Configurare gli eventi di protezione SLF e SQLF in Secure Analytics

Sommario

Introduzione

In questo documento vengono descritti due parametri che è possibile utilizzare per ottimizzare gli eventi di sicurezza SLF (Susspect Long Flow) e SQLF (Susspect Quad Long Flow).

Premesse

Un evento Suspect Long Flow è un tipo specifico di evento di sicurezza generato da Secure Analytics e progettato per rilevare conversazioni tra host più lunghe del normale. Esistono due tipi diversi di evento Suspect Long Flow: Flusso lungo sospetto e flusso lungo sospetto non interattivo.

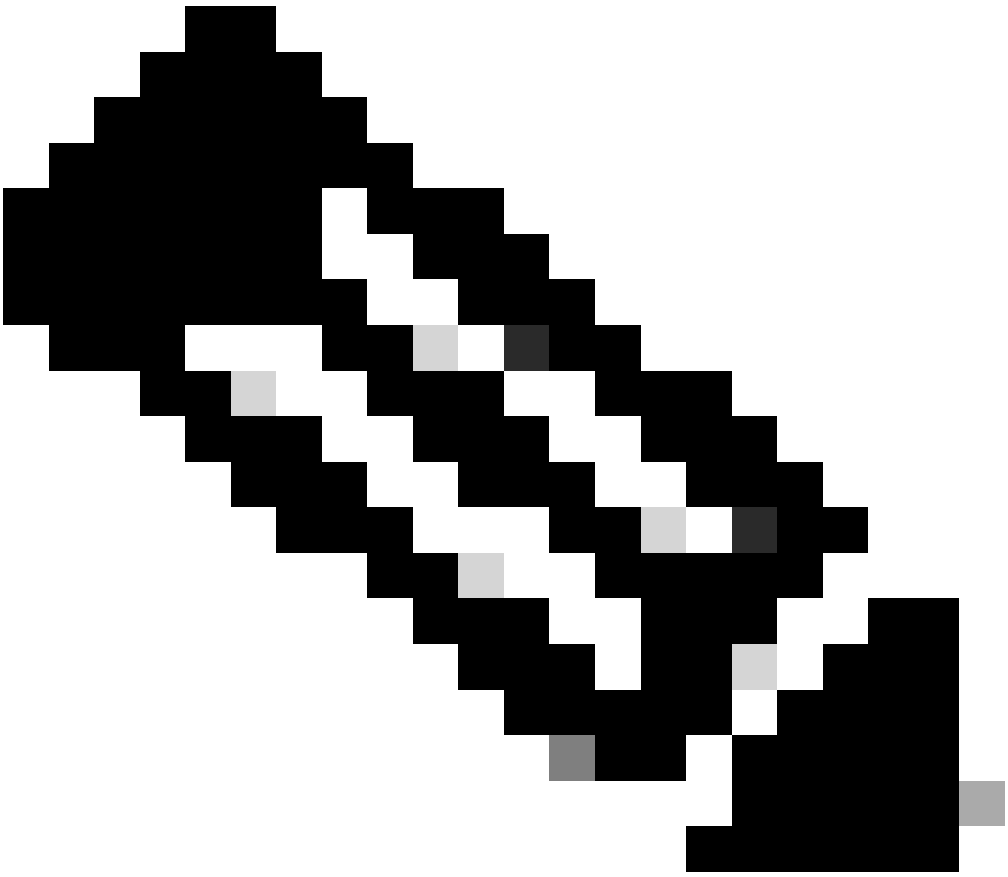
Si consideri di collegare il notebook al PC di casa tramite una VPN nascosta per 3 giorni, ma in genere né il PC di casa né il notebook offrono connessioni di lunga durata. Flow Collector rileva questa anomalia e attiva un evento di sicurezza a seconda della quantità di traffico trasmesso e della durata del flusso. Questi eventi hanno lo scopo di identificare i flussi di lunga durata e i flussi di lunga durata che passano il traffico minimo.

Ottimizzazione/Configurazione

Esistono principalmente 2 parametri di configurazione del raccoglitore di flussi che sono responsabili del controllo del comportamento di questi due eventi.

