検出イベント

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

検出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）

検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザアクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティポリシーは、収集するデータ、モニ

タするネットワーク セグメント、およびそのために使用する特定のハードウェア インターフェイスの種類を指定します。

検出およびアイデンティティ イベント テーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフローセットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみを表示するカスタム ワークフローを作成することもできます。

分析用にネットワーク検出およびアイデンティティ データを収集し、保存するには、ネットワーク検出およびアイデンティティ ポリシーを設定する必要があります。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザ データを提供します。アイデンティティ ポリシーは、権限のあるユーザー データを提供します。

次の検出イベント テーブルは、[分析（Analysis）] > [ホストおよび分析（Hosts and Analysis）] > [ユーザ（Users）] メニューにあります。

検出イベント テーブル	検出データが入力されますか。	アイデンティティ データが入力されますか。
ホスト（Hosts）	対応	×
ホストの侵害の兆候	対応	×
アプリケーション	対応	×
アプリケーション詳細（Application Details）	対応	×
サーバ	対応	×
ホスト属性（Host Attributes）	対応	×
検出イベント	対応	対応
ユーザの侵害の兆候（User Indications of Compromise）	対応	対応
アクティブ セッション（Active Sessions）	対応	対応
ユーザ アクティビティ（User Activity）	対応	対応
[ユーザー （Users）]	対応	対応
脆弱性（Vulnerabilities）	対応	×
サード パーティの脆弱性（Third-Party Vulnerabilities）	対応	×

ディスカバリ イベントの統計情報の表示

[ディスカバリ統計情報（Discovery Statistics）] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーション プロトコル、オペレーティング システムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバー、オペレーティング システム、またはオペレーティング システムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [検出統計（Discovery Statistics）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、統計情報を表示するデバイスを選択します。オプションで、Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて（All）] を選択します。

ステップ 3 次の選択肢があります。

- [統計情報サマリ（Statistics Summary）] セクション （4 ページ）で説明されているように、[統計サマリー（Statistics Summary）] に一般的な統計情報を表示します。
- [イベントの中断（Event Breakdown）] で、表示するイベント タイプをクリックします。イベントが 1 つも表示されない場合は、時間枠の変更で説明されているように、時間範囲を調整する必要があるかもしれません。
- [プロトコルの中断（Protocol Breakdown）] で、検出されたホストによって現在使用されているプロトコルを表示します。
- [アプリケーション プロトコルの中断（Application Protocol Breakdown）] で、表示するアプリケーション プロトコルの名前をクリックします。
- [OS の中断（OS Breakdown）] で、[OS 名（OS Name）] または [OS ベンダー（OS Vendor）] をクリックします。

関連トピック

[イベント分類（Event Breakdown）] セクション （5 ページ）
[プロトコル分類（Protocol Breakdown）] セクション （5 ページ）
[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション （5 ページ）

[OS 分類（OS Breakdown）] セクション （6 ページ）

[統計情報サマリ（Statistics Summary）] セクション

[統計情報サマリ（Statistics Summary）] セクションの行の説明は次のとおりです。

合計イベント数（Total Events）

Management Center に格納されているディスカバリ イベントの合計数。

過去 1 時間のイベントの合計（Total Events Last Hour）

最後の 1 時間に生成されたディスカバリ イベントの合計数。

過去 1 日のイベントの合計（Total Events Last Day）

最後の 1 日に生成されたディスカバリ イベントの合計数。

アプリケーションプロトコル合計数（Total Application Protocols）

検出されたホストで実行されているサーバのアプリケーション プロトコルの合計数。

IP ホストの合計（Total IP Hosts）

一意の IP アドレスによって特定された検出済みホストの合計数。

MAC ホストの合計（Total MAC Hosts）

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[MAC ホストの合計（Total MAC Hosts）] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

ルータの合計（Total Routers）

ルータとして識別された検出ノードの合計数。

ブリッジの合計（Total Bridges）

ブリッジとして識別された検出ノードの合計数。

ホスト制限の使用（Host Limit Usage）

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。

（注） ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワーク マップ上にホストは表示されなくなります。

最後に受け取ったイベント（Last Event Received）

最後のディスカバリ イベントが行われた日付と時間。

最後に受信した接続（Last Connection Received）

最後の接続が完了した日付と時間。

[イベント分類（Event Breakdown）] セクション

[イベント分類（Event Breakdown）] セクションには、データベースに格納されている各イベント タイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の 1 時間で発生したホスト入力イベントが示されます。

[イベント分類（Event Breakdown）] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

関連トピック

検出イベントおよびホスト入力イベント （10 ページ）

[プロトコル分類（Protocol Breakdown）] セクション

[プロトコル分類（Protocol Breakdown）] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコル スタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクション

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションには、検出されたホストで使用されているアプリケーション プロトコルが示されます。このセクションには、プロトコル名、最後の 1 時間にアプリケーション プロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数が表示されます。

[アプリケーション プロトコル分類（Application Protocol Breakdown）] セクションではさらに、検出されたプロトコルを使用しているサーバーの詳細を表示することもできます。

関連トピック

サーバー データ （35 ページ）

[OS 分類（OS Breakdown）] セクション

[OS 分類（OS Breakdown）] セクションには、監視対象ネットワーク上で稼動しているオペレーティング システム、およびオペレーティング システムのベンダー、各オペレーティング システムを実行しているホストの合計数が示されます。

オペレーティング システムの名前またはバージョンの値が unknown の場合は、オペレーティング システムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が pending の場合は、オペレーティング システムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS 分類（OS Breakdown）] セクションを使用して、検出されたオペレーティング システムの詳細を表示することができます。

関連トピック

ホスト データ （19 ページ）

ディスカバリ パフォーマンス グラフの表示

ディスカバリ イベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

始める前に

適切なネットワーク検出ポリシーを編集して、アプリケーション、ホスト、およびユーザーを含めます（これは、システム パフォーマンスに影響を与える可能性があります）。ネットワーク検出ルールの設定およびアクションと検出されるアセットを参照してください。

このタスクを実行するには、管理者ユーザーまたはメンテナンスユーザーである必要があります。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [検出パフォーマンス（Discovery Performance）]** を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、Management Center または対象とする管理対象デバイスを選択します。

ステップ 3 ディスカバリ パフォーマンス グラフ タイプ （7 ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックして、選択した統計情報をグラフ化します。

ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

処理されたイベント数/秒

Data Correlator が 1 秒間に処理するイベントの数を表します。

処理された接続数/秒

Data Correlator が 1 秒間に処理する接続の数を表します。

生成されたイベント数/秒

システムが 1 秒間に生成するイベントの数を表します。

メガビット/秒

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

平均バイト/パケット

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

キロパケット/秒

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

ディスカバリおよびアイデンティティ ワークフローの使用

Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティ データの分析で使用できるイベント ワークフローセットを提供します。ワークフローはネットワーク マップとともに、ネットワーク資産に関する主要な情報源になります。

Management Center には、ディスカバリおよびアイデンティティ データ、検出されたホストとそのホストの属性、サーバ、アプリケーション、アプリケーションの詳細、脆弱性、ユーザアクティビティ、ユーザに関する事前定義されたワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。

手順

ステップ 1 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：ディスカバリ イベントとホスト入力イベントの表示（17 ページ）を参照してください。
- ホスト データ：ホスト データの表示 （19 ページ）を参照してください。
- ホスト属性データ：ホスト属性の表示 （27 ページ）を参照してください。
- ホストまたはユーザの侵害の兆候データ：侵害兆候データの表示と処理 （30 ページ）を参照してください。
- サーバ データ：サーバー データの表示 （35 ページ）を参照してください。
- アプリケーション データ：アプリケーション データの表示 （39 ページ）を参照してください。
- アプリケーション詳細データ：アプリケーション詳細データの表示 （42 ページ）を参照してください。
- アクティブ セッション データ：アクティブ セッション データの表示 （64 ページ） を参照してください。
- ユーザー データ：ユーザー データの表示 （67 ページ）を参照してください。
- ユーザ アクティビティ データ：ユーザー アクティビティ データの表示 （70 ページ）を参照してください。
- ネットワーク マップ：ネットワーク マップの表示を参照してください。

ステップ 2 カスタム ワークフローにアクセスするには、**[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]** を選択します。

ステップ 3 カスタム テーブルに基づいたワークフローにアクセスするには、**[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]** を選択します。

ステップ 4 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- 列の制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（✕）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）]をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。

- 削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）]または[すべて削除（Delete

All）]をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

注意 [分析（Analysis）]>[ユーザー（Users）]>[ユーザー（Users）]**[分析（Analysis）]>[ユーザー（Users）]>[アクティブセッション（Active Sessions）]**ページで非 VPN セッションを削除する前に、そのセッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニターしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

