外部ツールを使用したイベントの分析

によるイベントの分析 Cisco Threat Response

Cisco Threat Response を使用して脅威を迅速に検出、調査、対応する Cisco Cloud の統合プラットフォームでは、Firepower を含む複数の製品から集約されたデータを使用してインシデントを分析することができます。

- Cisco Threat Response の一般情報については、次を参照してください。

  https://www.cisco.com/c/en/us/products/security/threat-response.html。

- Firepower と Cisco Threat Response の統合の詳細な手順については、次を参照してください。

- https://cisco.com/go/firepower-ctr-integration-docs にある『*Firepower and Cisco Threat Response Integration Guide*』

Cisco Threat Response でのイベント データの表示

始める前に

- https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html にある『*Firepower and Cisco Threat Response integration Guide* 』の説明に従って、統合をセットアップします。

- Cisco Threat Response のオンライン ヘルプを確認し、脅威の検出、調査、およびアクションを実行する方法を習得します。
- Cisco Threat Response にアクセスするにはクレデンシャルが必要です。

ステップ 1 Firepower Management Center で、次のいずれかを実行します。

- 特定のイベントから Cisco Threat Response にピボットするには、次の手順を実行します。

  a. [分析（Analysis）] > [侵入（Intrusions）] メニューで、サポートされているイベントが表示されているページに移動します。

  b. 送信元または宛先の IP アドレスを右クリックし、[Threat Response に表示（View in Threat Response）] を選択します。

- 通常のイベントの情報を表示するには、次の手順を実行します。

  a. [システム（System）] > [統合（Integrations）] > [クラウド サービス（Cloud Services）] に移動します。

  b. リンクをクリックして Cisco Threat Response にイベントを表示します。

ステップ 2 プロンプトが表示されたら、Cisco Threat Response にサインインします。

Splunk でのイベント分析

Cisco Firepower App for Splunk を使用し、Splunk 上に転送した Firepower イベント データを使用してネットワーク上の脅威をハントおよび調査します。

詳細については、「https://cisco.com/go/firepower-for-splunk」を参照してください。

を使用したイベント調査 Cisco Security Packet Analyzer

組織が Cisco Security Packet Analyzer（Firepower システムとは別個の製品）を展開している場合、Cisco Security Packet Analyzer を使用して Firepower システムが検出するインシデントや不審なイベントのコンテキスト情報を、フル パケット キャプチャの形式で収集できます。

Firepower Management Center のイベントから複数のCisco Security Packet Analyzer インスタンスで即座にクエリを実行し、Cisco Security Packet Analyzer の結果を処理したり、結果をダウンロードしてWireshark（TM）などの他のツールを使用したりしてタイムライン分析を実行することができます。

Cisco Security Packet Analyzer および Firepower Management Center は互いに独立して展開され、Firepower システムは Cisco Security Packet Analyzer の導入を認識しません。キャプチャされたデータはパケット アナライザと管理センター間を移動しません。

パケット アナライザの展開の要件

Cisco Security Packet Analyzer インスタンスを展開する際は次の点に留意してください。

- 最大 500 の Cisco Security Packet Analyzer インスタンスを Firepower Management Center に登録できます。スタック内の各パケット アナライザ インスタンスは個別に登録する必要があります。
- この統合でのサポート対象の Cisco Security Packet Analyzer モデルとバージョンについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html の『*Cisco Firepower Compatibility Guide*』を参照してください。
- 1 つのキャプチャ セッションで同時に複数の目的に対応でき、クエリによって展開の負荷が過大にならない場合を除いて、Firepower システムで使用するパケット アナライザのインスタンスは一般に、この目的専用とする必要があります。
- Cisco Security Packet Analyzer 分析するトラフィックをキャプチャでき、また、パケット アナライザ インスタンスと Firepower 管理対象デバイスが確認するトラフィックが同じである必要があります。
- Firepower Management Center はネットワーク上の各パケット アナライザにアクセスできる必要があります。
- パケット アナライザのインスタンスをセットアップし、この展開の前提条件を満たすには、https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/tsd-products-support-series-home.html の Cisco Security Packet Analyzer のドキュメントとパケット アナライザのオンライン ヘルプを使用します。
- 各パケット アナライザは、Firepower Management Center とその管理対象デバイスとして同じ NTP サーバを使用して時刻を同期させる必要があります。
- 各パケット アナライザで次を満たす必要があります。
  - パケット アナライザへの Web アクセスが有効になっている必要があります。
  - クエリのキャプチャ権限を持つ次のアカウントが必要です。
    - Firepower Management Center がクエリをパケット アナライザに送信するときに使用するユーザ アカウント。
    - 自分と、パケット アナライザにクエリの結果を表示する他の人のユーザ アカウント。

    Web ユーザ パスワードの制限文字については、Cisco Security Packet Analyzer のドキュメントを参照してください。

    ヒント：パケットアナライザでこれらのアカウントのクレデンシャルをテストし、機能することを確認します。
  - パケット アナライザの Web インターフェイスでクエリが正常に実行できる必要があります。

- パケット アナライザのキャプチャ セッションの要件と推奨事項 （4 ページ）で説明したキャプチャ セッションの要件を満たします。

これらのタスクの手順については、パケットアナライザのドキュメントを参照してください。

パケット アナライザのキャプチャ セッションの要件と推奨事項

- 各 Cisco Security Packet Analyzer インスタンスでキャプチャ セッションを作成する必要があります。
- 各パケット アナライザ インスタンスに設定する必要があるキャプチャ セッションは 1 つのみです。
- Firepower Management Center の登録形式のデフォルト キャプチャ セッション名は **`firepower_rolling_capture`** です。わかりやすくするために、別の名前を使用する理由がある場合を除いて、すべてのパケットアナライザインスタンスにこのキャプチャセッション名を使用します。
- 残りの値は次のとおりです。

