

Nuova ricerca

Salva come

Crea vista tabella

Chiudi

source="tutorialdata.zip:*" sourcetype="*" "Failed password" ip="*" | stats count by ip | where count > 5

Da 01/11/24 fino a 30/11/24

Q

✓ 4.564 eventi (01/11/24 00:00:00,000 - 01/12/24 00:00:00,000)

Nessun campionamento degli eventi

Processo

II

Modaltà intelligente

Eventi

Pattern

Statistiche (137)

Visualizzazione

20 per pagina

Formato

Anteprima

< Prec

1

2

3

4

5

6

7

Avanti >

ip	count
107.3.146.207	66
108.65.113.83	18
109.169.32.135	86
110.159.208.78	6
112.111.162.4	10
117.21.246.164	64
12.130.60.4	40
12.130.60.5	32
121.254.179.199	6
121.9.245.177	58
123.196.113.11	20
123.30.108.208	64
124.160.192.241	58
125.17.14.100	28
128.241.220.82	74
130.253.37.97	26

Conclusioni ChatGPT:

- **Attività sospette su IP specifici:** Alcuni IP hanno un numero significativamente alto di tentativi di accesso falliti, come:
 - 109.169.32.135 con 86 tentativi falliti
 - 107.3.146.207 con 66 tentativi falliti
 - 117.21.246.164 con 64 tentativi falliti
 - 112.111.162.4 e 123.196.113.11 con 64 tentativi falliti ciascuno.

Questi IP potrebbero indicare attività brute-force o altri tentativi non autorizzati di accesso.

- **Distribuzione degli IP:** Ci sono vari IP con un numero moderato di tentativi falliti (tra 10 e 40). Tuttavia, la presenza di molti IP con più di 5 tentativi falliti potrebbe indicare che l'infrastruttura è sotto un attacco distribuito, con diversi IP che provano ad accedere ripetutamente.
- **Importanza del monitoraggio continuo:** Il numero complessivo di eventi nella ricerca è di 4.564. Questo suggerisce che l'infrastruttura sta subendo un volume elevato di tentativi di accesso falliti, il che potrebbe necessitare ulteriori azioni di sicurezza, come bloccare IP con accessi falliti ripetuti o rafforzare le politiche di autenticazione.

Azioni consigliate:

- **Blocco temporaneo degli IP sospetti:** Implementare una regola di blocco temporaneo per gli IP con un elevato numero di tentativi di accesso falliti.
- **Aggiungere un sistema di alerting:** Configurare alert che notificano l'amministratore quando un IP supera una soglia di tentativi falliti.
- **Considerare il geofencing:** Se molti di questi IP non provengono da regioni fidate, valutare un blocco su base geografica per ridurre ulteriormente l'esposizione agli attacchi.

In sintesi, questo screenshot suggerisce una potenziale attività di accesso malevola o brute-force sulla rete, e sarebbe consigliabile un monitoraggio più attento e l'implementazione di contromisure per ridurre tali tentativi di accesso non autorizzato.