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, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf22

Automate Log Onboarding with Splunk!

PLA1107B

Steve Koelpin
Advisor | TransUnion

Konrad Biegaj
Lead Engineer | TransUnion

Steve Koelpin

Advisor | TransUnion

Konrad Biegaj

Lead Engineer | TransUnion

The 4 Types of Work

1. Business Projects (i.e. External Work, Planned Work)
2. Updates, Upgrades, and Changes
3. Unplanned Work (i.e. Drive-by's, Rework, Tech Bridges)
4. Internal IT Projects

Increase Efficiency of Your Engineers

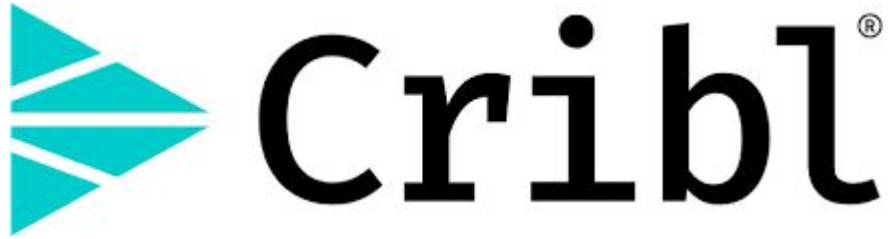
25% of our overall engineering work is log onboardings

FEATURE DELIVERED IN RELEASE : PI8

Formatted ID	Name	Preliminary Estimate	Preliminary Estimate Value	Leaf Story Plan Estimate Total	Accepted Leaf Story Count	Project	State
	Cloud Foundational - Log Onboarding - Logging (PI 8)	F-M	32	23	9	Cloud - Foundational Capabilities	Done/GA
	Identify any improvements to support the scaling with Log Onboarding process to application teams	F-S	16	35	6	Cloud - Foundational Capabilities	Done/GA
	Splunk integration with IAM and Address service in EC2	F-XXS	5	5	2	Cloud - Foundational Capabilities	Done/GA
	Cloud Ops : [Logging] - Install Cribl Infrastructure in CloudZ - Dev	F-M	32	5	2	Cloud - Foundational Capabilities	Done/GA
	Cloud Ops Logging - BAU & Security Remediation - PI8	F-S	16	61	36	Cloud - Foundational Capabilities	Done/GA
	BAU Splunk LogOnBoarding- handle areas already onboarded in DEV plus any new logs from these areas	F-XS	8	10	4	Cloud Ops - Logging	Done/GA
	Splunk Intake - On Prem Log Onboarding - PI8	F-L	60	30	15	Cloud Ops - Logging	Done/GA
	Splunk Intake - On Prem Application Installation Requests	F-XS	8	6	5	Cloud Ops - Logging	Done/GA
	Splunk BAU - Remedy tickets, WOs - PI8	F-S	16	55	20	Cloud Ops - Logging	Done/GA
	UK Operationalize new Splunk servers	F-S	16	4	3	Cloud Ops - Logging	Done/GA
	Splunk Enhancements/Upgrades	F-L	60	21	6	Cloud Ops - Logging	Done/GA

What can you do with a ~25% increase in engineering capacity?

Mission Critical Components



The Evolution of Log Onboardings

Crawl

1. Manually SSH into the box
2. Updating inputs.conf in /opt/splunkforwarder/etc/system/local
3. Restarting Splunk service manually

