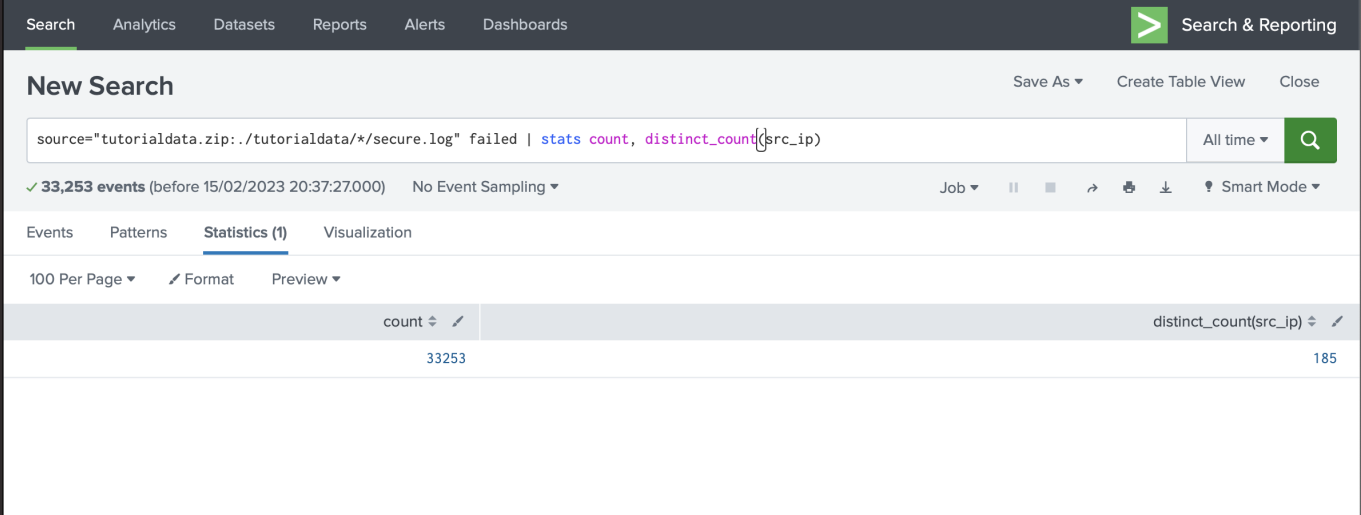


Activity 1: Can you find people trying to break into the servers?

1.1 How many hackers are trying to get access to our servers? And how many attempts are there?

Ans.

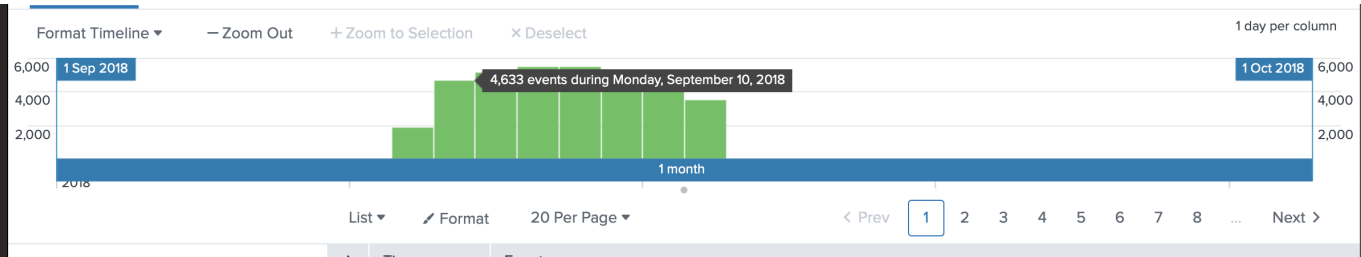
There is 185 hackers and 33253 times. using extra field by using regex (?P<src\_ip>[^ ]+) port (?P<src\_port>\d+)



1.2 What time do hackers appear to try to hack our servers?

Ans.

The hacking starts from 9 September to 17 September on every 12.15.05



1.3 Which server (mailsv, www1, www2, www3) seem to see the most attempts?

Ans.

www1 has the most attempts with 8798 attempts

source

4 Values, 100% of events

Selected

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%	
tutorialdata.zip:./tutorialdata/www1/secure.log	8,798	26.458%	<div></div>
tutorialdata.zip:./tutorialdata/www3/secure.log	8,267	24.861%	<div></div>
tutorialdata.zip:./tutorialdata/mailsv/secure.log	8,154	24.521%	<div></div>
tutorialdata.zip:./tutorialdata/www2/secure.log	8,034	24.16%	<div></div>

1.4 What is the most popular account that hackers use to try to break in?

Ans.

The most popular account is 10.3.10.46

## username

>100 Values, 86.939% of events

**Reports**

[Top values](#)
[Top values by time](#)
[Rare values](#)

[Events with this field](#)

×

Selected

Yes

No

Top 10 Values	Count	%
10.3.10.46	1,076	3.087%
administrator	1,020	2.927%
admin	938	2.691%
operator	923	2.648%
mailman	752	2.158%
irc	644	1.848%
email	626	1.796%
sys	586	1.681%
system	581	1.667%

## Activity 2: Sensitive Files on Web Servers

2.1 Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?

Ans. There are 2 files that are sensitive which are password.pdf (51 times for GET method) and anna\_nicole.html (62 times for GET method)

uri\_path

14 Values, 100% of events

Selected

**Reports**

Top values      Top values by time      Rare values

Events with this field

Top 10 Values	Count	%
/cart.do	12,653	32.007%
/product.screen	9,932	25.124%
/category.screen	6,885	17.416%
/oldlink	6,871	17.381%
/cart/success.do	2,154	5.449%
/cart/error.do	427	1.08%
show.do	90	0.228%
/stuff/logo.ico	84	0.212%
/productscreen.html	82	0.207%
/hidden/anna_nicole.html	73	0.185%

**New Search** Save As Create Table

source="tutorialdata.zip:./tutorialdata/\*/access.log" GET | stats count by file, uri\_path

✓ 24,866 events (before 15/02/2023 21:43:46.000) No Event Sampling

Job ⏏ ⏏ ⏏ ⏏ ⏏ ⏏

Events   Patterns   **Statistics (12)**   Visualization

100 Per Page ✎ Format Preview

file	uri_path
anna_nicole.html	/hidden/anna_nicole.html
cart.do	/cart.do
category.screen	/category.screen

## 2.2 What resource/file are hackers looking for?

Ans.

password.pdf and anna\_nicole.html which is located in hidden folder.

## Activity 3: (Optional)

Are there bots crawling our websites?

Ans.

Yes

3.2 Can you find any bots crawling our websites?

Yes, there are 2 bots which are YandexBot and GoogleBot

Events	Patterns	Statistics (4)	Visualization
100 Per Page ▾	✎ Format	Preview ▾	
useragent ⇅			count ⇅ ✎
Googlebot/2.1 ( http://www.googlebot.com/bot.html)			495
Googlebot/2.1 (http://www.googlebot.com/bot.html)			439
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)			532
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)			383