Cisco Secure Cloud Analytics

攻撃チェーンガイド

目次

はじめに

概要

このガイドでは、Cisco Secure Cloud Analytics の攻撃チェーンについて説明します。この機能は、より大きな脅威の一部である可能性のあるアラートを「攻撃チェーン」に関連付けることで、個々のアラートを調査するときに通常必要とされる時間を短縮します。攻撃チェーンは、調査の優先順位付けに役立つようにランク付けされます。

攻撃チェーンの構築方法

抽出されたアラートのメタデータを使用して、アラートに共通するもの（共通インジケータ）を判断します。一般的なインジケータには、デバイス、IP アドレス、ホスト名、およびユーザー名が含まれます。次に、MITRE ATT&CK® フレームワークに従って、戦術、手法、および手順（TTP）をさらに詳しく特定し、攻撃の早期兆候となる可能性があるアクションと脅威の動作の順序をモデル化します。

> すべてのアラートが共通のインジケータを共有するわけではありません。共通のインジケータを共有しないアラートは、個別に分析する必要があります。

攻撃チェーンの優先順位付けとランク付け

攻撃チェーンのランキングを使用すると、すぐに調査する必要がある攻撃チェーンに優先順位を付けることができます。評価された脅威レベルにより、各攻撃チェーンのシビラティ（重大度）ランキングが次の項目に基づいて割り当てられます。

- 特定された MITRE ATT&CK の戦術
- 関連するデバイスのサブネット感度
- 攻撃チェーン内のアラートの優先度（低/中/高）
- 攻撃チェーン内のアラートの数

> 固有の環境に合わせて、**サブネットの感度**と**アラートの優先順位**の設定を確認してください。詳細については、**アラート設定の確認**を参照してください。

ランク付けプロセスは、次のスコアを使用して調整されます。

- **標準アラートスコア**：アラートで識別されたデバイスのサブネット感度とアラートの優先順位を使用して計算される正規化されたスコアです。
- **標準戦術スコア**：チェーン内のアラートの MITRE ATT&CK 戦術の優先順位と、デバイスの対応するサブネット感度を使用して計算される正規化されたスコアです。このスコアでは、チェーン内の MITRE ATT&CK 戦術の進行状況を調べて、考え得るサイバーキルチェーンの異なるステージ間を移動する際の攻撃の意図を評価します。

各攻撃チェーンは、次のように低、中、高にランク付けされます。

ランク	説明
低 **黄色**	低とランク付けされた攻撃チェーンは、他の攻撃チェーンと比較した場合に、最小の潜在的リスクを環境にもたらします。複数の攻撃チェーンがある場合、優先順位付けは、アラートの優先順位、デバイスとサブネットの感度、MITRE ATT&CK 戦術の優先順位などの要因の組み合わせに基づいて行われます。
中 **オレンジ**	中とランク付けされた攻撃チェーンは、他の攻撃チェーンと比較した場合に、中程度のリスクを環境にもたらします。複数の攻撃チェーンがある場合、優先順位付けは、アラートの優先順位、デバイスとサブネットの感度、MITRE ATT&CK 戦術の優先順位などの要因の組み合わせに基づいて行われます。
高 **赤**	高とランク付けされた攻撃チェーンは、他の攻撃チェーンと比較した場合に、最大の潜在的リスクを環境にもたらします。複数の攻撃チェーンがある場合、優先順位付けは、アラートの優先順位、デバイスとサブネットの感度、MITRE ATT&CK 戦術の優先順位などの要因の組み合わせに基づいて行われます。

高にランク付けされた攻撃チェーンは、Cisco XDR または Cisco SecureX に自動的に送信され、修復を促進します（Cisco XDR または SecureX がインストール済みの場合）。

アラート設定の確認

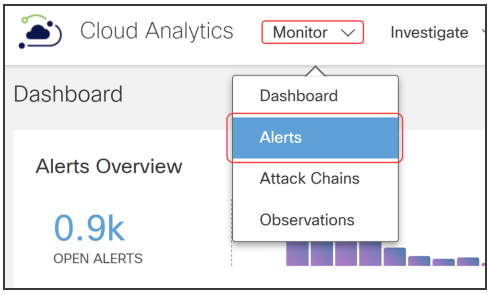
[サブネットの感度(Subnet Sensitivity)]と[アラートの優先順位(Alert Priority)]の設定は、攻撃チェーンの一部となる可能性のあるアラートに影響します。サブネットの感度は生成できるアラートに影響し、アラートの優先順位はサブネットトラフィックの監視の程度に影響します。

