RICCARDO LEPORE

SPLUNK W24D4

The Last Project

Start

CREA UNA QUERY SPLUNK PER IDENTIFICARE TUTTI I TENTATIVI DI ACCESSO FALLITI "FAILED PASSWORD".
LA QUERY DOVREBBE MOSTRARE IL TIMESTAMP, L'INDIRIZZO IP DI ORIGINE, IL NOME UTENTE E IL MOTIVO DEL FALLIMENTO.

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20failed%20password%20%7C%20search%20user&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample...

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search failed password | search user
```

Sempre

✓ **24.011 eventi** (prima di 01/11/24 10:44:09,000) Nessun campionamento degli eventi

Processo | Modalità intelligente

Eventi (24.011) | Pattern | Statistiche | Visualizzazione

Formato timeline | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 giorno per colonna

Elenco | Formato | 20 per pagina

< Prec 1 2 3 4 5 6 7 8 ... Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a source 4
- a sourcetype 1

CAMPI INTERESSANTI
- # date_hour 1
- # date_mday 8
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 7
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 2
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

+ Estrai nuovi campi

i	Ora	Evento
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[4994]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[2605]: Failed password for invalid user itmadmin from 194.8.74.23 port 4692 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5333]: Failed password for invalid user inet from 194.8.74.23 port 4564 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[3014]: Failed password for invalid user operator from 194.8.74.23 port 1491 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log

Cerca | 20°C Nuvole sparse | ITA | 10:48 01/11/2024

PATTERN

Ricerca | Splunk 9.3.1 — Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20failed%20password%20%7C%20search%20user&earliest=0&latest=&display.page.search.mode=verbose&dispatch.sam...

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search failed password | search user
```

Sempre

✓ **24.011 eventi** (prima di 02/11/24 11:03:37,000) | Nessun campionamento degli eventi | Processo | Modalità dettagliata

Eventi (24.011) | **Pattern** | Statistiche | Visualizzazione

Più piccolo — Più grande

13 pattern basato su un esempio di 9.288 eventi

```
10,22%  Wed <timestamp>mailsv1 sshd[1438]: Failed password for invalid user jabber from 193.33.170.23 port 3611 ssh2
 9,3%   Mon <timestamp>mailsv1 sshd[3105]: Failed password for invalid user irc from 201.28.109.162 port 3147 ssh2
8,89%   Thu <timestamp>www3 sshd[1370]: Failed password for invalid user administrator from 207.36.232.245 port 4438 ssh2
9,54%   Thu <timestamp>mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
8,55%   Sun <timestamp>mailsv1 sshd[3901]: Failed password for invalid user testing from 193.33.170.23 port 3125 ssh2
 8,6%   Sat <timestamp>mailsv1 sshd[1772]: Failed password for invalid user hsqldb from 27.102.11.11 port 3312 ssh2
9,01%   Thu <timestamp>www2 sshd[1210]: Failed password for invalid user inet from 64.66.0.20 port 4086 ssh2
8,53%   Tue <timestamp>mailsv1 sshd[5756]: Failed password for invalid user mantis from 124.160.192.241 port 3813 ssh2
8,48%   Fri <timestamp>mailsv1 sshd[1429]: Failed password for invalid user workshop from 91.210.104.143 port 4713 ssh2
7,96%   Thu <timestamp>www1 sshd[1089]: Failed password for invalid user local from 2.229.4.58 port 4910 ssh2
2,28%   Fri <timestamp>www2 sshd[4855]: Failed password for invalid user administrator from 87.194.216.51 port 1569 ssh2
2,24%   Tue <timestamp>www2 sshd[4356]: Failed password for invalid user postgres from 109.169.32.135 port 1129 ssh2
2,16%   Sat <timestamp>www2 sshd[2309]: Failed password for invalid user appserver from 110.138.30.229 port 4431 ssh2
```

Documentazione

Fare clic su un pattern per maggiori informazioni.

Attiva Windows

Cerca | ITA | 11:05 02/11/2024

SCRIVI UNA QUERY SPLUNK PER TROVARE TUTTE LE SESSIONI SSH APERTE CON SUCCESSO. LA QUERY DOVREBBE FILTRARE PER L'UTENTE "DJOHNSON" E MOSTRARE IL TIMESTAMP E L'ID UTENTE.

