## Customer Story 최고의 SPL 리뷰어가 되는 방법

삼성전자

온누리 책임 소프트웨어 엔지니어 이보영 소프트웨어 엔지니어 홍윤철 소프트웨어 엔지니어

**splunk** > turn data into doing<sup>\*\*</sup>



## How to Become The Best SPL Reviewer

#### Nuri On

Senior Software Engineer | Samsung Electronics

Boyoung Lee Software Engineer

Yuncheol Hong

Software Engineer Software Engineer | Samsung Electronics | Samsung Electronics







### Nuri On

Senior Software Engineer | Samsung Electronics

## **Boyoung Lee**

Software Engineer | Samsung Electronics

## **Yuncheol Hong**

Software Engineer Samsung Electronics

## Agenda

#### **1.** Background

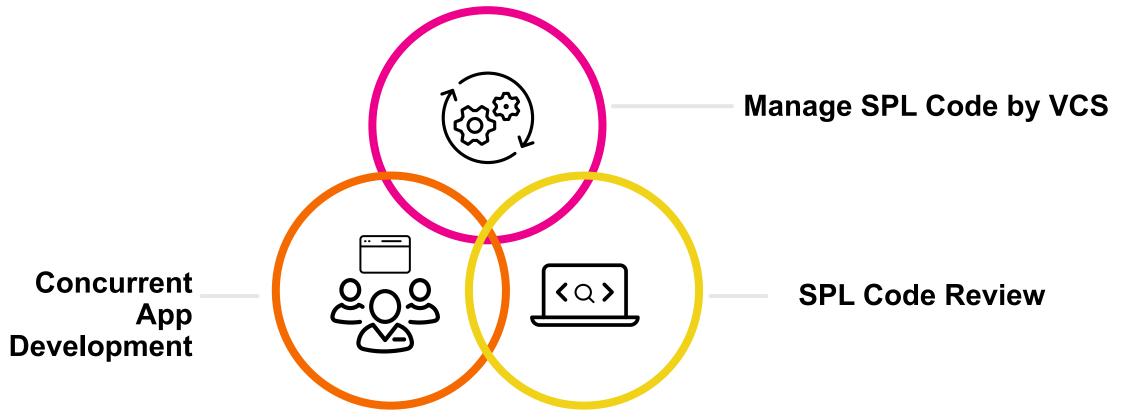
- **2.** Setup Code Review Environment
- **3.** How to Code Review for SPL
- **4.** Do Better SPL Code Review



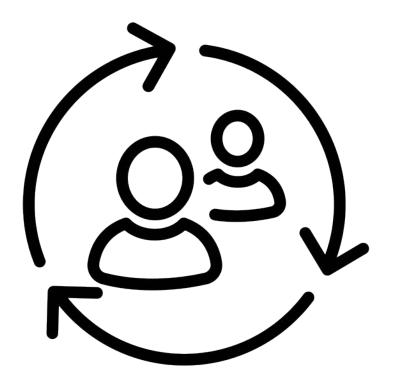


## 1. Background

The problem we want to solve is..







#### SPEAKER TRANSITION PLACEHOLDER

#### **Presenters:**

Use this slide to signal our video editors/production team that you will to transition from one speaker to the other, so they can cut the video between speakers. This slide will be cut from the final edit. Use the fields below to signal the from/to direction.

