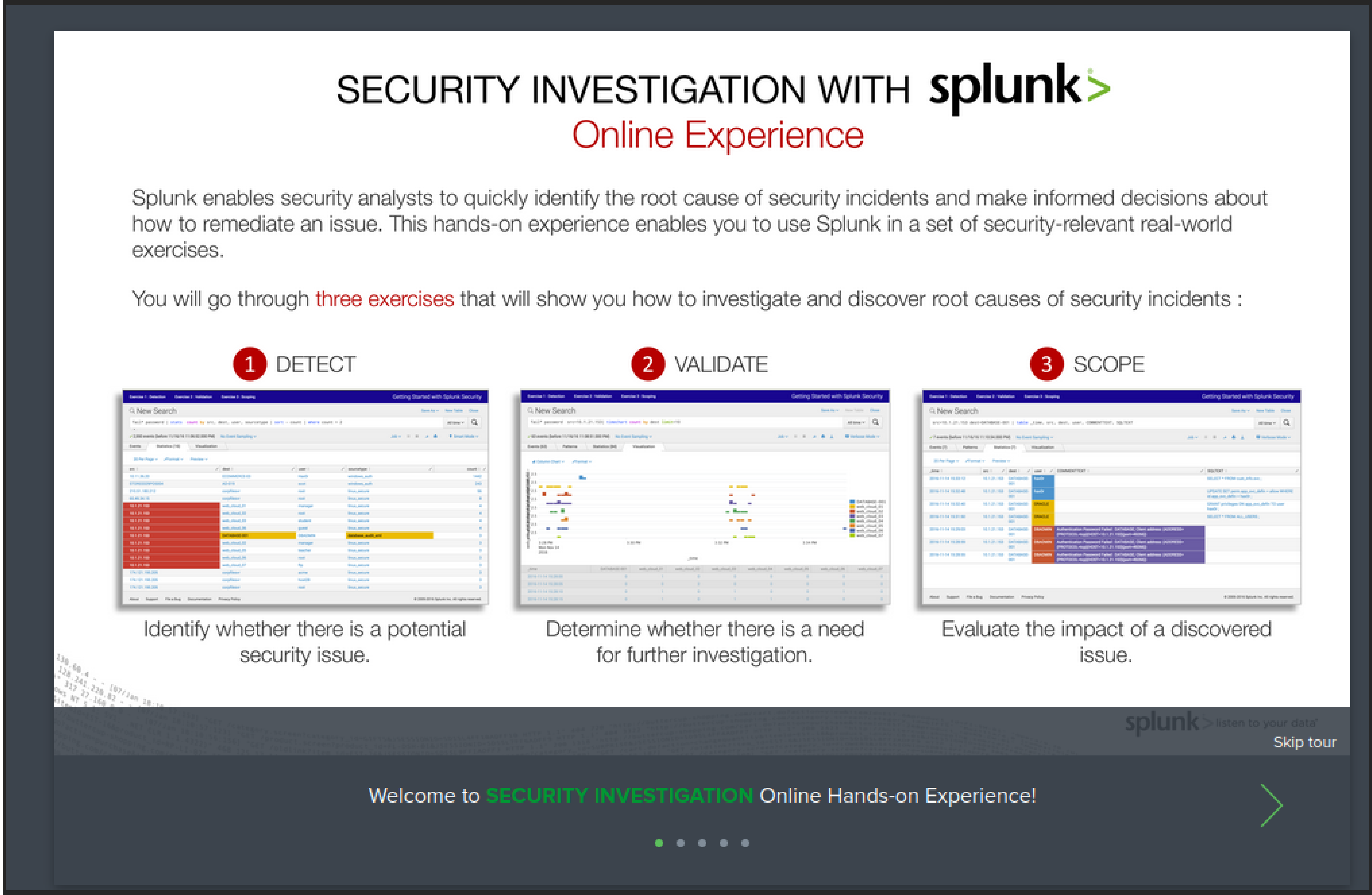
Splunk1

Here we go!

Splunk for Security Investigation: Threat Detection



SECURITY INVESTIGATION WITH splunk>

Online Experience

Splunk enables security analysts to quickly identify the root cause of security incidents and make informed decisions about how to remediate an issue. This hands-on experience enables you to use Splunk in a set of security-relevant real-world exercises.

You will go through three exercises that will show you how to investigate and discover root causes of security incidents :

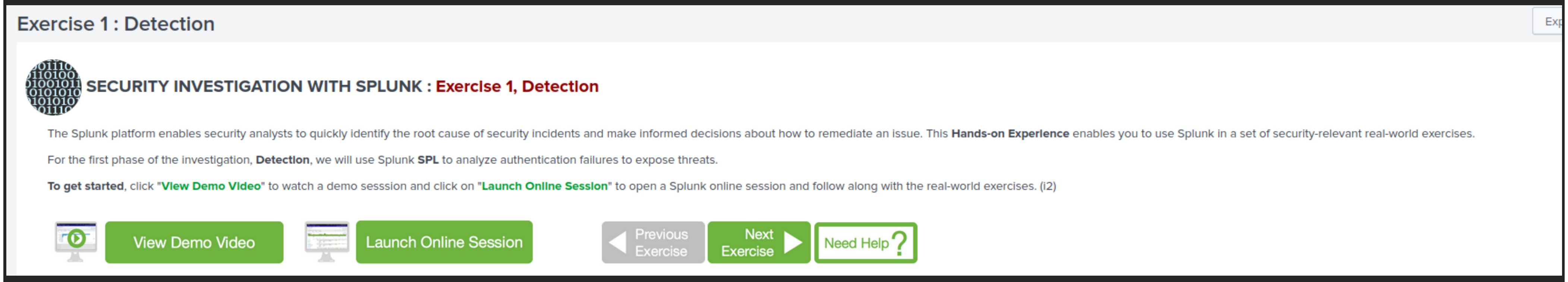
1 DETECT – Identify whether there is a potential security issue.

2 VALIDATE – Determine whether there is a need for further investigation.

3 SCOPE – Evaluate the impact of a discovered issue.

Welcome to SECURITY INVESTIGATION Online Hands-on Experience!