Ricerca | Splunk 9.3.1 — Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20sshd%20%7C%20search%20session%20opened%20for%20user%20djohnson%20%7C&earliest=0&latest=&display.page...

splunk>enterprise App ▾ | Administrator ▾ | Messaggi ▾ | Impostazioni ▾ | Attività ▾ | Guida ▾ | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come ▾ | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search sshd | search session opened for user djohnson |
```

Sempre ▾

✓ **1.065 eventi** (prima di 01/11/24 11:09:59,000) | Nessun campionamento degli eventi ▾ | Processo ▾ | Modalità intelligente ▾

Eventi (1.065) | Pattern | Statistiche | Visualizzazione

Formato timeline ▾ | − Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 giorno per colonna

Elenco ▾ | Formato | 20 per pagina ▾ | < Prec | 1 2 3 4 5 6 7 8 ... | Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a source 4
- a sourcetype 1
- # uid 1

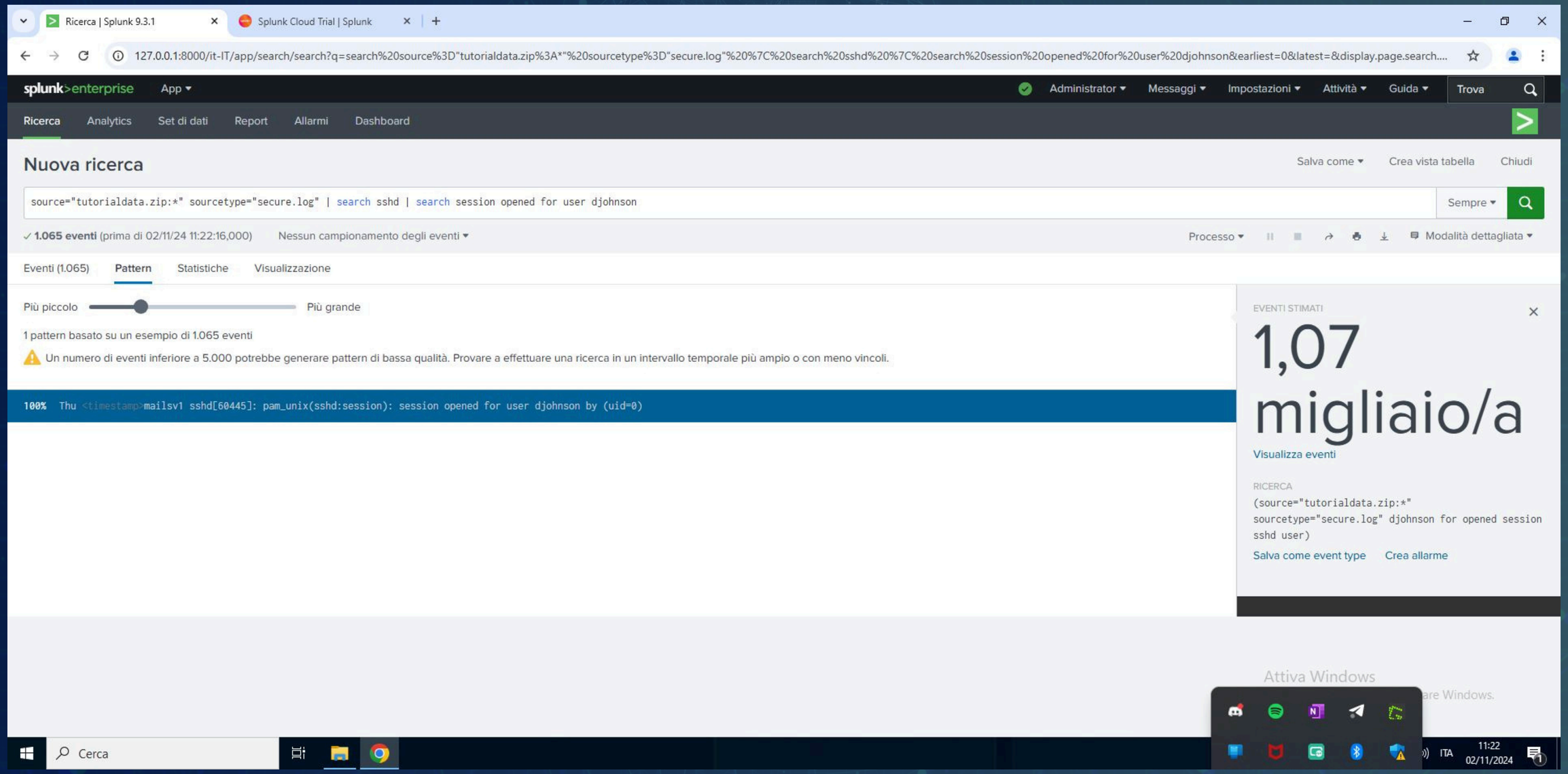
CAMPI INTERESSANTI
- # date_hour 1
- # date_mday 8
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 7
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 1
- a splunk_server 1
- # timeendpos 1

Ora	Evento
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[87066]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5860]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[71798]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[54980]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[58730]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0
29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[68740]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | uid = 0

Attiva Windows
Passa a Impostazioni per attivare Windows.

Cerca | 20°C Nuvole sparse | ITA | 11:12 01/11/2024

PATTERN


Ricerca | Splunk 9.3.1
Splunk Cloud Trial | Splunk