> サブネットの感度とアラートの優先順位がアラートにどのように影響するかについては、設定プロセス中に[Priorities(優先順位)]ページの[サブネットの感度マトリックス(Subnet Sensitivity Matrix)]リンクをクリックしてください。

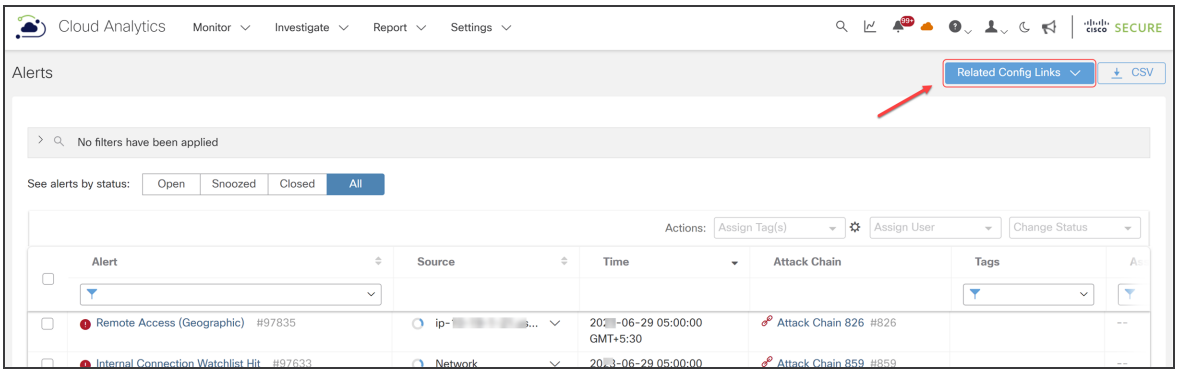
サブネット感度の設定

サブネットの感度を設定するには、次の手順を実行します。

1. [モニター(Monitor)]>[アラート(Alerts)]を選択します。

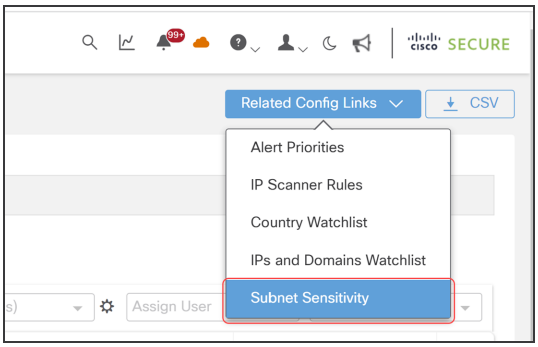


2. [アラート(Alerts)]ページで[関連設定リンク(Related Config Links)]をクリックします。

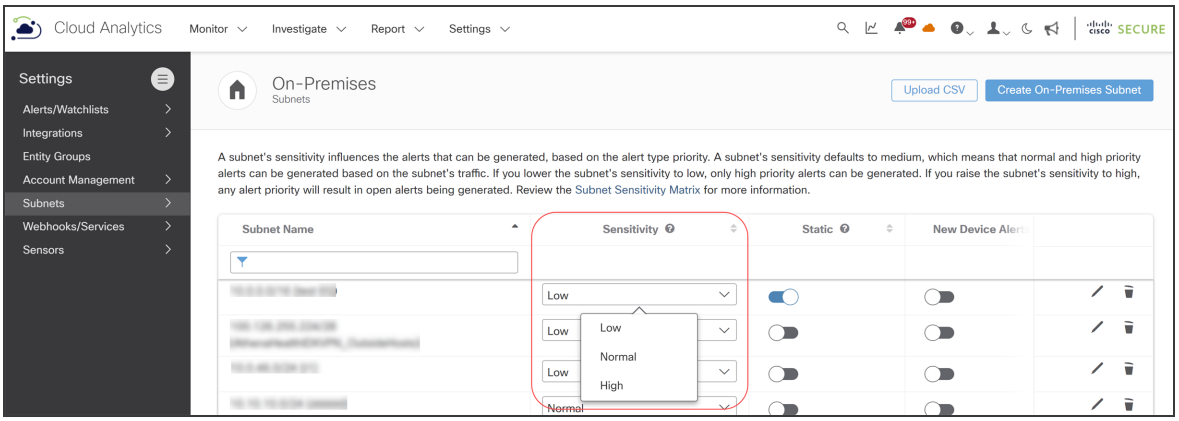


> アラートが攻撃チェーン内にどのように含まれているか詳細を表示するには、🔗([リンク(Link)])アイコンをクリックします。

