Build a JARVIS for Your SOC

Jonathan Pagett, Peter Littler
Cyber Defence Centre, Bank of England

Build a JARVIS for Your SOC

Jonathan Pagett

Head of Cyber Defence Centre

Peter Littler

DevOps, Cyber Defence Centre

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Overview

1. Our operating model and the challenges it introduces
2. Share some of our initial ideas for addressing them and how we built them
3. Introduce JARVIS
4. We will share all the code!

Who are the Bank of England?

Founded 1694

Gold reserves

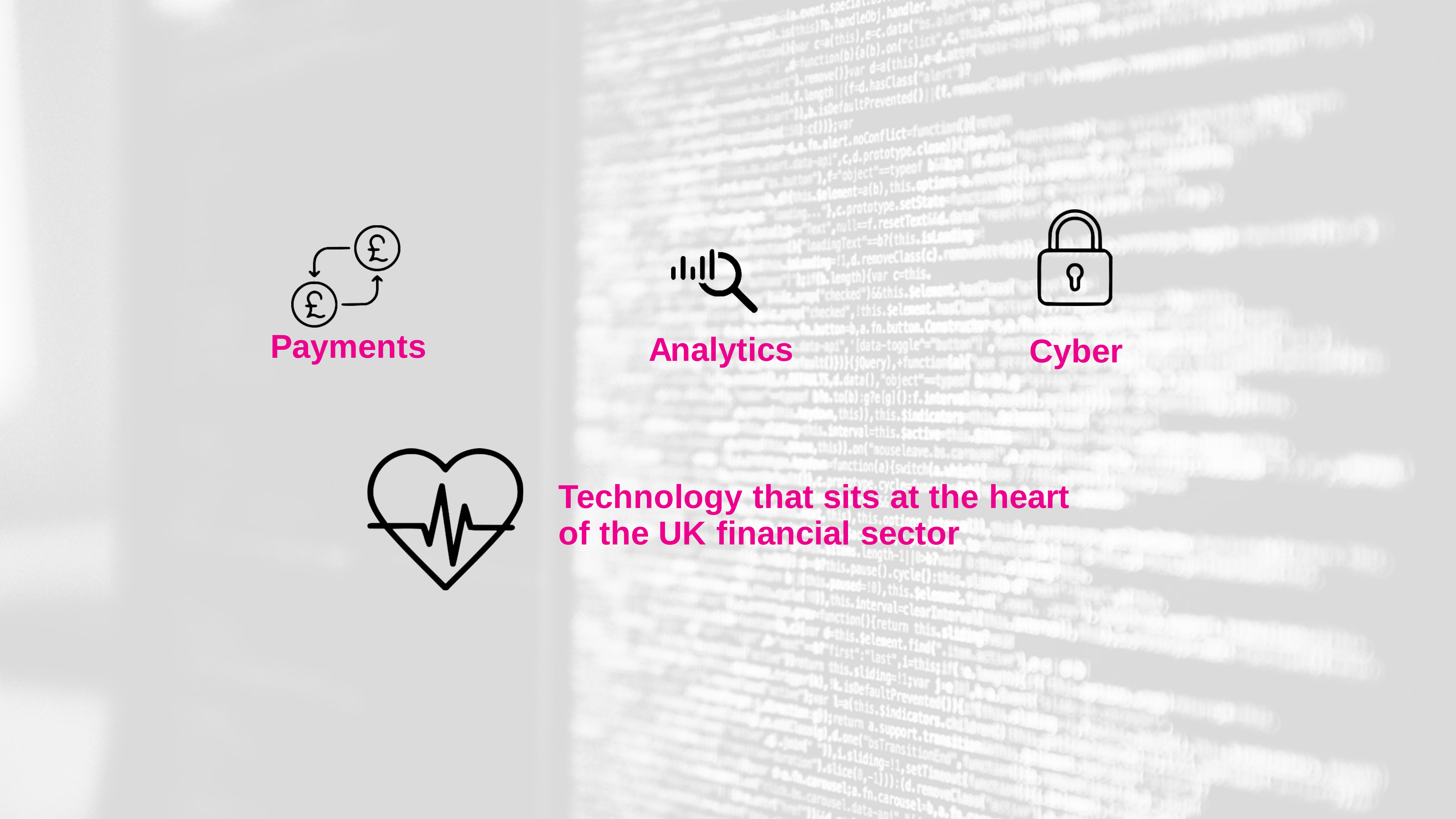
Monetary stability

Financial stability

Print banknotes

Run payments services

Provide “risk free” banking services



Payments

Analytics

Cyber

Technology that sits at the heart of the UK financial sector

Bank of England

In numbers . . .

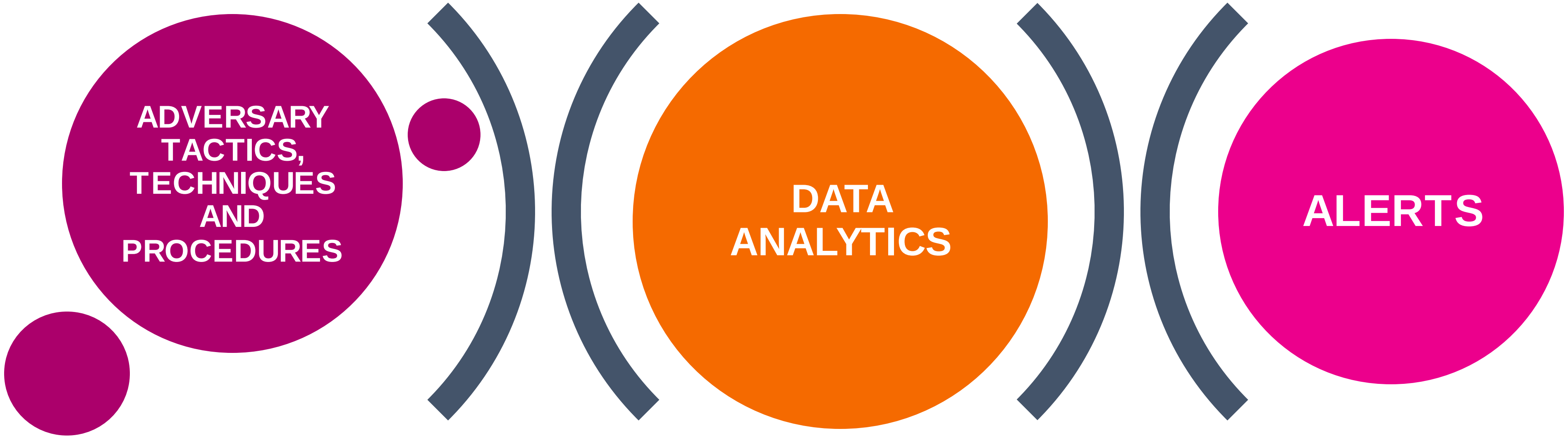
Daily payments	UK GDP everyday	Staff	Hosts	CDC staff
$1T	1/3	4,000	10,000	12

“**Detect** and **respond** to cyber-attacks against the Bank of England”

Cyber Defence Centre

Our operating model

And the challenges it introduces…



ADVERSARY TACTICS, TECHNIQUES AND PROCEDURES

DATA ANALYTICS

ALERTS

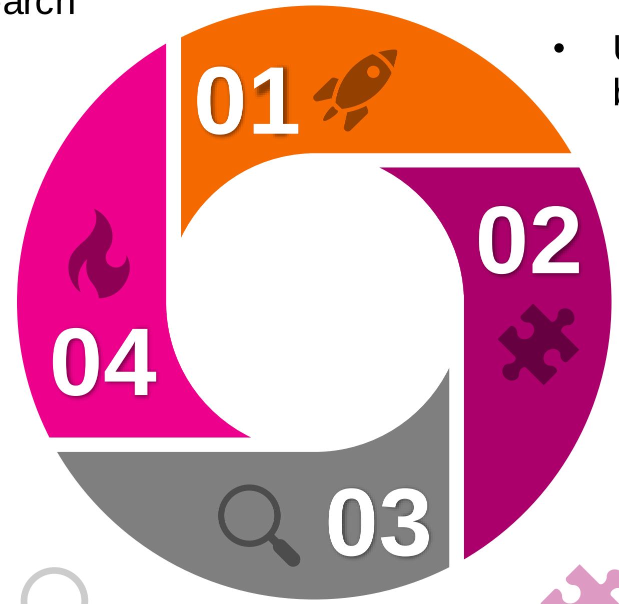
THREAT OPERATIONS

THREAT HUNTING

INCIDENT RESPONSE

Continual improvement model

- Research and intelligence based
- Continual improvement at heart – 80% of team time
- Data and adversary led
- 331 analytics developed
- Supported by team structure



