ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリ

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

マルウェアの影響を特定して軽減しやすくするため、Firepowerシステムのファイル制御、ネットワーク ファイル トラジェクトリ、およびネットワーク向け*AMP*の各コンポーネントによって、アーカイブ ファイル内のマルウェア ファイルとネストされたファイルを含むファイルの伝送を検出、追跡、キャプチャ、分析、ログ記録、および必要に応じてブロックできます。

また、システムを組織の *AMP for Endpoints* の展開に統合して、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候（IOC）をインポートできます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

（注） Firepower システムでは、Unicode（UTF-8）文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

ファイルおよびマルウェア イベント

Firepower Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイル イベントとは、ネットワーク向け AMP によって検出されたマルウェアを含むファイルを意味します。ファイル イベントには、AMP for Endpoints 関連のフィールドは含まれません。
- マルウェア イベントとは、ネットワーク向け AMP または AMP for Endpoints によって検出されたマルウェアを意味します。また、マルウェア イベントは、スキャンや検疫など、AMP for Endpoints の導入からの脅威以外のデータを記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、ネットワーク向け AMP によって検出されたファイルを意味します。

（注） ネットワーク向け AMP によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。

ファイル イベントおよびマルウェア イベントの種類

ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Firepower Management Center データベースへの関連する接続の終わりも記録します。

ネットワークベースのマルウェア イベント（ネットワーク向け AMP）

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。ネットワーク向け AMP は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテクスチュアルデータを含むマルウェア イベントを生成できます。

表 *1*：ネットワーク向け *AMP* でのマルウェア イベントの生成シナリオ

ネットワーク向け AMP によるファイル検出時の動作	性質
AMP クラウドにファイルの性質についてクエリを行い（マルウェア クラウド ルックアップを実行）、クエリに成功した場合	マルウェア、クリーン、または不明
AMP クライドにクエリを行ったものの、接続を確立できないか、他の理由でクライドが利用可能でない場合	応対不可 この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカルマルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合（手動でマルウェアとしてマークされている場合）	カスタム検出
ファイルがクリーン リストに設定されている場合（手動でクリーンとしてマークされている場合）	クリーン

レトロスペクティブ マルウェア イベント（ネットワーク向け AMP）

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。たとえば、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。先週クエリしたファイルの性質が変わると、AMP クラウドがシステムに通知します。その場合、以下の 2 つが行われます。

- Firepower Management Center が新しいレトロスペクティブ マルウェア イベントを生成します。

  この新しいレトロスペクティブ マルウェア イベントは、前の週に検出され、同じ SHA-256 ハッシュ値を持つ同じすべてのファイルの性質変更を表します。そのため、これらのイベントには限られた情報（Firepower Management Center に性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、および脅威名）が含まれます。IP アドレスや他のコンテキスト情報は含まれません。

- Firepower Management Center はレトロスペクティブ イベントの関連する SHA-256 ハッシュ値を持つすでに検出済みのファイルのファイル性質を変更します。

  ファイルの性質が Malware に変更されると、Firepower Management Center は新しいマルウェアイベントをデータベースに記録します。新しい性質を除き、この新しいマルウェアイベントの情報は、ファイルが最初に検出されたときに生成されたファイルイベントのものと同じです。

  ファイルの性質が [クリーン（Clean）] に変更された場合、Firepower Management Center はそのマルウェアイベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が [クリーン（Clean）] のファイルが含められることがありますが、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

エンドポイントベースのマルウェア イベント（AMP for Endpoints）

組織で AMP for Endpoints を使用している場合は、個々のユーザがエンドポイントに軽量コネクタ（コンピュータおよびモバイルデバイス）を取り付けます。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタは AMP クラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロッキング、クラウドリコールなど、他の種類のデータを Firepower Management Center に送信することもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

（注） エンドポイントベースのマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（そして、モニタ対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、AMP for Endpoints によってモニタされる組織内のエンドポイントが、ネットワーク向け AMP によってモニタされているものと同じホストではない可能性があります。

ファイルおよびマルウェア イベントのワークフローの使用

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	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

