Cisco Secure Network Analytics

v7.4.2 デフォルトのカスタムセキュリティイベントの設定ガイド

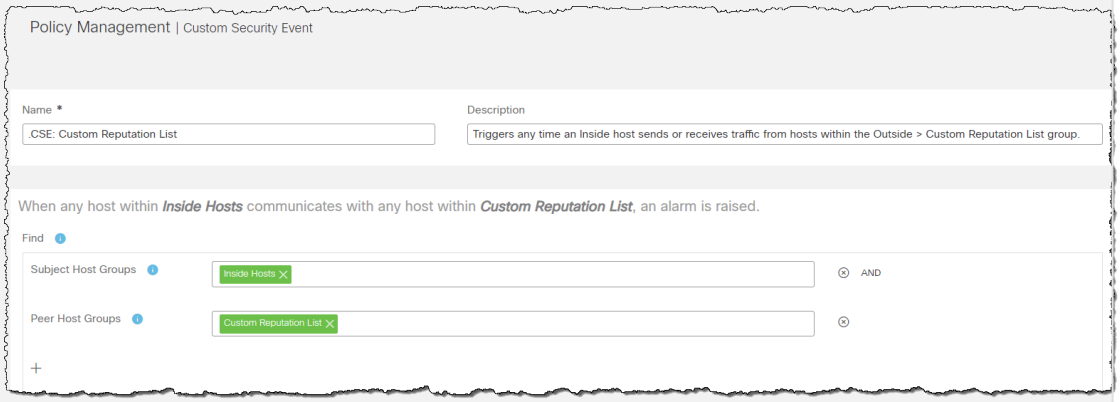
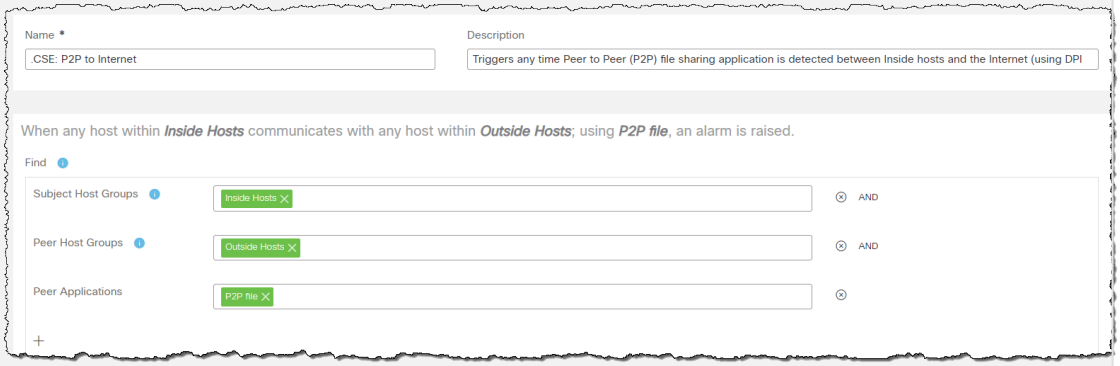
目次