127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20sshd%20%7C%20search%20session%20opened%20for%20user%20djohnson&earliest=0&latest=&display.page.search....
splunk>enterprise
App
Administrator
Messaggi
Impostazioni
Attività
Guida
Trova
Ricerca
Analytics
Set di dati
Report
Allarmi
Dashboard
Nuova ricerca
Salva come
Crea vista tabella
Chiudi
source="tutorialdata.zip:*" sourcetype="secure.log" | search sshd | search session opened for user djohnson
Sempre
1.065 eventi (prima di 02/11/24 11:22:16,000)
Nessun campionamento degli eventi
Processo
Modalità dettagliata
Eventi (1.065)
Pattern
Statistiche
Visualizzazione
Più piccolo
Più grande
1 pattern basato su un esempio di 1.065 eventi
Un numero di eventi inferiore a 5.000 potrebbe generare pattern di bassa qualità. Provare a effettuare una ricerca in un intervallo temporale più ampio o con meno vincoli.
100% Thu <timestamp>mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
EVENTI STIMATI
1,07 migliaio/a
Visualizza eventi
RICERCA
(source="tutorialdata.zip:*" sourcetype="secure.log" djohnson for opened session sshd user)
Salva come event type
Crea allarme
Attiva Windows
Cerca
ITA
11:22
02/11/2024

AI QUERY

OLTRE A CREARE DELLE QUERY MANUALMENTE HO VOLUTO CREARE DELLE QUERY PIU' DETTAGLIATE UTILIZZANDO ANCHE L'INTELLIGENZA ARTIFICIALE

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%7C%20rex%20"Accepted%20password%20for%20(%3F<user_id>%5CS%2B)"%0A%7C%20where%20user_id%3D"djohnson"%0A%7C%20t...

splunk>enterprise App | Administrator | Messaggi | Impostazioni | Attività | Guida | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log"| rex "Accepted password for (?<user_id>\S+)"
| where user_id="djohnson"
| table _time user_id
| rename _time as "Timestamp", user_id as "ID Utente"
| sort - _time
```