イベント ビューアでは、テーブルにファイルイベントとマルウェアイベントを表示できます。分析に関連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。イベントにアクセス

したときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。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。

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

次のいずれかを実行します。

- **[分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（File Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [マルウェア イベント（Malware Events）]**

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

ヒント 特定のファイルが検出された接続をすぐに表示するには、イベント ビューアーでチェック ボックスを使用してファイルを選択してから、[ジャンプ（Jump to）] ドロップダウン リストで [接続イベント（Connections Events）] を選択します。

関連トピック

ファイルおよびマルウェア イベント フィールド （5 ページ）
定義済みファイルのワークフロー
定義済みマルウェアのワークフロー
イベント ビュー設定の設定

ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェア イベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。

（注） ネットワーク向け AMP によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。また、ファイル イベントには AMP for Endpoints 関連のフィールドはありません。

アクション（Action）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

AMP クラウド（AMP Cloud）

AMP for Endpoints イベントが発信された AMP クラウドの名前。

アプリケーション ファイル名（Application File Name）

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

アプリケーション ファイル SHA256（Application File SHA256）

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

アプリケーション プロトコル（Application Protocol）

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーション プロトコル。

アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

アーカイブ深度（Archive Depth）

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

アーカイブ名（Archive Name）

マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の名前。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア行を右クリックしてコンテキスト メニューを開き、[アーカイブ コンテンツの表示（View Archive Contents）] をクリックします。

アーカイブ SHA256（Archive SHA256）

マルウェア ファイルが関連付けられているアーカイブ ファイル（存在する場合）の SHA-256 ハッシュ値。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア行を右クリックしてコンテキスト メニューを開き、[アーカイブ コンテンツの表示（View Archive Contents）] をクリックします。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

カテゴリ（Category）/ファイル タイプ カテゴリ（File Type Category）

ファイルタイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

クライアント（Client）

1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。

クライアント カテゴリまたはタグ（Client Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

メンバー数（Count）

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

検出名（Detection Name）

検出されたマルウェアの名前。

ディテクタ（Detector）

マルウェアを識別した AMP for Endpoints ディテクタ（ClamAV、Spero、SHA など）。

Device

ファイル イベントおよびネットワークベースのマルウェア イベントの場合、ファイルを検出したデバイスの名前。

エンドポイントベースのマルウェア イベントおよび AMP クラウドによって生成される遡及的マルウェア イベントの場合、Firepower Management Center の名前。

傾向（Disposition）/ファイル性質（File Disposition）

ファイルの性質：

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイル ポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

クリーン（Clean）

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

不明

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを正しく分類していませんでした。

カスタム検出（Custom Detection）

ユーザがカスタム検出リストにファイルを追加したことを示します。

応対不可（Unavailable）

システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

該当なし

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイル性質は、システムが AMP クラウドに問い合わせたファイルでのみ表示されます。

ドメイン（Domain）

ファイル イベントおよびネットワークベースのマルウェア イベントの場合、ファイルを検出したデバイスのドメイン。エンドポイントベースのマルウェア イベントおよびAMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

イベント サブタイプ（Event Subtype）

マルウェア検出につながった AMP for Endpoints アクション（[作成（Create）]、[実行（Execute）]、[移動（Move）]、[スキャン（Scan）] など）。

イベント タイプ（Event Type）

マルウェア イベントのサブタイプ。

ファイル名（File Name）

マルウェア ファイルの名前。

ファイル パス（File Path）

AMP for Endpoints によって検出されたマルウェア ファイルのファイル パス（ファイル名を含まない）。

ファイル ポリシー（File Policy）

ファイルを検出したファイル ポリシー。

ファイル ストレージ（File Storage）/保存（Stored）（検索のみ）

イベントに関連付けられたファイルのストレージ ステータス：

保存（Stored）

関連するファイルが現在保存されているすべてのイベントを返します。

関連保存（Stored in connection）

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

失敗しました（Failed）

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

ファイルのタイムスタンプ（File Timestamp）

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

HTTP 応答コード（HTTP Response Code）

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータス コード。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

