syslog を使用したクラウドへのイベントの送信

syslog 経由での統合について

リリース 6.3 以降では、syslog を使用してサポート対象のイベントをデバイスから Cisco Cloud へ直接送信できます。オンプレミス Cisco Security Services Proxy（CSSP）サーバーをセットアップし、このプロキシに syslog メッセージを送信するようにデバイスを設定する必要があります。

プロキシは収集したイベントを 10 分ごとに Security Services Exchange（SSE）へ転送します。そこから、SecureXに表示されるインシデントに自動または手動で昇格させることができます。

syslog を使用した統合の要件

要件のタイプ	要件
デバイス	サポートされているバージョンのソフトウェアを実行しているデバイス
バージョン	6.3 以降
使用予定の SecureX クラウドのアカウント	「SecureX アクセスに必要なアカウント」を参照してください。

要件のタイプ	要件
ライセンシング	この統合には特別なライセンスは必要ありません。だだし、これらのオプションの内容に注意してください。 • SecureX に送信するイベントを生成するには、お使いのシステムにライセンスが必要です。 詳細については、「ライセンス情報」を参照してください。 • この統合は評価ライセンスではサポートされていません。 • この環境は、エアギャップ環境に導入できません。
全般	システムが予期したとおりにイベントを生成しています。

syslog を使用した Cisco Cloud へのイベントの送信方法

（注） デバイスがすでにクラウドにイベントを送信している場合は、イベントの再送信を設定する必要はありません。SecureX および Cisco SecureX Threat Response （以前の Cisco Threat Response）は、同じイベントデータのセットを使用します。

	操作手順	詳細情報
ステップ	クラウドに送信するイベント、イベントの送信方法、使用する地域クラウドを決定する。	Secure Firewall Management Center と SecureX の統合についてのトピックを参照してください。
ステップ	要件を満たす。	syslog を使用した統合の要件 （1 ページ）を参照してください。
ステップ	デバイスを管理し、イベントをフィルタ処理するために使用する SecureX のポータルである Security Services Exchange（SSE）にアクセスする。	「Security Services Exchange へのアクセス」を参照してください。
ステップ	Cisco Security Services Proxy （CSSP）サーバーをインストールして構成する。	無料のインストーラと手順を Security Services Exchange からダウンロードします。 Security Services Exchange で、ブラウザウィンドウの右上の近くにある [Tools] アイコンから [Downloads] を選択します。

	操作手順	詳細情報
ステップ	Security Services Exchange で、機能を有効にする。	[Cloud Services] をクリックして次のオプションを有効にします。 • **Cisco SecureX Threat Response** • **Eventing**
ステップ	サポートされているイベントの syslog メッセージをプロキシサーバーに送信するようにデバイスを設定する。	「外部ツールを使用したイベント分析」の章に記載されている syslog の詳細については、Management Center のオンラインヘルプを参照してください。
ステップ	ご使用の製品で、各イベントを生成したデバイスをメッセージが識別していることを確認する。	Management Center の [Platform Settings] にある [Syslog settings] タブで [Enable Syslog Device ID] を選択し、識別子を指定します。
ステップ	システムがサポート対象イベントを生成する時間を確保する。	--
ステップ	イベントが予期したとおりに Security Services Exchange に表示されていることを確認し、必要に応じてトラブルシューティングを行う。	次を参照してください。 • イベントが Security Services Exchange に到達（syslog 経由）しているかの確認 （4 ページ）。 • syslog 統合のトラブルシューティング （5 ページ）。
ステップ	Security Services Exchange で、重要なイベントを自動的に昇格するようにシステムを設定します。	**重要** イベントの昇格を自動化しない場合は、SecureX で表示するために手動でイベントを確認して昇格させる必要があります。 イベントの昇格については、Security Services Exchange のオンラインヘルプの情報を参照してください。 SSE にアクセスするには、「Security Services Exchange へのアクセス」を参照してください。
ステップ	（任意）Security Services Exchange で、重要ではない特定イベントの自動削除を設定します。	イベントのフィルタリングの詳細については、Security Services Exchange オンラインヘルプを参照してください。 SSE にアクセスするには、「Security Services Exchange へのアクセス」を参照してください。

	操作手順	詳細情報
ステップ	SecureX でモジュールを追加する。	SecureX で、[Integration Modules] > [Integration] に移動して、モジュールを追加します。 このモジュールの詳細については、SecureX でオンラインヘルプを参照してください。

Security Services Exchange へのアクセス

始める前に

ブラウザで、ポップアップのブロッキングを無効にします。

ステップ 1 ブラウザウィンドウで、お客様のSecureX クラウドに移動します。

- 北米クラウド： https://securex.us.security.cisco.com
- ヨーロッパのクラウド： https://securex.eu.security.cisco.com
- アジア クラウド： https://securex.apjc.security.cisco.com

ステップ 2 SecureX、Secure Endpoint、Secure Malware Analytics または Cisco Security アカウントのログイン情報を使用してサインインします。

お客様のアカウントログイン情報は、地域クラウドに固有のものです。

ステップ 3 Security Services Exchange に移動します。

[Dashboard] > **[Applications & Integrations]** > **[Security Services Exchange]** の順に選択し、[Launch] をクリックします。

Security Services Exchange が新しいブラウザ ウィンドウで開きます。

イベントが Security Services Exchange に到達（syslog 経由）しているかの確認

始める前に

イベントが予期していたとおりにデバイスに表示されることを確認します。

ステップ 1 メッセージがプロキシから Security Services Exchange に転送できるようになるには、デバイスがサポート対象のイベントを検出してから約 15 分かかります。

ステップ 2 Security Services Exchange にアクセスします。詳細については「Security Services Exchange へのアクセス」を参照してください。

ステップ 3 Security Services Exchange で [イベント（Events）] をクリックします。

ステップ 4 デバイスからイベントを検索します。

予期していたイベントが表示されない場合は、syslog 統合のトラブルシューティング （5 ページ）のヒントを参照し、syslog を使用した Cisco Cloud へのイベントの送信方法 （2 ページ）でもう一度確認してください。

syslog 統合のトラブルシューティング

イベントが CSSP に到達していない

デバイスからネットワーク上の CSSP に到達できることを確認します。

クラウドへのアクセスに関する問題

- この統合の設定を試みる直前にクラウドアカウントをアクティブ化し、この統合の実装中に問題が発生した場合は、1 ～ 2 時間待ってから、クラウドアカウントへのログインを試します。
- アカウントに関連付けられている地域のクラウドの正しい URL にアクセスしていることを確認してください。

予期していたイベントが [Events] リストにない

次の点をチェックします。

- [Events] ページの [Refresh] ボタンをクリックしてリストを更新します。
- 予期していたイベントがデバイスに表示されることを確認します。
- SSE の [Cloud Services] ページの [Eventing] の設定で、自動削除（イベントのフィルタアウト処理）の設定を確認します。
- イベントの送信先の地域クラウドを調べていることを確認します。

syslog のフィールドに関する質問

syslog のフィールドと説明については、「Threat Defense Syslog Messages」[英語] を参照してください。

SecureX タイルから一部のイベントが欠落している

Management Center でグローバルブロックリストや許可リストなどのカスタム セキュリティ インテリジェンス オブジェクトを使用している場合は、それらのオブジェクトを使用して処理さ

れるイベントを自動昇格するようにSSEを設定する必要があります。イベントのインシデントへの昇格については、SSE オンラインヘルプの情報を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。