BUTTERCUP GAME

Analisi e Definizione dei Requisiti

Raccolta e Strutturazione dei Dati: Tutti i dati forniti sono stati raccolti e organizzati in base al loro utilizzo, successivamente divisi per indici.

Indici Creati:

- buttercup (Applicazione)
- wineventlog (Log Sistema)
- linux_stats (indice metrico, Log Hardware)

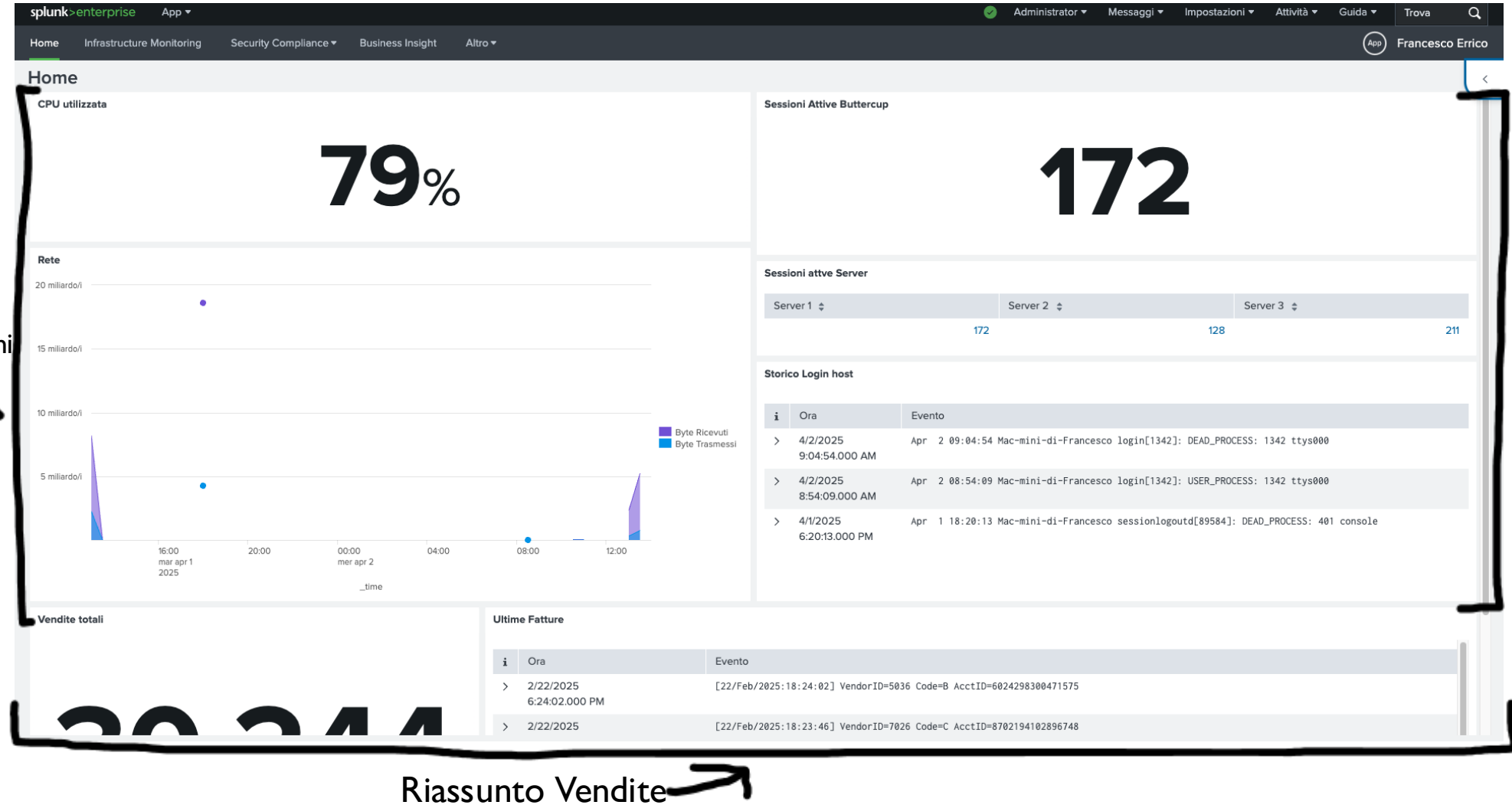
Caricamento dei Dati: Per il caricamento dei dati nel sistema, sono stati utilizzati script inclusi nell'addon TA_nix.

Creazione delle Dashboard:

- Dashboard principale per una visione globale.
- Infrastructure Monitoring per monitorare lo stato dell'infrastruttura.
- 3 Dashboard Security & Compliance, suddivise per app, server e host.
- Business Insight per le analisi aziendali.

Strumenti per la Ricerca: Durante lo sviluppo sono stati utilizzati diversi strumenti, tra cui Google, docs.splunk.com e ChatGPT per raccogliere informazioni e risolvere problemi.