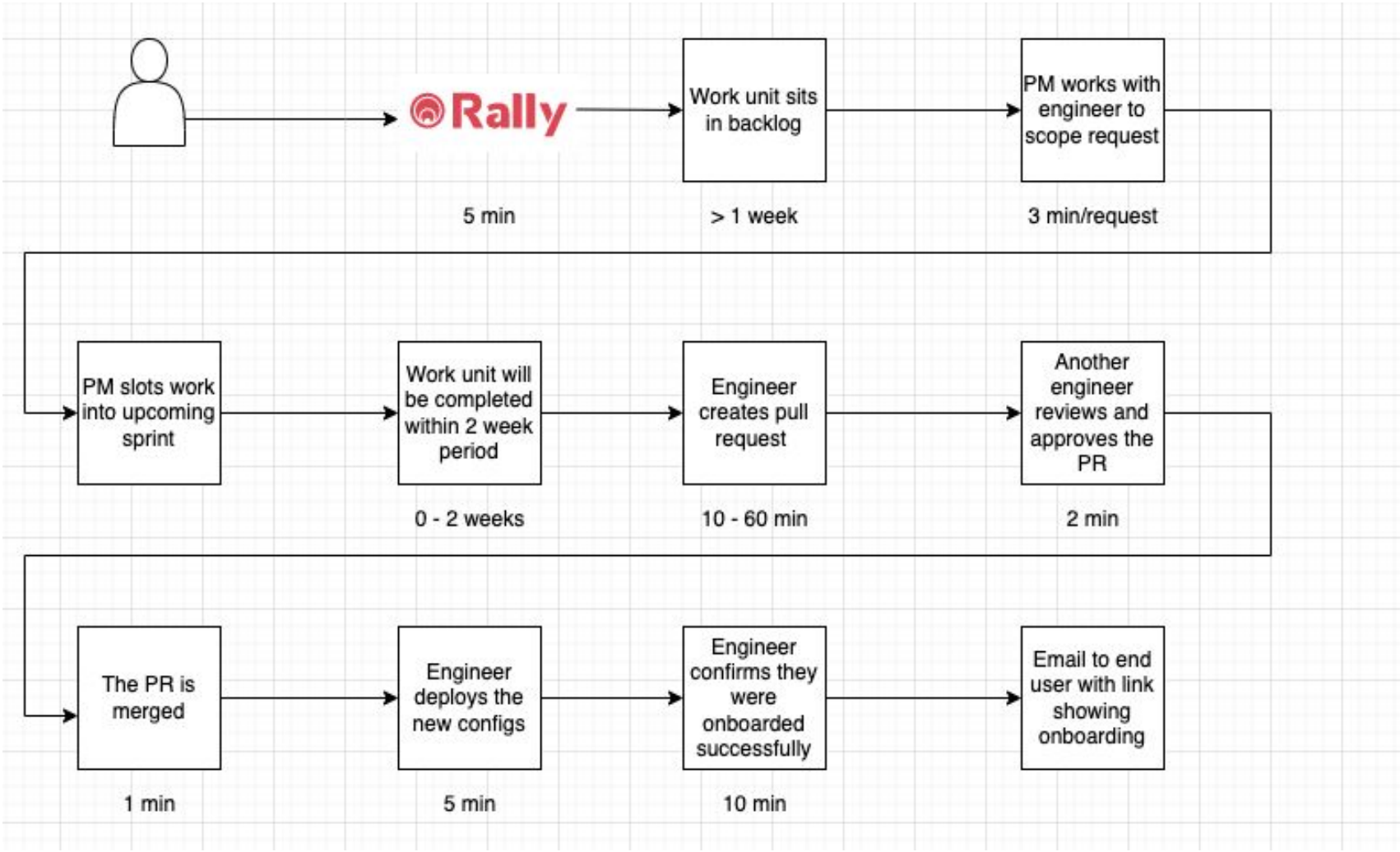
Walk

1. Using the deployment server
2. Updating inputs.conf within apps
3. Managing serverclasses effectively
4. Using version control to check in changes
5. Using props/transforms to linebreak, timestamp, and transform events