3. [サブネット感度(Subnet Sensitivity)]を選択すると、アラート生成対象のサブネットの感度を設定できます。



4. [感度(Sensitivity)]フィールドで[低(Low)]、[標準(Normal)]、または[高(High)]を選択します。

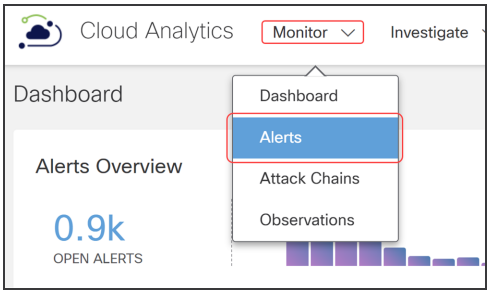


> Merit_AUTO_IGNORED でクローズされたアラートは、攻撃チェーンに含まれません。アラートに[低(Low)]を指定するかどうかを確認してください。

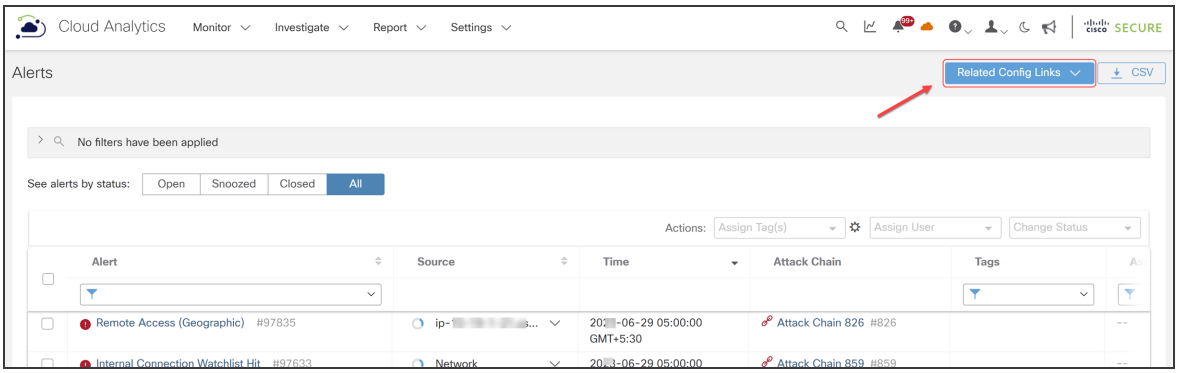
アラートの優先順位の設定

アラートの優先順位を設定するには、次の手順を実行します。

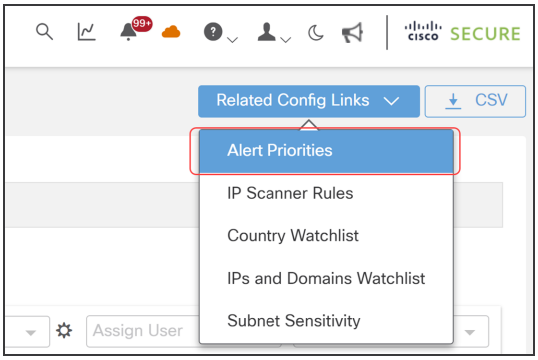
1. [モニター(Monitor)]>[アラート(Alerts)]を選択します。



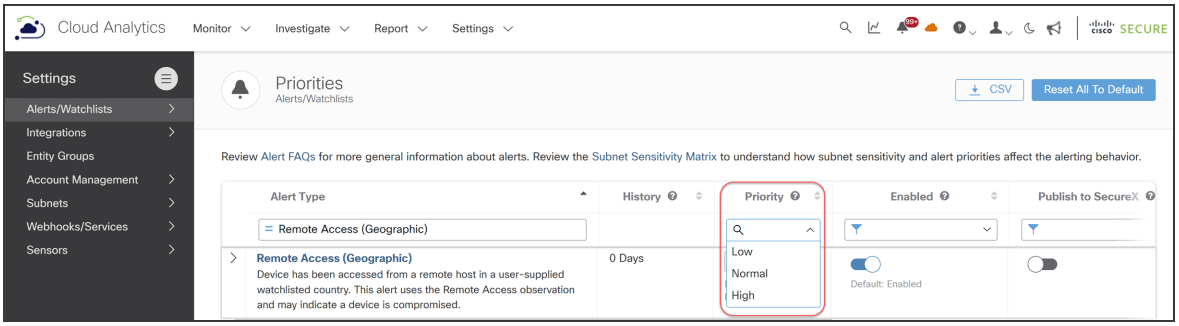
2. [アラート(Alerts)]ページで[関連設定リンク(Related Config Links)]をクリックします。