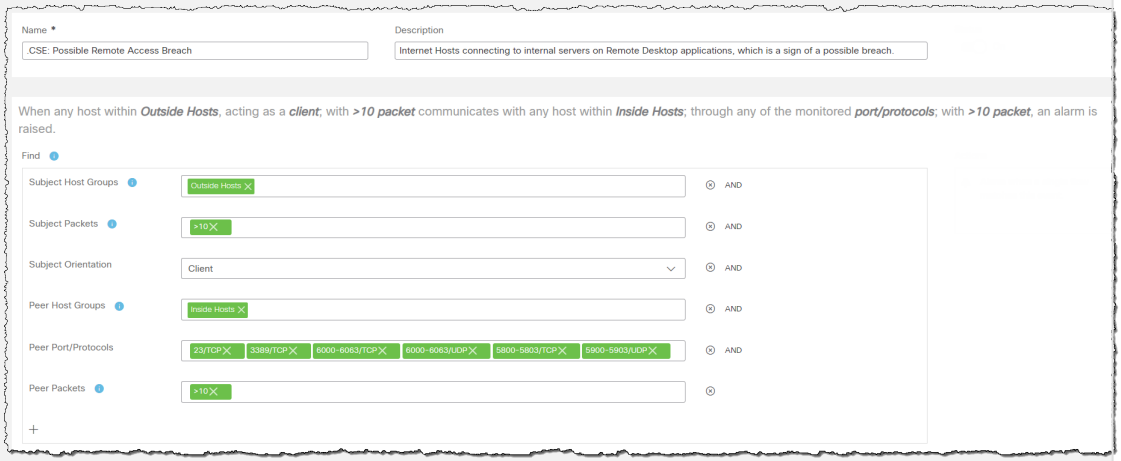
デフォルトのカスタム セキュリティ イベント

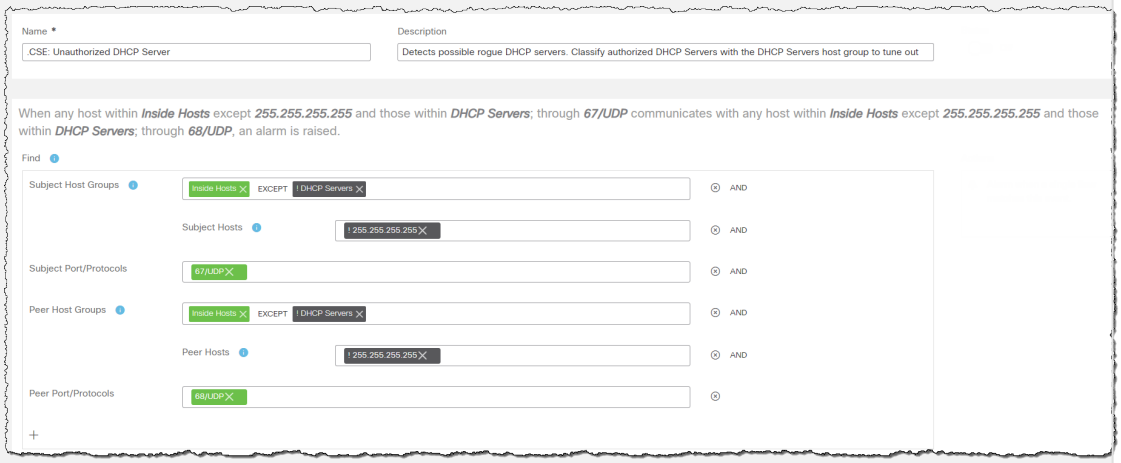
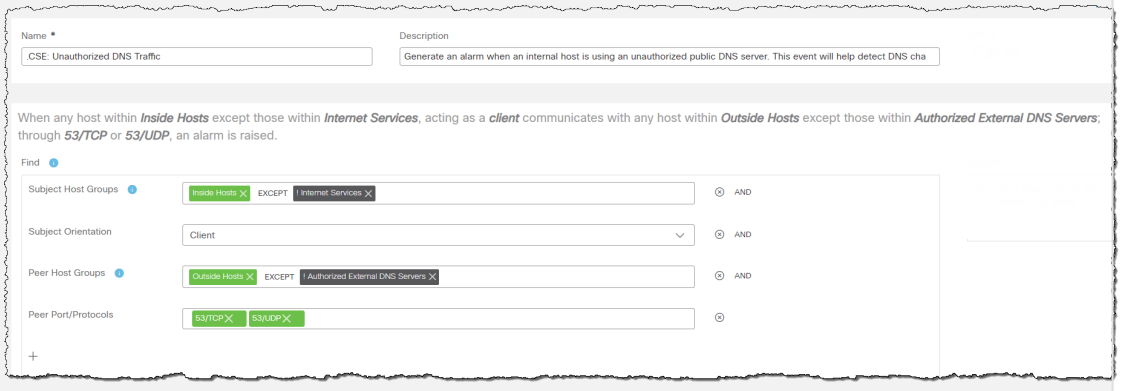
Cisco Secure Network Analytics（旧 Stealthwatch）の新しい導入（v7.1 以降）には、次の定義済みのカスタム セキュリティ イベント（CSE）が付属しています。アップグレードされたシステムにこれらのイベントを追加する場合は、これらの CSE で使用されるホストグループがお使いの環境に存在していることを確認します。詳細については、このガイドの最後のセクション「カスタム セキュリティ イベントのセットアップに関連するホストグループ」を参照してください。

