



Cybersecurity Progetto finale a cura

Di Renga Daniele

Progetto

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

Trarre delle conclusioni sui log analizzati utilizzando AI.

Fase 1:

Creazione della Query Splunk per identificare tutti i tentativi di accesso falliti "FAILED PASSWORD".

The screenshot shows the Splunk Enterprise web interface. The search bar contains the following query:

```
index=* failed password  
| rex "failed password for (invalid user )?(?<user>[a-z]) from (?<ip>[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)"  
| search user=guest  
| table _time ip user message
```

The results table shows 758 events. The columns are: _time, ip, user, and message. The first few rows are:

_time	ip	user	message
2025-05-09 13:22:27	95.130.170.231	guest	
2025-05-09 13:22:27	202.201.1.233	guest	
2025-05-09 13:22:27	27.96.128.0	guest	
2025-05-09 13:22:27	117.21.246.164	guest	
2025-05-09 13:22:27	27.102.11.11	guest	
2025-05-09 13:22:27	125.17.14.100	guest	
2025-05-09 13:22:27	198.35.3.23	guest	
2025-05-09 13:22:30	194.8.74.23	guest	
2025-05-09 13:22:30	91.208.184.24	guest	
2025-05-09 13:22:30	82.245.228.36	guest	

09/05/25
13:22:27.000

Azioni evento ▾

Tipo	<input checked="" type="checkbox"/>	Campo	Valore	Azioni
Selezionato	<input checked="" type="checkbox"/>	host ▾	DESKTOP-8CAJRTO	▾
	<input checked="" type="checkbox"/>	source ▾	tutorialdata.zip::www1/secure.log	▾
	<input checked="" type="checkbox"/>	sourcetype ▾	www1/secure	▾
Evento	<input type="checkbox"/>	ip ▾	95.130.170.231	▾
	<input type="checkbox"/>	user ▾	guest	▾
Ora ⚙		_time ▾	2025-05-09T13:22:27.000+02:00	
Default	<input type="checkbox"/>	index ▾	main	▾
	<input type="checkbox"/>	linecount ▾	1	▾
	<input type="checkbox"/>	punct ▾	{}~[]:~	▾
	<input type="checkbox"/>	splunk_server ▾	DESKTOP-8CAJRTO	▾

> 09/05/25
13:22:27.000

Thu May 09 2025 13:22:27 www1 sshd[5599]: Failed password for invalid user guest from 95.130.170.231 port 4078 ssh2
host = Computer_Esterno source = tutorialdata.zip::www1/secure.log sourcetype = www1/secure

Questa query ci indica dei tentativi falliti fatti da invalid user guest. Ci mostra anche alcune info molto importanti come quando si è connesso ,l' Ip usato e la porta.

Failed password for invalid user guest from 95.130.170.231 port 4078 ssh2

- **Dettagli dell'evento:**

- **Tipo di evento:** Fallito accesso SSH
- **Utente:** guest (utente non valido)
- **IP sorgente:** 95.130.170.231 (probabile attaccante)
- **Porta usata:** 4078
- **Protocollo:** SSH (versione 2)
- **Host di destinazione:** DESKTOP-8CAJRTO
- **Sorgente log:** tutorialdata.zip::www1/secure.log
- **Sourcetype:** www1/secure
- **Indice Splunk:** main

Per poter svolgere questa simulazione ho usato la query che riporterò di sotto :

```
index=* failed password | rex "Failed password for (invalid user )?(?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+)" | search user=guest | table _time ip user message
```

seguono i dettagli per far comprende meglio la funzionalità della query

1. *index=failed password**

- Cerca in **tutti gli indici** (index=*) gli eventi che contengono la stringa "failed password".
- Questo serve per identificare i **tentativi di accesso falliti**, in genere SSH.