Sempre

✓ **955 eventi** (prima di 01/11/24 11:53:37,000) | Nessun campionamento degli eventi | Processo | Modalità dettagliata

Eventi (955) | Pattern | Statistiche (955) | Visualizzazione

Formato timeline | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 giorno per colonna

Elenco | Formato | 20 per pagina | < Prec | 1 2 3 4 5 6 7 8 ... | Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a source 4
- a sourcetype 1

CAMPI INTERESSANTI
- # date_hour 1
- # date_mday 8
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 7

i	Ora	Evento
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[90328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = 127.0.0.1 | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log
>	29/10/24	Thu Oct 29 2024 04:36:28 mailsv1 sshd[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2

Attiva Win... Passa a Impos...

Cerca | 20°C Nuvole sparse

SCRIVI UNA QUERY SPLUNK PER TROVARE TUTTI I TENTATIVI DI ACCESSO FALLITI PROVENIENTI DALL'INDIRIZZO IP “86.212.199.60”. LA QUERY DOVREBBE MOSTRARE IL TIMESTAMP, IL NOME UTENTE E IL NUMERO DI PORTA.

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%2086.212.199.60%20%7C%20search%20failed%20%7C%20search%20user%20%7C%20search%20port&earliest=0&latest=...

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search 86.212.199.60 | search failed | search user | search port
```

Sempre

✓ **112 eventi** (prima di 01/11/24 11:23:58,000) Nessun campionamento degli eventi

Processo | Modalità intelligente

Eventi (112) | Pattern | Statistiche | Visualizzazione

Formato timeline | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 giorno per colonna

Elenco | Formato | 20 per pagina

< Prec 1 2 3 4 5 6 Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a source 4
- a sourcetype 1

CAMPI INTERESSANTI
- # date_hour 1
- # date_mday 7
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 6
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 1
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

+ Estrai nuovi campi

i	Ora	Evento
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[2079]: Failed password for invalid user services from 86.212.199.60 port 4740 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[2205]: Failed password for invalid user irc from 86.212.199.60 port 1203 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[3680]: Failed password for invalid user mysql from 86.212.199.60 port 4802 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[1679]: Failed password for invalid user pmuser from 86.212.199.60 port 1775 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[3243]: Failed password for invalid user ventrilo from 86.212.199.60 port 1465 ssh2 host = 127.0.0.1 source = tutorialdata.zip:.\mailsv/secure.log sourcetype = secure.log

Attiva Windows
Passa a Impostazioni per attivare Windows.

Cerca | 20°C Nuvole sparse | ITA | 11:24 01/11/2024

PATTERN

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7Csearch%2086.212.199.60%20%7C%20search%20failed%20%7C%20search%20user%20%7C%20search%20port&earliest=0&latest=&dis...

splunk>enterprise App ▾ Administrator ▾ Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" |search 86.212.199.60 | search failed | search user | search port
```

Sempre ▾

✓ **112 eventi** (prima di 02/11/24 11:34:51,000) Nessun campionamento degli eventi ▾ Processo ▾ Modalità dettagliata ▾

Eventi (112) **Pattern** Statistiche Visualizzazione

Più piccolo — Più grande

2 pattern basato su un esempio di 112 eventi

⚠ Un numero di eventi inferiore a 5.000 potrebbe generare pattern di bassa qualità. Provare a effettuare una ricerca in un intervallo temporale più ampio o con meno vincoli.

```
68,75%  Thu <timestamp>mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2

31,25%  Wed <timestamp>www3 sshd[3129]: Failed password for invalid user services from 86.212.199.60 port 1393 ssh2
```

Documentazione

Fare clic su un pattern per maggiori informazioni.

Attiva Windows

Cerca ITA 11:35 02/11/2024

Ricerca | Splunk 9.3.1 — Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20"86.212.199.60"%20%7C%20search%20"failed%20password"%0A%7C%20rex%20"Failed%20password%20for%20(%3F%...

splunk>enterprise App ▾ | Administrator ▾ | Messaggi ▾ | Impostazioni ▾ | Attività ▾ | Guida ▾ | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come ▾ | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search "86.212.199.60" | search "failed password"
| rex "Failed password for (?:invalid user )?(?<username>\S+) from (?<src_ip>\S+) port (?<port>\d+)"
| table _time username port
| rename _time as "Timestamp", username as "Nome Utente", port as "Numero di Porta"
| sort - _time
```

Sempre ▾

✓ **158 eventi** (prima di 02/11/24 11:27:55,000) | Nessun campionamento degli eventi ▾ | Processo ▾ | Modalità dettagliata ▾

Eventi (158) | Pattern | Statistiche (158) | Visualizzazione

Formato timeline ▾ | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 giorno per colonna

Elenco ▾ | Formato | 20 per pagina ▾ | < Prec | 1 2 3 4 5 6 7 8 | Avanti >

< Nascondi campi | ≡ Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a index 1
- a source 4
- a sourcetype 1
- a src_ip 1

CAMPI INTERESSANTI
- # date_hour 1
- # date_mday 7
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 6
- # date_year 1

i	Ora	Evento
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | src_ip = 86.212.199.60
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | src_ip = 86.212.199.60
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | src_ip = 86.212.199.60
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | src_ip = 86.212.199.60
>	29/10/24 04:36:28,000	Thu Oct 29 2024 04:36:28 mailsv1 sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\mailsv/secure.log | sourcetype = secure.log | src_ip = 86.212.199.60
>	29/10/24	Thu Oct 29 2024 04:36:28 mailsv1 sshd[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2

Cerca

CREA UNA QUERY SPLUNK PER IDENTIFICARE GLI INDIRIZZI IP CHE HANNO TENTATO DI ACCEDERE ("FAILED PASSWORD") AL SISTEMA PIÙ DI 5 VOLTE. LA QUERY DOVREBBE MOSTRARE L'INDIRIZZO IP E IL NUMERO DI TENTATIVI

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20rex%20"Failed%20password%20for%20(%3F%3Ainvalid%20user%20)%3F(%3F<username>%5CS%2B)%20from%20(%3F<src_i...

splunk>enterprise App ▾ | Administrator ▾ | Messaggi ▾ | Impostazioni ▾ | Attività ▾ | Guida ▾ | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come ▾ | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | rex "Failed password for (?:invalid user )?(?<username>\S+) from (?<src_ip>\S+)"
| stats count as attempts by src_ip
| where attempts > 5
| table src_ip attempts
| rename src_ip as "Indirizzo IP", attempts as "Numero di Tentativi"
| sort - attempts
```