メッセージ（Message）

マルウェア イベントに関連付けられる追加情報。ファイル イベントおよびネットワーク ベースのマルウェア イベントでは、このフィールドは、性質が変更された、つまり関連付けられた遡及的イベントがあるファイルに対してのみ入力されます。

受信側の大陸（Receiving Continent）

ファイルを受信するホストの大陸。

受信側の国（Receiving Country）

ファイルを受信するホストの国。

受信側 IP（Receiving IP）

ファイル イベントおよびネットワークベースのマルウェア イベントの場合、ファイルを受信するホストの IP アドレス。エンドポイント ベースのマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

受信側のポート（Receiving Port）

ファイルが検出されたトラフィックによって使用される宛先ポート。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの ASA FirePOWER だけです。

送信側の大陸（Sending Continent）

ファイルを送信するホストの大陸。

送信側の国（Sending Country）

ファイルを送信するホストの国。

送信側 IP（Sending IP）

ファイルを送信するホストの IP アドレス。

送信側のポート（Sending Port）

ファイルが検出されたトラフィックによって使用される送信元ポート。

SHA256/ファイル SHA256（File SHA256）

ファイルの SHA-256 ハッシュ値と、最後に検出されたファイル イベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン、およびネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコン。SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。

- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール
- AMP for Endpoints

サイズ（KB）（Size (KB)）/ファイル サイズ（KB）（ファイル サイズ（KB））

ファイルのサイズ（KB 単位）。ファイルが完全に受信される前にシステムがファイルのタイプを判別すると、ファイルサイズが計算されずに、このフィールドがブランクになる場合があるので注意してください。

SSL の実際の動作（SSL Actual Action）（検索のみ）

システムが暗号化トラフィックに適用したアクション。

ブロック（Block）/リセットしてブロック（Block With Reset）

ブロックされた暗号化接続を表します。

複合（再署名）（Decrypt (Resign)）

再署名サーバ証明書を使用して復号された発信接続を表します。

復号（キーの置き換え）（Decrypt (Replace Key)）

置き換えられた公開キーと自己署名サーバ証明書を使用して復号された発信接続を表します。

復号（既知のキー）（Decrypt (Known Key)）

既知の秘密キーを使用して復号された着信接続を表します。

デフォルト アクション（Default Action）

接続がデフォルト アクションによって処理されたことを示しています。

復号しない（Do Not Decrypt）

システムが復号しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL 証明書情報（SSL Certificate Information）（検索のみ）

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- 件名/発行元共通名（Subject/Issuer Common Name）
- 件名/発行元組織（Subject/Issuer Organization）
- 件名/発行元組織ユニット（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）、証明書フィンガープリント（Certificate Fingerprint）

- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）（検索のみ）

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明
- 不一致（No Match）
- Success
- キャッシュされないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- SSL 圧縮の使用（SSL Compression Used）
- パッシブ モードで復号できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号化エラー（Decryption Error）
- 保留サーバ名カテゴリ ルックアップ（Pending Server Name Category Lookup）
- 保留共通名カテゴリ ルックアップ（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- ネットワーク パラメータを使用できません（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- サーバ証明書フィンガープリントを使用できません（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできません（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできません（Cannot Cache Issuer DN）
- 不明の SSL バージョン（Unknown SSL Version）
- 外部証明書リストを使用できません（External Certificate List Unavailable）
- 外部証明書フィンガープリントを使用できません（External Certificate Fingerprint Unavailable）
- 内部証明書リストが無効です（Internal Certificate List Invalid）
- 内部証明書リストを使用できません（Internal Certificate List Unavailable）
- 内部証明書を使用できません（Internal Certificate Unavailable）

- 内部証明書フィンガープリントを使用できません（Internal Certificate Fingerprint Unavailable）
- サーバ証明書検証を使用できません（Server Certificate Fingerprint Unavailable）
- サーバ証明書検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルトアクション、または復号できないトラフィック アクション）に関連したアクション。ロック アイコン（  ）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

SSL 件名/発行元国（SSL Subject/Issuer Country）（検索のみ）

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

脅威名（Threat Name）

検出されたマルウェアの名前。

脅威スコア（Threat Score）

そのファイルに関連する最新の脅威スコア。脅威スコア アイコンは、[動的分析要約（Dynamic Analysis Summary）] レポートにリンクされています。

