Secure AnalyticsでのSLFおよびSQLFセキュリティイベントの設定

内容

はじめに

このドキュメントでは、疑わしいロングフロー(SLF)のセキュリティイベントと疑わしいサイレントロングフロー(SQLF)のセキュリティイベントを調整するために使用できる2つのパラメータについて説明します。

背景説明

Suspect Long Flowイベントは、Secure Analyticsによって生成される特定タイプのセキュリティイベントで、ホスト間の通常よりも長い会話を検出するように設計されています。Suspect Long Flowイベントには、Suspect Long FlowとSuspect Quiet Long Flowの2種類があります。

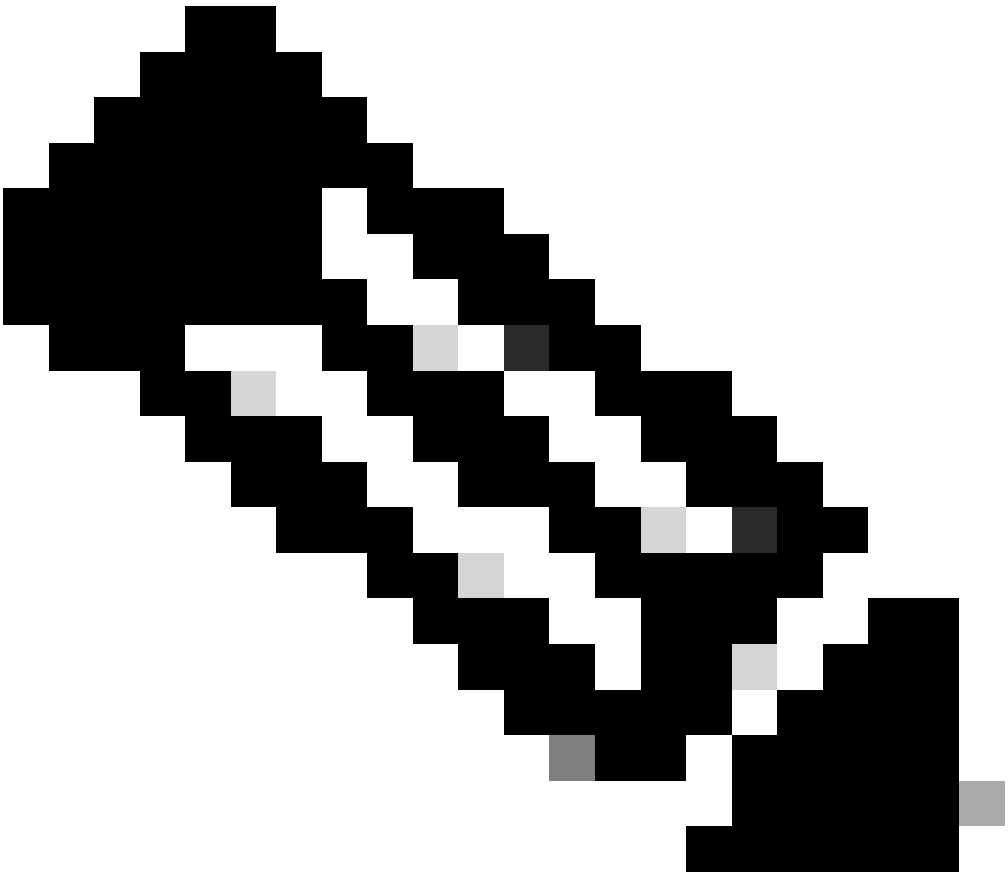
ラップトップを秘密のVPN経由で自宅のPCに3日間接続し、自宅のPCもラップトップも通常は長いフロー接続を実行していないと考えてください。Flow Collectorはこの異常を検出し、通過するトラフィック量とフローの期間に応じてセキュリティイベントをトリガーします。これらのイベントの目的は、最小限のトラフィックを通過する長時間実行フローと長時間実行フローを特定することです。

