S10 L1 **Luca Calvigioni**

Configurazione della Modalità “Monitora” in Splunk

Cos’è Splunk Enterprise?

Splunk Enterprise (il server centrale che riceve i dati)

- È il sistema principale che riceve, indicizza e analizza i dati provenienti da varie fonti.
- Funziona come un server centrale dove vengono inviati i dati raccolti dagli agenti distribuiti (come i forwarder).
- Offre un’interfaccia grafica avanzata per:
    - Configurare ricezione e analisi dei dati.
    - Creare dashboard, report e alert.
    - Effettuare ricerche avanzate sui dati.

Cos’è Splunk Forwarder?

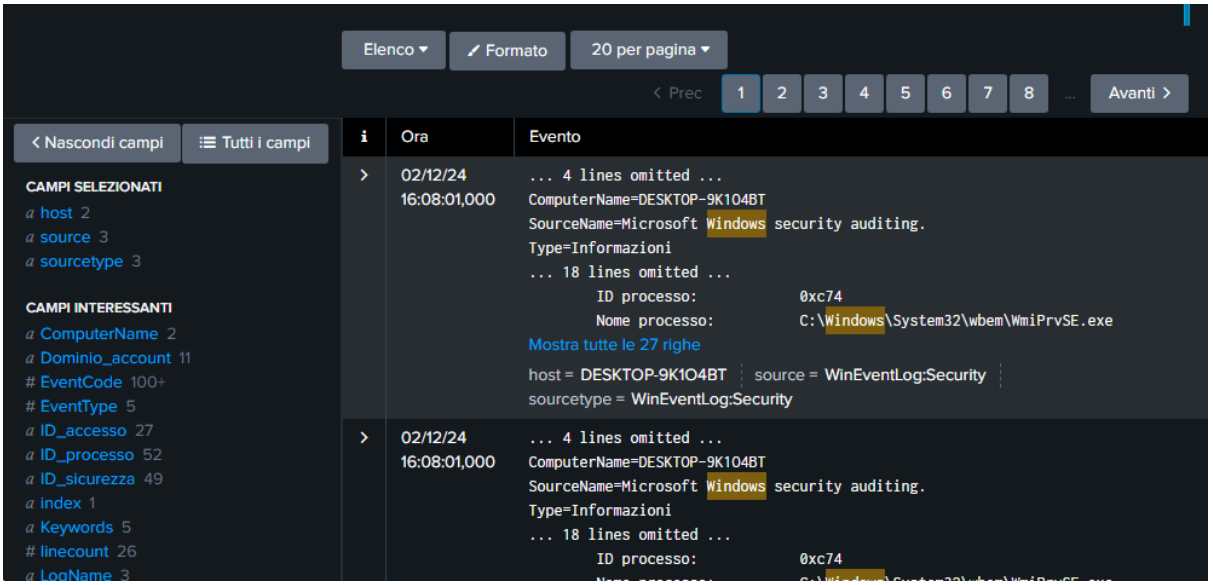
Splunk Universal Forwarder (l'agente che invia dati)

- È un client leggero progettato per raccogliere e **inviare i dati** al server Splunk Enterprise.
- Viene installato sui sistemi che contengono i dati da monitorare (ad esempio, workstation, server o applicazioni specifiche).
- È ottimizzato per inviare dati in tempo reale con basso impatto sulle risorse della macchina dove è installato.
- Non dispone di interfaccia grafica; la configurazione avviene tramite comandi o file di configurazione.

L’esercizio odierno ha riguardato la configurazione della modalità **Monitora** in Splunk, utilizzando Splunk Universal Forwarder su un sistema Windows 10 Pro per inviare dati a un’istanza di Splunk Enterprise su Windows Server 2022. La modalità **Monitora** consente di osservare e analizzare in tempo reale file o directory specifici.

Come passaggi principali abbiamo ovviamente installato Splunk Enterprise su windows server 2022 che farà da server centrale per analizzare i dati ricevuti, configurando una porta in ascolto nel nostro caso la porta 9997 e su windows 10 pro abbiamo installato Splunk Forwarder che raccoglie e invia i dati al server Splunk Enterprise attraverso la porta in ascolto.

Avviamo la fase Monitora dal menu di Enterprise, selezioniamo log di eventi locali, scegliamo le impostazioni che desideriamo. In questo caso, selezioniamo "Security", scriviamo nel campo dove ci viene richiesto il nome dell'host di cui vogliamo analizzare i file, il nome della macchina che interessa a noi, DESKTOP-9K1O4BT (win10 pro)



Splunk acquisisce i dati direttamente dal dispositivo in cui lo abbiamo installato.

L'immagine mostra che Splunk sta raccogliendo e analizzando eventi di sicurezza provenienti da un dispositivo Windows. Questi dati potrebbero essere utili per rilevare accessi non autorizzati, modifiche al sistema o altre attività sospette. I campi selezionati e interessanti offrono un'ampia gamma di informazioni utili per l'analisi della sicurezza, come l'ora e la data dell'evento, il nome del computer, e dettagli dell'account.

Conclusione

In conclusione possiamo dire che Splunk può essere utilizzato per analizzare grandi quantità di dati di log di sicurezza di Windows. Utilizzando i campi selezionati e interessanti, possiamo eseguire query avanzate per ottenere insight significativi sui nostri dati di sicurezza.