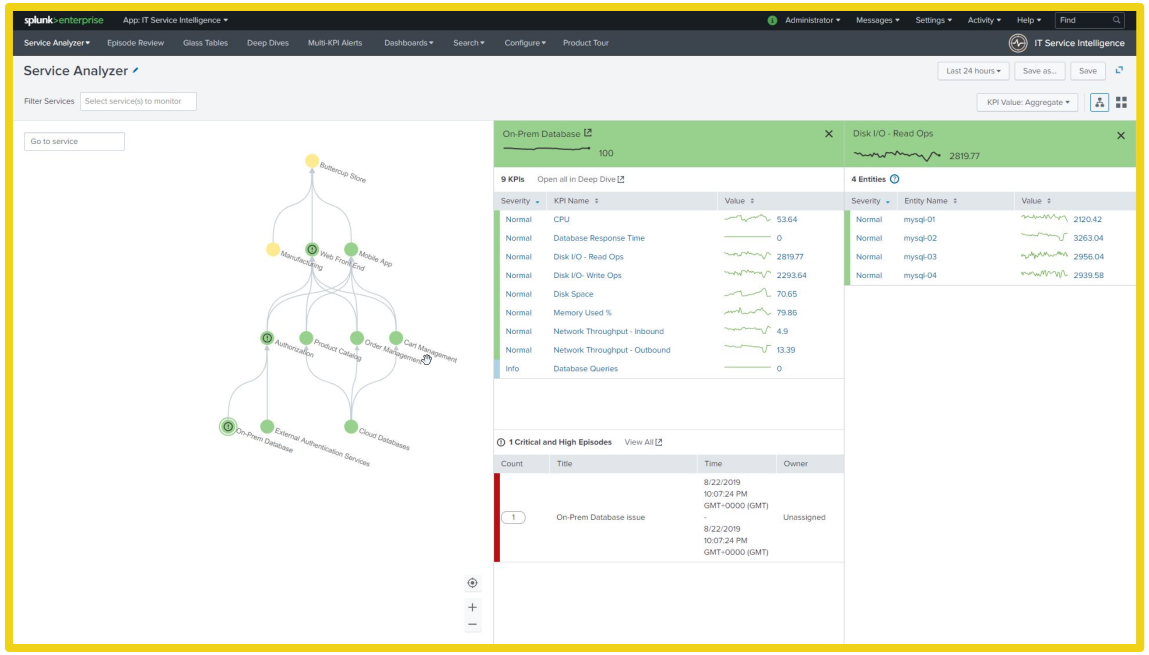
How are my services behaving?

View into your services by dependency

View KPI's and their impact on the overall service health

View related Episodes – covered later

Dynamic list of Entities



9 KPIs Open all in Deep Dive

Severity	KPI Name	Value
Normal	CPU	53.64
Normal	Database Response Time	0
Normal	Disk I/O - Read Ops	2819.77
Normal	Disk I/O- Write Ops	2293.64
Normal	Disk Space	70.65
Normal	Memory Used %	79.86
Normal	Network Throughput - Inbound	4.9
Normal	Network Throughput - Outbound	13.39
Info	Database Queries	0

4 Entities

Severity	Entity Name	Value
Normal	mysql-01	2120.42
Normal	mysql-02	3263.04
Normal	mysql-03	2956.04
Normal	mysql-04	2939.58

1 Critical and High Episodes View All

Count	Title	Time	Owner
1	On-Prem Database issue	8/22/2019 10:07:24 PM GMT+0000 (GMT) - 8/22/2019 10:07:24 PM GMT+0000 (GMT)	Unassigned

Host Details

Only a click away

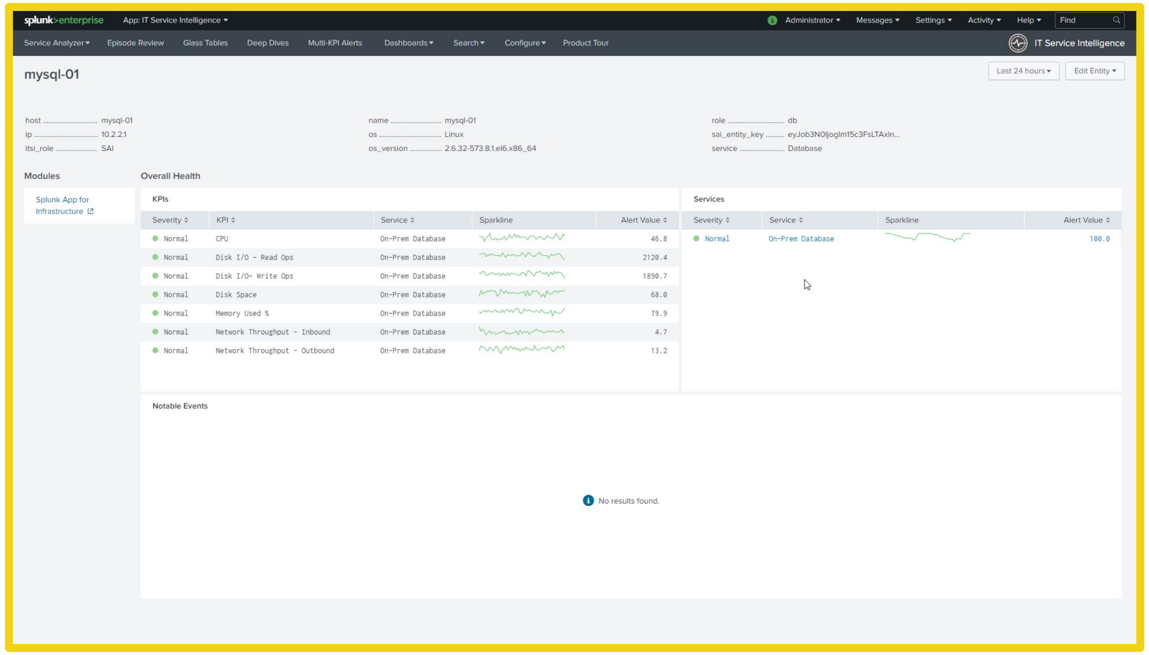
CPU

Mem

Network

Service Context

…. All a click away



mysql-01

host mysql-01
ip 10.2.2.1
itsi_role .... SAI

name mysql-01
os .... Linux
os_version .... 2.6.32-573.8.1.el6.x86_64

role .... db
sai_entity_key .... eyJob3N0IjogIm15c3FsLTAxIn...
service .... Database

Modules

Splunk App for Infrastructure

Overall Health

KPIs

Severity	KPI	Service	Sparkline	Alert Value
● Normal	CPU	On-Prem Database		46.8
● Normal	Disk I/O - Read Ops	On-Prem Database		2120.4
● Normal	Disk I/O- Write Ops	On-Prem Database		1890.7
● Normal	Disk Space	On-Prem Database		68.0
● Normal	Memory Used %	On-Prem Database		79.9
● Normal	Network Throughput - Inbound	On-Prem Database		4.7
● Normal	Network Throughput - Outbound	On-Prem Database		13.2