調整/設定

主に2つのフローコレクタ設定パラメータがあり、これら2つのイベントの動作を制御します。

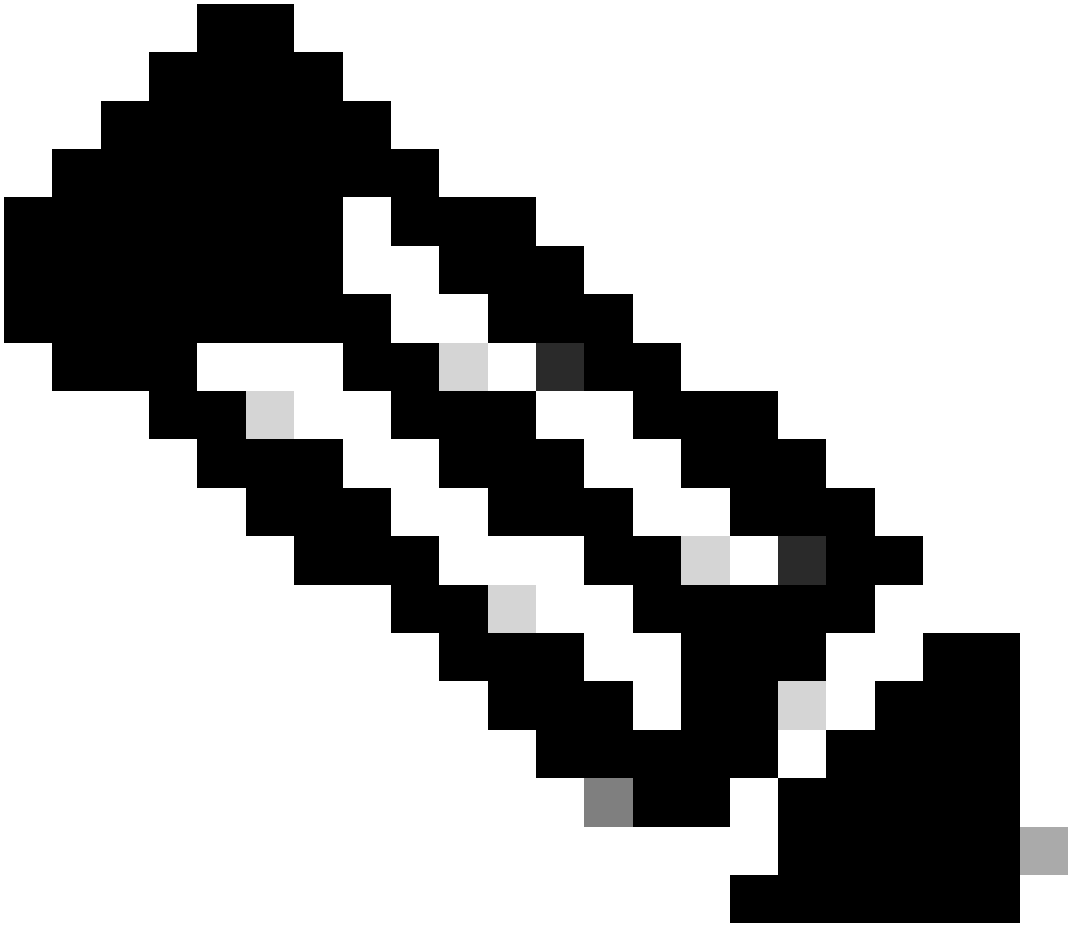
これらの設定は、マネージャアプライアンスのWebUIで設定>フローコレクタ>詳細ページにアクセスして調整できます。