Exercise 1 : Detection



Exercise 1 : Detection

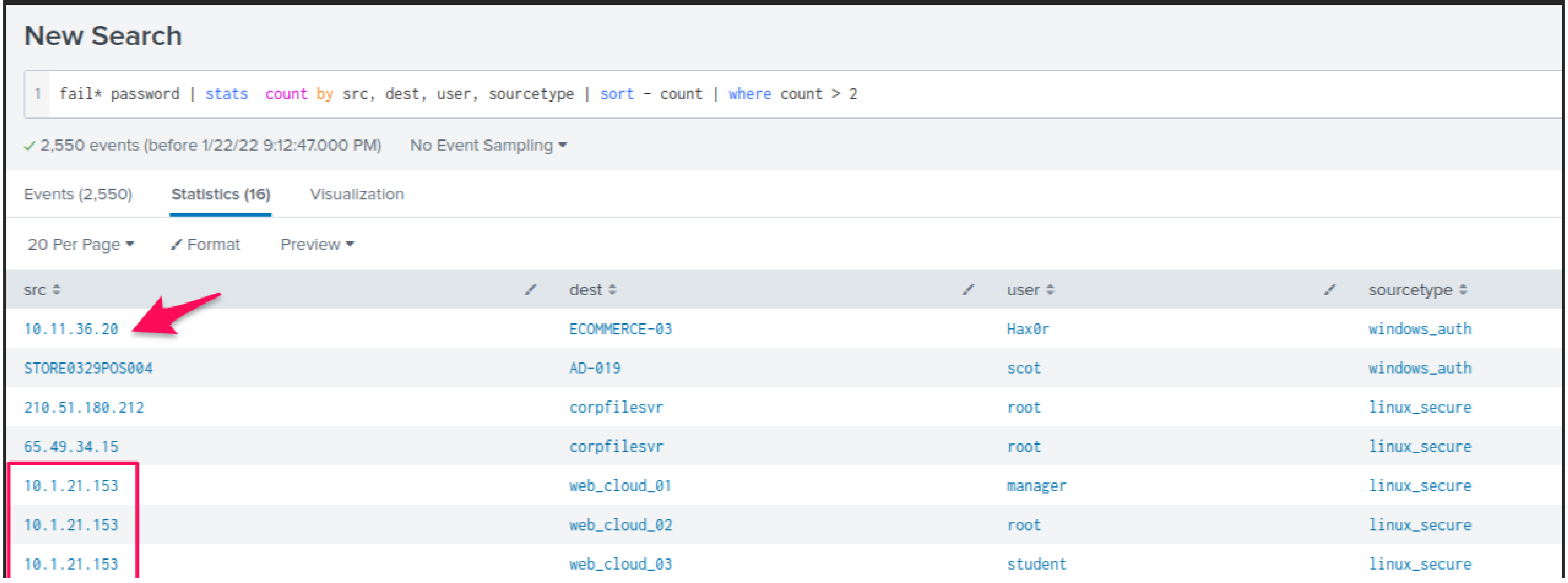
SECURITY INVESTIGATION WITH SPLUNK : Exercise 1, Detection

The Splunk platform enables security analysts to quickly identify the root cause of security incidents and make informed decisions about how to remediate an issue. This **Hands-on Experience** enables you to use Splunk in a set of security-relevant real-world exercises.

For the first phase of the investigation, **Detection**, we will use Splunk **SPL** to analyze authentication failures to expose threats.

To get started, click "**View Demo Video**" to watch a demo sesssion and click on "**Launch Online Session**" to open a Splunk online session and follow along with the real-world exercises. (i2)

fail* password | stats count by src, dest, user, sourcetype | sort - count | where count > 2

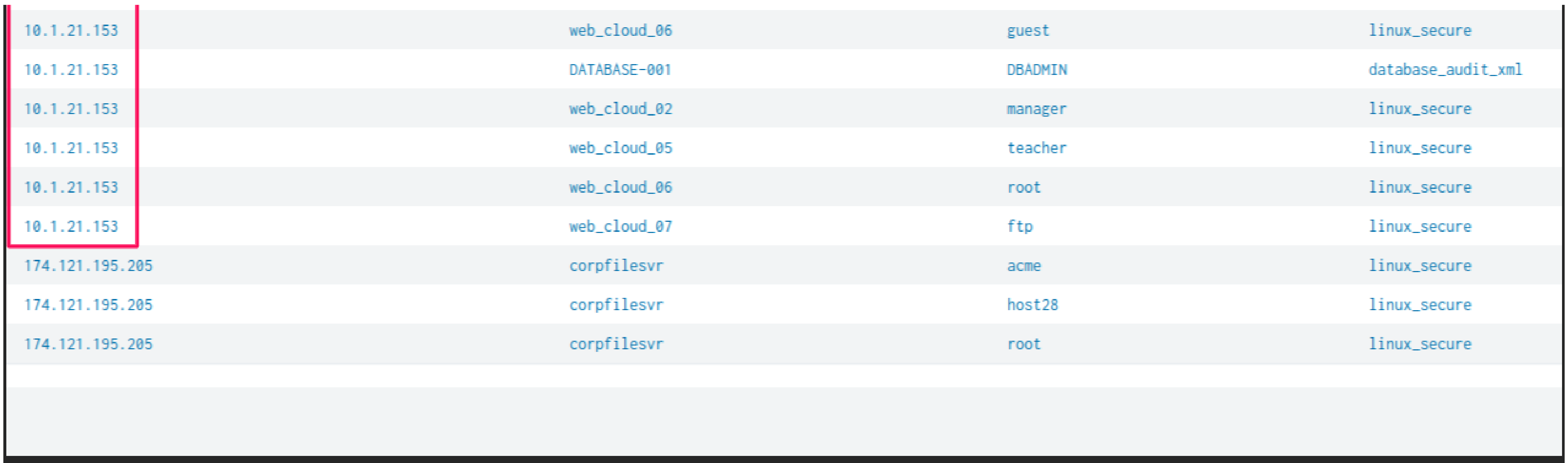


New Search

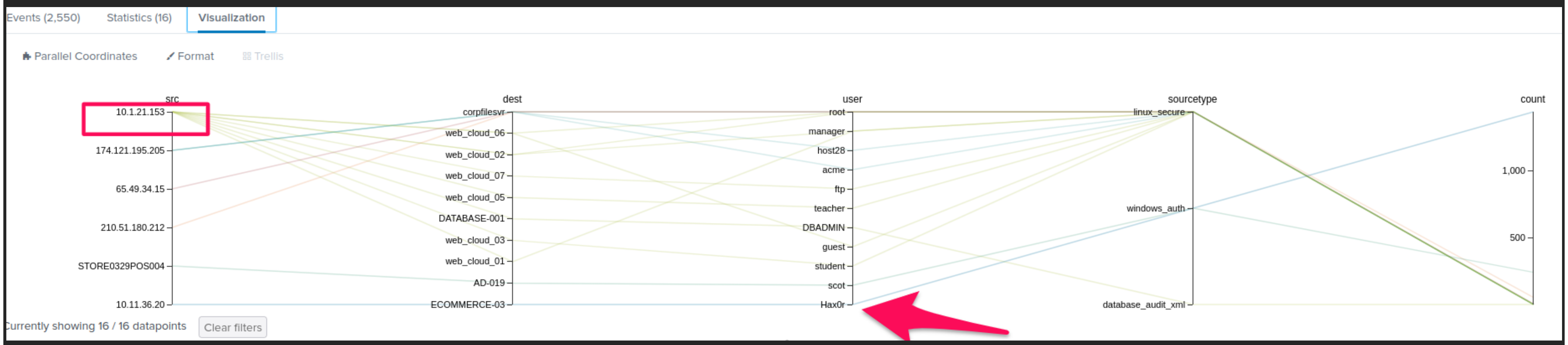
```
fail* password | stats  count by src, dest, user, sourcetype | sort - count | where count > 2
```