Data ingest

- Ingest data
- Update logging requirements based on incident findings

Create hypothesis

- Research
- Threat intelligence
- Business engagement

Threat hunting

- Statistical
- Correlation
- Machine learning

Repeatable analytic

- Scheduled saved search made for analytic

“Nobody gets up in the morning to triage alerts”

Issues with our operating model

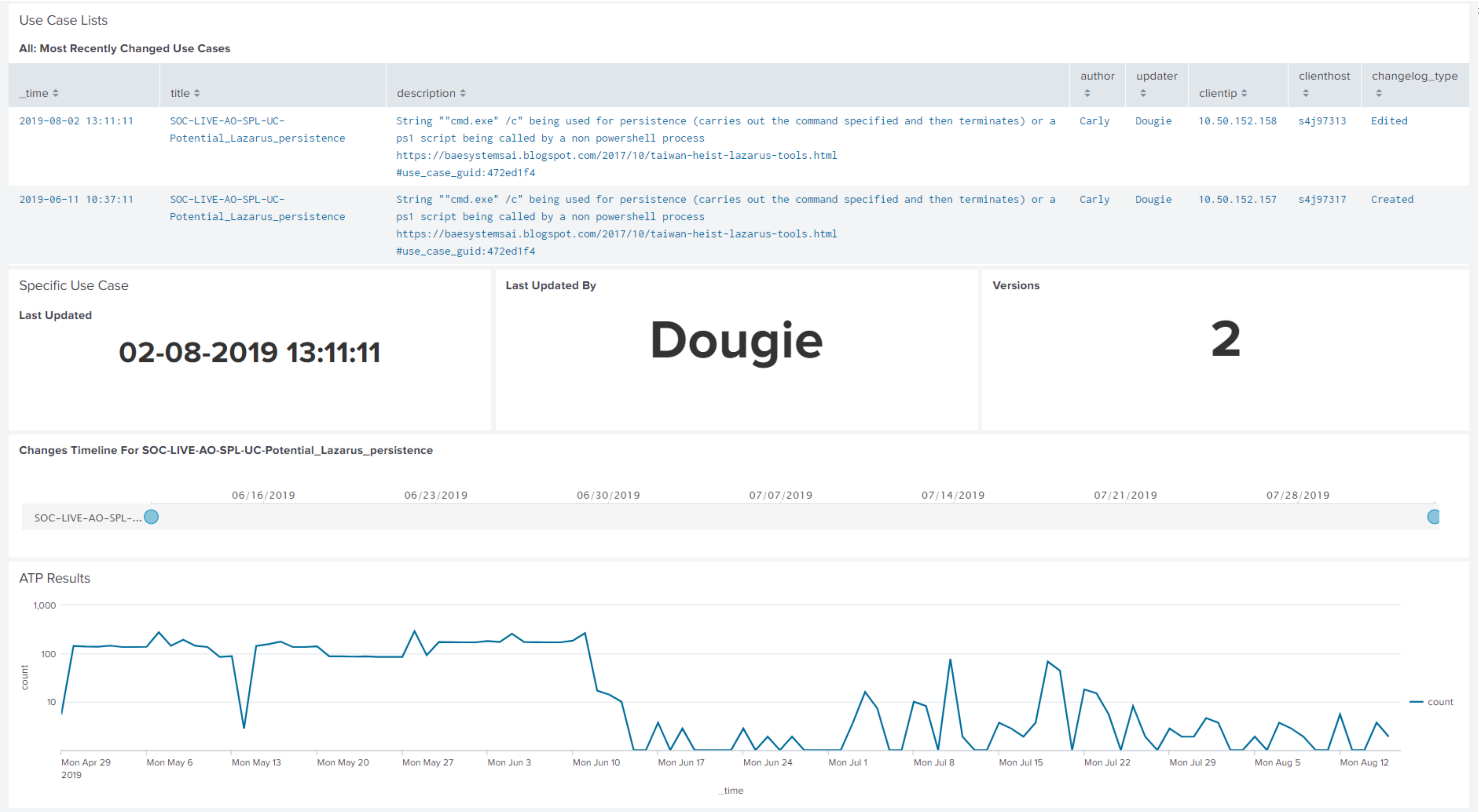
1. Everything is constantly changing!
2. Managing feedback – people triaging alerts are not always the author of searches

Our first go at fixing these problems - 2018

Dashboards, workflows

Search change log

“Git” within Splunk



Use Case Lists

All: Most Recently Changed Use Cases

_time	title	description	author	updater	clientip	clienthost	changelog_type
2019-08-02 13:11:11	SOC-LIVE-AO-SPL-UC-Potential_Lazarus_persistence	String ""cmd.exe" /c" being used for persistence (carries out the command specified and then terminates) or a ps1 script being called by a non powershell process https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html #use_case_guid:472ed1f4	Carly	Dougie	10.50.152.158	s4j97313	Edited
2019-06-11 10:37:11	SOC-LIVE-AO-SPL-UC-Potential_Lazarus_persistence	String ""cmd.exe" /c" being used for persistence (carries out the command specified and then terminates) or a ps1 script being called by a non powershell process https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html #use_case_guid:472ed1f4	Carly	Dougie	10.50.152.157	s4j97317	Created