- フローを長期間の設定として認定するのに必要な秒数は、疑わしいロングフローイベントの動作を制御します。



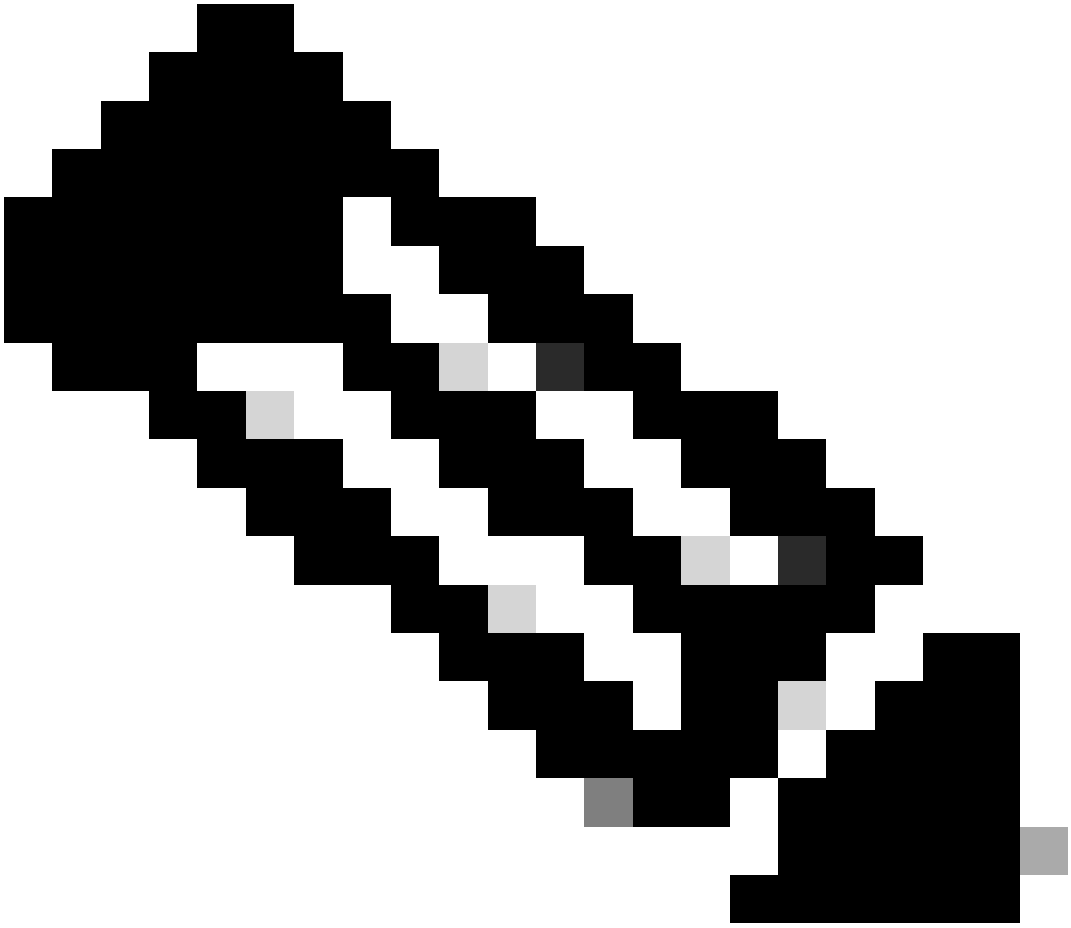
注:webUIのこの設定オプションは、フローコレクタlc_thresholds.txtコンフィギュレーションファイルのlong_flow_durationパラメータを設定します。