> From: To: Nuri On Yuncheol Hong

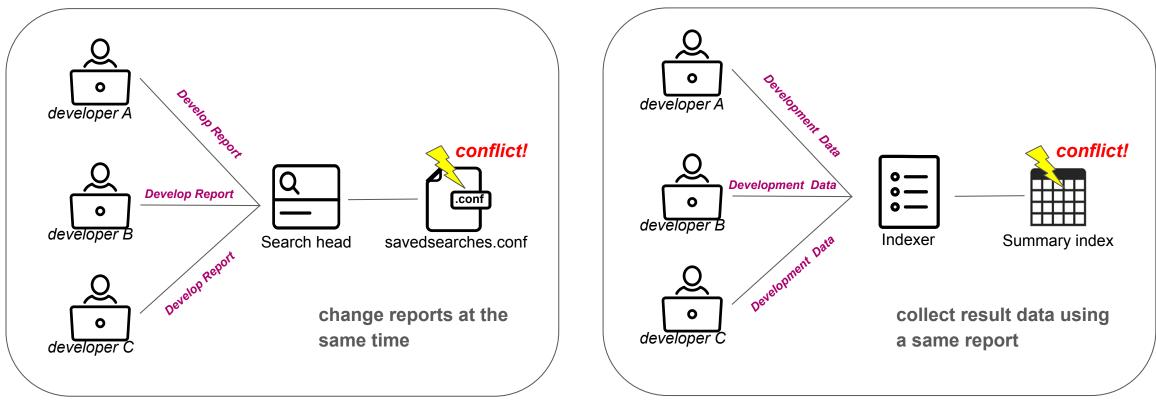






## 2. Setup Code Review Environment

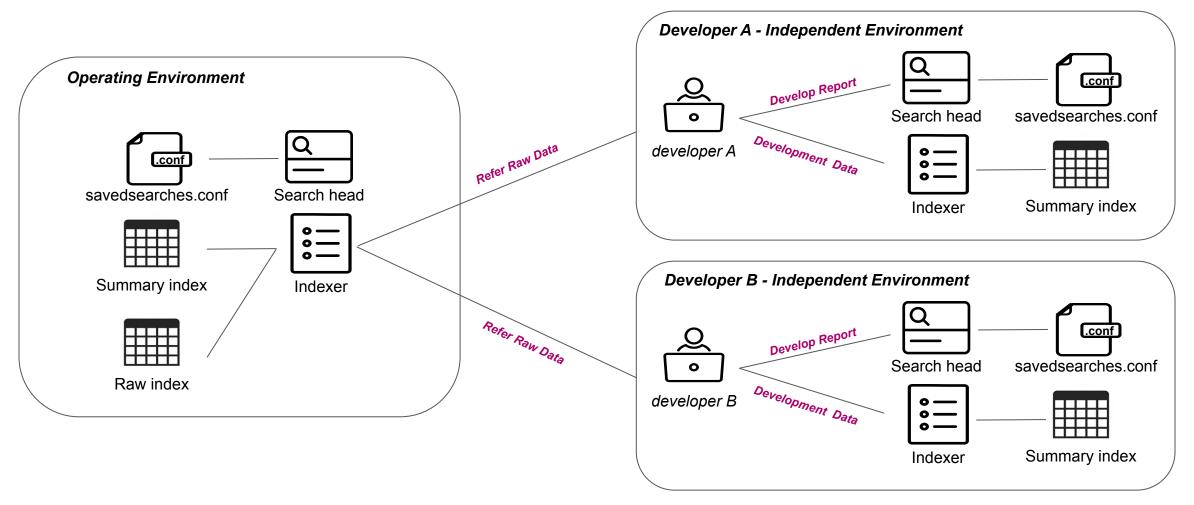
## **Two Difficulties about Splunk Development**



**Conflict - edit the report** 

**Conflict - collect using the report** 

## **Improved Development Environment**



## **Improved Development Environment**

## Developer Independent Environment

Users and Authentication

- > Access controls
- > Roles
- > Restrictions



- Access summary indexes in Developer env
- Access raw indexes in Operating env

## **Develop & Deploy**

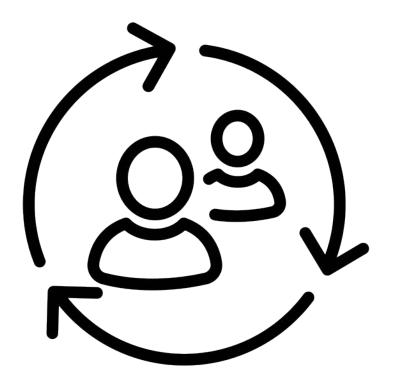
Developer Independent Environment

- Develop report (SPL Changes)
- Test to indexing summary data to indexes
- Make Commit And Push to VCS

**Operating Environment** 

- Pull from VCS dev/master branch
- Operate DEV/PROD environment





#### SPEAKER TRANSITION PLACEHOLDER

#### **Presenters:**

Use this slide to signal our video editors/production team that you will to transition from one speaker to the other, so they can cut the video between speakers. This slide will be cut from the final edit. Use the fields below to signal the from/to direction.