時刻（Time）

イベントが生成された日時。このフィールドは検索できません。

タイプ（Type）/ファイル タイプ（File Type）

ファイルのタイプ（HTML や MSEXE など）。

URI（URI）/ファイル URI（File URI）

ファイルの送信元の URI（ファイルをダウンロードした URL など）。

ユーザ（User）

イベントが発生したホスト（**受信 IP**）のユーザ

ファイルイベントおよびネットワークベースのマルウェアイベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、ユーザがマルウェア ファイルをアップロードしたマルウェア イベントに、ユーザは関連付けられていません。

エンドポイントベースのマルウェア イベントの場合、AMP for Endpoints がユーザ名を判別します。これらのユーザをユーザ検出または制御に関連付けることは**できません**。それらは[ユーザ（Users）] テーブルに含まれず、それらのユーザの詳細を表示することもできません。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックについて、内容を表すまたは URL を要求したアプリケーション。

Web アプリケーションのカテゴリまたはタグ（Web Application Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

マルウェア イベントのサブタイプ

次の表に、マルウェア イベントのサブタイプと、ネットワークベースまたはエンドポイントベースのマルウェアイベントにそのサブタイプを指定できるかどうか、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 *2:* マルウェア イベントのタイプ

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（Threat Detected in Network File Transfer）	Yes	No	Yes
ネットワーク ファイル転送時に検出された脅威（遡及的）（Threat Detected in Network File Transfer (retrospective)）	Yes	No	Yes
検出された脅威（Threat Detected）	No	Yes	Yes

マルウェア イベントのサブタイプ/検索値	ネットワーク向け **AMP**	エンドポイント向け **AMP**	ファイル トラジェクトリ
除外項目内で検出された脅威（Threat Detected in Exclusion）	No	Yes	Yes
検疫された脅威（Threat Quarantined）	No	Yes	Yes
AMP IOC（侵害の兆候）（AMP IOC (Indications of compromise)）	No	Yes	No
ブロックされた実行（Blocked Execution）	No	Yes	No
隔離のクラウドリコール（Cloud Recall Quarantine）	No	Yes	No
隔離のクラウドリコールの試行に失敗（Cloud Recall Quarantine Attempt Failed）	No	Yes	No
隔離のクラウドリコールの開始（Cloud Recall Quarantine Started）	No	Yes	No
隔離からのクラウドリコールの復元（Cloud Recall Restore from Quarantine）	No	Yes	No
隔離からのクラウドリコールの復元に失敗（Cloud Recall Restore from Quarantine Failed）	No	Yes	No
隔離からのクラウドリコールの復元の開始（Cloud Recall Restore from Quarantine Started）	No	Yes	No
隔離エラー（Quarantine Failure）	No	Yes	No
隔離されたアイテムの復元（Quarantined Item Restored）	No	Yes	No

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
隔離の復元に失敗（Quarantine Restore Failed）	No	Yes	No
隔離の復元の開始（Quarantine Restore Started）	No	Yes	No
スキャン完了、検出なし（Scan Completed, No Detections）	No	Yes	No
スキャンが検出ありで完了（Scan Completed With Detections）	No	Yes	No
スキャンに失敗（Scan Failed）	No	Yes	No
スキャン開始（Scan Started）	No	Yes	No

ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェア イベント フィールドの情報を表示するかどうかを示します。すべてのフィールドがすべてのイベントに読み込まれるわけではないことに留意してください。次に例を示します。

- ネットワーク向け AMP はネットワーク トラフィックでマルウェア ファイルを検出することから、ファイル イベントおよびネットワークベースのマルウェア イベントには、ファイルの送信に使用された接続に関する、ポート、アプリケーション プロトコル、および送信元 IP アドレスの情報が含まれます。
- エンドポイント向け AMP の展開からインポートされたマルウェア イベントと侵害の兆候（IOC）には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報（ファイル パス、呼び出し元クライアント アプリケーションなど）が含まれています。
- ファイル イベント テーブル ビューには、エンドポイント向け AMP 関連のフィールドは表示されません。

