FMC相関ポリシーの許可リストイベントでは、ネットワーク検出ポリシーを有効にする必要があります

内容

問題

Cisco Secure Firewall Management Center(FMC)で許可リストを使用して相関ポリシーを設定する場合、Network Discovery PolicyがTarget Network IPに設定されていないと、Allow List EventsとAllow List Violationsが生成されないことに注意してください。この設定を行わないと、Analysis > Correlation > Allow List EventsおよびAnalysis > Correlation > Allow List Violationsの下にイベントが表示されません。

ラボテスト中に、次の動作が観察されました。

- 設定されたターゲットネットワークに対して、相関イベントが正しく生成されます。
- Allow List EventsまたはAllow List Violationsは、ターゲットネットワークホストが非準拠になったときに生成されません。

環境

- Secure Firewall Management Center(FMC)で管理されるCisco Firepower Threat Defense(FTD)
- 特定のIPアドレスを対象とした許可リストを使用して設定された相関ポリシー
- 特定のWebアプリケーション、アプリケーション、またはプロトコルを許可するように構成された許可一覧

解決方法

広範なラボテストを実施し、開発チームと協議した結果、Allow List EventsおよびAllow List Violationsを生成するための前提条件として、Network Discoveryポリシーを有効にする必要があることが確認されました。

この問題を解決するには、次の手順を実行します。

手順1：ネットワーク検出ポリシーの有効化

FMCインターフェイスでPolicies > Network Discoveryの順に移動し、ルールが存在しない場合は作成します。

手順2：ネットワーク検出ルールの設定

適切な送信元ネットワーク設定を使用してネットワーク検出ルールを設定します。

- 内部ネットワーク範囲として送信元ネットワークを指定します。
- また、すべてのトラフィックの送信元をモニタする場合は、すべてのネットワーク(0.0.0.0/0)を使用します。
- Allow List Eventsの生成元となるネットワークが、ルールの対象になっていることを確認してください。

手順3：相関ポリシールールのアクティブ化

相関ポリシールールがアクティブであり、無効状態ではないことを確認します。

ステップ4：許可リストのイベント生成の確認

ネットワーク検出を有効にし、相関ポリシールールをアクティブにした後、次の手順を実行します。

1. – ブラウザを使用して、設定済みのターゲットネットワークからWebサイトにアクセスします（ホストを非準拠にします）。

2.- Analysis > Correlation > Allow List EventsおよびAnalysis > Correlation > Allow List Violationsの順に選択して、イベントを生成します。

3. – ホストが非準拠になるときにイベントが読み込まれることを確認します。

ラボテストでは、ネットワーク検出が有効になると、非準拠のホストに対してAllow List EventsおよびAllow List Violationsが正常に生成されることが確認されました。

原因

根本原因は、FMC相関ポリシーでAllow List Eventsを生成するために、ネットワーク検出ポリシーが必須の前提条件であることです。アクティブなネットワーク検出ポリシーがないと、システムは設定されているAllow Listに対してホストのコンプライアンスを正しく評価できず、ターゲットネットワークホストがコンプライアンス違反になってもAllow Listイベントは生成されません。

関連コンテンツ

- Cisco FMC相関コンプライアンスリストのドキュメント
- シスコのテクニカルサポートとダウンロード

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。