> From: To: Yuncheol Hong Boyoung Lee







## 3. How to Code Review for SPL

**splunk** > turn data into doing<sup>\*</sup>

#### Developers edit search (SPL) in their own Search Head $\rightarrow$ Let's do a Code Review

<b>plunk</b> >enterprise Apps <del>-</del>					<b>(2)</b> M	essages 🔻	Settings 🔻	Activity 🔻	Help 🔻	Find Q
Searches, Reports, and learches, reports, and alerts are saved		earch				×				
	pe: All 👻 App	Title Error	rs in the last 24 hours							10 per page 🔻
		Description opt	ional							
	Actions	Search 1	and a second back							
	Edit 🕶 Ru		error OR failed DR ( sour	cetype=access_* ( 404 <mark>OR</mark> 5	00))		nple			
	Edit 🔻 Ru	Earliest time -1d					nple			
	Edit 🔻 Ru		specifiers: y, mon, d, h, m, s <mark>Learn</mark>	More IZ			nple			
	Edit 🔻 Ru		ional specifiers: y, mon, d, h, m, s <mark>Learn</mark>	More 🛽			nple			
	Edit 🔻 Ru						nple			
	Edit 🕶 Ru				Cancel	Save	nple			
	Edit *	Federated Se	arch none	none	nobody	splunkapps	ample			
	Edit •									
	Edit 🔻									
	Edit 👻 Run 🗗									



splunk > turn data into doing

## **SPL Code Review**

git commit savedsearches.conf
 (Unsorted)
 ↓
 git push
 ↓
 pull request
 ↓
 diff savedsearches.conf
 (Difficult to Find Changes)

		•	local / savedsearches.conf	-		Before
$\langle \rangle$	Source	53	- [Errors in the last 24 hours]			
6	Commits	54 55	<ul> <li>dispatch.earliest_time = -1d</li> <li>search = error OR failed OR severe OR (</li> </ul>			
		55	sourcetype=access_* ( 404 OR 500 ) )			
و	Branches	56	-			
î۵	Pull requests	57 58	<pre>[stats with durable search] dispatch.indexed earliest = -10m</pre>	48 49	[stats with durable dispatch.indexed ea	
10	T di requesto	59	dispatch.indexed_latest = now	50	dispatch.indexed_la	
Q	Pipelines	+	@@ -63,3 +54,11 @@ search = index=_internal ep	s   sta	ats avg(eps) as avg, ma	x(eps) as max, min(eps)
•	Jira issues	↑ 63	_Indexing_Volume_in_MBs =	54	_Indexing_Volume_ir	n MBs =
			todaysBytesIndexed/1024/1024   timechart			/1024/1024   timechart
Φ	Security		<pre>avg(Daily_Indexing_Volume_in_MBs) by host</pre>			_Volume_in_MBs) by host
Đ	Downloads	64 65	<pre>dispatch.earliest_time = -7d search = index=_internal todaysBytesIndexed</pre>	55 56	dispatch.earliest_t search = index= int	time = -7d ternal todaysBytesIndex
-			LicenseManager-Audit NOT		LicenseManager-Aud	Contractor State
0	Repository settings		<pre>source=*web_service.log NOT</pre>		source=*web_service	-
			source=*web_access.log NOT source=*ui_access.log   eval Daily		source=*web_access.	and the second second
			Source= ur_access.log   eval bally	57	+	log   eval bally
				58	+ [Errors in the last	24 hours]
				59	+ dispatch.earliest_t	
	View side-by-	sid	е	60	+ search = error OR + sourcetype=access_*	
				61	+	( 404 01 500 ) )
				62	+ [Messages by minute	e last 3 hours]
				63	+ dispatch.earliest_t	time = -3h