Run

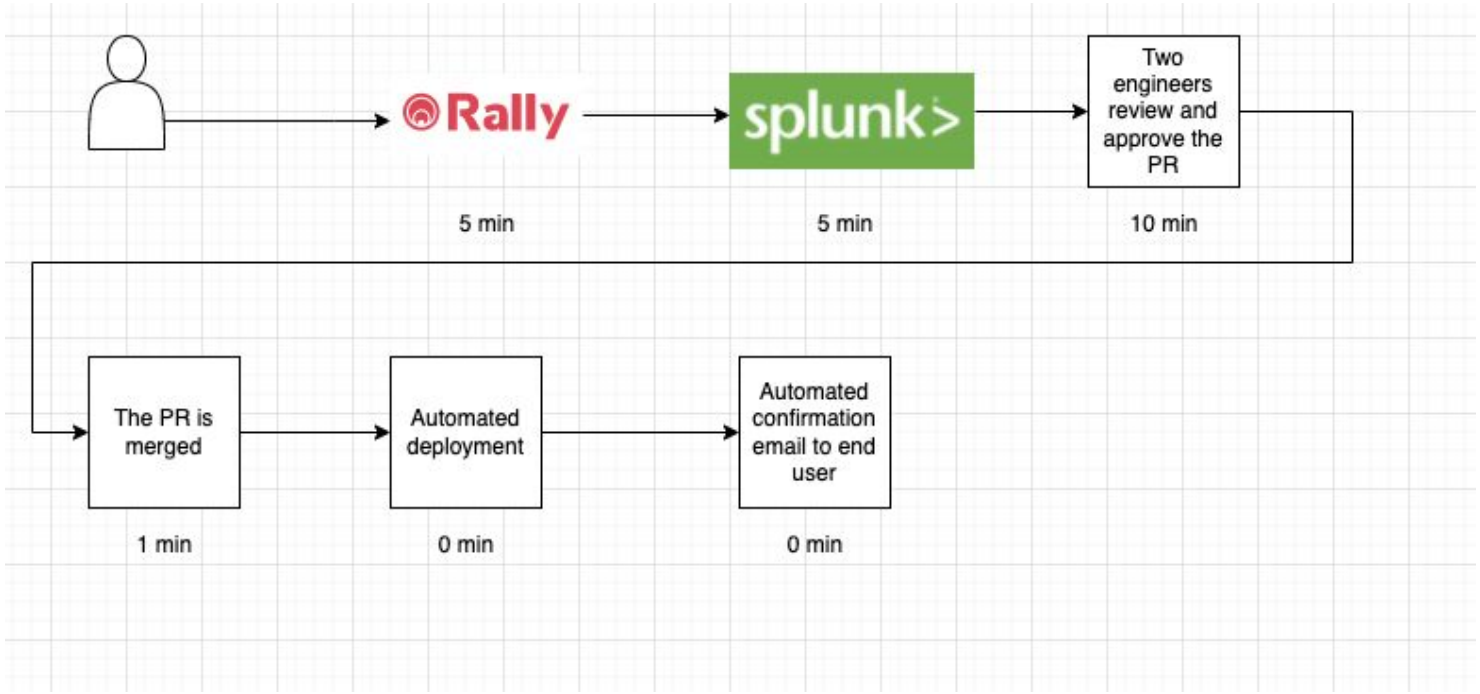
1. Full self-service automation
2. Shift work away from engineers to end users
3. Maintain onboarding quality with multiple engineering approvals
4. Break and transform events in motion using Cribl

Process Flow - Before Self-Service Automation



- User creates a request to onboard logs
- Engineer is responsible for doing the work and providing results to user
- This can easily turn into a full-time job

Process Flow - After Self-Service Automation



- This solution enables full self-service to user
- Engineers responsibility shifts away from doing the work to simply reviewing and approving