✓ 2,550 events (before 1/22/22 9:12:47.000 PM)   No Event Sampling ▾

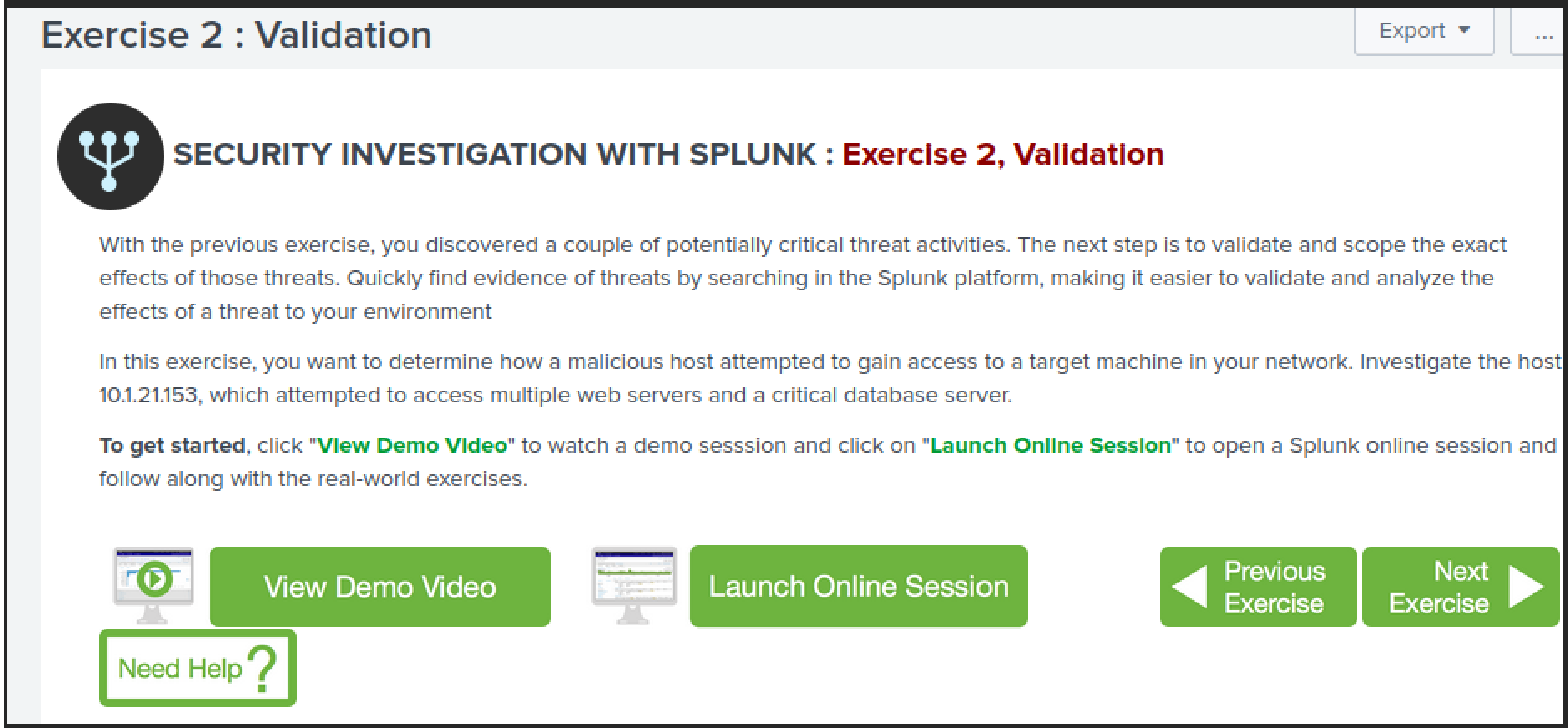
src	dest	user	sourcetype
10.11.36.20	ECOMMERCE-03	Hax0r	windows_auth
STORE0329POS004	AD-019	scot	windows_auth
210.51.180.212	corpfilesvr	root	linux_secure
65.49.34.15	corpfilesvr	root	linux_secure
10.1.21.153	web_cloud_01	manager	linux_secure
10.1.21.153	web_cloud_02	root	linux_secure
10.1.21.153	web_cloud_03	student	linux_secure



10.1.21.153	web_cloud_06	guest	linux_secure
10.1.21.153	DATABASE-001	DBADMIN	database_audit_xml
10.1.21.153	web_cloud_02	manager	linux_secure
10.1.21.153	web_cloud_05	teacher	linux_secure
10.1.21.153	web_cloud_06	root	linux_secure
10.1.21.153	web_cloud_07	ftp	linux_secure
174.121.195.205	corpfilesvr	acme	linux_secure
174.121.195.205	corpfilesvr	host28	linux_secure
174.121.195.205	corpfilesvr	root	linux_secure