2. *rex "Failed password for (invalid user)?(?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+)"*

- Usa **regex (espressioni regolari)** per estrarre due informazioni specifiche dal messaggio di log:
 - user: il nome dell'utente (es. guest)

- o ip: l'indirizzo IP da cui proviene il tentativo
- La regex riconosce sia:
 - o "Failed password for user ..."
 - o **che** "Failed password for invalid user ..."
 - (usando `?(invalid user)?` come parte opzionale)

3. search user=guest

- Filtra i risultati per mostrare solo i tentativi che coinvolgono l'**utente guest**.

4. table _time ip user message

- Crea una **tabella** con le colonne:
 - o `_time`: orario dell'evento
 - o `ip`: IP sorgente
 - o `user`: utente usato
 - o `message`: messaggio completo del log
- Serve per visualizzare in modo chiaro e ordinato gli eventi rilevanti.

«È stata utilizzata una query Splunk per filtrare e analizzare i tentativi di accesso SSH falliti con l'utente `guest`. La regex ha permesso di estrarre dinamicamente gli IP e gli utenti coinvolti, facilitando l'identificazione delle fonti di attacco. Il risultato è stato visualizzato in una tabella ordinata con data, IP, utente e messaggio di log.»

La seconda query SPL per trovare tutte le sessione SSH aperte con successo. La query dovrebbe filtrare per l'utente "djohnson" e mostrare il timestamo e l' ID utente.

splunk enterprise App ▾ Danielle Renga ▾ Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Ricerca Analytics Set di dati Report Allarmi Dashboard ➤ Search & Reporting

Nuova ricerca Salva come ▾ Crea vista tabella Chiudi

Index=* "Accepted password" "djohnson"
| rex "Accepted password for (?<user>\\w*)" from (?<ip>\\d\\.\\d\\.\\d\\.\\d) port (?<port>\\d)*"
| search user="djohnson"

Sempre 🔍

✓ 2.865 eventi (prima di 11/05/25 13:25:28,000) Nessun campionamento degli eventi ▾ Processo ▾ || || ↻ ⬇ ⬆ Modalità intelligente ▾

Eventi (2.865) Pattern Statistiche Visualizzazione

✓ Formato timeline ▾ — Zoom indietro + Zoom area selezionata × Deseleziona 1 giorno per colonna

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

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI
host 2
source 4
sourcetype 1

CAMPI INTERESSANTI
date_hour 1
date_mday 8
date_minute 1
date_month 1
date_second 4
date_wday 7
date_year 1

i	Ora	Evento
>	09/05/25 13:22:30,000	Thu May 09 2025 13:22:30 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = DESKTOP-8CAJRTO source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	09/05/25 13:22:30,000	Thu May 09 2025 13:22:30 mailsv1 sshd[98328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = DESKTOP-8CAJRTO source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	09/05/25 13:22:30,000	Thu May 09 2025 13:22:30 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = DESKTOP-8CAJRTO source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	09/05/25 13:22:30,000	Thu May 09 2025 13:22:30 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = DESKTOP-8CAJRTO source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	09/05/25 13:22:30,000	Thu May 09 2025 13:22:30 mailsv1 sshd[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2 host = DESKTOP-8CAJRTO source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

09/05/25 13:22:30,000

Azioni evento ▾

Tipo	✓ Campo	Valore	Azioni
Selezionato	✓ host ▾	DESKTOP-8CAJRTO	▾
	✓ source ▾	tutorialdata.zip:\mailsv\secure.log	▾
	✓ sourcetype ▾	www1/secure	▾
Evento	<input type="checkbox"/> ip ▾	10.3.10.46	▾
	<input type="checkbox"/> port ▾	5143	▾
	<input type="checkbox"/> user ▾	djohnson	▾
Ora ⌚	<input type="checkbox"/> _time ▾	2025-05-09T13:22:30.000+02:00	▾
Default	<input type="checkbox"/> index ▾	main	▾
	<input type="checkbox"/> linecount ▾	1	▾
	<input type="checkbox"/> punct ▾	_____ _____	▾
	<input type="checkbox"/> splunk_server ▾	DESKTOP-8CAJRTO	▾