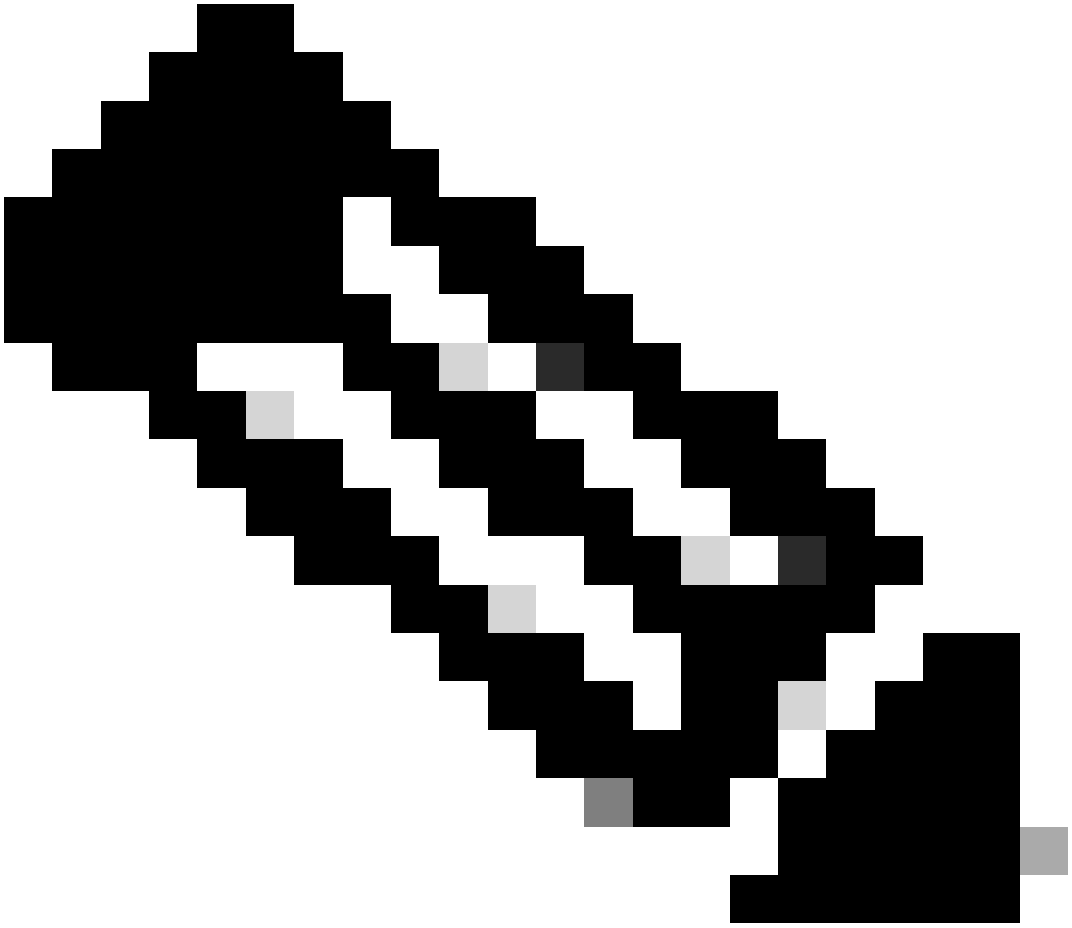
Per regolare queste impostazioni, accedere alla pagina Configurazione > Flow Collector > Avanzate nella WebUI dell'accessorio di gestione.

- I secondi necessari per qualificare un flusso come impostazione di durata lunga controllano il comportamento dell'evento di flusso lungo sospetto.