Specific Use Case

Last Updated

02-08-2019 13:11:11

Last Updated By

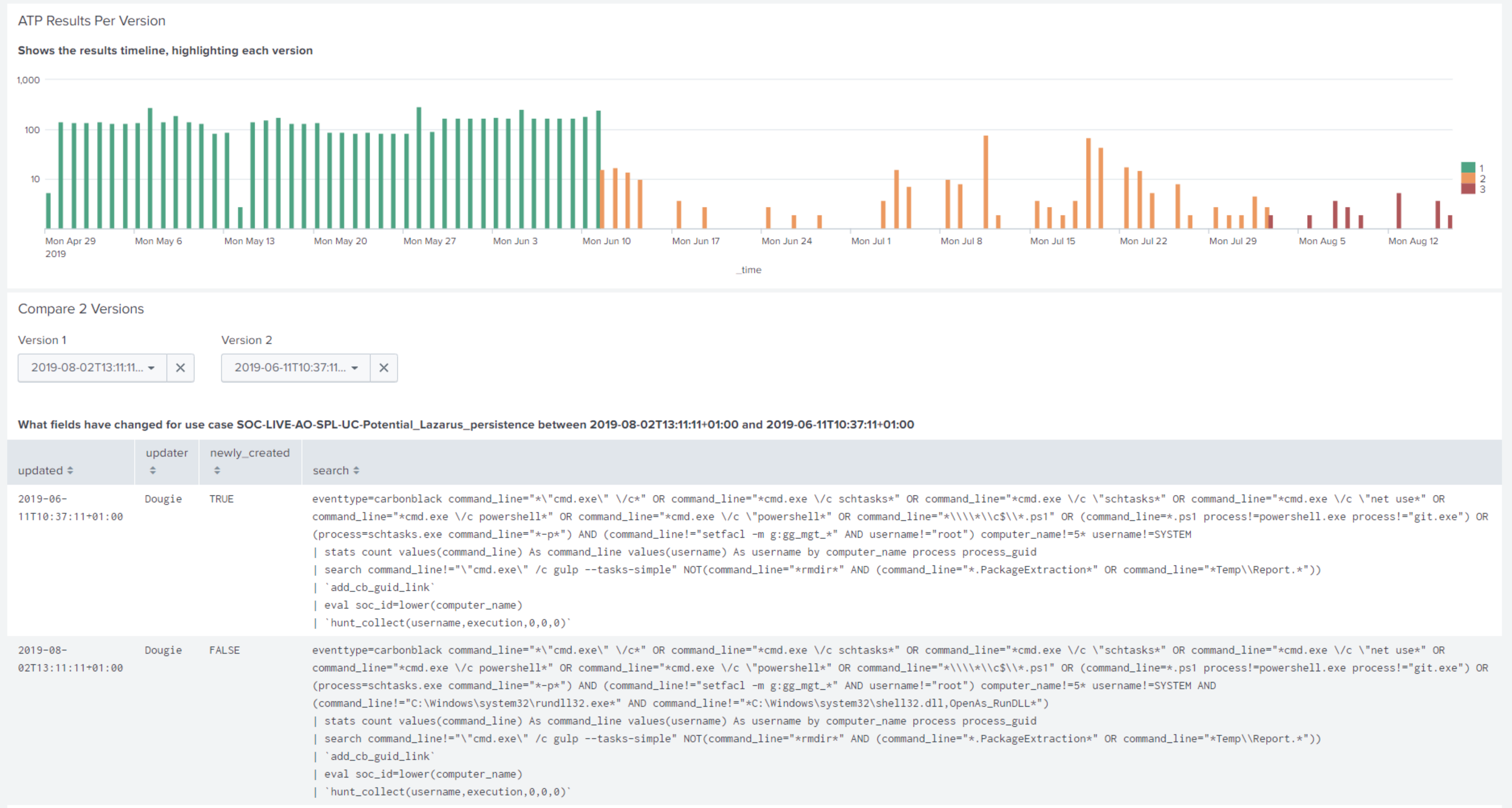
Dougie

Versions

2

Changes Timeline For SOC-LIVE-AO-SPL-UC-Potential_Lazarus_persistence

ATP Results



ATP Results Per Version

Shows the results timeline, highlighting each version

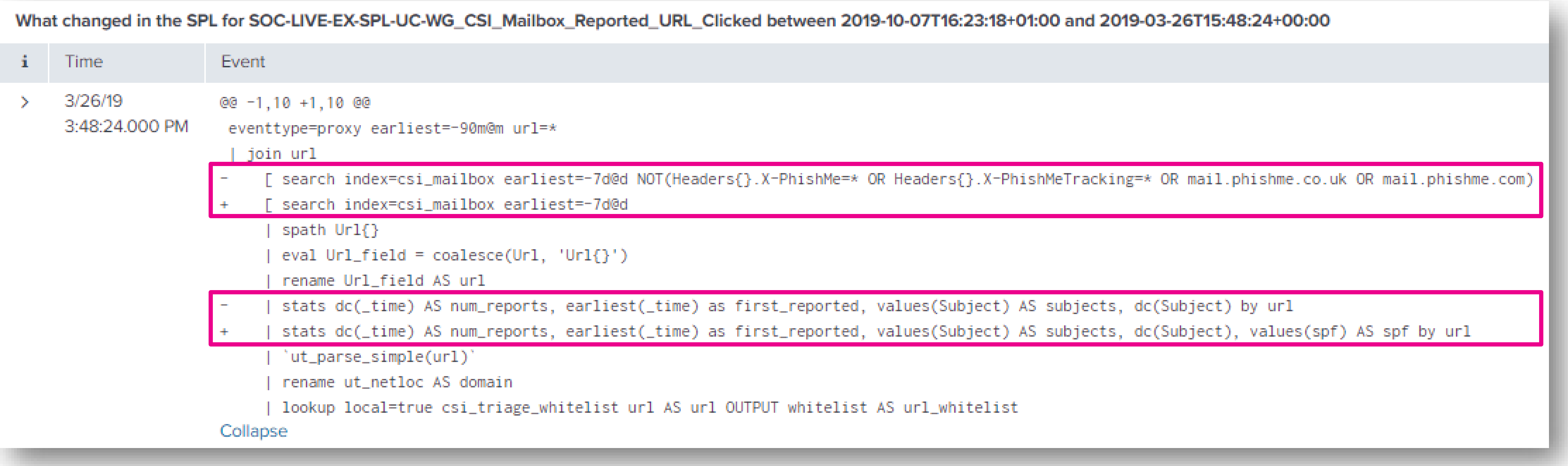
Compare 2 Versions

Version 1: 2019-08-02T13:11:11... ▾ ✕

Version 2: 2019-06-11T10:37:11... ▾ ✕

What fields have changed for use case SOC-LIVE-AO-SPL-UC-Potential_Lazarus_persistence between 2019-08-02T13:11:11+01:00 and 2019-06-11T10:37:11+01:00

<table>
<tr><th>updated ⬍</th><th>updater ⬍</th><th>newly_created ⬍</th><th>search ⬍</th></tr>
<tr><td>2019-06-11T10:37:11+01:00</td><td>Dougie</td><td>TRUE</td><td>eventtype=carbonblack command_line="*\"cmd.exe\" \/c*" OR command_line="*cmd.exe \/c schtasks*" OR command_line="*cmd.exe \/c \"schtasks*" OR command_line="*cmd.exe \/c \"net use*" OR command_line="*cmd.exe \/c powershell*" OR command_line="*cmd.exe \/c \"powershell*" OR command_line="\\\\c$\*.ps1" OR (command_line=*.ps1 process!=powershell.exe process!="git.exe") OR (process=schtasks.exe command_line="*-p*") AND (command_line!="setfacl -m g:gg_mgt_*" AND username!="root") computer_name!=5* username!=SYSTEM
| stats count values(command_line) As command_line values(username) As username by computer_name process process_guid
| search command_line!="\"cmd.exe\" /c gulp --tasks-simple" NOT(command_line="*rmdir*" AND (command_line="*.PackageExtraction*" OR command_line="*Temp\\Report.*"))
| `add_cb_guid_link`
| eval soc_id=lower(computer_name)
| `hunt_collect(username,execution,0,0,0)`</td></tr>
<tr><td>2019-08-02T13:11:11+01:00</td><td>Dougie</td><td>FALSE</td><td>eventtype=carbonblack command_line="*\"cmd.exe\" \/c*" OR command_line="*cmd.exe \/c schtasks*" OR command_line="*cmd.exe \/c \"schtasks*" OR command_line="*cmd.exe \/c \"net use*" OR command_line="*cmd.exe \/c powershell*" OR command_line="*cmd.exe \/c \"powershell*" OR command_line="\\\\c$\*.ps1" OR (command_line=*.ps1 process!=powershell.exe process!="git.exe") OR (process=schtasks.exe command_line="*-p*") AND (command_line!="setfacl -m g:gg_mgt_*" AND username!="root") computer_name!=5* username!=SYSTEM AND (command_line!="C:\Windows\system32\rundll32.exe*" AND command_line!="*C:\Windows\system32\shell32.dll,OpenAs_RunDLL*")
| stats count values(command_line) As command_line values(username) As username by computer_name process process_guid
| search command_line!="\"cmd.exe\" /c gulp --tasks-simple" NOT(command_line="*rmdir*" AND (command_line="*.PackageExtraction*" OR command_line="*Temp\\Report.*"))
| `add_cb_guid_link`
| eval soc_id=lower(computer_name)
| `hunt_collect(username,execution,0,0,0)`</td></tr>
</table>



What changed in the SPL for SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked between 2019-10-07T16:23:18+01:00 and 2019-03-26T15:48:24+00:00

i	Time	Event
>	3/26/19 3:48:24.000 PM	

```
@@ -1,10 +1,10 @@
 eventtype=proxy earliest=-90m@m url=*
 | join url
-    [ search index=csi_mailbox earliest=-7d@d NOT(Headers{}.X-PhishMe=* OR Headers{}.X-PhishMeTracking=* OR mail.phishme.co.uk OR mail.phishme.com)
+    [ search index=csi_mailbox earliest=-7d@d
     | spath Url{}
     | eval Url_field = coalesce(Url, 'Url{}')
     | rename Url_field AS url
-    | stats dc(_time) AS num_reports, earliest(_time) as first_reported, values(Subject) AS subjects, dc(Subject) by url
+    | stats dc(_time) AS num_reports, earliest(_time) as first_reported, values(Subject) AS subjects, dc(Subject), values(spf) AS spf by url
     | `ut_parse_simple(url)`
     | rename ut_netloc AS domain
     | lookup local=true csi_triage_whitelist url AS url OUTPUT whitelist AS url_whitelist
```

How it’s made

Techniques we found useful

1. REST is your friend

   Schedule a search to monitor **REST** API and save results to an index

```
| rest splunk_server=local /servicesNS/-/APP/saved/searches
| search NOT
        [search index=use_case_changelog
         | table title, updated]
| eval _time=now()
| collect index=use_case_changelog
```

How it’s made

Techniques we found useful

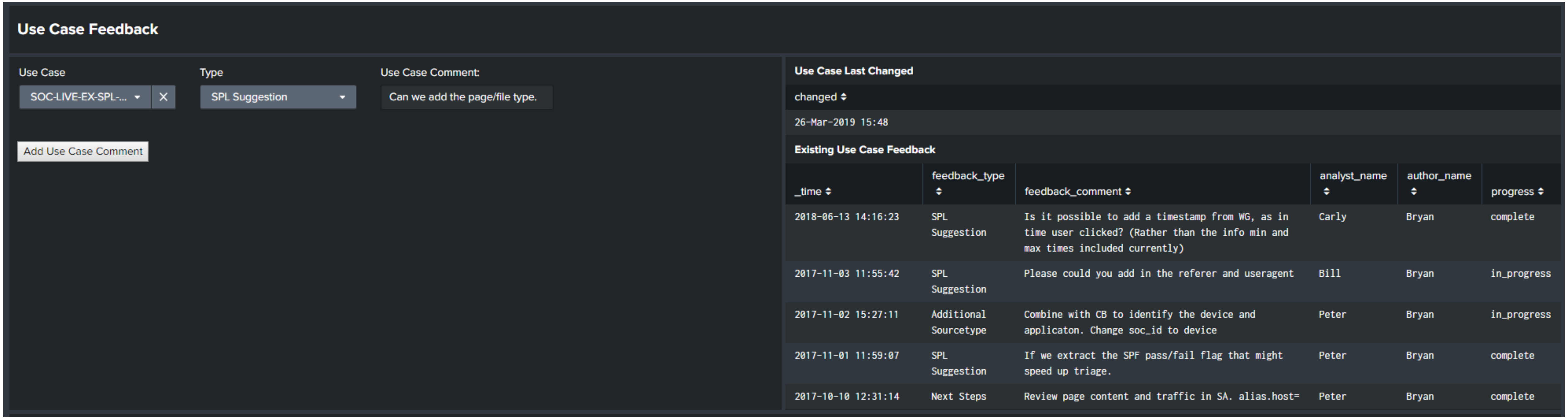
2. _internal is also your friend!

