



Integrating Splunk and VictorOps to Connect Alerts and Events

Delivering reliable software faster

Dave Wiedenheft

October 2018 | Version 1.0

Forward-Looking Statements

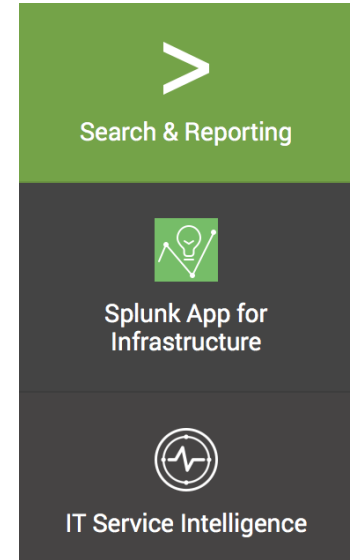
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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. © 2018 Splunk Inc. All rights reserved.

Agenda

- ▶ Why DevOps
- ▶ What is Collaborative Incident Management
- ▶ VictorOps Integrations
- ▶ Splunk + VictorOps Integrations
- ▶ VictorOps Tips



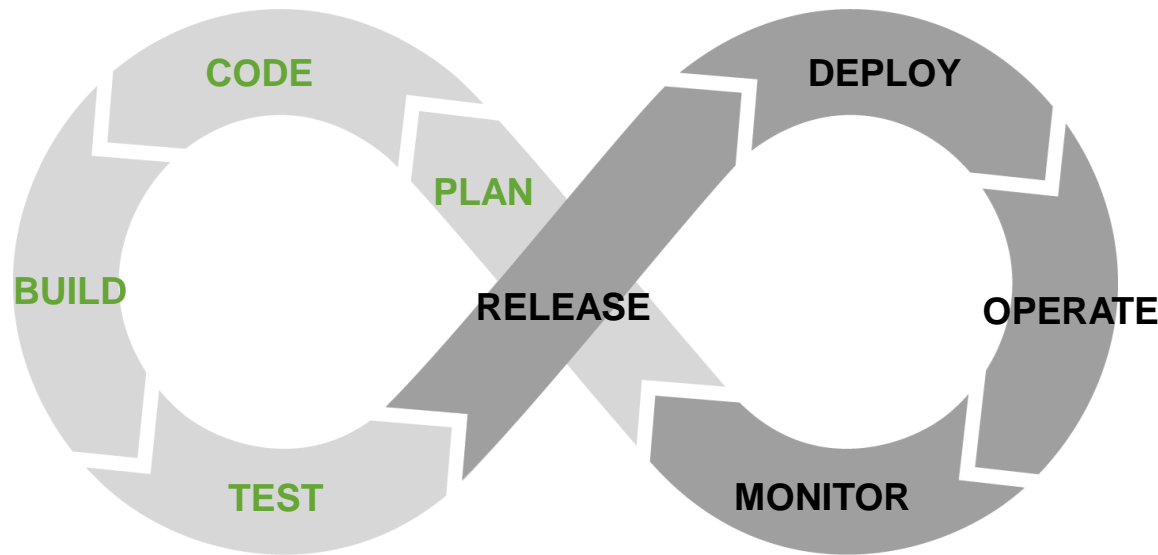


Why DevOps

Reliable software faster

Why DevOps

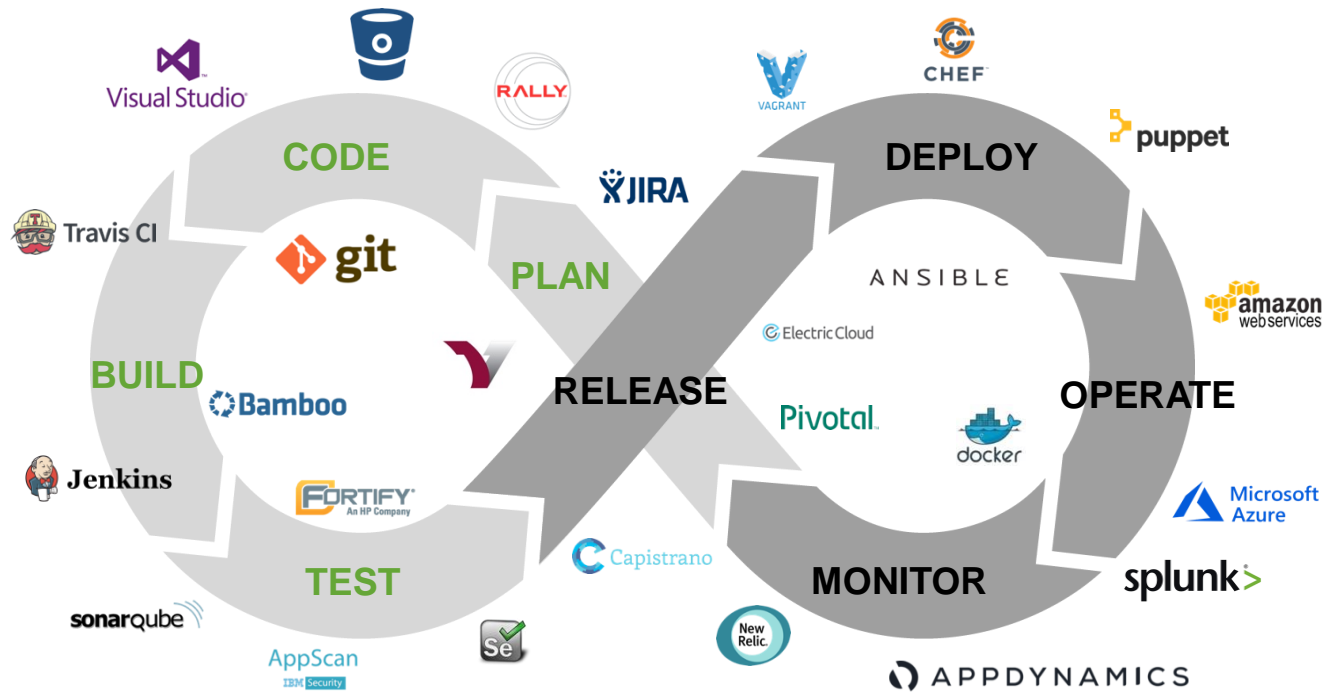
- ▶ **440x faster** from commit to deploy
- ▶ **46x more** frequent code deployments
- ▶ **96x faster** Recovery from downtime
- ▶ **5x lower** change fail rates
- ▶ **2.2x more** likely to recommend company to friends



