

M6 - Progetto Finale - Splunk

Obiettivo dell'esercitazione

L'attività ha l'obiettivo di acquisire familiarità con l'utilizzo di Splunk per l'analisi e la correlazione di log provenienti da diverse sorgenti. In particolare, sono state sviluppate query mirate per individuare eventi rilevanti come tentativi di autenticazione falliti e errori di tipo Internal Server Error. L'esercitazione ha previsto la formulazione delle ricerche, l'interpretazione dei risultati e la loro rappresentazione in formato tabellare e cronologico, al fine di supportare attività di monitoraggio e rilevamento di potenziali anomalie di sicurezza o di funzionamento di sistema.

Identificazione di "Failed Password"

Per identificare tutti i tentativi di accesso falliti (Failed password), è stata utilizzata la seguente query:

```
- index=tutorialdata "Failed password" | table _time src user message
```

La query cerca gli eventi con la frase "Failed password" nell'indice tutorialdata. I risultati sono stati visualizzati in una tabella che mostra il timestamp, il nome utente e il messaggio dell'evento, fornendo un quadro chiaro di tutti i tentativi di accesso non riusciti.

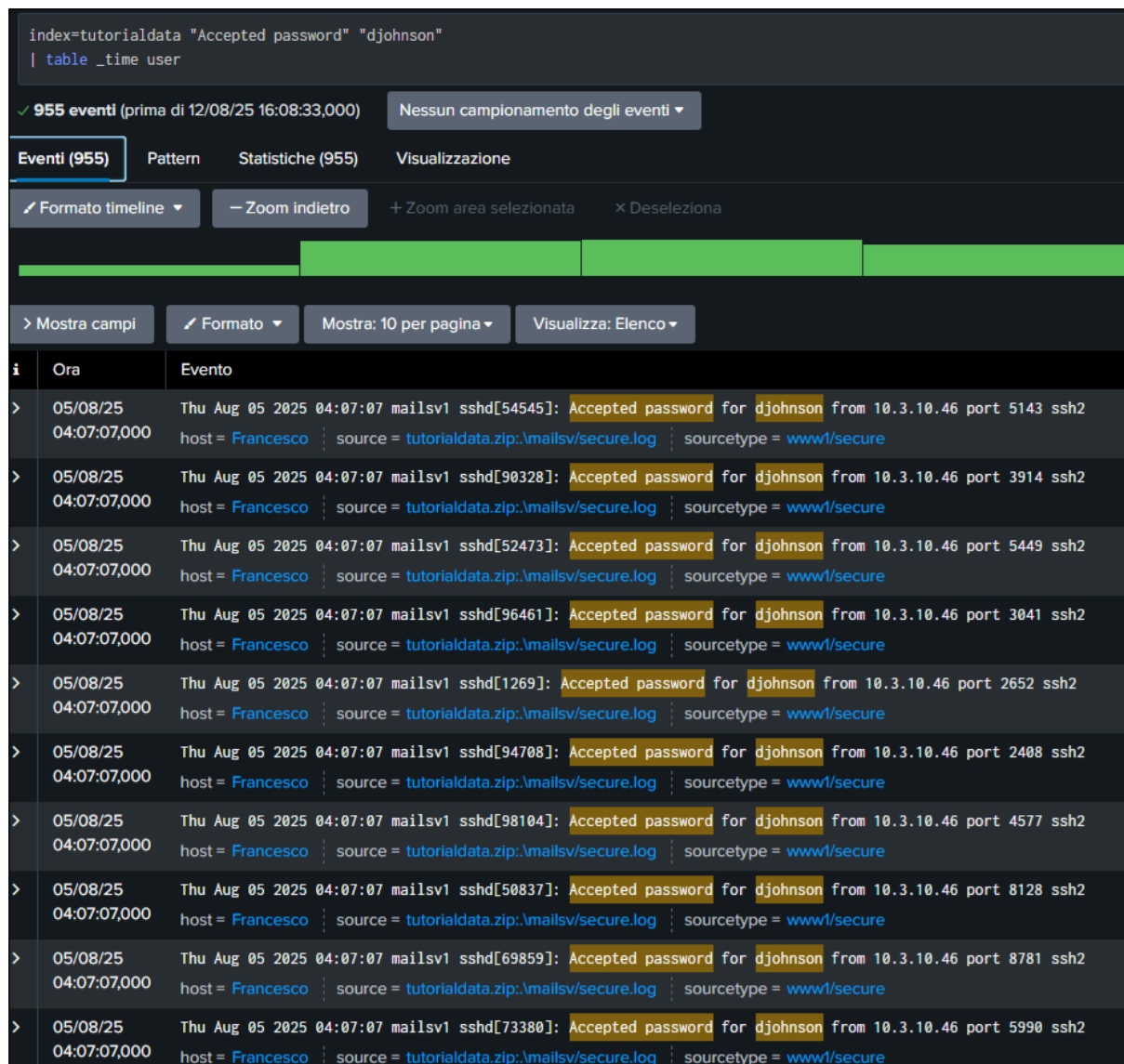
index=tutorialdata "Failed password" table _time src user message		
✓ 33.253 eventi (01/07/25 00:00:00,000 - 01/09/25 00:00:00,000) Nessun campionamento degli eventi ▼		
Eventi (33.253) Pattern Statistiche (33.253) Visualizzazione		
✓ Formato timeline ▼ — Zoom indietro + Zoom area selezionata × Deseleziona		
Mostra campi Formato ▼ Mostra: 10 per pagina ▼ Visualizza: Elenco ▼		
i	Ora	Evento
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