Dashboard Principale



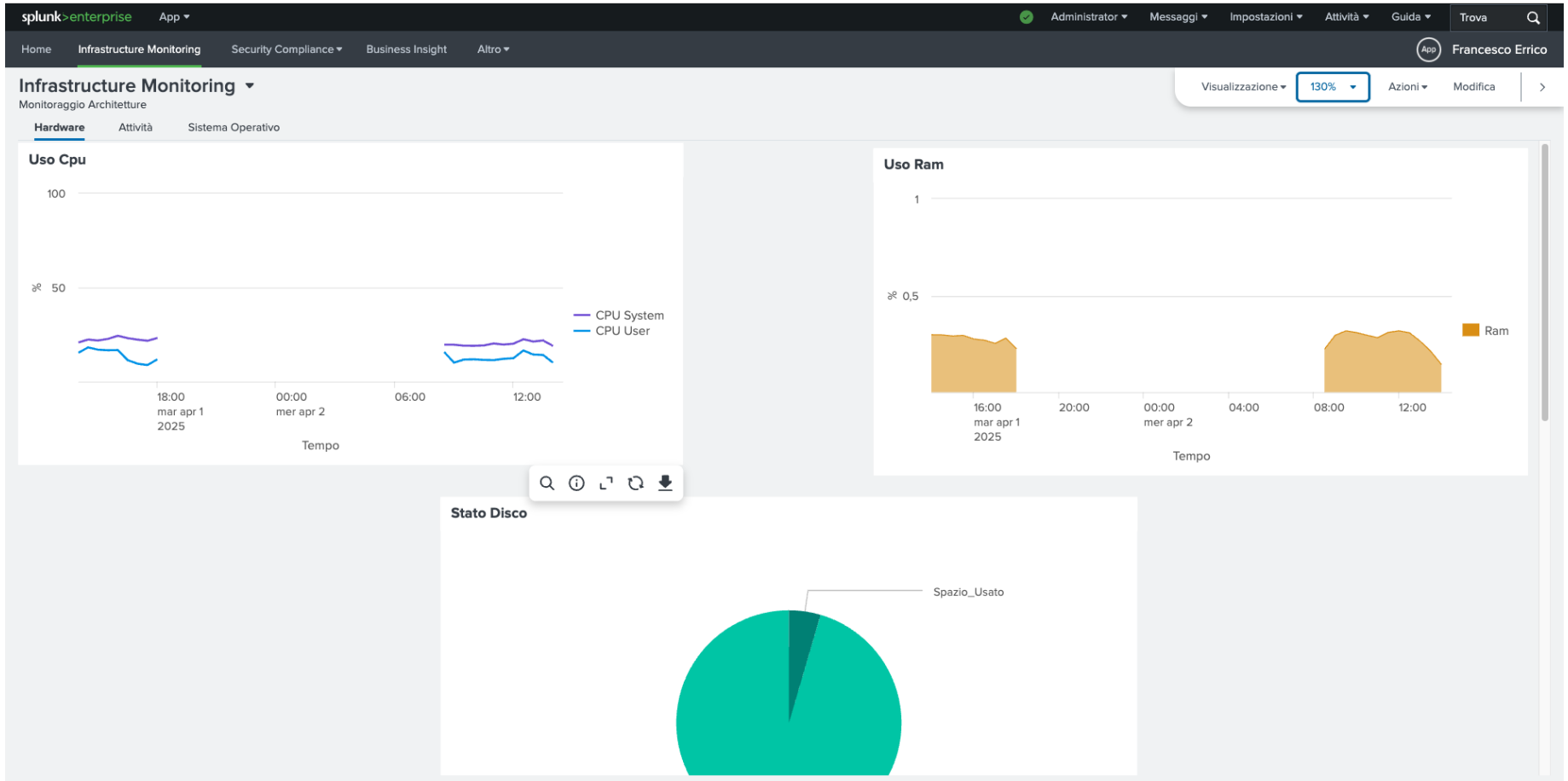
Prestazioni Hardware

Sicurezza

Riassunto Vendite

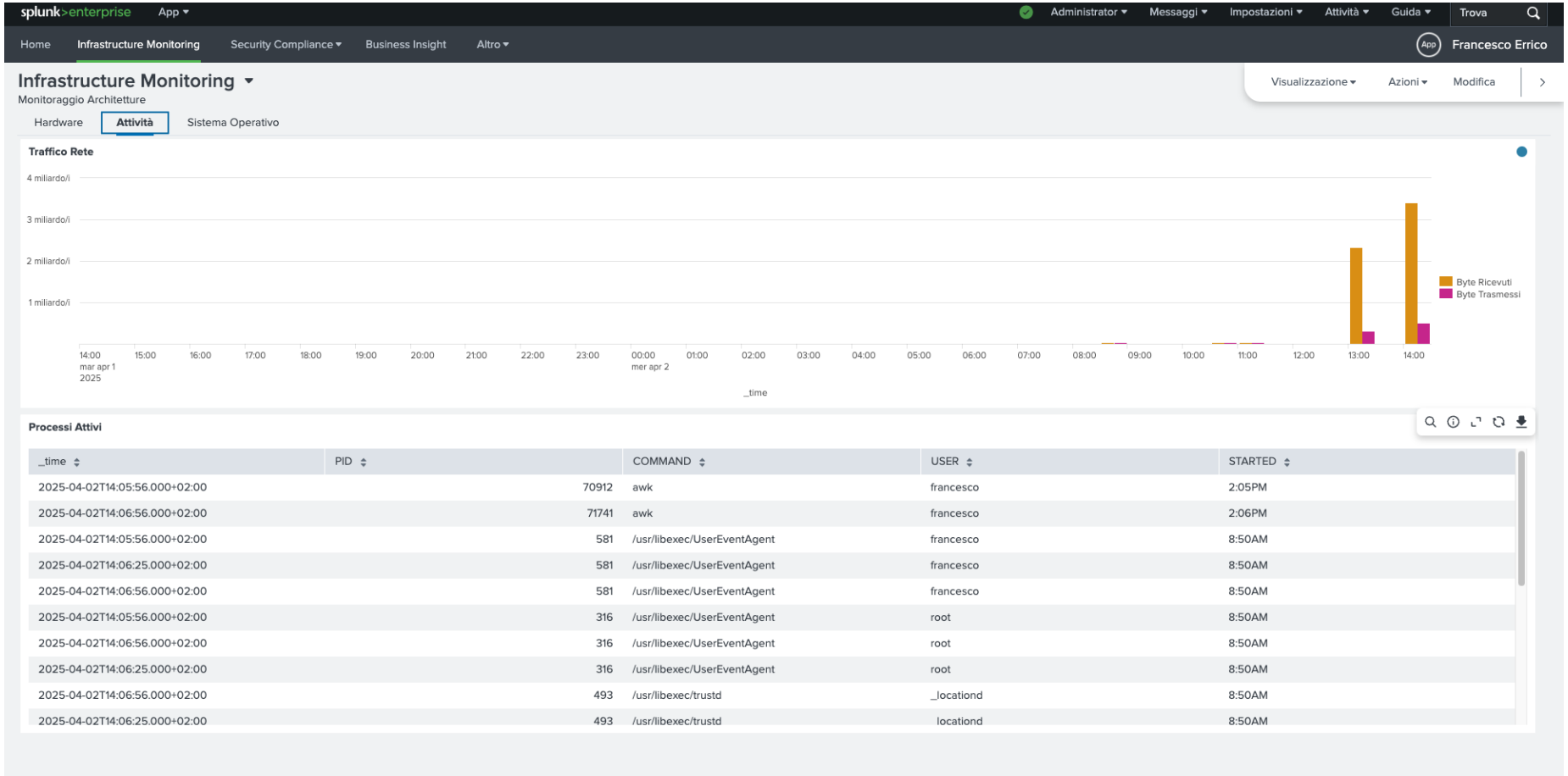
Infrastructure Monitoring

Attivita in tempo reale delle prestazioni Hardware



Infrastructure Monitoring

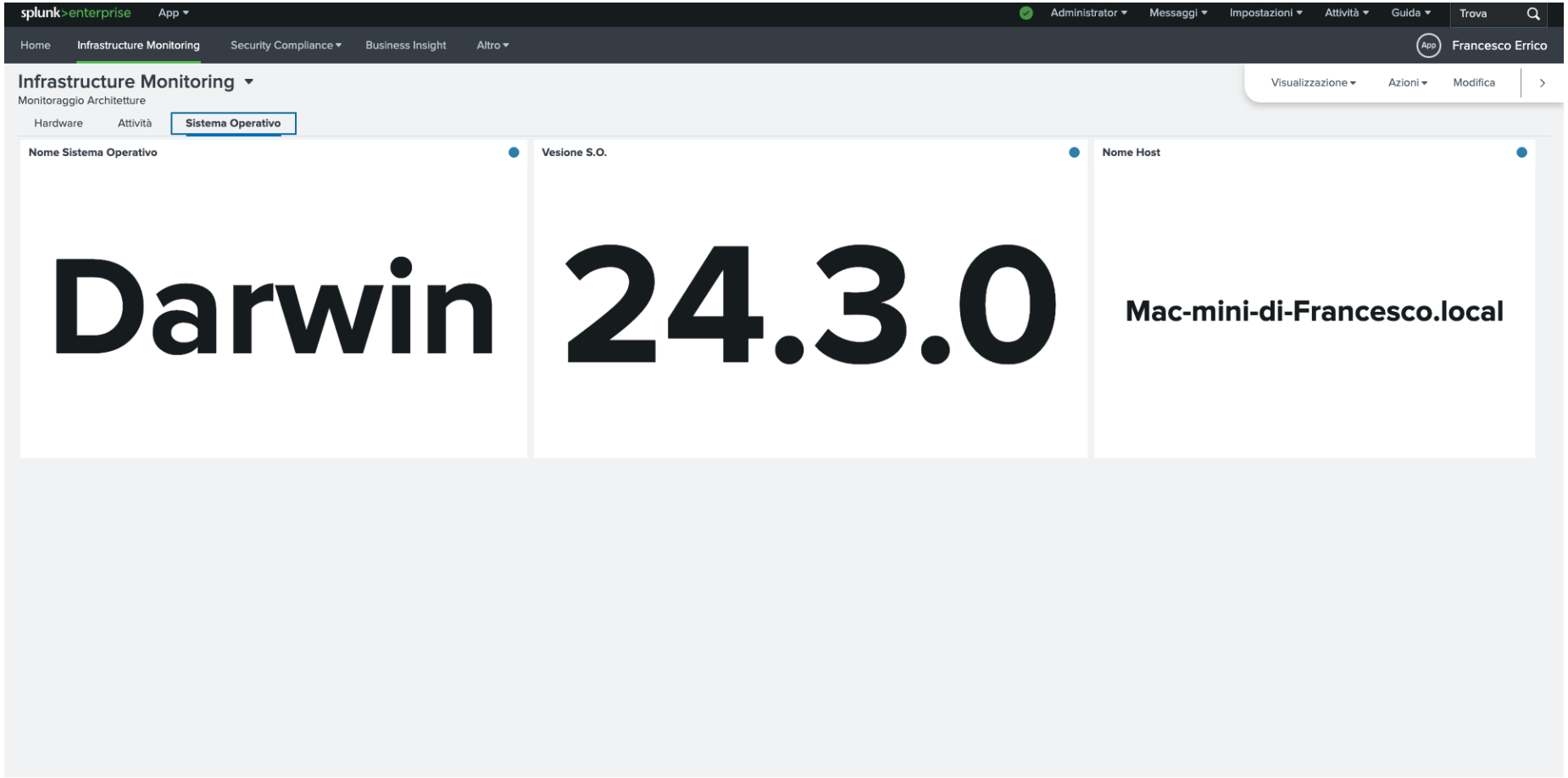
Attivita in tempo reale della rete e processi attivi



_time	PID	COMMAND	USER	STARTED
2025-04-02T14:05:56.000+02:00	70912	awk	francesco	2:05PM
2025-04-02T14:06:56.000+02:00	71741	awk	francesco	2:06PM
2025-04-02T14:05:56.000+02:00	581	/usr/libexec/UserEventAgent	francesco	8:50AM
2025-04-02T14:06:25.000+02:00	581	/usr/libexec/UserEventAgent	francesco	8:50AM
2025-04-02T14:06:56.000+02:00	581	/usr/libexec/UserEventAgent	francesco	8:50AM
2025-04-02T14:05:56.000+02:00	316	/usr/libexec/UserEventAgent	root	8:50AM
2025-04-02T14:06:56.000+02:00	316	/usr/libexec/UserEventAgent	root	8:50AM
2025-04-02T14:06:25.000+02:00	316	/usr/libexec/UserEventAgent	root	8:50AM
2025-04-02T14:06:56.000+02:00	493	/usr/libexec/trustd	_locationd	8:50AM
2025-04-02T14:06:25.000+02:00	493	/usr/libexec/trustd	locationd	8:50AM