Forsgren, Humble, Kim, *Accelerate*. Portland, OR: IT Revolution, 2018

Why DevOps

- ▶ **440x faster** from commit to deploy
- ▶ **46x more** frequent code deployments
- ▶ **96x faster** Recovery from downtime
- ▶ **5x lower** change fail rates
- ▶ **2.2x more** likely to recommend company to friends



Forsgren, Humble, Kim, *Accelerate*. Portland, OR: IT Revolution, 2018

Collaborative Incident Management





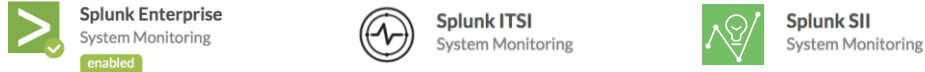
VictorOps Integrations

VictorOps works with your ecosystem

Lots of Integration Options

Open ecosystem

Splunk Integrations

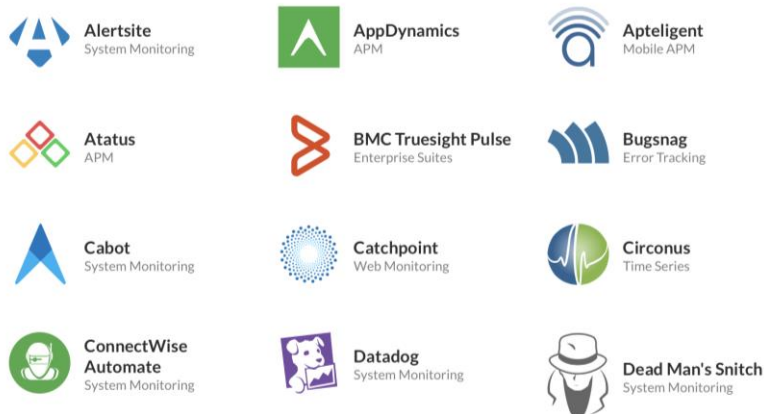


- ▶ ~100 integrations
- ▶ Best in class support
- ▶ Easy to set up and configure
- ▶ Some REST APIs

Other Integrations



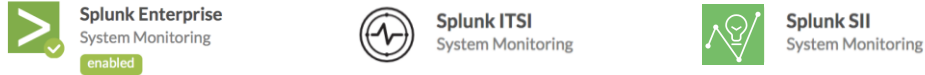
All Integrations



Lots of Integration Options

Open ecosystem

Splunk Integrations

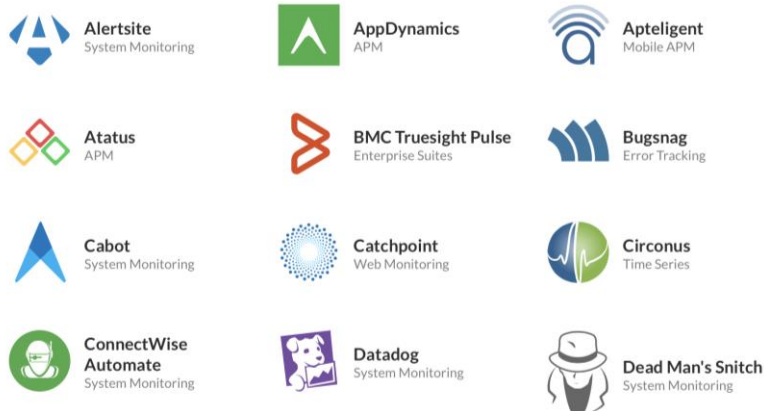


- ▶ ~100 integrations
- ▶ Best in class support
- ▶ Easy to set up and configure
- ▶ Some REST APIs

Other Integrations



All Integrations



Knowledge Base

Step by step guide to configuration

splunk > + VictorOps

PRODUCT PRICING DEMO ABOUT

Blog Resources Support Log In

Start Free Trial

Home > Integrations > Splunk Integration Guide – VictorOps (New)

Q Search

Contents

In VictorOps

In Splunk

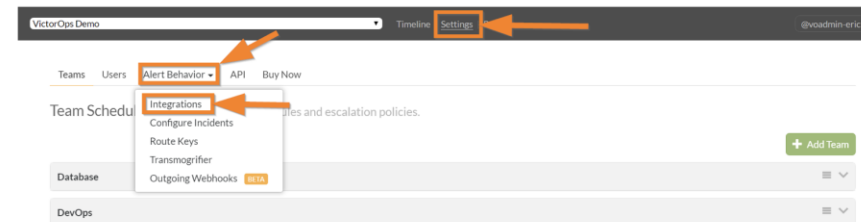
- [Modifying the Application](#)

Splunk Integration Guide – VictorOps (New)

Splunk transforms machine-generated data into valuable insights that can help make your business more productive, profitable and secure. The following guide will walk you through this integration.

