プロキシデバイスのアップロード

プロキシデバイスのアップロード

Cisco Secure Web Appliance（旧 Cisco Web セキュリティアプライアンスまたは WSA）や Blue Coat ProxySG などのプロキシデバイスから分析用のグローバル脅威アラートシステムに、ログファイルのテレメトリデータをアップロードします。

ステップ 1 ページ右上隅の歯車アイコンをクリックし、[デバイスアカウント（Device Accounts）] を選択して設定ウィザードを開きます。

（注） すでに既存のデバイスアカウントが 1 つ以上ある場合は、設定を省略して [デバイスアカウント（Device Accounts）] ページが表示されます。

ステップ 2 セットアップウィザードを開始してデバイスアカウントを追加する準備ができたら、[では始めましょう（Let's Get Started）] をクリックします。

ステップ 3 ドロップダウンから自動アップロードまたは手動アップロードのいずれかを選択して、テレメトリデータをデバイスからアップロードする方法を選択します。グローバル脅威アラートシステムは、一度に 1 つのアップロード方法のみをサポートします。組み合わせることはできません。

（注） 自動から手動にアップロード方法を切り替えるには、まず、すべてのプロキシデバイスを自動アップロード設定から削除する必要があります。

ステップ 4 自動アップロード方式を選択した場合は、[SCP] または [HTTPS] のいずれかを選択して、ログファイルの転送に使用するプロトコルを選択します。

a) このデバイスの名前を入力し、[アカウントの追加（Add Account）] をクリックします。

b) SCP を選択した場合：

- Cisco WSA の設定に情報（ホスト、ポート、ディレクトリ、ユーザ名）をコピーします。セキュリティ上の理由により、情報は 1 度しか表示されません。

プロキシデバイスのアップロード

- Cisco WSA の設定方法の詳細については、「Configure Cisco Secure Web Appliance to Upload Log Files to Cisco Global Threat Alerts」を参照してください。
- Cisco WSA 管理コンソールが SSH 公開キーを返したら、この SSH 公開キーをデバイスアカウントにコピーして貼り付けます。
- [終了（Finish）] をクリックします。
- また、[デバイスアカウント（Device Accounts）] ページに移動してデバイスをクリックすると、SSH 公開キーを後で入力できます。

c) HTTPS を選択した場合：

- 情報（ホスト、ポート、パス、ユーザ名、パスワード）をコピーして Blue Coat ProxySG 設定に貼り付けます。
- Blue Coat ProxySG の設定方法の詳細については、「Configure Blue Coat ProxySG to Upload Log Files to Cisco Global Threat Alerts」を参照してください。
- [終了（Finish）] をクリックします。

ステップ 5 手動アップロード方式を選択した場合：

a) ログファイルの形式を検証します。次の準備ガイドラインに従ってください。

- Cisco WSA および Blue Coat プロキシで作成された W3C ログファイルはサポートされています。
- すべてのログファイルは GZip（*.gz）形式で圧縮する必要があります。
- 各ログファイルは 1 GB 未満にする必要があります。1 GB を超えるログファイルは、複数の小さいファイルに分割する必要があります。それぞれの間隔が重複していないこと、すべてのファイルに同一の適切なヘッダーが含まれていることを確認します。
- ログファイルに必要な間隔の合計は 2 日以上です。
- 各ログファイルの間隔は、固有で重複しないようにする必要があります。
- 各ログファイルには、時間の昇順（古いエントリが前、新しいエントリが後）にログエントリを含める必要があります。
- ログファイルはアルファベット順/数字順にソートし、時間に応じた順序でアップロードする必要があります。古いファイルを新しいファイルの前にアップロードする必要があります。1回のアップロードの中では、アップロードコンポーネントが自動的にファイルをソートします。複数回アップロードする場合は、常に以前よりも新しいデータをアップロードしてください。プロキシログファイルでデフォルトで使用される命名規則が保持されている場合、ファイル名はすでに正しくソートされています。
- 前にアップロードしたデータよりも古いデータは処理されません。
- ログファイルの内容は、アップロードに有効な特定の基準に一致する必要があります。
  - シスコは、アップロード前にログファイルを確認するためのログ検証ツールを提供しています。

プロキシデバイスのアップロード

- ログファイルの先頭の 20 行をコピーしてログ検証ツールに貼り付け、エラーをチェックします。
- エラーが表示されたら、ユーザがそのエラーを修正すると同時に、ツールはエラーのチェックを自動的に継続します。

b) [ファイルの追加（Add files）] をクリックしてアップロードするログファイルを選択するか、ログファイルをアップロードボックスにドラッグアンドドロップします。

（注） [ファイルの削除（Clear files）] をクリックして、アップロードボックスに追加されたすべてのファイルをクリアします。

c) [アップロードを開始（Start upload）] をクリックすると、選択したログファイルが 解析用グローバル脅威アラートシステムにアップロードされます。グローバル脅威アラートシステムに結果が表示されるまでしばらく待ちます。

（注） データをドロップするリスクを最小限に抑えるため、グローバル脅威アラートシステムは 5 時間後にアップロードされたデータの処理を開始します。これにより、処理が開始される前にすべてのアップロードを完了して、すべてが適切な順序で配置されるようにできます。

注意 手動から自動に切り替えると、すべてのアップロードが中止し、アップロードデータの処理が停止されます。アップロードしたデータはすべて廃棄されます。

（注） ページを閉じたり、ページから移動したりすると、現在のファイルアップロードが停止されます。

（注） 最初にすべての手動アップロードを停止するまで、自動アップロードを使用することはできません。すべてのデータが処理される前に切り替えると、移行の際に一部の分析データが消失する場合があります。システムがデータをドロップしないようにするには、最後の手動アップロードから 24 時間後に切り替えを実行します。

次のタスク

[デバイスアカウント（Device Accounts）] ページには、プロキシデバイスとその情報が一覧で表示されます。[ステータス（Status）] 列には、各デバイスのステータスが表示されます。

- New - SCP の設定が未完了で、SSH 公開キーが消失している場合があります
- Provisioning - プロビジョニング中のアカウントの準備がまだできていません
- Ready - アカウントが正常に作成されました
- Error - ステータスにカーソルを合わせると、エラーを説明するポップアップメッセージが表示されます

この概要ページから、別のデバイスアカウントの追加、削除するデバイスの選択、SSH 公開キーの入力、トラブルシューティングを行うことができます。

プロキシデバイスのアップロード

複数のデバイス間またはアップロードプロセス間でアカウントを共有できますが、各デバイスに個別のアカウントを使用し、ファイル名の競合の可能性を最小限に抑え、アップロード問題のトラブルシューティングを簡単にすることを推奨します。

デバイスアカウントの準備が完了したら、クリックして [確認済み（Confirmed）] ページまたは [検出済み（Detected）] ページを表示し、ネットワーク内の疑わしいアクティビティを確認します。

（注） 通常、データは、プロビジョニングの完了後 2 ～ 3 日以内に利用可能になります。

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。