（注） [分析（Analysis）]>[ユーザ（Users）]>[アクティブ セッション（Active Sessions）]ページの VPN セッションに関する詳細については、「リモート アクセス VPN の現在のユーザの表示」を参照してください。

（注） サードパーティの場合とは異なり、シスコの脆弱性は削除**できません**。ただし、確認済みとしてマークすることはできます。

- ドリル ダウン：ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用を参照してください。
- 現在のページを移動する：現在のワークフロー ページ内を移動するには、ワークフロー ページのナビゲーション ツールを参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、その他のイベント ビューに移動するには、ワークフロー間のナビゲーションを参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホストプロファイルの表示：IP アドレスのホストプロファイルを表示するには、[ホストプロファイル（Host Profile）]をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される [侵害を受けたホスト（Compromised Host）] をクリックします。
- ユーザープロファイル：ユーザー ID 情報を表示するには、[ユーザーID（User Identity）]の隣に表示される [ユーザー（User）] アイコン、または IOC に関連付けられているユーザーの場合は [レッドユーザー（Red User）] をクリックします。 の表示

関連トピック

ワークフローの使用

Management Center データベースからのデータの消去

検出イベントおよびホスト入力イベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワークセグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワークアセットにおける何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出されたTCPまたはUDPサーバについて、新しいイベントを生成します。必要に応じて、エクスポートされたNetFlowレコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーションプロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーションプロトコルの検出を無効にして、NetFlowエクスポータをモニターできますが、管理対象デバイスをモニターするよう設定された検出ルールではできません。NetFlow以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワークマッピングが完了すると、続けてシステムは変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出されたアセットの設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Management CenterのWebインターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、相関ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワークトラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メールアラートの応答を起動します。

ホスト入力機能を使用して、ネットワークマップにデータを追加することができます。オペレーティングシステムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーションプロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

ディスカバリイベントタイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリイベントのタイプを設定できます。ディスカバリイベントのテーブルを表示すると、[イベント（Event）]カラムにイベントタイプが表示されます。次に、ディスカバリイベントタイプについて説明します。

ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しいMACアドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

クライアント タイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

DHCP：IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

DHCP：IP アドレスの再割り当て

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

ホップ数の変更

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカル セグメント上にあることを示している場合。

ホスト削除：ホスト制限に到達

このイベントは、Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

ホスト ドロップ：ホスト制限に到達

このイベントは、Management Center 上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、**[ポリシー（Policies）]**>**[ネットワーク検出（Network Discovery）]**>**[詳細（Advanced）]** を選択し、[ホストの制限に達した場合（When Host Limit Reached）] を [ホストをドロップ（Drop hosts）] に設定します。

ホスト IOC 設定

このイベントは、ホストに対してIOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワーク マップからホストがドロップされたときに生成されます。個々のホストのIPアドレスとMACアドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワーク マップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワーク デバイスであったことを認識したときに生成されます。

アイデンティティ競合

このイベントは、システムが、新しいサーバまたはオペレーティング システムに対する現行のアクティブなアイデンティティと競合する、そのサーバまたはオペレーティング システムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティ データを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティ データを取得するために、ホストを再スキャンしてアイデンティティ データをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

MAC 情報の変更

このイベントは、特定のMACアドレスまたはTTL値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに発生します。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホスト プロファイル内でその MAC アドレスを太字で表示し、イベント ビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトラフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わる可能性があります。

NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。

（注） 分析用にクライアント データを収集および格納するには、ネットワーク検出ポリシーのディスカバリ ルールでアプリケーションの検出が有効になっていることを確認します。

新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでホストを検出するように設定します。

新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル（IP、ARP など）と通信していることをシステムが検出したときに生成されます。

新しい OS

このイベントは、システムがホストの新しいオペレーティング システムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

新しい TCP ポート

このイベントは、ホスト上でアクティブな新しい TCP サーバ ポート（SMTP または Web サービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーション プロトコル、またはアプリケーション プロトコルに関連付けられているサーバの識別には使用されません。情報は、TCP Server Information Update イベントで伝送されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

新しいトランスポート プロトコル

このイベントは、ホストが新しいトランスポート プロトコル（TCP、UDP など）と通信していることをシステムが検出したときに生成されます。

新しい UDP ポート

このイベントは、システムが、ホスト上で稼動している新しい UDP サーバ ポートを検出したときに生成されます。

このイベントは、デバイスがネットワーク マップにすでに存在しないモニタ対象ネットワーク上のサーバを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

TCP ポート クローズ

このイベントは、システムが、ホスト上で TCP ポートがクローズしたことを検出したときに生成されます。

TCP ポート タイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムが TCP ポートからアクティビティを検出しなかったときに生成されます。

TCP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている TCP サーバでシステムが変更を検出したときに生成されます。

このイベントは、TCP サーバが更新されたときに生成される場合があります。

UDP ポート クローズ

このイベントは、システムが、ホスト上で UDP ポートがクローズしたことを検出したときに生成されます。

UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。

UDP サーバ情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバが更新されたときに生成される場合があります。

VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

関連トピック

ホスト入力イベント タイプ （15 ページ）

ホスト入力イベント タイプ

ディスカバリ イベントのテーブルを表示すると、[イベント（Event）] カラムにイベント タイプが表示されます。

ユーザが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリ イベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベント タイプの名前がわかると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

クライアントの追加（Add Client）

このイベントは、ユーザがクライアントを追加したときに生成されます。

ホストの追加（Add Host）

このイベントは、ユーザがホストを追加したときに生成されます。

プロトコルの追加（Add Protocol）

このイベントは、ユーザがプロトコルを追加したときに生成されます。

スキャン結果の追加（Add Scan Result）

このイベントは、システムが Nmap スキャンの結果をホストに追加したときに生成されます。

ポートの追加（Add Port）

このイベントは、ユーザがサーバ ポートを追加したときに生成されます。

クライアントの削除（Delete Client）

このイベントは、ユーザがシステムからクライアントを削除したときに生成されます。

ホスト/ネットワークの削除（Delete Host/Network）

このイベントは、ユーザがシステムから IP アドレスまたはサブネットを削除したときに生成されます。

プロトコルの削除（Delete Protocol）

このイベントは、ユーザがシステムからプロトコルを削除したときに生成されます。

ポートの削除（Delete Port）

このイベントは、ユーザがシステムからサーバ ポートまたはサーバ ポートのグループを削除したときに生成されます。

ホスト属性の追加（Host Attribute Add）

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

ホスト属性の削除（Host Attribute Delete）

このイベントは、ユーザが、ユーザ定義のホスト属性を削除したときに生成されます。

ホスト属性値の削除（Host Attribute Delete Value）

このイベントは、ユーザが、ホスト属性に割り当てられている値を削除したときに生成されます。

ホスト属性値の設定（Host Attribute Set Value）

このイベントは、ユーザがホストに対してホスト属性値を設定したときに生成されます。

ホスト属性の更新（Host Attribute Update）

このイベントは、ユーザが、ユーザ定義のホスト属性の定義を変更したときに生成されます。

ホスト重要度の設定（Set Host Criticality）

このイベントは、ユーザがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

オペレーティング システム定義の設定（Set Operating System Definition）

このイベントは、ユーザがホストに対してオペレーティング システムを設定したときに生成されます。

サーバ定義の設定（Set Server Definition）

このイベントは、ユーザがサーバに対してベンダーおよびバージョンの定義を設定したときに生成されます。

脆弱性影響認定の設定（Set Vulnerability Impact Qualification）

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

脆弱性を無効に設定（Vulnerability Set Invalid）

このイベントは、ユーザが 1 つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

脆弱性を有効に設定（Vulnerability Set Valid）

このイベントは、ユーザーが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

関連トピック

ディスカバリ イベント タイプ （10 ページ）

ディスカバリ イベントとホスト入力イベントの表示

ディスカバリ イベント ワークフローでは、ディスカバリ イベントとホスト入力イベント両方からのデータを表示できます。ユーザーは検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザーがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 **[分析（Analysis）] > [ホスト（Hosts）] > [検出イベント（Discovery Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更の説明に従って、時間範囲を調整します。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ディスカバリ イベントのフィールド （18 ページ）を参照）。

関連トピック

ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）

ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

時刻（Time）

システムがイベントを生成した時間。

イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

[IPアドレス（IP Address）]

イベントに関連するホストに関連付けられている IP アドレス。

ユーザー（User）

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のあるユーザが次にログインするまで、権限のあるユーザが現行のユーザとして保持されます。

[MAC アドレス（MAC Address）]

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトラフィックが通過したネットワーク デバイスの MAC アドレスになります。

[MAC ベンダー（MAC Vendor）]

ディスカバリ イベントをトリガーとして使用したネットワーク トラフィックが使用する NIC の MAC ハードウェア ベンダー。

[ポート（Port）]