In VictorOps

From the VictorOps web portal, select **Settings**, then **Alert Behavior**, then **Integrations**.

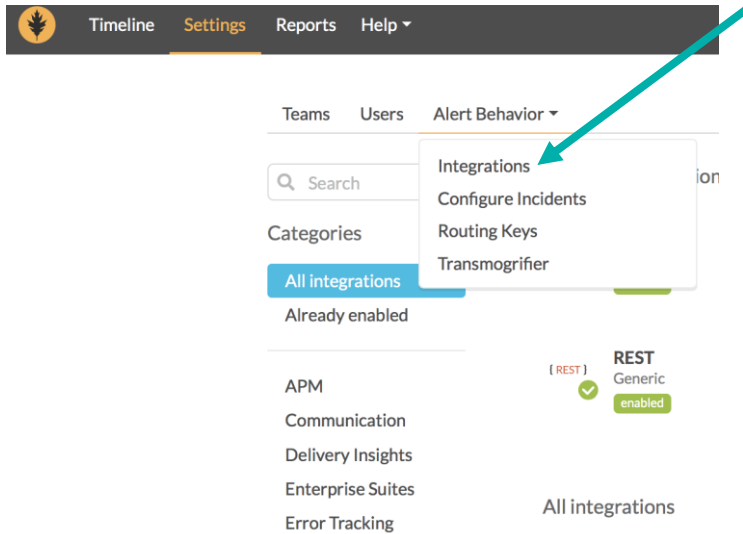


Select the **Splunk, Inc** integration option.



Easy to Enable

From the VictorOps portal



[Integrations](#) / [Splunk, Inc](#)



Splunk Inc. provides the leading platform for Operational Intelligence. Customers use Splunk to search, monitor, analyze and visualize machine data. This integration allows you to send Splunk alerts into VictorOps.

Learn more in the [knowledge base](#).

Service API Endpoint

[https://alert.victorops.com/integrations/generic/20131114/alert/fe\[redacted\]22/\\$routing_key](https://alert.victorops.com/integrations/generic/20131114/alert/fe[redacted]22/$routing_key)