Services

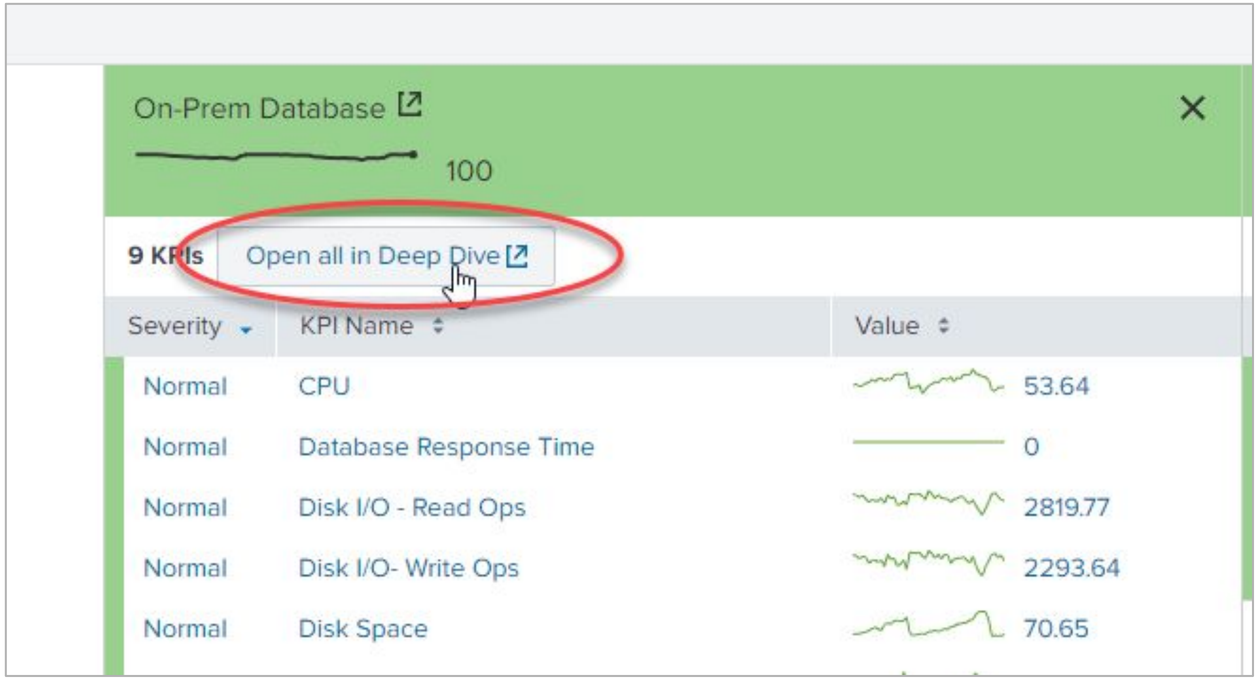
Severity	Service	Sparkline	Alert Value
● Normal	On-Prem Database		100.0

Notable Events

No results found.

Open In Deep Dive

So it’s time to start figuring out what it is the root cause
Lets navigate to a “Deep Dive” to start our RCA



On-Prem Database

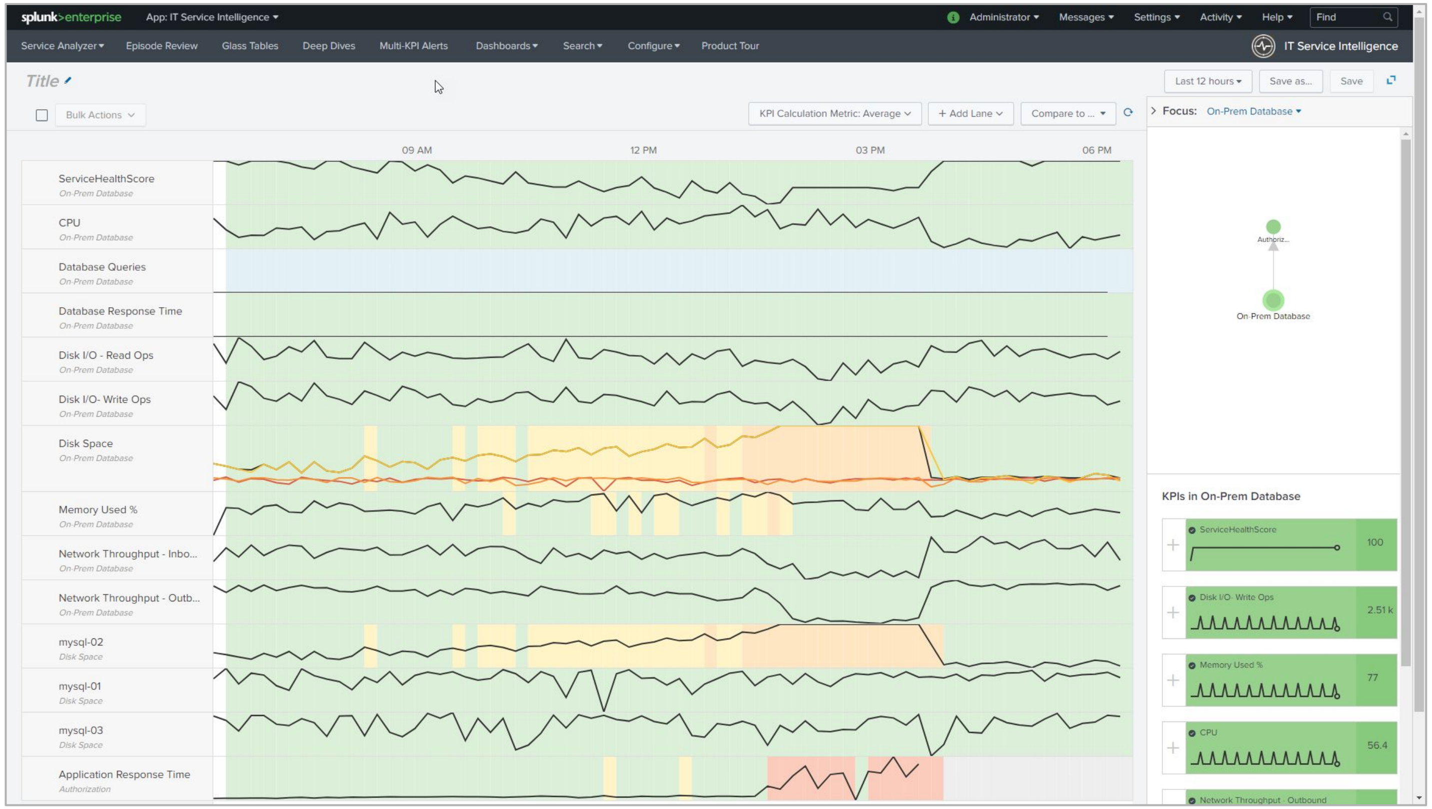
100

9 KPIs

Severity	KPI Name	Value
Normal	CPU	53.64
Normal	Database Response Time	0
Normal	Disk I/O - Read Ops	2819.77
Normal	Disk I/O- Write Ops	2293.64
Normal	Disk Space	70.65

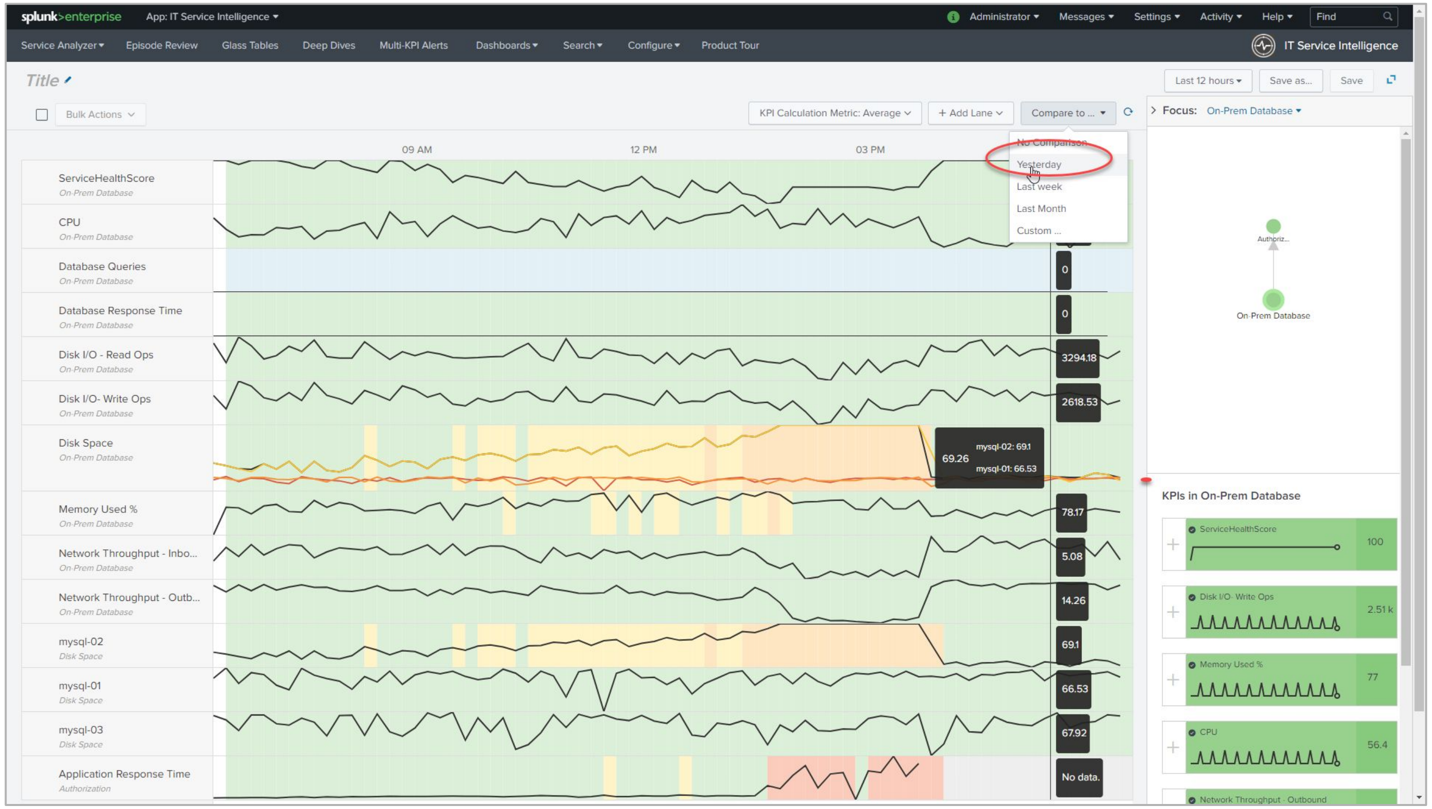
Deep Dive

- Swim lanes designed to help with trend analysis
- Quickly identify which KPI is impacting the service
- Add/subtract services to get a org-level understanding of the impact of the issue



Deep Dive Continued..