Contains a lot of data on interactions between users and Splunk

```
| join type=left title max=1 usetime=true earlier=true
  [ search index=_internal file=* file!=notify method=POST
user!="splunk-system-user" "*/APP/saved/searches/*"
    | rex field=uri "/APP/saved/searches/(?<rex_file>.*)/"
    | eval file = coalesce(rex_file, file)
    | eval file = urldecode(urldecode(file))
     …
    | sort - submission_epoch]
```

Use case feedback

Managing feedback between analysts



Use Case Feedback

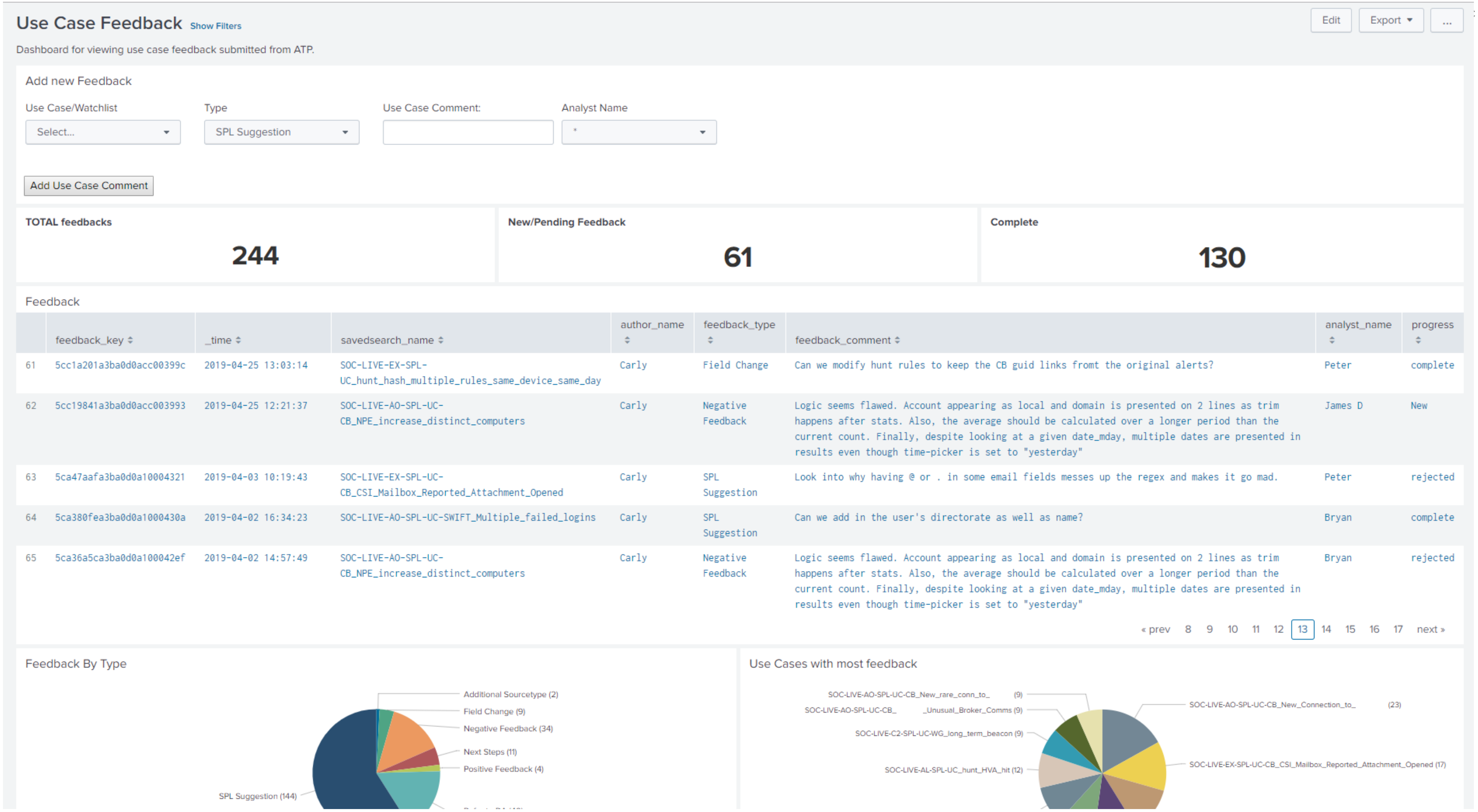
Use Case	Type	Use Case Comment:
SOC-LIVE-EX-SPL-... ✕	SPL Suggestion	Can we add the page/file type.

Use Case Last Changed

changed
26-Mar-2019 15:48

Existing Use Case Feedback

_time	feedback_type	feedback_comment	analyst_name	author_name	progress
2018-06-13 14:16:23	SPL Suggestion	Is it possible to add a timestamp from WG, as in time user clicked? (Rather than the info min and max times included currently)	Carly	Bryan	complete
2017-11-03 11:55:42	SPL Suggestion	Please could you add in the referer and useragent	Bill	Bryan	in_progress
2017-11-02 15:27:11	Additional Sourcetype	Combine with CB to identify the device and applicaton. Change soc_id to device	Peter	Bryan	in_progress
2017-11-01 11:59:07	SPL Suggestion	If we extract the SPF pass/fail flag that might speed up triage.	Peter	Bryan	complete
2017-10-10 12:31:14	Next Steps	Review page content and traffic in SA. alias.host=	Peter	Bryan	complete



Use Case Feedback

Dashboard for viewing use case feedback submitted from ATP.

Add new Feedback

Use Case/Watchlist	Type	Use Case Comment:	Analyst Name
Select... ▾	SPL Suggestion ▾		* ▾

TOTAL feedbacks	New/Pending Feedback	Complete
244	61	130

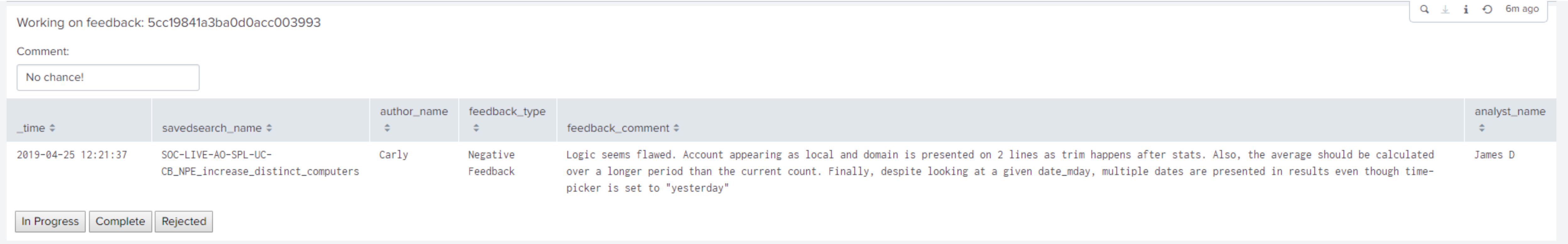
Feedback

	feedback_key ⇕	_time ⇕	savedsearch_name ⇕	author_name ⇕	feedback_type ⇕	feedback_comment ⇕	analyst_name ⇕	progress ⇕
61	5cc1a201a3ba0d0acc00399c	2019-04-25 13:03:14	SOC-LIVE-EX-SPL-UC_hunt_hash_multiple_rules_same_device_same_day	Carly	Field Change	Can we modify hunt rules to keep the CB guid links fromt the original alerts?	Peter	complete
62	5cc19841a3ba0d0acc003993	2019-04-25 12:21:37	SOC-LIVE-AO-SPL-UC-CB_NPE_increase_distinct_computers	Carly	Negative Feedback	Logic seems flawed. Account appearing as local and domain is presented on 2 lines as trim happens after stats. Also, the average should be calculated over a longer period than the current count. Finally, despite looking at a given date_mday, multiple dates are presented in results even though time-picker is set to "yesterday"	James D	New
63	5ca47aafa3ba0d0a10004321	2019-04-03 10:19:43	SOC-LIVE-EX-SPL-UC-CB_CSI_Mailbox_Reported_Attachment_Opened	Carly	SPL Suggestion	Look into why having @ or . in some email fields messes up the regex and makes it go mad.	Peter	rejected
64	5ca380fea3ba0d0a1000430a	2019-04-02 16:34:23	SOC-LIVE-AO-SPL-UC-SWIFT_Multiple_failed_logins	Carly	SPL Suggestion	Can we add in the user's directorate as well as name?	Bryan	complete
65	5ca36a5ca3ba0d0a100042ef	2019-04-02 14:57:49	SOC-LIVE-AO-SPL-UC-CB_NPE_increase_distinct_computers	Carly	Negative Feedback	Logic seems flawed. Account appearing as local and domain is presented on 2 lines as trim happens after stats. Also, the average should be calculated over a longer period than the current count. Finally, despite looking at a given date_mday, multiple dates are presented in results even though time-picker is set to "yesterday"	Bryan	rejected