splunk[®]>

+

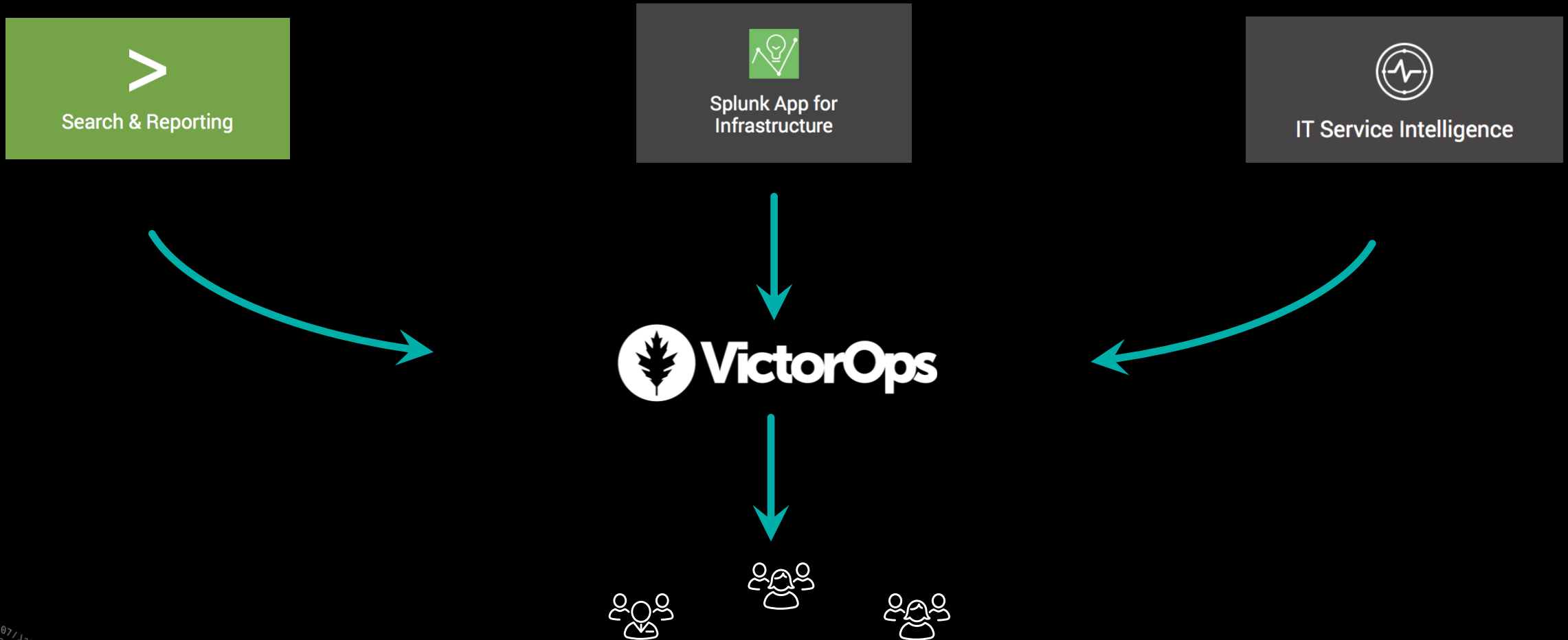


VictorOps

Your favorite Splunk products now with VictorOps

Engage the right person from your alerts

Engage the right person from your alerts




Splunk Enterprise + VictorOps







Turn your alerts into incidents

Get the VictorOps

Available for download in Splunkbase



VictorOps For Splunk






13 ratings
 Splunk AppInspect Passed

ADMINISTRATOR TOOLS:
[Manage App](#) | [View App](#) | [View Analytics](#)

Overview

Details

Splunk + VictorOps extends the alerting and messaging from Splunk Enterprise or Splunk Cloud into the VictorOps Incident Management platform. This allows you to leverage your existing team contact, scheduling, and escalation policies for your Splunk alerts.

VictorOps is a hub for centralizing the flow of information throughout the incident lifecycle. Driven by IT and DevOps system data, VictorOps provides a unified platform for real-time alerting, collaboration, and documentation.

Using VictorOps, teams resolve incidents faster to help minimize the impact of downtime and speed innovation.

NOTE: When upgrading to v1.0.7, be sure to check the "overwrite existing app" option, and re-enter the integration api key from the integration page.

Release Notes

Version 1.0.8 Sept. 27, 2018

- * Additional configurability for incident creation
- * updated help links

106
Installs

313
Downloads

Download

Rate this App

VERSION

1.0.8 ↕

BUILT BY

[Cordis Hall](#)

CATEGORY & CONTENTS

Categories: [IT Operations](#), [DevOps](#)

App Type: [App](#)

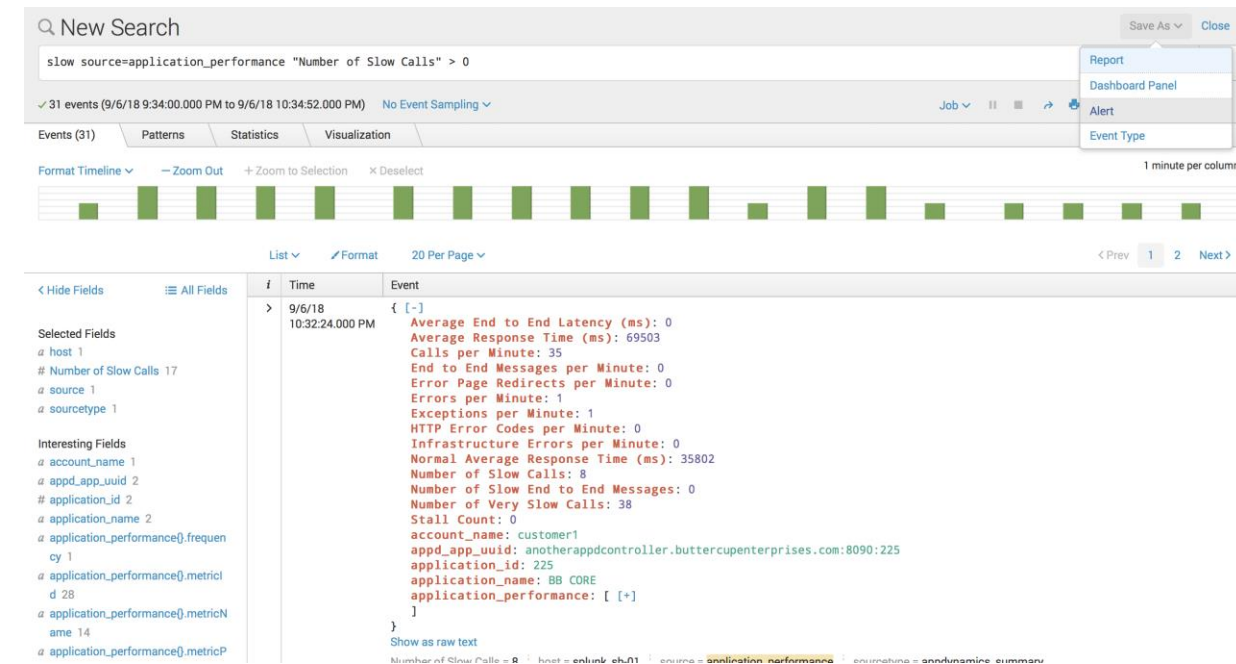
App Contents: [Alert Actions](#)

COMPATIBILITY

-

Splunk Enterprise + VictorOps

- ▶ Take your existing alerts and turn them into incidents
- ▶ Route them to the right team(s) (via Route Key)
- ▶ Customize id / message



Trigger Actions

When triggered

+ Add Actions

VictorOps

Message Type: **CRITICAL** (INFO, WARNING, ACKNOWLEDGEMENT, RECOVERY)

Monitoring Tool: Enter the message type to send to VictorOps.

Alert Entity ID: \$name\$ (Optional) Victorops Entity ID.