Is this a trend ? Has it happened before?
Allows to truly get to root cause quickly



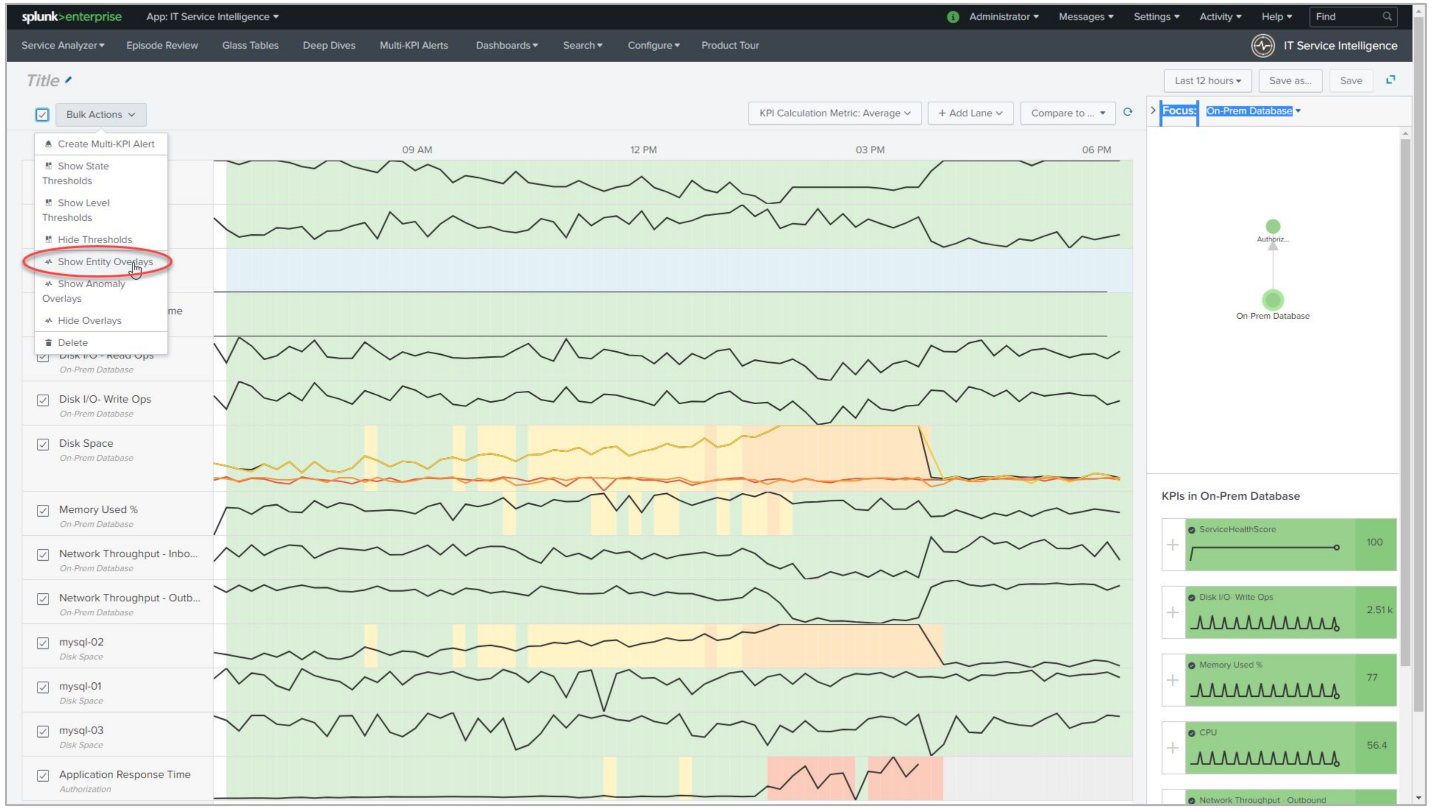
KPI Calculation Metric: Average

Last 12 hours

Focus: On-Prem Database

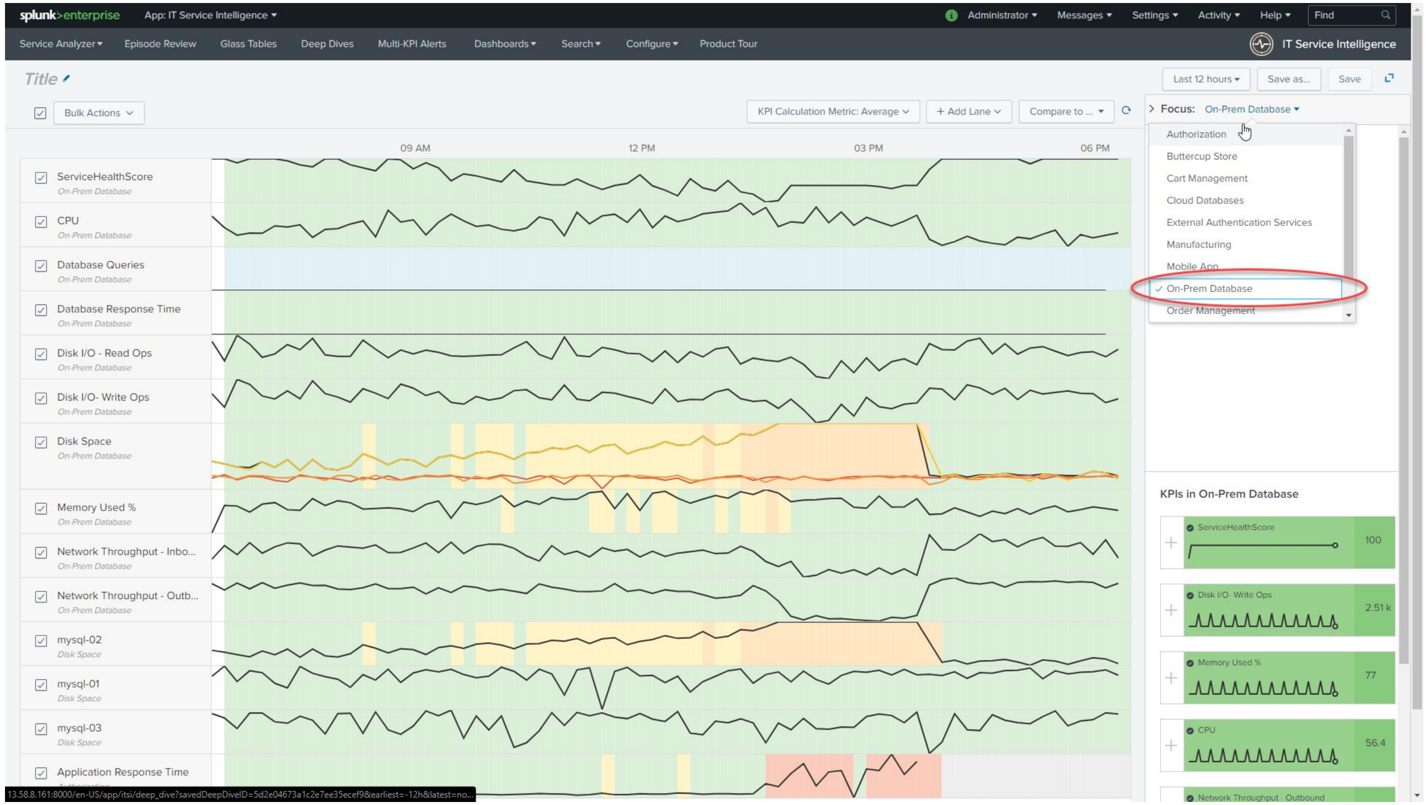
Deep Dive Continued..

