



Day 14 - Create Alerts and Dashboards in Kibana

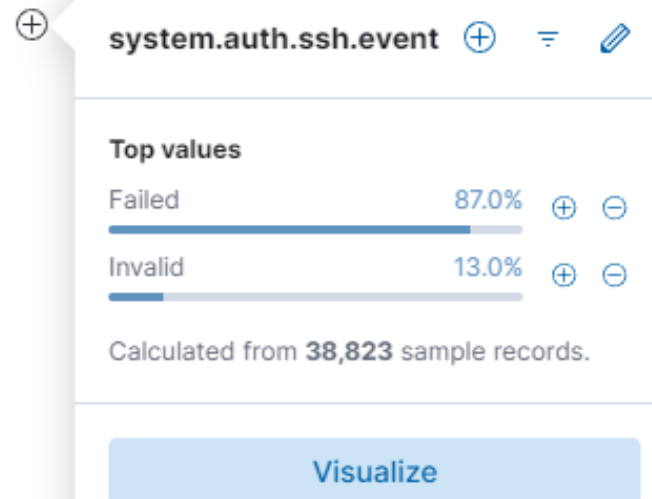
Obiettivo

- **Creare un alert per attività di Brute Force rilevate sul server Ubuntu (e capire da dove vengono)**

Creazione Alert e Dashboard per Attacchi Brute Force

Per prima cosa cerchiamo per campi quali: 'failed attempts', 'user', 'source ip'. Potremmo partire da un campo che comprende uno di questi, per cui lo includeremo nei risultati che filtriamo sul discover di **Kibana**, per evitare di avere dei record dove non c'è nulla filtriamo i dati in modo da ottenere il record solo se c'è il valore ('exists in any form').

- system.auth.ssh.event
- system.auth.ssh.method
- system.auth.sudo.command
- system.auth.sudo.pwd
- system.auth.sudo.tty
- system.auth.sudo.user
- system.auth.useradd.home
- system.auth.useradd.shell
- tags
- unit.id



system.auth.ssh.event

system.auth.ssh.event

: equals some value

: * exists in any form

Creazione Alert e Dashboard per Attacchi Brute Force

Qui aggiungiamo un campo che includa users. Mancano i source ip.

Oltre a questi aggiungeremo altri campi utili alla nostra ricerca.

Il risultato nella prossima slide

user.name



Top values

root	78.6%	+	-
ubuntu	1.1%	+	-
test	0.8%	+	-
test	0.8%	+	-
admin	0.7%	+	-
admin	0.7%	+	-
user	0.5%	+	-
user	0.5%	+	-
sysadmin	0.4%	+	-
sysadmin	0.4%	+	-
Other	15.5%		

Calculated from 5,000 sample records.

Multi fields

 user.name.text

Visualize

source.ip



Top values


167.71.224.199	73.5%	+	-
116.110.217.233	6.5%	+	-
40.117.97.0	1.7%	+	-
51.89.166.236	1.7%	+	-
190.104.135.18	1.7%	+	-
37.204.180.215	1.7%	+	-
111.67.194.81	1.5%	+	-
196.189.21.247	1.4%	+	-
45.118.146.109	1.3%	+	-
83.222.191.62	1.1%	+	-
Other	8.0%		

Calculated from 5,000 sample records.

Visualize

Creazione Alert e Dashboard per Attacchi Brute Force

Nel caso volessi filtrare solo per i risultati 'Failed' basta scorrere su col mouse e cliccare sul '+'.
+.




 <input type="checkbox"/> Sep 25, 2024 @ 17:50:13.000	<div><div><div>+</div><div>-</div><div>✓</div></div><div>iled</div></div>	root	167.71.224.199	India
--	---	------	----------------	-------

Documents (50,215) Field statistics

Get the best look at your search results

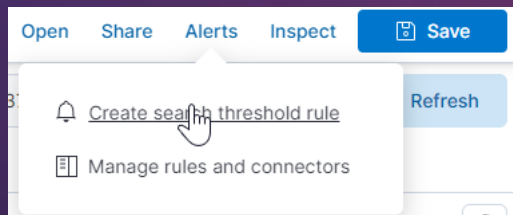
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tour Dismiss

