Konfigurieren von SLF- und SQLF-Sicherheitsereignissen in Secure Analytics

Inhalt

Einleitung

Hintergrundinformationen

Abstimmung/Konfiguration

Lösung

Einleitung

In diesem Dokument werden zwei Parameter beschrieben, die zum Anpassen der Sicherheitsereignisse "Suspect Long Flow" (SLF) und "Suspect Quiet Long Flow" (SQLF) verwendet werden können.

Hintergrundinformationen

Ein Suspect Long Flow-Ereignis ist ein bestimmter Typ von Sicherheitsereignissen, die von Secure Analytics generiert werden und dazu dienen, mehr als normale Gespräche zwischen Hosts zu erkennen. Es gibt zwei verschiedene Typen des Suspect Long Flow-Ereignisses: Suspect Long Flow und Suspect Quiet Long Flow.

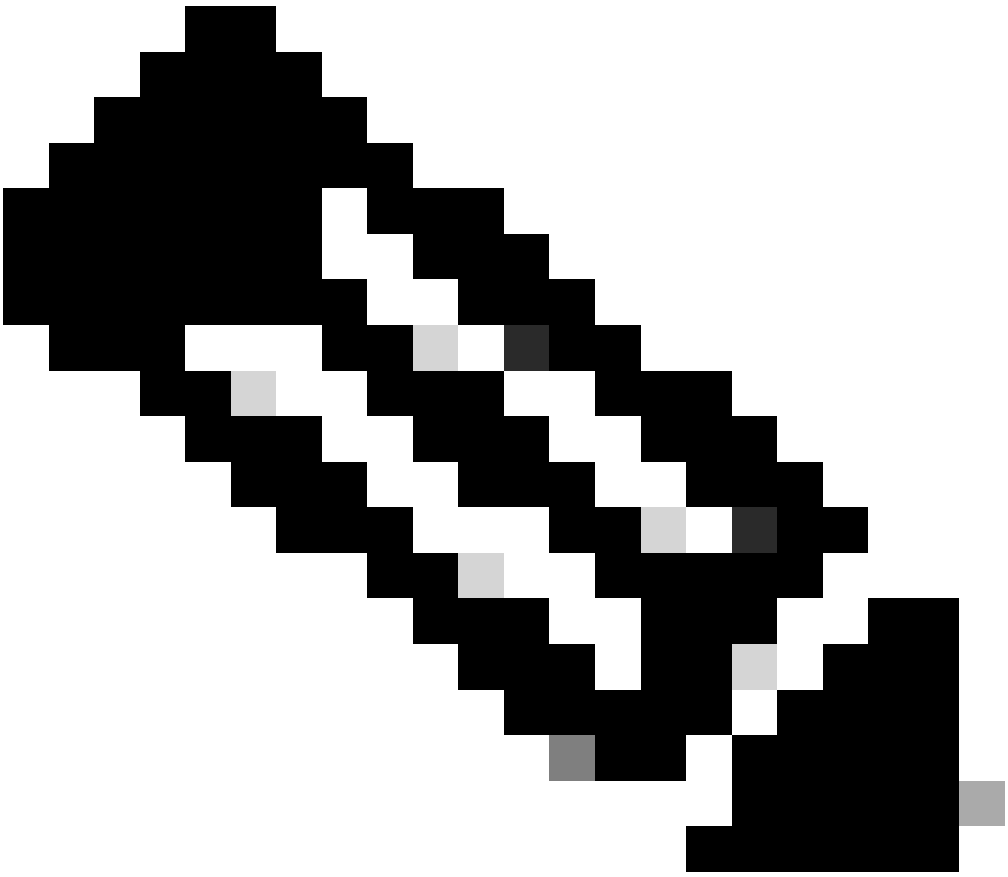
Denken Sie daran, dass Sie Ihren Laptop für 3 Tage über ein verdecktes VPN mit Ihrem Heim-PC verbinden, aber normalerweise führen weder der Heim-PC noch der Laptop lange Flow-Verbindungen aus. Flow Collector erkennt diese Anomalie und löst ein Sicherheitsereignis aus, das von der Menge des weitergeleiteten Datenverkehrs und der Dauer des Datenflusses abhängt. Diese Ereignisse sollen lange laufende Flows und lange laufende Flows identifizieren, die minimalen Datenverkehr passieren.