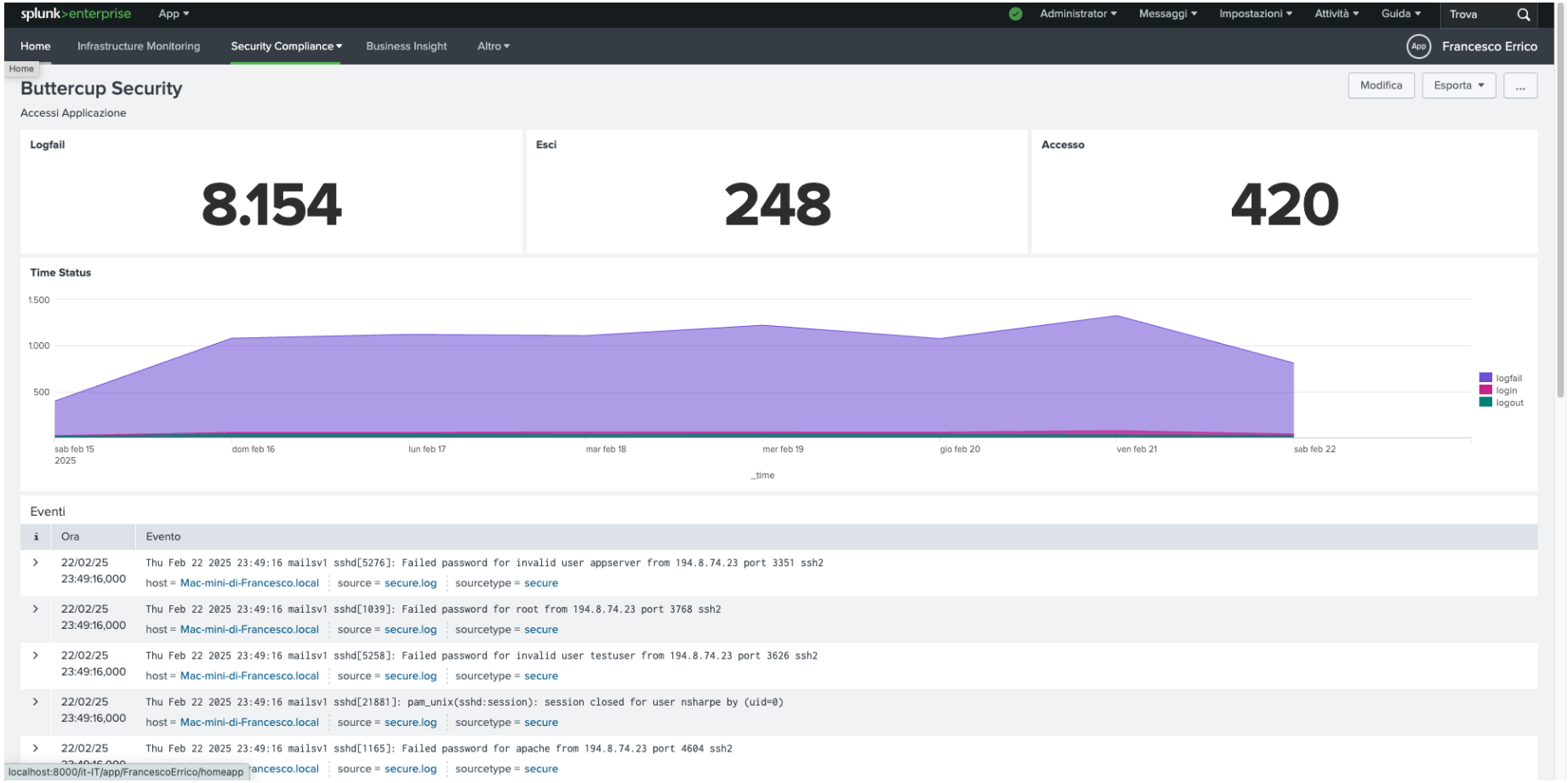
Infrastructure Monitoring

Informazioni Relative al Sistema Operativo



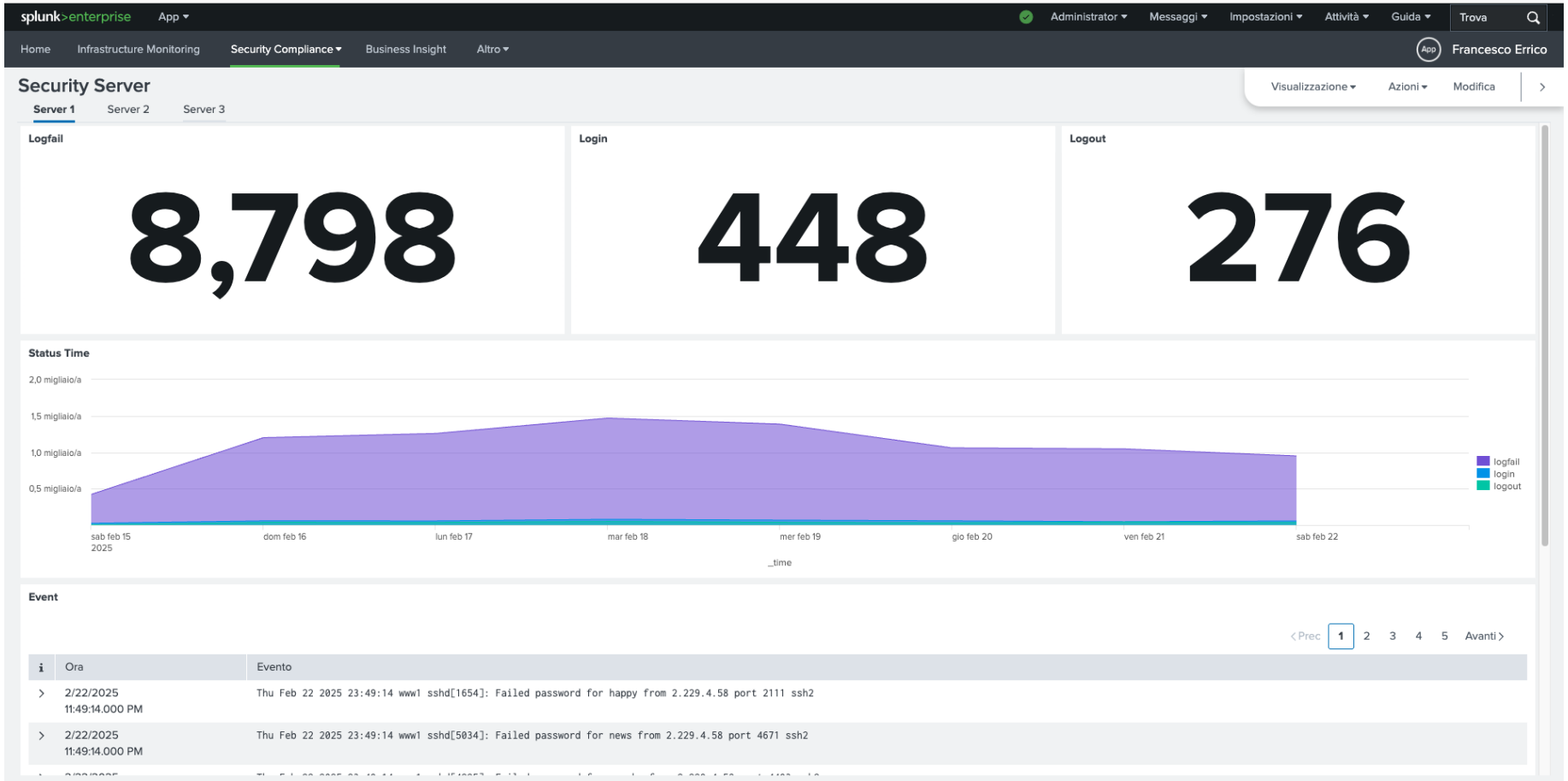
Security & Compliance

Informazioni Relative agli accessi all'app Buttercup



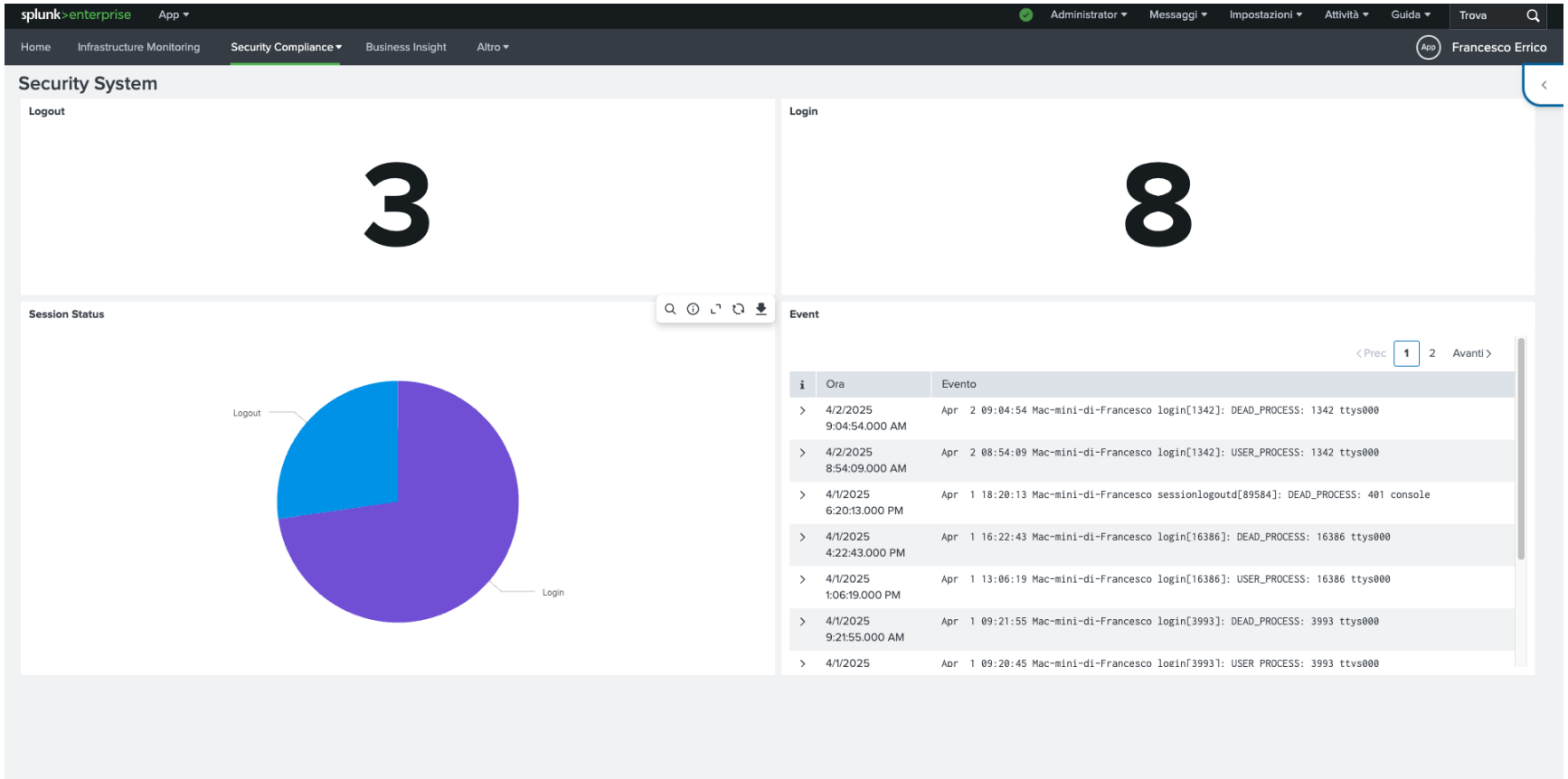
Security & Compliance

Informazioni Relative agli accessi relativi ai singoli server



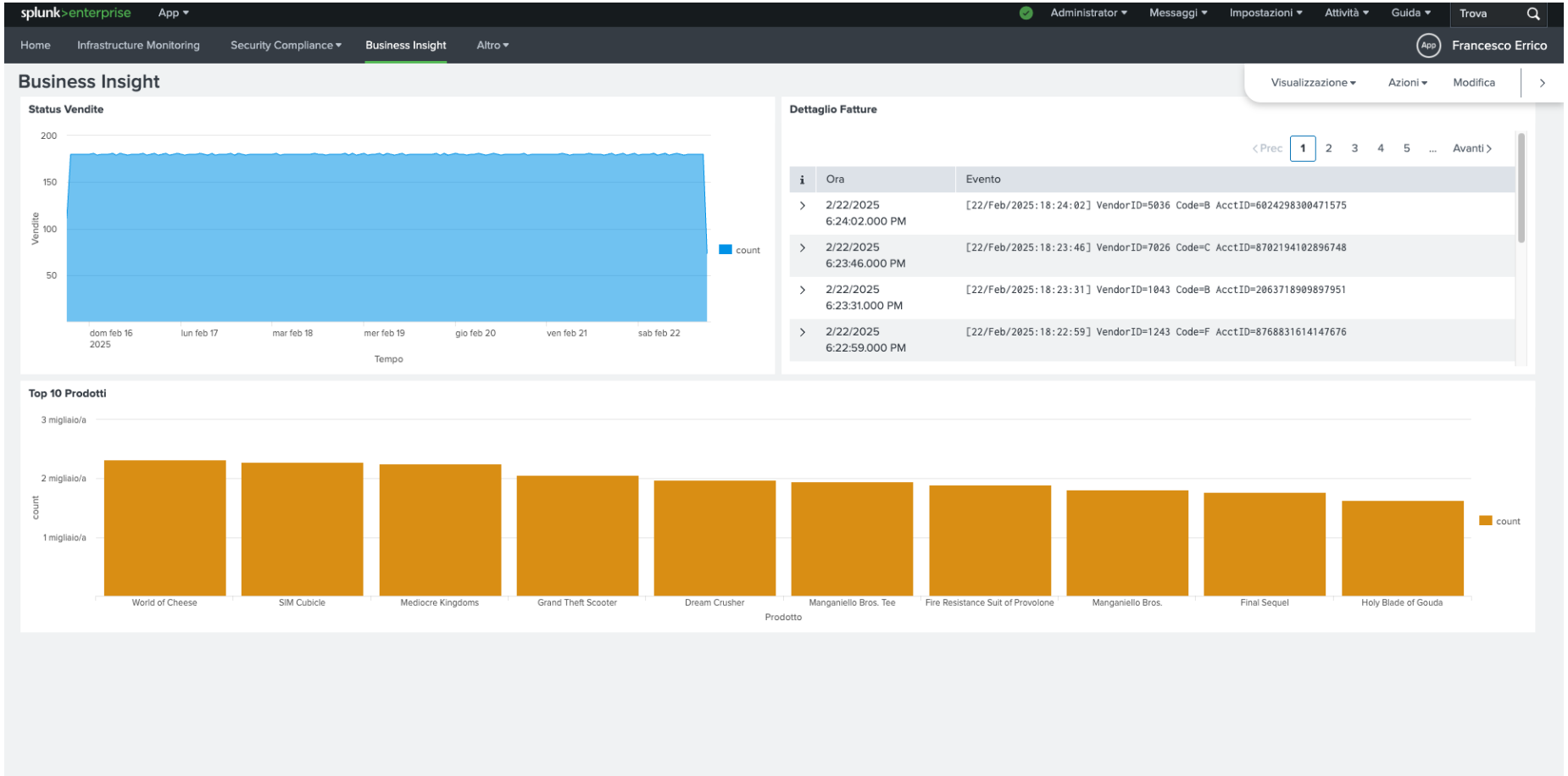
Security & Compliance

Informazioni Relative agli accessi all'host



Business Insight

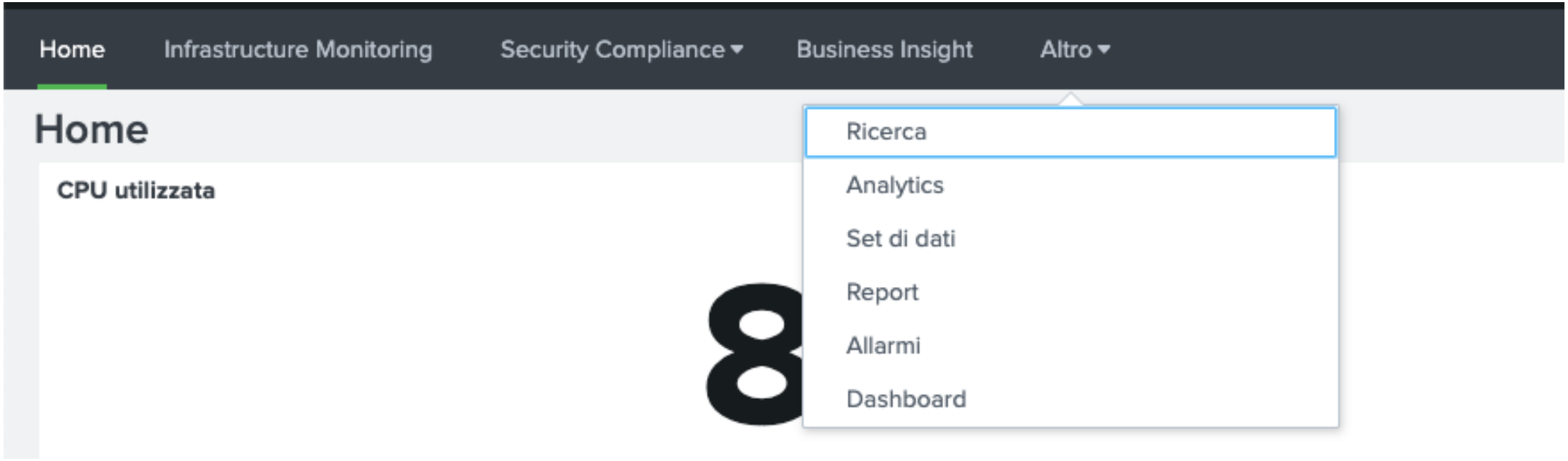
Informazioni Relative alle vendite



Menu

È stato diviso secondo i casi d'uso principali:

- Home
- Infrastructure Monitoring
- Secuity
- Business