3. [アラートの優先順位（Alert Priorities）] を選択すると、アラートの優先順位を設定できます。



4. [優先順位（Priorities）] ページの [優先順位（Priority）] フィールドで、[低（Low）]、[標準（Normal）]、または [高（High）] を選択します。



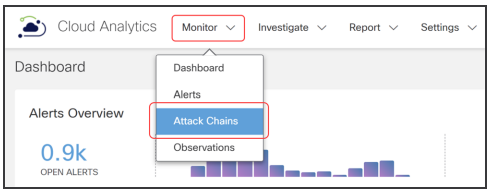
> Merit_AUTO_IGNORED でクローズされたアラートは、攻撃チェーンに含まれません。アラートに [低（Low）] を指定するかどうかを確認してください。

[攻撃チェーン（Attack Chains）] ページへのアクセス

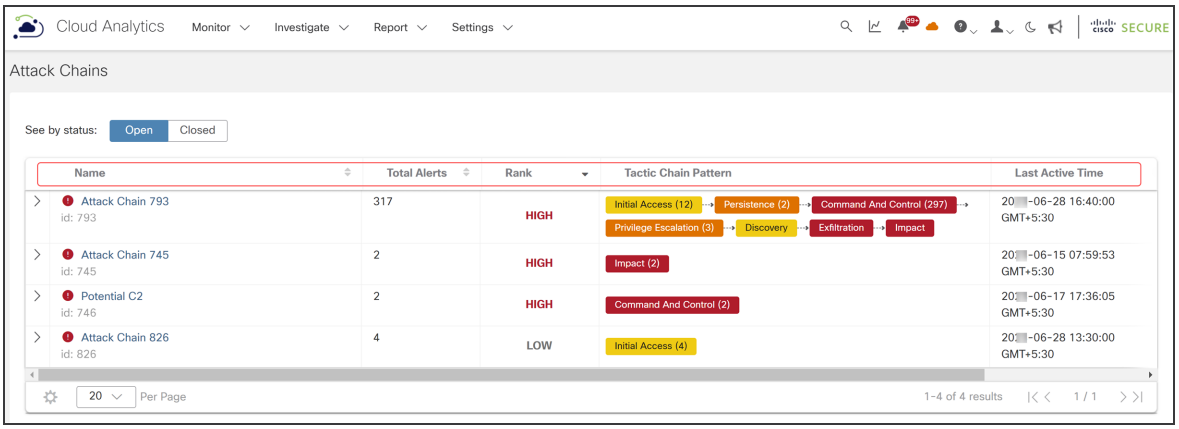
[攻撃チェーン（Attack Chains）] ページには、ランクでソートされた攻撃チェーンが表示され、環境に対するリスクが最も高い攻撃チェーンが視覚的に示されます。

[攻撃チェーン（Attack Chains）] ページにアクセスするには、次の手順を実行します。

1. ダッシュボードから、[モニター（Monitor）] > [攻撃チェーン（Attack Chains）] の順に選択します。



[攻撃チェーン（Attack Chains）] ページが表示され、デフォルトで [ステータス別の表示（See by status）] フィールドが [オープン（Open）] になります。[クローズ済み（Closed）] をクリックして、クローズされた攻撃チェーンを表示します。

