M6 - IA & Cybersecurity

Data: 01/03/2025

Team: ***DLLL Analyst***

Studenti

DANIELE NIEDDU

LUCIANO PANDOLFI

LORENZO D'UBALDI

LUCA VECCHIO

INDICE:

Traccia

Importare su Splunk i dati di esempio **“tutorialdata.zip”**:

1. 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.
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.
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.
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.
5. Crea una query Splunk per trovare tutti gli Internal Server Error.

Trarre delle conclusioni sui log analizzati utilizzando AI.

Introduzione

Introduzione

L’analisi dei log di sistema è una componente fondamentale nella Cyber Security, in quanto consente di individuare attività sospette, tentativi di intrusione e possibili vulnerabilità. In questo report, vengono analizzati i dati di esempio contenuti in *“tutorialdata.zip”* utilizzando **Splunk**, una piattaforma avanzata per la raccolta, l’indicizzazione e l’analisi dei log.

Cos’è Splunk e a cosa serve?

Splunk è una piattaforma di analisi dei dati che permette di raccogliere, analizzare e visualizzare in tempo reale i log generati da diversi sistemi, applicazioni e dispositivi di rete. Grazie alle sue capacità di ricerca e correlazione, Splunk aiuta le aziende e gli analisti di sicurezza a monitorare eventi critici, rilevare minacce informatiche e rispondere rapidamente a incidenti di sicurezza. La sua potenza risiede nella **Search Processing Language (SPL)**, un linguaggio avanzato che consente di estrarre informazioni rilevanti dai log e generare report dettagliati.

Svolgimento

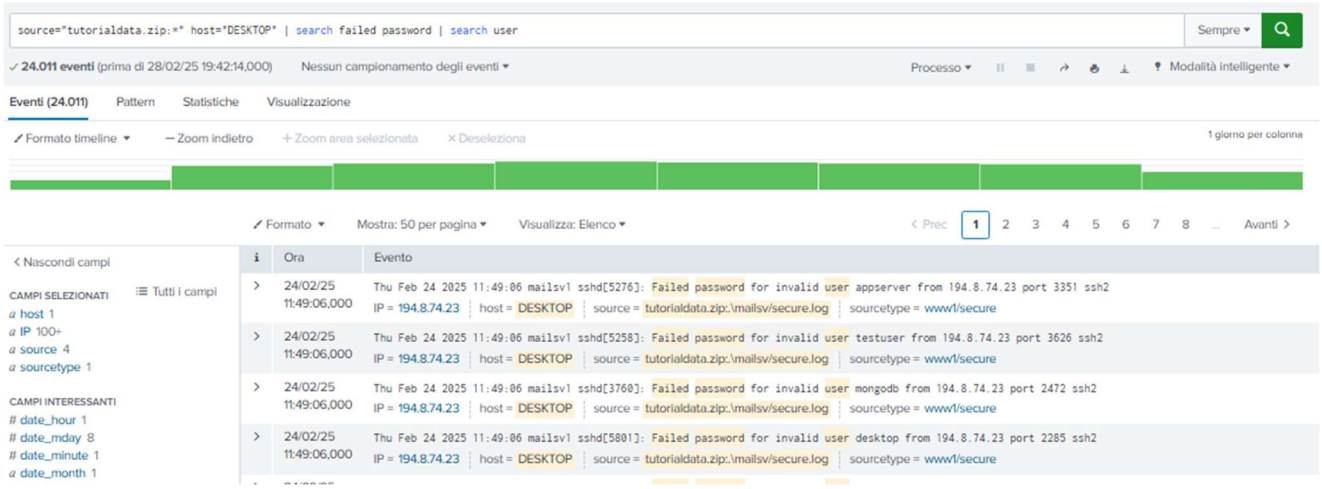
1. Identificazione di accessi falliti generici “Failed Password”

Traccia:

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.