L'immagine mostra un evento registrato da Splunk relativo a un **accesso SSH riuscito** per l'utente djohnson

Dettagli dell'Evento

- **Messaggio di log:**
Accepted password for djohnson from 10.3.10.46 port 5143 ssh2
- **Informazioni estratte:**
 - **Utente:** djohnson
 - **IP sorgente:** 10.3.10.46 (probabile indirizzo interno, rete privata)
 - **Porta di origine:** 5143
 - **Protocollo:** SSH2
 - **Host target:** DESKTOP-8CAJRTO
 - **Sorgente log:** tutorialdata.zip:\mailsv\secure.log
 - **Sourcetype:** www1/secure
 - **Indice Splunk:** main

È stato registrato un accesso riuscito via SSH da parte dell'utente djohnson, proveniente da un IP interno (10.3.10.46) su porta 5143. Questo evento indica una connessione autenticata correttamente, e fa parte del normale controllo degli accessi. Si raccomanda di correlare questo evento con altre attività dell'utente per garantire che non vi siano comportamenti anomali o azioni non autorizzate.

Di seguito mostrerò la seconda query come è stata scritta con relativa spiegazione:

```
index=* "Accepted password" "djohnson" | rex "Accepted password for (?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+) port (?<port>\d+)" | search user="djohnson"
```

Descrizione Tecnica della Query

Questa query è stata utilizzata per identificare e analizzare tutti gli **accessi SSH riusciti** per l'utente specifico `djohnson`. Di seguito viene illustrato in dettaglio il funzionamento di ciascun componente della query:

1. `index=* "Accepted password" "djohnson"`

- Questo primo stadio effettua una ricerca su **tutti gli indici di Splunk** (`index=*`) per trovare eventi che:
 - Contengano la stringa `"Accepted password"` → indica un accesso SSH riuscito.
 - Contengano anche `"djohnson"` → per limitare la ricerca all'utente di interesse.

2. `rex "Accepted password for (?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+) port (?<port>\d+)"`

- Questo comando applica una **espressione regolare** per estrarre automaticamente tre campi dal testo del log:
 - `user`: il nome utente che ha effettuato l'accesso (es. `djohnson`)
 - `ip`: l'indirizzo IP del sistema da cui è partita la connessione SSH
 - `port`: la porta TCP di origine usata per la connessione
- Questi campi vengono salvati come **campi personalizzati** utilizzabili nelle fasi successive.

3. `search user="djohnson"`

- Applica un **filtro finale** per mostrare solo i risultati dove il campo `user` è esattamente `djohnson`.
- Serve a garantire che solo gli accessi realmente effettuati da quell'utente siano visualizzati, anche se altre righe contengono la stringa `"djohnson"` in altri contesti.

Obiettivo della Query

L'obiettivo della query è quello di:

- Verificare che l'utente `djohnson` abbia effettuato un accesso SSH riuscito.
- Identificare **quando, da dove** (IP), e con quale **porta sorgente** si è collegato.

- Fornire visibilità sugli accessi per scopi di **audit**, **monitoraggio della sicurezza**, o per verificare eventuali attività non autorizzate.

Ora passeremo alla 3 query, ci viene richiesto di scrivere una query Splunk dove la sua funziona sarà quella di trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo ip 86.212.199.60.

Questa query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.