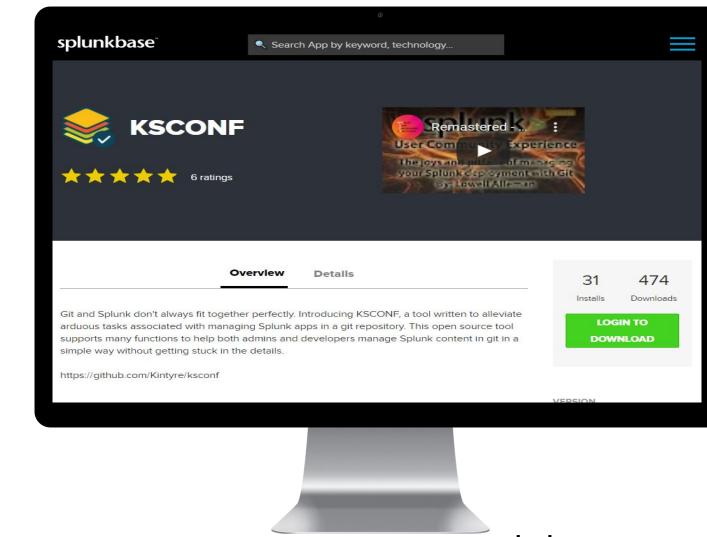
git commit savedsearches.conf
 (Unsorted)
 ↓
 git push
 ↓
 pull request
 ↓
 diff savedsearches.conf
 (Difficult to Find Changes)

		<b>*</b>	Iocal / savedsearches.conf	47		Before
$\langle \rangle$	Source	53	- [Errors in the last 24 hours]			
\$	Commits	54 55	<ul> <li>dispatch.earliest_time = -1d</li> <li>search = error OR failed OR severe OR (</li> </ul>			
		55	sourcetype=access_* ( 404 OR 500 ) )			
و	Branches		-			
ຳລ	Pull requests	57 58	[stats with durable search] dispatch.indexed_earliest = -10m	48 49	[stats with durable dispatch.indexed ear	
10	Turrequests	59	dispatch.indexed_latest = now	50	dispatch.indexed_la	
¢	Pipelines	*	@@ -63,3 +54,11 @@ search = index=_internal ep	s   sta	ts avg(eps) as avg, max	(eps) as max, min(eps)
•	Jira issues	↑ 63	_Indexing_Volume_in_MBs =	54	_Indexing_Volume_in	MBs =
			todaysBytesIndexed/1024/1024   timechart			.024/1024   timechart
Φ	Security		<pre>avg(Daily_Indexing_Volume_in_MBs) by host</pre>			/olume_in_MBs) by host
Fi	Downloads	64 65	<pre>dispatch.earliest_time = -7d search = index=_internal todaysBytesIndexed</pre>	55 56	dispatch.earliest_t:	.me = -7d ernal todaysBytesIndexe
		05	LicenseManager-Audit NOT	50	LicenseManager-Audi	a contract of the second se
0	Repository settings		<pre>source=*web_service.log NOT</pre>		source=*web_service	-
			source=*web_access.log NOT		source=*web_access.	The second second
			source=*ui_access.log   eval Daily	57	<pre>source=*ui_access.lo +</pre>	og   eval Daily
				58	+ [Errors in the last	24 hours]
				59	+ dispatch.earliest_t:	.me = -1d
	View side-by-s	side	6	60	+ search = error OR fa	
	·····			61	sourcetype=access_*	(404 OR 500 ))
				62	+ [Messages by minute	last 3 hours]
				63	+ dispatch.earliest_t:	.me = -3h



## **KSCONF** App

App Overview





## **KSCONF** App

git pre-commit hooks (sort)

## ★ KSConf latest Search docs CONTENTS Introduction Concepts

Installation Guide

Commands

Cheat Sheet Contributing

Developer setup Git tips & tricks

Pre-commit hooks

you repo

Git tricks

Random

Contact

Hooks provided by ksconf

Git configuration tweaks

Configuring pre-commit hooks in

Should my version of ksconf and

pre-commit plugins be the same?

#### **Git tips & tricks**

These tips & tricks are based on prior Splunk, git, and ksconf experience. None of this content is an endorsement of a particular approach or tool. Read the docs, and take responsibility. As always, your millage may vary.

#### **Pre-commit hooks**

Ksconf is setup to work as a pre-commit plugin. To use ksconf in this manner, simply configure the ksconf repo in your pre-commit configuration file. If you haven't done any of this before, it's not difficult to setup but is beyond the scope of this guide. We suggest that you read the pre-commit docs and review this section when you are ready to setup the hooks.

#### Hooks provided by ksconf

Three hooks are currently defined by the ksconf repository:

#### ksconf-check

Runs ksconf check to perform basic validation tests against all files in your repo that end with .conf or .meta. Any errors will be reported by the UI at commit time and you'll be able to correct mistakes before bogus files are committed into your repo. If you're not sure why you'd need this, check out Why validate my conf files?