- フローを疑わしいサイレントロングフロー設定として認定するのに必要な秒数は、疑わしいサイレントロングフローイベントの動作を制御します。



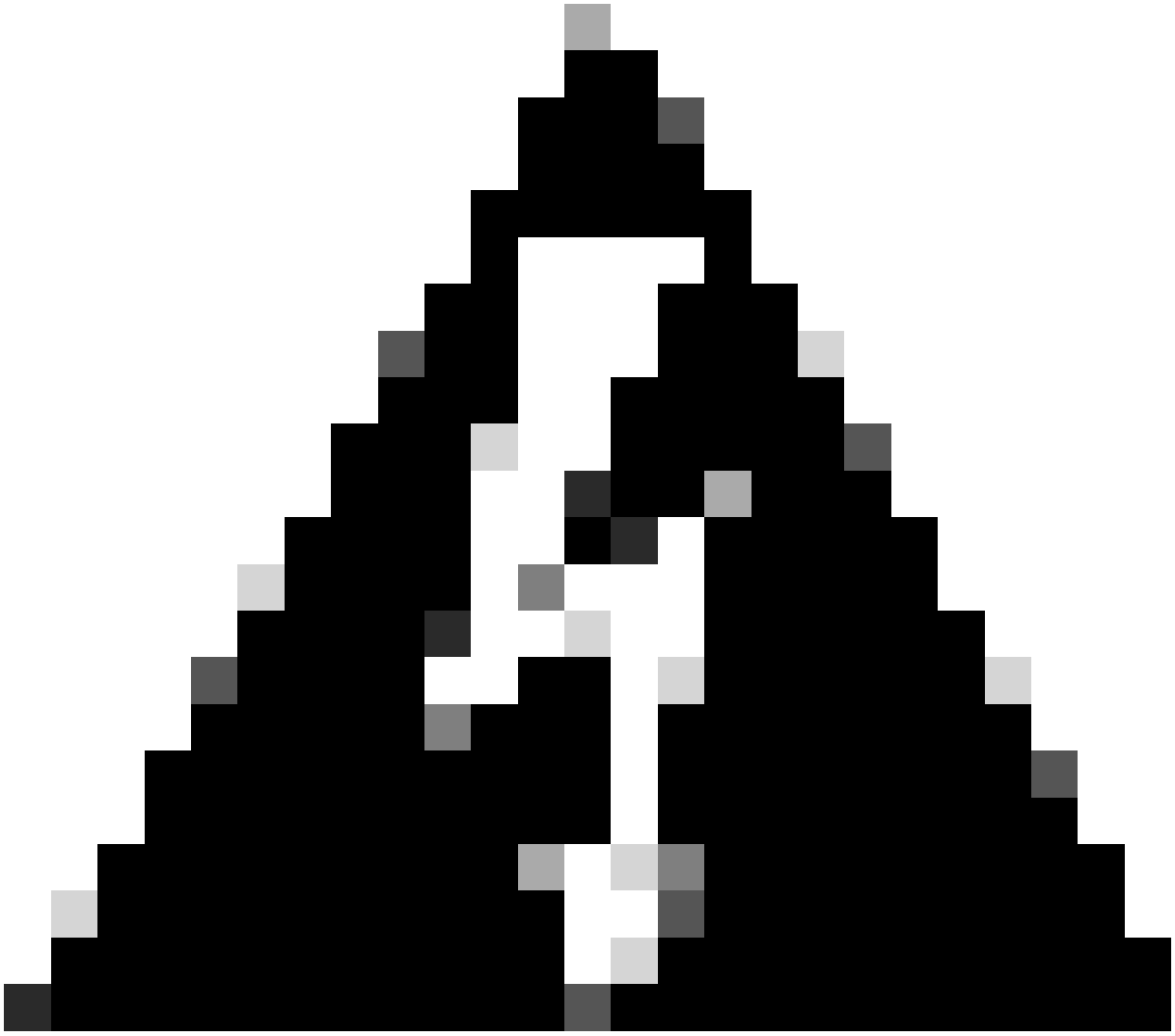
注:webUIのこの設定オプションは、フローコレクタlc_thresholds.txtコンフィギュレーションファイルのquiet_long_flow_durationパラメータを設定します。

両方のカウンタのデフォルト値は32400 秒（9時間）です。



注：これらのカウンタの変更に関しては、関連するCDET:

Cisco Bug ID CSCwm05128



警告：この問題は、v7.5.1以前のバージョンにのみ該当します。

この不具合は、疑わしい静かなロングフローが最初は疑わしいロングフローでなければならないことを指示します。つまり、フローを「疑わしい静かな長いフロー」として認定するのに必要な秒数を「長いフロー」として認定するのに必要な秒数よりも短い時間に変更すると、予期しない結果が生じる可能性があります。