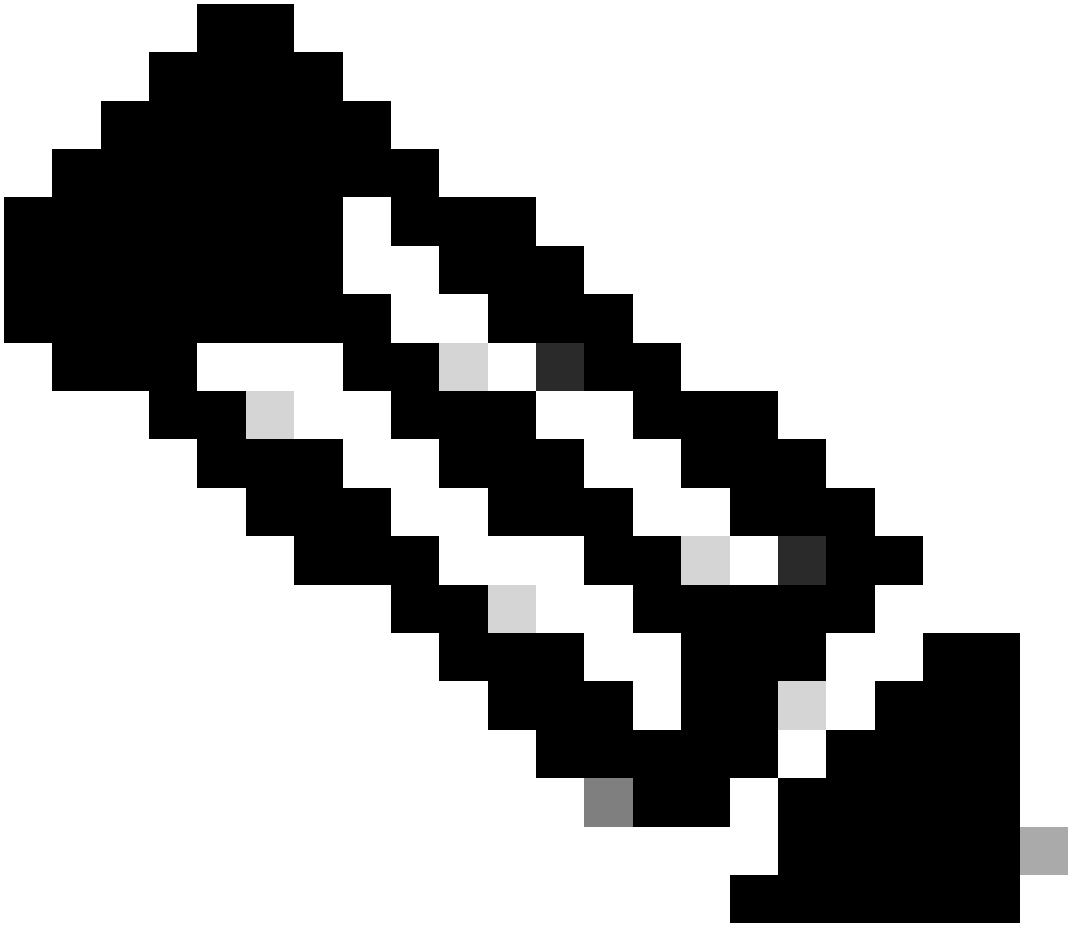
Nota: Questa opzione di configurazione in webUI imposta il parametro long_flow_duration nel file di configurazione lc_threshold.txt dei raccoglitori di flusso.

- I secondi necessari per qualificare un flusso come impostazione di flusso lungo silenzioso sospetto controllano il comportamento dell'evento Flusso lungo silenzioso sospetto.