オプション	値
[パケット スライス サイズ（Packet Slice Size）]	パケット全部をキャプチャする場合は ゼロ（0）
ストレージ タイプ	ファイル
[ディスク使用率（%）（Disk Utilization (%)）]	80
ファイルサイズ（MB）（File Size (MB)）	パケット アナライザ モデルでベスト パフォーマンスを得るための最大サイズ（2000 または 500）
ローテートファイル（Rotate Files）	ローリング キャプチャを有効にする場合に選択
All others	展開で有効な値

- 任意のユーザがクエリを実行する前にキャプチャ セッションを実行する必要があります。セッションを保存した後、[キャプチャ セッション（Capture Sessions）] ページに移動してキャプチャ セッションを選択し、[開始（Start）] ボタンをクリックします。

パケット アナライザ インスタンスの登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Security Analyst

マルチドメイン展開環境では、現在のドメインの Cisco Security Packet Analyzer インスタンスのみを作成、変更、または削除できます。現在のドメインおよび子孫ドメインのパケット アナライザ インスタンスに対してクエリを実行し、クエリの結果を表示できます。1 つのパケット アナライザ インスタンスは複数のドメインに登録できます。

始める前に

- Cisco Security Packet Analyzer の展開は、分析するパケットをキャプチャするようにパケット アナライザの展開の要件 （3 ページ）のガイドラインに従ってインストールし、設定し、適切に動作している必要があります。
- 各パケット アナライザ インスタンスには、パケット アナライザのキャプチャ セッションの要件と推奨事項 （4 ページ）のガイドラインを満たす 1 つのキャプチャ セッションが必要です。
- 登録するパケット アナライザごとに次の情報を収集します。
  - ホスト名または IP アドレス
  - ポート
  - 接続するために Firepower Management Center が使用するユーザ アカウントのクレデンシャル
  - キャプチャ セッション名

ステップ 1 [システム（System）] > [統合（Integration）] を選択します。

ステップ 2 [パケット アナライザ（Packet Analyzers）] タブをクリックします。

ステップ 3 [新規（New）] をクリックします。

ステップ 4 この手順のために前提条件で収集した値をフォームに入力します。

キャプチャ セッションの名前は、パケット アナライザで設定されているキャプチャ セッションの名前と一致する必要があります。

パケット アナライザが CA 署名付き証明書を提供しない場合は、[SSL/TLS 証明書の確認（Verify SSL/TLS certificate）] を無効にします。

ステップ 5 [保存（Save）] をクリックします。

システムはすぐに接続をテストして、キャプチャ セッションを検証します。

ステップ 6 各パケット アナライザ インスタンスに対してこれを繰り返します。

次のタスク

まだ実行していない場合は、各パケット アナライザ インスタンスでキャプチャ セッションを開始します。

クエリ パケット アナライザ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

特定のイベントに基づいて自動的に入力されるパラメータを持つ1つのクエリを使用して最大500 の Cisco Security Packet Analyzer インスタンスに同時にクエリを実行できます。

ヒント 特定のイベントに基づいていないクエリを実行するには、[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）] を選択し、[新しいクエリ（New Query）] をクリックします。

ステップ 1 パケット キャプチャ内に含まれているタイプのデータなどのイベントを表示する Firepower Management Center の次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューのメニュー オプション）

ステップ 2 イベントを右クリックし、[クエリ パケット アナライザ（Query Packet Analyzer）] を選択します。

使用可能なイベント データがクエリ フォームに事前に入力されます。

イベントまたはダッシュボード ページの時間枠でクエリのデフォルトの開始時刻と終了時刻が決まります。

ステップ 3 調査するチケットの数など、このクエリの名前を入力します。

ステップ 4 必要に応じてクエリ パラメータを編集します。

たとえば、30 秒ごとか、または数分ごとに時間枠を拡大してイベントに関してより多くのパケットをキャプチャします。

開始時刻と終了時刻の両方がないクエリの場合は、完了するまで時間がかかります。

アスタリスクの付いたフィールドには値が必要です。

[PCAP の分割（Split Pcaps At）] の値を大きくした場合は、選択したすべてのパケット アナライザ インスタンスと、クエリ結果を処理するその他のツールで入力するファイル サイズがサポートされていることを確認します。このオプションは、パケット アナライザ自体のクエリ ダイアログの [PCAP ファイルの最大サイズ（Max PCAP File Size）] オプションです。

[プレビューのフィルタ処理（Filter Preview）] のクエリ文字列を編集する場合は注意が必要です。シンタックスは検証されません。

ステップ 5 クエリを実行するパケット アナライザのインスタンスを選択します。

マルチドメイン展開環境では、現在のドメインと子孫のドメインから Cisco Security Packet Analyzer インスタンスを組み込むことができます。

ステップ 6 [クエリ（Query）] をクリックします。

次のタスク

クエリのステータスと結果を確認します。パケット アナライザのクエリ ステータスの表示 （7 ページ）およびパケット アナライザのクエリ結果の表示 （8 ページ）を参照してください。

パケット アナライザのクエリ ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

クエリ ステータス ページの各テーブル行にはすべての Cisco Security Packet Analyzer インスタンスの各クエリのステータスがまとめられており、行を展開することで個々のインスタンスの結果を表示できます。

マルチドメイン展開環境では、現在のドメインと子孫のドメインについてのみ、パケット アナライザのクエリ ステータスと結果を表示を表示できます。

ステップ 1 次のいずれかを実行します。

- ウィンドウ上部にあるメニュー バーの [メッセージ センター（Message Center）] アイコンをクリックし、次に [タスク（Tasks）] タブをクリックします。[クエリ パケット アナライザ（Query Packet Analyzers）] のタスクを検索し、[詳細の表示（View Details）] または [結果の表示（View Results）] をクリックします。
- [分析（Analysis ）] > [詳細（Advanced）] > [パケット アナライザのクエリ （Packet Analyzer Queries）] を選択します。

ステップ 2 クエリのステータスを特定するには、次を確認します。

[ステータス（Status）] 列には、クエリが正常に実行されたパケット アナライザ インスタンスの数と、失敗したインスタンスの数が表示されます。特定のステータスを表示するには、カーソルをアイコンの上に置きます。

