統合イベント

次のトピックでは、統合イベントの使用方法について説明します。

統合イベントについて

統合イベントは、複数タイプのファイアウォールイベント（接続、侵入、ファイル、マルウェア、および一部のセキュリティ関連の接続イベント）の単一画面ビューを提供します。相互に関連付けられているイベントはテーブル内で一緒にスタックされ、セキュリティイベントに関する統合ビューと詳細なコンテキストが提供されます。[統合イベント（Unified Events）]テーブルに侵入イベントがある場合、その侵入イベントをクリックすると、関連付けられている接続イベントが強調表示されます。その後、複数のイベントビューアを切り替えることなく、接続イベントを侵入イベントと相関させて、ネットワークの問題をよりよく理解し、トラブルシューティングすることができます。

[統合イベント（Unified Events）]テーブルは、高度なカスタマイズが可能です。カスタムフィルタを作成して適用することにより、イベントビューアに表示される情報を微調整できます。統合イベントビューアには、特定のニーズに頻繁に使用するカスタムフィルタを保存し、保存したフィルタをすばやくロードするオプションもあります。また、列を追加または削除したり、列をピン留めしたり、列をドラッグして並べ替えたりすることで、イベントビューアテー

ブルを調整できます。Also, you can make a tailored event viewer table by adding or removing columns, pin columns, or drag and re-order the columns.

[統合イベント（Unified Events）] テーブルの [ライブビュー（Live View）] オプションを使用すると、ファイアウォールイベントをリアルタイムで表示し、ネットワーク上のアクティビティをモニターすることができます。たとえば、ファイアウォール管理者の場合、ポリシーの変更後にイベントの更新をリアルタイムで表示すると、ポリシーの変更がネットワークに正しく適用されていることを確認するために役立ちます。

統合イベントの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- セキュリティ アナリスト（Security Analyst）

統合イベントビューアでの作業

複数のイベントビューアを切り替えることなく、さまざまなタイプのファイアウォールイベントを 1 つのテーブルで表示および操作できます。

次のことを行うには、このビューを使用します。

- 異なるタイプのイベント間の関係を統合ビューで表示する。
- ポリシー変更の影響をリアルタイムで確認する。

始める前に

このタスクを実行するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 時間範囲（固定またはスライド）を選択します。詳細については、「統合イベントビューアでの時間範囲の設定」を参照してください。

ステップ 3 Secure Network Analytics アプライアンスにリモートでイベントを保存していて、データソースを変更する正当な理由がある場合は、データソースを選択します。「Cisco Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Cisco Secure Firewall Management Center での作業」で重要な情報を参照してください。

ステップ 4 統合イベントビューアが最初に表示するファイアウォールイベントの膨大なリストをフィルタ処理して、ネットワーク内のイベントのより詳細な状況を把握できます。詳細については、「統合イベントビューアのフィルタ」を参照してください。

ステップ 5 その他のオプションの選択：

目的	操作手順
列のカスタマイズ	• 列の追加または削除： 列ピッカー（）をクリックして、列を選択します。一部のフィールドの値は、イベントタイプによって異なります。各フィールドの横に表示される以下のアイコンは、対応するイベントタイプを示します。 • 接続イベント（（）） • セキュリティ関連の接続イベント（） • 侵入イベント（（）） • ファイルイベント（（）） • マルウェアイベント（（）） 列セットフィルタ処理オプションの横にあるイベントアイコンをクリックして、選択したイベントタイプに従ってイベントフィールドのリストをフィルタ処理します。 （注） 多くの列を含めると、パフォーマンスが低下する可能性があります。イベント行を展開してイベントの詳細を表示すると、非表示の列のデータを表示できます。 • 列の順序変更： 列の見出しをドラッグアンドドロップします。 • 列がスクロールしないようにするための、テーブルの左側または右側での列の固定（静止）： 列をテーブルの左まで右側までドラッグします。 または、列の見出しを固定エリアにドラッグアンドドロップします。 列の固定を解除するには、列を固定エリアの外にドラッグします。 • 列のサイズを変更します。 • 列をデフォルトの設定に戻します。 • 列の設定を保存します。詳細については、「統合イベントビューアでの列セットの保存」を参照してください。 データは常に時間順に並べ替えられ、最新のイベントが上に表示されます。