The screenshot shows the Splunk Enterprise Search & Reporting interface. The search query entered is:

```
index=* "Failed password" "86.212.199.60"
| rex "Failed password for (invalid user )?(?<user>[a-z]) from (?<ip>86\.212\.199\.60) port (?<port>[0-9])"
| table _time user port
```

The results show 474 events. The table below displays the first 10 results:

_time	user	port
2025-05-03 13:22:30	administrator	2558
2025-05-03 13:22:30	appserver	4979
2025-05-03 13:22:30	britany	4639
2025-05-02 13:22:30	shoutcast	2227
2025-05-02 13:22:30	nagios	3362
2025-05-02 13:22:30	oracle	2411
2025-05-02 13:22:30	noone	2381
2025-05-02 13:22:30	email	2213
2025-05-02 13:22:30	testuser	1622
2025-05-02 13:22:30	dean	1136
2025-05-02 13:22:30	desktop	4564

Below the table, the event details for the first three results are shown:

- > 03/05/25 13:22:30,000 Fri May 03 2025 13:22:30 mailsrv sshd[2721]: Failed password for invalid user administrator from 86.212.199.60 port 2558 ssh2 host = DESKTOP-8CAJRTO | source = tutorialdata.zip:\mailsv\secure.log | sourcetype = www1/secure
- > 03/05/25 13:22:30,000 Fri May 03 2025 13:22:30 mailsrv sshd[2721]: Failed password for invalid user administrator from 86.212.199.60 port 2558 ssh2 host = DESKTOP-8CAJRTO | source = tutorialdata.zip:\mailsv\secure.log | sourcetype = www1/secure
- > 03/05/25 13:22:30,000 Fri May 03 2025 13:22:30 mailsrv sshd[2721]: Failed password for invalid user administrator from 86.212.199.60 port 2558 ssh2 host = Computer_Esterno | source = tutorialdata.zip:\mailsv\secure.log | sourcetype = www1/secure

Il risultato di questa query ci indica tre tentativi di accesso SSH falliti sono stati registrati contemporaneamente da 86.212.199.60, con l'utente administrator. Questi eventi rappresentano un pattern classico di attacco automatizzato ed è fondamentale bloccare la sorgente e monitorare eventuali accessi riusciti anomali.

Failed password for invalid user administrator from 86.212.199.60 port 2558 ssh2

Dettagli Tecnici

- **Utente tentato:** administrator (non esistente o disabilitato → *invalid user*)
- **IP sorgente:** 86.212.199.60
- **Porta di origine:** 2558
- **Protocollo:** SSH2
- **Sorgente log:** tutorialdata.zip:\mailsv\secure.log
- **Sourcetype:** www1/secure
- **Host di destinazione:** DESKTOP-8CAJRTO e Computer_Esterno

Questo evento è un tentativo di accesso fallito via SSH da un IP pubblico (86.212.199.60), verso un sistema che ha il demone SSH attivo.

L'utente administrator è comunemente preso di mira nei brute force attacks o scansioni automatizzate.

I tre eventi sono identici per timestamp e contenuto, ma provengono da host diversi, indicando che il log è stato replicato o che più istanze dello stesso evento sono state indicizzate.

La query che è stata scritta è la seguente a seguire anche la spiegazione della stessa.

```
index=* "Failed password" "86.212.199.60" | rex "Failed password for (invalid user )?(?<user>\w+) from (?<ip>86\.212\.199\.60) port (?<port>\d+)" | table _time user port
```

Descrizione Tecnica della Query

Questa query è progettata per individuare **tentativi di accesso SSH falliti** provenienti dall'indirizzo IP 86.212.199.60, estraendo e visualizzando le informazioni più rilevanti.

1. index=* "Failed password" "86.212.199.60"

- Cerca in **tutti gli indici di Splunk** eventi che contengano:
 - La stringa "Failed password": indica un tentativo di accesso SSH non riuscito.
 - L'indirizzo IP "86.212.199.60": IP da cui proviene il tentativo fallito.

2. rex "Failed password for (invalid user)?(?<user>\w+) from (?<ip>86\.212\.199\.60) port (?<port>\d+)"

- Applica una **regex (espressione regolare)** per estrarre automaticamente i seguenti campi:
 - user: il nome dell'utente usato nel tentativo (es. root, admin, guest)
 - ip: fissato a 86.212.199.60 (per sicurezza e precisione)
 - port: la porta sorgente da cui il client ha tentato la connessione
- Gestisce anche il caso di "invalid user" (utente inesistente), grazie alla parte opzionale (invalid user)?.

