AMATO SARA

S10 L1

**Configurazione della Modalità Monitora in Splunk**

**Introduzione**

Splunk è una piattaforma avanzata per la gestione e l'analisi dei dati di log generati da infrastrutture IT, applicazioni e dispositivi. Una delle sue funzionalità principali è la modalità "Monitora", che consente di raccogliere dati in tempo reale da fonti specifiche come file di log, cartelle e registri di sistema. Questa funzione è particolarmente utile per il monitoraggio continuo della sicurezza, consentendo di rilevare e analizzare rapidamente attività sospette.

L'obiettivo di questo esercizio è configurare la modalità Monitora per raccogliere dati dai registri di sicurezza di un sistema Windows, analizzare uno degli eventi raccolti e comprendere come queste informazioni possano essere utilizzate per migliorare la sicurezza dell'infrastruttura IT.

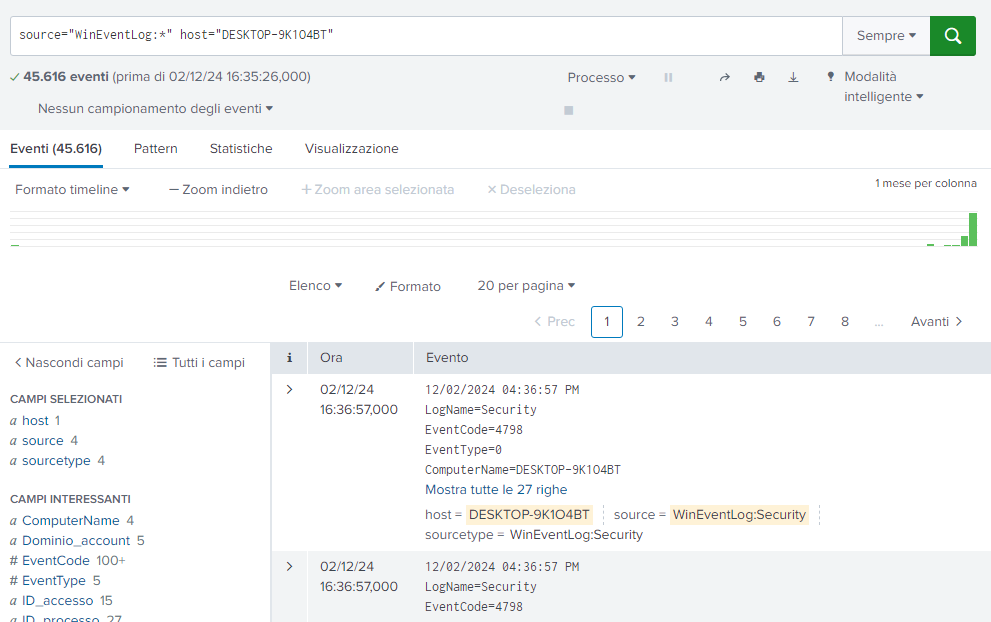
Accesso a Splunk:

Effettuare il login al pannello di amministrazione di Splunk utilizzando le credenziali appropriate.

Accedere alla sezione dedicata all'aggiunta di nuove fonti di dati.

Impostazione della Modalità Monitora:

Selezionare Impostazioni > Aggiungi dati > Monitora dal menu principale di Splunk.

Specificare come sorgente i Windows Event Logs, selezionando la categoria Security. Questo consente di raccogliere eventi che riguardano la sicurezza del sistema, come accessi, modifiche di account o tentativi di accesso non autorizzato.Configurare Splunk per monitorare questi log in tempo reale, assicurandosi che il polling sia impostato su un intervallo adeguato per garantire un flusso continuo di dati.

L'evento catturato dallo screenshot rappresenta un log di sicurezza generato da Windows e raccolto da Splunk. Analizzando i dettagli riportati, possiamo trarre informazioni utili.

Host e sorgente:

Host: DESKTOP-9K1O4BT – Questo è il nome del dispositivo che ha generato il log. Rappresenta l'origine dei dati e consente di identificare il computer specifico nella rete.

Sorgente: WinEventLog:Security – Indica che il registro analizzato appartiene alla categoria di sicurezza, che include eventi come accessi, modifiche di account e operazioni amministrative.

Informazioni sull'evento:

EventCode: 4798 – Questo codice evento segnala che è stata effettuata una query sugli account locali. È una tipica attività amministrativa o di monitoraggio, ma può anche essere un indicatore di un tentativo di enumerazione da parte di un utente o attaccante.

EventType: 0 – Specifica che si tratta di un evento generico registrato nel log.

ID\_processo: 0x1040 – Rappresenta il processo specifico che ha generato l'evento. Può essere utile per identificare l'applicazione o il servizio responsabile.

ID\_sicurezza: S-1-5-18 – Questo SID (Security Identifier) appartiene all'account SYSTEM, un'entità interna di Windows con privilegi elevati. È normale vedere questa identità associata a operazioni di sistema.

Parole chiave:

"Controllo riuscito" – Indica che l'azione eseguita è stata completata con successo. Questo può essere utile per distinguere eventi benigni da quelli che richiedono attenzione (es. accesso negato).

Osservazioni

L'evento sembra indicare un'attività legittima, ma se accompagnato da un numero elevato di richieste simili in breve tempo, potrebbe suggerire un tentativo di enumerazione degli account locali da parte di un attaccante.

La presenza di numerosi EventCode 4798 può essere un segnale di scansioni sospette o operazioni amministrative non autorizzate.

Ipotesi sui vettori di attacco

Dall'analisi dell'evento e dei dati raccolti, possiamo ipotizzare diversi scenari:

Enumerazione degli account locali:

Un utente o un attaccante potrebbe tentare di raccogliere informazioni sugli account esistenti per identificare potenziali obiettivi o vulnerabilità.

Accesso non autorizzato:

Se l'evento è accompagnato da tentativi di accesso falliti (EventCode 4625), potrebbe indicare un attacco di forza bruta.

Monitoraggio legittimo:

L'evento potrebbe anche essere generato da uno script di monitoraggio legittimo utilizzato dall'amministratore per controllare gli account locali.

Azioni consigliate e prevenzione

Analisi dei dati storici:

Verificare se ci sono stati eventi simili in passato e controllare la frequenza con cui compaiono.

Abilitazione di alert personalizzati:

Configurare Splunk per inviare notifiche in tempo reale in caso di eventi ripetitivi o sospetti (es. più EventCode 4798 in un breve periodo).

Protezione degli account:

Applicare politiche di accesso rigorose, come il blocco degli account dopo un certo numero di tentativi falliti.

Auditing regolare:

Monitorare regolarmente i log di sicurezza per identificare attività anomale e prevenire escalation.

Conclusioni

L'esercizio ha dimostrato l'efficacia della modalità Monitora di Splunk per il monitoraggio continuo dei log di sicurezza. Grazie all'analisi dettagliata degli eventi raccolti, è possibile identificare potenziali minacce e adottare misure preventive mirate. Questo approccio proattivo è essenziale per garantire la sicurezza delle infrastrutture IT e mitigare i rischi associati ad attività malevole.