Web アプリケーション のポリシー管理機能（[設定（Configure）] > [検出ポリシーの管理（DETECTION Policy Management）] > [カスタムイベント（Custom Events）] タブ）を使用して、以下で定義した各 CSE を手動で追加できます。CSE の設定方法の詳細については、Web アプリケーション のオンラインヘルプのトピック「**カスタムポリシー（カスタム セキュリティ イベント）の設定**」を参照してください。

いずれかの CSE を有効または無効にするには、[カスタムイベント（Custom Events）] タブの [トグル（Toggle）] アイコンを使用します。

カスタム セキュリティ イベント名	説明
v7.1 で追加	
	
CSE：カスタム レピュテーション リスト	[外部（Outside）] > [カスタム レピュテーション リスト（Custom Reputation List）] ホストグループ内のホストからトラフィックを送受信するたびにトリガーされます。 **このカスタム セキュリティ イベントはいつアラームをトリガーしますか？** 内部ホスト内のホストが**カスタム レピュテーション リスト**内の任意のホストと通信すると、アラームが発生します。 **このカスタム セキュリティ イベントでアラームが発生できるようにするには、何をする必要がありますか？** このカスタム セキュリティ イベントを有効にし、**カスタム レピュテーション リスト** のホストグループを入力する必要があります。
	
CSE：P2P からインターネット	内部ホストとインターネットの間でピアツーピア（P2P）ファイル共有アプリケーションが検出されるたびにトリガーされます。P2P ファイル共有アプリケーションは、リモートの悪用に対して脆弱である可能性があり、使用状況によってはポリシー違反を示す可

カスタム セキュリティ イベント名	説明
	能性があります。 **このカスタム セキュリティ イベントはいつアラームをトリガーしますか？** 外部ホスト内のホストが内部ホスト内の任意のホストと P2P ファイルを使用して通信すると、アラームが発生します。 **このカスタム セキュリティ イベントでアラームが発生できるようにするには、何をする必要がありますか？** このカスタム セキュリティ イベントを有効にし、フローセンサー を所有する必要があります。
	
CSE：リモートアクセス違反の可能性	インターネットホストがリモート デスクトップ アプリケーションの内部サーバーに接続するたびにトリガーされます。これは、違反の可能性があることを示しています。 **このカスタム セキュリティ イベントはいつアラームをトリガーしますか？** クライアントとして機能している外部ホスト内のホストが内部ホスト内の任意のホストと任意の監視対象ポートやプロトコルを経由して通信している場合は、アラームが発生します。 **このカスタム セキュリティ イベントでアラームが発生できるようにするには、何をする必要がありますか？** このカスタム セキュリティ イベントを有効にする必要があります。

カスタム セキュリティ イベント名	説明
	
CSE：DHCP サーバーへの不正接続	不正だと思われる DHCP サーバーを検出し、悪意のあるアクティビティやポリシー違反の可能性を示します。 **このカスタム セキュリティ イベントはいつアラームをトリガーしますか？** 内部ホスト内の任意のホスト（255.255.255.255 および **DHCP サーバー**内のホストを除く）が 67/UDP を介して内部ホスト内の任意のホスト（255.255.255.255 および **DHCP サーバー**内のホストを除く）と 68/UDP を通じて通信すると、アラームが発生します。 **このカスタム セキュリティ イベントでアラームが発生できるようにするには、何をする必要がありますか？** このカスタム セキュリティ イベントを有効にし、DHCP ホストグループを許可された DHCP サーバーに追加して、許可された DHCP サーバートラフィックを調整する必要があります。
	