Abstimmung/Konfiguration

Es gibt in erster Linie zwei Konfigurationsparameter für den Flow Collector, die für die Steuerung des Verhaltens dieser beiden Ereignisse verantwortlich sind.

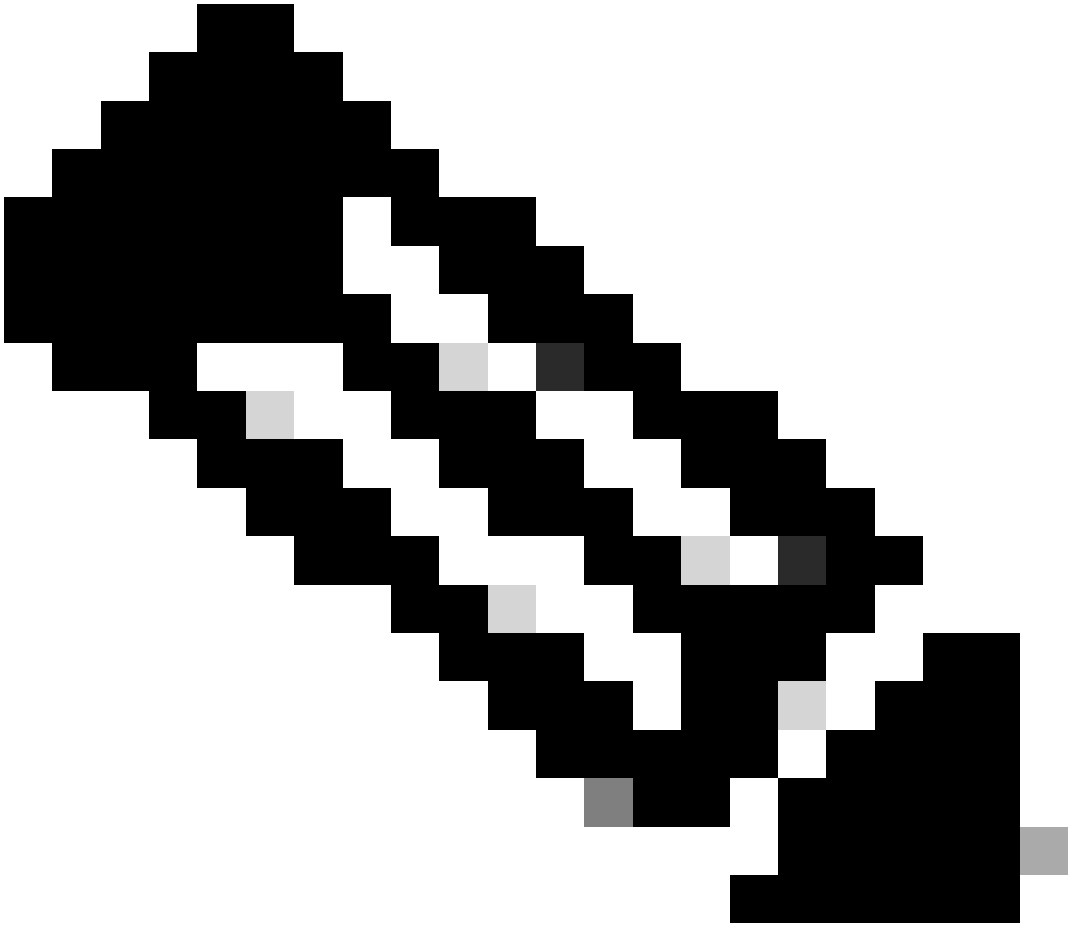
Diese Einstellungen können über die Seite Konfigurieren > Flow Collectors > Erweitert in der WebUI der Manager-Appliance angepasst werden.

- Die Sekunden, die erforderlich sind, um einen Fluss als Langzeitereignis zu qualifizieren, steuern das Verhalten des verdächtigen Langzeitereignisses.



