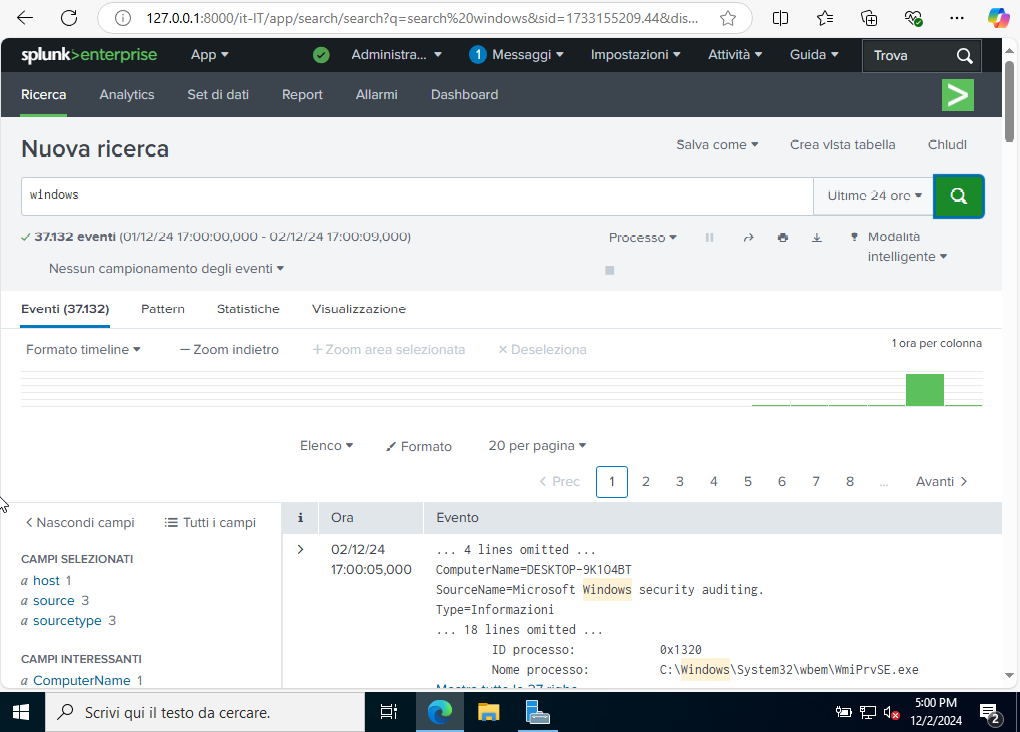
S10-L1 **Monitora Splunk**

Esercizio di oggi: Configurazione della Modalità Monitora in Splunk Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora". Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione. In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

**CONFIGURAZIONE**

Per configurare la modalità "Monitora" in Splunk, eseguiremo questi passaggi:

1. **Accedi a Splunk**
   * Apri il tuo browser e accedi all'interfaccia web di Splunk.
2. **Aggiunta di dati**
   * Vai su **Impostazioni > Aggiungi dati**.
   * Seleziona l'opzione **Monitora**.
3. **Scelta del file o directory da monitorare**
   * Indica il percorso del file o della directory da monitorare in tempo reale.
   * Ad esempio, puoi scegliere di monitorare un file di log specifico (ad esempio, /var/log/syslog).
4. **Configurazione delle impostazioni di input**
   * Configura i dettagli come:
     + Sorgente dei dati.
     + Tipo di host.
     + Nome dell'indice in cui inviare i dati (ad esempio, main).
5. **Revisione e salvataggio**
   * Verifica le impostazioni configurate.
   * Fai clic su **Salva** per completare.
6. **Conferma della configurazione**
   * Accedi al motore di ricerca di Splunk e verifica che i dati siano in arrivo con query come:
   * index=main sourcetype="tuo\_sourcetype"



**SPLUNK**

Splunk è una piattaforma software progettata per raccogliere, analizzare e visualizzare grandi quantità di dati generati da macchine (machine data) in tempo reale. È ampiamente utilizzata per il monitoraggio, la gestione di log, l'analisi della sicurezza e l'osservabilità in diversi settori, tra cui IT, DevOps e cyber security.

**Come funziona Splunk?**

1. **Raccolta dei dati**
   * Splunk raccoglie dati non strutturati o semi-strutturati da diverse fonti: file di log, metriche di rete, eventi di sistema, output di applicazioni, e altro.
   * Supporta input da server, dispositivi IoT, applicazioni cloud, container e molte altre fonti.
2. **Indicizzazione**
   * I dati raccolti vengono indicizzati e resi ricercabili. Splunk trasforma i dati grezzi in un formato comprensibile e utilizzabile per analisi successive.
3. **Analisi e visualizzazione**
   * Attraverso il suo potente motore di ricerca, puoi interrogare i dati con un linguaggio chiamato **Search Processing Language (SPL)**.
   * Splunk permette di creare dashboard, grafici, avvisi e report personalizzati per visualizzare e comprendere i dati in modo chiaro.

**Caratteristiche principali**

* **Monitoraggio in tempo reale:** Splunk rileva eventi, anomalie o problemi immediatamente.
* **Gestione centralizzata dei log:** Raccolta e organizzazione di log da più sistemi in un unico luogo.
* **Sicurezza e conformità:** Aiuta a identificare potenziali minacce e a rispettare le normative.
* **Machine Learning:** Offre strumenti integrati per analizzare dati complessi e prevedere comportamenti futuri.
* **Scalabilità:** Adatto a piccole implementazioni o a grandi infrastrutture distribuite.

**Dove si usa Splunk?**

* **Cybersecurity:** Monitoraggio delle minacce e risposta agli incidenti.
* **Gestione delle operazioni IT:** Identificazione e risoluzione di problemi nelle infrastrutture IT.
* **Analisi aziendale:** Tracciamento di metriche di business e miglioramento dell’efficienza operativa.
* **DevOps:** Monitoraggio delle applicazioni e analisi delle performance.