Query utilizzata

```
source=” tutorialdata.zip: *” host=”DESKTOP” | search failed password | search user
```



Descrizione query e risultati ottenuti

Per individuare tutti i tentativi di accesso falliti con il messaggio “Failed password”, è stata utilizzata una query in Splunk che filtra i log provenienti dal file tutorialdata.zip, selezionando solo quelli generati dall’Host “DESKTOP”. Il successivo filtro “Failed password” isola i tentativi di accesso non riusciti, mentre “user” affina ulteriormente la ricerca per individuare gli utenti coinvolti. L’esecuzione della query fornisce un elenco dettagliato degli eventi, includendo il timestamp, l’indirizzo IP di origine, il nome utente e il messaggio di errore, utile per identificare possibili attacchi brute-force o attività sospette.

Analisi effettuata da IA

Data e Ora: L'evento si è verificato il Giovedì 24 febbraio 2025 alle 11:49:13.

Indirizzo IP: L'indirizzo IP di origine del tentativo di accesso non riuscito è 194.8.74.23.

Host: L'Host coinvolto nell'evento è identificato come "DESKTOP".

Origine del Log: La voce di log proviene da "tutorialdata.zip:\mailsv\secure.log".

Nome del server: mailsv1 | **ID del processo SSH daemon:** sshd[5276] | **Tipo di evento:** Fallito

Dettaglio dell'evento: Failed Password | **Stato dell'utente:** Non valido

Nome utente: appserver | **Numero di porta:** 3351 | **Versione del protocollo SSH:** ssh2

Conclusione e considerazioni:

L'evento analizzato suggerisce un possibile tentativo di accesso non autorizzato, che potrebbe rientrare in un attacco brute-force.
Per mitigare tali rischi, è consigliabile investigare l'indirizzo IP di origine e verificare se si tratta di un comportamento ricorrente. Misure di sicurezza aggiuntive come il blocco degli IP sospetti, l'implementazione dell'autenticazione a più fattori e l'adozione di politiche di password robuste possono contribuire a prevenire accessi non autorizzati e garantire un livello di sicurezza adeguato.