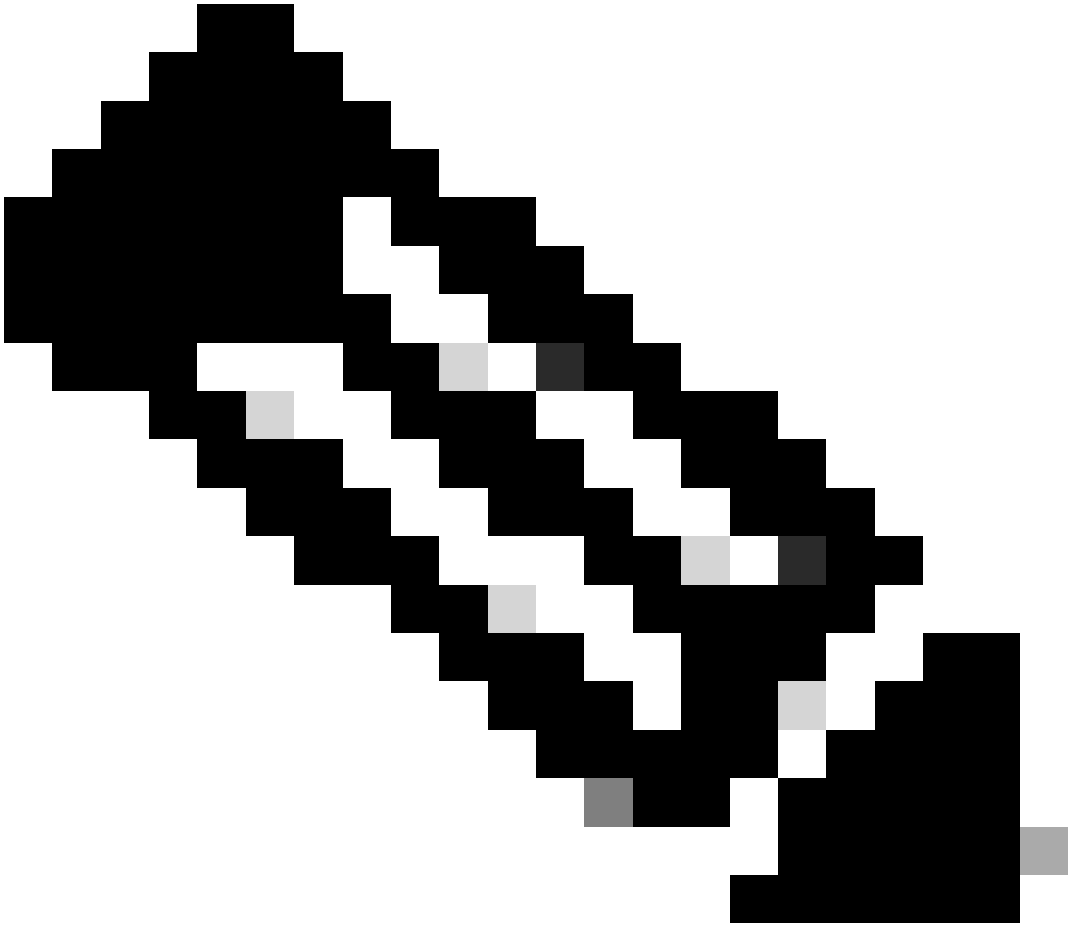
Anmerkung: Diese Konfigurationsoption in der WebUI legt den Parameter long_flow_duration in der Konfigurationsdatei flow collectors lc_threshold.txt fest.

- Die Sekunden, die erforderlich sind, um einen Datenfluss als verdächtige Einstellung für stille lange Datenflüsse zu qualifizieren, steuern das Verhalten des Ereignisses "Verdächtiger stille lange Datenfluss".