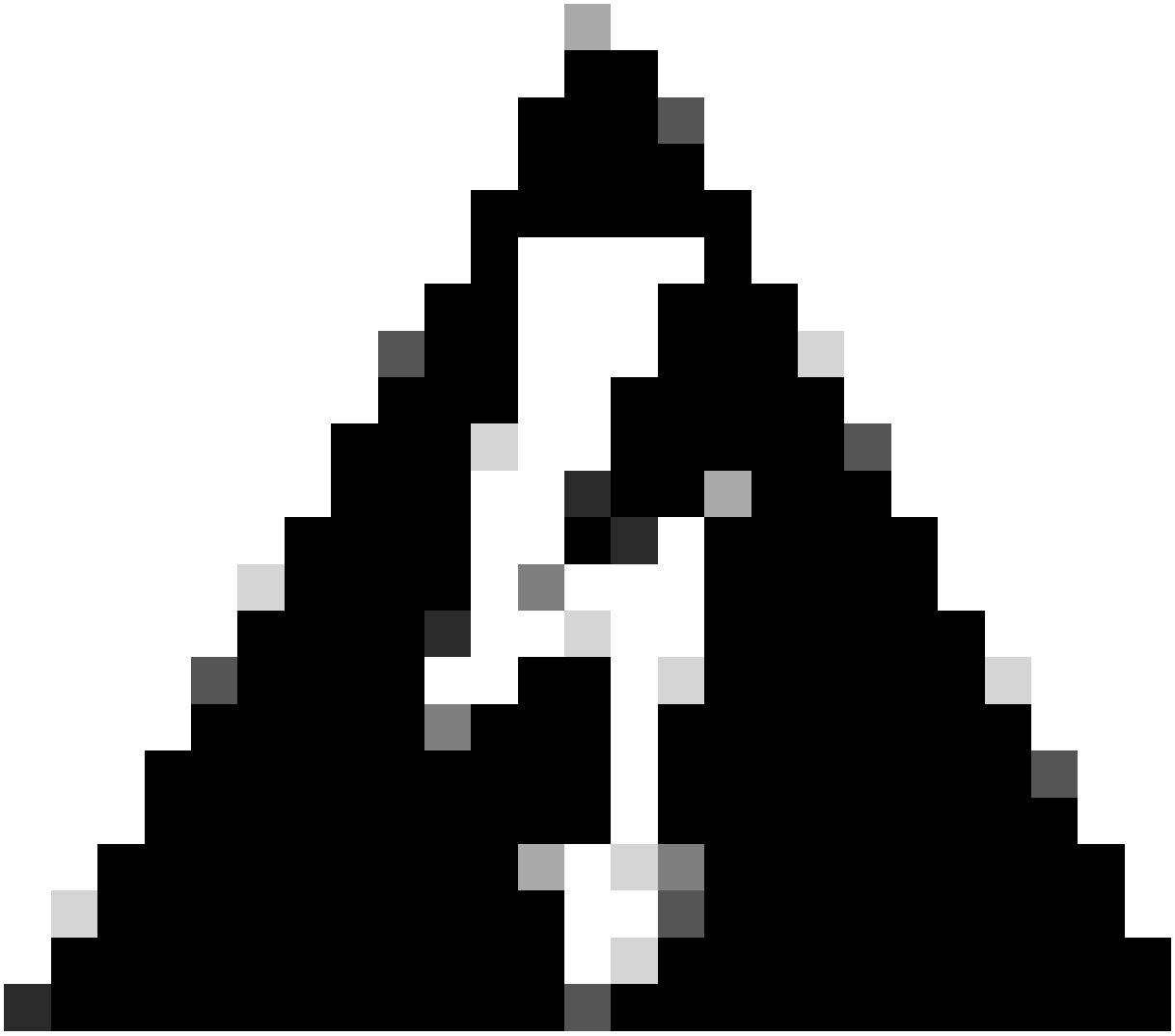
Nota: Questa opzione di configurazione in webUI imposta il parametro quiet_long_flow_duration nel file di configurazione lc_threshold.txt dei raccoglitori di flusso.

Il valore predefinito per entrambi i contatori è 32400 secondi (9 ore).



Nota: Per quanto riguarda la modifica di questi contatori, il relativo CDET:

ID bug Cisco CSCwm05128



Avviso: Ciò influisce solo su v7.5.1 o versioni precedenti.

Questo difetto impone che un flusso lungo e tranquillo sospetto deve prima essere anche un flusso lungo sospetto. Ciò significa che se si modificano i secondi richiesti per qualificare un flusso come flusso lungo e silenzioso sospetto in una durata inferiore ai secondi richiesti per qualificare un flusso come impostazione di durata lunga, è probabile che si verifichino risultati imprevisti.

Se si modifica una o entrambe le impostazioni avanzate, il rilevamento dei flussi lunghi potrebbe non riuscire.