Feedback By Type

Use Cases with most feedback

SOC-LIVE-AO-SPL-UC-CB_New_rare_conn_to_ (9)
SOC-LIVE-AO-SPL-UC-CB_ _Unusual_Broker_Comms (9)
SOC-LIVE-C2-SPL-UC-WG_long_term_beacon (9)
SOC-LIVE-AL-SPL-UC_hunt_HVA_hit (12)
SOC-LIVE-AO-SPL-UC-CB_New_Connection_to_ (23)
SOC-LIVE-EX-SPL-UC-CB_CSI_Mailbox_Reported_Attachment_Opened (17)



Working on feedback: 5cc19841a3ba0d0acc003993

Comment: No chance!

_time	savedsearch_name	author_name	feedback_type	feedback_comment	analyst_name
2019-04-25 12:21:37	SOC-LIVE-AO-SPL-UC-CB_NPE_increase_distinct_computers	Carly	Negative Feedback	Logic seems flawed. Account appearing as local and domain is presented on 2 lines as trim happens after stats. Also, the average should be calculated over a longer period than the current count. Finally, despite looking at a given date_mday, multiple dates are presented in results even though time-picker is set to "yesterday"	James D

How it's made

Techniques we found useful

1. Dashboard > KV store

   Use JavaScript to write dashboard inputs to KV stores

   Tutorial on Splunk dev website

Introducing JARVIS

Dashboards are so 2018

Context aware information within our normal workflows”

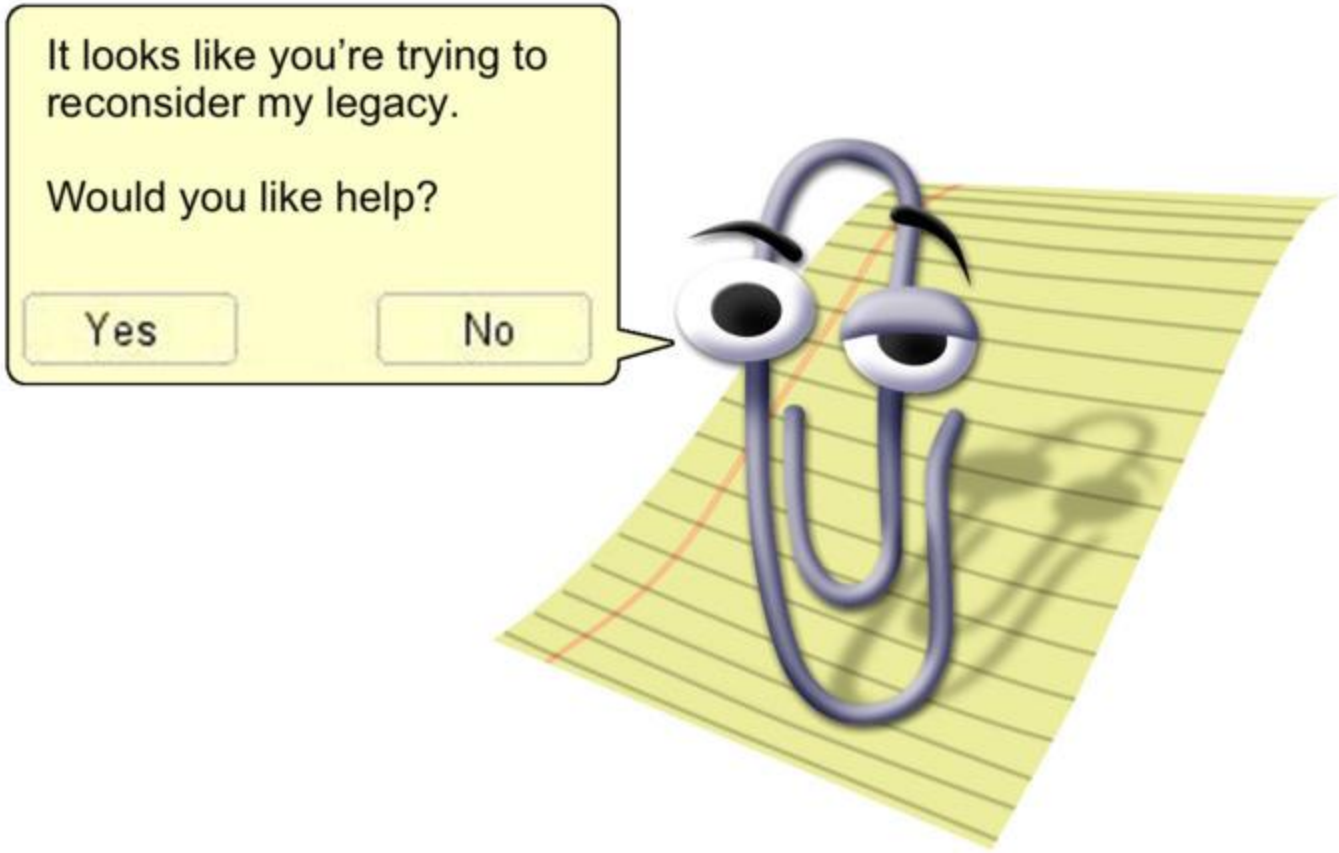
JARVIS

Our requirements

1. Reminding you of things
2. Keep an eye out for things you may have forgotten or not realised
3. Anticipating your needs