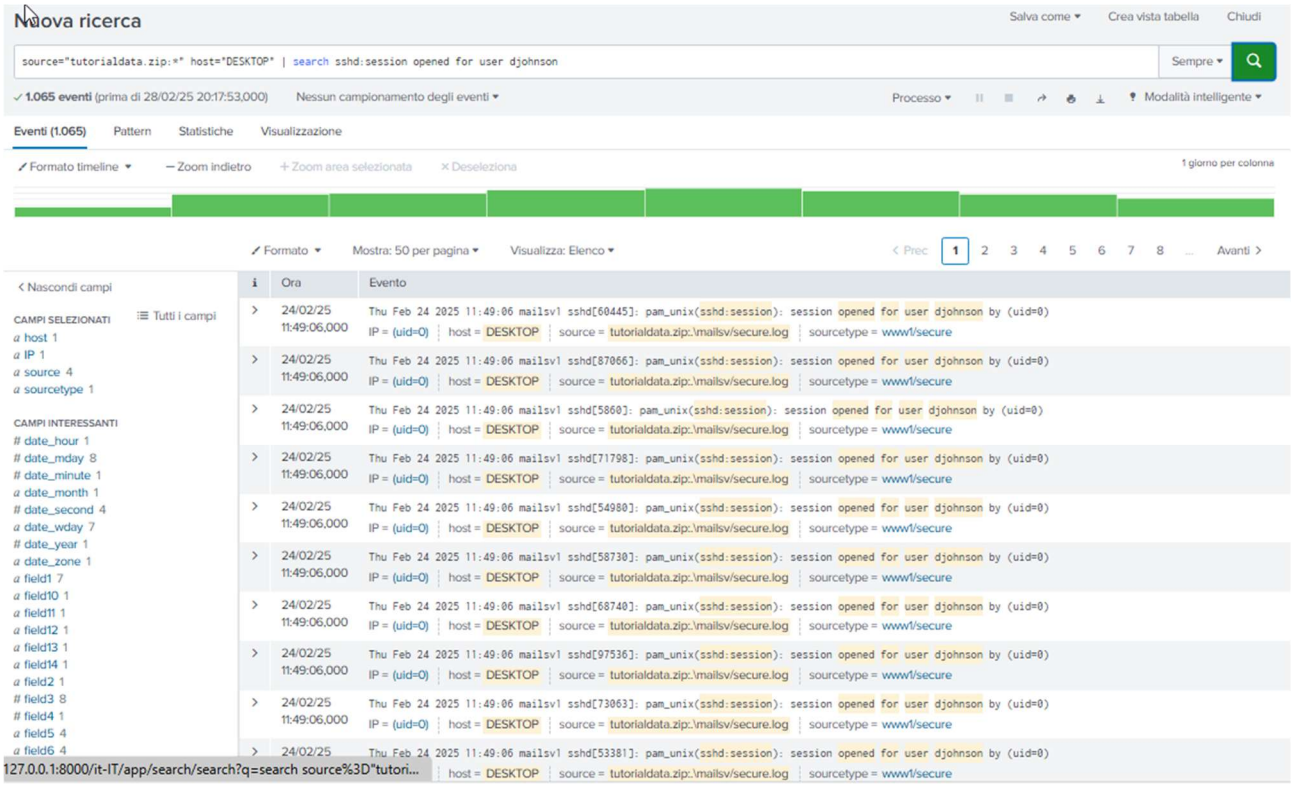
2. Identificazione sessioni SSH aperte

Traccia:

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.

Query utilizzata

```
source=" tutorialdata.zip: *" Host="DESKTOP" | search sshd: session opened for user djohnson
```



Descrizione query e risultati ottenuti

La query Splunk specifica analizza i log provenienti dall'archivio **tutorialdata.zip** generati dall'host DESKTOP.

Filtra i risultati per mostrare solo le righe contenenti la stringa:

"sshd: session opened for user Djohnson", permettendo di identificare le sessioni SSH aperte con successo per l'utente Djohnson.

Il numero di sessioni SSH aperte in un intervallo di tempo ristretto potrebbe indicare una possibile attività sospetta, specialmente se si osservano accessi provenienti da indirizzi IP inconsueti o da località non previste.

Analisi effettuata da IA

Data e Ora: 24 febbraio 2025 alle 11:49:13.

Host: DESKTOP.

Origine: tutorialdata.zip: \mailsv\secure.log.

Utente: Djohnson.

Evento: sshd [60445]: pam_unix (sshd: session): session opened for user djohnson by (uid=0).

_time: 2025-02-24T11:49:13.000+01:00.

Sourcetype: www1/secure.

Descrizione dell'Evento:

Il log indica che è stata aperta con successo una sessione SSH per l'utente "Djohnson". Questo evento è stato registrato dal daemon SSH (sshd) e ha coinvolto il sistema PAM (Pluggable Authentication Module), nello specifico il modulo pam_unix.

Informazioni sull'Utente e sull'Host:

L'utente coinvolto è "Djohnson" e la sessione è stata aperta sull'Host "DESKTOP". L'ID utente associato a questo evento è 0, che di solito corrisponde all'utente root, indicando che la sessione è stata aperta con privilegi di root.

Fonte e Indice:

L'evento è stato originato da "tutorialdata.zip: \mailsv\secure.log" ed è stato indicizzato sotto "main". Il tipo di origine è "www1/secure" e il server Splunk che ha elaborato questo log è "DESKTOP ".

Conclusione e Considerazioni

L'analisi dei log ha evidenziato l'apertura di una sessione SSH con privilegi di root per l'utente "Djohnson" su un Host identificato come "DESKTOP ". Sebbene l'evento di apertura della sessione possa essere legittimo, la presenza di privilegi elevati, unita alla correlazione di più sessioni in breve tempo, potrebbe indicare comportamenti sospetti. È fondamentale monitorare l'attività dell'utente, specialmente se i log successivi mostrano tentativi di accesso non autorizzato o provenienti da IP non riconosciuti. Ulteriori analisi potrebbero includere l'esame di eventi correlati per identificare attività anomale, come accessi preceduti da tentativi di brute-force.