目的	操作手順
関連イベントの特定	行をクリックして、このイベントに関連する他のイベントを強調表示します。 必要に応じて、イベントをフィルタして、十分に少ないイベントのセットを表示します。 （注） 接続のイニシエータは、マルウェアファイルの送信者と同じである必要はありません。[送信元または宛先IP（Source or Destination IP）] フィルタを使用して統合イベントビューアをフィルタ処理することにより、接続イベントに関連付けられているファイルまたはマルウェアイベントを検索します。
イベントの詳細の表示	行の左端にある [>]（展開）アイコンをクリックします。イベントの詳細には、表示するデータがないフィールドは含まれません。 ヒント または、イベント行をダブルクリックして、[イベントの詳細（Event Details）]ペインを表示します。[イベントの詳細（Event Details）]ペインが開いている場合は、テーブル内の任意のイベント行をクリックして、そのイベントの詳細をロードします。
パケットトレーサを使用したイベントのトラブルシューティング	1. パケットトレースを実行する行の横にある省略記号アイコン（ ） をクリックします。 2. [パケットトレーサで開く（Open in Packet Tracer）] を選択して、イベントの送信元アドレスと宛先アドレス、およびプロトコル特性に基づいてパケットトレーサツールでパケットをシミュレーションします。シミュレーションしたパケットをトレースし、トレース結果を使用してセキュリティイベントのトラブルシューティングを行います。パケットトレーサツールの使用方法の詳細については、パケット トレーサの使用を参照してください。
リアルタイムでのイベントの表示	[ライブ表示（Go Live）] をクリックします。詳細については、「統合イベントビューアでのイベントのライブビュー」を参照してください。 イベントのストリームが速すぎる場合は、フィルタ基準を入力します。
外部リソースへの相互起動	テーブルセルの省略記号 （ ） をクリックすると、そのセル値に使用可能なオプションが表示されます（存在する場合）。 詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。

目的	操作手順
複数の統合イベントビューアのタブ/ウィンドウを開く	• 複数のブラウザのタブまたはウィンドウを使用して、統合イベントビューアのさまざまなビューを表示できます。 • 新しいタブまたはウィンドウには、最後に変更されたタブ/ウィンドウの特性があります。 • 開いているタブ/ウィンドウをテンプレートにするには、それに対して小さな変更を加えます。 • システムは、複数のタブのクエリを順番に処理します。 • ビューによっては（複雑なクエリや、着信イベントレートが高い場合のライブビューモードでの表示など）、4 つより多くのタブが同時に開かれていると、パフォーマンスが低下する場合があります。
検索の保存	カスタム検索をお気に入りとして保存し、後ですばやくロードできます。詳細については、「統合イベントビューアでの検索の保存」を参照してください。
クエリ結果のブックマークまたは共有	ブラウザウィンドウでURLをブックマークするか、コピーして貼り付けます。 • スライド時間範囲が使用されている場合、URL では後で異なるイベントが取得されます。 • 列の可視性、サイズ、順序、およびリアルタイムストリーミング設定は、URL にキャプチャされません。

統合イベントビューアでの時間範囲の設定

特定期間のファイアウォールイベントを表示するには、統合イベントビューアで時間範囲を設定します。時間範囲を変更すると、統合イベントビューアが自動的に更新され、変更が反映されます。

選択した時間範囲は、イベントビューアの他のテーブルには適用されません。たとえば、接続イベントを表示するときに選択した時間範囲は統合イベントビューアには適用されず、その逆も同様です。

重要 時間枠が接続イベントの保持期間を超える場合は、**[分析（Analysis）]**>**[接続（Connections）]**>**[セキュリティ関連の接続イベント（Security-Related Connection Events）]** のテーブルでセキュリティ関連の接続イベントを探します。

始める前に

このタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 **[分析（Analysis）]** > **[統合イベント（Unified Events）]** を選択します。

デフォルトでは、統合イベントビューアには、過去 1 時間のイベントが表示されます。

ステップ 2 現在の時間範囲をクリックします。

ステップ 3 次のいずれかを選択します。

- 固定時間範囲のイベントを表示する場合は、[固定時間範囲（Fixed Time Range）] をクリックし、[開始時刻（Start time）] と [終了時刻（End time）] を選択します。

  ヒント [終了時刻（End time）] を現在の時刻に素早く設定するには、[現在（Now）] をクリックします。

- 指定された長さのスライドするデフォルト時間枠を設定する場合は、[スライド時間枠（Sliding Time Range）] をクリックします。

  アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューを更新すると時間枠がスライドして、常に最後の 1 時間内のイベントが表示されます。

ステップ 4 [Apply] をクリックします。

統合イベントビューアでのイベントのライブビュー

イベントビューアを手動で更新しなくてもファイアウォールイベントがリアルタイムで表示されるように統合イベントビューアを設定します。[ライブビュー（Live View）] モードでは、ネットワークでセキュリティイベントが発生すると、イベントログがリアルタイムで表示されるため、問題のトラブルシューティングに役立ちます。