イベントをトリガーとして使用したトラフィックが使用するポート（該当する場合）。

説明

テキストによるイベントの説明。

ドメイン

ホストを検出したデバイスのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバーのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

関連トピック

イベントの検索

ホスト データ

システムがホストを検出し、ホストプロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトラフィックのプロファイル、およびコンプライアンスのallowリストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホストグループに割り当てることもできます。その後で、相関ルールおよびポリシーの中でこれらの重要度の値、allowリスト、およびトラフィックプロファイルを使用できます。

システムは、エクスポートされたNetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

ホスト データの表示

Management Center を使用して、システムが検出したホストのテーブルを表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローは両方ともホスト ビューで終了しますが、このホスト ビューには、ユーザーの制約を満たすすべてのホストのホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [ホスト（Hosts）]** を選択します。
- ホストのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホスト（Hosts）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト データ フィールド （20 ページ）を参照）。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定 （29 ページ）を参照）。
- 特定のホストのトラフィック プロファイルを作成します（選択したホストのトラフィック プロファイルの作成 （25 ページ）を参照）。
- 特定のホストに基づいて、コンプライアンスの allow リストを作成します（選択したホストに基づいたコンプライアンスの許可（Allow）リストの作成 （26 ページ）を参照）。

ホスト データ フィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティング システムなどが含めることが可能です。ユーザは、ホストのテーブル ビューでこれらの情報の一部を表示することができます。

ホスト テーブルで表示および検索できるフィールドの説明が続きます。

前回の検出（Last Seen）

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出（Last Seen）] の値は、ホストの IP アドレスに対してシステムが新しいホスト イベントを生成したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティング システムのデータを更新しているホストでは、[前回の検出（Last Seen）] の値は、そのデータが最初に追加された日付と時間を表します。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

MAC アドレス（MAC Address）

ホストが検出した NIC の MAC アドレス。

[MAC アドレス（MAC Address）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC アドレス（MAC Address）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

MAC ベンダー（MAC Vendor）

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC ベンダー（MAC Vendor）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC ベンダー（MAC Vendor）] フィールドを追加できます。

- [ホスト（Hosts）] テーブルのフィールドが含まれているカスタム テーブル
- [ホスト（Hosts）] テーブルに基づいたカスタム ワークフローのドリルダウン ページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関係するイベントを照合します。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ホストに割り当てられている、ユーザ指定の重要度の値。

NetBIOS 名（NetBIOS Name）

ホストのNetBIOS名。NetBIOSプロトコルを実行しているホストにのみ、NetBIOS名があります。

VLAN ID（Admin. VLAN ID）

ホストが使用する VLAN ID。

ホップ（Hops）

ホストを検出したデバイスからホストへのネットワークのホップ数。

ホスト タイプ（Host Type）

ホストのタイプ。ホスト、モバイル デバイス、jailbroken モバイル デバイス、ルータ、ブリッジ、NAT デバイス、ロード バランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol（CDP）メッセージの分析。ネットワークのデバイスおよびそれらのタイプ（シスコ デバイスのみ）を特定できます。
- スパニング ツリー プロトコル（STP）の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロード バランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、`!host` と入力してすべてのネットワーク デバイスを検索します。

ハードウェア（Hardware）

モバイル デバイスのハードウェア プラットフォーム。

OS

次のいずれかです。

- ホスト上で検出されたオペレーティング システム（名前、ベンダー、およびバージョン）、または Nmap かホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`

- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で [カスタム分析（Custom Analysis）] ウィジェットからホスト イベント ビューを起動したときに表示されます。また、これは [ホスト（Hosts）] テーブルに基づいたカスタム テーブルのフィールド オプションです。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 競合（OS Conflict）

このフィールドは検索専用です。

OS ベンダー（OS Vendor）

次のいずれかです。

- ホストで検出されたオペレーティング システムのベンダー、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのベンダー。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS 名（OS Name）

次のいずれかです。

- ホスト上で検出されたオペレーティング システム、またはNmapかホスト入力機能を使用して更新されたオペレーティング システム。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は unknown
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は pending

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/a と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

OS バージョン（OS Version）

次のいずれかです。

- ホストで検出されたオペレーティング システムのバージョン、またはNmapかホスト入力機能を使用して更新されたオペレーティング システムのバージョン。
- オペレーティング システムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティング システムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a` と入力して、オペレーティング システムがまだ識別されていないホストを含めます。

ソース タイプ（Source Type）

ホストのオペレーティング システムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加されたNmapまたはスキャナ）
- システムによって検出されたオペレーティング システムの場合は `Firepower`

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

信頼性（Confidence）

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティング システムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能やNmapスキャナなどのアクティブなソースによって識別されたオペレーティング システムの場合）。
- `unknown`（システムがオペレーティング システムのアイデンティティを特定できないホスト、およびNetFlowデータに基づいてネットワーク マップに追加されたホストの場合）。

このフィールドを検索するときは、`n/a` と入力して、NetFlow データに基づいてネットワーク マップに追加されたホストを含めます。

注記（Notes）

[注記（Notes）] ホスト属性の、ユーザ定義のコンテンツ。

ドメイン（Domain）

ホストに関連付けられているドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワークマップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

カウント（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索
オペレーティング システムのアイデンティティの競合

選択したホストのトラフィック プロファイルの作成

トラフィック プロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

[ホスト（Hosts）] ページを使用して、指定するホスト グループのトラフィック プロファイルを作成できます。トラフィック プロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 ホスト ワークフローのテーブル ビューで、トラフィック プロファイルを作成するホストの隣にあるチェック ボックスをオンにします。

ステップ 2 ページの下部で [トラフィック プロファイルの作成（Create Traffic Profile）] をクリックします。

ステップ 3 特別なニーズに応じて、トラフィック プロファイルを変更し、保存します。

関連トピック

トラフィック プロファイルの概要

選択したホストに基づいたコンプライアンスの許可（Allow）リストの作成

コンプライアンスのallowリストでは、ネットワーク上で許可されるオペレーティングシステム、クライアント、ネットワーク、トランスポート、またはアプリケーションプロトコルを指定することができます。

[ホスト（Hosts）]ページを使用して、ユーザーが指定するホストグループのホストプロファイルに基づいて、コンプライアンスのallowリストを作成することができます。ソートおよび検索機能を使用して、allowリストの作成に使用するホストを分離することができます。

始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 ホストワークフローのテーブルビューで、allowリストを作成するホストの隣にあるチェックボックスをオンにします。

ステップ 2 ページの下部で [**許可リスト（Allow List**）の作成（Create White List）] をクリックします。

ステップ 3 特別なニーズに応じて、allowリストを変更し、保存します。

関連トピック

コンプライアンス許可（Allow）リストの概要

ホスト属性データ

システムは、検出したホストに関する情報を収集し、その情報を使用してホストプロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホストプロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホストプロファイルの認定でホスト属性を使用することができます。これにより、トラフィックプロファイルの作成中に収集するデータを制約し、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

関連トピック

ホスト属性の表示 （27 ページ）
セット属性修復の設定

ホスト属性の表示

Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。その後、探している情報に応じて表示方法を操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブル ビューが含まれており、ホスト ビュー ページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホスト プロファイルが含まれています。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ホスト属性（Host Attributes）]** を選択します。
- ホスト属性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [属性（Attributes）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ホスト属性データ フィールド （28 ページ）を参照）。
- ホスト属性を特定のホストに割り当てます（選択したホストのホスト属性の設定 （29 ページ）を参照）。

ホスト属性データ フィールド

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

[IPアドレス（IP Address）]

ホストに関連付けられている IP アドレス。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に[低（Low）]、[中（Medium）]、[高（High）]、または [なし（None）] を割り当てることができます。

注記（Notes）

他のアナリストに提示する、ホストに関する情報。

コンプライアンス allow リストの属性を含む、ユーザー定義のホスト属性（Any user-defined host attribute, including those for compliance allow lists）

ユーザー定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

ドメイン（Domain）

ホストに関連付けられているドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索

選択したホストのホスト属性の設定

ホストワークフローから、事前定義済のホスト属性とユーザー定義のホスト属性を設定できます。

手順

ステップ 1 ホストワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

ヒント ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

ステップ 2 ページの下部にある [属性の設定（Set Attributes）] をクリックします。

ステップ 3 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）] を選択できます。

ステップ 4 必要に応じて、テキスト ボックスで、選択したホストのホスト プロファイルにメモを追加します。

ステップ 5 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

ステップ 6 [保存（Save）] をクリックします。

侵害の兆候データ

システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、セキュリティインテリジェンス、接続イベント、ファイルまたはマルウェアイベント）との関連性を示します。イベントデータの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。このようなホストのIPアドレスは**侵害を受けているホストの赤いアイコン**でイベントビューに表示されます。