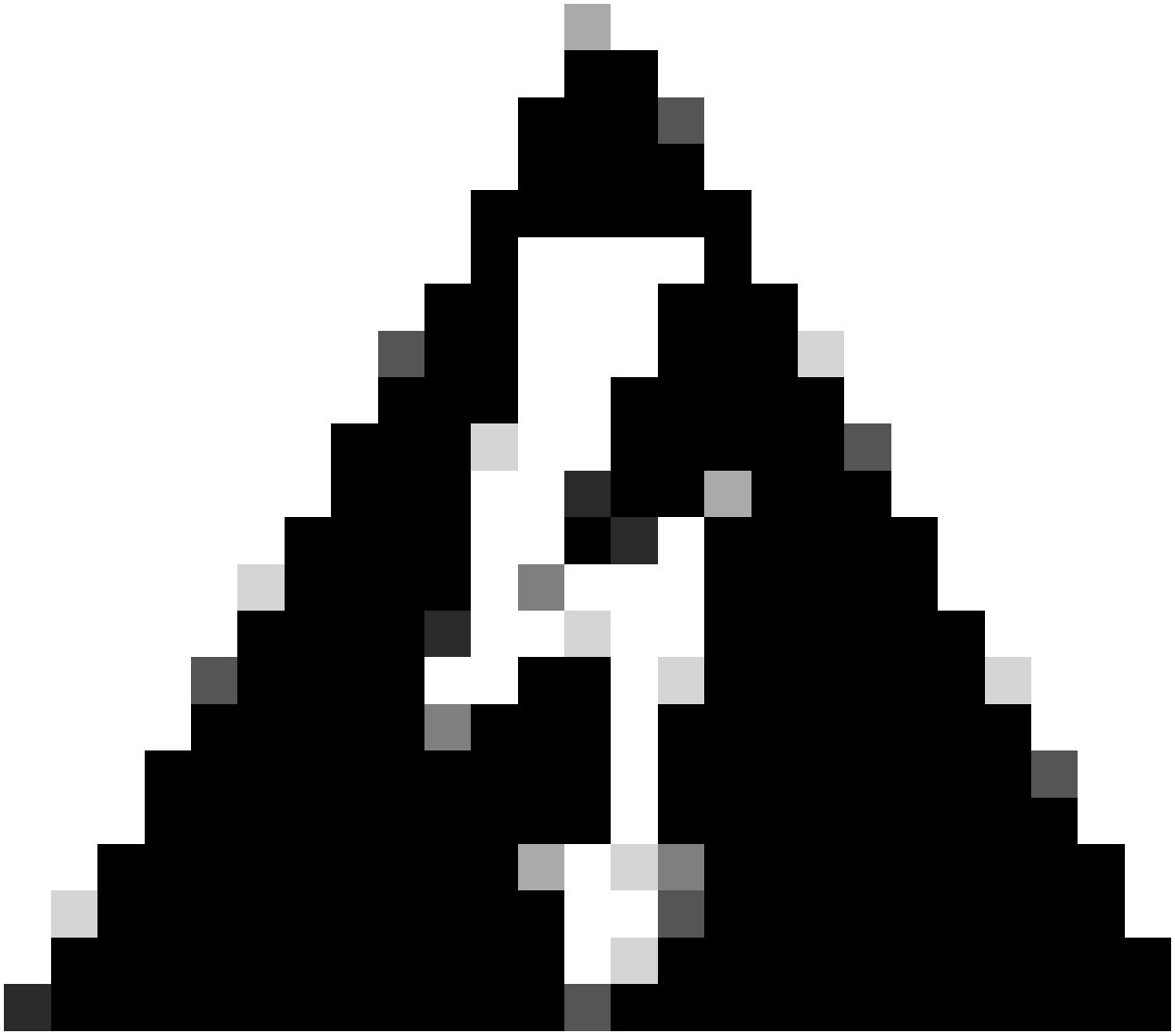
Anmerkung: Diese Konfigurationsoption in der WebUI legt den Parameter "peace_long_flow_duration" in der Konfigurationsdatei "flow collectors lc_threshold.txt" fest.

Der Standardwert für beide Zähler beträgt 32400 Sekunden (9 Stunden).



Anmerkung: In Bezug auf die Änderung dieser Zähler, CDET:

Cisco Bug-ID CSCwm05128



Warnung: Dies betrifft nur v7.5.1 oder frühere Versionen.

Dieser Mangel legt fest, dass ein verdächtiger langer Fluss zunächst auch ein verdächtiger langer Fluss sein muss. Das bedeutet, dass unerwartete Ergebnisse wahrscheinlich sind, wenn Sie die Sekunden, die erforderlich sind, um einen Fluss als verdächtigen langen Fluss zu qualifizieren, auf eine Dauer ändern, die kürzer ist als die Sekunden, die erforderlich sind, um einen Fluss als langen Fluss zu qualifizieren.

Wenn Sie eine oder beide dieser erweiterten Einstellungen ändern, kann dies dazu führen, dass die Erkennung langer Datenflüsse fehlschlägt.