Exercise 2 : Validation



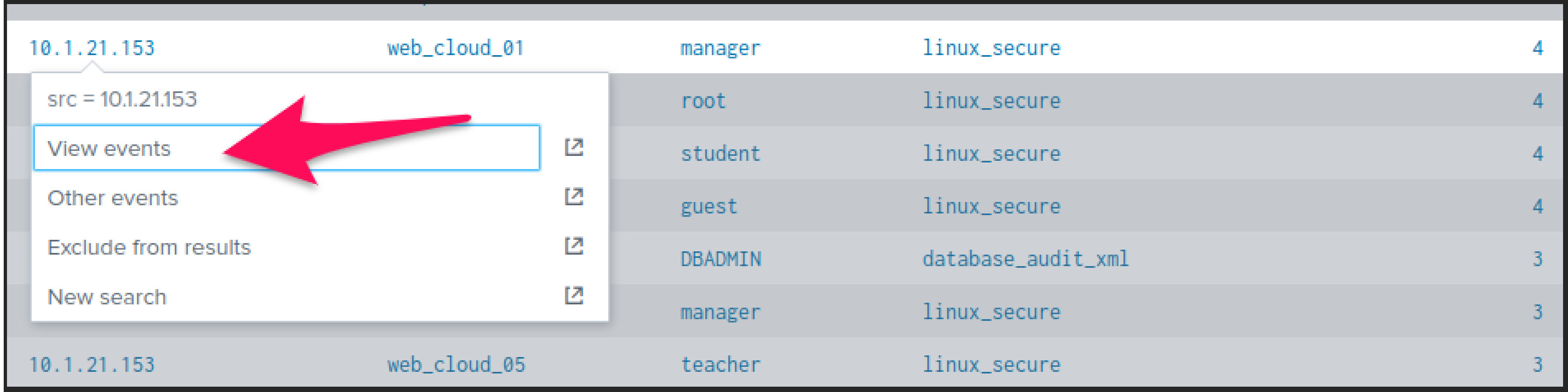
Exercise 2 : Validation

SECURITY INVESTIGATION WITH SPLUNK : Exercise 2, Validation

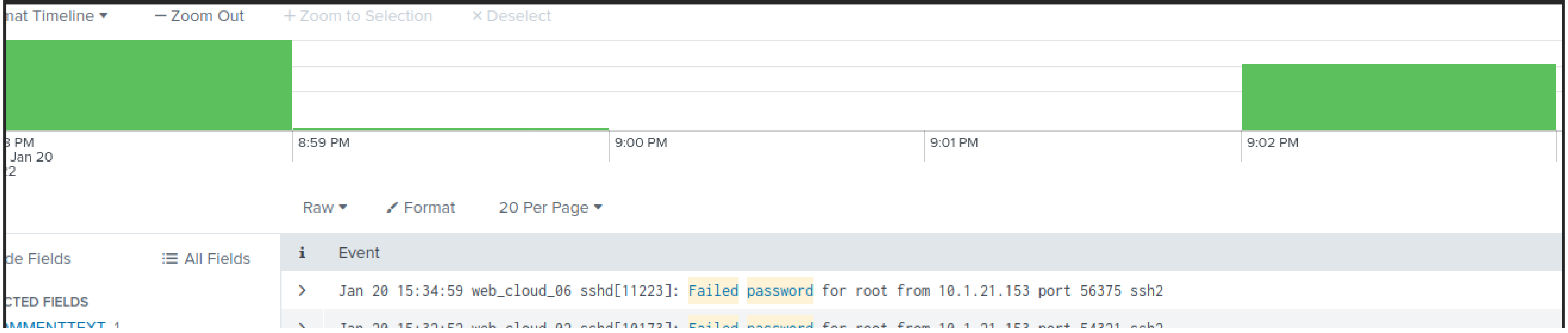
With the previous exercise, you discovered a couple of potentially critical threat activities. The next step is to validate and scope the exact effects of those threats. Quickly find evidence of threats by searching in the Splunk platform, making it easier to validate and analyze the effects of a threat to your environment

In this exercise, you want to determine how a malicious host attempted to gain access to a target machine in your network. Investigate the host 10.1.21.153, which attempted to access multiple web servers and a critical database server.

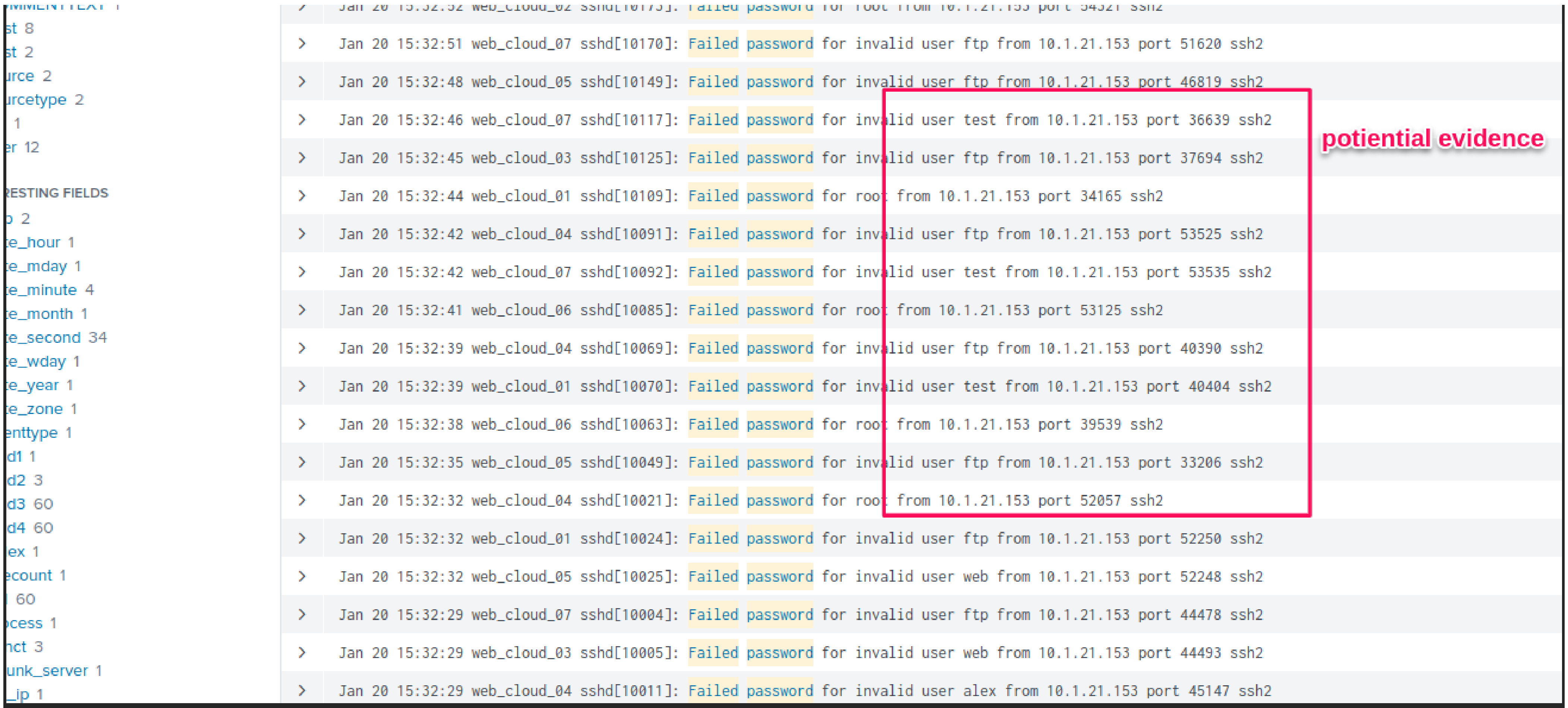
To get started, click "**View Demo Video**" to watch a demo sesssion and click on "**Launch Online Session**" to open a Splunk online session and follow along with the real-world exercises.