[継続時間（Duration）] 列には、クエリが完了または失敗するまでにかかった時間が表示されます。

継続時間は、クエリ、ネットワーク状態などの特異性の影響を受けます。

ステップ 3 次のいずれかを実行します。

- クエリの結果を表示します。パケット アナライザのクエリ結果の表示 （8 ページ）を参照してください。
- どのパケットアナライザインスタンスが失敗したか、クエリの完了までに時間がかかったかを特定するには、キャレット記号をクリックしてクエリの行を展開した後、失敗したインスタンスや通常よりも長い時間を要したインスタンスを探します。
- 問題または予期していなかったステータスのトラブルシューティングを実行します。Packet Analyzer クエリのトラブルシューティング （9 ページ）を参照してください。
- 進行中のクエリをキャンセルするか、または個々のパケットアナライザインスタンスのクエリをキャンセルします。キャンセルすると、パケット アナライザのクエリもキャンセルされます。
- 完了済みまたは失敗したクエリか、または個々のパケットアナライザインスタンスのクエリを削除します。クエリを削除してもパケット アナライザでキャプチャされたデータは削除されません。

ステップ 4 このページの結果を更新するには、ページをリロードします。

パケット アナライザのクエリ結果の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

Cisco Security Packet Analyzer でクエリに一致するパケットの表示および分析したり、または別のツールで表示および分析するパケットをダウンロードすることができます。

マルチドメイン展開環境では、現在のドメインと子孫のドメインについてのみ、パケットアナライザのクエリの結果を表示できます。

始める前に

表示するクエリの結果を保持するパケット アナライザ インスタンスにアクセスできる Cisco Security Packet Analyzer ユーザ アカウントのクレデンシャルがあることを確認します。

ステップ 1 [分析（Analysis ）] > [詳細（Advanced）] > [パケット アナライザのクエリ （Packet Analyzer Queries）] を選択します。

ステップ 2 キャレット記号をクリックし、クエリに対応する行を展開します。

ステップ 3 次のアイコンが表示されている 1 つ以上のパケット アナライザ インスタンスを見つけます。

[該当なし（No results）] は、クエリに一致するそのパケット アナライザ インスタンスのパケットがなかったことを示します。

予想どおりの結果が得られなかった場合は、Packet Analyzer クエリのトラブルシューティング （9 ページ）を参照してください。

ステップ 4 次のいずれかを実行します。

a) キャプチャしたパケットを Cisco Security Packet Analyzer で表示して処理するには、[Open link] アイコン（） をクリックします。

b) PCAP ファイルをダウンロードし、サードパーティ製のパケット分析ツールに表示するには、[Download] アイコン（） をクリックします。

パケット アナライザ インスタンスによって別の Web ブラウザ ウィンドウが開かれ、クレデンシャルが要求されます。

ステップ 5 パケット アナライザにサインインします。

ステップ 6 Firepower Management Center に戻り、ダウンロード アイコンかリンクを開くためのアイコンをもう一度クリックします。

ステップ 7 キャプチャされたパケットを希望のアプリケーションまたはツールで処理します。たとえば、Cisco Security Packet Analyzer では、キャプチャされたパケットを復号してから、秘密キーの復号化やファイルの抽出などのタスクを実行して何が転送されたかを確認します。

Packet Analyzer クエリのトラブルシューティング

クエリの結果が出ない

考えられる原因と解決策：

- キャプチャ セッションは、Packet Analyzer では実行されません。これが問題の原因である場合は、クエリを実行しているイベントのデータはありません。将来のイベントのパケット収集を有効にするには、パケット アナライザでキャプチャ セッションを開始します。
- クエリの時間枠がキャプチャされたファイルの時間枠から外れているか、キャプチャ セッションが上書きされています。
- Packet Analyzer が正しいパケットをキャプチャしていません。
- 関連データを含むキャプチャ セッション ファイルがバッファに書き込まれ続けています。ファイルへの書き込みが完了するまで、セッションに対するクエリを実行できません。数分間待ってからもう一度試してください。
- https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/products-user-guide-list.html の *Cisco Security Packet Analyzer*ユーザ ガイド のトラブルシューティングの情報を参照してください。

クエリに時間がかかりすぎる

- 各 Packet Analyzer で一度に 1 つのみのクエリを実行できます。特定のクエリに先立ってキューイングされた複数のクエリが存在する場合、クエリの完了までに長い時間がかかります。複数のクエリ送信元がある場合でも、存在するのは単一のキューです。
- 開始時刻と終了時刻を両方とも指定していないクエリの場合、プロセスの時間は大幅に長くなります。
- 開始時刻から終了時刻までの期間が長くなるほど、システムで検索を完了するのにかかる時間も長くなります。

Web ベースのリソースを使用したイベントの調査

Firepower Management Center 外部の Web ベースのリソースにおける潜在的な脅威についての情報をすばやく検索するには、contextual cross-launch 機能を使用します。例：

- Cisco または既知の疑わしい脅威に関する情報を公開するサードパーティ製クラウドホステッド サービスの疑わしい送信元 IP アドレスを検索する、または
- 組織の履歴ログで特定の脅威に関する過去のインスタンスを検索する（組織がセキュリティ情報とイベント管理（SIEM）アプリケーションでそのデータを格納している場合）。
- 組織で Cisco AMP for Endpoints を導入している場合は、ファイル トラジェクトリ情報などの特定のファイルに関する情報を検索します。

イベントを調査する際は、Firepower Management Center のイベント ビューアまたはダッシュボードのイベントから直接、外部リソースの関連情報をクリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットを表示し、記載されている送信元 IP アドレスのいずれかに関する詳細情報を検索すると仮定します。この IP アドレスに関して、Talos がどのような情報を公開しているか確認したいので、「Talos IP」リソースを選択します。Talos Web サイトが開き、この特定の IP アドレスに関する情報が書かれたページが表示されます。

一般的に使用されているシスコやサードパーティ製の脅威インテリジェンス サービスへの一連の事前定義されたリンクから選択し、その他の Web ベースのインターフェイスおよび Web インターフェイスを持つ SIEM または他の製品へのカスタム リンクを追加できます。一部のリソースでは、アカウントまたは製品の購入が必要になる場合があります。