- Is this a trend ? Has it happened before?
- Allows to truly get to root cause quickly
- Understand quickly which entity is having an issue by using Entity overlay on the swim lanes



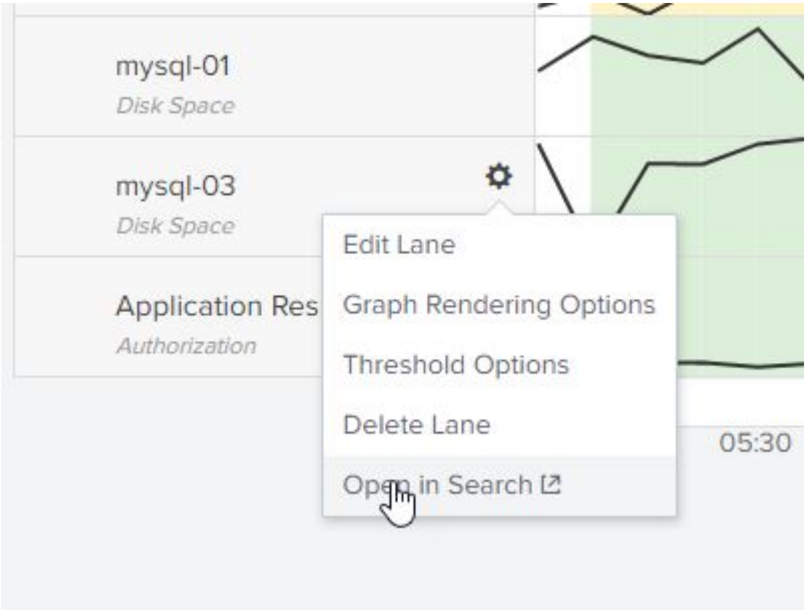
Deep Dive Continued..

- Is this a trend ? Has it happened before?
- Allows to truly get to root cause quickly
- Understand quickly which entity is having an issue by using Entity overlay on the swim lanes
- Quickly drag in KPI’s that are related to other services



Deep Dive Continued..

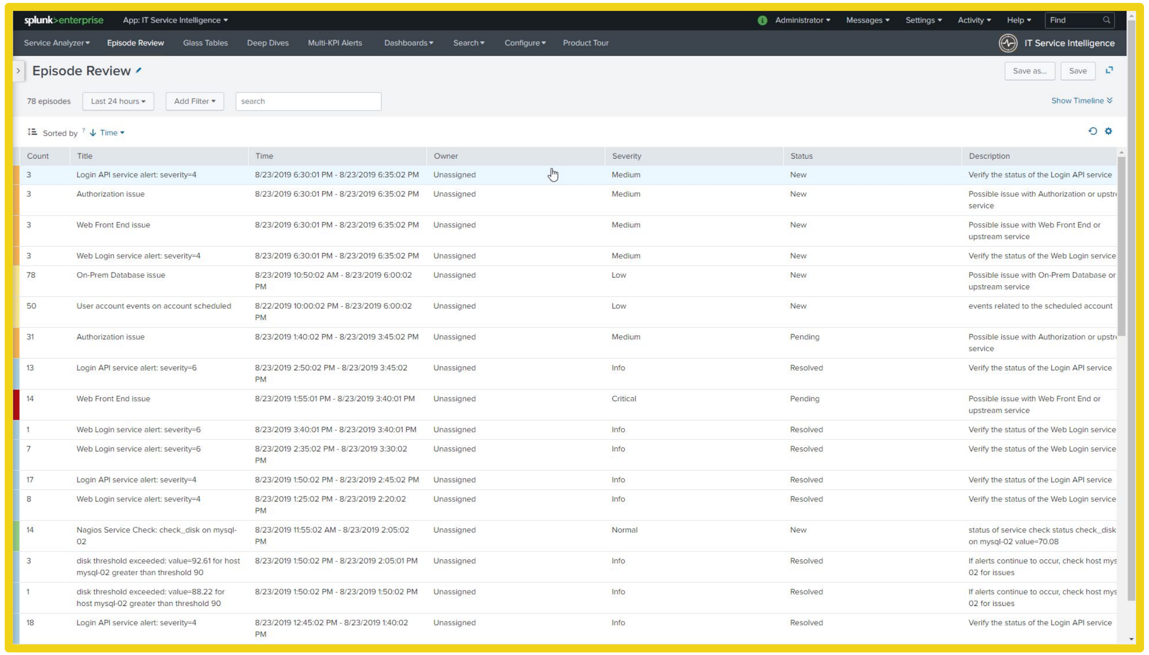
- Is this a trend ? Has it happened before?
- Allows to truly get to root cause quickly
- Understand quickly which entity is having an issue by using Entity overlay on the swim lanes
- Quickly drag in KPI’s that are related to other services
- Drill down to the search and to deeper root-cause analysis