What the boss asked for…

…what we thought



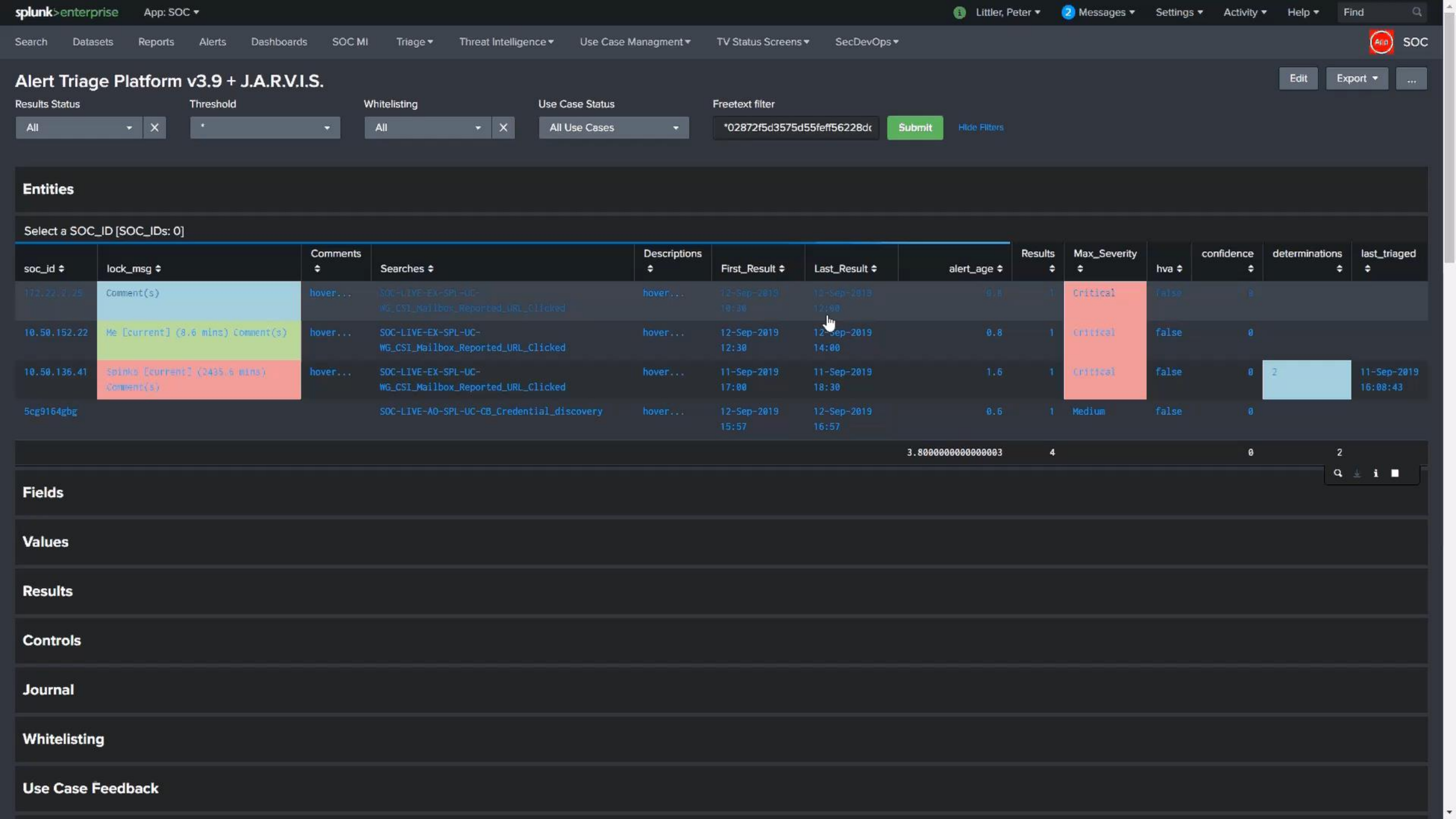
Interactive options

1. JavaScript persona

   - Passive information

2. Modal popups

   - Urgent information requiring your attention



Alert Triage Platform v3.9 + J.A.R.V.I.S.

Results Status: All

Threshold: *

Whitelisting: All

Use Case Status: All Use Cases

Freetext filter: *02872f5d3575d55feff56228dc

Entities

Select a SOC_ID [SOC_IDs: 0]

soc_id	lock_msg	Comments	Searches	Descriptions	First_Result	Last_Result	alert_age	Results	Max_Severity	hva	confidence	determinations	last_triaged
172.22.2.25	Comment(s)	hover...	SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked	hover...	12-Sep-2019 10:30	12-Sep-2019 12:00	0.8	1	Critical	false	0		
10.50.152.22	Me [current] (8.6 mins) Comment(s)	hover...	SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked	hover...	12-Sep-2019 12:30	12-Sep-2019 14:00	0.8	1	Critical	false	0		
10.50.136.41	Spinks [current] (2435.6 mins) Comment(s)	hover...	SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked	hover...	11-Sep-2019 17:00	11-Sep-2019 18:30	1.6	1	Critical	false	0	2	11-Sep-2019 16:08:43
5cg9164gbg			SOC-LIVE-AO-SPL-UC-CB_Credential_discovery	hover...	12-Sep-2019 15:57	12-Sep-2019 16:57	0.6	1	Medium	false	0		
							3.8000000000000003	4			0	2	