Sempre ▾

✓ **109.864 eventi** (prima di 01/11/24 11:47:46,000) | Nessun campionamento degli eventi ▾ | Processo ▾ | Modalità dettagliata ▾

Eventi (109.864) | Pattern | **Statistiche (182)** | Visualizzazione

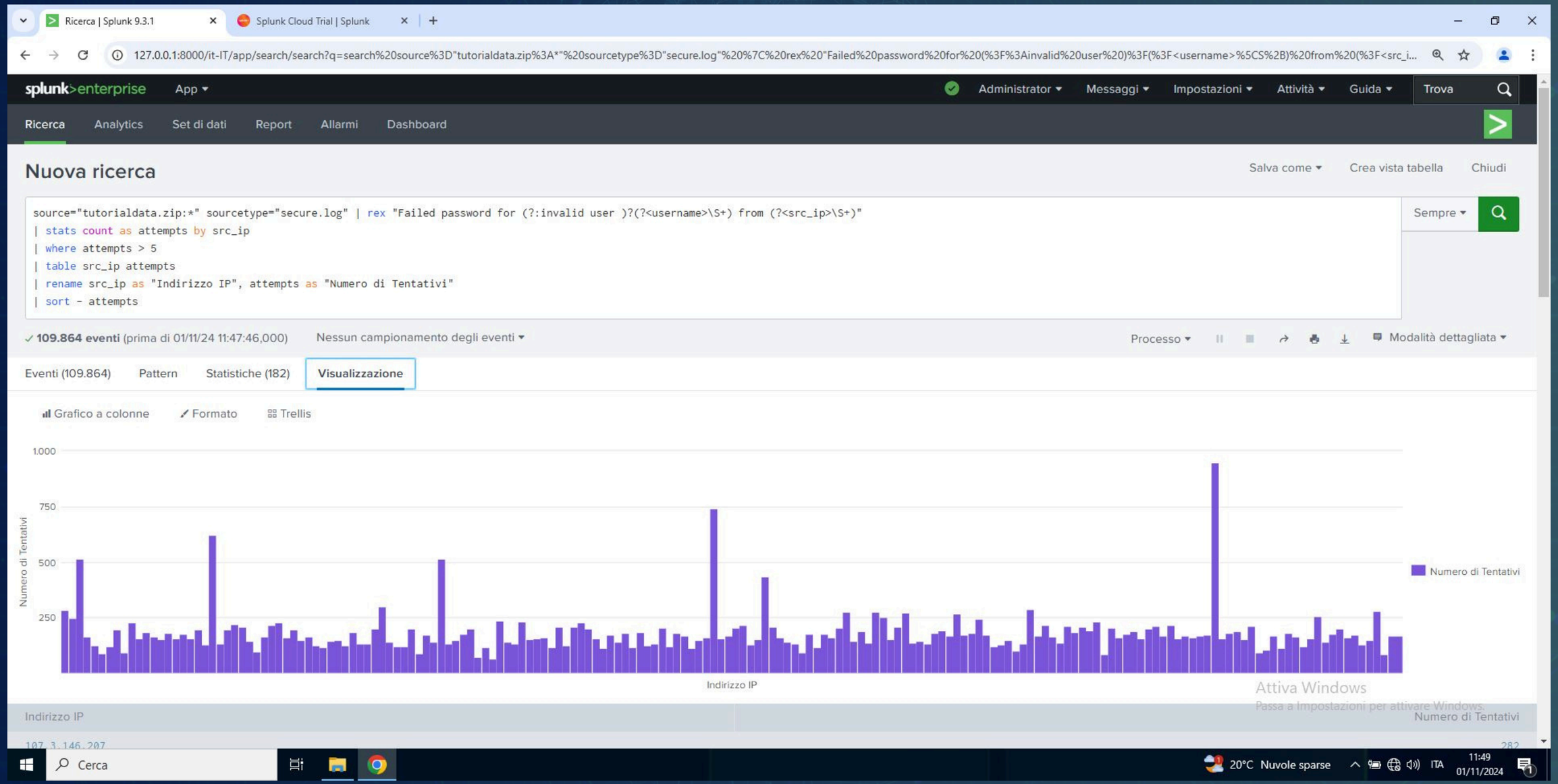
20 per pagina ▾ | Formato | Anteprima ▾ | < Prec | 1 2 3 4 5 6 7 8 ... | Avanti >