#### ksconf-sort

Runs ksconf sort to normalize any of your .conf or .meta files which will make diffs more readable and merging more predictable. As with any hook, you can customize the filename





#### pre-commit hook

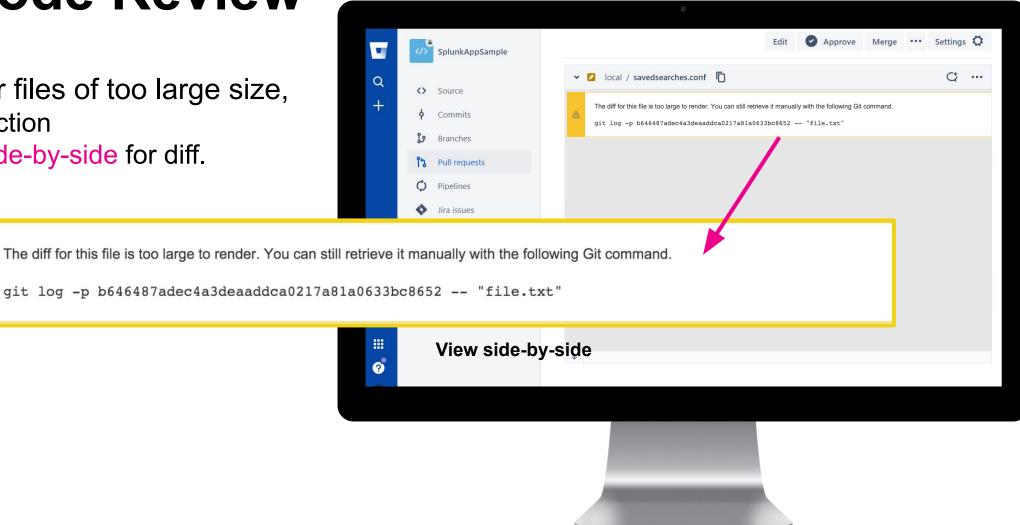


	SplunkAppSample		E	dit	After (Case A)
		~	local / savedsearches.conf		After (Case A)
$\diamond$	Source	$\uparrow$	@@ -15,7 +15,7 @@		
¢	Commits	15	<pre># modify the values by following the spec outlined in savedsearches.conf.spec.</pre>	15	<pre># modify the values by following the spec outlined in savedsearches.conf.spec.</pre>
ទ្រ	Branches	16 17	[Errors in the last hour]	16 17	[Errors in the last hour]
ใว	Pull requests	18	<pre>- search = error OR failed OR severe OR (    sourcetype=access_* ( 404 OR 500 OR 503 ) )</pre>	18	<pre>+ search = error OR failed OR (     sourcetype=access_* ( 404 OR 500 OR 503 )</pre>
Ø	Pipelines	19 20	<pre>dispatch.earliest_time = -2h</pre>	19 20	<pre>dispatch.earliest_time = -2h</pre>
•	Jira issues	21 ↓	[KB indexed per hour last 24 hours]	21	[KB indexed per hour last 24 hours]
•		$\uparrow$	@@ -24,7 +24,7 @@ search = index=_internal metr	ics gr	<pre>roup=per_index_thruput NOT debug NOT sourcetyp</pre>
Ψ	Security	24	dispatch.earliest_time = -1d	24	dispatch.earliest_time = -1d
Đ	Downloads	25 26	[Messages by minute last 3 hours]	25 26	[Messages by minute last 3 hours]
0	Repository settings	27	<pre>- search = index=_internal eps "group=per_source_thruput" NOT filetracker   eval events=eps*kb/kbps   timechart fixedrange=t span=1m s</pre>	27	<pre>+ search = index=_internal eps "group=per_source_thruput"   eval events=eps*kb/kbps   timechart fixedrange= span=1m s</pre>
		28 29	um(events) by series dispatch.earliest time = -3h	28	um(events) by series
	View side-by			29 30	dispatch.earliest_time = -3h