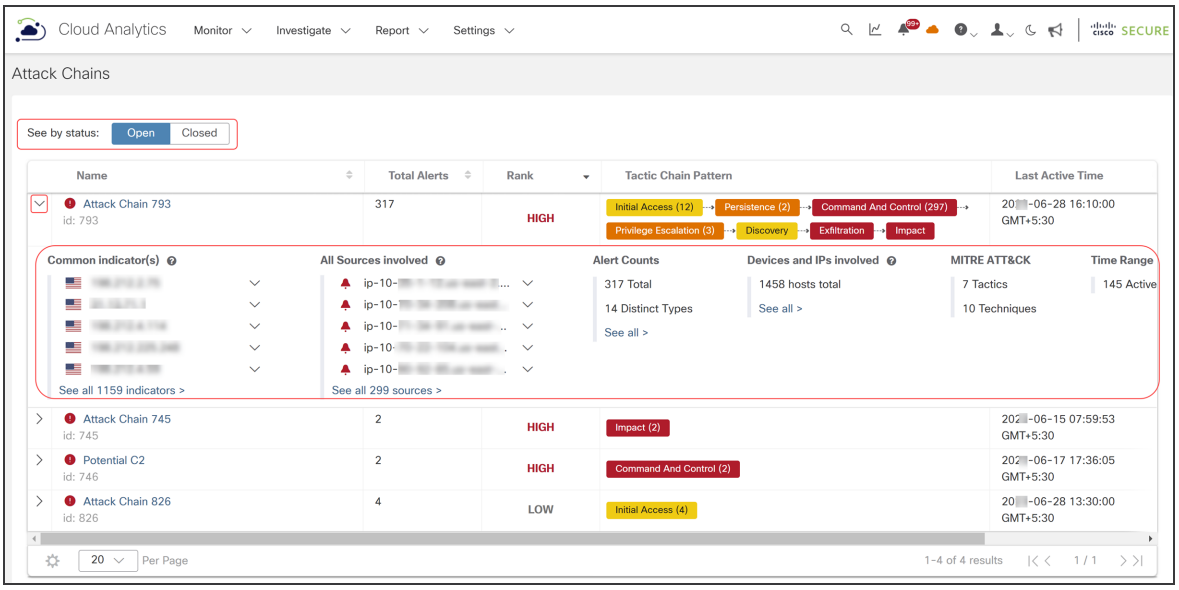


2. 列のタイトルをクリックして、攻撃チェーンの表示方法をソートします。次の表に、各列の説明を示します。

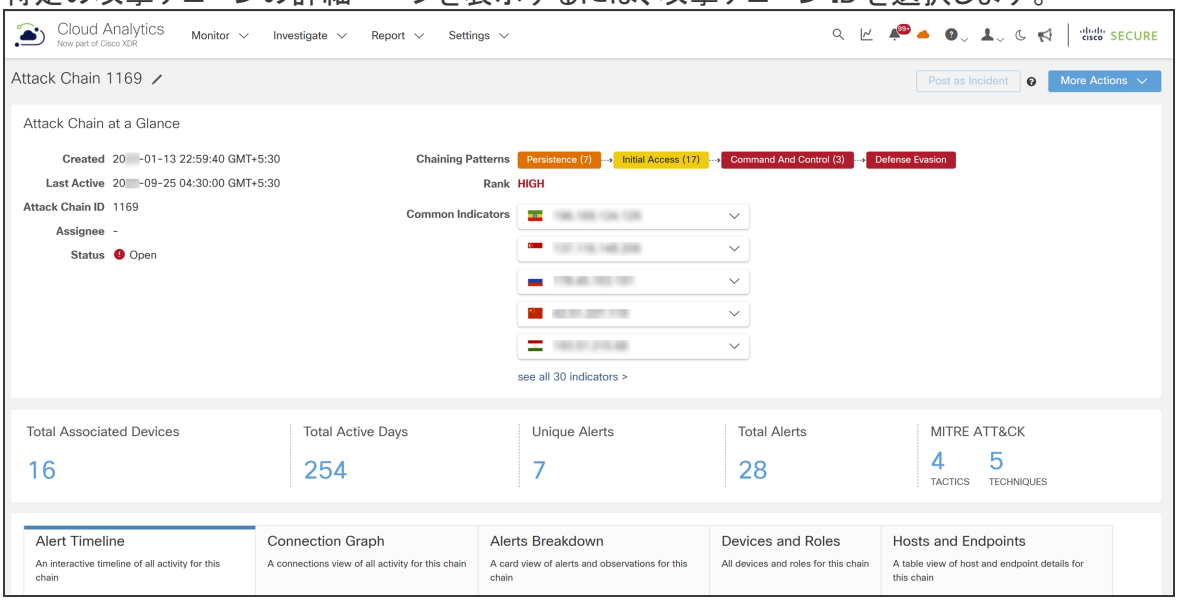
列のタイトル	説明
名前	特定の攻撃チェーンを識別するために使用される名前
アラートの総数	攻撃チェーン内のアラートの総数
ランク	黄色 = 低、オレンジ = 中、赤 = 高
戦術チェーン パターン	攻撃チェーンの動作を示す MITRE ATT&CK 戦術のパターンシーケンス

列のタイトル	説明
最終アクティブ時刻（Last Active Time）	攻撃チェーン内のアラートの観測が最後に更新された時刻
作成時刻	攻撃チェーンの最初のアラートが作成された時刻

3. 攻撃チェーン ID の横にある ＞（**右矢印**）アイコンをクリックすると、一般的なインジケータ、関連するすべての送信元、アラート数、関連するデバイスと IP、MITRE ATT&CK、時間範囲など、攻撃チェーンに関する追加情報が表示されます。追加情報の表示を閉じるには、（**下矢印**）アイコンをクリックします。



4. 特定の攻撃チェーンの詳細ページを表示するには、攻撃チェーン ID を選択します。



特定の攻撃チェーンの詳細ページには、攻撃チェーンが作成または更新された日時、攻撃チェーンのステータス、および以下の合計数など、攻撃チェーンに関する詳細が表示されます。