Indirizzo IP	Numero di Tentativi
107.3.146.207	282
108.65.113.83	249
109.169.32.135	515
110.138.30.229	
110.159.208.78	
111.161.27.20	
112.111.162.4	
117.21.246.164	
118.142.68.222	
12.130.60.4	

Attiva Win
Passa a Impos

Cerca | 20°C Nuvole sparse

IP PIU' UTILIZZATI



CREA UNA QUERY SPLUNK PER TROVARE TUTTI GLI INTERNAL SERVER ERROR

Ricerca | Splunk 9.3.1 — Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%20%7C%20search%20500&earliest=0&latest=&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&display.event...

splunk>enterprise | App | Administrator | Messaggi | Impostazioni | Attività | Guida | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log" | search 500
```

Sempre

✓ **781 eventi** (prima di 02/11/24 10:32:11,000) | Nessun campionamento degli eventi

Processo | Modalità dettagliata

Eventi (781) | Pattern | Statistiche | Visualizzazione

Formato timeline | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 ora per colonna

22 ott 2024 18:00 — 5 events 27 ott 2024 da 01:00:00 a 02:00:00 — 29 ott 2024 19:00

7 days 1 hour

Elenco | Formato | 20 per pagina

< Prec | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a index 1
- a JSESSIONID 100+
- a source 3
- a sourcetype 1

CAMPI INTERESSANTI
- a action 5
- a categoryId 8
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 7
- # date_year 1
- a date_zone 1
- a itemId 14

i	Ora	Evento
>	29/10/24 18:18:59,000	198.35.1.75 - - [29/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 JSESSIONID = SD10SL2FF4ADFF53099 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24 18:18:55,000	198.35.1.75 - - [29/Oct/2024:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2809 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 JSESSIONID = SD10SL2FF4ADFF53099 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24 17:42:03,000	125.89.78.6 - - [29/Oct/2024:17:42:03] "POST /cart.do?action=changequantity&itemId=EST-16&JSESSIONID=SD10SL8FF3ADFF52952 HTTP 1.1" 500 1165 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 230 JSESSIONID = SD10SL8FF3ADFF52952 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www2/access.log | sourcetype = secure.log
>	29/10/24 17:17:00,000	194.146.236.22 - - [29/Oct/2024:17:17:00] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD4SL3FF2ADFF52813 HTTP 1.1" 500 299 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-13" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 749 JSESSIONID = SD4SL3FF2ADFF52813 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24 17:15:13,000	121.254.179.199 - - [29/Oct/2024:17:15:13] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL9FF10ADFF52799 HTTP 1.1" 500 2243 "http://www.buttercupgames.com/oldlink?itemId=EST-13" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 642 JSESSIONID = SD0SL9FF10ADFF52799 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www3/access.log | sourcetype = secure.log

Attiva Windows

Cerca | ITA | 10:33 02/11/2024

Ricerca | Splunk 9.3.1 | Splunk Cloud Trial | Splunk

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20sourcetype%3D"secure.log"%7Csearch%20"500"%0A%7C%20table%20_time%20host%20uri%20status%0A%7C%20rename%20_time%20as%20"Timestamp"%2C%20host%...

splunk>enterprise App ▾ | Administrator ▾ | Messaggi ▾ | Impostazioni ▾ | Attività ▾ | Guida ▾ | Trova

Ricerca | Analytics | Set di dati | Report | Allarmi | Dashboard

Nuova ricerca

Salva come ▾ | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="secure.log"|search "500"
| table _time host uri status
| rename _time as "Timestamp", host as "Host", uri as "URL", status as "Stato"
| sort - _time
```

