

セキュアアクセスアクティビティ検索で不明なルール名が表示される

内容

問題

UmbrellaからSSEへの移行の際に、Secure Access Activity Searchイベントでは、名前付きポリシールールが表示される代わりに、ルール名がUNKNOWNと表示されます。この動作は、chatgpt.comへの要求など、許可されたトラフィックを含む、さまざまなトラフィックタイプで観察されました。問題は、これらの未知のルール名のエントリが、修復を必要とするポリシー設定の問題または移行の問題を示しているかどうかでした。

環境

- シスコセキュアアクセス(SSE)
- UmbrellaからSSEへの移行を進めている組織
- Secure Accessアクティビティ検索レポート
- 新たに検出されたドメインとして分類されたトラフィック

解決方法

Rule Name UNKNOWNの動作は、お客様が作成/名前付きルールではなく、Secure Accessシステムロジックによって処理されるイベントに対しては予期されており、正常なものです。これは通常、新たに検出されたドメインに分類されたトラフィックに対して発生します。この場合、ドメインはクエリー時に新たに検出され、アクティビティ検索レポートまたはセキュリティアクティビティレポートにレポートされます。

不明なルール名を使用したアクティビティ検索イベントの解釈

ルール名がUNKNOWNのイベントが発生した場合は、次のイベントフィールドを確認して適用理由を判別し、適切なポリシーが適用されていることを確認します。

- Action : トラフィックが許可されたか、ブロックされたかを表示します
- イベントブロックの理由/ブロックの理由 : 特定の強制の詳細を提供します
- Categories : コンテンツの分類 (新しく認識されたドメインなど) を表示します。
- Destination domain/IP : 要求のターゲット
- ユーザ/送信元ID : トラフィックの送信元
- Timestamp : イベントの発生時刻

Categories フィールドにNewly Seen Domainsと表示される場合、rule-nameフィールドのUNKNOWNは予期される動作であり、移行の失敗やポリシーの破損を示すものではありません。

予期しない動作の検証手順

トラフィックが特定の名前付きルールに一致することが予期されていたが、UNKNOWNが表示される場合は、ポリシーパス検証のために次の情報を収集します。

- 2 ~ 3サンプルイベントタイムスタンプ
- 各イベントの宛先ドメイン/IP
- 各イベントのユーザー/ソースID

この情報を使用して、予想されるポリシーパスを実際のイベント動作と比較し、さらなる調査が必要かどうかを判断できます。

原因

UNKNOWNルール名は、Secure Accessシステムロジックが、お客様が作成/名前付きポリシール

ールを適用するのではなく、トラフィックを処理するときに表示されます。この動作は、特定のトラフィックカテゴリ、特に新たに検出されたドメインに対して文書化されており、初期ドメイン評価時には、名前付きルールよりも組み込みの分類および処理メカニズムが優先されます。

関連コンテンツ

- [新しく検出されたドメインのセキュリティを有効にする](#)
- [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。