始める前に

このタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 **[分析（Analysis）]** > **[統合イベント（Unified Events）]** を選択します。

デフォルトでは、統合イベントビューアには、過去 1 時間のイベントが表示されます。

ステップ 2 ライブイベント更新を表示するには、[ライブに移行（Go Live）] をクリックします。

新しいイベントは、イベントテーブルの一番上に表示されます。時間範囲セクションには、統合イベントビューアのライブ期間を通知するタイマーが表示されます。

次のタスク

ライブビューモードを終了するには、[ライブ（Live）] をクリックします。

統合イベントビューアのフィルタ

統合イベントビューアには、最初に過去1時間の複数タイプのファイアウォールイベントが表示されます。[統合イベント（Unified Events）] のデフォルトビューをフィルタ処理して、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは、排他フィルタ条件と包含フィルタ条件をサポートしています。

フィルタを使用すると、重要な情報にすばやくアクセスできます。たとえば、ファイアウォール管理者は、特定のアプリケーションへのアクセスを一部のユーザーに許可または拒否する場合、ファイアウォールログをスキャンするようにユーザー検索条件を設定できます。イベントビューアに、検索条件に一致するイベントログが表示されます。

始める前に

次のタスクを実行するには、管理者 権限または セキュリティ アナリスト（Security Analyst）権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 フィルタ条件を入力します。

- フィルタ条件を手動で入力するには、検索テキストフィールドに正確な条件を入力するか、ドロップダウンリストから条件を選択します。その後、フィルタ条件の値を指定します。値を入力する際、可能な場合は常に、ドロップダウンリストに候補が表示されます。
- テーブル内のイベントのセル内のドットをクリックし、その値をフィルタ基準に含めるか除外するオプションを選択します。

  ヒント
  - 包含フィルタ条件をすばやく追加するには、**Ctrl キーを押しながらクリック**（Windows）するか **Command キーを押しながらクリック**（Mac）します。
  - 排他フィルタ条件をすばやく追加するには、**Alt キーを押しながらクリック**（Windows）するか **Option キーを押しながらクリック**（Mac）します。

- フィルタ基準を絞り込みます。ワイルドカードと検索の動作に関する重要な情報については、イベントの検索を参照してください。
- 値フィールドの値の前に、演算子（<、>、！など）を含めます。たとえば、[アクション（Action）] フィールドに `!Allow` と入力して、Allow 以外のアクションを持つすべてのイベントを検索します。

ステップ 3 検索を実行します。

ヒント **Ctrl キーを押しながら Enter キーを押す**（Windows）か **Command キーを押しながら Enter キーを押す**（Mac）ことで、検索を開始できます。

統合イベントビューアのイベントは、表示されたすべての列が同じ値を保持している場合は、集約されません。フィルタ基準に一致するすべてのイベントが個別に表示されます。

次のタスク

カスタムフィルタを保存するには、トピック「統合イベントビューアでの検索の保存」を参照してください。

統合イベントビューアでの検索の保存

始める前に

検索を保存するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 [分析（Analysis）] > [統合イベント（Unified Events）]を選択します。

ステップ 2 「統合イベントビューアのフィルタ」統合イベントビューアのフィルタ （8 ページ） トピックの説明に従って、検索条件を確立します。

ステップ 3 検索テキストボックスの [お気に入り検索（Favorite Search）]（☆）アイコンをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しい検索を保存するには、検索名を指定し、[新規として保存（Save as new）] をクリックします。
- 保存済みの検索を上書きするには、上書きする保存済み検索で [編集（Edit）] をクリックし、[上書き（Overwrite）] をクリックします。

次のタスク

保存した検索をロードするには、トピック「統合イベントビューアでの保存済み検索のロード」を参照してください。

統合イベントビューアでの保存済み検索のロード

始める前に

- このタスクを実行するには、管理者 または セキュリティ アナリスト（Security Analyst）権限が必要です。
- 「統合イベントビューアでの検索の保存」トピックの説明に従って、保存された検索を作成します。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 検索テキストボックスの [お気に入り検索（Favorite Search）]（☆）アイコンをクリックします。

ステップ 3 ロードする保存済み検索をクリックします。

統合イベントビューアでの列セットの保存

始める前に

列セットを保存するには、管理者 または セキュリティ アナリスト（Security Analyst） 権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 列ピッカーアイコン（▥）をクリックし、保存する列のセットを選択します。

ステップ 3 お気に入り列セット（☆）アイコンをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しい列セットを保存するには、列セット名を指定し、[新規として保存（Save as new）] をクリックします。
- お気に入りの列セットを上書きするには、上書きする列セットで[編集（Edit）] (⋮) をクリックし、[上書き（Overwrite）] をクリックします。