Episode Review

Event grouping allows for more effective troubleshooting

Event grouping allows for more effective troubleshooting



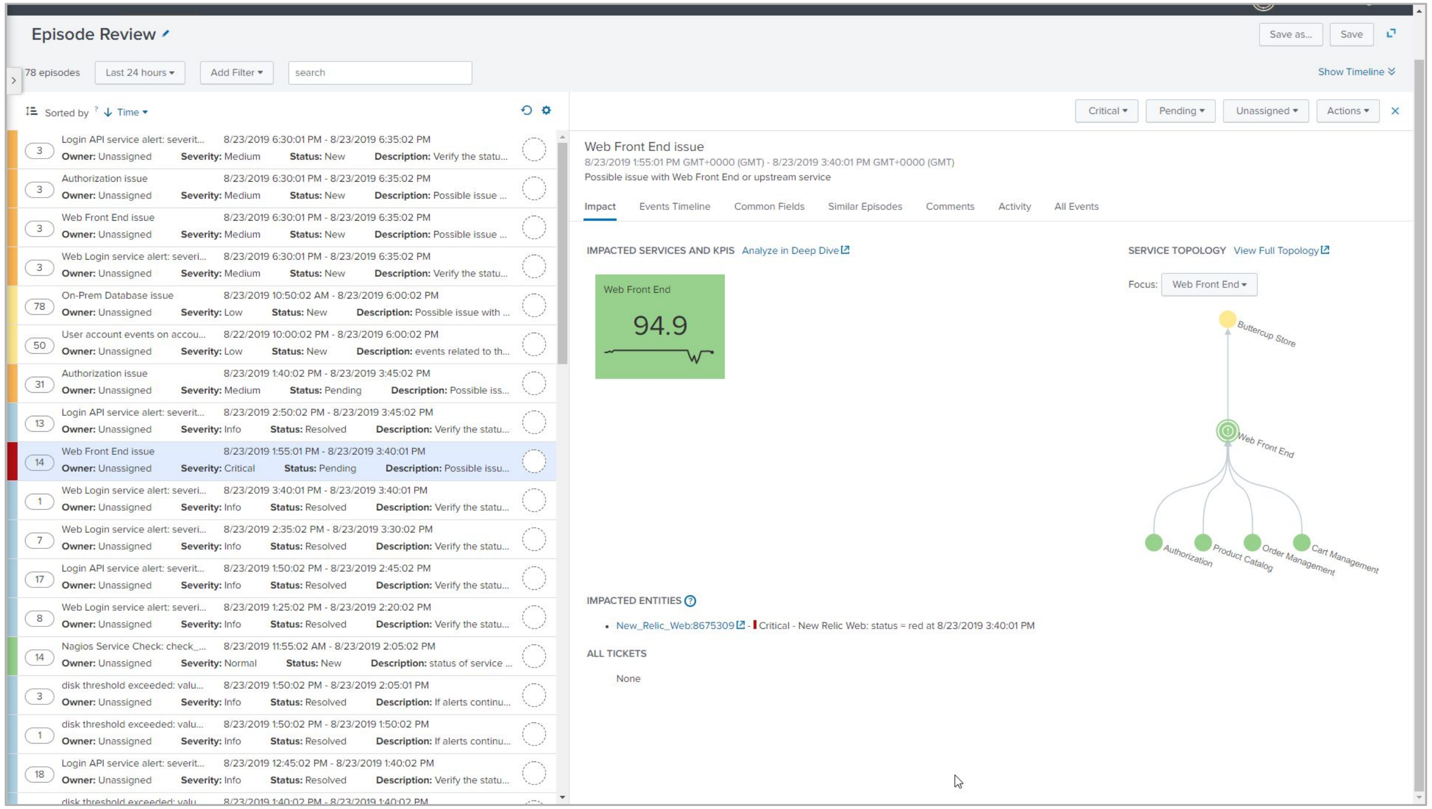
Episode Review

78 episodes

Count	Title	Time	Owner	Severity	Status	Description
3	Login API service alert: severity=4	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	Unassigned	Medium	New	Verify the status of the Login API service
3	Authorization issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	Unassigned	Medium	New	Possible issue with Authorization or upstr service
3	Web Front End issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	Unassigned	Medium	New	Possible issue with Web Front End or upstream service
3	Web Login service alert: severity=4	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	Unassigned	Medium	New	Verify the status of the Web Login service
78	On-Prem Database issue	8/23/2019 10:50:02 AM - 8/23/2019 6:00:02 PM	Unassigned	Low	New	Possible issue with On-Prem Database or upstream service
50	User account events on account scheduled	8/22/2019 10:00:02 PM - 8/23/2019 6:00:02 PM	Unassigned	Low	New	events related to the scheduled account
31	Authorization issue	8/23/2019 1:40:02 PM - 8/23/2019 3:45:02 PM	Unassigned	Medium	Pending	Possible issue with Authorization or upstr service
13	Login API service alert: severity=6	8/23/2019 2:50:02 PM - 8/23/2019 3:45:02 PM	Unassigned	Info	Resolved	Verify the status of the Login API service
14	Web Front End issue	8/23/2019 1:55:01 PM - 8/23/2019 3:40:01 PM	Unassigned	Critical	Pending	Possible issue with Web Front End or upstream service
1	Web Login service alert: severity=6	8/23/2019 3:40:01 PM - 8/23/2019 3:40:01 PM	Unassigned	Info	Resolved	Verify the status of the Web Login service
7	Web Login service alert: severity=6	8/23/2019 2:35:02 PM - 8/23/2019 3:30:02 PM	Unassigned	Info	Resolved	Verify the status of the Web Login service
17	Login API service alert: severity=4	8/23/2019 1:50:02 PM - 8/23/2019 2:45:02 PM	Unassigned	Info	Resolved	Verify the status of the Login API service
8	Web Login service alert: severity=4	8/23/2019 1:25:02 PM - 8/23/2019 2:20:02 PM	Unassigned	Info	Resolved	Verify the status of the Web Login service
14	Nagios Service Check: check_disk on mysql-02	8/23/2019 11:55:02 AM - 8/23/2019 2:05:02 PM	Unassigned	Normal	New	status of service check status check_disk on mysql-02 value=70.08
3	disk threshold exceeded: value=92.61 for host mysql-02 greater than threshold 90	8/23/2019 1:50:02 PM - 8/23/2019 2:05:01 PM	Unassigned	Info	Resolved	If alerts continue to occur, check host mys 02 for issues
1	disk threshold exceeded: value=88.22 for host mysql-02 greater than threshold 90	8/23/2019 1:50:02 PM - 8/23/2019 1:50:02 PM	Unassigned	Info	Resolved	If alerts continue to occur, check host mys 02 for issues
18	Login API service alert: severity=4	8/23/2019 12:45:02 PM - 8/23/2019 1:40:02 PM	Unassigned	Info	Resolved	Verify the status of the Login API service

Episode Review..

Event grouping allows for more effective troubleshooting
Service context gives the operator information to make a solid decision



3	Login API service alert: severit...	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Verify the statu...
3	Authorization issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Possible issue ...
3	Web Front End issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Possible issue ...
3	Web Login service alert: severi...	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Verify the statu...
78	On-Prem Database issue	8/23/2019 10:50:02 AM - 8/23/2019 6:00:02 PM	**Owner:** Unassigned	**Severity:** Low	**Status:** New	**Description:** Possible issue with ...
50	User account events on accou...	8/22/2019 10:00:02 PM - 8/23/2019 6:00:02 PM	**Owner:** Unassigned	**Severity:** Low	**Status:** New	**Description:** events related to th...
31	Authorization issue	8/23/2019 1:40:02 PM - 8/23/2019 3:45:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** Pending	**Description:** Possible iss...
13	Login API service alert: severit...	8/23/2019 2:50:02 PM - 8/23/2019 3:45:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
14	Web Front End issue	8/23/2019 1:55:01 PM - 8/23/2019 3:40:01 PM	**Owner:** Unassigned	**Severity:** Critical	**Status:** Pending	**Description:** Possible issu...
1	Web Login service alert: severi...	8/23/2019 3:40:01 PM - 8/23/2019 3:40:01 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
7	Web Login service alert: severi...	8/23/2019 2:35:02 PM - 8/23/2019 3:30:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
17	Login API service alert: severit...	8/23/2019 1:50:02 PM - 8/23/2019 2:45:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
8	Web Login service alert: severi...	8/23/2019 1:25:02 PM - 8/23/2019 2:20:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
14	Nagios Service Check: check_...	8/23/2019 11:55:02 AM - 8/23/2019 2:05:02 PM	**Owner:** Unassigned	**Severity:** Normal	**Status:** New	**Description:** status of service ...
3	disk threshold exceeded: valu...	8/23/2019 1:50:02 PM - 8/23/2019 2:05:01 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** If alerts continu...
1	disk threshold exceeded: valu...	8/23/2019 1:50:02 PM - 8/23/2019 1:50:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** If alerts continu...
18	Login API service alert: severit...	8/23/2019 12:45:02 PM - 8/23/2019 1:40:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
	disk threshold exceeded: valu...	8/23/2019 1:40:02 PM - 8/23/2019 1:40:02 PM				

Web Front End issue

8/23/2019 1:55:01 PM GMT+0000 (GMT) - 8/23/2019 3:40:01 PM GMT+0000 (GMT)

Possible issue with Web Front End or upstream service

IMPACTED SERVICES AND KPIS Analyze in Deep Dive

Web Front End 94.9

SERVICE TOPOLOGY View Full Topology

Focus: Web Front End ▾

IMPACTED ENTITIES

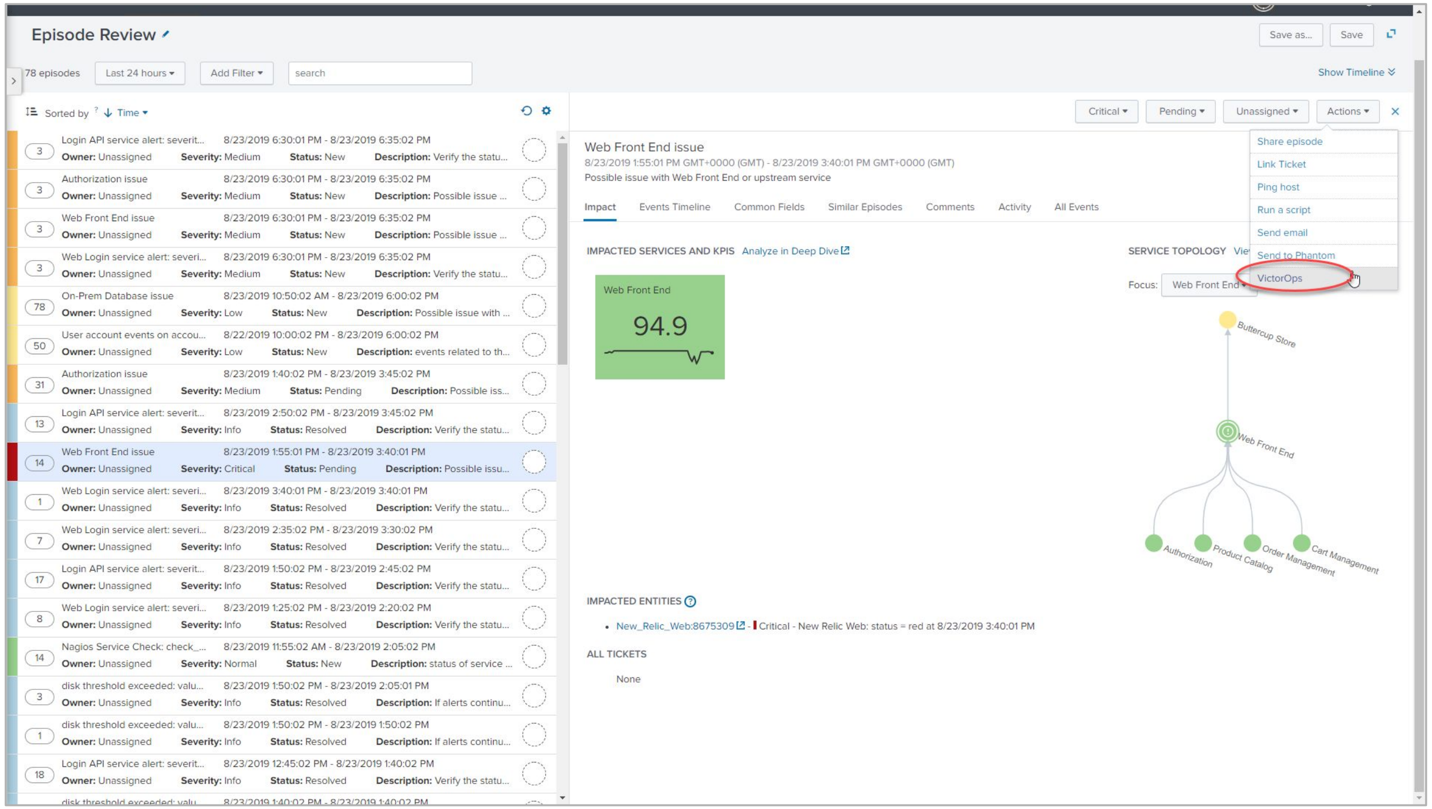
- New_Relic_Web:8675309 - Critical - New Relic Web: status = red at 8/23/2019 3:40:01 PM