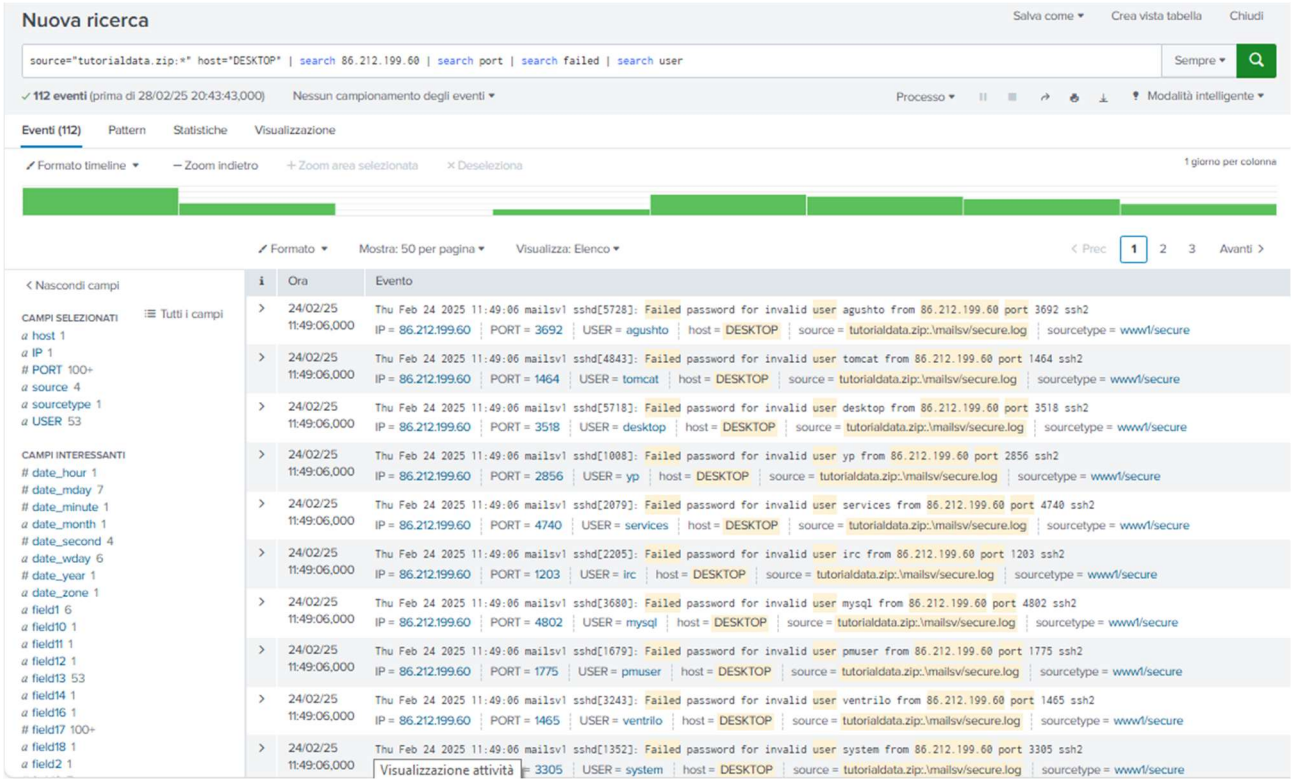
3. Identificazione degli accessi falliti provenienti dall'indirizzo IP “86.212.199.60”

Traccia:

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.

