

W24D4 – Pratica

Epic Education Srl

Analisi del malware e Splunk

Simone Giordano

30/12/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Query Splunk..... 3

 Query 1..... 3

 Query 2..... 4

 Query aggiuntiva 5

 Query 3..... 6

 Query 4..... 7

 Query 5..... 8

Conclusioni AI sui log analizzati..... 8

Query Splunk

Query 1

Importate su Splunk i dati di esempio "tutorialdata.zip":

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.

Ho importato i file di tutorialdata tramite **Settings > Add Data > Upload**.

Ho inserito una query che mostra tutti i risultati contenenti il testo "Failed password".

Nell'immagine in basso possiamo visualizzare il timestamp (1), l'indirizzo IP di origine (2), l'utente (3) e il motivo del fallimento (4).

source="tutorialdata.zip:*" | search "Failed password"

33,253 events (before 12/18/25 12:31:09.000 PM) No Event Sampling

Events (33,253) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

i	Time	Event
>	12/17/25 6:45:49.000 AM (1)	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2 (3) (4)
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2 host = mailsv1 source = tutorialdata.zip:/mailsv1/secure.log sourcetype = secure-2

Query 2

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.

Source="tutorialdata.zip" | search "accepted password" AND "ssh2" AND "djohnson"

source="tutorialdata.zip" limita la ricerca ai dati contenuti nel file **tutorialdata.zip**, - **search** applica un filtro che combina le tre stringhe: **"accepted password"**, **"ssh2"** **"djohnson"**, tramite l'operatore logico **AND**, restituendo solo gli eventi che contengono tutte e tre le stringhe.

Il risultato mostra quindi tutti i tentativi di accesso SSH riusciti (accepted password) tramite protocollo SSH2 effettuati dall'utente djohnson.

The screenshot displays the Splunk search results for the query: `source="tutorialdata.zip:*" | search "accepted password" AND "ssh2" AND "djohnson"`. The interface shows 955 events. The results are displayed in a table format with columns for index, time, and event details. The events are filtered to show only successful SSH logins for the user 'djohnson'.

i	Time	Event
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[90328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[94708]: Accepted password for djohnson from 10.3.10.46 port 2408 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 06:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[98104]: Accepted password for djohnson from 10.3.10.46 port 4577 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2

Query aggiuntiva

source="tutorialdata.zip:* – Limita la ricerca ai log provenienti dal file sorgente **tutorialdata.zip**. Il simbolo ***** indica **tutti i file contenuti** nell'archivio

| **search sshd:session** - Filtra gli eventi che contengono la stringa sshd:session

| search "session opened for user djohnson" - Seleziona solo gli eventi in cui la sessione SSH è stata aperta con successo e l'utente coinvolto è djohnson

| **rex field=_raw "uid=(?<ID>\d+)"** - Usa una espressione regolare (regex) sul campo _raw (log grezzo), estrae il valore numerico dopo uid= e salva il risultato in un nuovo campo chiamato ID

| **table_time ID** - Mostra il risultato in formato tabellare, visualizza solo: _time (timestamp dell'evento) e ID (user ID) estratti dal log.

[illegible]

Query 3

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.

source="tutorialdata.zip" limita la ricerca ai dati contenuti nel file **tutorialdata.zip**,
- **search** applica un filtro che combina le tre stringhe: **"failed password"** e **"86.212.199.60"**, tramite l'operatore logico **AND**, restituendo solo gli eventi che contengono tutte e due le stringhe.