カスタム セキュリティ イベント名	説明
CSE：不正な DNS トラフィック	内部ホストが無許可のパブリック DNS サーバーを使用するとアラームが生成されます。このイベントは、マルウェアやポリシー違反の可能性がある DNS チェンジャーの種類を検出するのに役立ちます。 **このカスタム セキュリティ イベントはいつアラームをトリガーしますか？** **インターネットサービス**内のホストを除く内部ホスト内のホストがクライアントとして機能し、53/UDP または 53/TCP を通じて**許可された外部 DNS サーバー**内のホストを除く外部ホスト内の任意のホストと通信すると、アラームが発生します。 **このカスタム セキュリティ イベントでアラームが発生できるようにするには、何をする必要がありますか？** このカスタム セキュリティ イベントを有効にし、**許可された外部 DNS サーバー**のホストグループまたは子ホストグループ（DNS サーバー、NAT ゲートウェイ、プロキシ）を追加する必要があります。

カスタム セキュリティ イベントの設定に関連するホストグループ

Secure Network Analytics の新しい導入（v7.1 以降）には、定義済みのカスタム セキュリティ イベントが多数付属しています。

次の各ホストグループは、これらのカスタム セキュリティ イベントの 1 つと組み合わせて使用されます。Secure Network Analytics システムをアップグレードする場合、追加および設定するカスタム セキュリティ イベントに応じて、次の 1 つ以上のホストグループを環境に追加する必要があります。

マネージャ（旧 Stealthwatch Management Console）でホストグループ管理機能（[設定（Configure）] > [検出ホストグループ管理（DETECTION Host Group Management）]）を使用して、追加するホストグループのインターネット IP 範囲を定義できます。詳細については、マネージャ ヘルプのトピック**「ホストグループの管理と設定」**にある「ホストグループの詳細の表示」セクションを参照してください。

ホストグループ名	説明
v7.1 より前に追加	
DHCP サーバー	このホストグループを使用して、組織で使用する DHCP サーバーを定義します。このホストグループを [CSE：無許可DHCPトラフィック（CSE: Unauthorized DHCP Traffic）] カスタム セキュリティ イベントと組み合わせて使用すると、内部ホスト内のホスト（255.255.255.255 を除く）および DHCP サーバー内のホスト（67/UDP を使用）が、内部ホスト内のホスト（255.255.255.255 を除く）および DHCP サーバー内のホスト（68/UDP を使用）と通信したときに、アラームを生成できます。
v7.1 で追加	
許可済み外部 DNS サーバー	マルウェアが原因で、ホストの DNS サーバーが、フィッシングや不正な配信に使用されるサイトにリクエストを転送する場合があります。同様に、承認されていない DNS サーバーをネットワークユーザーが使用して、内部ポリシーで禁止されている Web リソースにアクセスしてしまう場合もあります。[許可済み外部DNSサーバー（Authorized External DNS Servers）] ホストグループを使用して、組織で使用するパブリック DNS リゾルバを定義します。このホストグループを [CSE: 無許可DNSトラフィック（CSE: Unauthorized DNS Traffic）] カスタム セキュリティ イベントと組み合わせて使用すると、内部ホストが無許可のパブリック DNS サーバーを使用したときにアラームを生成できます。このイベントは、DNS チェンジャータイプのマルウェアを検出するのに役立ちます。

ホストグループ名	説明
カスタム レピュテーション リスト	多くの組織は、不審なインターネットホストのインターネットウォッチ リストを独自に保持しています。[カスタム レピュテーション リスト（Custom Reputation List）] ホストグループを [CSE: カスタム レピュテーション リスト（CSE: Custom Reputation List）] カスタム セキュリティ イベントと組み合わせて使用すると、内部ホストが [カスタム レピュテーション リスト（Custom Reputation List）] ホストグループ内のホストとの間でトラフィックを送受信するたびに、その送受信を検出できます。
インターネットサービス	このホストグループと子ホストグループ（DNS サーバー、NAT ゲートウェイ、プロキシ）を使用して、組織内でインターネットサービスを定義します。[インターネットサービス（Internet Services）] ホストグループを [CSE: 無許可DNSトラフィック（CSE: Unauthorized DNS Traffic）] カスタム セキュリティ イベントと組み合わせて使用すると、既知の内部インターネットサービス以外の内部ホストがパブリック DNS サーバーを使用したときにアラームを生成できます。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 2 月	最初のバージョン

著作権情報