Query utilizzata

```
source=” tutorialdata.zip: *” host=”DESKTOP” | search 86.212.199.60 | search port | search failed | search user
```



Descrizione query e risultati ottenuti

La query analizzata si concentra su log provenienti da un archivio compresso, tutorialdata.zip. Vengono selezionati solo i log relativi all'Host denominato "DESKTOP" e, successivamente, filtrati per l'indirizzo IP specifico 86.212.199.60, per restringere ulteriormente i risultati ai tentativi di accesso falliti. La ricerca si concentra anche sulle porte utilizzate e sui tentativi di connessione falliti, filtrando quelli che contengono la parola "user", per identificare i nomi utente associati ai fallimenti. Il risultato di questa query restituirà una serie di eventi che mostrano i tentativi di accesso non riusciti da parte dell'IP 86.212.199.60. Ogni evento includerà informazioni come il timestamp del tentativo, l'indirizzo IP di origine, il nome utente, la porta utilizzata per il tentativo e il messaggio di errore, che può rivelare dettagli come una password errata o l'accesso negato. Se si osservano ripetuti tentativi falliti in breve tempo, potrebbe trattarsi di un attacco di tipo brute-force. Inoltre, se l'IP non appartiene a un utente autorizzato, è probabile che si tratti di un tentativo di intrusione esterna. L'analisi di questi risultati potrebbe essere integrata con ulteriori query per verificare eventuali successi nell'autenticazione, suggerendo così un potenziale accesso compromesso.

Analisi effettuata da IA

Data e Ora: 24 febbraio 2025 alle 11:49:13.

Host: DESKTOP

Origine: tutorialdata.zip: \mailsv\secure.log.

Server: mailsv1.

Processo: sshd [5728].

Descrizione dell'Evento: Tentativo di accesso fallito tramite SSH con password.

Utente: Utente non valido "Agushto".

Indirizzo IP: 86.212.199.60.

Analisi degli Eventi

Tentativo di Accesso Non Riuscito:

- Il log indica un tentativo di accesso fallito tramite SSH sul server "mailsv1". Il nome utente utilizzato è "agushto", che non è un utente valido, e il tentativo è stato effettuato sulla porta 3692.

Origine del Tentativo:

- Il tentativo di accesso è stato effettuato dall'indirizzo IP 86.212.199.60. Questo suggerisce che l'accesso potrebbe provenire da una fonte esterna non autorizzata.

Processo Coinvolto:

- Il processo coinvolto è "sshd" con l'ID processo 5728. Questo conferma che il tentativo è stato fatto utilizzando il protocollo Secure Shell (SSH).

Dettagli di Autenticazione:

- Il tentativo di accesso ha fallito a causa di una password non valida per un utente non riconosciuto. Questo è indicativo di un potenziale attacco brute force o un tentativo di accesso non autorizzato.

Conclusioni e Considerazioni:

L'analisi dei log suggerisce che l'indirizzo IP **86.212.199.60** stia tentando ripetutamente di accedere al sistema con credenziali non valide. Questo comportamento, se ripetuto nel tempo, potrebbe indicare un tentativo di attacco di tipo brute-force, mirato a ottenere accesso a una risorsa protetta. È essenziale monitorare costantemente questi tentativi e adottare misure proattive per proteggere il sistema. L'analisi storica dei log potrebbe aiutare a identificare eventuali pattern ricorrenti, fornendo ulteriori informazioni per mitigare il rischio di attacchi futuri.

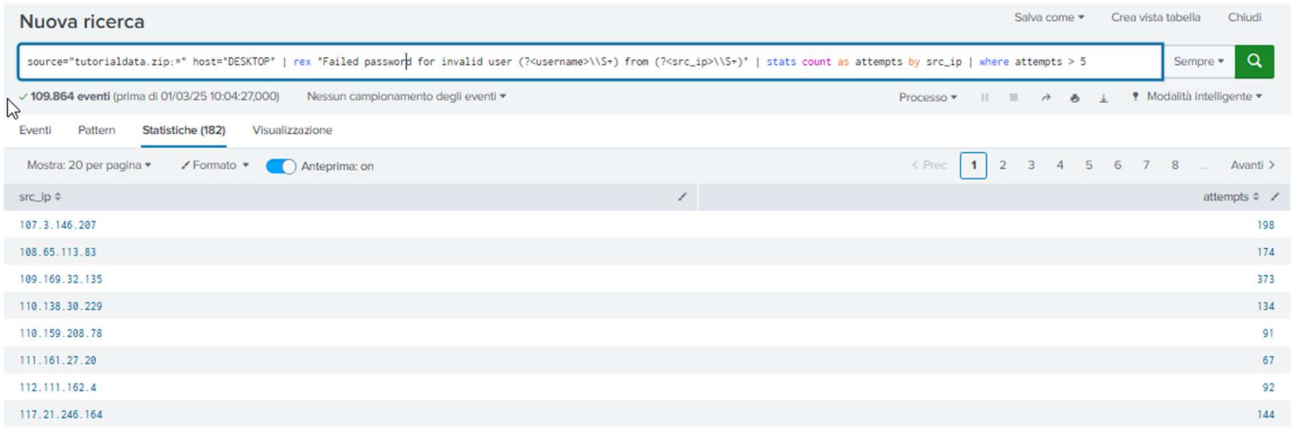
4. Identificazione degli IP che hanno tentato di accedere (“Failed password”) al sistema più di 5 volte