Analisi delle sessioni SSH di "djohnson"

Per identificare tutte le sessioni SSH aperte con successo per l'utente djohnson, è stata usata la seguente query:

```
- index=tutorialdata "Accepted password" "djohnson" | table _time user
```

La query ricerca gli eventi nell'indice tutorialdata che indicano un'autenticazione riuscita (Accepted password) per l'utente djohnson. I risultati sono presentati in una tabella che mostra il timestamp e l'ID utente, fornendo una lista delle sessioni SSH andate a buon fine.



index=tutorialdata "Accepted password" "djohnson"
| table _time user

✓ 955 eventi (prima di 12/08/25 16:08:33,000) Nessun campionamento degli eventi ▼

Eventi (955) Pattern Statistiche (955) Visualizzazione

Formato timeline ▼ - Zoom indietro + Zoom area selezionata × Deseleziona

> Mostra campi Formato ▼ Mostra: 10 per pagina ▼ Visualizza: Elenco ▼

i	Ora	Evento
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[90328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[94708]: Accepted password for djohnson from 10.3.10.46 port 2408 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[98104]: Accepted password for djohnson from 10.3.10.46 port 4577 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[50837]: Accepted password for djohnson from 10.3.10.46 port 8128 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[69859]: Accepted password for djohnson from 10.3.10.46 port 8781 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[73380]: Accepted password for djohnson from 10.3.10.46 port 5990 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

Analisi dei tentativi falliti dall'IP 86.212.199.60

Per identificare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP 86.212.199.60, è stata utilizzata la seguente query:

```
- index=tutorialdata "Failed password" "86.212.199.60" | table _time user port
```

La query filtra gli eventi per la frase "Failed password" e l'indirizzo IP specifico. I risultati sono presentati in una tabella che mostra il timestamp, il nome utente e il numero di porta, fornendo una panoramica completa dei tentativi falliti da quell'indirizzo IP.

index=tutorialdata "Failed password" "86.212.199.60" table _time user port		
✓ 158 eventi (prima di 12/08/25 16:11:17,000) Nessun campionamento degli eventi ▼		
Eventi (158)	Pattern	Statistiche (158) Visualizzazione
✓ Formato timeline ▼	– Zoom indietro	+ Zoom area selezionata × Deseleziona
> Mostra campi ✓ Formato ▼ Mostra: 10 per pagina ▼ Visualizza: Elenco ▼		
i	Ora	Evento
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2079]: Failed password for invalid user services from 86.212.199.60 port 4740 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2205]: Failed password for invalid user irc from 86.212.199.60 port 1203 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3680]: Failed password for invalid user mysql from 86.212.199.60 port 4802 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1679]: Failed password for invalid user pmuser from 86.212.199.60 port 1775 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

Individuazione degli IP con più di 5 tentativi di accesso falliti

Per identificare gli indirizzi IP che hanno tentato di accedere più di 5 volte, è stata utilizzata la seguente query:

- `index=tutorialdata "Failed password" | stats count AS tentativi by src_ip | where tentativi > 5 | table src_ip tentativi`

La query filtra prima gli eventi che contengono "Failed password". Successivamente, raggruppa gli eventi per indirizzo IP di origine (src_ip), conta il numero di tentativi e lo rinomina come tentativi. Infine, mostra solo gli IP con un numero di tentativi superiore a 5, visualizzando l'indirizzo IP e il numero di tentativi.

```
index=tutorialdata "Failed password"
| stats count AS tentativi by src_ip
| where tentativi > 5
| table src_ip tentativi
```

✓ 33.253 eventi (prima di 12/08/25 16:18:13,000) Nessun campionamento degli eventi ▾