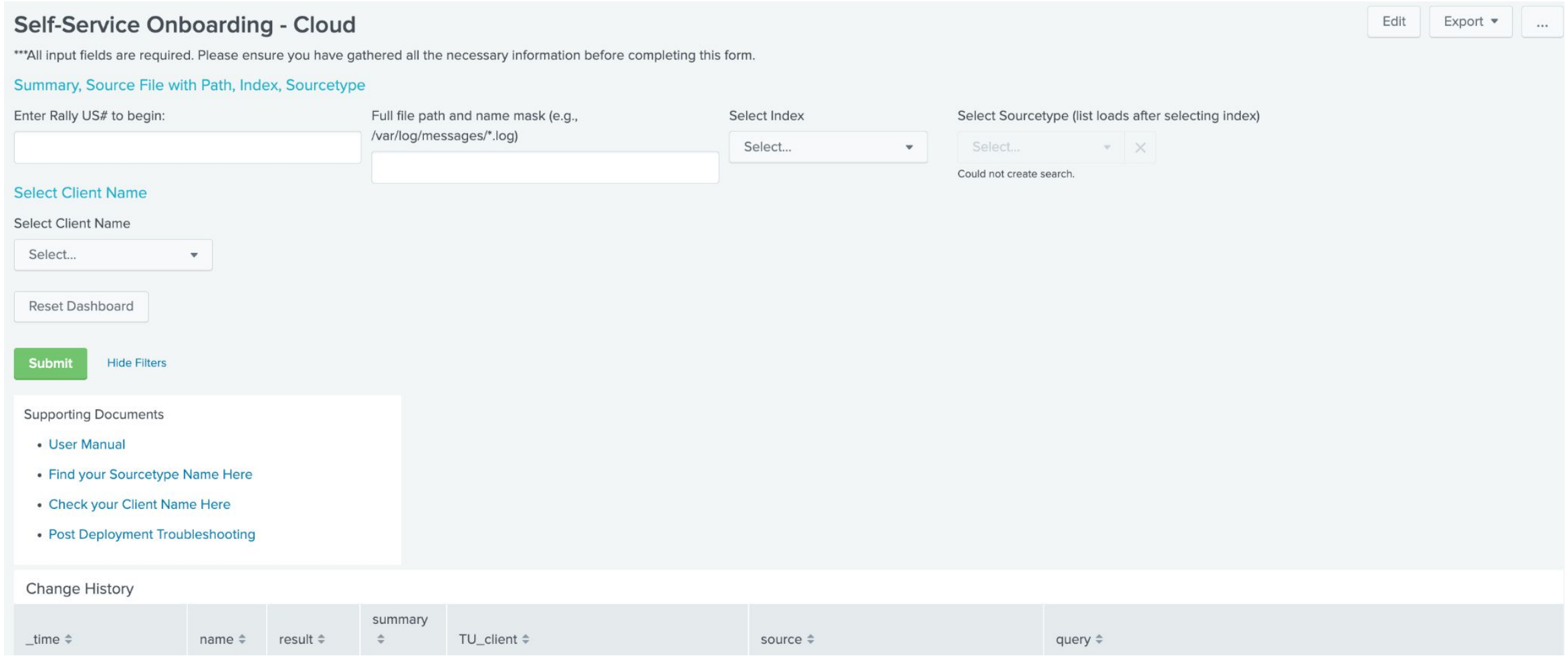
The Sourcetype Ledger

*Credit to Dave Olivas for contributing to this solution

Sourcetype Management

	Rule Name	Filter Condition	Event Breaker Type	Timestamp Anchor	Timestamp Format	Default Timezone	Earliest timestamp allowed	Future timestamp allowed	Max Event Bytes	Fields	Enabled	Actions
1		sourcetype==...	Regex	^	**Auto:** 150	local			99999999		Yes	
2		sourcetype==...	Regex	^	**Auto:** 150	local			99999999		Yes	
3		sourcetype==...	Regex	^	**Auto:** 150	local			99999999		Yes	
4		sourcetype==...	Regex	"instant":{"epochSecond	**Format:** %s	local			99999999		Yes	
5		sourcetype==...	Regex	eventTime=	**Auto:** 150	local			99999999		Yes	
6		sourcetype==...	Regex	^\w+\s	**Format:** %d %b %Y %H:%...	local			99999999		Yes	
7		sourcetype==...	Regex	^	**Auto:** 150	local			99999999		Yes	
8		sourcetype==...	Regex	^	**Format:** %Y-%m-%d %H:...	local	-420weeks	+1week	99999999		Yes	
9		sourcetype==...	Regex	^	**Current Time**	local			51200		Yes	
10		sourcetype==...	Regex	^	**Format:** %Y%m%d%H%...	local			99999999		Yes	
11		sourcetype==...	Regex	\<log_time\>	**Format:** %Y%m%d-%H:%...	local			99999999		Yes	
12		sourcetype==...	Regex	^Date\=\"	**Format:** %m/%d/%Y %H:...	local	-420weeks	+1week	99999999		Yes	
13		sourcetype==...	Regex	^	**Format:** %d-%b-%y %I.%...	local	-420weeks	+1week	99999999		Yes	
14		sourcetype==...	Regex	^	**Format:** %Y-%m-%d %H:...	local	-420weeks	+1week	99999999		Yes	
15		sourcetype==...	Regex	^LogTimestamp=	**Format:** %Y-%m-%dT%H:...	local	-420weeks	+1week	99999999		Yes	
16		sourcetype==...	Regex	^\d+\.\d+\.\d+\.\d+\s\-	**Format:** %d/%b/%Y:%H:...	local	-420weeks	+1week	99999999		Yes	
17		sourcetype==...	Regex	^\w{8}\-\w{4}\-\w{4}\-\	**Format:** %Y-%m-%d %H:...	local	-420weeks	+1week	99999999		Yes	

Intake Process



*Credit to Keryn Key for contributing to this solution

splunk> .conf22

```
| makeresults count=1
| eval header="{\"Content-Type\":\"application/json\"}"
| eval serverclass="[serverClass:us_dev_cloud-zero_corpdev_appltest_appltest:app:us_dev_cloud-zero_corpdev_appltest_appltest]
restartSplunkWeb = 0
restartIfNeeded = 1
stateOnClient = enabled
issueReload = true

[serverClass:us_dev_cloud-zero_corpdev_appltest_appltest]
whitelist.0 = us_dev_cloud-zero_corpdev_appltest_appltest"
| eval inputs="[monitor:///var/log/messages/*log]
index=summary
sourcetype=stash
disabled=0
_meta = app::appltest sub_app::appltest env::dev splunk_ta::us_dev_cloud-zero_corpdev_appltest_appltest"
| eval source="/var/log/messages/*log"
| eval email_address="::email=[redacted]"
| rex field=inputs mode=sed s/<APP>/"..."/g
| eval name="::user=[redacted]
| eval data='serverclass'.'inputs'.'name'.'email_address'

| curl method=post uri=[redacted]3Wg#Splunk_Pull_Request debug=true data=data headerfield=header verify=False

| eval result=if(curl_status="200","Your pull request was successful","Error in your pull request")
| eval name='[redacted]'
| eval email="[redacted]"
| eval summary="US560245"
| eval TU_client="us_dev_cloud-zero_corpdev_appltest_appltest"
| eval query="[redacted]/en-US/app/search/search?earliest=-30d@d&latest=now&q=search index=summary sourcetype=stash app=appltest sub_app=appltest"
| rex field=query mode=sed s/\s/"%20"/g
| fields + result curl_message name email summary TU_client query source
| head 1
| sendemail to=[redacted] subject="PR Created for 'US560245'" message="Your PR has been created: [redacted]_us_uf_deployment_server/pull-requests Validation search: [redacted]en-US/app
  /search/search?earliest=-30d@d&latest=now&q=search%20index=summary%20sourcetype=stash%20app=appltest%20sub_app=appltest"
| outputlookup ss_onboarding_records.csv  append=t
```

Supporting Documents

- User Manual
- Find your sourcetype name here
- Post Deployment Troubleshooting

Click for Pull Request

PR_click
Click to create pull request

Change History

_time	name	result	summary	TU_client	source	query
2022-04-06 15:48:04	Koelpin, Steve	Your pull request was successful	US560245	us_dev_cloud-zero_corpdev_appltest_appltest	/var/log/messages/*log	/en-US/app/search/search?earliest=-30d@d&latest=now&q=search%20index=summary%20sourcetype=stash%20app=appltest%20sub_app=appltest

serverclass.conf entry

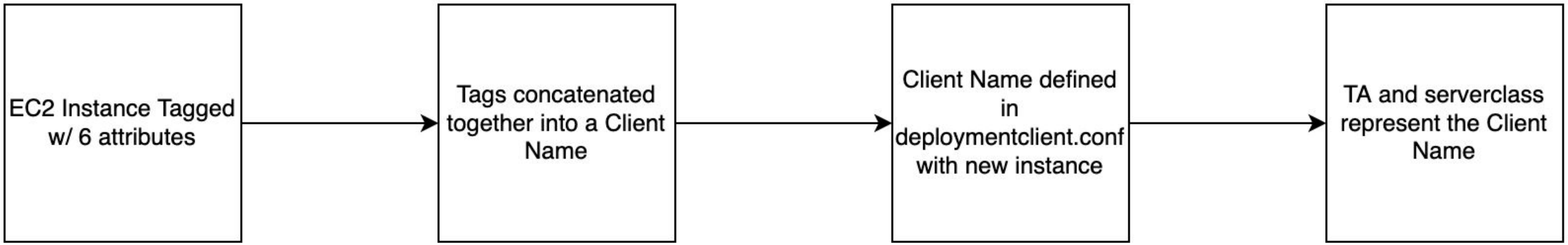
```
15740 +  [serverClass:us_dev_cloud-zero_corpdev_appltest_appltest:app:us_dev_cloud-zero_corpdev_appltest_appltest]
15741 +  restartSplunkWeb = 0
15742 +  restartIfNeeded = 1
15743 +  stateOnClient = enabled
15744 +  issueReload = true
15745 +
15746 +  [serverClass:us_dev_cloud-zero_corpdev_appltest_appltest]
15747 +  whitelist.0 = us_dev_cloud-zero_corpdev_appltest_appltest
15748 +
```