10.1.21.153	web_cloud_01	manager	linux_secure	4
		root	linux_secure	4
		student	linux_secure	4
		guest	linux_secure	4
		DBADMIN	database_audit_xml	3
		manager	linux_secure	3
10.1.21.153	web_cloud_05	teacher	linux_secure	3

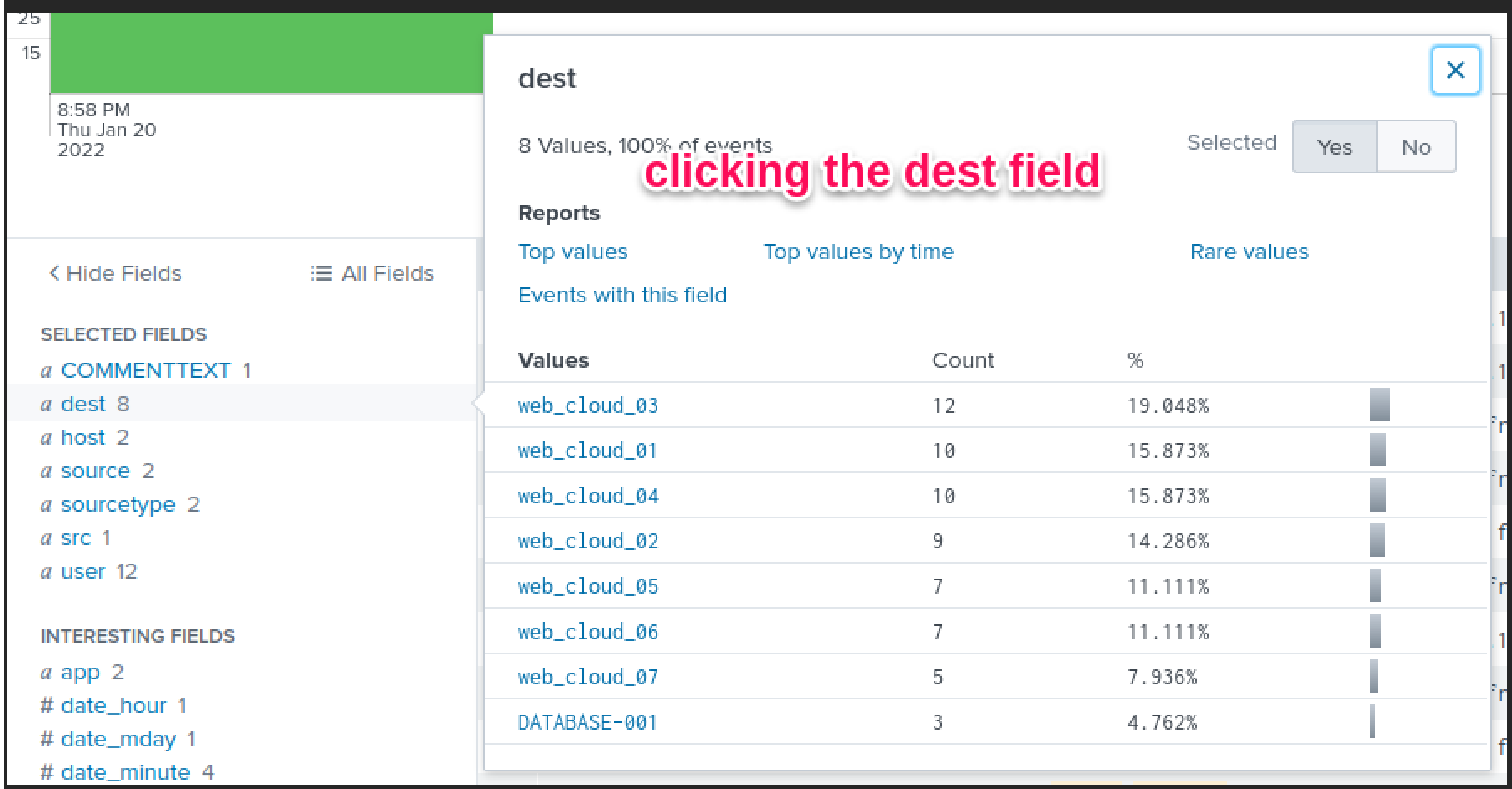


```
> Jan 20 15:34:59 web_cloud_06 sshd[11223]: Failed password for root from 10.1.21.153 port 56375 ssh2
> Jan 20 15:32:52 web_cloud_02 sshd[10173]: Failed password for root from 10.1.21.153 port 54321 ssh2
```



```
Jan 20 15:32:52 web_cloud_02 sshd[10173]: Failed password for root from 10.1.21.153 port 54321 ssh2
Jan 20 15:32:51 web_cloud_07 sshd[10170]: Failed password for invalid user ftp from 10.1.21.153 port 51620 ssh2
Jan 20 15:32:48 web_cloud_05 sshd[10149]: Failed password for invalid user ftp from 10.1.21.153 port 46819 ssh2
Jan 20 15:32:46 web_cloud_07 sshd[10117]: Failed password for invalid user test from 10.1.21.153 port 36639 ssh2
Jan 20 15:32:45 web_cloud_03 sshd[10125]: Failed password for invalid user ftp from 10.1.21.153 port 37694 ssh2
Jan 20 15:32:44 web_cloud_01 sshd[10109]: Failed password for root from 10.1.21.153 port 34165 ssh2
Jan 20 15:32:42 web_cloud_04 sshd[10091]: Failed password for invalid user ftp from 10.1.21.153 port 53525 ssh2
Jan 20 15:32:42 web_cloud_07 sshd[10092]: Failed password for invalid user test from 10.1.21.153 port 53535 ssh2
Jan 20 15:32:41 web_cloud_06 sshd[10085]: Failed password for root from 10.1.21.153 port 53125 ssh2
Jan 20 15:32:39 web_cloud_04 sshd[10069]: Failed password for invalid user ftp from 10.1.21.153 port 40390 ssh2
Jan 20 15:32:39 web_cloud_01 sshd[10070]: Failed password for invalid user test from 10.1.21.153 port 40404 ssh2
Jan 20 15:32:38 web_cloud_06 sshd[10063]: Failed password for root from 10.1.21.153 port 39539 ssh2
Jan 20 15:32:35 web_cloud_05 sshd[10049]: Failed password for invalid user ftp from 10.1.21.153 port 33206 ssh2
Jan 20 15:32:32 web_cloud_04 sshd[10021]: Failed password for root from 10.1.21.153 port 52057 ssh2
Jan 20 15:32:32 web_cloud_01 sshd[10024]: Failed password for invalid user ftp from 10.1.21.153 port 52250 ssh2
Jan 20 15:32:32 web_cloud_05 sshd[10025]: Failed password for invalid user web from 10.1.21.153 port 52248 ssh2
Jan 20 15:32:29 web_cloud_07 sshd[10004]: Failed password for invalid user ftp from 10.1.21.153 port 44478 ssh2
Jan 20 15:32:29 web_cloud_03 sshd[10005]: Failed password for invalid user web from 10.1.21.153 port 44493 ssh2
Jan 20 15:32:29 web_cloud_04 sshd[10011]: Failed password for invalid user alex from 10.1.21.153 port 45147 ssh2
```