- 攻撃チェーンで特定されたデバイス
- 攻撃チェーンがアクティブだった日数
- 攻撃チェーンで一意のアラートを強調表示するアラート数
- 攻撃チェーン内の MITRE ATT&CK の戦術と手法の数

5. 詳細については、次のいずれかのタブを選択します。

- **[アラートタイムライン（Alert Timeline）]**：タイムライン内のアラートの概要ビューを表示します。
- **[接続グラフ（Connection Graph）]**：アラートと一般的なインジケータの接続されたネットワークグラフを表示し、可視性を向上させます。
- **[アラートの内訳（Alerts Breakdown）]**：攻撃チェーン内のアラートに関する詳細を提供します。
- **[デバイスとロール（Devices and Roles）]**：チェーン内のすべての内部デバイスと対応するロールの概要ビューを表示します。
- **[すべてのホストとエンドポイント（All Hosts and Endpoints）]**：チェーンに参加しているすべてのホストのチェーンビュー内のすべてのホストの概要、属性（ソース、インジケータ）、関連するアラートの数、MITRE ATT&CK の戦術と手法の詳細が表示されます。

攻撃チェーンの管理

攻撃チェーンは、最新のアラートアクティビティから 1 年間利用可能です。攻撃チェーンが自動的にクローズされ、新しい攻撃チェーンにマージされた場合、最新のアラートアクティビティから 90 日間は元の攻撃チェーンが保持されます。

攻撃チェーンを作成した後は、名前を変更したり、解決する担当者に割り当てたり、クローズしたり開いたり、Cisco XDR または SecureX に送信したりすることができます。

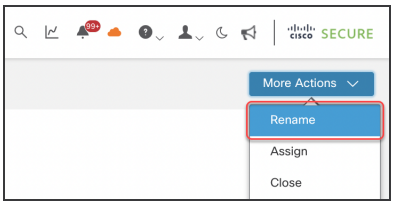
次のタスクは、攻撃チェーンの管理に役立ちます。

- **攻撃チェーンの名前変更**
- **攻撃チェーンの割り当て**
- **攻撃チェーンをクローズする**
- **攻撃チェーンを開く**
- **インシデントとしての攻撃チェーンの送信**

攻撃チェーンの名前変更

攻撃チェーンの名前を変更するには、次の手順を実行します。

1. [モニター(Monitor)] > [攻撃チェーン(Attack Chains)] の順に選択して、[攻撃チェーン(Attack Chains)] ページにアクセスします。
2. [攻撃チェーン(Attack Chains)] ページで、[攻撃チェーン ID(Attack Chain ID)] を選択して、特定の攻撃チェーンの詳細ページを表示します。
3. [その他のアクション(More Actions)] > [名前の変更(Rename)] の順に選択します。



4. 攻撃チェーンの新しい名前を入力します。

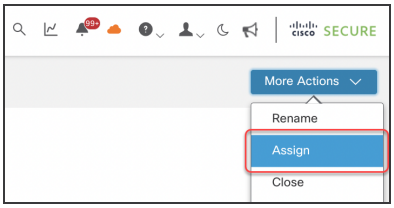
5. [保存(Save)]をクリックします。

攻撃チェーンの割り当て

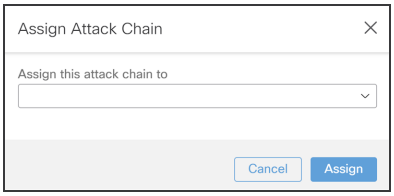
攻撃チェーンを割り当てるまたは再割り当てするには、次の手順を実行します。

1. [モニター(Monitor)] > [攻撃チェーン(Attack Chains)] の順に選択して、[攻撃チェーン(Attack Chains)] ページにアクセスします。
2. [攻撃チェーン(Attack Chains)] ページで、[攻撃チェーン ID(Attack Chain ID)] を選択して、特定の攻撃チェーンの詳細ページを表示します。

3. [その他のアクション（More Actions）] > [割り当て（Assign）] の順に選択します。



4. [この攻撃チェーンの割り当て先（Assign this attack chain to）] ドロップダウンリストから名前を選択します。



> [この攻撃チェーンの割り当て先（Assign this attack chain to:）] フィールドの横にある [x] をクリックして、現在の割り当て対象をクリアします。これにより、攻撃チェーンを再割り当てしていない場合は、現在の割り当て対象が削除されます。

5. [割り当て（Assign）] をクリックします。
6. [割り当て対象（Assignee）] フィールドを確認して、攻撃チェーンが正常に割り当てまたはクリアされたことを確認します。

