

splunk>enterprise App ▾ Administrator ▾ 1 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca

host=dati_test source="tutorialdata.zip:*" sourcetype="*" "Failed password" Da 01/11/24 fino a 30/11/24

✓ 6.454 eventi (01/11/24 00:00:00,000 - 01/12/24 00:00:00,000) Nessun campionamento degli eventi ▾ Processo ▾ || ▾ ▾ ▾ ▾ ▾ Modalità intelligente ▾

Eventi (6.454) Pattern Statistiche Visualizzazione

Formato timeline ▾ - Zoom indietro + Zoom area selezionata X Deseleziona 1 giorno per colonna

Elenco ▾ Formato 50 per pagina ▾ < Prec 1 2 3 4 5 6 7 8 ... Avanti >

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI
a host 1
a ip 100+
a source 4
a sourcetype 1

CAMPI INTERESSANTI
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 2
a date_wday 1
date_year 1
a date_zone 1
a Index 1
linecount 1

i	Ora	Evento
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = dati_test ip = 194.8.74.23 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = dati_test source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = dati_test ip = 194.8.74.23 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = dati_test source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = dati_test ip = 194.8.74.23 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = dati_test source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[1020]: Failed password for root from 194.8.74.23 port 3807 ssh2

Conclusioni ChatGPT:

- **Indirizzo IP sospetto:** Tutti gli eventi registrati sono associati all'IP `194.8.74.23`. Questo indica che questo IP sta tentando di accedere al sistema in modo non autorizzato, provando diverse combinazioni di nome utente e password.
- **Tentativi di accesso falliti con utenti diversi:** Gli eventi mostrano tentativi di accesso falliti per una varietà di nomi utente, come `appserver`, `root`, `testuser`, `apache`, `mongodb`, e `mail`. Questo è un chiaro segnale di "attacco brute-force" o "attacco dizionario", in cui l'attaccante cerca di accedere utilizzando nomi utente comuni o privilegiati.
- **Frequenza e persistenza dell'attacco:** I tentativi sono registrati a pochi millisecondi di distanza l'uno dall'altro, come evidenziato dal timestamp (es. tutti alle `04:36:40,000` del 1° novembre 2024). Questo comportamento suggerisce che si tratta di un attacco automatizzato piuttosto che di tentativi manuali.
- **Differenti porte SSH utilizzate:** L'attaccante sta provando a connettersi tramite porte SSH diverse, come `3351`, `3768`, `3626`, `4604`, ecc. Questa tecnica può indicare che l'attaccante sta cercando porte aperte alternative al fine di eludere eventuali regole di firewall o monitoraggio che possano bloccare la porta SSH predefinita (generalmente la 22).

Azioni consigliate:

- **Bloccare l'IP sospetto:** L'IP `194.8.74.23` dovrebbe essere bloccato immediatamente a livello di firewall per prevenire ulteriori tentativi di accesso.
- **Limitazione della frequenza di tentativi di accesso (Rate limiting):** Implementare un limite di tentativi di accesso falliti per ogni IP per ridurre l'efficacia di attacchi brute-force.
- **Utilizzare l'autenticazione a due fattori (2FA):** Applicare l'autenticazione a due fattori sugli account con privilegi elevati, come `root` e altri account amministrativi, per aumentare la sicurezza.
- **Monitoraggio continuo e alerting:** Configurare alert per notificare gli amministratori di sistema quando un singolo IP registra un alto numero di tentativi falliti o quando ci sono accessi falliti su nomi utente privilegiati.

- **Rafforzamento della sicurezza SSH:** Considerare di limitare le connessioni SSH solo alle reti affidabili, configurare un meccanismo di blocco temporaneo su SSH dopo più tentativi falliti, e cambiare la porta SSH predefinita.