

Oggi Vediamo una veloce infarinatura di Splunk:

Splunk è una piattaforma per la raccolta, l'analisi e la visualizzazione dei dati generati da macchine, come i log di sistema, i dati di rete, e altre fonti strutturate o non strutturate. Splunk aiuta a monitorare, analizzare e rispondere a eventi in tempo reale, rendendolo popolare in ambiti come la sicurezza informatica, l'analisi delle prestazioni, e la gestione dei dati aziendali.

Funzionamento di Splunk

1. Raccolta dati:

- Splunk raccoglie dati da varie fonti, come log di applicazioni, server, dispositivi di rete, sensori IoT e altri.
- Può connettersi a sorgenti dati usando agenti Forwarder (installati sui dispositivi da monitorare) o attraverso API e connessioni dirette.

2. Indicizzazione:

- I dati raccolti vengono indicizzati, ossia organizzati in un formato che permette ricerche rapide.
- Splunk assegna timestamp e metadata ai dati per agevolare l'analisi.

3. Ricerca e analisi:

- Gli utenti utilizzano un linguaggio di query chiamato **SPL (Search Processing Language)** per cercare e analizzare i dati.
- È possibile eseguire ricerche ad hoc, creare filtri e applicare trasformazioni ai dati.

4. Dashboard e visualizzazione:

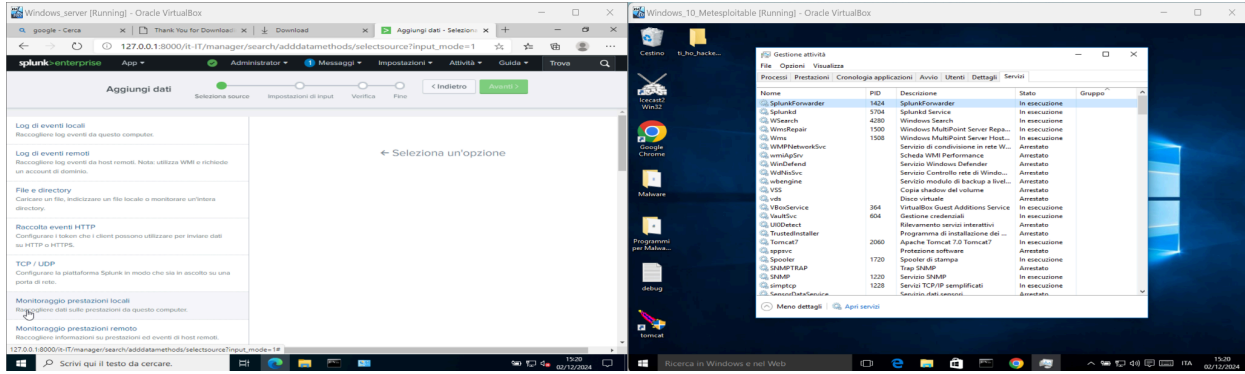
- Splunk consente di creare dashboard personalizzabili per visualizzare i dati in tempo reale tramite grafici, tabelle e mappe.
- Questo aiuta a identificare rapidamente tendenze, anomalie e potenziali problemi.

5. Alert e automazione:

- Splunk può generare avvisi basati su condizioni specifiche nei dati (ad esempio, un numero elevato di tentativi di accesso non riusciti).
- È possibile configurare risposte automatizzate, come notifiche o esecuzione di script.

6. Integrazione con altri strumenti:

- Splunk si integra con molti altri sistemi, come strumenti SIEM (Security Information and Event Management), piattaforme cloud, e strumenti DevOps.
- Può essere esteso con app e add-on disponibili nello Splunkbase.



Analizzando il File:

Nuova ricerca

Salva comeCrea vista tabellaChiudi

Death Attacks

Sempre

✓ 1 evento (prima di 02/12/24 16:02:46,000) Nessun campionamento degli eventiProcessoModalità intelligente

Eventi (1)PatternStatisticheVisualizzazione

Formato timelineZoom indietroZoom area selezionataDeseleziona1 millisecondo per colonna

ElencoFormato20 per pagina

< Nascondi campi

CAMPI SELEZIONATI

Tutti i campi

a host 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

a additional_info 1

a attacker_ip 1

01/06/24

22:30:00,000

2024-06-01 22:30:00, Ping of Death Attack, 192.168.1.22, 10.0.0.1, Ping of Death attack detected on Epicode.com by Elliot, Large ICMP packet causing disruption

host = DESKTOP-9K1O4BT

source = Z:\Shadow (1)\Shadow.csv

sourcetype = csv