3. table _time user port

- Visualizza i risultati in formato tabellare con tre colonne:
 - _time: orario esatto dell'evento
 - user: nome utente usato nel tentativo fallito
 - port: porta di origine dell'attaccante

Obiettivo della Query

- Raccogliere evidenze su **quali utenti** sono stati presi di mira.
- Identificare la **porta TCP** usata per capire se gli attacchi seguono un pattern.
- Permettere un'analisi forense o l'automazione della risposta (es. blocco IP o alert).

Query Splunk 4.

Questa query che andremmo a creare servirà per identificare gli indirizzi IP che hanno tentato di accedere (“Failed Password”) al sistema piu di 5 volte.

La query dovrebbe mostrare l’indirizzo IP e il numero di tentativi.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following query: `index=* "Failed password" | rex "failed password for (invalid user)?(?<user>\w*) from (?<ip>\d+\.\d+\.\d+\.\d+)" | stats count by ip | where count > 5 | sort -count`. The results are displayed in a table with 71 events. The table has two columns: 'ip' and 'count'. The top results are:

ip	count
107.3.146.207	54
109.169.32.135	15
110.138.30.229	6
110.159.208.78	27
121.254.179.199	54
121.9.245.177	21
124.160.192.241	48
125.89.78.6	68
128.241.220.82	90
142.162.221.28	57
142.233.200.21	6
170.192.178.10	45

The screenshot shows the Splunk Enterprise search interface with the same query as above, but with an additional filter: `| search ip="107.3.146.207"`. The results are displayed in a table with 54 events. The table has two columns: 'Ora' and 'Evento'. The top results are:

Ora	Evento
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[3491]: Failed password for invalid user vpxuser from 107.3.146.207 port 1087 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwt/secure
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[2395]: Failed password for invalid user system from 107.3.146.207 port 1383 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwt/secure
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[2832]: Failed password for invalid user vmware from 107.3.146.207 port 3172 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwt/secure
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[2332]: Failed password for invalid user noone from 107.3.146.207 port 3995 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwt/secure
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[1169]: Failed password for queasy from 107.3.146.207 port 3737 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwt/secure
03/05/25 13:22:30,000	Fri May 03 2025 13:22:30 mailsv sshd[15083]: Failed password for bin from 107.3.146.207 port 3278 ssh2

È stata condotta un’analisi su oltre 3.200 tentativi di accesso SSH falliti, estraendo automaticamente gli indirizzi IP e il numero di eventi generati. L’IP 107.3.146.207 ha effettuato 54 tentativi non autorizzati, utilizzando diversi nomi utente generici. L’attività è compatibile con un attacco di tipo brute force automatizzato.

Sono stati rilevati **54 eventi**, tutti provenienti dallo stesso IP, verso lo stesso host (DESKTOP-8CAJRT0) i tentativi sono stati effettuati usando numerosi nomi utente diversi:

```
vpxuser, system, vmware, noone, queasy, bin...
```

Le porte di origine cambiano a ogni connessione, segno di un attacco automatizzato con rotazione.

La query scritta è la seguente:

```
index=* "Failed password" | rex "Failed password for (invalid user )?(?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+)" | stats count by ip | where count > 5 | sort -count uente:
```

Descrizione Tecnica della Query

Questa query è progettata per **identificare gli indirizzi IP** che hanno effettuato **più di 5 tentativi di accesso SSH falliti**, con lo scopo di rilevare comportamenti anomali, attacchi brute force o scansioni automatizzate.