コンテキスト クロス起動のリソースの管理について

[分析（Analysis）]>[詳細（Advanced）]>[コンテキスト クロス起動（Contextual Cross-Launch）] ページを使用して外部の Web ベースのリソースを管理します。

シスコが提供している事前定義のリソースにはシスコのロゴが付いています。残りのリンクはサードパーティのリソースです。

必要がないリソースは無効にするか、または削除できます。あるいは、たとえば名前の前に小文字の「z」を追加するなどして名前を変更し、そのリソースをリストの下部に分類することができます。削除されたリソースは、元に戻すことはできませんが、再作成できます。

リソースを追加するには、コンテキスト クロス起動のリソースの追加 （11 ページ）を参照してください。

カスタム コンテキスト クロス起動のリソースの要件

カスタム contextual cross-launch リソースを追加する場合は、次の点に留意します。

- リソースは Web ブラウザを介してアクセスできる必要があります。
- http プロトコルと https プロトコルのみがサポートされています。
- GET 要求のみがサポートされています。POST 要求はサポートされていません。
- URL の変数のエンコーディングはサポートされていません。IPv6 アドレスをエンコードするにはコロンで区切る必要がある場合がありますが、ほとんどのサービスでこのエンコーディングは必要ありません。
- 事前に定義されたリソースを含めて、最大 100 のリソースを設定できます。

コンテキスト クロス起動のリソースの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin/Security Analyst

脅威インテリジェンス サービスやセキュリティ情報とイベント管理（SIEM）の ツールなどの contextual cross-launch リソースを追加できです。

マルチドメイン展開環境では、親ドメインのリソースを表示および使用できますが、現在のドメインで実行できるのはリソースの作成と編集のみです。すべてのドメインのリソースの合計数は 100 に制限されています。

始める前に

- カスタム コンテキスト クロス起動のリソースの要件 （11 ページ）を参照してください。
- リソースに必要な場合は、アクセスに必要なアカウントとクレデンシャルにリンクするか、作成するか、または取得します。必要に応じて、アクセスが必要な各ユーザにクレデンシャルを割り当てて配布します。
- リンク先のリソースのクエリ リンクのシンタックスを特定します。

ブラウザ経由でリソースにアクセスし、必要に応じてそのリソースのドキュメントを使用して、たとえばIPアドレスなど、検索するクエリ リンクの特定のタイプの情報の検索に必要なクエリ リンクを作成します。

クエリを実行して、結果のURLをブラウザのロケーション バーからコピーします。

たとえば、クエリURL **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`** が表示される場合があります。

ステップ1 [分析（Analysis）] > [詳細（Advanced）] > [コンテキストクロス起動（Contextual Cross-Launch）] を選択します。

ステップ2 [新しいクロス起動（New Cross-Launch）] をクリックします。

表示されたフォームのアスタリスクの付いたすべてのフィールドに値が必要です。

ステップ3 一意のリソース名を入力します。

ステップ4 作業中のURLの文字列をリソースから[URLテンプレート（URL Template）]フィールドに貼り付けます。

ステップ5 クエリ文字列内の特定のデータ（IPアドレスなど）を適切な変数で置き換えます。変数を挿入するには、カーソルを置いて変数ボタン（[ip] など）を1回クリックします。

上記の「開始する前に」の項の例では、URLは **`https://www.talosintelligence.com/reputation_center/lookup?search= {ip}`** になります。contextual cross-launchリンクを使用すると、URL内の{ip}変数は、イベント ビューアまたはダッシュボードでユーザが右クリックするIPアドレスに置き換わります。

各変数の説明については、変数ボタンの上にカーソルを置きます。

1つのツールまたはサービスに複数のcontextual cross-launchリンクを作成するには、それぞれに異なる変数を使用します。

ステップ6 [データ例を使用したテスト（Test with example data）] アイコン（）をクリックしてデータ例を使用してリンクをテストします。

ステップ7 問題を修正します。

ステップ8 **[保存（Save）]** をクリックします。

コンテキスト クロス起動を使用したイベントの調査

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	[管理者（Admin）]/[セキュリティ アナリスト（Security Analyst）]/[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read-only)）]

始める前に

アクセスするリソースにクレデンシャルが必要な場合は、それらのクレデンシャルがあることを確認します。

ステップ 1 Firepower Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベント ビューア ページ（イベントのテーブルが含まれている [分析（Analysis）] メニューのメニュー オプション）

ステップ 2 対象のイベントを右クリックして、使用する contextual cross-launch のリソースを選択します。

必要に応じて、コンテキスト メニューを下にスクロールして使用可能なすべてのオプションを確認します。

右クリックしたデータ タイプによって表示されるオプションが異なります。たとえば、IP アドレスを右クリックした場合は、IP アドレスに関連する contextual cross-launch のオプションのみが表示されます。

そのため、たとえば、[上位攻撃者（Top Attackers）] ダッシュボード ウィジェットに送信元 IP アドレスに関して Cisco Talos からの脅威情報を表示させるには、[Talos SrcIP] または [Talos IP] を選択します。

リソースに複数の変数が含まれている場合、そのリソースを選択するオプションは、含まれている各変数に可能な 1 つの値を持つイベントにのみ使用できます。

別のブラウザ ウィンドウに contextual cross-launch のリソースが開きます。

クエリを実行するデータの量、リソースの速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 必要に応じて、リソースにサインインします。

セキュリティ イベントの syslog メッセージの送信について

接続、セキュリティ インテリジェンス、侵入、およびファイルとマルウェアのイベントに関連するデータは、syslog を介してセキュリティ情報およびイベント管理（SIEM）ツールまたは、外部のイベント ストレージおよび管理ソリューションに送信できます。

これらのイベントを Snort® イベントと呼ぶこともあります。

syslog にセキュリティ イベントのデータを送信するためのシステムの設定について

セキュリティ イベントを syslog に送信するようにシステムを設定するには、次を知っておく必要があります。

- セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス （14 ページ）
- セキュリティ イベントの syslog の設定場所 （15 ページ）
- セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定
- ポリシーで syslog の設定を変更した場合、それらの変更を有効にするには展開する必要があります。

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティス

デバイスとバージョン	設定の場所
Firepower Threat Defense バージョン 6.3 以降	1. FTD プラットフォーム設定（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [脅威に対する防御設定（Threat Defense Settings）] > [Syslog]）を設定します。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定も参照してください。 2. アクセス コントロール ポリシーの [ロギング（Logging）] タブで、FTD プラットフォーム設定の使用を選択します。 3. （侵入イベントの場合）アクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用するように侵入ポリシーを設定します。（これはデフォルトです）。 これらの設定の上書きは推奨していません。

デバイスとバージョン	設定の場所
その他のすべてのデバイス	1. アラート応答を作成します。 2. アラート応答を使用するには、アクセス コントロール ポリシーの [ロギング（Logging）] タブを設定します。 3. （侵入イベントの場合）侵入ポリシーで syslog 設定を構成します。

セキュリティ イベントの syslog の設定場所

接続およびセキュリティ インテリジェンス イベント の syslog の設定場所（すべてのデバイス）

多くの場所でロギング設定を実行できます。次の表を使用して、必要なオプションが設定されていることを確認します。

重要

- syslog の設定を行う場合、特に他の設定から継承したデフォルトを使用する際には細心の注意が必要です。下の表に示すように、オプションの中にはすべての管理対象デバイス モデルやソフトウェア バージョンに使用できないものもあります。
- 接続ロギングを設定する際の重要な情報については、接続ロギングの章を参照してください。

設定の場所	説明と詳細情報
[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	このオプションは、バージョン 6.3 以降を実行している Firepower Threat Defense のデバイスにのみ適用されます。 ここで行う設定は、アクセス コントロール ポリシーのロギング設定に指定でき、この表の残りのポリシーとルールに使用するか、それらをオーバーライドできます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定とSyslog についておよびサブトピックを参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	ここで行う設定は、この表の残りの行で指定する場所の子孫のポリシーおよびルールにあるデフォルトをオーバーライドしない限り、すべての接続イベントとセキュリティ インテリジェンス イベントの syslog のデフォルト設定になります。 6.3 以降を実行している FTD デバイスの推奨設定：FTD プラットフォーム設定を使用します。詳細については、セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定とSyslog についておよびサブトピックを参照してください。 その他のすべてのデバイスに必要な設定：syslog アラートを使用します。 syslog アラートを指定する場合は、Syslog アラート応答の作成を参照してください。 [ロギング（Logging）]タブの設定に関する詳細については、アクセス コントロール ポリシーのロギング設定を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>[ルール（Rules）] タブ、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）]ボタン（  ））	ロギングのアクセス コントロール ポリシーに関連付けられているデフォルト アクションを設定します。 アクセス コントロール ルール章とポリシーのデフォルト アクションによる接続のロギングのロギングに関する情報を参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ルール（Rules）] タブ、<各ルール>、[ロギング（Logging）] タブ	特定のルールの設定をアクセス制御ポリシーにログインします。 アクセス コントロール ルール章のロギングに関する情報を参照してください。

設定の場所	説明と詳細情報
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[セキュリティ インテリジェンス（Security Intelligence）] タブ、[ロギング オプション（Logging Options）] ボタン（  ）	セキュリティ インテリジェンス ブラックリストのロギング設定 次のボタンをクリックして設定します。 • [DNS ブラックリスト ロギング オプション（DNS Blacklist Logging Options）] • [URL ブラックリスト ロギング オプション（URL Blacklist Logging Options）] • [ネットワーク ブラックリスト ロギング オプション（Network Blacklist Logging Options）]（ブロックされたリスト上の IP アドレス用） 前提条件を含めてセキュリティ インテリジェンスの設定とサブトピックおよびリンクを参照してください。
[ポリシー（Policies）]>[SSL]、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）]（  ）ボタン	SSL ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギングを参照してください。
[ポリシー（Policies）]>[SSL]、<各ポリシー>、<各ルール>、[ロギング（Logging）] タブ	SSL ルールのロギング設定。 TLS/SSL ルールのコンポーネントを参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、[デフォルト アクション（Default Action）] 行、[ロギング（Logging）]（  ）ボタン	プレフィルタ ポリシーに関連付けられているデフォルト アクションのロギング設定。 ポリシーのデフォルト アクションによる接続のロギングを参照してください。
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各プレフィルタ>、[ロギング（Logging）] タブ	プレフィルタ ポリシーの各プレフィルタのロギング設定。 トンネルとプレフィルタ ルールのコンポーネントを参照してください
[ポリシー（Policies）]>[プレフィルタ（Prefilter）]、<各ポリシー>、<各トンネル ルール>、[ロギング（Logging）] タブ	プレフィルタ ポリシーの各トンネル ルールのロギング設定。 トンネルとプレフィルタ ルールのコンポーネントを参照してください
FTD クラスタ設定の追加 syslog の設定：	Firepower Threat Defense 用のクラスタリングの章には syslog について複数の言及があります。「syslog」の章を検索してください。

侵入イベントの syslog の設定場所（FTD 6.3 デバイス）

侵入ポリシーの syslog 設定はさまざまな場所で指定でき、必要に応じてアクセス コントロール ポリシーまたは FTD プラットフォーム設定、あるいはその両方から設定を継承できます。

設定の場所	説明と詳細情報
[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	ここで設定した syslog の宛先は、侵入ポリシーのデフォルトとして使用可能なアクセス コントロール ポリシーの [ロギング（Logging）] タブで指定できます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定と Syslog についておよびサブトピックを参照してください。
[ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	侵入ポリシーに他のロギング ホストが指定されていない場合は、侵入イベントの syslog の宛先のデフォルト設定。 アクセス コントロール ポリシーのロギング設定を参照してください。
[ポリシー（Policies）]>[侵入（Intrusion）]、<各ポリシー>、[詳細設定（Advanced Settings）]、[syslog アラート（Syslog Alerting）] を有効化、[編集（Edit）] をクリック	アクセス コントロール ポリシーの [ロギング（Logging）] タブで指定した宛先以外の syslog コレクタを指定するには、侵入イベントの Syslog アラートの設定を参照してください。 [重大度（Severity）] または [ファシリティ（Facility）]、あるいはその両方を侵入ポリシーで設定されているとおりに使用する場合は、ポリシーにロギング ホストを設定する必要があります。アクセス コントロール ポリシーに指定されているロギング ホストを使用する場合は、侵入ポリシーに指定されている重大度とファシリティは使用されません。