表 *3:* ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイル イベント	ネットワーク向け **AMP** マルウェア イベント	ネットワーク向け **AMP** レトロスペクティブ イベント	エンドポイント向け **AMP** マルウェア イベント
操作（Action）	Yes	Yes	Yes	No

フィールド	ファイル イベント	ネットワーク向けAMP マルウェア イベント	ネットワーク向けAMP レトロスペクティブイベント	エンドポイント向け AMP マルウェア イベント
AMP クラウド（AMP Cloud）	No	No	No	Yes
アプリケーションファイル名（Application File Name）	No	No	No	Yes
アプリケーションファイル SHA256（Application File SHA256）	No	No	No	Yes
アプリケーションプロトコル	Yes	Yes	No	No
アプリケーションプロトコルカテゴリまたはタグ（Application Protocol Category or Tag）	Yes	Yes	Yes	No
アプリケーションのリスク（Application Risk）	Yes	Yes	Yes	No
アーカイブ深度（Archive Depth）	Yes	Yes	No	Yes
アーカイブ名（Archive Name）	Yes	Yes	No	Yes
アーカイブ SHA256（Archive SHA256）	Yes	Yes	No	Yes
ビジネスとの関連性（Business Relevance）	Yes	Yes	Yes	No
カテゴリ/ファイル タイプ カテゴリ（Category / File Type Category）	Yes	Yes	No	Yes
クライアント（Client）	Yes	Yes	Yes	No

フィールド	ファイル イベント	ネットワーク向けAMP マルウェア イベント	ネットワーク向けAMP レトロスペクティブイベント	エンドポイント向け AMP マルウェア イベント
クライアント カテゴリまたはタグ（Client Category or Tag）	Yes	Yes	Yes	No
メンバー数（Count）	Yes	Yes	Yes	Yes
検出名（Detection Name）	No	Yes	No	No
ディテクタ（Detector）	No	No	No	Yes
Device	Yes	Yes	Yes	Yes
処理/ファイルの処理（Disposition / File Disposition）	Yes	Yes	Yes	No
ドメイン（Domain）	Yes	Yes	Yes	Yes
イベント サブタイプ（Event Subtype）	No	No	No	Yes
イベント タイプ（Event Type）	No	Yes	Yes	Yes
ファイル名（File Name）	Yes	Yes	No	Yes
ファイル パス（File Path）	No	No	No	Yes
ファイル ポリシー（File Policy）	Yes	No	No	No
ファイルのタイムスタンプ（File Timestamp）	No	No	No	Yes
HTTP 応答コード（HTTP Response Code）	Yes	Yes	No	No
IOC（侵害の兆候）（IOC (Indication of Compromise)）	No	Yes	Yes	Yes

フィールド	ファイル イベント	ネットワーク向けAMP マルウェア イベント	ネットワーク向けAMP レトロスペクティブイベント	エンドポイント向け AMP マルウェア イベント
メッセージ（Message）	Yes	Yes	No	Yes
受信側の大陸（Receiving Continent）	Yes	Yes	Yes	No
受信側の国（Receiving Country）	Yes	Yes	No	No
受信側 IP（Receiving IP）	Yes	Yes	No	Yes
受信側のポート（Receiving Port）	Yes	Yes	No	No
セキュリティ コンテキスト（Security Context）	Yes	Yes	Yes	Yes
送信側の大陸（Sending Continent）	Yes	Yes	Yes	No
送信側の国（Sending Country）	Yes	Yes	No	No
送信側 IP（Sending IP）	Yes	Yes	No	No
送信側のポート（Sending Port）	Yes	Yes	No	No
SHA256/ファイル SHA256（SHA256 / File SHA256）	Yes	Yes	Yes	Yes
サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）	Yes	Yes	No	Yes
SSL の実際のアクション（SSL Actual Action）（検索のみ）	Yes	Yes	No	No