inputs.conf entry

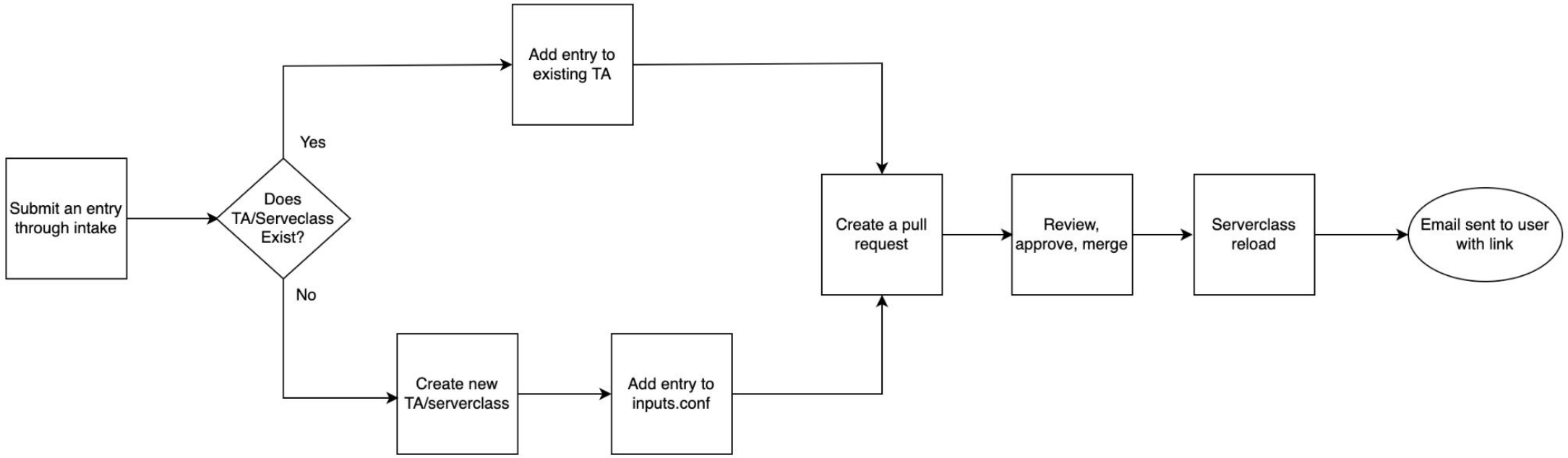
us_dev_cloud-zero_corpdev_appltest_appltest / local / **inputs.conf** ADDED

```
1 +
2 +  [monitor:///var/log/messages/*log]
3 +  index=summary
4 +  sourcetype=stash
5 +  disabled=0
6 +  _meta = app::appltest sub_app::appltest env::dev splunk_ta::us_dev_cloud-zero_corpdev_appltest_appltest
```

Automation



Automation



The **REAL** value of this

Automatically associate newly created instances with a common grouping that represents the serverclass

Lessons Learned Along the Way

Provide Users with Feedback

- When buttons are clicked, display an output showing the result of the action
- This prevents users from clicking the button multiple times
- Also helps users understanding why solution did not work as expected

Enforce Standardization

- Standard sourcetype names are REQUIRED
- Use Cribl to build and maintain sourcetype names

Don’t Give Up When Things Get Hard

- Difficult to implement

Thank You

splunk> .conf22