ALL TICKETS

None

Episode Review..

- Event grouping allows for more effective troubleshooting
- Service context gives the operator information to make a solid decision
- Allows the operator to take action to remediate the problem



78 episodes

3 Login API service alert: severit... 8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM
Owner: Unassigned **Severity:** Medium **Status:** New **Description:** Verify the statu...

3 Authorization issue 8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM
Owner: Unassigned **Severity:** Medium **Status:** New **Description:** Possible issue ...

3 Web Front End issue 8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM
Owner: Unassigned **Severity:** Medium **Status:** New **Description:** Possible issue ...

3 Web Login service alert: severi... 8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM
Owner: Unassigned **Severity:** Medium **Status:** New **Description:** Verify the statu...

78 On-Prem Database issue 8/23/2019 10:50:02 AM - 8/23/2019 6:00:02 PM
Owner: Unassigned **Severity:** Low **Status:** New **Description:** Possible issue with ...

50 User account events on accou... 8/22/2019 10:00:02 PM - 8/23/2019 6:00:02 PM
Owner: Unassigned **Severity:** Low **Status:** New **Description:** events related to th...

31 Authorization issue 8/23/2019 1:40:02 PM - 8/23/2019 3:45:02 PM
Owner: Unassigned **Severity:** Medium **Status:** Pending **Description:** Possible iss...

13 Login API service alert: severit... 8/23/2019 2:50:02 PM - 8/23/2019 3:45:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

14 Web Front End issue 8/23/2019 1:55:01 PM - 8/23/2019 3:40:01 PM
Owner: Unassigned **Severity:** Critical **Status:** Pending **Description:** Possible issu...

1 Web Login service alert: severi... 8/23/2019 3:40:01 PM - 8/23/2019 3:40:01 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

7 Web Login service alert: severi... 8/23/2019 2:35:02 PM - 8/23/2019 3:30:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

17 Login API service alert: severit... 8/23/2019 1:50:02 PM - 8/23/2019 2:45:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

8 Web Login service alert: severi... 8/23/2019 1:25:02 PM - 8/23/2019 2:20:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

14 Nagios Service Check: check_... 8/23/2019 11:55:02 AM - 8/23/2019 2:05:02 PM
Owner: Unassigned **Severity:** Normal **Status:** New **Description:** status of service ...

3 disk threshold exceeded: valu... 8/23/2019 1:50:02 PM - 8/23/2019 2:05:01 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** If alerts continu...

1 disk threshold exceeded: valu... 8/23/2019 1:50:02 PM - 8/23/2019 1:50:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** If alerts continu...

18 Login API service alert: severit... 8/23/2019 12:45:02 PM - 8/23/2019 1:40:02 PM
Owner: Unassigned **Severity:** Info **Status:** Resolved **Description:** Verify the statu...

disk threshold exceeded: valu... 8/23/2019 1:40:02 PM - 8/23/2019 1:40:02 PM

Web Front End issue
8/23/2019 1:55:01 PM GMT+0000 (GMT) - 8/23/2019 3:40:01 PM GMT+0000 (GMT)
Possible issue with Web Front End or upstream service

IMPACTED SERVICES AND KPIS

SERVICE TOPOLOGY

IMPACTED ENTITIES

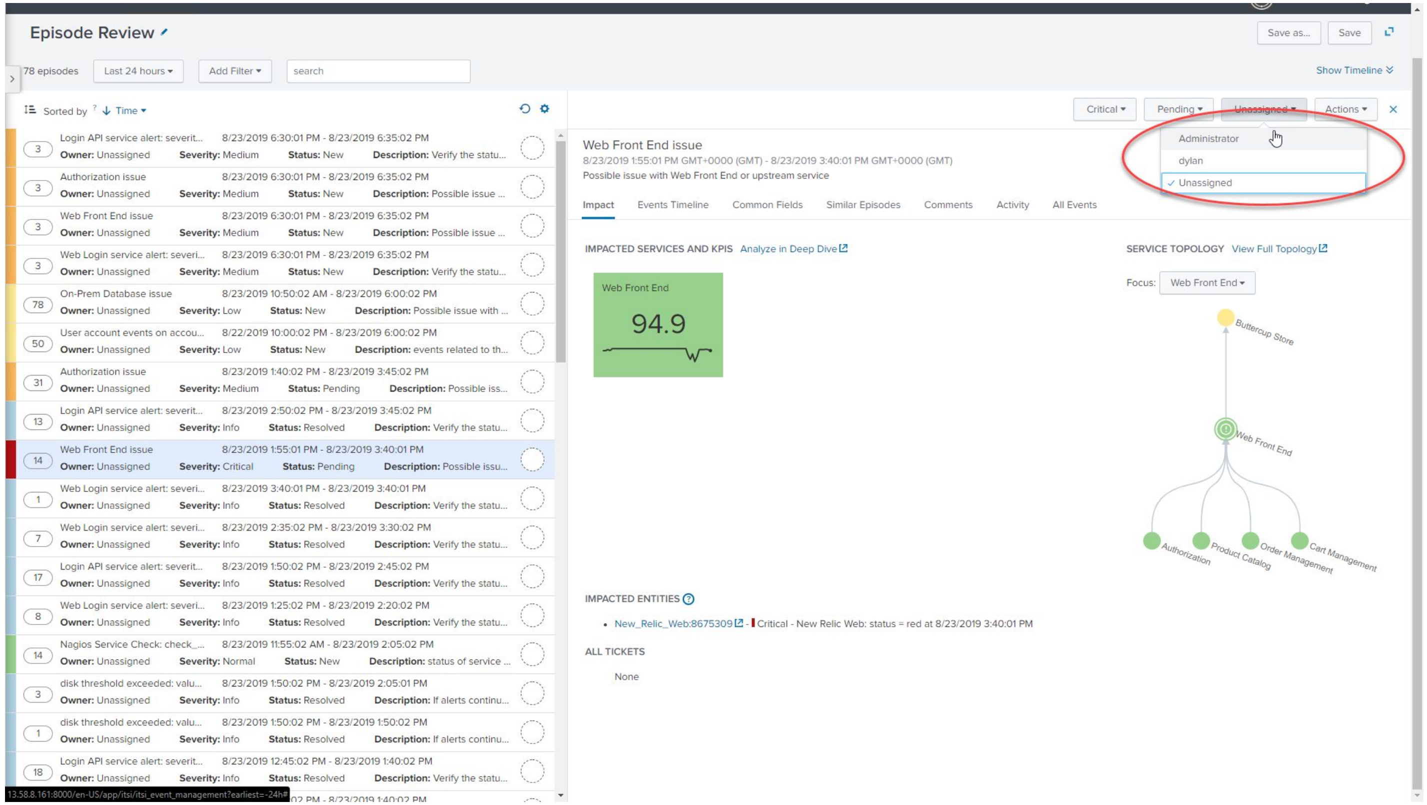
- New_Relic_Web:8675309 - Critical - New Relic Web: status = red at 8/23/2019 3:40:01 PM

ALL TICKETS

None

Episode Review..