Spiegazione passo-passo

```
index=* "Failed password"
```

- Cerca nei log di **tutti gli indici** (`index=*`) gli eventi che contengono la stringa "Failed password", tipica dei tentativi di accesso SSH non riusciti. `rex "Failed password for (invalid user)?(?<user>\w+) from (?<ip>\d+\.\d+\.\d+\.\d+)"`
- Applica una **regex** per estrarre due elementi dal messaggio:
 - `user`: il nome utente usato nel tentativo
 - `ip`: l'indirizzo IP del client che ha effettuato il tentativo
- Gestisce sia utenti validi che "invalid user" con una parte opzionale nella regex. `stats count by ip`
- Conta quanti eventi sono stati generati da **ciascun indirizzo IP**. `where count > 5`
- Mostra solo gli IP che hanno **più di 5 tentativi falliti**, escludendo quindi casi isolati o sporadici. `sort -count`
- Ordina il risultato in **ordine decrescente**, mettendo in cima gli IP più attivi (più pericolosi o sospetti).

Obiettivo della Query

- Identificare potenziali **attacchi brute force SSH**.
- Evidenziare IP con **comportamenti anomali o automatizzati**.
- Facilitare il **blocco di IP ostili** a livello di firewall o IDS.

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



Spiegazione riga per riga

◆ index=* "500"

- Cerca in **tutti gli indici** log che contengono esattamente la stringa "500", **in qualsiasi campo non strutturato** (come `_raw`).
- Tuttavia, **non cerca nel campo `status`** (a meno che il valore 500 non sia anche nel testo grezzo dell'evento).

◆ | `table _time host source`

- Costruisce una **tabella** che mostra:
 - `_time`: data e ora dell'evento
 - `host`: nome del server o sorgente che ha generato il log
 - `source`: percorso o nome del file log da cui proviene l'evento

La query in questione è stata scritta così :

`index=* "500" | table _time host source`

Ultima fase vedremo un'analisi fornita dall'IA sui vari log fornitogli

Rapporto Sintetico di Analisi Log - Sicurezza Informatica



1. Tentativi di Accesso Non Autorizzati

Durante l'analisi dei log sono stati individuati numerosi **tentativi di accesso falliti** al sistema tramite protocollo SSH, provenienti da indirizzi IP sospetti. Tra i più attivi:

- **194.215.205.19** → 12 tentativi
- **86.212.199.60** → 7 tentativi
- **94.229.0.21** → 1 tentativo

Questi comportamenti sono **tipici degli attacchi brute-force**, dove un utente malintenzionato prova a indovinare nome utente e password ripetutamente. Anche se nessuno di questi tentativi ha avuto successo, rappresentano una **minaccia concreta** alla sicurezza del sistema.



2. Accessi Autenticati

È stato registrato un **accesso riuscito** da parte dell'utente `djohnson`, proveniente dall'IP **10.3.10.46** sulla porta **9606** (protocollo SSH).

Al momento l'attività sembra lecita, ma è importante continuare a monitorarla nel tempo per assicurarsi che rimanga coerente con il comportamento previsto dell'utente.

3. Errori Server (HTTP 500)

Tra i log web è stato rilevato un **errore interno del server** (codice 500) legato a una richiesta HTTP inviata dall'IP **81.18.148.190**.

Questi eventi possono essere sintomo di:

- un **malfunzionamento interno** dell'applicazione web,
- oppure un possibile **tentativo di attacco** per generare crash o instabilità (es. attacchi DoS leggeri).

Sebbene isolato, un errore 500 su input anomalo deve essere valutato con attenzione.

□ 4. Osservazioni Finali e Raccomandazioni

I dati analizzati mostrano **attività potenzialmente malevole**, soprattutto in relazione ai tentativi di accesso ripetuti e agli errori generati sul web server.

Si consiglia di:

- **Bloccare automaticamente gli IP sospetti** dopo un certo numero di tentativi falliti, ad esempio con strumenti come *Fail2Ban*.
 - **Implementare l'autenticazione a due fattori** per aumentare la sicurezza degli accessi remoti.
 - **Monitorare regolarmente i log di sistema e web**, per identificare in tempo reale comportamenti anomali.
 - **Indagare sugli errori 500** per comprendere se si tratta di bug applicativi o tentativi mirati di causare instabilità.
-