Traccia:

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.

Query utilizzata

source=” tutorialdata.zip: *” host=”DESKTOP” | rex "Failed password for invalid user (? <username>\S+) from (? <src_ip>\S+)" | stats count as attempts by src_ip | where attempts > 5



Descrizione query e risultati ottenuti

La query che abbiamo utilizzato per l’analisi dei log SSH si articola in diverse sezioni.
Prima di tutto, definiamo la fonte dei log attraverso il parametro **source="tutorialdata.zip: *"** e specifichiamo l’host da cui provengono i dati con **host="DESKTOP"**.
Successivamente, l’espressione regolare:
rex "Failed password for invalid user (? <username>\S+) from (? <src_ip>\S+)" ci consente di estrarre due informazioni fondamentali: il nome utente (**username**) e l’indirizzo IP di origine (**src_ip**).
Per avere una panoramica dei tentativi, utilizziamo il comando: **stats count as attempts by src_ip** che calcola il numero di tentativi di accesso falliti per ciascun indirizzo IP.
Infine, il filtro **where attempts > 5** ci consente di concentrarci esclusivamente sugli indirizzi IP che hanno effettuato più di cinque tentativi di accesso falliti. L’esecuzione della query produce una tabella con due colonne principali:

l’indirizzo IP di origine (src_ip) e il numero di **tentativi di accesso falliti (attempts)** per ciascun IP, includendo solo quelli con un numero di tentativi superiore a cinque.

Analisi effettuata da IA

Analisi dei Risultati

Analizzando i risultati, possiamo notare che ci sono diversi indirizzi IP con un numero significativo di tentativi di accesso falliti. Gli indirizzi IP con il numero più elevato di tentativi potrebbero rappresentare potenziali minacce di sicurezza e meritano ulteriori investigazioni.

Opinione Personale

In base ai dati analizzati, è evidente che ci sono tentativi di accesso non autorizzati ripetuti provenienti da diverse sorgenti IP. Questi tentativi potrebbero essere indicativi di attacchi brute force. Consiglierei di adottare misure di sicurezza aggiuntive, come il blocco degli indirizzi IP sospetti e l'implementazione di autenticazione a due fattori (2FA) per migliorare la sicurezza dell'accesso.

Conclusioni e Considerazioni

La query Splunk ci ha permesso di identificare indirizzi IP con un numero elevato di tentativi di accesso falliti per utenti non validi. È essenziale monitorare regolarmente questi log e adottare misure di sicurezza appropriate per proteggere i sistemi da potenziali attacchi.