Alert Entity Display Name: \$name\$ (Optional) Victorops Entity Display Name.

State Message: \$description\$ (Optional) Enter the state message to send to VictorOps. The message can include tokens that insert text based on the results of the search. [Learn More](#)

Routing Key: SRE (Optional) Override the globally configured VictorOps routing key.

Cancel Save

Splunk Enterprise + VictorOps



The diagram illustrates the integration between Splunk Enterprise and VictorOps. On the left, a Splunk search interface shows a search for "slow source=application_performance \"Number of Slow Calls\" > 0". The search results are displayed in a table with columns for Time, Event, and Fields. A green arrow points from the Splunk search results to the VictorOps incident view on the right.

VictorOps Incident View:

- Incident #3599 Splunk, Inc** (Sep. 6 - 4:39 PM)
- Description:** Splunk, Inc: Slow Calls from anotherappdcontroller.buttercupenterprises.com:8090:225
- Policies:** A team : Standard
- Annotations:** 2 Annotations
- Alerts:** 1 Alert
- Incident Details:**
 - Splunk, Inc** (Sep. 6 - 4:39 PM)
 - Critical:** Slow Calls from anotherappdcontroller.buttercupenterprises.com:8090:225
 - Number of Slow Calls:** 8
 - #3599 / 2 annotations**
 - [Alert Payload](#)

Incident #3599 Details:

- Incident #3599** (Sep. 6 - 4:39 PM)
- Description:** Splunk, Inc: Slow Calls from anotherappdcontroller.buttercupenterprises.com:8090:225
- Policies:** A team : Standard
- Paging:** mgourlay2
- Details:**
 - 1. Look at Runbooks
 - 2. Splunk Alert Link
 - 3. Runbooks
 - 4. JIRA Link
 - 5. Create ServiceNow Ticket

Splunk Enterprise + VictorOps

Timeline Settings Reports Help
Customize View v votest-vo2

Timeline

Filters v

Incident #3599 Splunk, Inc
Sep. 6 - 4:39 PM

Splunk, Inc: Slow Calls from anotherappdcontroller.buttercupenterprises.com:8090:225

Policies: **A team : Standard**

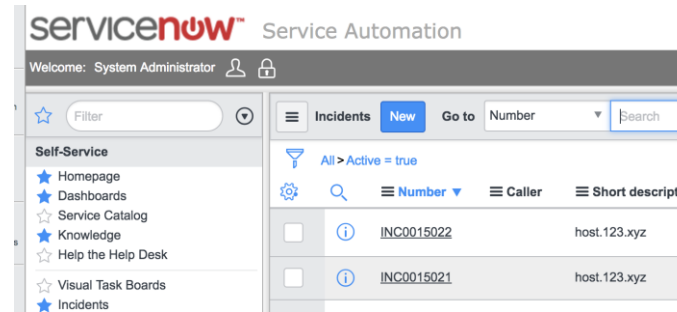
2 Annotations
 1 Alert
Incident Details

Splunk, Inc
Sep. 6 - 4:39 PM

Critical: Slow Calls from anotherappdcontroller.buttercupenterprises.com:8090:225

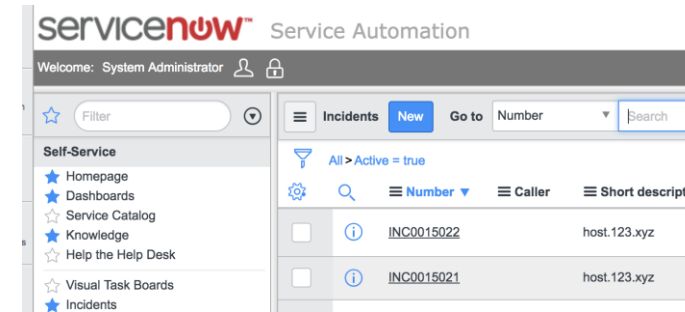
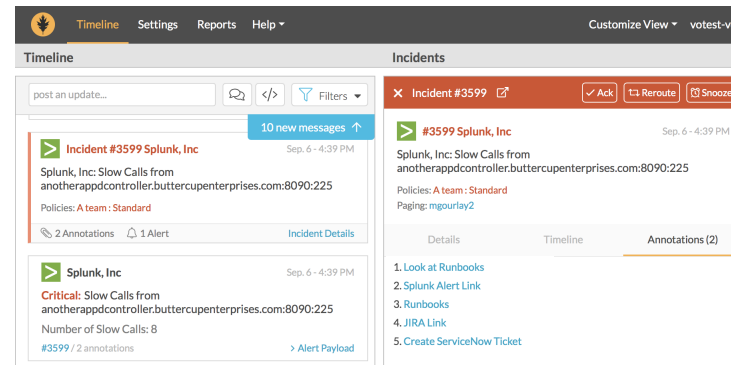
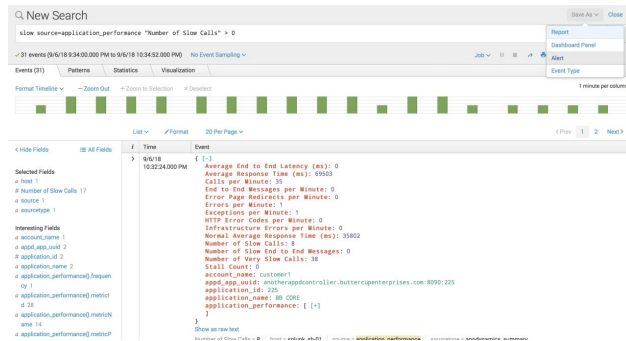
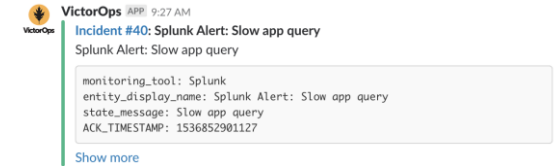
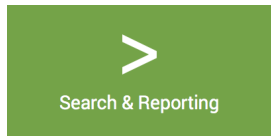
Number of Slow Calls: 8