次のタスク

保存された列セットをロードするには、「統合イベントビューアでの保存済み列セットのロード」トピックを参照してください。

統合イベントビューアでの保存済み列セットのロード

始める前に

- このタスクを実行するには、管理者 権限またはセキュリティ アナリスト（Security Analyst） 権限が必要です。
- 「統合イベントビューアでの列セットの保存」トピックの説明に従って、お気に入りの列セットを保存します。

手順

ステップ 1 **[分析（Analysis）] > [統合イベント（Unified Events）]** を選択します。

ステップ 2 列ピッカーアイコン（▥）をクリックします。

ステップ 3 [お気に入りの列セット（Favorite column sets）] アイコン（☆）をクリックします。
ステップ 4 ロードする列セットをクリックします。

統合イベントビューアのカラムの説明

一部のフィールドの値は、イベントタイプによって異なります。デフォルトフィールドのフィールド対応は次のとおりです。

統合イベントビューアのフィールド名	接続イベントまたはセキュリティインテリジェンスイベントのフィールド名	侵入イベントのフィールド名	ファイルイベントのフィールド名	マルウェアイベントのフィールド名
時刻（Time）	最初のパケット（First Packet） 次の（注）を参照してください。	時刻（Time）	時刻（Time）	時刻（Time）
イベント タイプ	--	--	--	--
アクション（Action）	操作	インライン結果	操作	操作
理由	理由	理由	（非該当）	（非該当）
ソース IP（Source IP）	[イニシエータ IP（Initiator IP）]	ソース IP（Source IP）	送信側 IP（Sending IP）	送信側 IP（Sending IP）
宛先 IP（Destination IP）	レスポンダ IP（Responder IP）	宛先 IP（Destination IP）	受信側 IP（Receiving IP）	受信側 IP（Receiving IP）
送信元ポート/ICMP タイプ（Source Port/ICMP Type）	送信元ポート（Source Port）	送信元ポート（Source Port）	送信側のポート（Sending Port）	送信側のポート（Sending Port）
送信先ポート/ICMP タイプ（Destination Port/ ICMP Type）	宛先ポート	宛先ポート	受信側のポート（Receiving Port）	受信側のポート（Receiving Port）

統合イベントビューアのフィールド名	接続イベントまたはセキュリティインテリジェンスイベントのフィールド名	侵入イベントのフィールド名	ファイルイベントのフィールド名	マルウェアイベントのフィールド名
[Webアプリケーション（Web Application）]	Web アプリケーション	Web アプリケーション	Web アプリケーション	Web アプリケーション
Rule	アクセス コントロール ルール（Access Control Rule）	アクセス コントロール ルール（Access Control Rule）	（非該当）	（非該当）
ポリシー	アクセス コントロール ポリシー（Access Control Policy）	侵入ポリシー（Intrusion Policy）	ファイルポリシー（File Policy）	ファイルポリシー（File Policy）
Device	Device	Device	Device	デバイス

列ピッカー（▥）アイコンをクリックして、すべてのイベントフィールドとその対応関係を表示します。

フィールドの説明については、次のトピックを参照してください。

- 接続およびセキュリティ関連の接続イベントフィールド
- 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

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意も参照してください。

（注） 接続の開始時にロギングを有効にしていない場合でも、システムはこの値を持ち、統合イベントビューアの時間フィールドとして使用します。接続の開始時と終了時に接続イベントがログに記録されたかどうかを判断するには、イベントの行を展開して詳細を表示します。接続の両端がログに記録されている場合は、[最後のパケット（Last Packet）] フィールドが表示されます。

統合イベントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
統合イベントビューアのパケットトレーサ	7.4.1	任意（Any）	[統合イベントビューア（Unified Event Viewer）] ページからパケットトレーサを開いて、セキュリティイベントをトラブルシューティングできるようになりました。 パケットトレースを実行するイベントの横にある省略記号アイコン（⋮）（[展開（Expand）]）をクリックし、[パケットトレーサで開く（Open in Packet Tracer）] をクリックします。
統合イベントビューアの改善	7.4	任意（Any）	お気に入りの列セットの保存と検索機能の改善。
お気に入りの検索を保存する	7.3	任意（Any）	列セットと検索をお気に入りとして保存し、後ですばやく起動できます。
統合イベントビューア	7.0	任意（Any）	接続（セキュリティインテリジェンスを含む）、侵入、ファイル、マルウェアの複数のイベントタイプを 1 つのテーブルで表示および操作します。 新規/変更されたページ：**[分析（Analysis）]** > **[統合イベント（Unified Events）]** の新しいページ。 サポートされているプラットフォーム： Management Center

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。