Sempre ▾

✓ **781 eventi** (prima di 02/11/24 11:48:49,000) | Nessun campionamento degli eventi ▾ | Processo ▾ | Modalità dettagliata ▾

Eventi (781) | Pattern | Statistiche (781) | Visualizzazione

Formato timeline ▾ | – Zoom indietro | + Zoom area selezionata | × Deseleziona | 1 ora per colonna

Elenco ▾ | Formato | 20 per pagina ▾ | < Prec | 1 2 3 4 5 6 7 8 ... | Avanti >

< Nascondi campi | Tutti i campi

CAMPI SELEZIONATI
- a host 1
- a index 1
- a JSESSIONID 100+
- a source 3
- a sourcetype 1

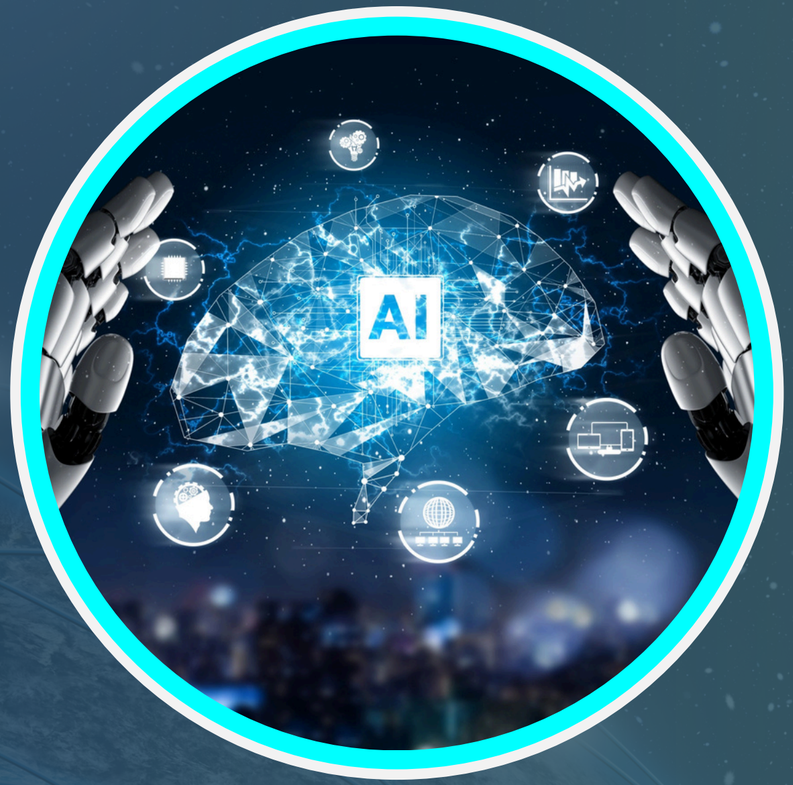
CAMPI INTERESSANTI
- a action 5
- a categoryId 8
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 7