フィールド	ファイル イベント	ネットワーク向けAMP マルウェア イベント	ネットワーク向けAMP レトロスペクティブイベント	エンドポイント向け AMP マルウェア イベント
SSL 証明書情報（SSL Certificate Information）（検索のみ）	Yes	Yes	No	No
SSL 障害の理由（SSL Failure Reason）（検索のみ）	Yes	Yes	No	No
SSL ステータス（SSL Status）	Yes	Yes	No	No
SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）	Yes	Yes	No	No
ファイル ストレージ/保存済み（File Storage / Stored）（検索のみ）	Yes	Yes	No	No
脅威名（Threat Name）	No	Yes	Yes	Yes
脅威スコア（Threat Score）	Yes	Yes	No	No
時刻（Time）	Yes	Yes	Yes	Yes
タイプ/ファイル タイプ（Type / File Type）	Yes	Yes	No	Yes
URI/ファイル URI（URI / File URI）	Yes	Yes	No	No
ユーザ（User）	Yes	Yes	No	Yes
Webアプリケーション（Web Application）	Yes	Yes	Yes	No
Webアプリケーション カテゴリまたはタグ（Web Application Category or Tag）	Yes	Yes	Yes	No

ローカル マルウェア分析（Local Malware Analysis）

ローカル マルウェア分析では、管理対象デバイスで Cisco Talos Security Intelligence and Research Group（Talos）から提供される検出ルールを使用して、実行可能ファイル、PDF、Office 文書、およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカル マルウェア分析ではファイルを AMP クラウドに送信する必要はなく、ファイルを実行することもしないので、時間とシステム リソースを節約できます。

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明（Unknown）] から [マルウェア（Malware）] に更新します。その上で、システムは新しいマルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を [不明（Unknown）] から [正常（Clean）] に更新することはしません。ローカル マルウェア分析を実行した後、システムはファイル情報（SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など）をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。

イベント ビューアで、コンテキスト メニューを使用してローカル マルウェア分析用にファイルを 1 つずつ手動で送信することも、最大 25 個のキャプチャ済みフィルを同時に送信することもできます。システムはローカル分析を実行してから、それらのファイルをダイナミック分析対象としてクラウドに送信します。ただし、ローカル分析がファイル ポリシーで有効になっておらず、分析用のファイルを手動で送信する場合は、ファイルが動的分析用としてしか送信されません。

ローカル マルウェア分析では、AMP Threat Grid クラウドとの通信を確立する必要はありません。ただし、マルウェアとして事前に分類したファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカルマルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

ファイル構成

ローカルマルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイル タイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

動的分析（Dynamic Analysis）

AMP クラウドの精度を改善し、追加のマルウェア分析および脅威の特定を提供するには、AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスに、キャプチャさ

れた適格なファイルを動的分析用に送信します。AMP クラウドでは、ファイルがサンドボックス環境で実行され、ファイルにマルウェアが含まれているかどうかが判別されます。

動的分析用にファイルを送信できるかどうかは、次によって異なります。

- ファイル タイプ
- ファイル サイズ
- ファイル ルールのアクション
- 自動送信用にマルウェアとしてシステムで事前に分類されたファイル

マルウェアをブロックするか、マルウェア クラウド ルックアップを実行するようにルールが設定されている場合は、不明または使用不可の性質を持つ一致するファイルのみが送信されます。

AMP Threat Grid クラウドでは、動的分析用にファイルがキューに登録され、各ファイルがサンドボックス環境で実行されます。クラウドは、ファイルにマルウェアが含まれている確率の詳細を示す脅威スコアを返します。脅威スコアが定義されているしきい値を超えるファイルを自動的にブロックできます。

イベント ビューア、キャプチャされたファイル ビュー、またはネットワーク ファイル トラジェクトリから、ファイルが動的分析用に送信されたかどうかの特定、ローカルマルウェアおよびファイルの動的分析用の手動送信、またはクラウドに脅威スコアが割り当てられている理由のサマリーの表示を行うことができます。また、動的分析のサマリー レポートも取得できます。これには、全体的な脅威スコアを構成する各種評価、およびクラウドによるファイル実行の試行時に開始されたその他のプロセスが示されます。