Da ein Quiet Long Flow definitionsgemäß auch ein Long Flow sein muss, liegt die Logik bei der richtigen Handhabung dieser beiden Einstellungen darin, dass der Flow zunächst den Long Flow-Bedarf übersteigt, bevor er auf einen ruhigen Long Flow getestet wird.

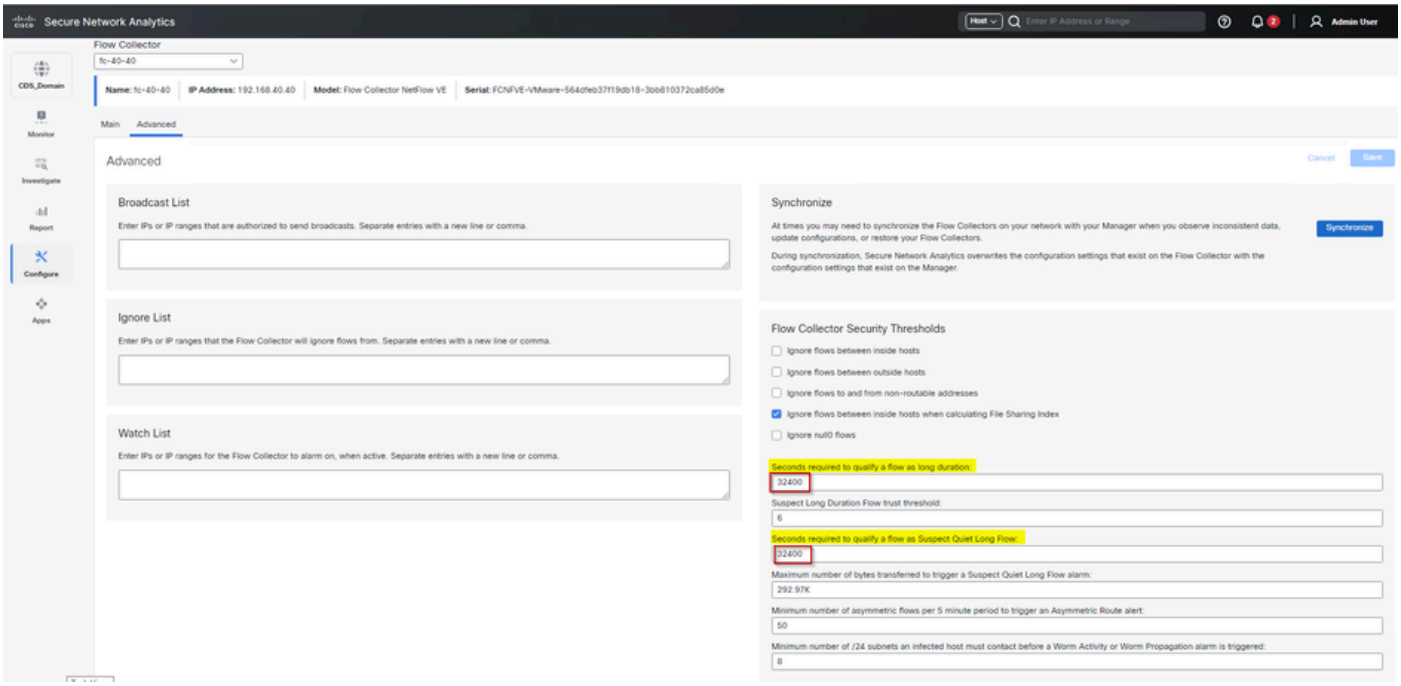
Wenn z. B. long_flow_duration auf dem Standardwert von 9 Stunden belassen wird und still_long_flow_duration auf einen niedrigeren Wert gesetzt wird, z. B. auf 8 Stunden, löst der

Motor kein stille Langzeit-Flow-Ereignis aus, bis der Flow mindestens 9 Stunden lang ist.

Wenn long_flow_duration auf dem Standardwert von 9 Stunden belassen wird und "silly_long_flow_duration" auf 10 Stunden festgelegt ist, deaktiviert diese Konfiguration das Flow-Ereignis mit langer Laufzeit effektiv (es sei denn, es handelt sich um einen einzelnen Export mit einer Dauer > silly_long_flow_duration von 10 Stunden).

Lösung

Beide erweiterten Einstellungen müssen auf den gleichen Sollwert gesetzt werden, oder der Wert für "silly_long_flow_duration" muss immer >= long_flow_duration sein.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.