i	Ora	Evento
>	29/10/24 18:18:59,000	198.35.1.75 - - [29/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 JSESSIONID = SD10SL2FF4ADFF53099 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24 18:18:55,000	198.35.1.75 - - [29/Oct/2024:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2809 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 JSESSIONID = SD10SL2FF4ADFF53099 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24 17:42:03,000	125.89.78.6 - - [29/Oct/2024:17:42:03] "POST /cart.do?action=changequantity&itemId=EST-16&JSESSIONID=SD10SL8FF3ADFF52952 HTTP 1.1" 500 1165 "http://www.buttercupgames.com/product "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 230 JSESSIONID = SD10SL8FF3ADFF52952 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www2/access.log | sourcetype = secure.log
>	29/10/24 17:17:00,000	194.146.236.22 - - [29/Oct/2024:17:17:00] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD4SL3FF2ADFF52813 HTTP 1.1" 500 299 "http://www.buttercupgames.com/cart.do?a a/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 749 JSESSIONID = SD4SL3FF2ADFF52813 | host = 127.0.0.1 | index = main | source = tutorialdata.zip:.\www1/access.log | sourcetype = secure.log
>	29/10/24	121.254.179.199 - - [29/Oct/2024:17:15:13] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL9FF10ADFF52799 HTTP 1.1" 500 2243 "http://www.bu

Cerca

CONCLUSIONI CON AI

PER FARE UN ANALISI IL PIU' DETTAGLIATA POSSIBILE HO SCARICATO TUTTI I FILE DI LOG DELLA CONSEGNA E LI HO FATTI ANALIZZARE DALL AI.
POI UTILIZZANDO VARI PROMPT HO CERCAATO DI ISTRUIRE L AI PER AVERE UN RISULTATO QUANTO PIU' SPECIFICO E DETTAGLIATO POSSIBILE.



POSSIBILI ATTACCHI RILEVATI

Tentativi di Brute Force su Accessi SSH
Nei log SSH, sono presenti diversi tentativi di accesso da vari indirizzi IP, con alcuni che compaiono frequentemente. La presenza di tentativi falliti suggerisce l'ipotesi di un attacco di forza bruta, in cui gli attaccanti provano ripetutamente combinazioni di credenziali per accedere ai sistemi. Questo tipo di attacco può essere confermato ulteriormente attraverso l'analisi della frequenza dei tentativi in brevi intervalli di tempo.

Ricognizione tramite Enumerazione di Sessioni e Processi
La presenza di dettagli su processi e sessioni indica che alcuni accessi potrebbero essere finalizzati a raccogliere informazioni piuttosto che a ottenere accessi permanenti. Questo tipo di attività è tipico di un attacco di ricognizione, dove l'attaccante mira a identificare sessioni attive, processi e vulnerabilità specifiche che potrebbe sfruttare in una fase successiva.

POSSIBILI ATTACCHI RILEVATI

Attività Malevole di Automazione sul Sito Web

La registrazione di azioni come "addtocart" e "changequantity" in un contesto HTTP potrebbe suggerire la presenza di bot automatizzati, specialmente se si notano pattern anomali nella frequenza di queste azioni. Potrebbero esserci tentativi di frode o scraping (ad esempio, per monitorare prezzi o disponibilità dei prodotti) tramite bot, che effettuano ripetute richieste HTTP per simulare il comportamento degli utenti.

Attacco di Credential Stuffing

La presenza di IP che appaiono ripetutamente nei log SSH, combinata con stati di connessione falliti, potrebbe indicare un tentativo di attacco di credential stuffing. In questo tipo di attacco, l'attaccante utilizza credenziali compromesse da altre piattaforme, cercando di accedere ai server SSH. Questo tipo di attività può essere confermata analizzando l'origine IP e il comportamento anomalo associato.

POSSIBILI ATTACCHI RILEVATI

Potenziale SQL Injection o Abuso di API sul Sito Web

Anche se non direttamente osservabile dai log, la registrazione di azioni specifiche e ripetute su un sito web (come "addtocart" o "changequantity") può suggerire un tentativo di abuso delle API o di SQL injection, qualora i dati inseriti risultino atipici o contengano caratteri speciali usati comunemente in attacchi di injection.

CONCLUSIONI

Questi possibili tipi di attacco indicano una combinazione di tentativi di accesso non autorizzati, esplorazione del sistema e potenziale abuso di risorse web.
Ulteriori analisi, come il monitoraggio della frequenza e della provenienza IP, sono fondamentali per confermare queste ipotesi e per attuare strategie di mitigazione specifiche. Questi dati possono quindi fornire statistiche preziose per rafforzare le misure di sicurezza contro minacce ricorrenti e mirate.

FINE PRESENTAZIONE

RICCARDO LEPORE