- Altro (Menu classico di splunk)



Search

Sono state utilizzate ricerche relativamente semplici, con un maggiore utilizzo dei comandi stats per aggregazioni, timechart per la visualizzazione dei dati temporali, table per la creazione di tabelle e mpreview per le ricerche sull'indice metrico. Durante il processo, sono state effettuate numerose estrazioni dei campi necessari per le ricerche, al fine di ottenere i dati richiesti.

```
| mpreview index="linux_stats"
| search source=df MountedOn="/" Filesystem=disk3s1
| stats first("metric_name:df_metric.Used_KB") as Spazio_Usato, first("metric_name:df_metric.Size_KB") as Spazio_Totale
| eval Spazio_Disponibile = Spazio_Totale - Spazio_Usato
| table Spazio_Usato, Spazio_Disponibile
| transpose
| rename "row 1" as Valore, column as Categoria
```

Ricerca per creazione grafico a torta spazio sul disco, è stato usato mpreview per l'indice, frist per prendere il campo che ci interessava e transpose e rename per otternere correttamente il grafico

Ricerca per il grafico dei login, logout e logfail per l'applicazione Buttercup, è stato utilizzato append per creare un timechart singolo

```
index="buttercup" mailsv1 "Failed" source="secure.log"
| timechart span=1d count AS "logfail"
| append [
    search index="buttercup" source="secure.log" mailsv1 "pam_unix(sshd:session): session opened"
    | timechart span=1d count AS "login"
]| append [
    search index="buttercup" source="secure.log" mailsv1 "pam_unix(sshd:session): session closed"
    | timechart span=1d count AS "logout"
]
```

```
index="buttercup"
| lookup prices.csv productId OUTPUT product_name
| stats count by product_name
| sort -count
| head 10
```

Ricerca per top 10 prodotti/categorie per l'area business con l'uso della lookup

Fine

In conclusione, è stata sviluppata un'app per il monitoraggio dell'infrastruttura hardware, dei server e delle applicazioni, con un focus particolare sul monitoraggio delle vendite. Questo approccio consente una visione completa e approfondita delle performance, garantendo un'analisi tempestiva e accurata delle metriche critiche.