potiential evidence



dest ✕

8 Values, 100% of events

Selected [✓ Yes] No

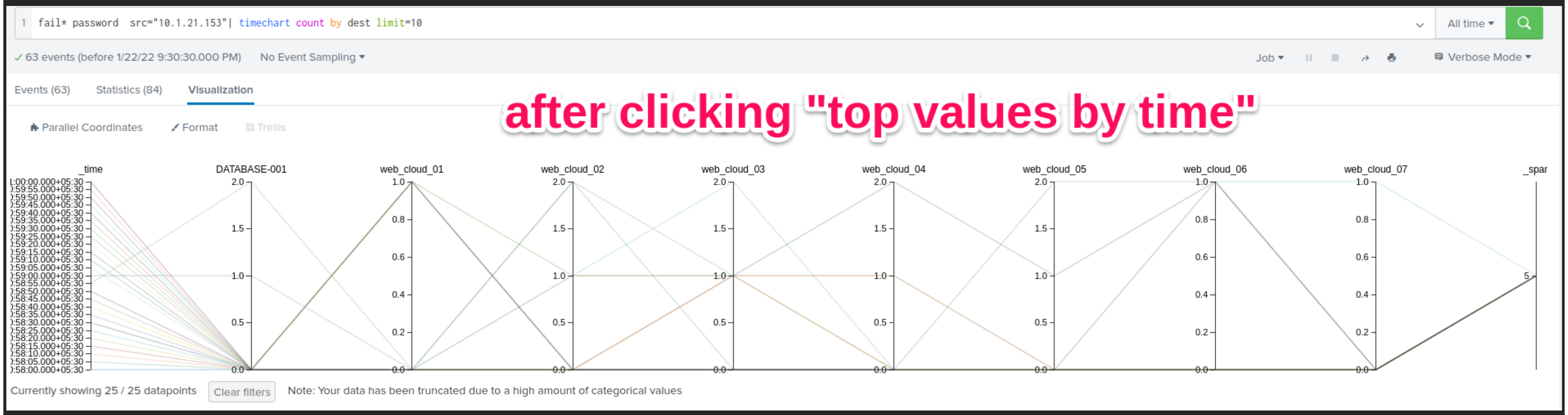
clicking the dest field

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
web_cloud_03	12	19.048%
web_cloud_01	10	15.873%
web_cloud_04	10	15.873%
web_cloud_02	9	14.286%
web_cloud_05	7	11.111%
web_cloud_06	7	11.111%
web_cloud_07	5	7.936%
DATABASE-001	3	4.762%



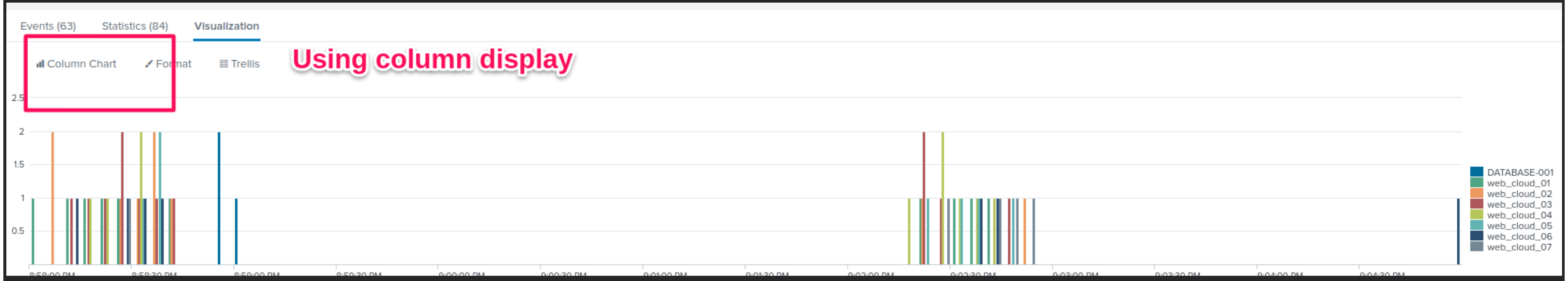
```
fail* password  src="10.1.21.153"| timechart count by dest limit=10
```

✓ 63 events (before 1/22/22 9:30:30.000 PM) No Event Sampling ▾

after clicking "top values by time"