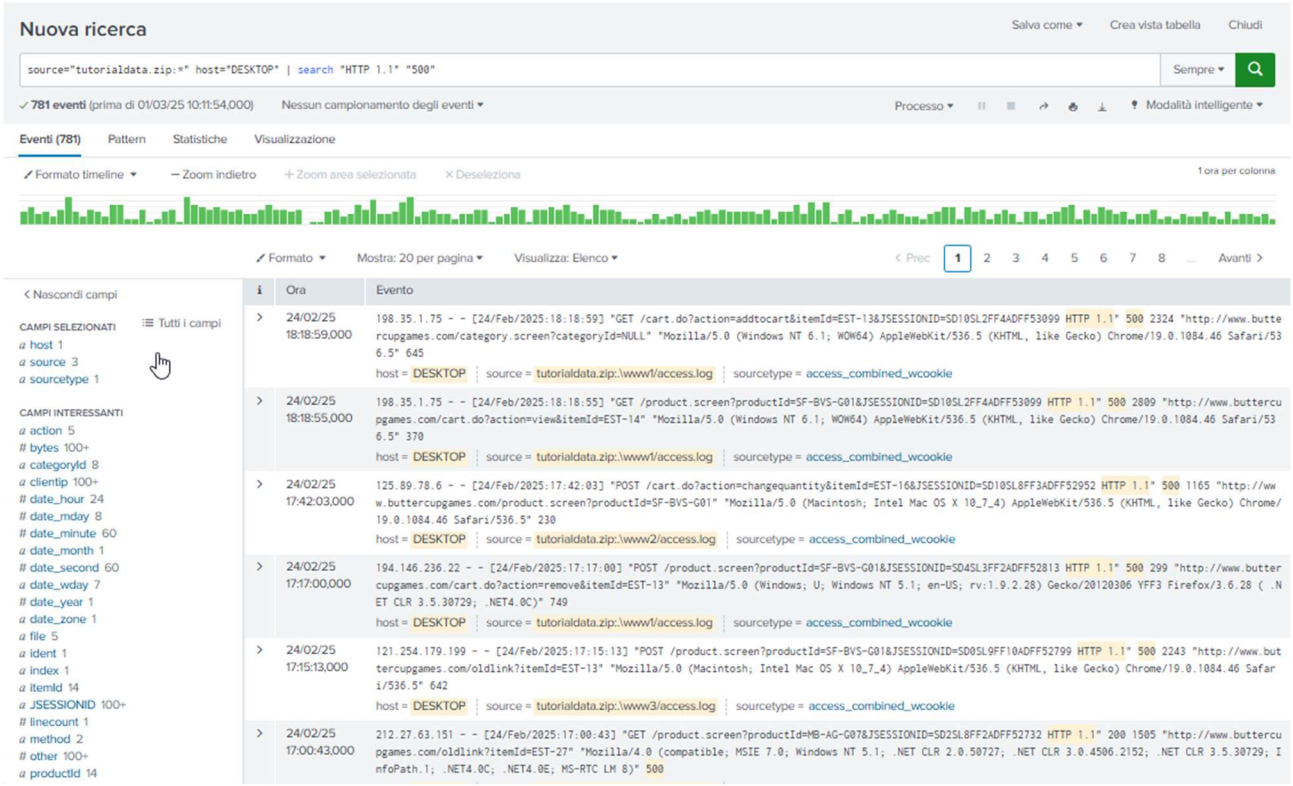
5. Ricerca di tutti gli Internal Server Error

Traccia:

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

Query utilizzata

source=” tutorialdata.zip: *” host=”DESKTOP” | search “HTTP 1.1” “500”



Descrizione query e risultati ottenuti

La query utilizzata è stata progettata per filtrare e analizzare i log contenuti nel file tutorialdata.zip. Il filtro si concentra sui log provenienti dal sistema con hostname "DESKTOP" e contiene la ricerca dei termini "HTTP 1.1" e "500", al fine di individuare gli errori di tipo Internal Server Error (errore 500). I risultati ottenuti mostrano una richiesta GET specifica al percorso "/cart.do", che tenta di aggiungere un articolo al carrello dell’utente, con un errore di tipo 500 registrato nel log.

Analisi effettuata da IA

Errore del Server:

- Il log indica un errore "500 Internal Server Error", che è un errore generico del server. Significa che il server ha incontrato una condizione inaspettata che gli ha impedito di soddisfare la richiesta.

Richiesta HTTP GET:

- La richiesta HTTP GET è per l'URL /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099.
  Questa richiesta tenta di aggiungere un articolo (itemId=EST-13) al carrello.