@timestamp ⌚	↓ system.auth.ssh.event	user.name	source.ip	source.geo.country_name
 <input type="checkbox"/> Sep 25, 2024 @ 17:50:13.000	Failed	root	167.71.224.199	India
 <input type="checkbox"/> Sep 25, 2024 @ 17:50:08.000	Failed	root	167.71.224.199	India
 <input type="checkbox"/> Sep 25, 2024 @ 17:50:03.000	Failed	root	167.71.224.199	India

Creazione Alert e Dashboard per Attacchi Brute Force

Salviamo la ricerca cliccando su 'Save' in alto a destra, procediamo ora con la creazione di un alert a cui daremo un nome, selezioneremo poi le threshold per far scattare l'alert



Create rule

Define your query

+ ×

×

Set the group, threshold, and time window ⓘ

WHEN count()

OVER all documents

IS ABOVE 5

FOR THE LAST 5 hours

Set the number of documents to send ⓘ

SIZE 100

☐ Exclude matches from previous runs

Add more fields to alert details

× × × × ▼

▶ Test query

📄 Copy query

Query matched 0 documents in the last 5h.

Check every ⓘ

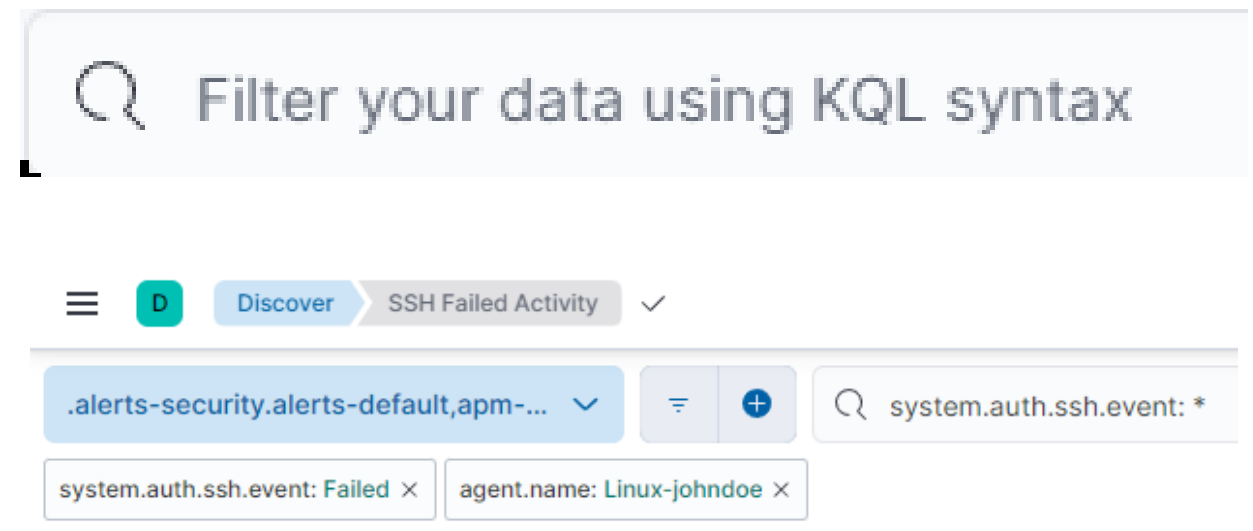
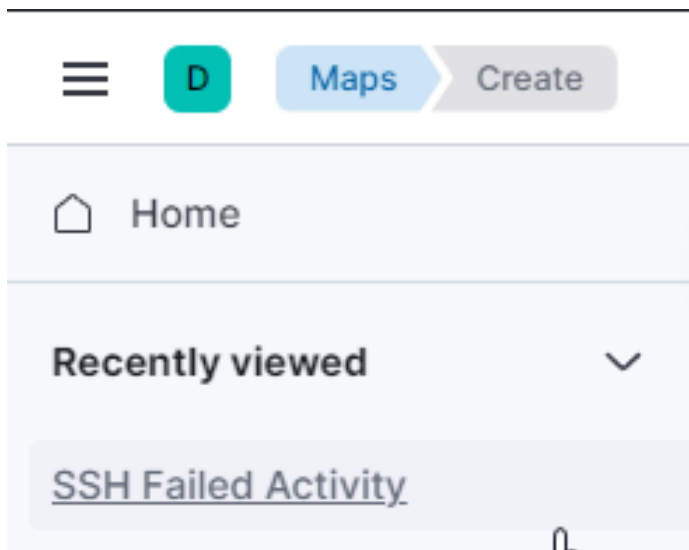
1

minute

▼

Creazione Alert e Dashboard per Attacchi Brute Force

Creiamo ora una dashboard per visualizzare i risultati della ricerca, clicchiamo su 'Maps' e nel campo di ricerca riporteremo la query appena elaborata più i filtri che abbiamo utilizzato.