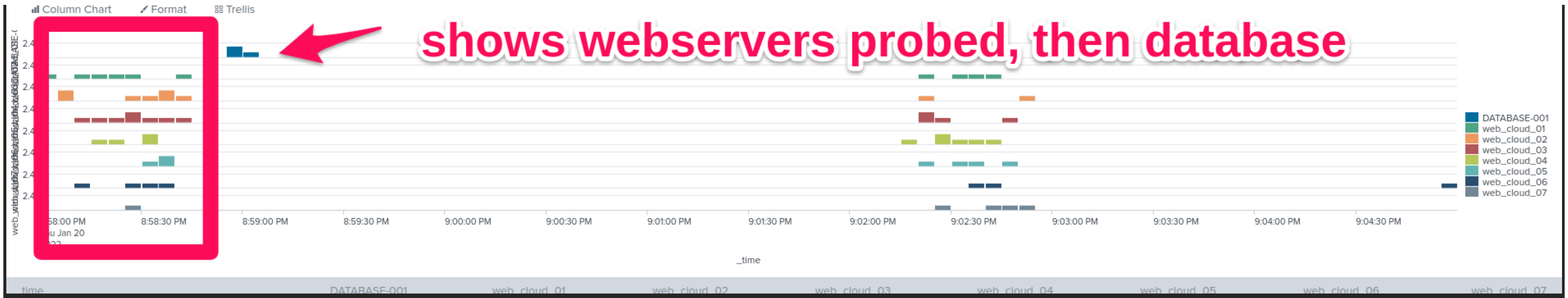
Currently showing 25 / 25 datapoints

Note: Your data has been truncated due to a high amount of categorical values



Using column display

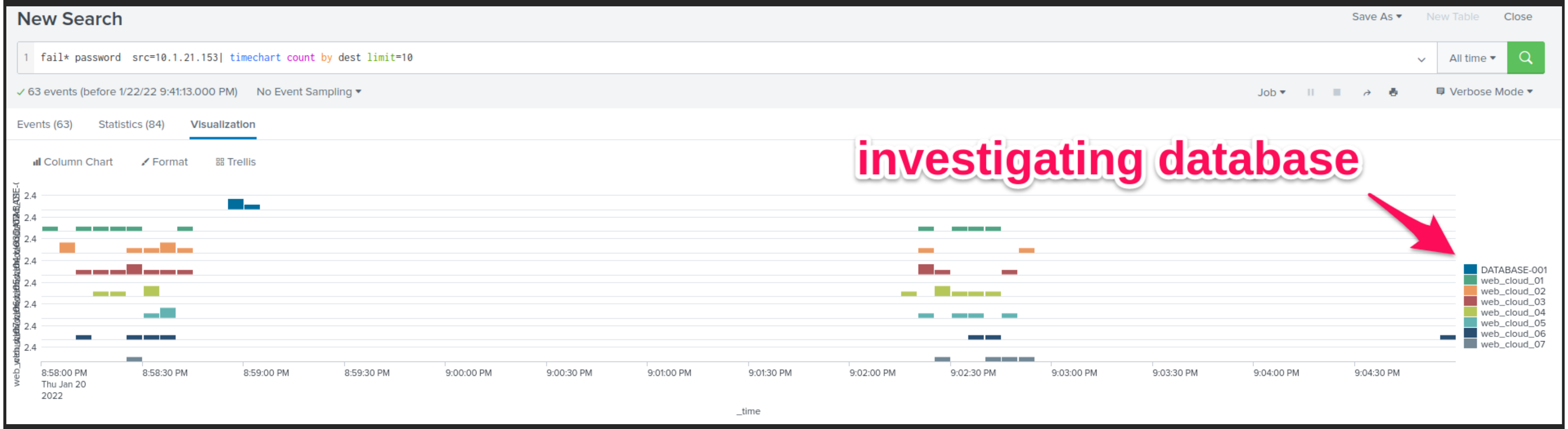
In format > multi-series mode



shows webservers probed, then database

Exercise 3 : Scoping

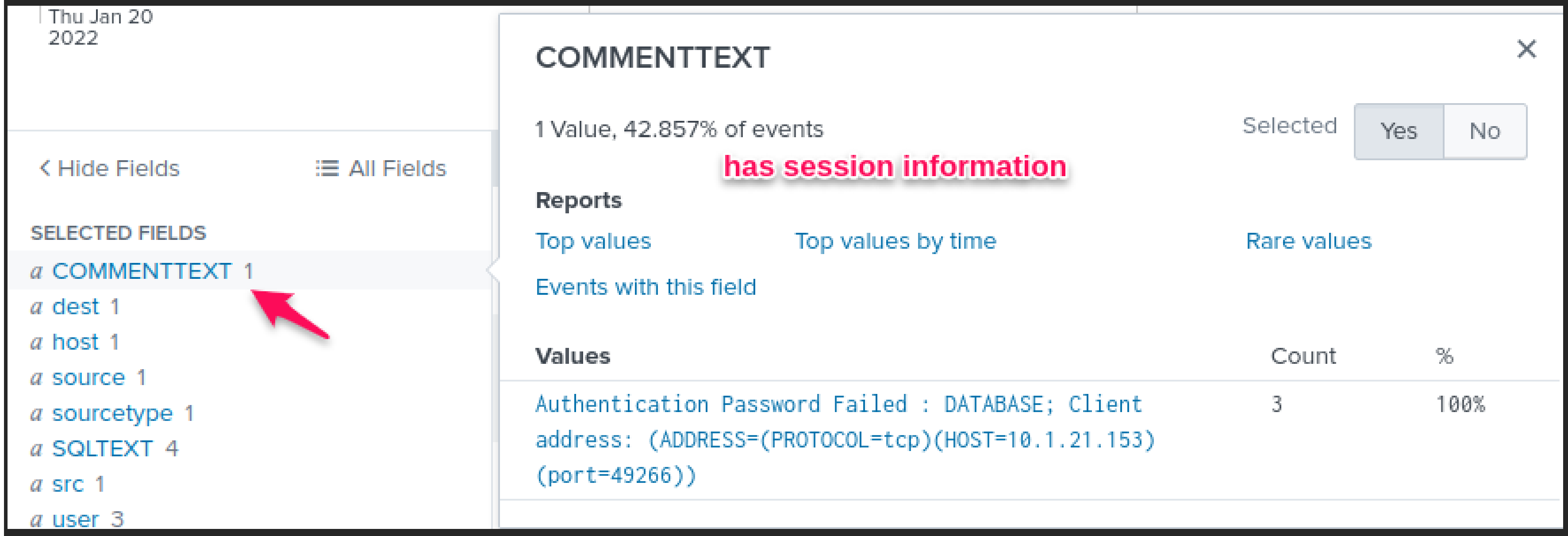
Splunk for Security Investigation: Threat Scoping



```
fail* password  src=10.1.21.153| timechart count by dest limit=10
```

✓ 63 events (before 1/22/22 9:41:13.000 PM) No Event Sampling ▾

investigating database



Thu Jan 20
2022

< Hide Fields ☰ All Fields

SELECTED FIELDS

- a COMMENTTEXT 1
- a dest 1
- a host 1
- a source 1
- a sourcetype 1
- a SQLTEXT 4
- a src 1
- a user 3