#3599 / 2 annotations > Alert Payload



Splunk Enterprise + VictorOps

► Automatically sync data across tools



All Systems Operational

Notifications - SMS	✓	Notifications - Google Push	✓
Notifications - Apple Push	✓	Notifications - Email	✓
Notifications - Phone	✓	Alert Ingestion	✓
Alert Ingestion - Inbound email	✓	API	✓
Web client (portal)	✓	Android client	✓

Splunk ITSI + VictorOps

Incidents from Notable Event Groups



Notable Events to VictorOps



Splunk IT Service
Intelligence™



Notable Events Review

212 groups Last 24 hours Add Filter search Show Time

Sorted by Time

	Customer Transaction Issue	9/17/2018 8:14:31 PM - 9/17/2018 8:56:...	
100+	Owner: Unassigned Severity: Medium Status: Resolved Descri...		
4	Change Event	9/17/2018 7:48:27 PM - 9/17/2018 8:24:...	
	Owner: Unassigned Severity: High Status: Resolved Descrip...		
72	Nagios Service Check check_dh...	9/17/2018 7:21:25 PM - 9/17/2018 8:22:...	
	Owner: Unassigned Severity: Normal Status: Resolved Descrip...		
63	Nagios Service Check check_ntp...	9/17/2018 7:21:25 PM - 9/17/2018 8:22:...	
	Owner: Unassigned Severity: Normal Status: Resolved Descrip...		
12	Nagios Service Check check_ssl...	9/17/2018 7:21:25 PM - 9/17/2018 8:22:...	
	Owner: Unassigned Severity: Critical Status: Resolved Descrip...		
4	Change Event	9/17/2018 8:13:28 PM - 9/17/2018 8:13:...	
	Owner: Unassigned Severity: High Status: New Description: R...		
1	SNOW Change Request: comple...	9/17/2018 8:04:28 PM - 9/17/2018 8:09:...	
	Owner: Unassigned Severity: Low Status: Resolved Descrip...		
9	Nagios Service Check check_ntp...	9/17/2018 7:21:25 PM - 9/17/2018 8:03:...	
	Owner: Unassigned Severity: Medium Status: Resolved Descri...		
100+	Customer Transaction Issue	9/17/2018 7:14:27 PM - 9/17/2018 7:57:...	
	Owner: Unassigned Severity: Medium Status: Resolved Descri...		
36	Entity level alert on KPI: CPU Lo...	9/17/2018 4:01:07 PM - 9/17/2018 7:55:...	
	Owner: Unassigned Severity: Medium Status: New Description...		
4	Change Event	9/17/2018 6:48:23 PM - 9/17/2018 7:24:...	
	Owner: Unassigned Severity: High Status: Resolved Descrip...		
63	Nagios Service Check check_ntp...	9/17/2018 6:21:22 PM - 9/17/2018 7:22:...	
	Owner: Unassigned Severity: Normal Status: Resolved Descrip...		
72	Nagios Service Check check_dh...	9/17/2018 6:21:22 PM - 9/17/2018 7:22:...	
	Owner: Unassigned Severity: Normal Status: Resolved Descrip...		

Customer Transaction Issue
9/17/2018 8:14:31 PM - 9/17/2018 8:56:20 PM

Overview Grouped Events Comments Activity

Description
customer-facing issue that should be triaged ASAP

Group Aggregation Details
539 Notable Events are grouped based on the aggregation policy: [Transaction Errors](#)

487 38 14

All Tickets
None

Contributing KPIs [Open all in Deep Dive](#)

- Database Service Response Time
- Database Service Errors
- Storage Free Space: %

Possible Affected Services [Open all in Deep Dive](#)

- Database
- Web Store
- Middleware

Common Fields

> NetObject: 5 values (expand for details)
> account_id: 2 values (expand for details)
active: true
> activity_due: 8 values (expand for details)
alert: Orion GSMC alert response test down
> alert_color: 3 values (expand for details)
> alert_level: 3 values (expand for details)
> alert_severity: 3 values (expand for details)
> alert_value: 5 values (expand for details)
all_service_kpi_ids: 92eae0d1-7ea0-4d52-8500-d6c19bd48dfa:f83e69070f542a13e2b9c56 92eae0d1-7ea0-4d52-8500-d6c19bd48dfa:722da88e4903202b4a22ad5a 92eae0d1-7ea0-4d52-8500-d6c19bd48dfa:bd0bb11ebebefce1ab5bb75a
application_summary.apdex_score: 0.0
> application_summary.apdex_target: 2 values (expand for details)

Incident #53 Triggered

Sep. 17 - 4:10 PM

API: ITS: Customer Transaction Issue

Policies: **Web**: Web On-Call

3 Annotations 1 Alert

[Incident Details](#)