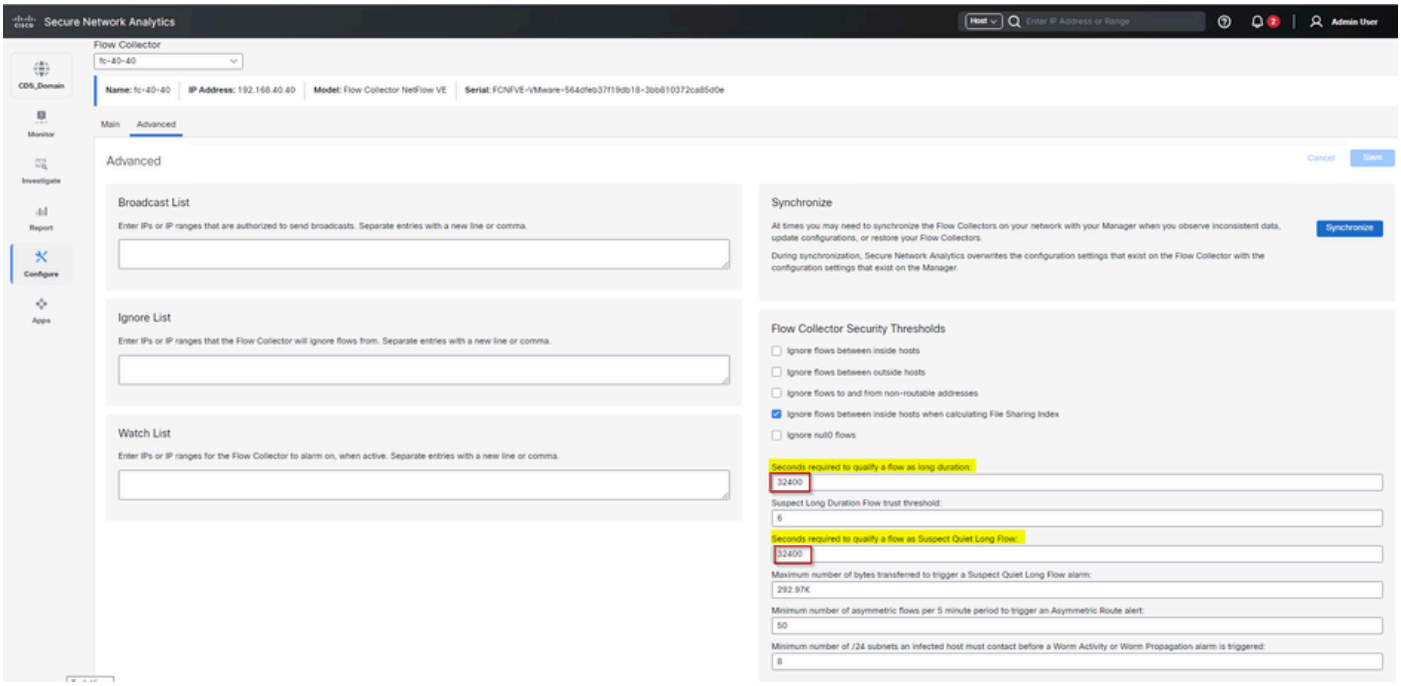
Poiché un flusso lungo silenzioso per definizione deve anche essere un flusso lungo, la logica nella corretta gestione di queste due impostazioni è che il flusso superi il requisito del flusso lungo prima di provare che sia un flusso lungo silenzioso.

Ad esempio, se long_flow_duration viene lasciato sul valore predefinito di 9 ore e quiet_long_flow_duration viene impostato su un valore inferiore, ad esempio 8 ore, il motore non genera un evento di flusso di durata piuttosto lunga finché il flusso non dura almeno 9 ore.

In alternativa, se long_flow_duration viene lasciato al valore predefinito di 9 ore e quiet_long_flow_duration è impostato su 10 ore, questa configurazione disabilita in modo efficace l'evento di flusso quieto di lunga durata (a meno che il flusso non sia una singola esportazione con una durata > quiet_long_flow_duration di 10 ore).

Soluzione

Entrambe queste impostazioni avanzate devono essere impostate sullo stesso valore desiderato oppure quiet_long_flow_duration deve essere sempre >= long_flow_duration.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).