これらの詳細設定のいずれかまたは両方を変更すると、長いフローの検出が失敗する可能性があります。

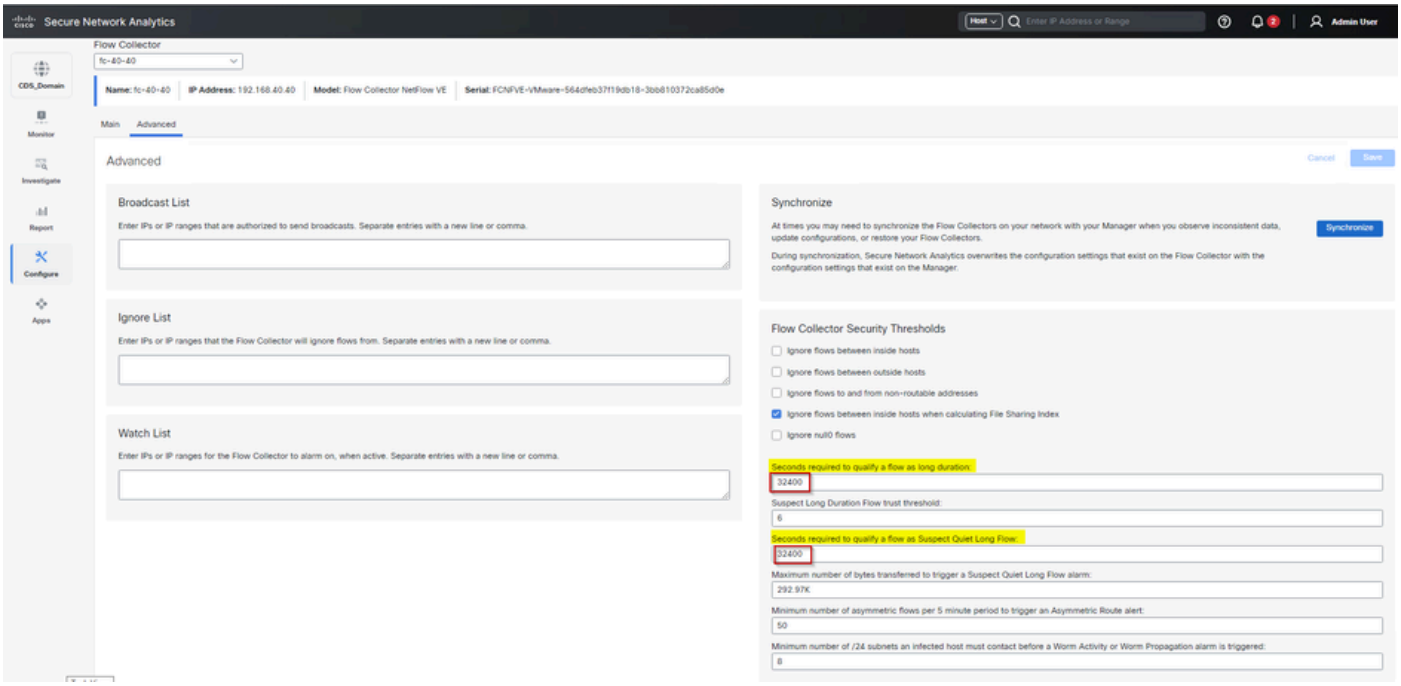
定義によるQuiet Long FlowもLong Flowである必要があるため、これら2つの設定を適切に処理するロジックは、フローがLong Flowの要件を超えてから、Quiet Long Flowであることをテストすることです。

たとえば、long_flow_durationをデフォルト値の9時間のままにし、quiet_long_flow_durationを8時間などの低い値に設定した場合、エンジンはフローの長さが9時間以上になるまで静かな長時間流動イベントを発生させません。

代替策として、long_flow_durationを9時間のデフォルト値のままにし、quiet_long_flow_durationを10時間に設定した場合、この設定は実質的にクワイエットロングデュレーションフローイベントを無効にします（フローが、duration > quiet_long_flow_durationの値が10時間のシングルエクスポートである場合を除く）。

解決方法

これらの詳細設定は、両方とも同じ目的の値に設定する必要があります。または、quiet_long_flow_durationが常に>= long_flow_durationである必要があります。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。