Alert e Dashboard per Attacchi Brute Force

Selezioniamo 'Choropleth' come Layer per visualizzare le statistiche sulla mappa. In base al numero di entries, il colore della mappa sarà più o meno intenso.



Choropleth

Shade areas to compare statistics across boundaries

Boundaries source

- ☒ Administrative boundaries from the Elastic Maps Service
- ☐ Points, lines, and polygons from Elasticsearch

EMS boundaries

World Countries

Join field

ISO 3166-1 alpha-2 code

Statistics source

Data view

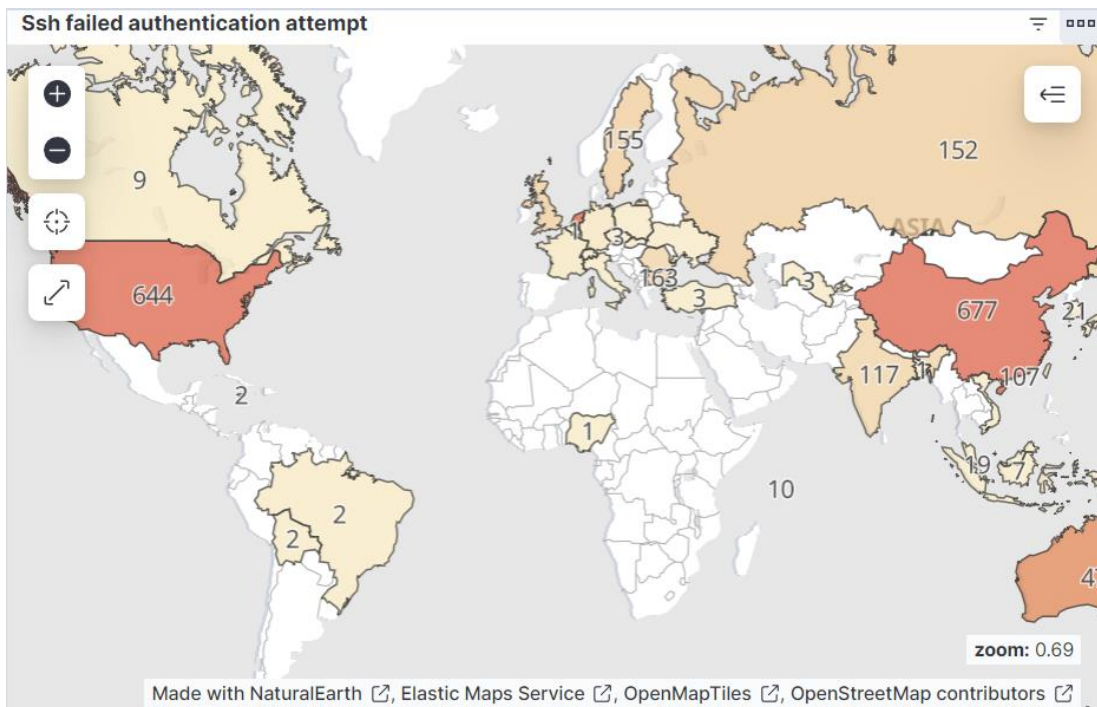
.alerts-security.alerts-default,apm-*-transaction*,audi...

Join field

source.geo.country_iso_code

Alert e Dashboard per Attacchi Brute Force

Dopo aver aggiunto il layer, possiamo visualizzare i risultati sulla mappa e ottenere diverse visualizzazioni in base all'intervallo temporale selezionato.



World Countries

> Source details

Layer settings

Name

Visibility ☐ Zoom levels 0 → 24

Opacity 75 %

☒ Include layer in fit to data bounds computation

☒ Show tooltips

[Discard changes](#)

[Remove layer](#)

[✓ Keep changes](#)