COMMENTTEXT ✕

1 Value, 42.857% of events

Selected Yes No

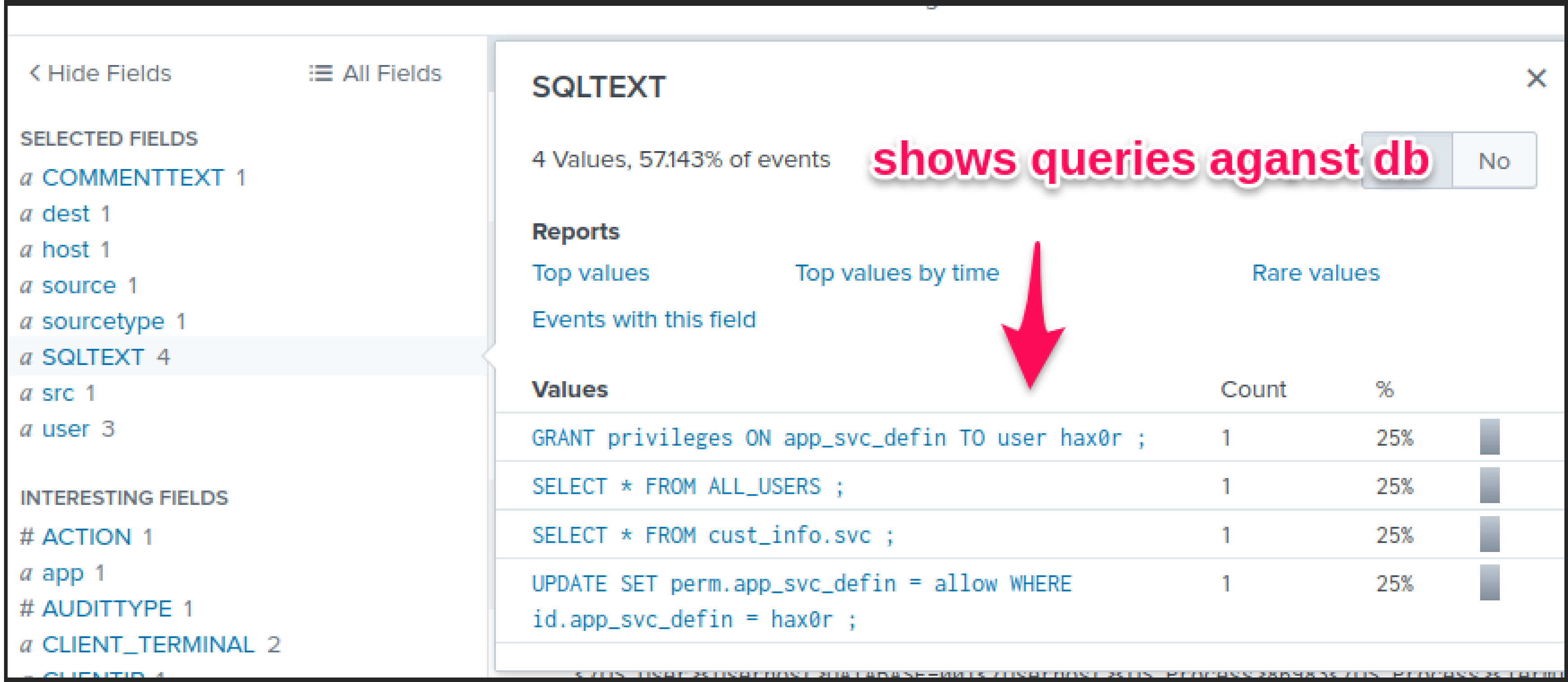
has session information

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Authentication Password Failed : DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.1.21.153)(port=49266))	3	100%



< Hide Fields ☰ All Fields

SELECTED FIELDS

- a COMMENTTEXT 1
- a dest 1
- a host 1
- a source 1
- a sourcetype 1
- a SQLTEXT 4
- a src 1
- a user 3

INTERESTING FIELDS

- # ACTION 1
- a app 1
- # AUDITTYPE 1
- a CLIENT_TERMINAL 2

SQLTEXT ✕

4 Values, 57.143% of events

shows queries aganst db

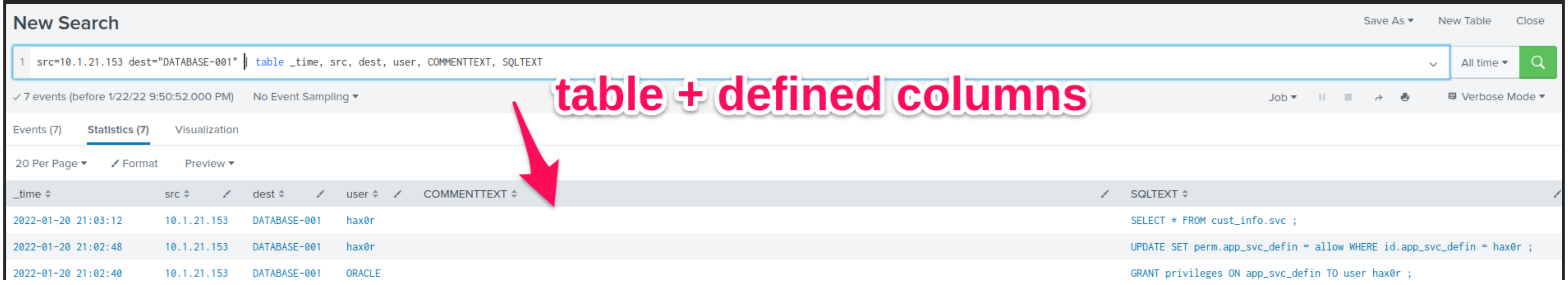
No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
GRANT privileges ON app_svc_defin TO user hax0r ;	1	25%
SELECT * FROM ALL_USERS ;	1	25%
SELECT * FROM cust_info.svc ;	1	25%
UPDATE SET perm.app_svc_defin = allow WHERE id.app_svc_defin = hax0r ;	1	25%

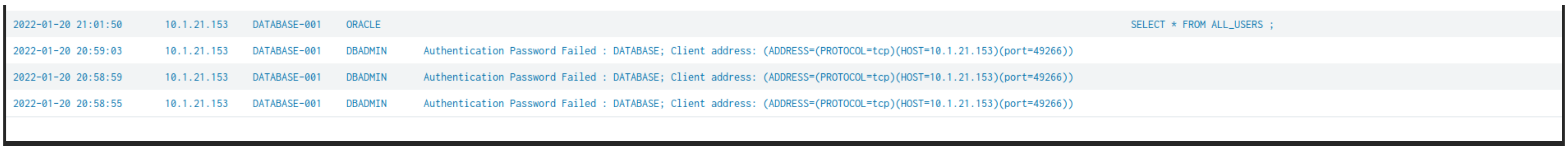


```
src=10.1.21.153 dest="DATABASE-001" | table _time, src, dest, user, COMMENTTEXT, SQLTEXT
```

✓ 7 events (before 1/22/22 9:50:52.000 PM) No Event Sampling ▾

table + defined columns

_time	src	dest	user	COMMENTTEXT	SQLTEXT
2022-01-20 21:03:12	10.1.21.153	DATABASE-001	hax0r		SELECT * FROM cust_info.svc ;
2022-01-20 21:02:48	10.1.21.153	DATABASE-001	hax0r		UPDATE SET perm.app_svc_defin = allow WHERE id.app_svc_defin = hax0r ;
2022-01-20 21:02:40	10.1.21.153	DATABASE-001	ORACLE		GRANT privileges ON app_svc_defin TO user hax0r ;



```
2022-01-20 21:01:50   10.1.21.153   DATABASE-001   ORACLE                                                                                                                    SELECT * FROM ALL_USERS ;
2022-01-20 20:59:03   10.1.21.153   DATABASE-001   DBADMIN   Authentication Password Failed : DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.1.21.153)(port=49266))
2022-01-20 20:58:59   10.1.21.153   DATABASE-001   DBADMIN   Authentication Password Failed : DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.1.21.153)(port=49266))
2022-01-20 20:58:55   10.1.21.153   DATABASE-001   DBADMIN   Authentication Password Failed : DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.1.21.153)(port=49266))
```

^Shows user "hax0r" logged in as ORACLE and escalated to DBADMIN