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 （1 ページ）
- syslog を使用した統合の要件 （2 ページ）
- syslog を使用した Cisco Cloud へのイベントの送信方法 （2 ページ）
- syslog 統合のトラブルシューティング （6 ページ）

syslog 経由での統合について

Firepower リリース 6.3 以降では、サポートされているイベントを Firepower デバイスから Cisco Cloud に syslog を使用して送信できます。オンプレミス Cisco Security Services Proxy（CSSP）サーバをセットアップし、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、Cisco SecureX Threat Response 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
Firepower デバイス	サポートされているバージョンの Firepower ソフトウェアを実行しているデバイス
Firepower のバージョン	6.3 以降
使用予定の Cisco SecureX Threat Response クラウドのアカウント	Cisco SecureX Threat Response のアクセスに必要なアカウント を参照してください。
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。ただし、これらのオプションの内容に注意してください。 • Cisco SecureX Threat Response に送信するイベントを生成するには、Firepower システムにライセンスが必要です。 詳細については、「https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html」を参照してください。 • この統合は Firepower 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	Firepower 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 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	送信するイベント、それらのイベントの送信方法、使用する地域クラウドなどを決定します。	次のトピックを参照してください。 Firepower との統合に関する重要な情報： Cisco SecureX Threat Response

	操作手順	詳細情報
ステップ	要件を満たす。	syslog を使用した統合の要件 （2 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 Cisco SecureX Threat Response のポータルである Security Services Exchange（SSE）にアクセスする。	アクセス Security Services Exchange （5 ページ）を参照してください。
ステップ	Cisco Security Services Proxy（CSSP）サーバをインストールし、設定する。	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。 SSE で、ブラウザ ウィンドウの右上の近くにある [ツール（Tools）] ボタン（🛠）から [ダウンロード（Downloads）] を選択します。
ステップ	Security Services Exchange で、機能を有効にする。	[クラウド サービス（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 Service**
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に送信するように Firepower デバイスを設定する。	• Firepower Device Manager（FDM）によって管理されているデバイスの場合は次の手順を実行します。 「侵入イベントの syslog の設定」の詳細については、FDM オンラインヘルプを参照してください。 • Firepower Management Center（FMC）によって管理されているデバイスの場合は次の手順を実行します。 「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、FMC のオンラインヘルプを参照してください。

	操作手順	詳細情報
ステップ	Firepower 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。	• Firepower Device Manager で次の手順を実行します。 [デバイス（Device）] > [ホスト名（Hostname）] でホスト名を指定します。 • Firepower Management Center で、次の手順を実行します。 [プラットフォーム設定（Platform Settings）] の [syslog 設定（Syslog settings）] タブで [syslog デバイス ID の有効化（Enable Syslog Device ID）] を選択し、識別子を指定します。
ステップ	Firepower 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します。	--
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。	参照先： • イベントが Security Services Exchange に到達（syslog 経由）しているかの確認 （5 ページ） • syslog 統合のトラブルシューティング （6 ページ）
ステップ	重要でない特定のイベントを自動的に削除し、特定のイベントを自動的にインシデントに昇格させて に表示されるようにCisco SecureX Threat Response Security Services Exchange を設定する。	イベントのフィルタ処理と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、アクセス Security Services Exchange （5 ページ）を参照
ステップ	SecureX で、Firepower モジュールを追加します。 このモジュールが設定されている場合、CTR は、侵入イベントがまだ昇格されていない場合でも、SSE内の侵入イベントからの検知物を返します。	SecureX で、[Integration Modules] > [Available Integration Modules] に移動して、Firepower 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。
ステップ	Cisco SecureX Threat Response で、昇格したイベントが予期したとおりに Incident Manager に表示されることを確認します。	Cisco SecureX Threat Response で [インシデント（Incidents）] をクリックします。

アクセス Security Services Exchange

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。

手順

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

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

ステップ 2 SecureX、エンドポイント向け AMP、Cisco Threat Grid、またはシスコのセキュリティ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。

[モジュール（Modules）] > [デバイス（Devices）] > [管理デバイス（Managing Devices）] を選択します。

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

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 Firepower に表示されることを確認します。

手順

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、Firepower デバイスがサポートされているイベントを検出してから 15 分待ちます。

ステップ 2 アクセス Security Services Exchange （5 ページ）。

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 （6 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 イベントリストにない

次の点をチェックします。

- [イベント（Events）] ページの [更新（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 Firepower 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、https://www.cisco.com/c/en/us/support/security/defense-center/products-system-message-guides-list.html にある『Cisco Firepower Threat Defense Syslog Messages』ガイド を参照してください。