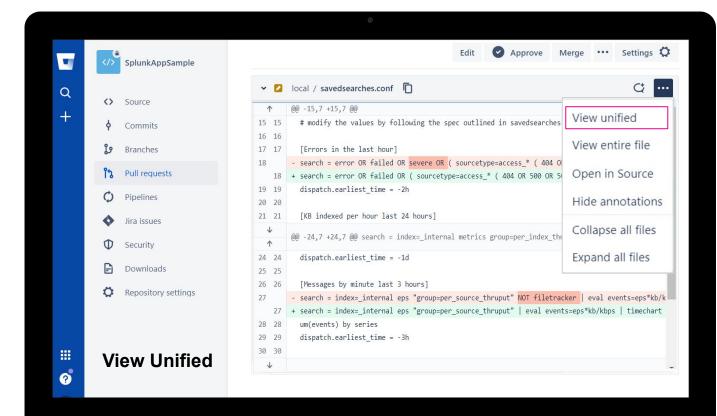
splunk > turn data into doing

## **SPL Code Review**

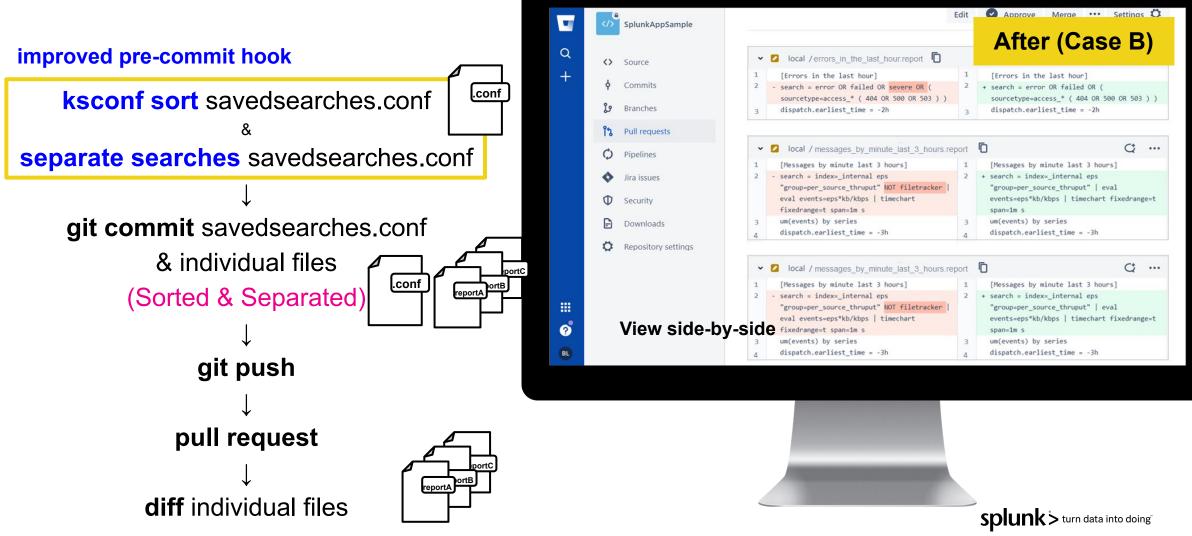
However, for files of too large size, there is restriction on viewing side-by-side for diff.



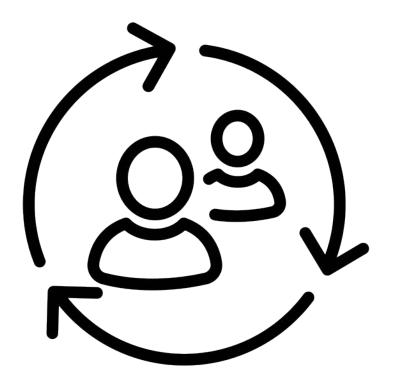
**Unified diffs** are suitable for reviewing small changes, so for large file context can leave out important information.







Cas	0	side-by-side dif	f	unified diff				
Cas		small .conf file	large .conf file	small .conf file	large .conf file			
-	Default	x	Х	Х	Х			
Α	ksconf sort (pre-commit hook)	Good	Х	Good	Good			
в	separate searches (improved pre-commit hook)	Best	Best	Good	Good			



#### SPEAKER TRANSITION PLACEHOLDER

#### **Presenters:**

Use this slide to signal our video editors/production team that you will to transition from one speaker to the other, so they can cut the video between speakers. This slide will be cut from the final edit. Use the fields below to signal the from/to direction.