Sep. 17 - 4:10 PM

Critical: ITS: Customer Transaction Issue

ITS: Customer Transaction Issue

#53 / 3 annotations

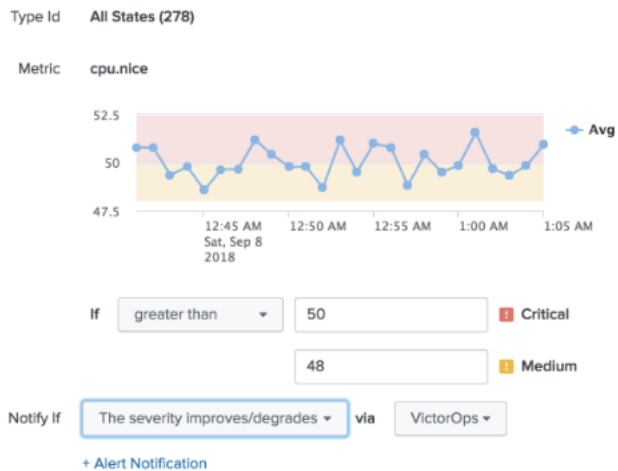
[Alert Payload](#)



Splunk App for Infrastructure + VictorOps

Send alerts to VictorOps

App for Infrastructure



Incident #54 Triggered

Sep. 17 - 4:16 PM

API: SII: CPU > 50%

Policies: Web : Web On-Call

3 Annotations 1 Alert

[Incident Details](#)

Splunk SII

Sep. 17 - 4:16 PM

Critical: SII: CPU > 50%

CPU > 50%

#54 / 3 annotations

[Alert Payload](#)

VictorOps Tips

Getting the most out of your free trial

Timeline (s)

Overall timeline

- ▶ Everything shows up here
- ▶ Easy-to-use filtering
- ▶ Clear incident status

Incident Specific Timeline

Incident #295
Resolve
Reroute
Snooze

#295 Acknowledged
Sep. 30 - 1:16 PM

API: Customer Transaction Issue
Policies: SRE : SRE Primary On-Call
Acked by: dwiedenheft2

Annotations

- JIRA Link
- Look at Runbooks
- ITSI Notable Events View
- Create ServiceNow Ticket

Details

post an update...

Incident #295 Acknowledged
Sep. 30 - 1:19 PM

API: Customer Transaction Issue
Policies: SRE : SRE Primary On-Call
Acked by: dwiedenheft2

4 Annotations 21 Alerts

@dwiedenheft2
Sep. 30 - 1:19 PM

Looks like the database is running slow #incident295

@dwiedenheft2
Sep. 30 - 1:19 PM

I'm looking into this #incident295

Splunk ITSI
Sep. 30 - 1:16 PM

Critical: Customer Transaction Issue
Customer Transaction Issue
4 annotations

Splunk ITSI
Sep. 30 - 1:16 PM

Timeline

Timeline

post an update...

8 messages hidden

Paging cancelled for dviola
Sep. 28 - 10:00 PM

Paging cancelled for hose
Sep. 28 - 10:00 PM

Incident #481 Pingdom
Sep. 28 - 10:00 PM

Pingdom: demo.acme.com / demo.acme.com
Policies: Operations Support : Business Hours, Operations Support : Nights and Weekends
Resolved by: todd

0 Annotations 3 Alerts

Incident Details

Nagios
Sep. 28 - 10:00 PM

Recovery: demo.acme.com / demo.acme.com
PingdomAlert UP: demo.acme.com (demo.acme.com) is up again at 04:00:05
Host: demo.acme.com
State: UP
Output: UP

#481

Alert Payload

Trying to contact dviola for #481, sending EMAIL
Sep. 28 - 9:59 PM

Trying to contact hose for #481, sending EMAIL
Sep. 28 - 9:59 PM

Paging cancelled for hweldon
Sep. 28 - 9:59 PM

Incident #490 AWS CloudWatch
Sep. 28 - 9:59 PM

AWS CloudWatch: EBS Alarm
Policies: Infrastructure : Primary
Resolved by: toddvernon

splunk> .conf18

At a glance visibility into your team

See who is engaged

The screenshot shows the 'People' section of a Splunk dashboard. It has tabs for 'Teams' and 'Users', with a search icon. Below these are filter buttons: 'On-call', 'Engaged', 'Teammates', and 'All Users'. A list of team members is displayed, each with a green dot, name, and handle. The first member, Dave Wiedenheft, is highlighted by a red arrow from the text 'See who is engaged'. The second member, Todd Untrecht, has a red 'Data' label and a red on-call icon, highlighted by a red arrow from the text 'See who is on-call'. The third member, Alex H, has a red 'Mobile' label and a red on-call icon. The fourth member, Maria R, has a red 'Web' label and a red on-call icon. The fifth member, Bill B, has no label or icon.

Name	Handle	Status	On-call
Dave Wiedenheft	@dwiedenheft2		
Todd Untrecht	@tuntrecht	Data	Yes
Alex H	@aleXH	Mobile	Yes
Maria R	@mariar	Web	Yes
Bill B			


See who is on-call

Powerful Customization via Rules


Add/modify incoming alerts

Conditional Annotations


Things you can do with the transmogriker...

- 

Annotate alerts with images, links, and notes.