Fields

Values

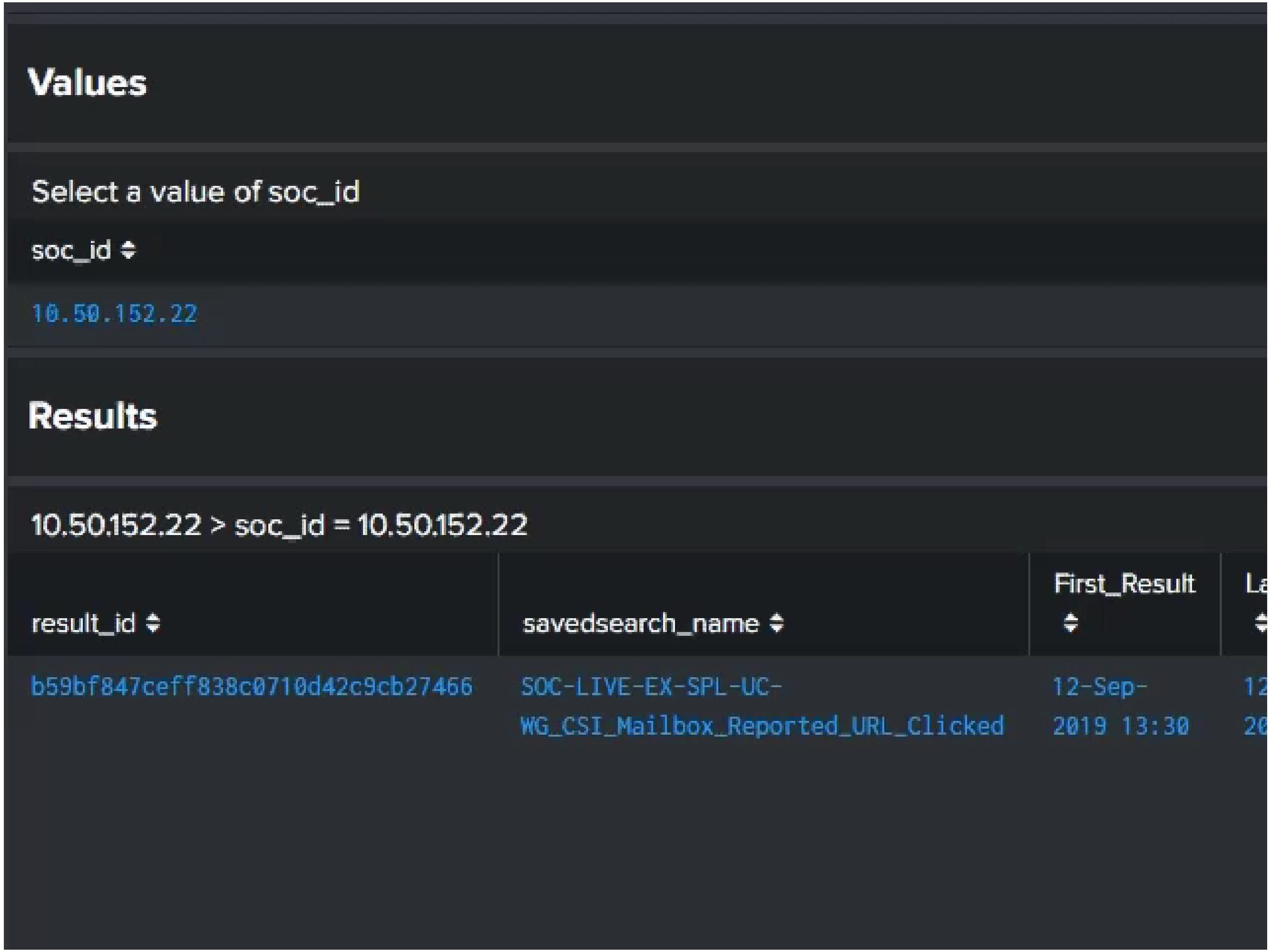
Results

Controls

Journal

Whitelisting

Use Case Feedback



Values

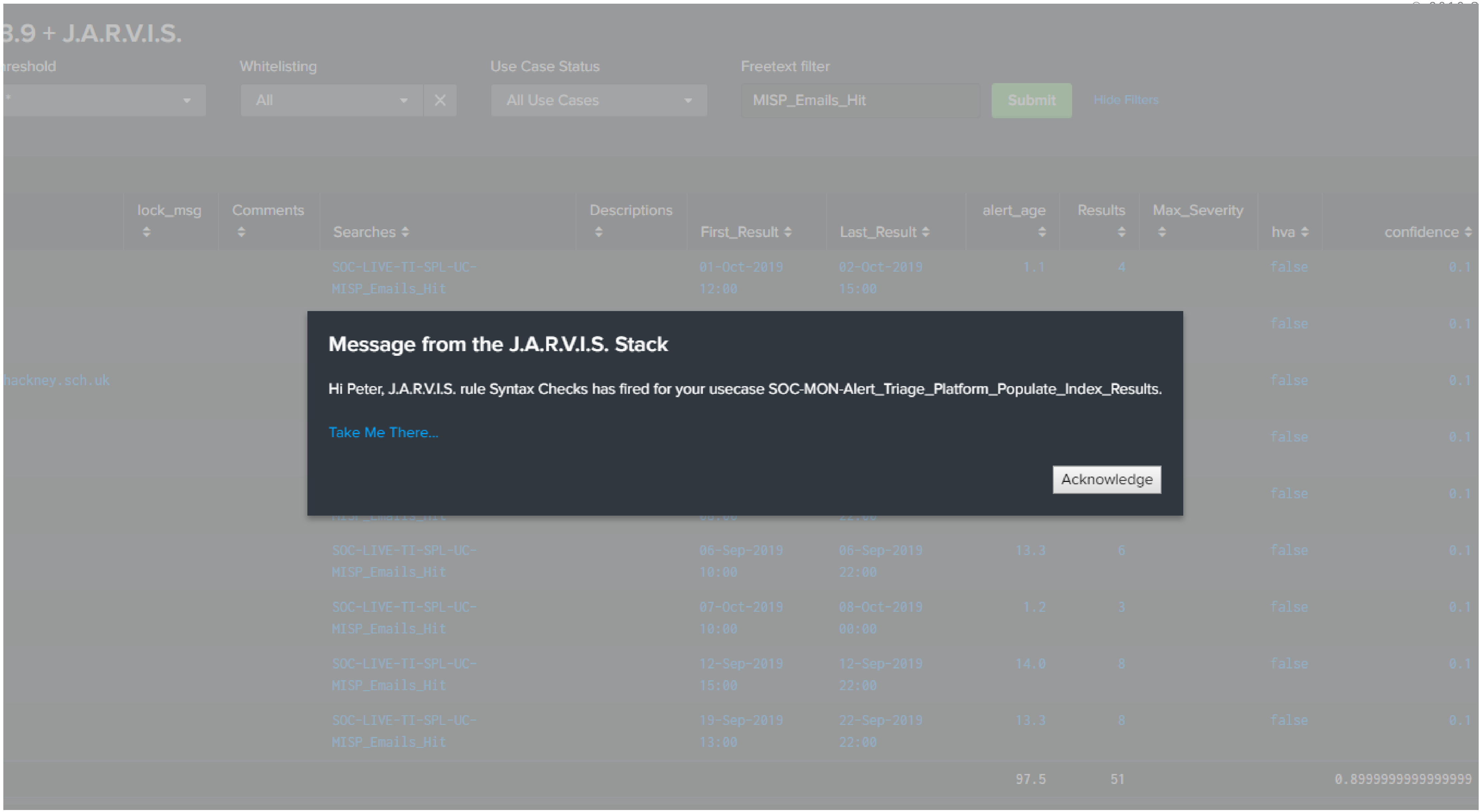
Select a value of soc_id

soc_id ⇕
10.50.152.22

Results

10.50.152.22 > soc_id = 10.50.152.22

result_id ⇕	savedsearch_name ⇕	First_Result ⇕	La ⇕
b59bf847ceff838c0710d42c9cb27466	SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked	12-Sep-2019 13:30	12 20



3.9 + J.A.R.V.I.S.

reshold: *

Whitelisting: All

Use Case Status: All Use Cases

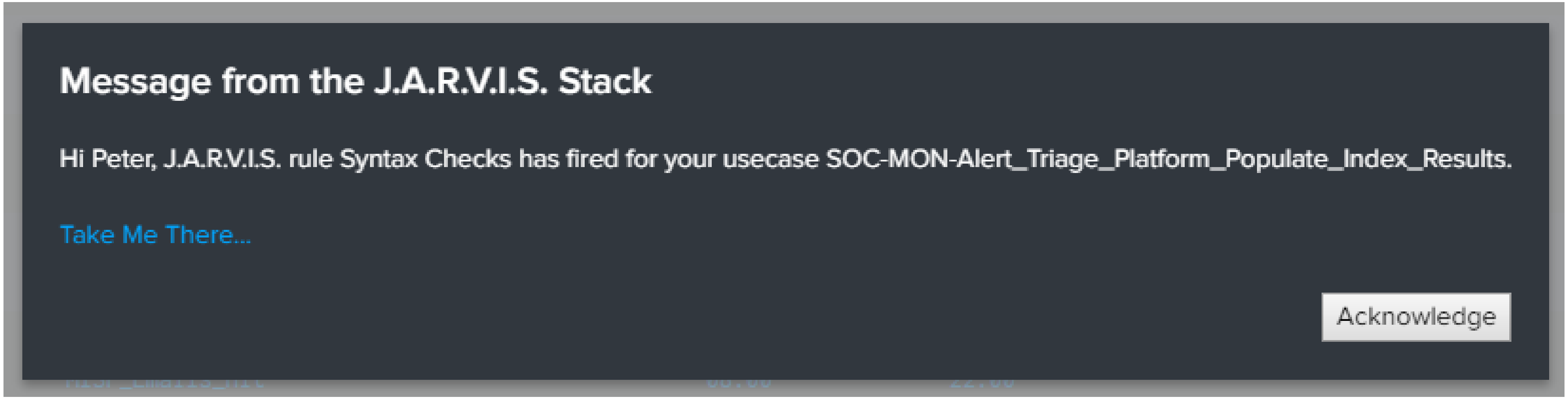
Freetext filter: MISP_Emails_Hit

	lock_msg	Comments	Searches	Descriptions	First_Result	Last_Result	alert_age	Results	Max_Severity	hva	confidence
			SOC-LIVE-TI-SPL-UC-MISP_Emails_Hit		01-Oct-2019 12:00	02-Oct-2019 15:00	1.1	4		false	0.1
										false	0.1
hackney.sch.uk										false	0.1
										false	0.1
			MISP_Emails_Hit							false	0.1
			SOC-LIVE-TI-SPL-UC-MISP_Emails_Hit		06-Sep-2019 10:00	06-Sep-2019 22:00	13.3	6		false	0.1
			SOC-LIVE-TI-SPL-UC-MISP_Emails_Hit		07-Oct-2019 10:00	08-Oct-2019 00:00	1.2	3		false	0.1
			SOC-LIVE-TI-SPL-UC-MISP_Emails_Hit		12-Sep-2019 15:00	12-Sep-2019 22:00	14.0	8		false	0.1
			SOC-LIVE-TI-SPL-UC-MISP_Emails_Hit		19-Sep-2019 13:00	22-Sep-2019 22:00	13.3	8		false	0.1
							97.5	51			0.8999999999999999

Message from the J.A.R.V.I.S. Stack

Hi Peter, J.A.R.V.I.S. rule Syntax Checks has fired for your usecase SOC-MON-Alert_Triage_Platform_Populate_Index_Results.

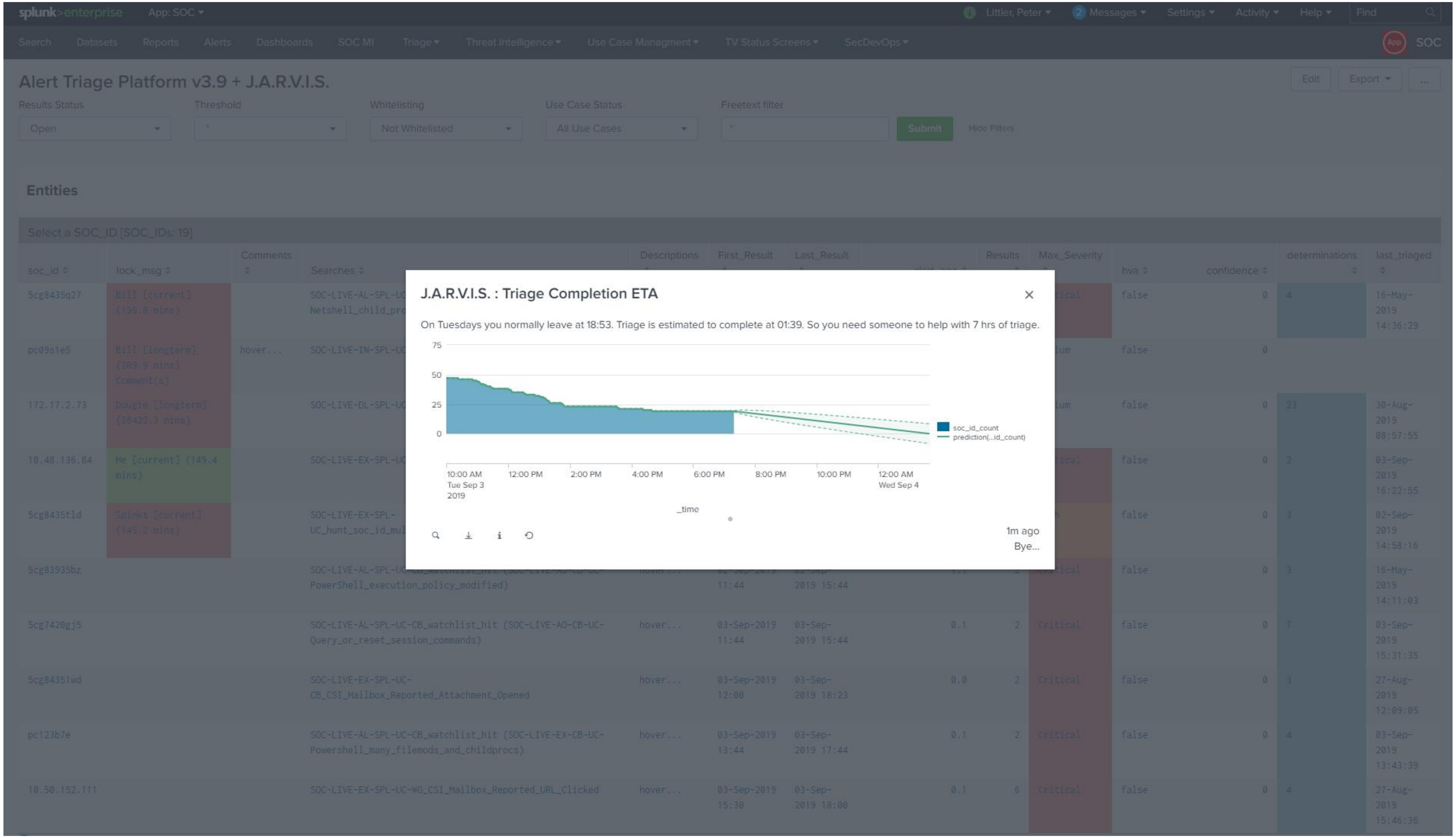
Take Me There...