自動ダイナミック分析と Spero 分析

ファイル ポリシーは、マルウェアとして事前分類されたファイルを自動的にダイナミック分析に提出するように設定できます。

クエリ対象にするファイルを自動的に Spero 分析に提出することで、ダイナミック分析を補足することができます。Spero 分析は SHA-256 ハッシュ値の分析を補うもので、実行可能ファイル内のマルウェアをより正確に識別できます。

Spero 分析では、ファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいて Spero シグネチャを生成した後、デバイスはそれを AMP クラウド内の Spero ヒューリスティック エンジンに送信します。Spero シグネチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが返します。現時点のファイル処理が [不明（Unknown）] であれば、システムは [マルウェア（Malware）] のファイル処理を割り当てます。

Spero 分析のために実行可能ファイルを送信できるのは、検出時だけなので注意してください。後から手動で送信することはできません。ダイナミック分析にはファイルを送信せずに、Spero 分析にのみファイルを送信することもできます。

動的分析用のファイルの手動送信

イベント ビューア、コンテキスト メニュー、ネットワーク ファイル トラジェクトリから、保管されたファイルをダイナミック分析の対象として手動で送信できます。キャプチャ ファイル ビュー（[分析（Analysis）] > [ファイル（Files）] > [キャプチャ ファイル（Captured Files）]）から、一度に最大 25 個の保存済みファイルを手動で送信できます。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（.swf、.jar など）も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。

ローカル分析がファイル ポリシー内で有効になっておらず、分析用のファイルを手動で送信する場合は、ファイルが動的分析用としてしか送信されません。

（注） 動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムは AMP クラウドを検査します（この検査は、一日に 1 回だけ行われます）。

動的分析とキャパシティ処理

容量処理によって、現在、ファイルを動的分析のためにクラウドに送信できない場合に一時的にデバイスでファイルを保存できます。デバイスでは、そのハード ドライブまたはマルウェア ストレージ パックにファイルが保存されます。

システムでは、動的分析を有効にして、マルウェア クラウド ルックアップを実行する任意のファイルを一時的に保存できます。ファイルがマルウェアとして事前に分類されており、デバイスがクラウドへの最大送信数に到達したか、クラウドと通信できない場合に、システムはこのファイルを保存します。

デバイスでは、次のいずれかの場合に保存されているファイルがクラウドに再送信されます。

- デバイスがクラウドと通信できず、クラウド コミュニケーションを再確立する場合
- デバイスがクラウドへの最大送信数に到達し、十分な時間が経過した場合

脅威スコアと動的分析のサマリ レポート

脅威スコア

表 *4:* 脅威スコア レーティング

脅威スコア	アイコン
Low	●○○○

脅威スコア	アイコン
Medium	
High	
Very High	

Firepower Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後から検出されると、AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスが再クエリされる代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

動的分析のサマリー

動的分析のサマリーを使用できる場合、脅威スコアのアイコンをクリックすると、それが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示できます。

サマリーには、脅威スコアを構成する各コンポーネントの脅威がリストされています。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMP クラウドの調査結果もリストされます。

プロセス ツリーには、AMP Threat Grid クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示（View Full Report）] をクリックすることにより、AMP クラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

Cisco AMP Threat Grid パブリック クラウドの動的分析結果の表示

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	サポートされるドメイン	アクセス（Access）
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

Cisco AMP Threat Grid では、分析されたファイルに関して、Firepower Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Cisco AMP Threat Grid パブリック クラウドのアカウントがあれば、Cisco AMP Threat Grid ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示することができます。

始める前に

Firepower Management Center と Cisco AMP Threat Grid パブリック クラウド アカウントを関連付けます。パブリック クラウドでの動的分析の結果へのアクセスの有効化を参照してください。

手順

ステップ 1 Threat Grid ドキュメントで提供されるアドレスで、Cisco AMP Threat Grid パブリック クラウドのポータルにアクセスします。