Eventi (33.253) Pattern Statistiche (0) Visualizzazione

✓ Formato timeline ▾ - Zoom indietro + Zoom area selezionata X Deseleziona

> Mostra campi ✓ Formato ▾ Mostra: 10 per pagina ▾ Visualizza: Elenco ▾

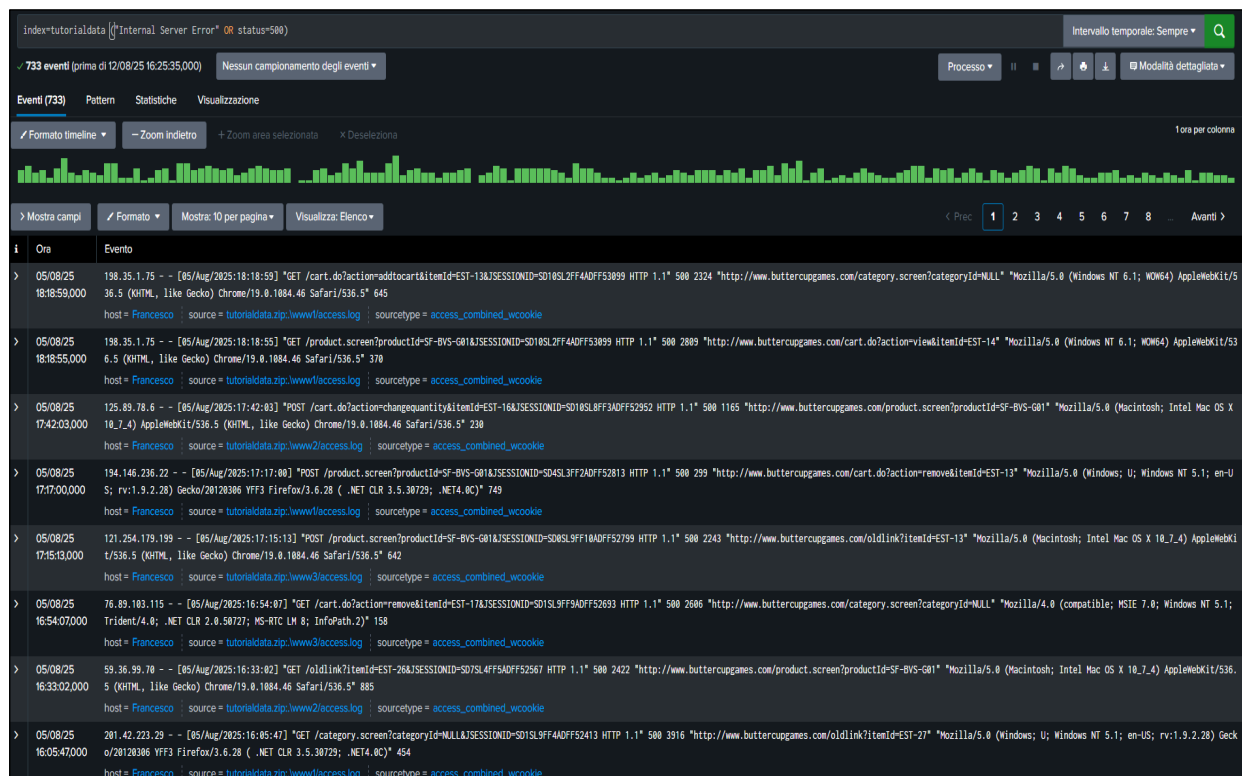
i	Ora	Evento
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1256]: Failed password for nobody from 203.45.206.135 port 3070 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2436]: Failed password for invalid user jabber from 203.45.206.135 port 4664 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2591]: Failed password for invalid user email from 203.45.206.135 port 2262 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5744]: Failed password for invalid user jessica from 203.45.206.135 port 3711 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3799]: Failed password for invalid user jabber from 203.45.206.135 port 4328 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[1523]: Failed password for invalid user postgres from 203.45.206.135 port 3682 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3090]: Failed password for invalid user gitolite from 203.45.206.135 port 1813 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[3250]: Failed password for invalid user irc from 89.106.20.218 port 4299 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[5440]: Failed password for invalid user sales from 89.106.20.218 port 3953 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
>	05/08/25 04:07:07,000	Thu Aug 05 2025 04:07:07 mailsv1 sshd[2799]: Failed password for games from 89.106.20.218 port 2766 ssh2 host = Francesco source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

Individuazione degli Internal Server Error

Per trovare tutti gli eventi di tipo "Internal Server Error", è stata usata la seguente query:

- `index=tutorialdata "Internal Server Error" OR status=500`

Questa query ricerca gli eventi nell'indice tutorialdata che contengono la frase "Internal Server Error" o che hanno il codice di stato status=500. Questo metodo garantisce di trovare tutti i potenziali errori, sia quelli descritti nel messaggio sia quelli identificati dal codice standard.



Conclusioni

- Identificazione di attività anomale: le query hanno permesso di individuare e analizzare in dettaglio i tentativi di accesso falliti (**Failed password**), che rappresentano potenziali attacchi di tipo brute-force. È stato possibile identificare specifici indirizzi IP (**86.212.199.60**) e utenti che sono stati oggetto di questi tentativi.
- Analisi della sicurezza: Grazie alla capacità di filtrare gli eventi, è stato possibile creare una panoramica delle minacce alla sicurezza, evidenziando gli IP che hanno tentato di accedere al sistema più volte.
- Monitoraggio operativo: Oltre agli aspetti di sicurezza, le query hanno permesso di rilevare e monitorare eventi legati al funzionamento del sistema, come gli **Internal Server Error**, essenziali per la gestione e la manutenzione.