侵入イベントの syslog の設定場所（FTD 以外のデバイスと 6.3 よりも前のバージョン）

- （デフォルト）アクセス コントロール ポリシー（アクセス コントロール ポリシーのロギング設定syslog アラートを指定した場合）（Syslog アラート応答の作成を参照）
- または侵入イベントの Syslog アラートの設定を参照してください。

デフォルトでは、侵入ポリシーはアクセス コントロール ポリシーの [ロギング（Logging）] タブの設定を使用します。FTD 6.3 以外のデバイスに適用される設定がない場合は、FTD 6.3 以外のデバイスに syslog は送信されず、警告は表示されません。

ファイルとマルウェア イベントの syslog の設定場所

設定の場所	説明と詳細情報
アクセス コントロール ポリシーで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、[ロギング（Logging）] タブ	これは、ファイルとマルウェアのイベントの syslog を送信するようにシステムを設定するための主要な場所です。 FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成を参照してください。
Firepower Threat Defense プラットフォーム設定で、次の手順を実行します。 [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]、[Threat Defense 設定ポリシー（Threat Defense Settings policy）]、[Syslog]	これらの設定は、サポート対象のバージョンを実行しており、FTD プラットフォームを使用するようにアクセス コントロール ポリシーの [ロギング（Logging）] タブを設定している場合にのみ、Firepower Threat Defense デバイスにのみ適用されます。 セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定とSyslog についておよびサブトピックを参照してください。
アクセス コントロール ルールで次の手順を実行します。 [ポリシー（Policies）]>[アクセス制御（Access Control）]、<各ポリシー>、<各ルール>、[ロギング（Logging）] タブ	FTD プラットフォームの syslog 設定を使用しない場合は、アラート応答も作成する必要があります。Syslog アラート応答の作成を参照してください。

セキュリティイベントの syslog メッセージの分析

FTD 6.3 以降からのセキュリティ イベント メッセージの例（侵入イベント）

```
        1              2          3      4   5    6
Sep 24 13:42:01 192.168.0.81 SFIMS : %FTD-5-430001:SrcIP:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994, DstPort: 445,
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Revision: 2,
Message: "DCE2_EVENT__SMB_INVALID_DSIZE", Classification:
Potentially Bad Traffic, User: No Authentication Required,
Client: NetBIOS-ssn (SMB) client, ApplicationProtocol: NetBIOS-
ssn (SMB), ACPolicy: test, NAPPolicy: Balanced Security and
Connectivity, InlineResult: Blocked
```

表 *1:* セキュリティ イベントの *syslog* メッセージのコンポーネント

サンプル メッセージの項目数	ヘッダー要素	説明
1	タイムスタンプ	syslog メッセージがデバイスから送信された日付と時刻。 • （バージョン 6.3 以降を実行している FTD デバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合か、または [FTD プラットフォーム設定（FTD Platform Settings）] のこの形式を使用するように指定されている場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイム ゾーンを示しています。 • （バージョン 6.3 以降を実行しているその他すべてのデバイスから送信された syslog）アクセス コントロール ポリシーとその子孫の設定を使用して送信した syslog の場合、日付形式は RFC 5424 に指定されている ISO 8601 タイムスタンプ形式（yyyy-MM-ddTHH:mm:ssZ）に定義されている形式になります。この形式では文字 Z は UTC タイム ゾーンを示しています。 • それ以外の場合は UTC タイム ゾーンの月、日、時刻になりますが、タイム ゾーンは表示されません。 [FTD プラットフォーム設定（FTD Platform Settings）] のタイムスタンプの設定を行うには、Syslog 設定を参照してください。
2	メッセージが送信されたデバイスまたはインターフェイス。 ここに表示される値は次のとおりです。 • インターフェイスの IP アドレス • デバイスのホスト名 • カスタム デバイス識別子	（FTD デバイス バージョン 6.3 以降のみから送信された syslog の場合） [FTD プラットフォーム設定（FTD Platform Settings）] を使用して syslog メッセージが送信された場合で、[Syslog デバイス ID の有効化（Enable Syslog Device ID）] オプションが指定されているときは、これはそのオプションの [Syslog 設定（Syslog Settings）] タブに設定されている値になります。 それ以外の場合、この要素はヘッダーには表示されません。 [FTD プラットフォーム設定（FTD Platform Settings）] でこの設定を行うには、Syslog 設定を参照してください。

サンプル メッセージの項目数	ヘッダー要素	説明
3	カスタム値	アラート応答を使用してメッセージが送信された場合、これは、メッセージを送信したアラート応答に設定されている**タグ**値がある場合は、その値になります。（Syslogアラート応答の作成 を参照）。 それ以外の場合、この要素はヘッダーには表示されません。
4	%FTD %NGIPS	メッセージを送信したデバイスのタイプ。 • %FTD は Firepower Threat Defense バージョン 6.3 以降 • %NGIPS はバージョン 6.3 以降を実行しているその他すべてのデバイス • バージョン 6.2.3 以前を実行しているデバイスから送信されたメッセージの場合、この要素は表示されません。
5	Severity	メッセージをトリガーしたポリシーの syslog 設定に指定されている重要度。 重大度の説明については、重大度またはsyslog 重大度レベルを参照してください。
6	イベント タイプ識別子	バージョン 6.3 以降を実行しているデバイスから送信されたメッセージの場合： • 430001：侵入イベント • 430002：接続の開始時に記録された接続イベント • 430003：接続の終了時に記録された接続イベント バージョン 6.4 以降を実行しているデバイスから送信されたメッセージの場合は、次のイベント タイプ ID も使用されます。 • 430004：ファイル イベント • 430005：ファイル マルウェア イベント バージョン 6.2.3 以前を実行しているデバイスから送信されたメッセージの場合、イベント タイプ識別子は表示されません。

サンプル メッセージの項目数	ヘッダー要素	説明
--	ファシリティ	セキュリティ イベントの syslog メッセージのファシリティ（22 ページ）を参照してください。
--	メッセージの残りの部分	コロンで区切られたフィールドと値。 空または不明な値のあるフィールドはメッセージから省略されます。 フィールドの説明については、次を参照してください。 • 接続イベントとセキュリティ インテリジェンス イベントのフィールド。 • 侵入イベント フィールド • ファイルおよびマルウェア イベント フィールド （注） フィールド説明のリストには、syslog フィールドとイベント ビューア（Firepower Management Center の Web インターフェイスの [分析（Analysis）] メニューのメニュー オプション）に表示されるフィールドの両方が含まれています。syslog 経由で使用可能なフィールドはそれを示すラベルが付けられます。 イベント ビューアに表示される一部のフィールドは、syslog 経由では使用できません。また、一部の syslog フィールドはイベント ビューアには含まれていません（ただし、検索を使用すると表示できる場合があります）。また、一部のフィールドは結合されているか、または個別になっています。

セキュリティ イベントの syslog メッセージのファシリティ

一般に、セキュリティ イベントの syslog メッセージではファシリティ値は関連性がありません。ただし、ファシリティが必要な場合は、次の表を使用してください。

Device	接続イベントにファシリティを含める場合	侵入イベントにファシリティを含める場合	syslog メッセージ内の場所
FTD 6.3 以降	[FTD プラットフォーム設定（FTD Platform Settings）] の [EMBLEM] オプションを使用します。 [FTD プラットフォーム設定（FTD Platform Settings）] を使用して syslog メッセージを送信すると、ファシリティは常に、接続イベントに対して [アラート（ALERT）] になります。	[FTD プラットフォーム設定（FTD Platform Settings）] の [EMBLEM] オプションを使用するか、または侵入ポリシーの syslog 設定を使用してロギングを設定します。侵入ポリシーを使用した場合は、侵入ポリシー設定にロギング ホストも指定する必要があります。	ファシリティはメッセージ ヘッダーには表示されませんが、syslog コレクタが RFC 5424、セクション 6.2.1 に基づいて値を派生させることができます。
6.3 より前の FTD	アラート応答を使用します。	侵入ポリシーの高度な設定の syslog 設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	
FTD 以外のデバイス	アラート応答を使用します。	侵入ポリシーの高度な設定の syslog 設定、またはアクセス コントロール ポリシーの [ロギング（Logging）] タブで識別されているアラート応答を使用します。	

詳細については、侵入 syslog アラートの重大度およびSyslog アラート応答の作成を参照してください。

Firepower syslog メッセージのタイプ

Firepower は、次の表で説明するように、複数の syslog データ タイプを送信できます。

syslog データ タイプ	参照先
FMC からの監査ログ	syslog への監査ログのストリーミングおよびシステムの監査の章

syslog データ タイプ	参照先
従来型デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）からの監査ログ	従来型デバイスからの監査ログのストリーミングおよびシステムの監査の章 CLI コマンド： syslog
FTD デバイスからのデバイス ヘルスとネットワーク関連のログ	Syslog について およびサブトピック
FTD デバイスからの接続、セキュリティ インテリジェンスおよび侵入イベント ログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （14 ページ）。
クラッシック デバイスからの接続、セキュリティ インテリジェンスおよび侵入イベント ログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （14 ページ）
ファイルおよびマルウェアのイベントのログ	syslog にセキュリティ イベントのデータを送信するためのシステムの設定について （14 ページ）

セキュリティ イベントの syslog の制限事項

- syslog コレクタにイベントを表示するには最大 15 分かかる場合があります。
- 次のファイルおよびマルウェアのイベントのデータは syslog 経由で使用できません。
  - レトロスペクティブ イベント
  - エンドポイント向け AMP によって生成されたイベント

eStreamer サーバ ストリーミング

Event Streamer（eStreamer）を使用すると、Firepower Management Center または 7000 または 8000 シリーズ デバイスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、『*Firepower System Event Streamer Integration Guide*』を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 *2 : eStreamer* サーバで送信可能なイベント タイプ

イベント タイプ	説明	FMC で使用可能	7000 & 8000 シリーズ デバイスで使用可能
侵入イベント	管理対象デバイスによって生成される侵入イベント	はい	はい
侵入イベント パケット データ	侵入イベントに関連付けられたパケット	はい	はい
侵入イベント追加データ	HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ	はい	はい
検出イベント	ネットワーク検出イベント	はい	いいえ（No）
相関およびホワイトリスト イベント	相関およびホワイトリスト イベント	はい	いいえ（No）
インパクト フラグ アラート	FMC によって生成されたインパクト アラート	はい	いいえ（No）
ユーザ イベント	ユーザ イベント	はい	いいえ（No）
マルウェア イベント	マルウェア イベント	はい	いいえ（No）
ファイル イベント	ファイル イベント	はい	いいえ（No）
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッション トラフィックに関する情報	はい	はい

セキュリティ イベントの syslog と eStreamer の比較

一般に、現在 eStreamer に重大な既存イベントがない組織は、セキュリティ イベント データを外部で管理するのに eStreamer ではなく syslog を使用する必要があります。

Syslog	eStreamer
カスタマイズの必要なし	各リリースの変更に対応するには、大幅なカスタマイズと継続メンテナンスが必要
標準（Standard）	専用