From: Boyoung Lee
To: Nuri On



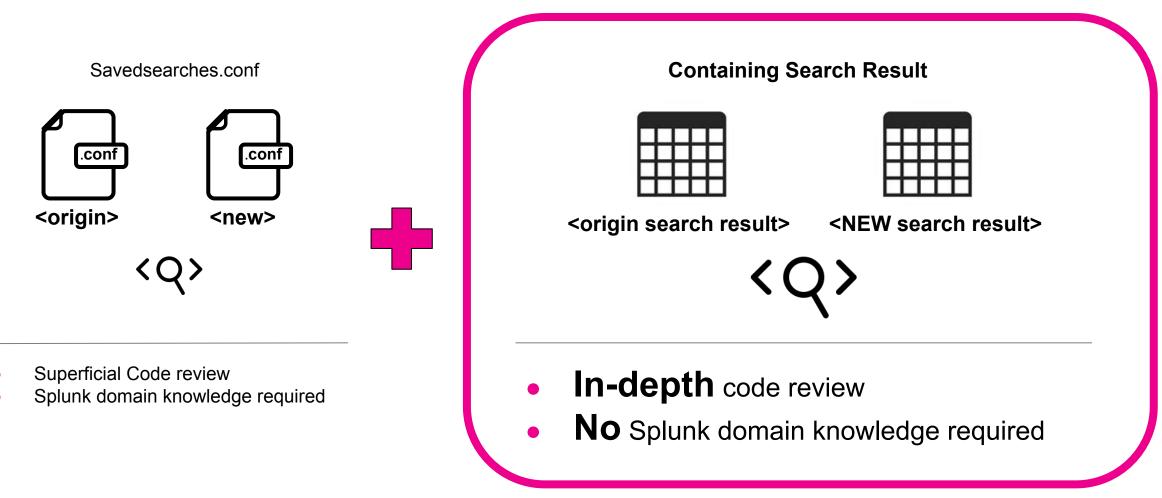


# $\swarrow$ ( 2027

## 4. Do Better SPL Code Review

**splunk** > turn data into doing<sup>\*</sup>

## Let's do better SPL code review



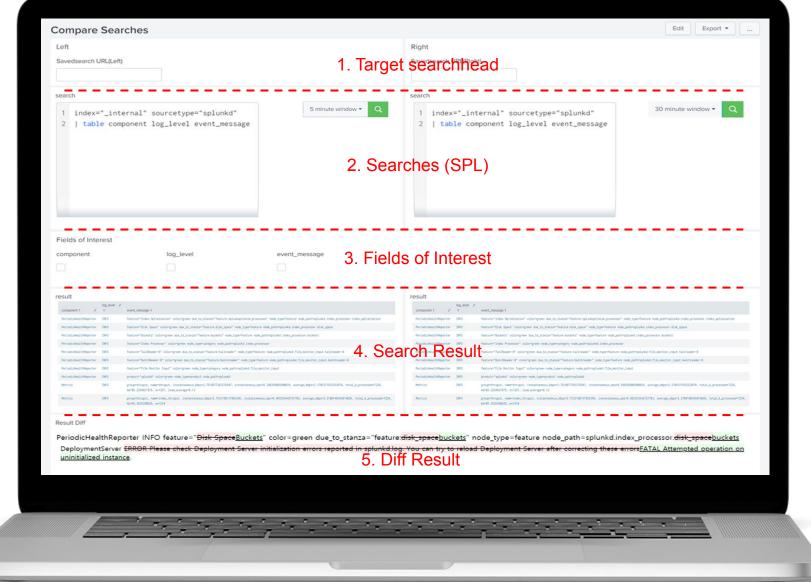
## Our new 'compare search app'

#### 

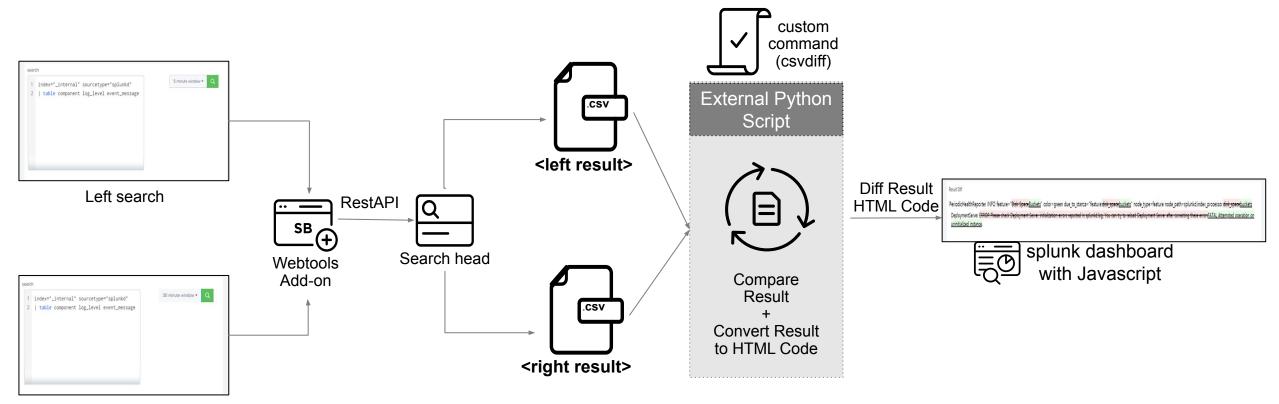
1. Enter each searchhead's server info on both sides.

- 2. Enter searches on both sides
- 3. Filter on fields to compare
- 4. Compare Results with table

5. Visualize Search Diff (Use diff-match-patch python lib)

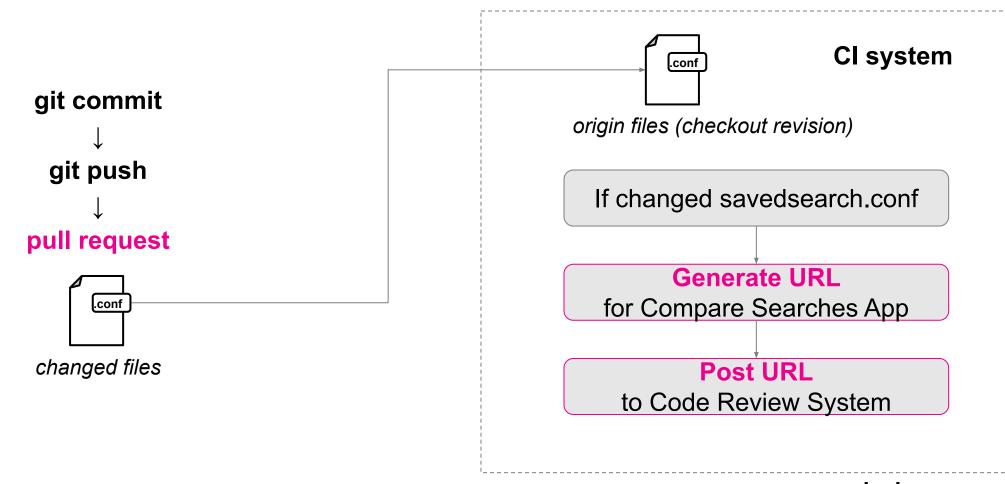


## How to Make Compare Search App



Right search

## **Compare Search App in CI Environment**



## Compare Search App in CI environment

enki	ins •	<b></b>	<b></b>	0			5	2 1	Buik	
4m 23s	start	check changed report	make compare URL	comp sear		end				
	### [m - Print Message ktraceinfo - Shell Script									
No	Changed Rep	ort			Comp	are S	earc	h L	ink	
1	alert_savedsea	alert_savedsearch1				<۵>				
2	alert_savedsea	arch2			<۵>					
3	report_saveds	earch1				<	Q۶			
4	report_saveds	earch2				<	Q>			



## **SPL Code Review Benefits**



SPL Development Skill 🔺

Reliability & Availability

Performance & Maintainability



## **SPL Code Review Benefits**



SPL Development Skill 🔺

Reliability & Availability

Performance & Maintainability



# Thank You



## Resources

- Splunk base ksconf : <u>https://splunkbase.splunk.com/app/4383/</u>
- Configuring ksconf pre-commit hook : <u>https://ksconf.readthedocs.io/en/latest/git.html#</u>
  - Splunk Docs : <u>https://docs.splunk.com/Documentation/Splunk/8.2.1</u>/
- Bitbucket : <u>https://support.atlassian.com/bitbucket-cloud/</u>
- Splunk base Webtools Add-on: <u>https://splunkbase.splunk.com/app/4146/</u>