Sessione e Indirizzo IP:

- La richiesta è associata a una sessione specifica (JSESSIONID=SD10SL2FF4ADFF53099) e proviene dall'indirizzo IP 198.35.1.75.

Referer e User Agent:

- Il referer è http://www.buttercupgames.com/category.screen?categoryId=NULL, suggerendo che l'utente stava navigando nella categoria degli articoli prima di aggiungere l'articolo al carrello.
- L'User Agent indica che la richiesta è stata effettuata da un browser Chrome su Windows NT 6.1 (Windows 7).

Conclusioni e Considerazioni

L'errore 500 può derivare da diversi fattori, tra cui problemi nel codice del server, mancanza di risorse come memoria o spazio su disco, configurazioni errate o malfunzionamenti di componenti backend. Per risolvere il problema, è fondamentale esaminare il codice del server responsabile della gestione dell'endpoint "/cart.do", in modo da identificare eventuali bug o problemi logici. È anche importante verificare che il server disponga di risorse adeguate a gestire le richieste, controllando l'utilizzo della CPU, della memoria e dello spazio su disco. L'abilitazione dei log di debug può fornire informazioni dettagliate su dove si verifica l'errore, permettendo di individuare con precisione il punto di fallimento. Per evitare simili problematiche in futuro, potrebbe essere utile eseguire test di carico sul server per identificare eventuali colli di bottiglia e monitorare costantemente le risorse del sistema. Implementare un sistema di monitoraggio continuo potrebbe contribuire a risolvere tempestivamente eventuali altri errori e ottimizzare le performance del server.

Azioni preventive e Conclusione Generale

Blocco IP e autenticazione avanzata:

Blocco IP: Implementare un sistema di blacklist per bloccare automaticamente gli indirizzi IP noti per attività sospette o malevole. Questo riduce il rischio di attacchi ripetuti da fonti già identificate.
Autenticazione avanzata: Utilizzare metodi di autenticazione a più fattori (MFA) per l'accesso SSH. Questo assicura che solo utenti autorizzati possano accedere al sistema, aggiungendo un livello di sicurezza attraverso qualcosa che l'utente conosce (password) e qualcosa che possiede (es. telefono per l'OTP).

Monitoraggio avanzato:

Monitoraggio continuo: Stabilire un sistema di monitoraggio in tempo reale che controlli costantemente tutte le attività di rete e di sistema per identificare comportamenti anomali. o
Alerting su azioni sospette: Implementare meccanismi di allarme che notifichino immediatamente gli amministratori in caso di attività sospette, come tentativi ripetuti di accesso falliti o incremento del traffico anomalo. Questo permette interventi rapidi per mitigare potenziali minacce.

Controllo e limitazione delle API:

Protezione delle API: Implementare controlli di accesso rigidi per le API esposte, utilizzando chiavi di accesso e limiti di rate per prevenire abusi.
Anti-bot: Utilizzare soluzioni come CAPTCHA per distinguere tra traffico umano e bot, riducendo il rischio di automazione malevola e proteggendo il sito da scraping e altre attività dannose.

Implementazione di meccanismi di difesa:

Contro SQL Injection: Utilizzare tecniche di parametrizzazione delle query e validazione dei dati di input per proteggere il database dagli attacchi di iniezione SQL.
Monitoraggio del credential stuffing: Implementare sistemi di rilevamento per identificare e bloccare tentativi di accesso non autorizzati che sfruttano credenziali rubate da altre fonti. Questo può includere l'uso di database di credenziali compromesse per confrontare gli accessi.

Conclusione:

In conclusione, l'analisi approfondita dei log ha mostrato chiaramente che il nostro sistema è un bersaglio attraente per gli attacchi esterni. Le misure preventive proposte sono essenziali per fortificare la nostra infrastruttura contro le minacce. Adottando queste azioni, non solo miglioriamo la nostra sicurezza, ma aumentiamo anche la resilienza complessiva del sistema, garantendo così una protezione più solida e affidabile contro tentativi di compromissione futuri.