Syslog	eStreamer
syslog 標準規格では、データ損失に対する保護はありません（特に UDP を使用している場合）	データ損失に対する保護
デバイスから直接送信	FMC から送信（処理オーバーヘッドが加わる）
ファイルイベントとマルウェアイベント、接続イベント（セキュリティ インテリジェンス イベントを含む）、および侵入イベントをサポートします。	eStreamer サーバ ストリーミング （24 ページ）に示されているすべてのイベント タイプをサポートします。
一部のイベントデータは、FMC からのみ送信できます。eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ （26 ページ）を参照してください。	デバイスから syslog を介して直接送信することができないデータが含まれます。eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ （26 ページ）を参照してください。

eStreamer 経由でのみ送信され、syslog 経由では送信されないデータ

次のデータは Firepower Management Center からのみ使用可能であるため、デバイスから syslog を介して送信することはできません。

- パケット ログ
- 侵入イベント追加データ イベント

  説明については、eStreamer サーバ ストリーミング （24 ページ）を参照してください。
- 統計情報と集約イベント
- ネットワーク検出イベント
- ユーザ アクティビティとログイン イベント
- 相関イベント
- ホワイトリスト イベント
- マルウェア イベントの場合：
  - レトロスペクティブな判定
  - 関連する SHA に関する情報がすでにデバイスに同期されている場合を除き、脅威の名前と性質
- 次のフィールド：
  - [Impact] および [ImpactFlag] フィールド

説明については、eStreamer サーバ ストリーミング （24 ページ）を参照してください。

- [IOC_Count] フィールド

- ほとんどの raw ID と UUID。

  次に例外を示します。

  - 接続イベントの syslog には次のものがあります。FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI_CategoryID、SSL_PolicyUUID、および SSL_RuleID
  - 侵入イベントの syslog には、IntrusionPolicyUUID、GeneratorID、および SignatureID が含まれます。

- 以下を含むがこれらに限定されない拡張メタデータ：

  - 氏名、部署、電話番号などの LDAP によって提供されるユーザの詳細。

    syslog では、イベントのユーザ名のみが提供されます。

  - SSL 証明書の詳細などの状態ベースの情報の詳細。

    syslog は、証明書のフィンガープリントなどの基本的な情報を提供しますが、cert CN など、証明書のその他の詳細は提供しません。

  - アプリケーション タグやカテゴリなどの詳細なアプリケーション情報。

    syslog はアプリケーション名のみを提供します。

  一部のメタデータ メッセージには、オブジェクトに関する追加情報も含まれています。

- 地理位置情報

eStreamer イベントタイプの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	FMC 7000 & 8000 シリーズ	いずれか（Any）	Admin

eStreamer サーバで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）]チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、『*Firepower System Event Streamer Integration Guide*』を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバ ストリーミング （24 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 **[保存（Save）]** をクリックします。

eStreamer クライアント通信の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	FMC 7000 & 8000 シリーズ	いずれか（Any）	Admin/Discovery Admin

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 **[Save]** をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にあるファイルのダウンロードアイコン（）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。

eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

外部ツールを使用したイベント データの分析の履歴

機能	バージョン	詳細
Cisco Threat Response との統合	6.3（syslog 経由、プロキシ コレクタを使用） 6.4（直接）	Cisco Threat Response の強力な分析ツールを使用し、Firepower 侵入イベント データを他のソースのデータと統合して、ネットワーク上の脅威を統合ビューに表示します。 変更された画面（バージョン 6.4）：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] の新規オプション。 サポートされるプラットフォーム：バージョン 6.3（syslog 経由）または 6.4 を実行している Firepower Threat Defense デバイス

機能	バージョン	詳細
ファイルとマルウェアのイベントの syslog サポート	6.4	完全修飾ファイルおよびマルウェアのイベント データが syslog 経由で管理対象デバイスから送信できるようになりました。 変更された画面：[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] > [ロギング（Logging）] タブ。 サポート対象プラットフォーム：バージョン 6.4 を実行している管理対象のすべてのデバイス
Splunk との統合	すべての 6.x バージョンのサポート	Splunk のユーザは、新しい個別の Splunk アプリケーションである Cisco Firepower App for Splunk を使用してイベントを分析できます。 どの機能を使用できるかは、Firepower のバージョンによって異なります。 Splunk でのイベント分析 （2 ページ）を参照してください。

機能	バージョン	詳細
Cisco Security Packet Analyzer との統合	6.3	導入された機能：Cisco Security Packet Analyzer にイベントに関連するパケットについてすぐにクエリを実行した後、クリックして Cisco Security Packet Analyzer の結果を調べるか、またはダウンロードして別の外部ツールで分析します。 新規画面： **[システム（System）] > [統合（Integration）] > [パケット アナライザ（Packet Analyzer）]** **[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニューのページのイベントテーブルを右クリックしたときの [クエリ パケットアナライザ（Query Packet Analyzer）] のメニュー項目 サポートされるプラットフォーム Firepower Management Center
コンテキスト クロス起動	6.3	導入された機能：イベントを右クリックし、事前に定義されているか、またはカスタム URL ベースの外部リソースの関連情報を検索します。 新規画面：**[分析（Analysis）] > [詳細（Advanced）] > [コンテキスト クロス起動（Contextual Cross-Launch）]** 新規メニュー オプション：[ダッシュボード（Dashboard）] ページおよび [分析（Analysis）] メニュー ページのイベントテーブルを右クリックしたときに表示される複数のオプション サポートされるプラットフォーム Firepower Management Center

機能	バージョン	詳細
接続イベントと侵入イベントの syslog メッセージ	6.3	統合され、簡略化された新しい設定を使用して、完全修飾接続および侵入イベントを外部ストレージおよびツールに syslog 経由で送信する機能。メッセージヘッダーが標準化されてイベント タイプ識別子が組み込まれ、メッセージが小型になりました。これは、不明な値や空の値が含まれたフィールドが省略されるためです。 サポート対象プラットフォーム： • すべての新機能：バージョン 6.3 を実行している FTD デバイス。 • 一部の新機能：バージョン 6.3 を実行している FTD 以外のデバイス。 • 少数の新機能：6.3 よりも前のバージョンを実行しているすべてのデバイス。 詳細については、セキュリティ イベントの syslog メッセージの送信について（14 ページ）のトピックとサブトピックを参照してください。
eStreamer	6.3	eStreamer の内容をホストのアイデンティティ ソースに関する章からこの章に移動し、eStreamer と syslog を比較した概要を追加しました。