- Event grouping allows for more effective troubleshooting
- Service context gives the operator information to make a solid decision
- Allows the operator to take action to remediate the problem
- Allows for easy assignment of the episode to work the issue more effectively



Episode Review

78 episodes Last 24 hours ▾ Add Filter ▾ search

Sorted by ↓ Time ▾

3	Login API service alert: severit...	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Verify the statu...
3	Authorization issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Possible issue ...
3	Web Front End issue	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Possible issue ...
3	Web Login service alert: severi...	8/23/2019 6:30:01 PM - 8/23/2019 6:35:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** New	**Description:** Verify the statu...
78	On-Prem Database issue	8/23/2019 10:50:02 AM - 8/23/2019 6:00:02 PM	**Owner:** Unassigned	**Severity:** Low	**Status:** New	**Description:** Possible issue with ...
50	User account events on accou...	8/22/2019 10:00:02 PM - 8/23/2019 6:00:02 PM	**Owner:** Unassigned	**Severity:** Low	**Status:** New	**Description:** events related to th...
31	Authorization issue	8/23/2019 1:40:02 PM - 8/23/2019 3:45:02 PM	**Owner:** Unassigned	**Severity:** Medium	**Status:** Pending	**Description:** Possible iss...
13	Login API service alert: severit...	8/23/2019 2:50:02 PM - 8/23/2019 3:45:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
14	Web Front End issue	8/23/2019 1:55:01 PM - 8/23/2019 3:40:01 PM	**Owner:** Unassigned	**Severity:** Critical	**Status:** Pending	**Description:** Possible issu...
1	Web Login service alert: severi...	8/23/2019 3:40:01 PM - 8/23/2019 3:40:01 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
7	Web Login service alert: severi...	8/23/2019 2:35:02 PM - 8/23/2019 3:30:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
17	Login API service alert: severit...	8/23/2019 1:50:02 PM - 8/23/2019 2:45:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
8	Web Login service alert: severi...	8/23/2019 1:25:02 PM - 8/23/2019 2:20:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...
14	Nagios Service Check: check_...	8/23/2019 11:55:02 AM - 8/23/2019 2:05:02 PM	**Owner:** Unassigned	**Severity:** Normal	**Status:** New	**Description:** status of service ...
3	disk threshold exceeded: valu...	8/23/2019 1:50:02 PM - 8/23/2019 2:05:01 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** If alerts continu...
1	disk threshold exceeded: valu...	8/23/2019 1:50:02 PM - 8/23/2019 1:50:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** If alerts continu...
18	Login API service alert: severit...	8/23/2019 12:45:02 PM - 8/23/2019 1:40:02 PM	**Owner:** Unassigned	**Severity:** Info	**Status:** Resolved	**Description:** Verify the statu...

13.58.8.161:8000/en-US/app/itsi/itsi_event_management?earliest=-24h#

02 PM - 8/23/2019 1:40:02 PM

Save as... Save

Show Timeline

Critical ▾ Pending ▾ Unassigned ▾ Actions ▾

- Administrator
- dylan
- ✓ Unassigned

Web Front End issue

8/23/2019 1:55:01 PM GMT+0000 (GMT) - 8/23/2019 3:40:01 PM GMT+0000 (GMT)

Possible issue with Web Front End or upstream service

Impact Events Timeline Common Fields Similar Episodes Comments Activity All Events

IMPACTED SERVICES AND KPIS Analyze in Deep Dive

Web Front End 94.9

SERVICE TOPOLOGY View Full Topology

Focus: Web Front End ▾

IMPACTED ENTITIES

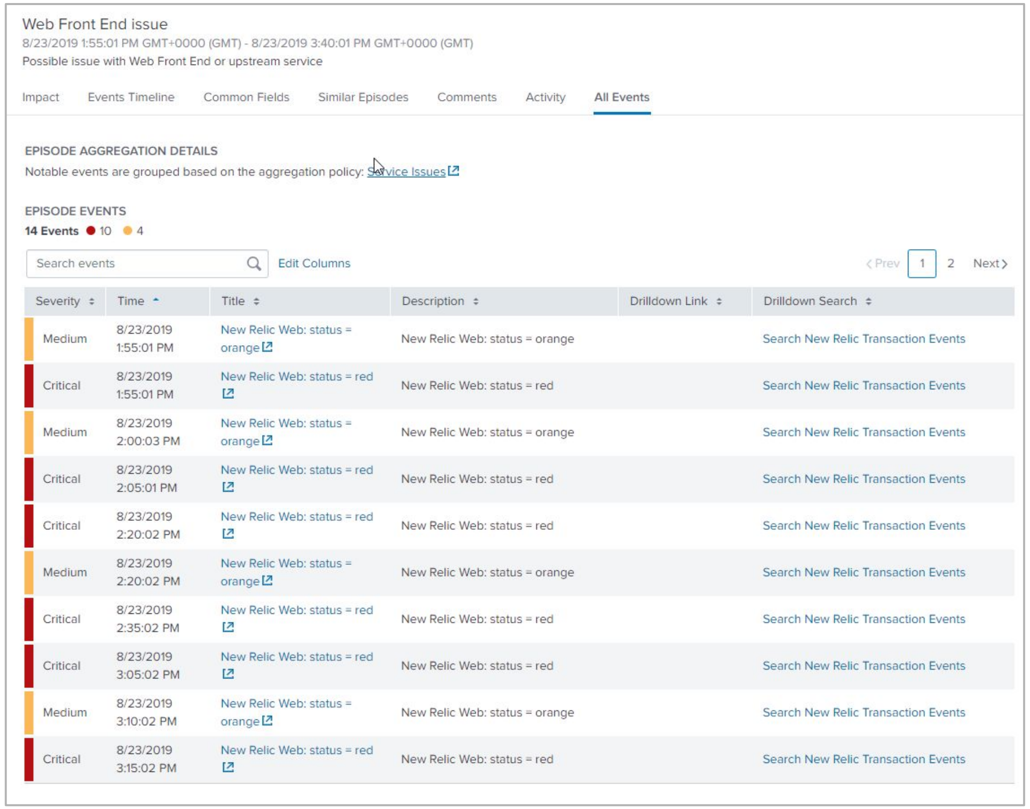
- New_Relic_Web:8675309 - Critical - New Relic Web: status = red at 8/23/2019 3:40:01 PM

ALL TICKETS

None

Episode Review..

- Event grouping allows for more effective troubleshooting
- Service context gives the operator information to make a solid decision
- Allows the operator to take action to remediate the problem
- Allows for easy assignment of the episode to work the issue more effectively
- Full details on each event that make up the episode



Web Front End issue

8/23/2019 1:55:01 PM GMT+0000 (GMT) - 8/23/2019 3:40:01 PM GMT+0000 (GMT)