Il risultato mostra quindi tutti i tentativi di accesso falliti (failed password) dall'IP 86.212.199.60, mostrando il time stamp (1), l'utente (2) e il numero di porta (3).

source=tutorialdata.zip:* | search "failed password" AND "86.212.199.60"

158 events (before 12/18/25 12:59:46.000 PM) No Event Sampling

Events (158) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 50 Per Page View: List

i	Time	Event
>	12/17/25 (1) 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5728]: Failed password for invalid user agusho from 86.212.199.60 port 3692 ssh2 host = mailsv (2) : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[4843]: Failed password for invalid user tomat from 86.212.199.60 port 1464 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[1008]: Failed password for invalid user yd from 86.212.199.60 port 2856 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2
>	12/17/25 6:45:49.000 AM	Thu Dec 17 2025 06:45:49 mailsv1 sshd[2079]: Failed password for invalid user services from 86.212.199.60 port 4740 ssh2 host = mailsv : source = tutorialdata.zip:/mailsv/secure.log : sourcetype = secure-2

Query 4

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.

```
source="tutorialdata.zip:*" | search "failed password" | rex field=_raw "from (?<ip>[\d\.]+)" | stats count AS failed_attempts by ip | where failed_attempts > 5 | sort - failed_attempts | table ip failed_attempts
```

source="tutorialdata.zip:*" - Dice a Splunk di cercare dentro il file tutorialdata.zip, in tutti i file contenuti
search "failed password" - Mostra solo i log che contengono la stringa "failed password" (tentativi di login falliti)

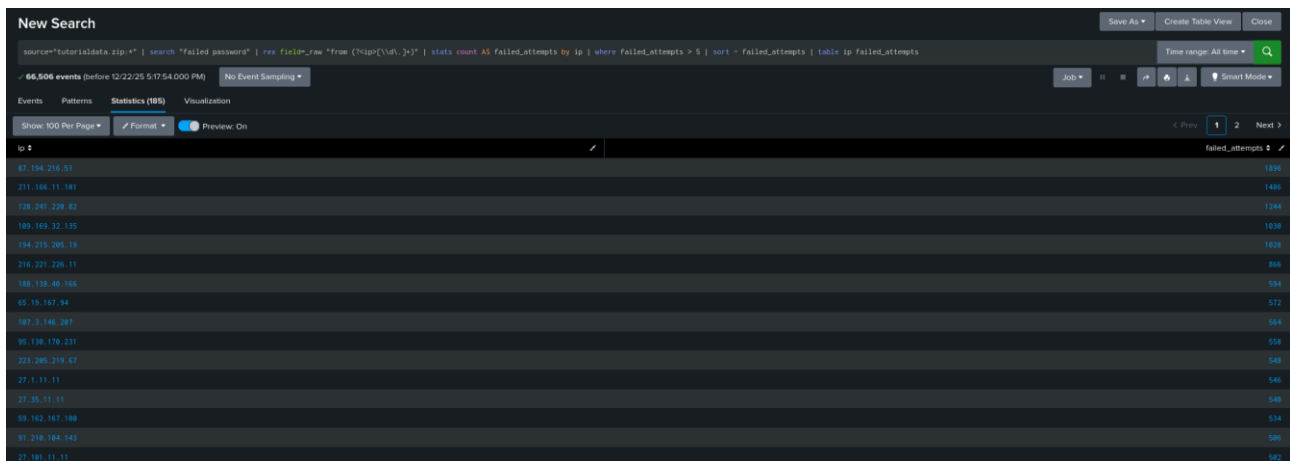
rex field=_raw "from (?<ip>[\d\.]+)" – Regex che cerca nel testo del log (_raw) un IP dopo la parola from e lo salva nel campo ip

stats count AS failed_attempts by ip - Conta quanti tentativi falliti ci sono per ogni indirizzo IP

where failed_attempts > 5 - Mostra solo gli IP che hanno più di 5 tentativi falliti

sort - failed_attempts - Ordina gli IP dal numero più alto al più basso di tentativi falliti

table ip failed_attempts - Mostra solo le colonne IP e numero di tentativi falliti



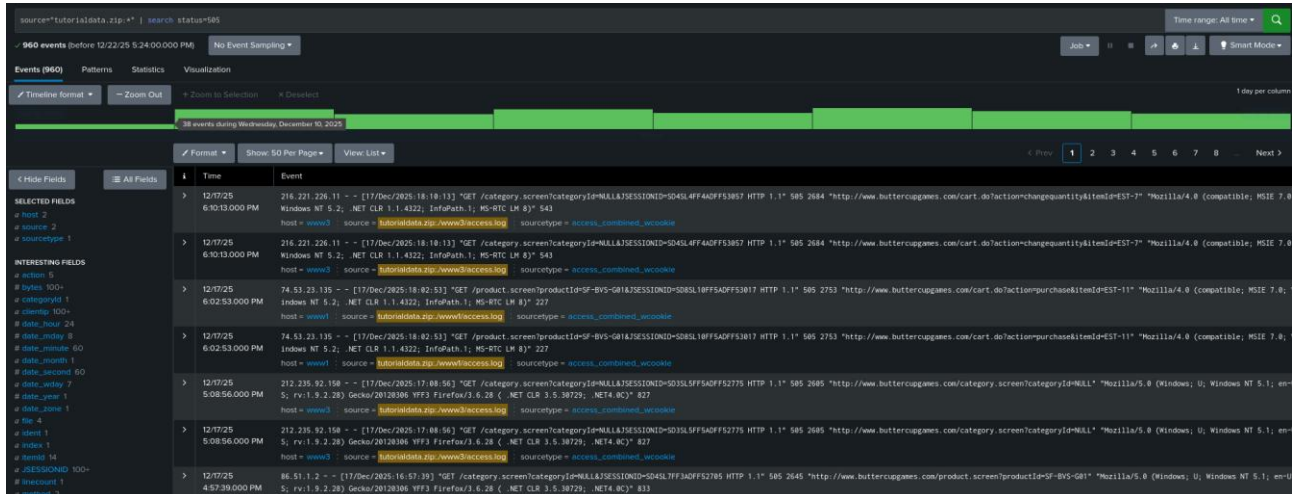
ip	failed_attempts
87.194.216.51	1838
211.166.11.181	1488
128.241.228.82	1244
102.162.32.135	1038
194.215.285.19	1028
216.221.226.11	868
188.128.40.166	594
65.19.167.84	572
187.9.146.287	564
95.138.176.231	558
223.285.219.67	548
27.1.11.11	546
27.35.11.11	548
59.162.167.188	534
91.218.184.142	508
27.181.11.11	501

Query 5

Crea una query Splunk per trovare tutti gli Internal Server Error.

Gli Internal Server Error hanno come codice di stato 505, quindi per filtrare i risultati ho utilizzato la seguente query.

Source="tutorialdata.zip:*" | search status=505



Conclusioni AI sui log analizzati

Trarre delle conclusioni sui log analizzati utilizzando AI.

Dalle conclusioni tratte dai log forniti, sembra esserci un problema diffuso con richieste API non valide che generano errori HTTP 400.

Analisi dei Log

- **Errori HTTP 400 Diffusi:** I log mostrano un numero significativo di risposte con codice di stato **400 Bad Request**. Questo indica che le richieste inviate dal client al server non sono state comprese o non erano valide a causa di sintassi errata, parametri mancanti o dati non corretti.
- **Servizio AWS Coinvolto:** L'intestazione x-amzn-errortype suggerisce che il servizio in questione sia gestito su **Amazon Web Services (AWS)**, probabilmente tramite Amazon API Gateway o servizi simili.
- **Tipi di Richieste (Metodi HTTP):** Vengono registrate richieste di tipo POST, GET, PUT e DELETE. Le richieste POST e PUT sono spesso utilizzate per inviare o aggiornare dati, mentre GET e DELETE per recuperare o rimuovere risorse.
- **Attività Utente Sospetta/Ripetitiva:** La ripetizione frequente degli errori 400 potrebbe indicare:
 - Un client mal configurato che invia costantemente richieste errate.
 - Un tentativo di accesso fallito ripetuto troppe volte.
 - Un'attività anomala o un attacco informatico (come un tentativo di brute force o fuzzing) dato il contesto di log di sicurezza/monitoraggio visualizzato.

I log documentano principalmente una serie di interazioni fallite con un'API AWS, probabilmente a causa di richieste formate male da parte del client.