ホストが侵害されている可能性があると識別された場合、その侵害に関連付けられているユーザにもタグが付けられます。そのようなユーザーは、**赤色のユーザーアイコン**でイベントビューに表示されます。

マルウェアが含まれているファイルが300秒以内にIOCというタグが付けられて再度表示される場合は、別のIOCは生成されません。同じファイルが300秒以上経ってから表示された場合は、新しいIOCが生成されます。

侵害の兆候としてイベントにタグを付けるように設定するには、Cisco Secure Firewall Management Centerデバイス構成ガイドの「Enabling Indications of Compromise Rules」を参照してください。

関連トピック

サーバーのアイデンティティの編集

侵害兆候データの表示と処理

Management Center を使用して、侵害の兆候（IOC）を示すテーブルを表示できます。検索する情報に応じてイベント ビューを操作します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

表示されるページは、使用するワークフローによって異なります。事前定義の IOC ワークフローはプロファイル ビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザのホストプロファイルまたはユーザプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

始める前に

- システムで侵害の兆候（IOC）を検出してタグを付けるには、ネットワーク検出ポリシーの IOC 機能をアクティブにして、少なくとも 1 つの IOC ルールを有効にする必要があります。『Cisco Secure Firewall Management Center デバイス構成ガイド』の「侵害の兆候ルールの有効化」を参照してください。
- アクティブなアイデンティティ ポリシーでユーザーが認識される必要があります。

手順

ステップ 1 Web インターフェイスのどの場所のニーズを満たす情報があるかを特定します。

侵害兆候データを表示または処理するには、次の場所を使用できます。

- イベントビューア（[分析（Analysis）] メニューの下）：接続、セキュリティ インテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーする、Secure Endpoint によって生成されたマルウェアイベントは、イベントタイプが `AMP IOC` であり、侵害を指定するイベントサブタイプと一緒に表示されることに注意してください。
- ダッシュボード：ダッシュボードでは、サマリーダッシュボードの [脅威（Threats）] に、ホスト別とユーザー別の IOC タグがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- コンテキスト エクスプローラ：コンテキスト エクスプローラの [侵害の兆候（Indications of Compromise）] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- [ネットワークマップ（Network Map）] ページ：[分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] にある [侵害の兆候（Indications of Compromise）] には、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。

- [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] 詳細ページ：[分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[分析（Analysis）] > [ホスト（Hosts）] メニューの下の [ホストの侵害の兆候（Host Indications of Compromise）] ページには、モニタ対象ホストの一覧がIOCタグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- [ユーザの侵害の兆候（User Indications of Compromise）] ページ：[分析（Analysis）] > [ユーザ（Users）] メニューの下の [ユーザの侵害の兆候（User Indications of Compromise）] ページには、IOCの可能性があるイベントに関連付けられているユーザの一覧がIOCタグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ホスト プロファイル ページ：侵害されている可能性があるホストのホスト プロファイルには、そのホストに関連付けられているすべてのIOCタグが表示され、IOCタグの解決とIOC ルール状態の設定ができます。
- ユーザ プロファイル ページ：IOC の可能性があるイベントに関連付けられているユーザのユーザ プロファイルには、そのユーザに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます（Management Center の Web インターフェイスでは、ユーザープロファイルは「ユーザーアイデンティティ（User Identity）」とラベルが付けられています）。

ステップ 2 必要に応じて、次のうちのいずれかを実行し、この手順の残りのステップを使用します。

オプション	説明
ホストのIOCを調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [侵害の兆候（Indications of Compromise）]** を選択します。 • ホスト IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ホストの侵害の兆候（Host Indications of Compromise）] を選択します。
ユーザに関連付けられているIOCを調べるには、以下を実行します。	• 事前定義されたワークフローを使用する場合、[分析（Analysis）] > [ユーザ（Users）] > [侵害の兆候（Indications of Compromis）] を選択します。 • ユーザ IOC のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザの侵害の兆候（User Indications of Compromise）] を選択します。

ステップ 3 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（侵害の兆候データ フィールド （32 ページ）を参照）。
- [ホストの侵害の兆候（Host Indications of Compromise）] ページ：[IPアドレス（IP Address）] 列にある [侵害を受けたホスト（Compromised Host）] をクリックして、侵害を受けたホストのホストプロファイルを表示します。
- [ユーザーの侵害の兆候（User Indications of Compromise）]：[ユーザー（User）] 列の [赤色のユーザー（Red User）] をクリックして、侵害に関連付けられているユーザープロファイルを表示します。
- IOC イベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェック ボックスをオンにして、[解決済みとマークを付ける（Mark Resolved）] をクリックします。
- [最初の確認日時（First Seen）] または [前回の検出（Last Seen）] 列にある[表示（View）]（  ）をクリックして、IOC をトリガーしたイベントの詳細を表示します。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

侵害の兆候データ フィールド

以下は、ホストまたはユーザの IOC（侵害の兆候）テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

IP アドレス（IP Address）（ホストの IOC データを表示する場合）

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

ユーザ（User）（ユーザの IOC データを表示する場合）

IOC をトリガーしたイベントに関連付けられているユーザのユーザ名、レルム、および認証ソース。

カテゴリ

`Malware Executed` や `Impact 1 Attack` など、示された侵害のタイプの簡単な説明。

イベントタイプ

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

説明

侵害される可能性のあるホストへの影響の説明（[このホストはリモート制御下にある可能性があります（This host may be under remote control）] や [このホスト上でマルウェアが実行されました（Malware has been executed on this host）] など）。

最初の確認日時/最新の確認日時（First Seen/Last Seen）

IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

ドメイン（Domain）

IOC をトリガーとして使用したホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

関連トピック

イベントの検索

単一ホストまたはユーザにおける侵害の兆候のルール状態の編集

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストと、そのネットワーク上の IOC イベントに関連付けられている権限のあるユーザーに適用されます。個々のホストまたはユーザのルールを無効にして、無用な IOC タグを回避できます（たとえば、DNS サーバに対する IOC タグが表示されないようにできます）。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストまたはユーザに対して有効にすることができません。特定のホストに対してルールを無効にしても、同じイベントに関与するユーザーのタグ付けには影響がなく、その逆もまた同じです。

手順

ステップ 1 ホストまたはユーザ プロファイルの [侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 [ルール状態の編集（Edit Rule States）] をクリックします。

ステップ 3 ルールの [有効（Enabled）] 列で、スライダをクリックしてこれを有効または無効にします。

ステップ 4 [保存（Save）] をクリックします。

侵害の兆候のタグのソース イベントの表示

ホスト プロファイルやユーザー プロファイルの [侵害の兆候（Indications of Compromise）] セクションを使用して、IOC タグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の[表示（View）]（）をクリックすると、関連するイベントタイプのイベントのテーブルビューに移動します。ここでは、IOC タグをトリガーしたイベントのみが表示されます。

ユーザー IOC の最初のインスタンスのみが Management Center に表示されます。後続のインスタンスは DNS サーバによって捕捉されます。

手順

ステップ 1 ホストまたはユーザープロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 調べたい IOC タグの [最初の痕跡（First Seen）] または [最後の痕跡（Last Seen）] 列にある[表示（View）]（）をクリックします。

侵害の兆候タグの解決

侵害の兆候（IOC）タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルおよびユーザープロファイルから削除されます。プロファイル上のアクティブな IOC タグがすべて解決されると、**侵害されたホスト** またはユーザーが侵害の兆候に関連付けられていることを示す**赤色のユーザーアイコン** は表示されなくなります。解決した IOC についても、IOC のトリガー元であるイベントは引き続き表示できます。

IOC タグをトリガーしたイベントが繰り返された場合、ホストまたはユーザに対する IOC ルールが無効にされていない限り、このタグが再び設定されます。

手順

ステップ 1 ホストまたはユーザ プロファイルで、[侵害の兆候（Indications of Compromise）] セクションに移動します。

ステップ 2 次の 2 つの選択肢があります。

- 個別の IOC タグに解決済みとマークするには、解決するタグの右にある [削除（Delete）]（  ） をクリックします。
- プロファイル上のすべての IOC タグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける（Mark All Resolved）] をクリックします。

サーバー データ

システムは、モニター対象ネットワークセグメント上のホストで稼動しているすべてのサーバーに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワーク プロトコル
- サーバのベンダーとバージョン
- サーバを実行しているホストに関連付けられている IP アドレス
- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリ イベントを生成します。Management Center の Web インターフェイスを使用して、サーバ イベントを表示、検索、削除できます。

また、サーバイベントを相関ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼働している ircd などのチャット サーバーを検出したときに相関ルールをトリガーできます。

システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（NetFlow データと管理対象デバイス データの違いを参照）。

サーバー データの表示

Management Center を使用して、検出されたサーバーのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがサーバにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義のすべてのワークフローはホスト ビューで終了しますが、このホスト ビューには、制約を満たすすべてのホストに対して 1 つずつホスト プロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、サーバ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[サーバー（Servers）]** を選択します。
- サーバのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [サーバ（Servers）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サーバー データ フィールド （36 ページ）を参照）。
- 編集するサーバーのイベントの横にあるチェック ボックスをオンにし、[サーバー アイデンティティの設定（Set Server Identity）] をクリックすることによって、サーバーのアイデンティティを編集します。
- オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

サーバー データ フィールド

サーバ テーブルで表示および検索できるフィールドの説明は次のとおりです。

前回の使用（Last Used）

ネットワーク上でサーバが最後に使用された日付と時間、またはホスト入力機能を使用してサーバが最初に更新された日付と時間。[前回の使用（Last Used）] の値は、システムがサーバ情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

[IPアドレス（IP Address）]

サーバを実行しているホストに関連付けられている IP アドレス。

ポート

サーバが稼動しているポート。

プロトコル

サーバが使用するネットワークまたはトランスポート プロトコル。

アプリケーション プロトコル（Application Protocol）

次のいずれかです。

- サーバのアプリケーション プロトコルの名前
- `pending`：システムで、いずれかの理由でサーバをポジティブまたはネガティブに識別できない場合

- unknown：既知のサーバ フィンガープリントに基づいてシステムでサーバを識別できない場合、またはホストの入力を介してサーバが追加され、アプリケーションプロトコルが含まれていなかった場合

アプリケーションプロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Application Protocols）

アプリケーション プロトコルに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ベンダー（Vendor）

次のいずれかです。

- サーバのベンダー：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのベンダー
- 空白：システムが既知のサーバフィンガープリントに基づいてベンダーを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

バージョン（Version）

次のいずれかです。

- サーバのバージョン：システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバのバージョン
- 空白：システムが既知のサーバ フィンガープリントに基づいてバージョンを識別できなかった場合、またはNetFlowデータを使用してサーバがネットワーク マップに追加された場合

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーション プロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性（Category, Tags, Risk, or Business Relevance for Web Applications）

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

ヒット数（Hits）

サーバがアクセスされた回数。ホスト入力機能を使用して追加されたサーバの場合、この値は必ず 0 になります。

ソース タイプ（Source Type）

次の値のいずれかを指定します。

- [ユーザ（User）]：user_name
- [アプリケーション（Application）]：app_name
- スキャナ：scanner_type（ネットワーク検出の設定を介して追加された Nmap またはスキャナ）
- システムによって検出されたサーバーの `Firepower`、`Firepower Port Match`、または `Firepower Pattern Match`
- NetFlow データを使用して追加されたサーバの `NetFlow`

ドメイン（Domain）

サーバーを実行しているホストのドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

トラフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

カウント（Count）

各行に表示される情報と一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後のみです。

関連トピック

イベントの検索

アプリケーション データとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。システムは、電子メール、インスタントメッセージ、ピアツーピア、Webアプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用したIPアドレス、製品、バージョン、および使用が検出された回数を記録します。Webインターフェイスを使用して、アプリケーションイベントを表示、検索、および削除できます。ホスト入力機能を使用して、1つ以上のホスト上のアプリケーションデータを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、その情報をもとにホスト プロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメールクライアントを使用させたい場合は、システムが、いずれかの対象ホストで別のメール クライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

アプリケーションディテクタに関する最新情報は、各システム更新のリリースノート、各VDB更新のアドバイザリをよくご確認ください。

分析用にアプリケーションデータを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

アプリケーション データの表示

Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションにアクセスするときに表示されるページは、使用するワークフローによって異なります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[アプリケーション詳細（Application Details）]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーション データ フィールド（40 ページ）を参照）。
- クライアント、アプリケーションプロトコル、Web アプリケーションの横にある [アプリケーション詳細ビュー（Application Detail View）] をクリックすることによって、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。
- イベント値を右クリックして、システムの外部にあるソース内のデータを表示します。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。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。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。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。

アプリケーション データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーション テーブルで表示および検索できるフィールドについて説明します。

Application

検出されたアプリケーションの名前。

IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

タイプ（Type）

アプリケーションのタイプであり、次のものがあります。

アプリケーション プロトコル（Application Protocols）

ホスト間の通信を意味します。

クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

Web アプリケーション（Web Applications）

HTTP トラフィックの内容や要求された URL を意味します。

カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。

リスク（Risk）

アプリケーションが組織のセキュリティポリシーに違反することがある目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Risk、Client Risk、Web Application Risk の 3 つ（存在する場合）の中で最も高いものとなります。

ビジネスとの関連性（Business Relevance）

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低（Very Low）] から [極めて高（Very High）] までです。

侵入イベントをトリガーしたトラフィックで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の 3 つ（存在する場合）の中で最も低いものとなります。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索

アプリケーション詳細データの表示

Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、アプリケーション詳細データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション詳細（Application Details）]** を選択します。
- アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [クライアント（Clients）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（アプリケーションの詳細データ フィールド （43 ページ）を参照）。
- クライアントの横にある [アプリケーション詳細ビュー（Application Detail View）] をクリックして、特定のアプリケーションの [アプリケーション詳細ビュー（Application Detail View）] を開きます。
- イベント値を右クリックして、システムの外部で利用可能なソース内のデータを表示します。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。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。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審

な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。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。

アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、またはWebアプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

前回の使用（Last Used）

アプリケーションが前回使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用（Last Used）]の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

クライアント（Client）

アプリケーションの名前。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

バージョン（Version）

アプリケーションのバージョン。

クライアント、アプリケーション プロトコル、および Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性（Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications）

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

アプリケーション プロトコル（Application Protocol）

アプリケーションで使用されるアプリケーションプロトコル。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーション プロトコル名に `client` が付加されて一般名が表示されます。

Web アプリケーション（Web Application）

HTTP トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーション プロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

ヒット数（Hits）

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に 0 になります。

ドメイン（Domain）

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

現在のユーザー（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索

脆弱性データ

システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。ホストで稼動しているオペレーティング システム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。

- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーション プロトコルが Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

関連トピック

サーバの脆弱性のマッピング

脆弱性データのフィールド

注記がある場合を除き、これらのフィールドは、[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下のすべてのページに表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

National Vulnerability Database（NVD）でこの脆弱性の詳細を表示するには、CVE ID を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択します。

発行日（Date Published）

脆弱性が公開された日付。

説明

National Vulnerability Database（NVD）からの脆弱性の簡単な説明。

完全な説明については、CVE ID を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択して、National Vulnerability Database（NVD）の詳細を表示します。

影響

「脆弱性の影響（Vulnerability Impact）」（下記）を参照してください。

影響修飾子（Impact Qualification）

このフィールドは、[脆弱性の詳細（Vulnerability Details）] ページでのみ使用できます。

ドロップダウン リストを使用して、脆弱性を有効または無効にします。Management Center は、影響の相関関係において、無効な脆弱性を無視します。

ユーザがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザが値を選択するホスト プロファイルに脆弱性が限定されないかが決まります。

[リモート（Remote）]

脆弱性がリモートで不正利用されるかどうかを示します（TRUE/FALSE）。

重大度

National Vulnerability Database（NVD）の基本スコアと Common Vulnerability Scoring System スコア（CVSS）。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

SVID

脆弱性を追跡するためにシステムで使用する脆弱性の識別番号。

この脆弱性の詳細を表示するには、[表示（View）]（  ）をクリックします。

脆弱性の影響/影響

脆弱性のシビラティ（重大度）。0～10 の値で、10 は最も重大であることを示します。

関連トピック

イベントの検索

脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システムが、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブ化されません）。

IP アドレスによって制約されて**いない**脆弱性ワークフロー内である 1 つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの 2 ページ目の [ネットワーク上の脆弱性（Vulnerabilities on the Network）]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。

- 脆弱性ワークフロー（カスタムまたは事前定義）のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

1 台のホストに対して 1 つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワーク マップの使用、ホストのホスト プロファイルの使用、または脆弱性を非アクティブ化する対象の 1 つ以上のホストの IP アドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数の IP アドレスを持つホストの場合、この機能はそのホストの選択された 1 つの IP アドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインの脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフ ドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

関連トピック

個々のホストに関する脆弱性の非アクティブ化
個々の脆弱性の非アクティブ化
複数の脆弱性の非アクティブ化 （49 ページ）

脆弱性データの表示

Management Center を使用して、脆弱性のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザは事前定義のワークフローを使用できますが、これには脆弱性のテーブル ビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブル ビューにはデータベース内の各脆弱性に対して 1 つのローが含まれています。事前定義のワークフローの 2 ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザが非アクティブにしていないもの）に対して 1 つのローが含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

ヒント 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択します。
- 脆弱性テーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- 脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします（複数の脆弱性の非アクティブ化 （49 ページ）を参照）。
- SVID カラムの [表示（View）]（👁） をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。脆弱性の詳細の表示 （48 ページ）でその他の詳細を表示するオプションを確認してください。
- タイトルを右クリックして [フルテキストの表示（Show Full Text）] を選択することによって、脆弱性タイトルのフルテキストを表示します。

脆弱性の詳細の表示

手順

脆弱性の詳細は、次の方法のいずれかで表示できます。

- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択し、SVID の横にある [表示（View）]（👁） をクリックします。
- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[サードパーティの脆弱性（Third-Party Vulnerabilities）]** を選択し、SVID の横にある [表示（View）]（👁） をクリックします。
- **[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]** を選択し、[脆弱性（Vulnerabilities）] をクリックします。
- 脆弱性の影響を受けるホストのプロファイルを表示し（**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]**（[Analysis] > [Hosts] > [Network Map]）、[ホスト（Hosts）] をクリックし、調査しているホストをドリルダウンしてクリックします）、そのプロファイルの [脆弱性（Vulnerabilities）] セクションを展開します。
- [分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下にある任意のテーブルで、[CVE ID] 列の値を右クリックし、[NVDで説明を表示する（View description in NVD）] を選択して、NVD（National Vulnerabilities Database）Web サイトでその CVE を表示します。

複数の脆弱性の非アクティブ化

IPアドレスで制約されて**いない**脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフドメインは、先祖ドメインで脆弱性がアクティブ化されていれば、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できます。

手順

ステップ 1 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[脆弱性（Vulnerabilities）]** を選択します。
- 脆弱性テーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

ステップ 2 [ネットワークの脆弱性（Vulnerabilities on the Network）] をクリックします。

ステップ 3 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

ステップ 4 ページ下部の [レビュー（Review）] をクリックします。

関連トピック

個々のホストに関する脆弱性の非アクティブ化
個々の脆弱性の非アクティブ化

サードパーティの脆弱性データ

システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリンティング機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。

システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップ データで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンドラインでファイルのインポートを作成できなければなりません。詳細については、*Firepower* システムホスト入力 *API* ガイドを参照してください。

インポートしたデータを影響の相関に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティングシステムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

サードパーティの脆弱性データの表示

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Management Centerを使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザーは、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2 つの事前定義されたワークフローがあります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）]** を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [送信元別の脆弱性（Vulnerabilities by Source）] または [IP アドレス別の脆弱性（Vulnerabilities by IP Address）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（サードパーティの脆弱性データのフィールド （50 ページ）を参照）。
- SVIDカラムの[表示（View）]（  ）をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

脆弱性ソース（Vulnerability Source）

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

脆弱性 ID（Vulnerability ID）

ソースの脆弱性に関連付けられている ID 番号。

IPアドレス（IP Address）

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

ポート

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号。

SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、[表示（View）]（） をクリックします。

Snort ID

[Snort ID]（SID）データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

タイトル（Title）

脆弱性のタイトル。

説明

脆弱性についての簡単な説明。

ドメイン（Domain）

この脆弱性を持つホストのドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

関連トピック

イベントの検索

アクティブ セッション、ユーザー、およびユーザー アクティビティ データ

アイデンティティ ソースは、アクティブなセッション データ、ユーザ データ、およびユーザ アクティビティ データを収集します。データは、次の個々のユーザ関連のワークフローに表示されます。

- [アクティブなセッション（Active Sessions）]：このワークフローには、ネットワーク上の現在のすべてのユーザ セッションが表示されます。複数の同時アクティブ セッションを実行する単一ユーザは、この表で複数の行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはアクティブ セッション データ （63 ページ）を参照してください。
- ユーザ：このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では 1 ユーザが 1 つの行を占めます。このワークフローに表示されるユーザ データの種類について、詳しくはユーザー データ（User Data） （65 ページ）を参照してください。
- ユーザ アクティビティ：このワークフローは、ネットワークで認識されるすべてのユーザ アクティビティを表示します。この表では、複数のユーザ アクティビティ インスタンスを持つ 1 ユーザが複数の行を占めます。このワークフローに表示されるユーザ アクティビティの種類の詳細については、ユーザー アクティビティ データ （68 ページ）を参照してください。

これらのワークフローの入力元であるユーザー アイデンティティ ソースの詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「」を参照してください。

ユーザー関連フィールド

ユーザ関連データは、アクティブ セッション、ユーザ、およびユーザ アクティビティのテーブルに表示されます。

（注） Azure AD レルムユーザーのアクティブセッションは、新しい UI レイアウトの [アクティブセッション（Active Sessions）] にのみ表示され、レガシー UI には表示されません。

表 *1*:アクティブ セッション、ユーザ、およびユーザ アクティビティのフィールドの説明

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
アクティブセッション数（Active Session Count）	ユーザに関連付けられているアクティブセッションの数。	×	対応	×
認証タイプ（Authentication Type）	認証のタイプ：[認証なし（No Authentication）]、[パッシブ認証（Passive Authentication）]、[アクティブ認証（Active Authentication）]、[ゲスト認証（Guest Authentication）]、[失敗した認証（Failed Authentication）]、または [VPN 認証（VPN Authentication）]。 各認証タイプでサポートされるアイデンティティソースの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。	対応	×	対応
ポリシーに使用可能	値 [はい（Yes）] は、ユーザーがユーザー ストア（Active Directory など）から取得されたことを意味します。 値 [いいえ（No）] は、Management Center がそのユーザーのログインのレポートを取得したものの、そのユーザーがユーザーストアに存在しないことを意味します。これは、除外されたグループのユーザーがユーザー ストアにログインした場合に発生することがあります。レルムを設定するときにグループをダウンロード対象から除外することができます。 ポリシーに使用できないユーザーは、Management Center には記録されますが、管理対象デバイスには送信されません。	×	対応	×

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
メンバー数（Count）	（注） [カウント（Count）] フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。 テーブルに応じて、特定の行に表示される情報と一致するセッション、ユーザー、またはアクティビティ イベントの数。	対応	対応	対応
現在の IP（Current IP）	（「現在の IP/ドメイン（Current IP/Domain）」および「IP アドレス（IP address）」も参照してください） ユーザがログインしたホストに関連付けられている IP アドレス。 ユーザにアクティブセッションがない場合、[ユーザ（Users）] テーブルでこのフィールドが空白になります。	対応	×	×
部署名（Department）	ユーザの部署（レルムが取得）。サーバ上のユーザに明示的に関連付けられている部門がない場合、この部門は、サーバが割り当てるいずれかのデフォルト グループとして示されます。たとえば、Active Directory では、これは `Users (ad)` となります。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。	対応	対応	×
説明	セッション、ユーザ、またはユーザ アクティビティについての詳細情報（利用可能な場合）。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
Device	トラフィックベースの検出またはアクティブ認証アイデンティティ ソースによって検出されたユーザ アクティビティの場合は、ユーザを識別したデバイスの名前。 他のタイプのユーザー アクティビティの場合は、管理している側の Management Center になります。 （注） 高可用性展開で VPN を構成した場合、アクティブな VPN セッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。	対応	×	対応
ディスカバリ アプリケーション（Discovery Application）	ユーザの検出に使用されるアプリケーションまたはプロトコル。 • トラフィックベースの検出によって検出されたユーザ アクティビティの場合は、ldap、pop3、imap、oracle、sip、http、ftp、mdns、または aim のいずれか。 （注） ユーザは SMTP ログインに基づいてデータベースに追加されません。 • 他のすべてのユーザ アクティビティの場合：ldap。	対応	対応	対応
[現在の IP ドメイン（Current IP Domain）]/[ドメイン（Domain）]	[アクティブセッション（Active Sessions）] テーブルでは、ユーザー アクティビティが検出されたマルチテナンシー ドメイン。 [ユーザー（Users）] テーブルでは、ユーザーのレルムに関連付けられたマルチテナンシー ドメイン。 [ユーザ アクティビティ（User Activity）] テーブルでは、ユーザ アクティビティが検出されたマルチテナンシー ドメイン。 このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。	対応	対応	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
E メール（Email）	ユーザーのメール アドレス。以下の場合、このフィールドは空白になります。 • AIM ログインによってユーザがデータベースに追加された。 • LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メールアドレスが存在しない。	対応	対応（電子メールとして）	×
終了ポート（End Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の終了値を示します。ユーザの TS エージェントセッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	×	×	対応
エンドポイントロケーション（Endpoint Location）	ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。ISE を設定していない場合、このフィールドは空白です。	×	×	対応
エンドポイントプロファイル（Endpoint Profile）	Cisco ISE によって識別されるユーザのエンドポイント デバイス タイプ。ISE を設定していない場合、このフィールドは空白です。	×	×	対応
イベント	ユーザ アクティビティのタイプ。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
First Name	ユーザの名（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている名がない。	対応	対応	×

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
[IPアドレス（IP Address）]	[ユーザー ログイン（User Login）] ユーザー アクティビティの場合は、次のログインに関連する IP アドレスまたは内部 IP アドレス。 • LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログイン：ユーザのホストのアドレス • SMTP および Oracle のログイン：サーバのアドレス • SIP ログイン：セッション発信者のアドレス （「現在の IP（Current IP）」および「現在の IP/ドメイン（Current IP/Domain）」も参照してください） 関連付けられている IP アドレスは、そのユーザが IP アドレスの現行のユーザであることを意味するわけではありません。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
Last Name	ユーザの姓（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている姓がない。	対応	対応	×
前回の検出（Last Seen）	ユーザのセッションが最後に開始された（またはユーザ データが更新された）日時。	対応	対応	×
ログイン時刻（Login Time）	ユーザのセッションが開始した日時。	対応	×	×
Phone Number	ユーザの電話番号（レルムが取得）。以下の場合、このフィールドは空白になります。 • レルムを設定していない。 • Management Center が、Management Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）。 • サーバに、対象のユーザと関連付けられている電話番号が存在しない。	対応（電話として）	対応	×
レルム	ユーザに関連付けられているアイデンティティ レルム。	対応	対応	対応
セキュリティ グループ タグ（Security Group Tag）	パケットが信頼できる TrustSec ネットワークへ送信されたときに、Cisco TrustSec によって適用される [セキュリティ グループ タグ（Security Group Tag）]（SGT）属性。ISE を設定していない場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（Active Sessions）] テーブル	[ユーザテーブル（Users Table）]	[ユーザアクティビティ（User Activity）] テーブル
セッション時間（Session Duration）	[ログイン時刻（Login Time）] と現在の時刻から計算されたユーザ セッションの期間。	対応	×	×
開始ポート（Start Port）	TS エージェントによってユーザが報告され、そのユーザのセッションが現在アクティブである場合、このフィールドは、ユーザに割り当てられたポート範囲の開始値を示します。ユーザのTSエージェントセッションが非アクティブである場合、またはユーザが別のアイデンティティ ソースによって報告された場合、このフィールドは空白になります。	×	×	対応
時刻（Time）	システムがユーザ アクティビティを検出した時間。	×	×	対応
[ユーザー（User）]	このフィールドには少なくとも、ユーザのレルムとユーザ名が表示されます。たとえば、`Lobby\jsmith` と表示された場合は、Lobby がレルム、jsmith がユーザ名です。 レルムがLDAPサーバから追加のユーザ データをダウンロードし、システムがそれをユーザに関連付けた場合は、このフィールドにユーザの名、姓、タイプも表示されます。たとえば、`John Smith (Lobby\jsmith, LDAP)` と表示された場合は、John Smith がユーザの名前、LDAP がそのタイプです。 （注） トラフィックベースの検出では失敗した AIM ログインが記録される可能性があるため（たとえば、ユーザが正しくないユーザ名を入力した場合など）、Management Center は無効な AIM ユーザを保存する可能性があります。	対応	対応	×
Username	ユーザに関連付けられているユーザ名。	対応	対応	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN 受信バイト数（VPN Bytes In）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Threat Defense がリモートピアまたはクライアントから受信した合計バイト数。 （注） ユーザの VPN セッションが終了した後、受信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN 送信バイト数（VPN Bytes Out）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Threat Defense がリモートピアまたはクライアントに伝送された合計バイト数。 （注） ユーザの VPN セッションが終了した後、送信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応
VPN クライアントのアプリケーション（VPN Client Application）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、リモートユーザーの Cisco Secure Client の AnyConnect VPN モジュール アプリケーション。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN クライアントの国（VPN Client Country）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN クライアントによって報告された国名。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN クライアントの OS（VPN Client OS）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPNによって報告されたリモートユーザーのエンドポイント オペレーティング システム。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN クライアントのパブリック IP（VPN Client Public IP）	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN デバイスのパブリックルーティング可能な IP アドレス。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN 接続期間（VPN Connection Duration）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションがアクティブだった合計時間（HH:MM:SS）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	×	×	対応
VPN 接続プロファイル（VPN Connection Profile）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションで使用される接続プロファイル（トンネル グループ）の名前。接続プロファイルは、リモートアクセス VPN ポリシーに含まれます。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応

フィールド	説明	[アクティブなセッション（**Active Sessions**）] テーブル	[ユーザテーブル（**Users Table**）]	[ユーザアクティビティ（**User Activity**）] テーブル
VPN グループ ポリシー（VPN Group Policy）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、VPNセッションが確立されたときにクライアントに割り当てられたグループ ポリシーの名前。これは VPN 接続プロファイルに関連付けられた静的に割り当てられたグループ ポリシー、またはRADIUS が認証に使用されている場合は動的に割り当てられたグループ ポリシーです。RADIUS サーバによって割り当てられている場合、このグループ ポリシーは VPN 接続プロファイル用に設定された静的ポリシーよりも優先されます。グループ ポリシーは、リモート アクセス VPN ポリシーのユーザ グループに共通の属性を設定します。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応
VPN セッション タイプ（VPN Session Type）	リモート アクセス VPN の報告によるユーザ アクティビティの場合は、セッションのタイプ（[LAN 間（LAN-to-LAN）] または [リモート（Remote）]）。 他のタイプのユーザアクティビティの場合、このフィールドは空白です。	対応	×	対応

アクティブ セッション データ

[分析（Analysis）] > **[ユーザ（Users）]** > **[アクティブなセッション（Active Sessions）]** ワークフローには、現在のユーザ セッションに関する選択情報が表示されます。ネットワーク上のユーザーが複数のセッションを同時に実行するとき、システムは次の場合にセッションを一意に識別できます。

- 一意の **IP アドレス**値を持っている。
- Cisco Terminal Services（TS）エージェントによって提供される、一意の**開始ポート**値と**終了ポート**値を持っている。
- 一意の**現在の IP ドメイン**値を持っている。
- 異なるアイデンティティ ソースによって認証された。
- 異なるアイデンティティ レルムと関連付けられた。

システムによって保存されるユーザおよびユーザ アクティビティ データの詳細については、ユーザー データ（User Data） （65 ページ） およびユーザー アクティビティ データ （68 ページ） を参照してください。

一般的なユーザー関連イベントのトラブルシューティングとリモートアクセス VPN のトラブルシューティングの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「the *Troubleshoot Realms and User Downloads*」および「*VPN Troubleshooting*」を参照してください。

アクティブ セッション データの表示

アクティブ セッションのテーブルを表示して、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

手順

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用している場合は、**[分析（Analysis）] > [ユーザー（Users）] > [アクティブセッション（Active Sessions）]** をクリックします。
- アクティブ セッションのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [アクティブなセッション（Active Sessions）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べるには、アクティブ セッション データ （63 ページ） およびユーザー関連フィールド （52 ページ） を参照してください。

ユーザー データ（User Data）

アイデンティティ ソースが、データベースに存在しないユーザーのユーザー ログインを報告した場合、そのログイン タイプが特に制限されていない限り、そのユーザーはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザ データベースを更新します。

- Management Center のユーザーが、[ユーザー（Users）] テーブルから権限のないユーザーを手動で削除する。
- アイデンティティ ソースが、そのユーザによるログオフを報告する。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE によって報告されたホスト データを使用してユーザー制御を実行することはできません。

システムによって検出されたユーザ ログインのタイプに応じて、新しいユーザのどの情報が保存されるかが決まります。

ID ソース	ログイン タイプ	格納されるユーザ データ
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• ユーザ名 • 現行の IP アドレス • セキュリティ グループ タグ（SGT）（ISE-PIC ではサポートされていない） • エンドポイントのプロファイル/デバイス タイプ（ISE-PIC ではサポートされていない） • エンドポイントの場所/場所 IP（ISE-PIC ではサポートされていない） • タイプ（LDAP）

ID ソース	ログイン タイプ	格納されるユーザ データ
TS エージェント	Active Directory	• ユーザ名 • 現行の IP アドレス • 開始ポート • 終了ポート • タイプ（LDAP）
キャプティブ ポータル	Active Directory LDAP	• ユーザ名 • 現行の IP アドレス • タイプ（LDAP）
トラフィック ベースの検出	LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • タイプ（AD）
	POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • タイプ（`pop3` または `imap`）

（注） このテーブルには、Microsoft Azure Active Directory ユーザーに関するデータは表示されません。

ユーザを自動的にダウンロードするようにレルムを設定すると、Management Center は指定した間隔に基づいてサーバに対するクエリを実行します。システムが新しいユーザのログインを検出してから、Management Center データベースがユーザのメタデータを更新するまでに、5～10 分かかることがあります。Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- ユーザ名
- 姓と名

- 電子メール アドレス
- 部署
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ（SGT）（使用可能な場合）
- エンドポイントのプロファイル（使用可能な場合）
- エンドポイントの場所（使用可能な場合）
- 開始ポート（使用可能な場合）
- 終了ポート（使用可能な場合）

Management Center がデータベースに格納できるユーザの数は、Management Center のモデルによって異なります。ホストに対して権限を持たないユーザがログインしていることが検出された場合、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることができます。ただし、ホストに対して権限を持つユーザのログインが検出された後は、権限を持つ別のユーザがログインした場合にのみ、現行ユーザが変わります。

AIM、Oracle、および SIP のログインがトラフィックベースで検出された場合は、システムが LDAP サーバから取得したどのユーザ メタデータにも関連付けられないため、これらのログインにより重複したユーザ レコードが作成されることに注意してください。これらのプロトコルから重複したユーザ レコードを取得することに起因するユーザ カウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザを検索、表示、削除することができます。また、データベースからすべてのユーザを消去することもできます。

一般的なユーザー関連のイベント トラブルシューティングについては、Cisco Secure Firewall Management Center デバイス構成ガイド を参照してください。

ユーザー データの表示

ユーザーのテーブルを表示して、検索する情報に応じてイベント ビューを操作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ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザが記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

手順

ステップ 1 次のように、ユーザ データにアクセスします。

- 事前定義されたワークフローを使用する場合は、**[分析（Analysis）]**>**[ユーザー（Users）]**>**[ユーザー（Users）]** を選択します。
- ユーザのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ（Users）] を選択します。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザー関連フィールド （52 ページ）を参照）。

ユーザー アクティビティ データ

システムは、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムがユーザアクティビティを検出すると、そのユーザアクティビティデータはデータベースに記録されます。ユーザアクティビティは、表示、検索、および削除することも、すべてのユーザ アクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

システムは、ユーザーアクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザ アクティビティは、相関ルールで使用することもできます。相関ルールは、ユーザ アクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相関ルールが相関ポリシーで使用される場合、ネットワーク トラフィックが条件を満たしたときは、相関ルールが修復およびアラートの応答を起動します。

（注） ISE/ISE-PIC が設定されている場合は、ユーザ テーブルにホスト データが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE によって報告されたホスト データを使用してユーザー制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

新しいユーザのアイデンティティ（New User Identity）

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

ユーザ ログイン（User Login）

このタイプのイベントは、次のことが発生した後に生成されます。

- キャプティブ ポータルのユーザー認証の実行が成功または失敗した。
- トラフィック ベースの検出がユーザ ログインの成功または失敗を検出した。

（注） トラフィック ベースの検出で検出された SMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、権限のあるユーザーがそのホストにログインした後は、別の権限のあるユーザーによるログインだけが現行ユーザーを変更します。

キャプティブ ポータルまたはトラフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ認証データについて、次の点に注意してください。

- トラフィック ベースの検出（LDAP、IMAP、FTP、および POP3 トラフィック）から報告された失敗したログインは、ユーザアクティビティのテーブル ビューに表示されますが、ユーザのテーブル ビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗した場合、システムではそのユーザ名として [失敗した認証（Failed Authentication）] を使用します。
- キャプティブ ポータルから報告された失敗した認証は、ユーザ アクティビティのテーブル ビューとユーザのテーブル ビューの両方に表示されます。既知のユーザが認証に失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

ユーザのアイデンティティの削除（Delete User Identity）

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

ドロップ（廃棄）されたユーザのアイデンティティ：ユーザ制限に到達（User Identity Dropped: User Limit Reached）

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザー制限に達すると、ほとんどの場合、データベースへの新しいユーザーの追加が停止されます。新しいユーザーを追加するには、古いユーザーまたは非アクティブなユーザーをデータベースから手動で削除するか、データベースからすべてのユーザーを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

ユーザの侵害の兆候イベント

次のユーザの IOC の変化がユーザ アクティビティ データベースに記録されます。

- 侵害の兆候が解決された場合。
- 侵害の兆候ルールがユーザーに対して有効または無効にされた場合。

一般的なユーザー関連のイベント トラブルシューティングについては、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ユーザー アクティビティ データの表示

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ユーザー アクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。ユーザアクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザ アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザの詳細が含まれている、ユーザの詳細ページで終了します。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 次のように、ユーザ アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、**[分析（Analysis）]** > **[ユーザー（Users）]** > **[ユーザーアクティビティ（User Activity）]** を選択します。
- ユーザ アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックして [ユーザ アクティビティ（User Activity）] を選択します。

ヒント イベントが表示されない場合は、時間範囲の調整が必要な可能性があります（時間枠の変更を参照）。

ステップ 2 次の選択肢があります。

- [(ワークフローの切り替え)（(switch workflow)）]をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します（ディスカバリおよびアイデンティティ ワークフローの使用 （7 ページ）を参照）。
- テーブルのカラムの内容について詳しく調べます（ユーザー関連フィールド （52 ページ）を参照）。

ユーザー プロファイルとホスト履歴

特定のユーザーの詳細については、[ユーザー（User）]ポップアップ ウィンドウを表示して確認することができます。表示されるページ（このマニュアルでは「ユーザ プロファイル」と呼んでいます）には、Web インターフェイスで「ユーザのアイデンティティ（User Identity）」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザー データを他の種類のイベントに関連付けるすべてのイベント ビュー
- アクティブなセッションのテーブル ビュー
- ユーザーのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザー データは、ユーザーのテーブル ビューで表示されるものと同じです。

[侵害の兆候（Indications of Compromise）] セクション

このセクションについては、次のセクションを参照してください。

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Indications of Compromise*」
- 侵害の兆候データ フィールド （32 ページ）
- 単一ホストまたはユーザにおける侵害の兆候のルール状態の編集 （33 ページ）
- 侵害の兆候タグの解決 （34 ページ）
- 侵害の兆候のタグのソース イベントの表示 （33 ページ）

[ホストの履歴（Host History）] セクション

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザーがログインおよびログオフしたホストの IP アドレスのリストには、ログインとログアウトの概算時間が棒グラフで示されます。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メール サーバに対する定期的な自

動ログインは複数回の短時間のセッションとして示されますが、（勤務時間中などの）長時間のログインは、長時間のセッションとして示されます。

トラフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザの履歴データベースに格納されます。このデータベースには、デフォルトで 1000 万のユーザ ログイン イベントが格納されます。ホストの履歴に特定のユーザーに関するデータが表示されない場合、そのユーザーが非アクティブであるか、またはデータベースの制限を増やさなければならないことがあります。

関連トピック

ユーザー データのフィールド

ユーザの詳細およびホスト履歴の表示

手順

以下の 2 つの対処法があります。

- ユーザーをリストする任意のイベントビューで、ユーザー ID の**ユーザーアイコン**、または、侵入の痕跡に関連付けられているユーザーの場合は**赤色のユーザーアイコン**の横に表示されるユーザーをクリックします。
- いずれかのユーザ ワークフローで、[ユーザ（Users）] の最終ページをクリックします。

検出イベントの操作の履歴

表 *2*:

機能	最小 Management Center	最小 Threat Defense	詳細
脆弱性ページの変更	6.7	任意（Any）	Bugtraq とその脆弱性データは使用できなくなりました。次の変更が行われました。 • 現在、ほとんどの脆弱性データは National Vulnerability Database（NVD）から取得されています。 • 廃止された冗長なフィールドが削除されました。 • 新しい [CVE ID] 列がテーブルビューに追加され、新しい [シビラティ（重大度）（Severity）] フィールドがテーブルと詳細のページに追加されました。 • テーブルで CVE ID を右クリックすると、NVD のその脆弱性に関する詳細を表示できるようになりました。 • テーブルの [脆弱性の影響（Vulnerability Impact）] 列の名前が [影響（Impact）] に変更されました。（詳細ビューのフィールド名は変更されていません。） • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] > [ホスト（Hosts）] でホストプロファイルの脆弱性を表示するときに、脆弱性の詳細（サードパーティの脆弱性を除く）により新しい一連のフィールドが使用されます。 • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] > [脆弱性（Vulnerabilities）] ページの [脆弱性（Vulnerabilities）] オプションから、[Bugtraq] オプションが削除されました。 変更された画面： • [分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）] の下のすべてのページ • [分析（Analysis）] > [ホスト（Hosts）] > [ネットワークマップ（Network Map）] ページの [ホスト（Hosts）] タブと [脆弱性（Vulnerabilities）] タブ サポート対象プラットフォーム： 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。