Get the info you need to make decisions in the moment by surfacing documentation, runbooks, or graphs based on alert contents. [Learn about annotations.](#)
- 

Overwrite alert fields or add new fields.

Change where alerts get routed, add your own data, or quiet noisy alarms. [Learn about transforms.](#)
- 

Go big with advanced features.

Use variable expansion to build dynamic annotations, create cascading rules, and more. [Learn about advanced features.](#)

When `message_type` matches `CRITICAL`

🔗 Annotate the alert with:

- URL [Create ServiceNow Ticket](#)
- URL [JIRA Link](#)
- URL [Look at Runbooks](#)

Conditional Logic

When `entity_display_name` matches `*SNOW*`

✂ Transform these alert fields:

- Set `ServiceNow_Integration` to new value `true`
- Set `ServiceNowField_u_test_custom_field_name` to new value `{{state_message}}+{{monitoring_tool}}`

↓ Continue processing after this rule has been applied



Full Stack Reporting

Post-Incident Reviews

Analyze incidents and mark action steps to continuously improve

EVENT: #21305 was OPENED for SERVICE vicv2-12287609/

21:55 GMT-0700
Location San Francisco, CA
reluc.com/accounts/39...

EVENT: #21306 was OPENED for SERVICE vicv2-12287606/

22:05 GMT-0700
Location Sydney, AU
reluc.com/accounts/39...

FX: Trying to contact vicv2@victorops.com for 2 incidents: #21306, #21305, sending EMAIL

Timeline notes
Hover over a moment in the timeline and click the note icon to add a Timeline note. Notes you add will also show here.

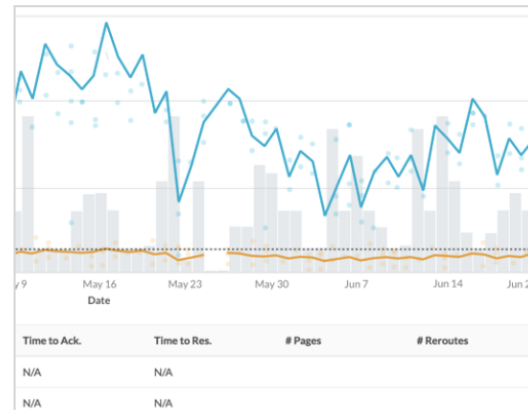
Action Items

- Look into getting raw/log data from cloudflare to identify failed requests as well as affected orgs (delete)
- Identify how we decide when & how to create a statuspage event - ask ops support to prescribe this to us (delete)
- Figure out how to share schedule maintenance info with more context (for example, the person on-call during that event) (delete)

+ add action item

Performance (MTTA/MTTR)

Evaluate your organizational and team incident metrics



On-Call

Understand individual On-Call and incident workload

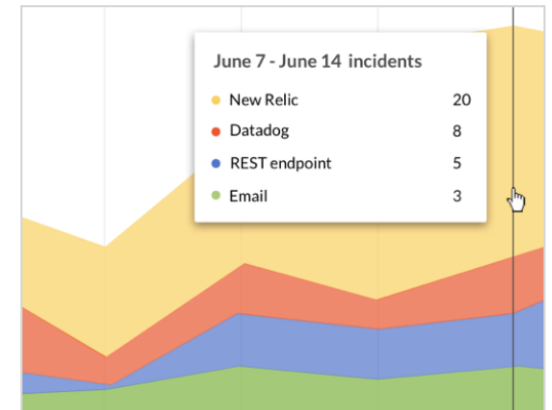
Date	Time On-call	Esc. Policy	Rotation
Dec. 18, 2017	10:24 (13:36 - 24:00)	On-Call	DevOps Rotation (H)
Dec. 19, 2017	24:00 (00:00 - 24:00)	On-Call	DevOps Rotation (H)
Dec. 20, 2017	10:30 (00:00 - 10:30)	On-Call	DevOps Rotation (H)
Dec. 29, 2017	13:30 (10:30 - 24:00)	On-Call	DevOps Rotation (V)
Dec. 30, 2017	24:00 (00:00 - 24:00)	On-Call	DevOps Rotation (V)
Dec. 31, 2017	24:00 (00:00 - 24:00)	On-Call	DevOps Rotation (V)
Jan. 1, 2018	24:00 (00:00 - 24:00)	On-Call	DevOps Rotation (V)
Jan. 2, 2018	10:30 (00:00 - 10:30)	On-Call	DevOps Rotation (V)

Incidents worked on by charlie waneke

Incident	Timeline
[21866]disk/	Dec. 20, 2017 - 10:08 PAGED
	Dec. 20, 2017 - 10:08 ACKED


Incident Frequency

Pinpoint the frequent incident causing parts of your ecosystem




Key Takeaways



- ▶ DevOps can help you move faster and be more reliable
- ▶ Minimizing downtime requires:
 - Proactive approach and continuous improvement
 - Delivering the right information the right person
- ▶ **splunk>** +  **VictorOps**
powerful combination to help you minimize downtime

Key Takeaways



- ▶ DevOps can help you move faster and be more reliable
- ▶ Minimizing downtime requires:
 - Proactive approach and continuous improvement
 - Delivering the right information the right person
- ▶ **splunk>** +  **VictorOps**
powerful combination to help you minimize downtime

Test Drive VictorOps today with your free trial

Thank You

Don't forget to **rate this session**
in the **.conf18** mobile app

.conf18

splunk>