Message from the J.A.R.V.I.S. Stack

Hi Peter, J.A.R.V.I.S. rule Syntax Checks has fired for your usecase SOC-MON-Alert_Triage_Platform_Populate_Index_Results.

Take Me There...



Alert Triage Platform v3.9 + J.A.R.V.I.S.

Results Status: Open

Threshold: *

Whitelisting: Not Whitelisted

Use Case Status: All Use Cases

Freetext filter: *

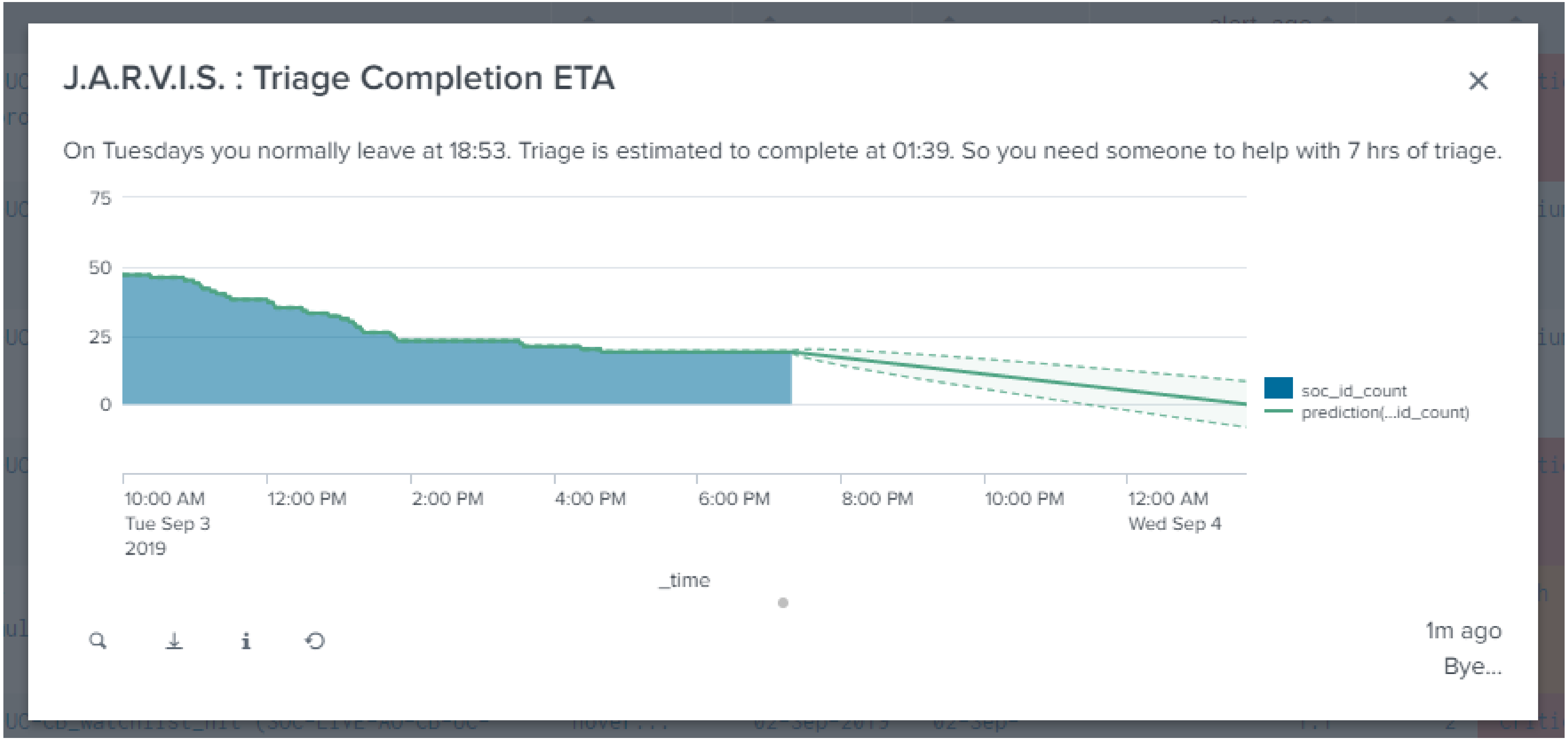
Entities

Select a SOC_ID [SOC_IDs: 19]

J.A.R.V.I.S. : Triage Completion ETA

On Tuesdays you normally leave at 18:53. Triage is estimated to complete at 01:39. So you need someone to help with 7 hrs of triage.

soc_id	lock_msg	Comments	Searches	Descriptions	First_Result	Last_Result		Results	Max_Severity	hva	confidence	determinations	last_triaged
5cg8435q27	Bill [current] (196.8 mins)		SOC-LIVE-AL-SPL-UC Netshell_child_pro						tical	false	0	4	16-May-2019 14:36:29
pc09s1e5	Bill [longterm] (209.9 mins) Comment(s)	hover...	SOC-LIVE-IN-SPL-UC						ium	false	0		
172.17.2.73	Dougie [longterm] (28422.3 mins)		SOC-LIVE-DL-SPL-UC						ium	false	0	23	30-Aug-2019 08:57:55
10.48.136.84	Me [current] (149.4 mins)		SOC-LIVE-EX-SPL-UC						tical	false	0	2	03-Sep-2019 16:22:55
5cg8435tld	Spinks [current] (145.2 mins)		SOC-LIVE-EX-SPL-UC_hunt_soc_id_mul						h	false	0	3	02-Sep-2019 14:58:16
5cg83935bz			SOC-LIVE-AL-SPL-UC PowerShell_execution_policy_modified)		11:44	2019 15:44				false	0	3	16-May-2019 14:11:03
5cg7420gj5			SOC-LIVE-AL-SPL-UC-CB_watchlist_hit (SOC-LIVE-AO-CB-UC-Query_or_reset_session_commands)	hover...	03-Sep-2019 11:44	03-Sep-2019 15:44	0.1	2	Critical	false	0	7	03-Sep-2019 15:31:35
5cg84351wd			SOC-LIVE-EX-SPL-UC-CB_CSI_Mailbox_Reported_Attachment_Opened	hover...	03-Sep-2019 12:00	03-Sep-2019 18:23	0.0	2	Critical	false	0	3	27-Aug-2019 12:09:05
pc123b7e			SOC-LIVE-AL-SPL-UC-CB_watchlist_hit (SOC-LIVE-EX-CB-UC-Powershell_many_filemods_and_childprocs)	hover...	03-Sep-2019 13:44	03-Sep-2019 17:44	0.1	2	Critical	false	0	4	03-Sep-2019 13:43:39
10.50.152.111			SOC-LIVE-EX-SPL-UC-WG_CSI_Mailbox_Reported_URL_Clicked	hover...	03-Sep-2019 15:30	03-Sep-2019 18:00	0.1	6	Critical	false	0	4	27-Aug-2019 15:46:36



J.A.R.V.I.S. : Triage Completion ETA

On Tuesdays you normally leave at 18:53. Triage is estimated to complete at 01:39. So you need someone to help with 7 hrs of triage.

1m ago

Bye...

How it's made

Some techniques we found useful

1. Scheduled, Dashboard, and JS initiated searches.
2. KVStore and JS callbacks to allow pop-ups in any dash, anytime.
3. Enhanced Modals to show search results.
4. 3rd party JavaScript implementation of Clippy.
5. **PREDICT** function for estimating future events.

Takeaways

1. Think about how to make information more accessible to your users within their normal workflows (without pivoting to other tools)

2. Splunk contains a lot of data about how we interact with it – use that to streamline your operations

References

Some sources we used

KVStores & Dashboards:

http://dev.splunk.com/view/webframework-tutorials/SP-CAAAEZT

Modals:

https://www.hurricanelabs.com/splunk-tutorials/splunk-custom-modal-view-creation-part-1-revealing-a-path-toward-enhanced-visibility-and-functionality

JavaScript Clippy:

https://www.smore.com/clippy-js

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION