セキュアアクセスWebhook統合のためのIP範囲およびファイアウォールの設定

お問い合わせ内容

サードパーティの統合はCisco Secure Access(SSE)ダッシュボードに正常にロードされますが、SIEM統合用のオンプレミスHTTPコネクタでWebフックベースのセキュリティイベントが受信されません。ファイアウォールルールを適切に設定し、Webフックイベント配信を有効にするには、Cisco SSE送信元のIP範囲（地域固有のIPを含む）を明確にする必要があります。

環境

- 製品：Cisco Secure Access(SSE)
- テクノロジー：ソリューションサポート – セキュアアクセスのレポートとロギング
- 統合タイプ：Webhookベースのサードパーティ統合
- ターゲットコネクタ：オンプレミスのHTTPコネクタサーバー

解決策

Cisco Secure Access統合を使用してWebフック配信の問題を解決するには、指定したSSE送信元IP範囲からオンプレミスコネクタへのインバウンドHTTPSトラフィックを許可するようにファイアウォールルールを設定します。

Cisco SSE送信元のIP範囲

次のCisco SSE送信元IP範囲からの着信HTTPS接続を許可するようにファイアウォールを設定します。

```
146.112.161.0/24
146.112.163.0/24
146.112.165.0/24
146.112.167.0/24
```

ファイアウォールの設定手順

ステップ1：サードパーティの統合ステータスの確認

SSEダッシュボードでAdmin > Third Party Integrationsに移動し、統合が組織に対して正しくロードされていることを確認します。

ステップ2：ファイアウォールルールの設定

SSE送信元IP範囲からオンプレミスのコネクタサーバーへのインバウンドHTTPSトラフィック（ポート443）を許可するためのファイアウォール規則を作成します。インターネットとコネクタサーバー間のネットワークファイアウォールと介在するファイアウォールの両方に規則が適用されていることを確認してください。

ステップ3:Webhookイベント配信の検証

ファイアウォールの変更を実装した後、オンプレミスのHTTPコネクタを監視して、Cisco SSEからWebhookイベントを受信していることを確認します。

地域IP情報

Cisco SSEは、EUおよび米国の地域の共有IP範囲のみを使用します。指定されたIP範囲は、両方の地域展開に対応しており、組織がどのプライマリリージョンに属しているかにかかわらず設定する必要があります。

原因

Cisco Secure AccessからのWebhookイベントは、SSE送信元IPアドレスからオンプレミスのHTTPコネクタサーバへのインバウンドHTTPS接続を許可しないファイアウォール規則によってブロックされます。SSEダッシュボードでは統合ロードが正常に行われていることが示されますが、実際のWebフック配信では、シスコのインフラストラクチャからのトラフィックがユーザコ

ネクタエンドポイントに到達できるように、特定のファイアウォール設定が必要です。

関連コンテンツ

- Cisco Secure Access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。