Possible issue with Web Front End or upstream service

EPISODE AGGREGATION DETAILS

Notable events are grouped based on the aggregation policy: Service Issues

EPISODE EVENTS

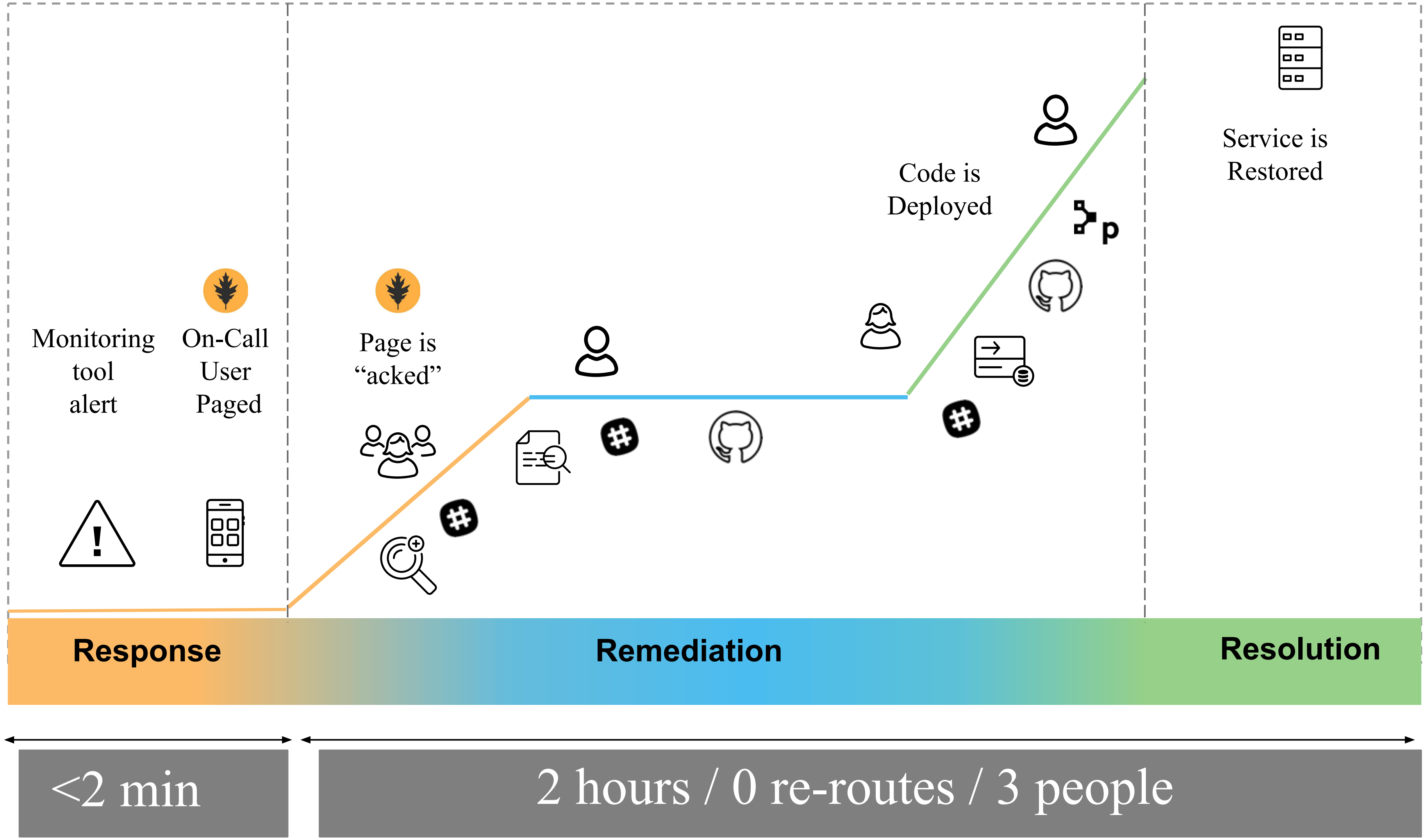
14 Events ● 10 ● 4

Severity	Time	Title	Description	Drilldown Link	Drilldown Search
Medium	8/23/2019 1:55:01 PM	New Relic Web: status = orange	New Relic Web: status = orange		Search New Relic Transaction Events
Critical	8/23/2019 1:55:01 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events
Medium	8/23/2019 2:00:03 PM	New Relic Web: status = orange	New Relic Web: status = orange		Search New Relic Transaction Events
Critical	8/23/2019 2:05:01 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events
Critical	8/23/2019 2:20:02 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events
Medium	8/23/2019 2:20:02 PM	New Relic Web: status = orange	New Relic Web: status = orange		Search New Relic Transaction Events
Critical	8/23/2019 2:35:02 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events
Critical	8/23/2019 3:05:02 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events
Medium	8/23/2019 3:10:02 PM	New Relic Web: status = orange	New Relic Web: status = orange		Search New Relic Transaction Events
Critical	8/23/2019 3:15:02 PM	New Relic Web: status = red	New Relic Web: status = red		Search New Relic Transaction Events

Live DEMO

splunk> .conf19

Simplify Incident Response with VictorOps



Monitoring tool alert

On-Call User Paged

Page is "acked"

Code is Deployed

Service is Restored

Response

Remediation

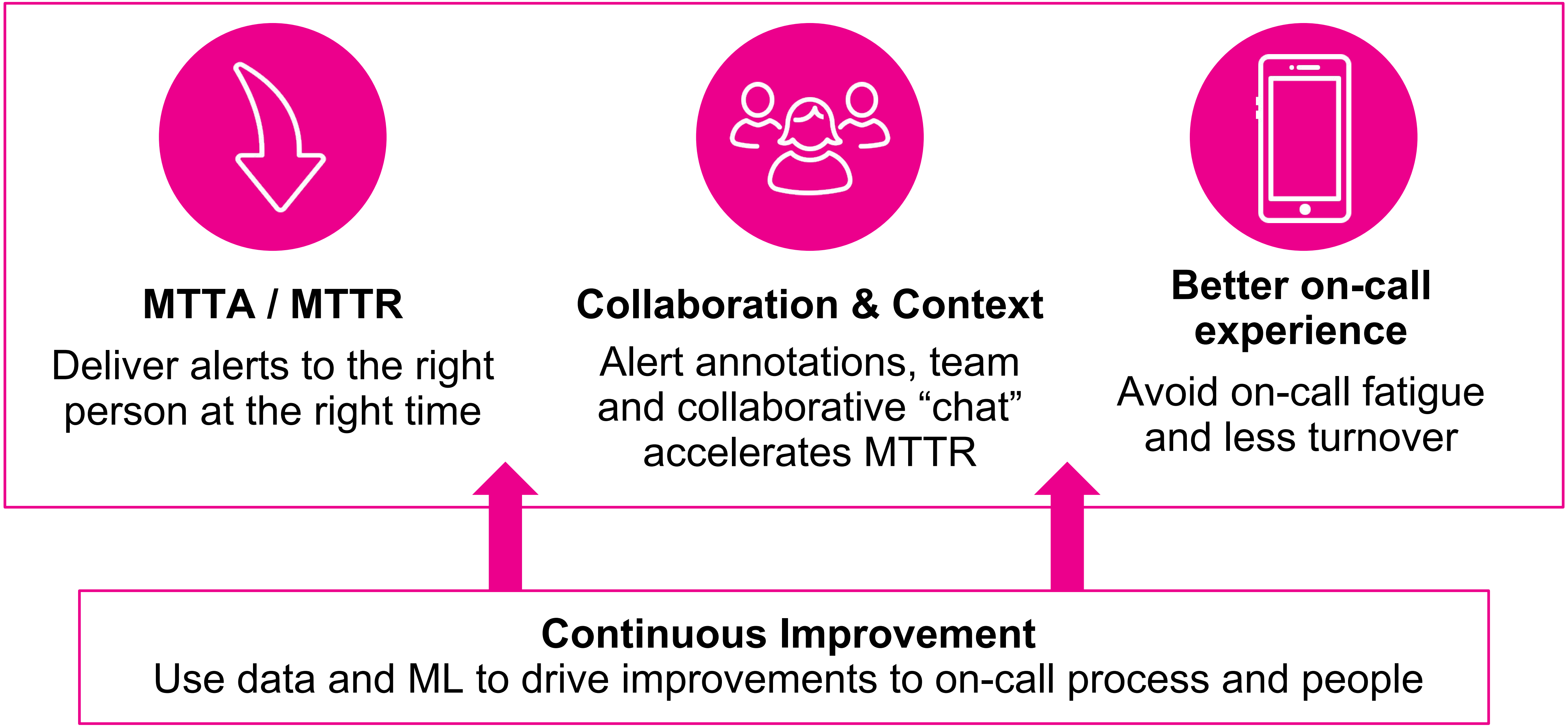
Resolution

<2 min

2 hours / 0 re-routes / 3 people

Before
25-45 min

Before
6 hours / 5 re-routes / 8 people



MTTA / MTTR

Deliver alerts to the right person at the right time

Collaboration & Context

Alert annotations, team and collaborative “chat” accelerates MTTR

Better on-call experience

Avoid on-call fatigue and less turnover

Continuous Improvement

Use data and ML to drive improvements to on-call process and people

ITSI+VO enables you to Identify, Investigate and Resolve Critical Service Issues FASTER

Today you have:

- Guesswork
- Reactive
- Unproductive

with ITSI + VO:

- NO Guesswork -Context
- Proactive -Early Warning KPIs
- Productive -Reduced Distractions

ITSI+VO enables you to Identify, Investigate and Resolve Critical Service Issues FASTER

Guesswork

Reactive

Unproductive

splunk> + VictorOps

Try VictorOps Free

Try.VictorOps.com for a 14-Day, Free Trial

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION