

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing 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. ©2021 Splunk, Inc. All rights reserved.

How To Become the Best SPL Reviewer

DEV1132B

Nuri On

Senior Software Engineer | Samsung Electronics

Boyoung Lee

Software Engineer | Samsung Electronics

Yuncheol Hong

Software Engineer | Samsung Electronics

splunk> **.conf21**





**Nuri
On**

Senior Software Engineer |
Samsung Electronics



**Boyoung
Lee**

Software Engineer |
Samsung Electronics



**Yuncheol
Hong**

Software Engineer |
Samsung Electronics

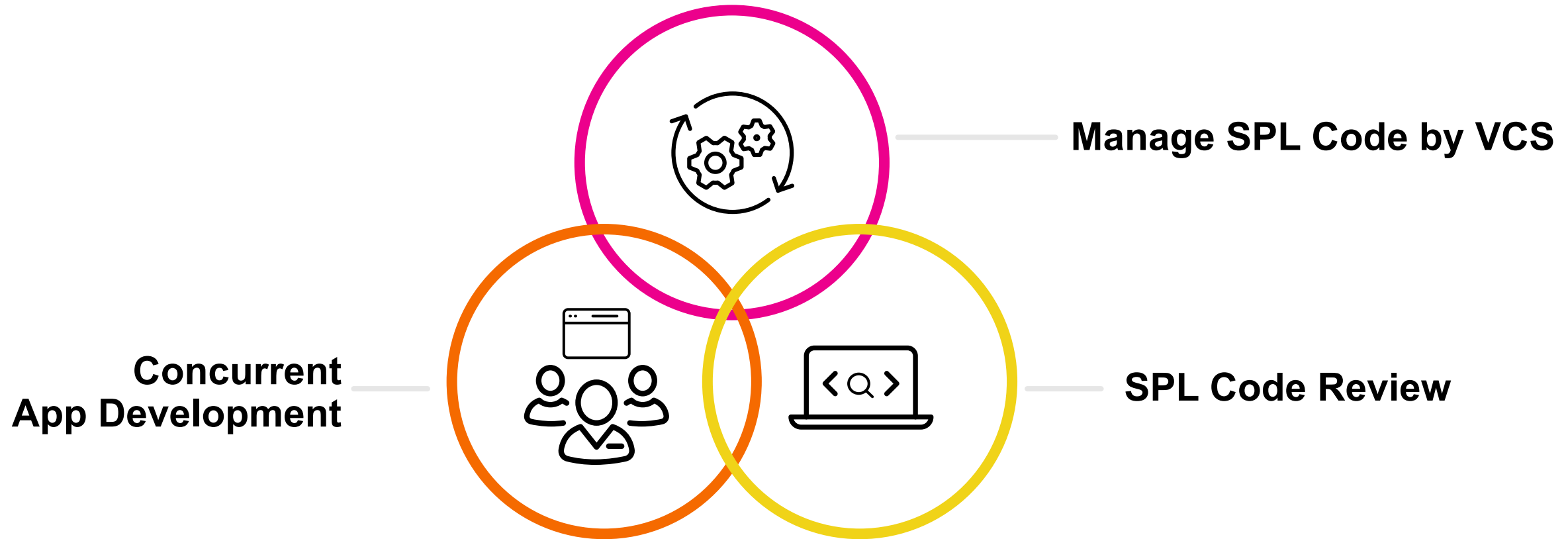
Agenda

- 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..



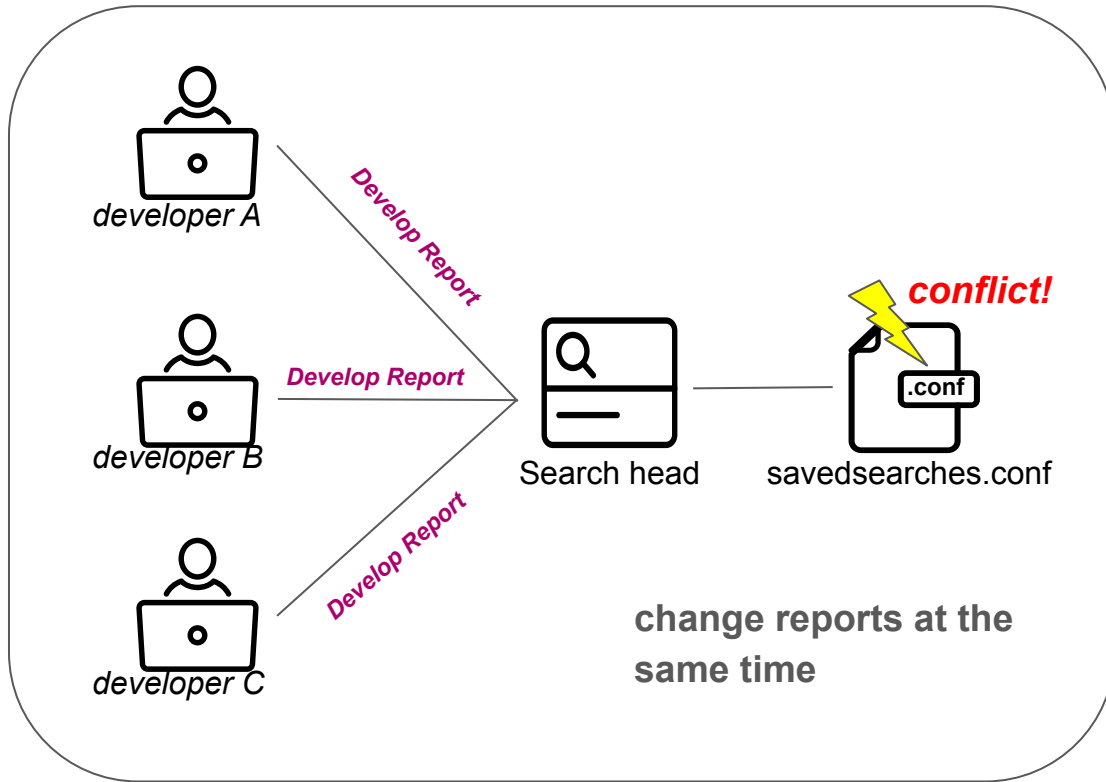


2) Setup Code Review Environment

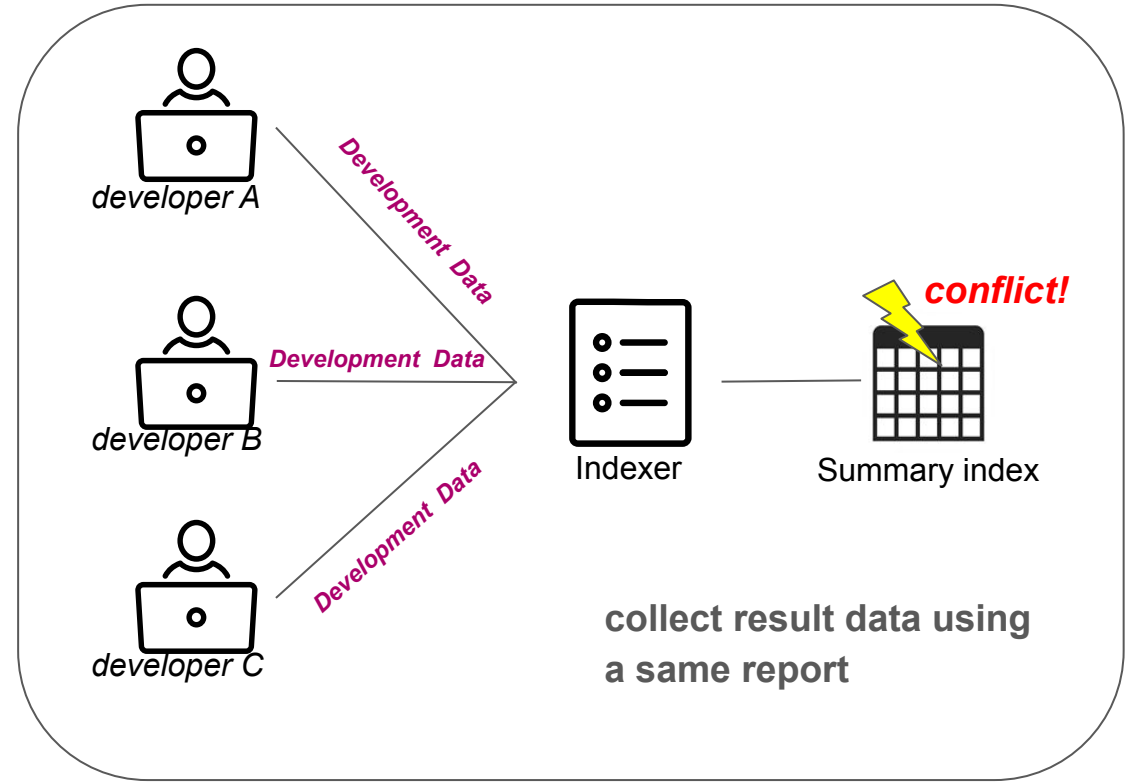
splunk>

.conf21

Two Difficulties about Splunk Development

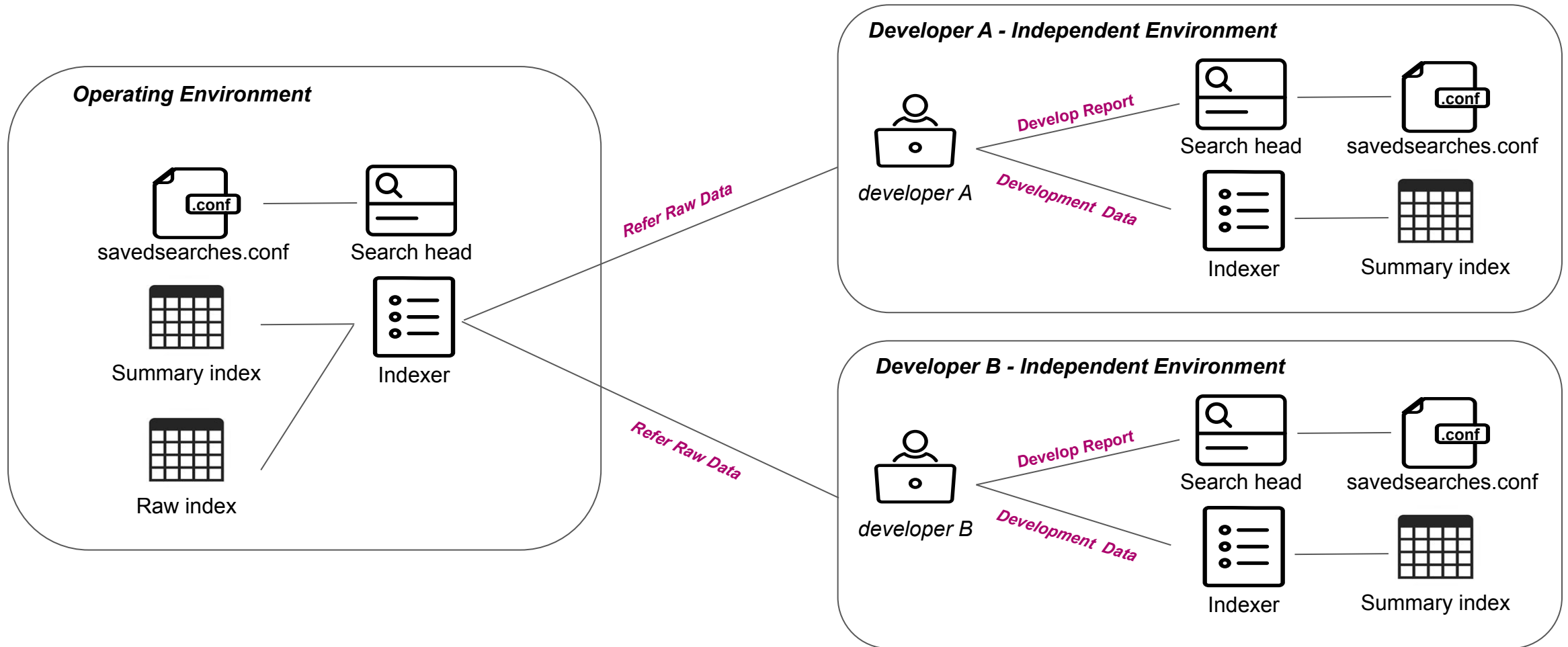


Conflict - edit the report



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



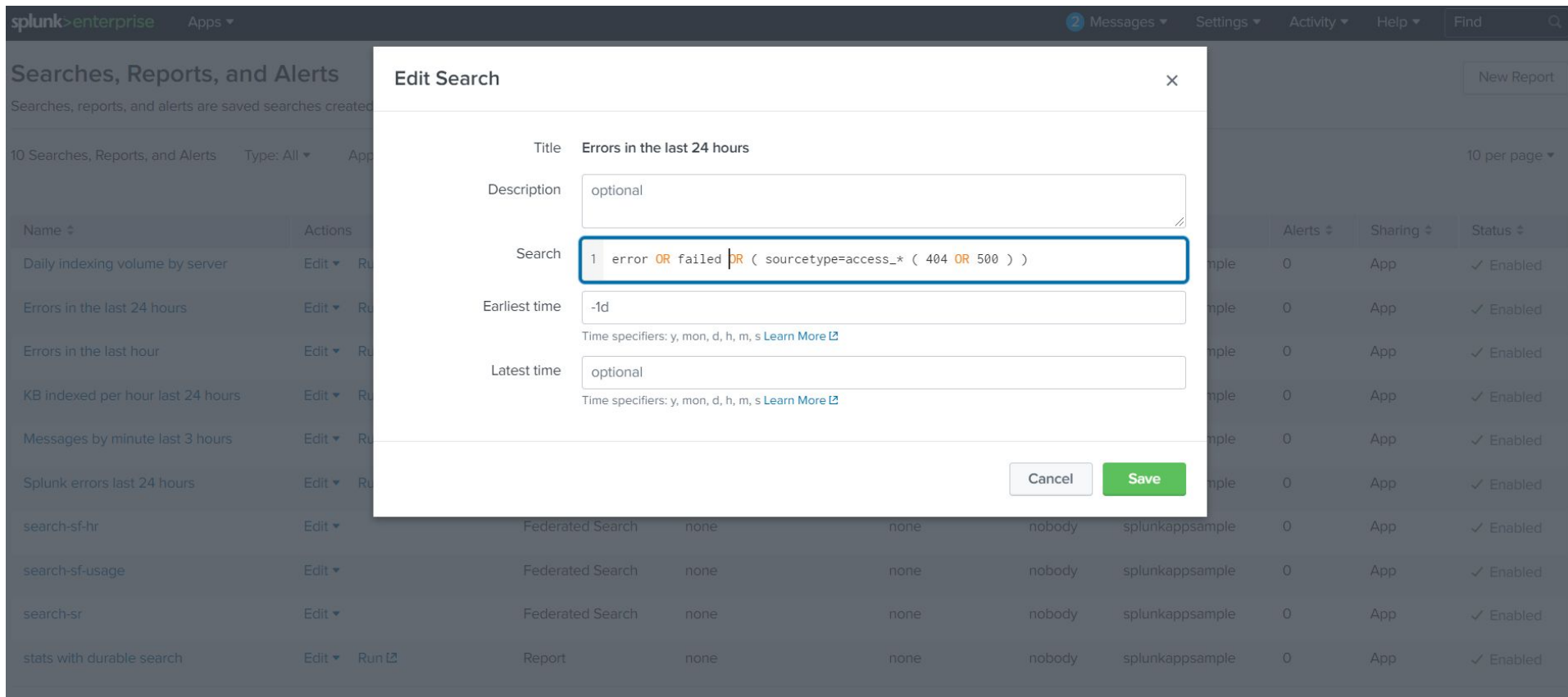
3) How to Code Review for SPL

splunk>

.conf21

SPL Code Review

Developers edit search (SPL) in their own Search Head → **Let's do a Code Review**

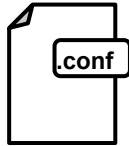


The screenshot displays the Splunk 'Edit Search' dialog box. The search query is: `1 error OR failed OR (sourcetype=access_* (404 OR 500))`. The dialog includes fields for Title, Description, Earliest time, and Latest time. The background shows a list of searches and reports.

Name	Actions
Daily indexing volume by server	Edit Run
Errors in the last 24 hours	Edit Run
Errors in the last hour	Edit Run
KB indexed per hour last 24 hours	Edit Run
Messages by minute last 3 hours	Edit Run
Splunk errors last 24 hours	Edit Run
search-sf-hr	Edit Run
search-sf-usage	Edit Run
search-sr	Edit Run
stats with durable search	Edit Run

SPL Code Review

git commit savedsearches.conf



(Unsorted)



git push

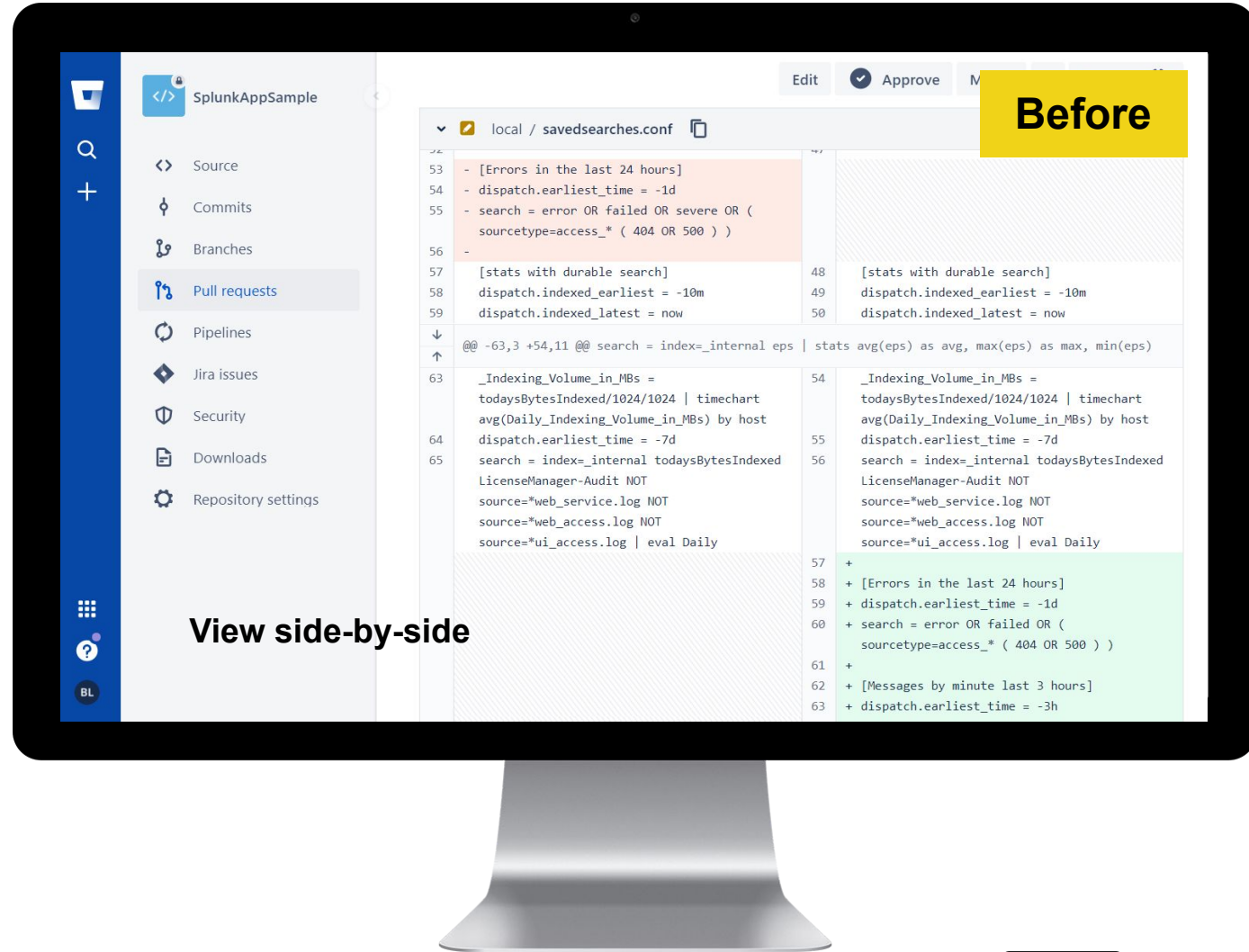
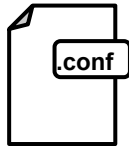


pull request

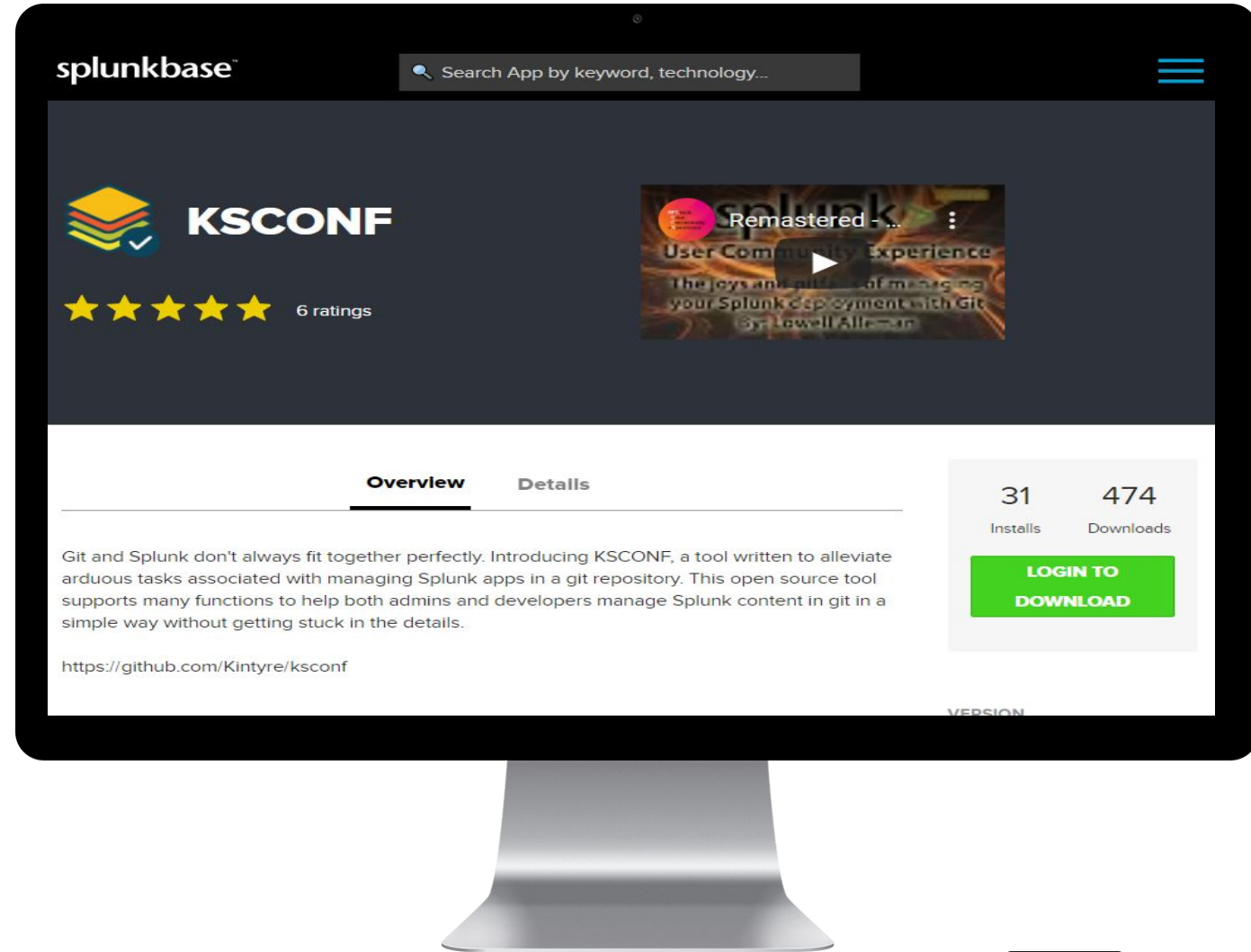


diff savedsearches.conf

(Difficult to Find Changes)



KSCONF App



App Overview

KSCONF App

git pre-commit hooks (sort)



SPL Code Review

pre-commit hook

`ksconf sort savedsearches.conf`

`git commit savedsearches.conf`

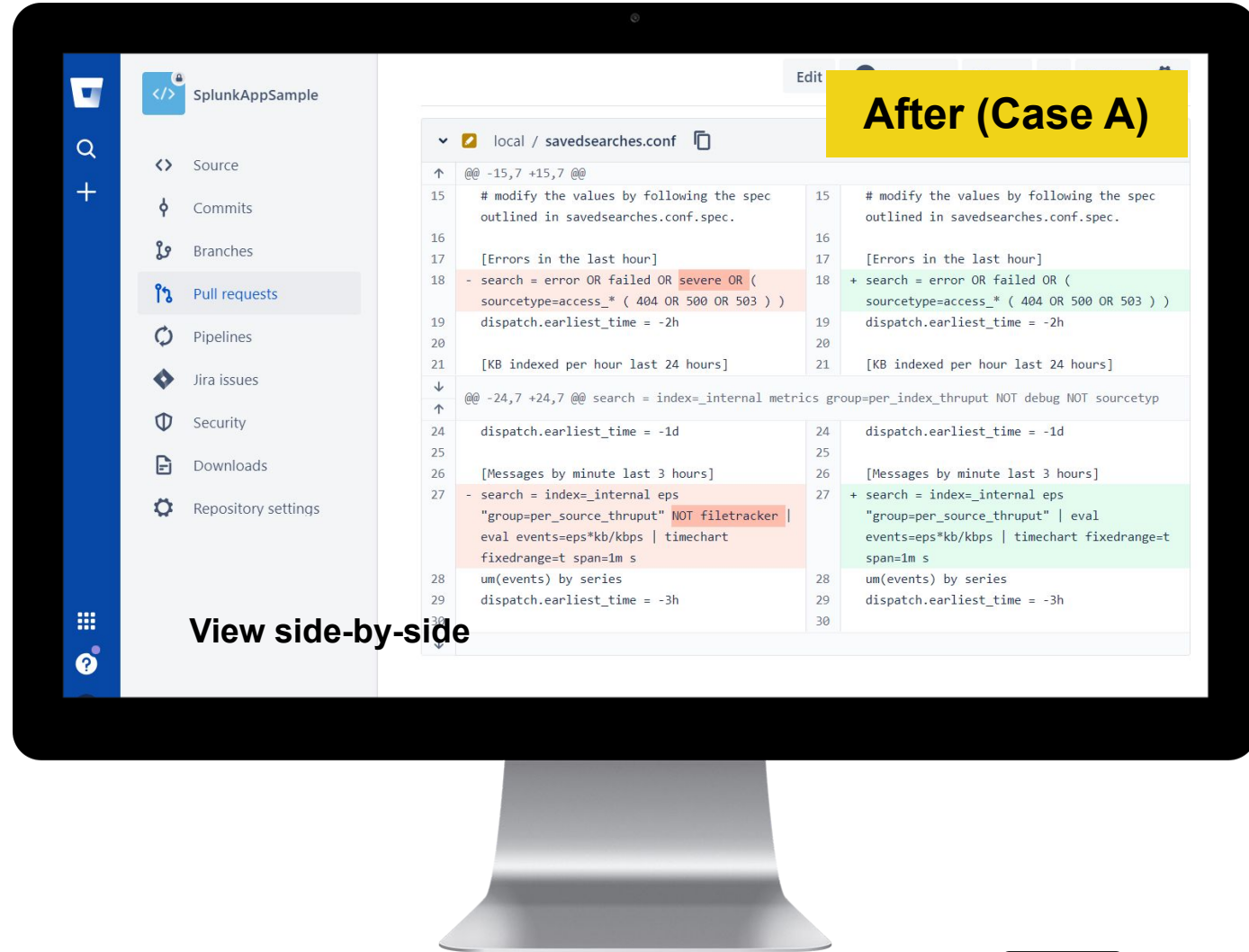
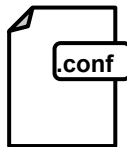
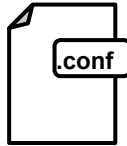
(Sorted)

`git push`

pull request

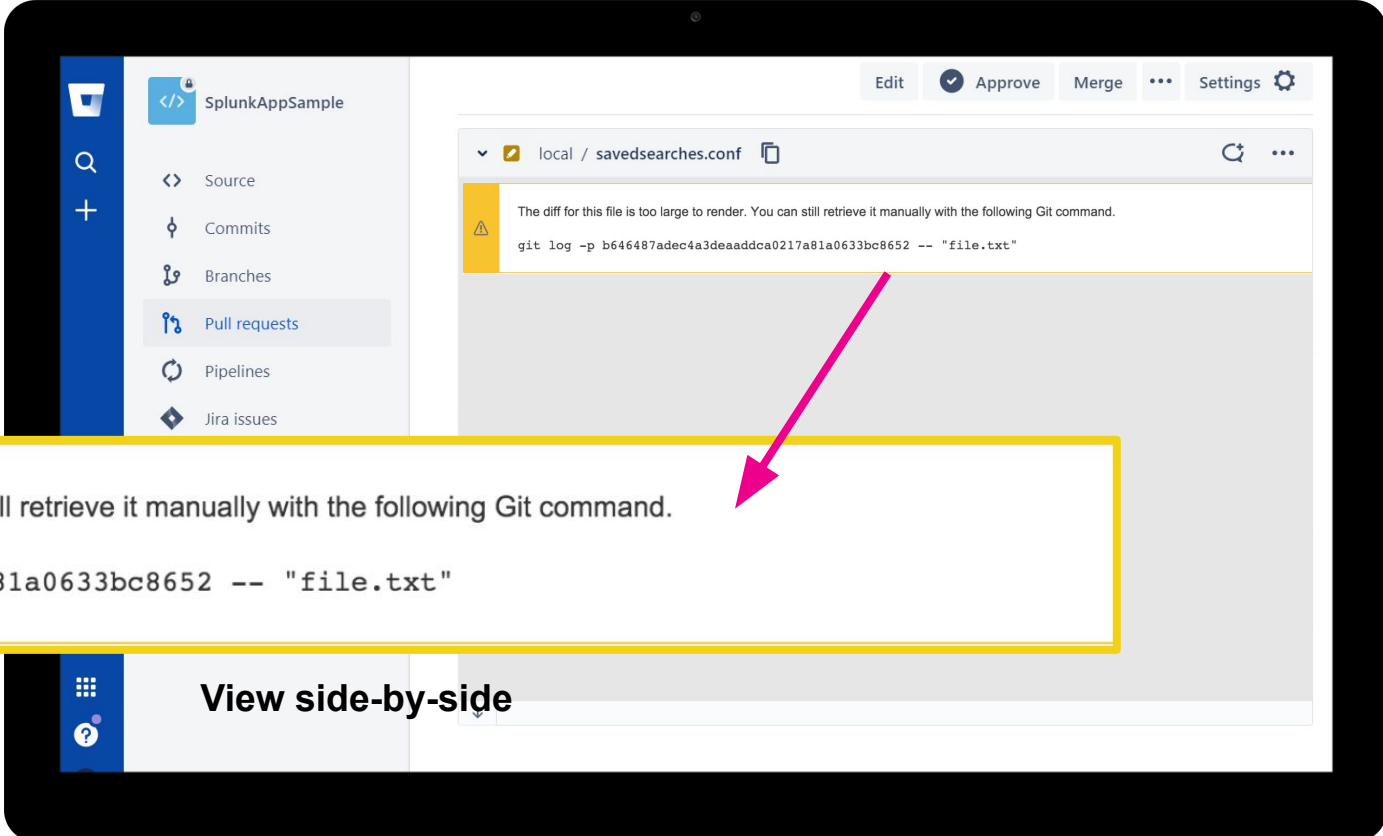
`diff savedsearches.conf`

(Easy to Code Review)



SPL Code Review

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



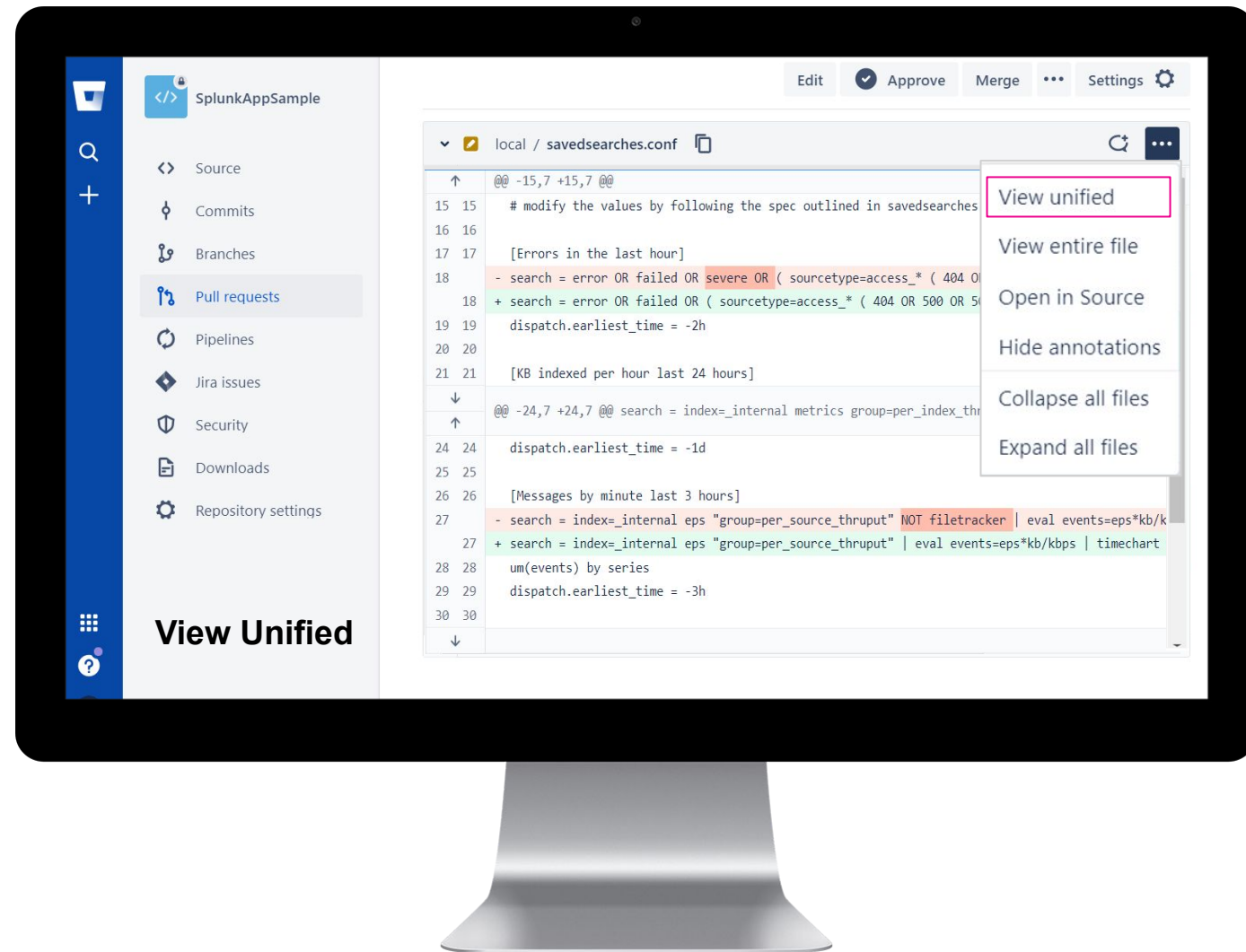
The diff for this file is too large to render. You can still retrieve it manually with the following Git command.

```
git log -p b646487adec4a3deaaddca0217a81a0633bc8652 -- "file.txt"
```

View side-by-side

SPL Code Review

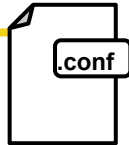
Unified diffs are suitable for reviewing small changes, so for large file context can leave out important information.



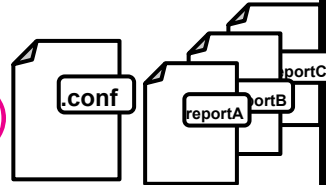
SPL Code Review

improved pre-commit hook

ksconf sort savedsearches.conf
&
separate searches savedsearches.conf



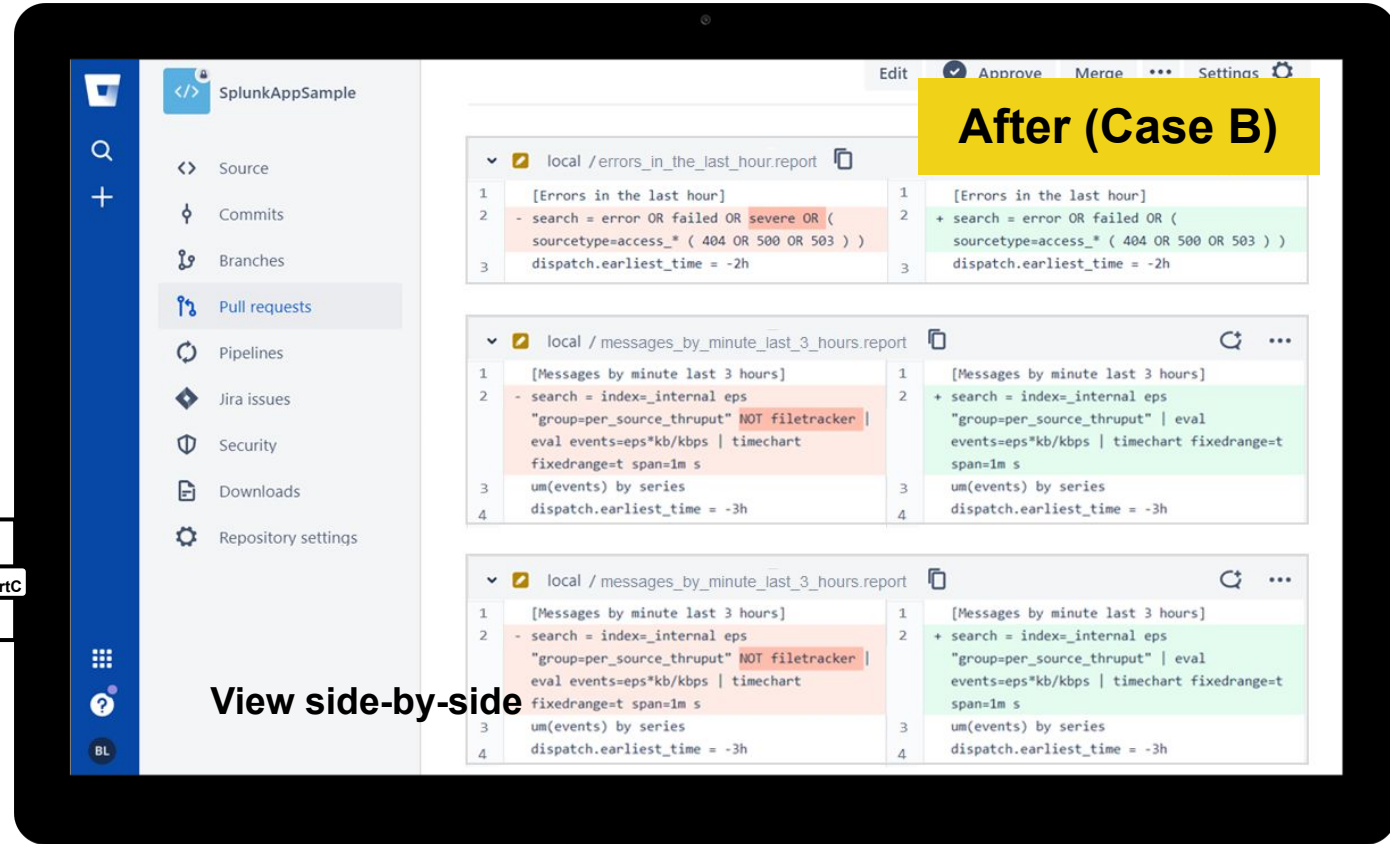
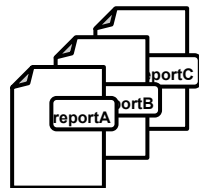
git commit savedsearches.conf
& individual files
(Sorted & Separated)



git push

pull request

diff individual files



View side-by-side

SPL Code Review

Case	side-by-side diff		unified diff	
	small .conf file	large .conf file	small .conf file	large .conf file
- Default	X	X	X	X
A ksconf sort (pre-commit hook)	Good	X	Good	Good
B separate searches (improved pre-commit hook)	Best	Best	Good	Good



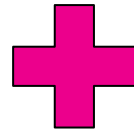
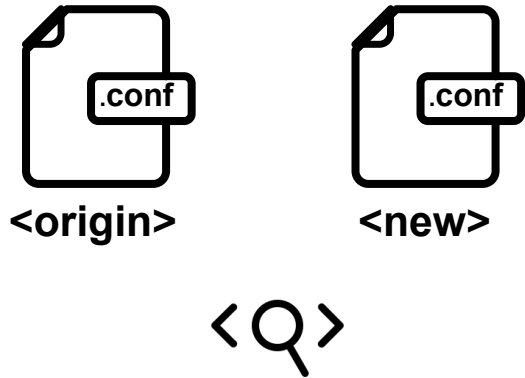
4) Do Better SPL Code Review

splunk>

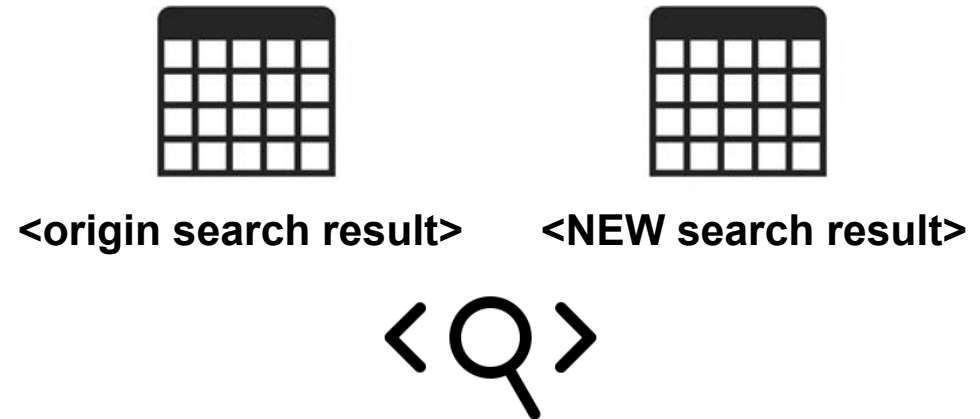
.conf21

Let's do better SPL code review

Savedsearches.conf



Containing Search Result



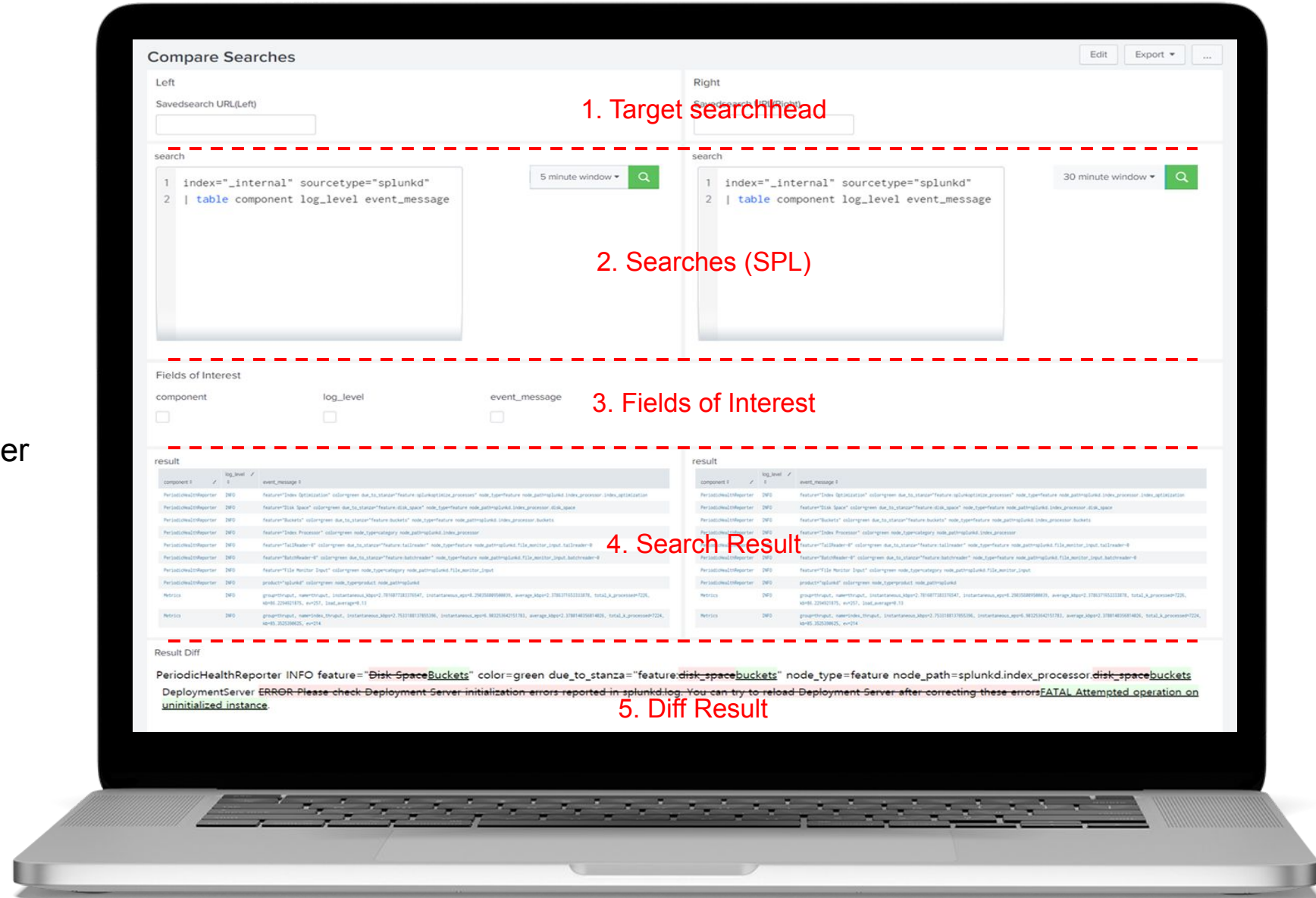
- Superficial Code review
- Splunk domain knowledge required

- **In-depth** code review
- **No** Splunk domain knowledge required

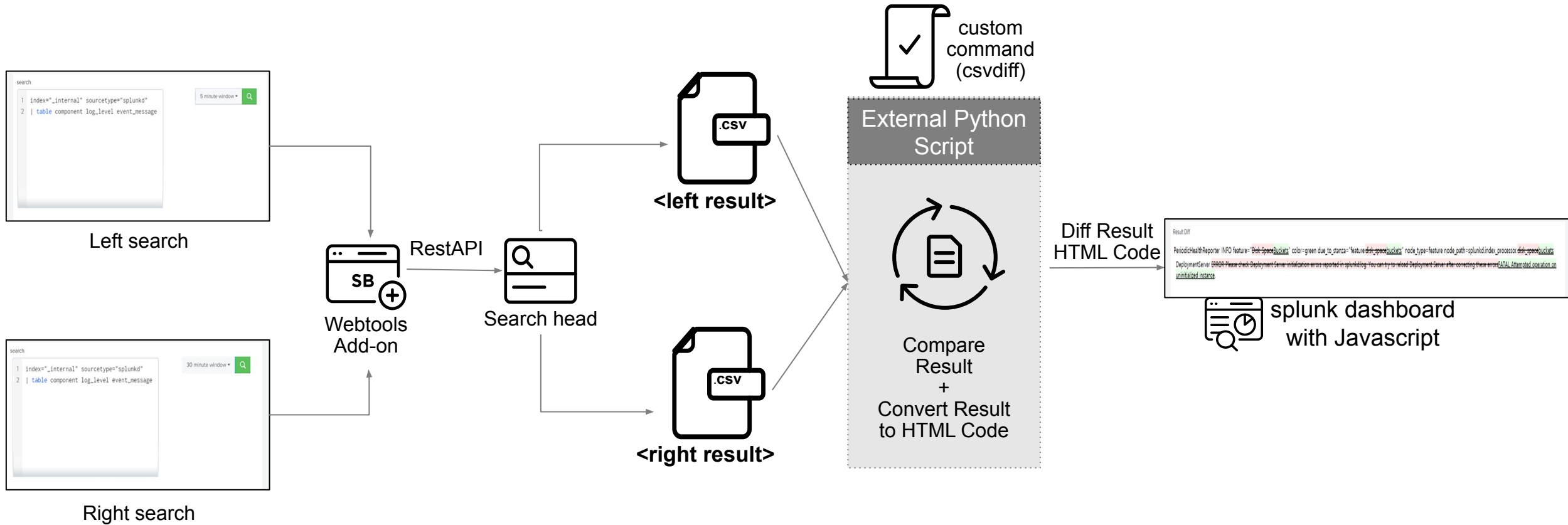
Our new 'compare search app'



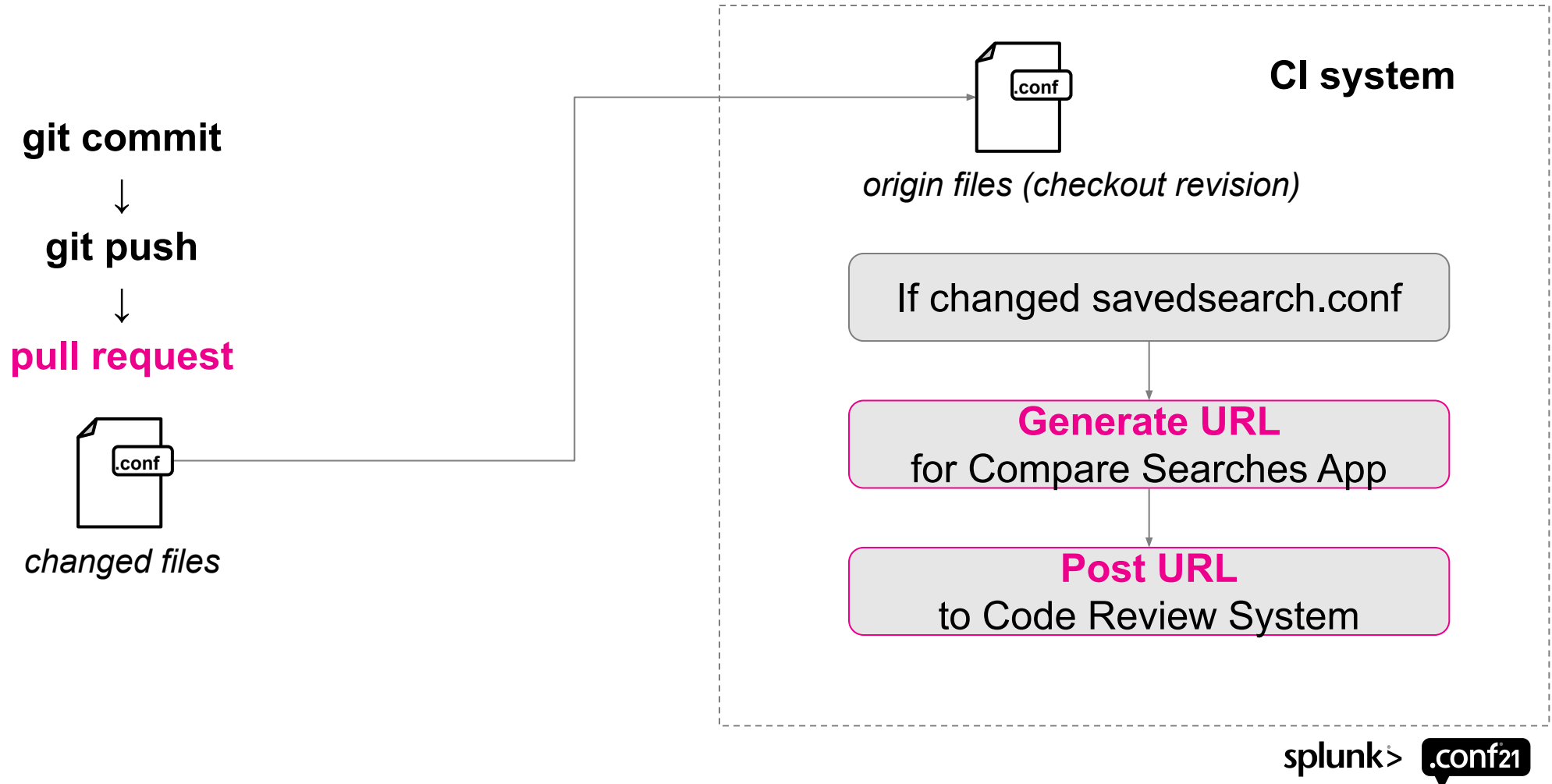
- 1) Enter each searchhead's server info on both sides.
 - 2) Enter searches on both sides
 - 3) Filter on fields to compare
 - 4) Compare Results with table
 - 5) Visualize Search Diff
- (Use diff-match-patch python lib)



How to Make Compare Search App



Compare Search App in CI Environment



Compare Search App in CI environment

The screenshot shows a Jenkins pipeline for 'SplunkAppSample'. The pipeline consists of five stages: 'start', 'check changed report', 'make compare URL', 'compare search', and 'end'. The 'check changed report' and 'make compare URL' stages are marked with green checkmarks, indicating they passed. The 'compare search' stage is marked with a blue refresh icon, indicating it is currently running. The 'end' stage is marked with a grey circle, indicating it has not yet started. The pipeline is currently in a 'Build' state, as indicated by the '1 Build' badge in the top right corner.

Below the pipeline, the console output shows the following commands:

```
[35m ### Stage Test ### [m - Print Message
./gradlew test --stacktrace --info - Shell Script
```

The console output also shows a table with the following data:

No	Changed Report	Compare Search Link
1	alert_savedsearch1	<Q>
2	alert_savedsearch2	<Q>
3	report_savedsearch1	<Q>
4	report_savedsearch2	<Q>

SPL Code Review Benefits

Education



SPL Development Skill ▲

Prevent Defect



Reliability & Availability ▲

Optimization



Performance & Maintainability ▲

Resources

- Splunk base - ksconf :
<https://splunkbase.splunk.com/app/4383/>
- Configuring ksconf pre-commit hook :
<https://ksconf.readthedocs.io/en/latest/git.html#>
- Splunk Docs :
<https://docs.splunk.com/Documentation/Splunk/8.2/.1/>
- Bitbucket :
<https://support.atlassian.com/bitbucket-cloud/>
- Splunk base - Webtools Add-on:
<https://splunkbase.splunk.com/app/4146/>