攻撃チェーンをクローズする

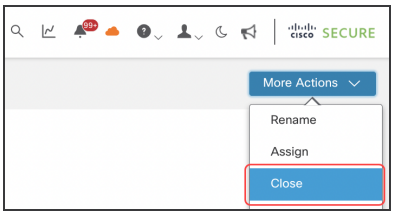
攻撃チェーンをクローズする場合は、**攻撃チェーンを開く**セクションの指示に従って開くことができます。

高ランクの攻撃チェーンは、Cisco XDR または SecureX に自動的に送信され、修復を促進します（Cisco XDR または SecureX がインストール済みの場合）。インシデントが Cisco XDR または SecureX でクローズされると、SCA の攻撃チェーンは自動的にクローズされます。

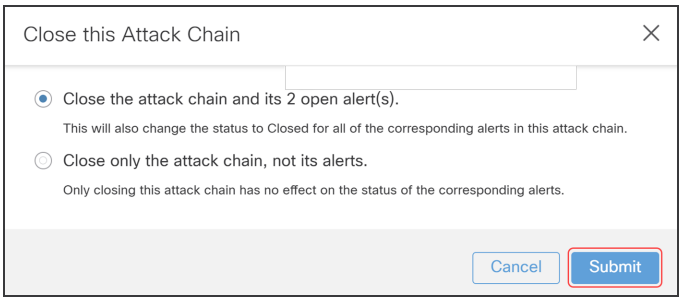
> Cisco XDR または SecureX に送信する前に、攻撃チェーンを開いてください。攻撃チェーンはクローズされていると、Cisco XDR または SecureX に送信できません。

攻撃チェーンをクローズするには、次の手順を実行します。

1. [モニター（Monitor）] > [攻撃チェーン（Attack Chains）] の順に選択して、[攻撃チェーン（Attack Chains）] ページにアクセスします。
2. [攻撃チェーン（Attack Chains）] ページで、[攻撃チェーン ID（Attack Chain ID）] を選択して、特定の攻撃チェーンの詳細ページを表示します。
3. [その他のアクション（More Actions）] > [クローズする（Close）] の順に選択します。



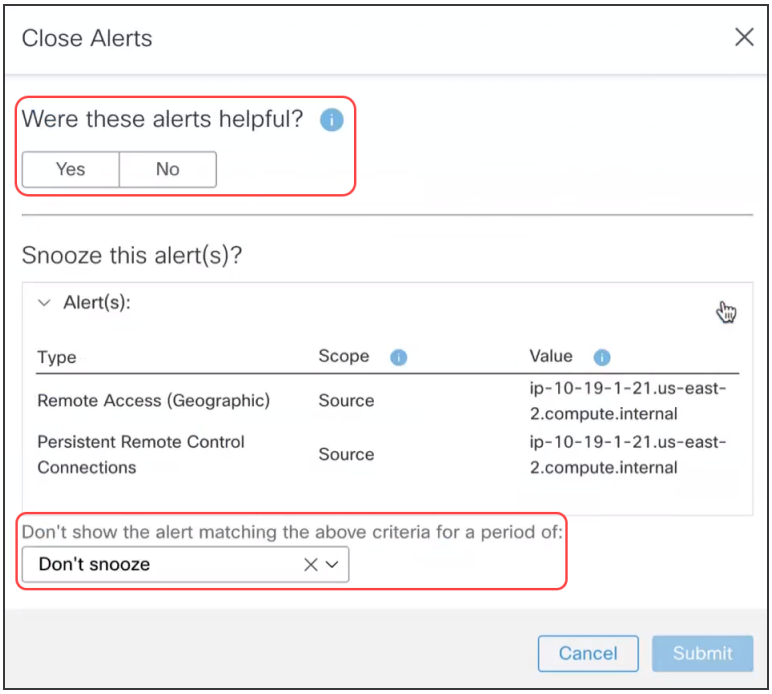
[この攻撃チェーンをクローズする(Close this Attack Chain)]ダイアログボックスが表示されます。



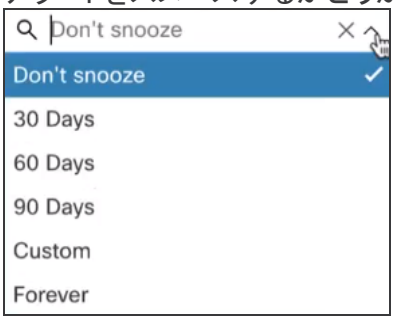
4. アラート付きで攻撃チェーンをクローズするかどうかを選択し、[送信(Submit)]をクリックします。

   アラートなしで攻撃チェーンをクローズすることを選択すると、攻撃チェーンを正しくクローズしたことを確認するメッセージが右下に表示されます。

   アラートとともに攻撃チェーンをクローズすることを選択すると、[アラートをクローズする(Close Alerts)]ダイアログボックスが表示されます。



5. [はい(Yes)] または [いいえ(No)] をクリックして、アラートが役に立ったかどうかを示します。
6. アラートをスヌーズするかどうかを選択します。スヌーズする場合は、期間も選択します。



7. [送信(Submit)] をクリックします。
   攻撃チェーンを正しくクローズしたことを確認するメッセージが右下に表示されます。

> [攻撃チェーン(Attack Chains)] ページで [クローズ済み(Closed)] に切り替えると、クローズした攻撃チェーンのみが表示されます。攻撃チェーンが自動的にクローズまたはマージされた場合は、表示されません。

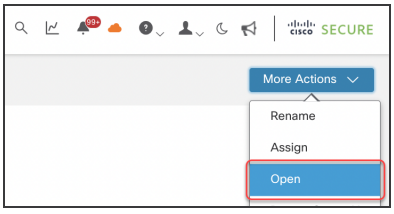
攻撃チェーンを開く

自動的にクローズされた攻撃チェーンではなく、ユーザーがクローズした攻撃チェーンのみを開くことができます。

> 攻撃チェーンを開いても、攻撃チェーン内のアラートのステータスには影響しません。アラートのステータスを変更するには、[アラート(Alerts)] ページに移動します。

攻撃チェーンを開くには、次の手順を実行します。

1. [モニター(Monitor)] > [攻撃チェーン(Attack Chains)] の順に選択して、[攻撃チェーン(Attack Chains)] ページにアクセスします。
2. [攻撃チェーン(Attack Chains)] ページで、[攻撃チェーン ID(Attack Chain ID)] を選択して、特定の攻撃チェーンの詳細ページを表示します。
3. [その他のアクション(More Actions)] > [開く(Open)] の順に選択します。



[攻撃チェーンを開く(Open Attack Chain)] ダイアログボックスが表示されます。

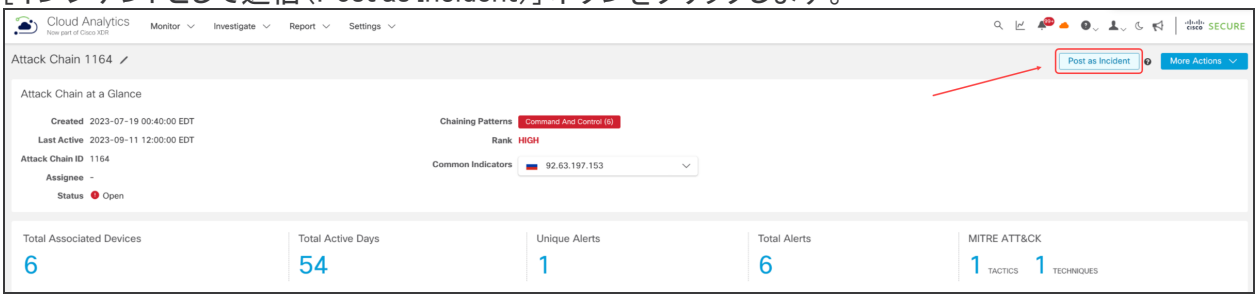
4. 攻撃チェーンを開く場合は、[送信(Submit)]をクリックします。

インシデントとしての攻撃チェーンの送信

高にランク付けされた攻撃チェーンは、Cisco XDR または SecureX に自動的に送信されます(Cisco XDR または SecureX がインストール済みの場合)。

低または中ランクの攻撃チェーンを Cisco XDR または SecureX に送信するには、次の手順を実行します。

1. [モニター(Monitor)]>[攻撃チェーン(Attack Chains)]の順に選択して、[攻撃チェーン(Attack Chains)]ページにアクセスします。
2. [攻撃チェーン(Attack Chains)]ページで、[攻撃チェーン ID(Attack Chain ID)]を選択して、特定の攻撃チェーンの詳細ページを表示します。
3. [インシデントとして送信(Post as Incident)]ボタンをクリックします。



4. Cisco XDR または SecureX に移動して、攻撃チェーンが正常に送信されたことを確認します。

> Cisco XDR または SecureX がインストールされていない場合、[インシデントとして送信(Post as Incident)]ボタンはグレー表示され、使用できなくなります。

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

リビジョン	改訂日	説明
1.0	2023 年 7 月 31 日	初版
1.1	2023 年 9 月 26 日	Cisco XDR に関連するコンテンツを更新。

著作権情報