ステップ 2 このタスクへの前提条件で関連付けを作成するために使用したアカウントの資格情報を使用してログインします。

ステップ 3 組織によって送信されたファイルを表示するか、SHA を使用して特定のファイルを検索します。

不明な点がありましたら、Threat Grid ドキュメントを参照してください。

ファイル分析評価

Spero 分析とローカル マルウェア分析、動的分析、またはこれらの組み合わせの結果に基づいて、システムはファイルの性質を更新することがあります。

システムは、ファイルに対して最初に Spero 分析、次にローカル マルウェア分析、動的分析の順に実行します。システムがマルウェアを特定した場合でも、ファイルがマルウェアとして事前分類されていれば、ファイルは AMP Threat Grid クラウドに送信されます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。事前分類の結果としてファイルの性質が変更されることはありません。

次の表に、ファイル分析の各タイプの利点と欠点、および分析に基づいたファイルの性質の変更方法について説明します。

表 *5:* ファイル分析のタイプの比較

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します。	ローカルマルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカルマルウェア分析	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます。	動的分析よりも結果の詳細度が低くなります。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
動的分析	AMP Threat Grid クラウドを使用してサンドボックス環境でファイルを実行することで、結果の詳細度がより高くなります。	ローカルマルウェア分析単独の場合よりも消費するリソースが多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーに設定されている脅威スコアしきい値に基づいて性質が変更されます。
Spero 分析とローカル マルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカルマルウェア分析と動的分析を設定するよりも少ないリソースを消費します。	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析と動的分析	ファイルおよび Spero シグネチャの送信時に AMP クラウドの全機能を使用します。	ローカルマルウェア分析を使用する場合よりも結果の取得に時間がかかります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイル ポリシーで設定されている脅威スコアしきい値に基づいて、および Spero 分析でマルウェアが特定された場合は、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます。	どちらか一方の場合よりも消費するリソースが多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	最も詳細な結果になります。	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります。	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。

キャプチャ ファイルとファイル ストレージ

ファイル ポリシーの設定に基づき、ファイル制御機能を使用して、ファイルの検出およびブロックを行えます。ただし、疑わしいホストまたはネットワークからのファイルや、ネットワーク上の監視対象ホストに送信された大量のファイルについては、さらに分析が必要になる場合があります。ファイル ストレージ機能を使用することにより、選択したファイル（トラフィックで検出された）をキャプチャして、それらをデバイスのハードドライブかマルウェア ストレージ パック（インストールされている場合）に自動的に保存できます。

デバイスがトラフィックでファイルを検出すると、そのファイルをキャプチャできます。このようにして作成されたコピーは、ダイナミック分析のために、システムが保存したり送信したりできます。デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカル コンピュータにダウンロードする。
- ダイナミック分析用に、AMP クラウドにファイルを送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。

（注） ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイル イベントを生成できます。ただし、ファイル ルールがマルウェア クラウド ルックアップを行う場合は、システムが AMP クラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが2回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- イベント ビューアからのキャプチャされたファイルに関する情報（ダイナミック分析のためにファイルが保存されたのか送信されたかどうか、ファイル判定結果、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーン リストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイル ポリシーでファイル ルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイル ポリシーをアクセス コントロール ポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致

ファイルが検出され、保存されます。また、保存するファイルサイズの最小値と最大値を設定できます。保存したファイルは、システム バックアップ ファイルには含まれません。

マルウェア ストレージ パック

ファイル ポリシー構成によっては、デバイスがハード ドライブにかなりの量のファイル データを保存することがあります。デバイスにマルウェア ストレージ パックを設置できます。システムがファイルをマルウェア ストレージ パックに保存することにより、イベントおよび設定ファイルを保存するために、プライマリ ハード ドライブにより多くスペースを確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリ ハード ドライブに使用可能な領域が十分でなく、マルウェア ストレージパックも設置されていない場合、ファイルを保存することはできません。

⚠

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハードドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージパック キットは、シスコから**のみ**購入でき、8000 シリーズデバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower System Malware Storage Pack Guide*を参照してください。

マルウェア ストレージ パックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリ ハード ドライブのスペースの特定の部分がキャプチャ ファイル ストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハード ドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェア ストレージ パックを設置してファイル ストレージまたは容量処理を設定すると、デバイスはマルウェア ストレージ パック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェア ストレージ パックに他の情報を保存することはできません。

キャプチャ ファイル ストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェア ストレージ パックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリ ハード ドライブに保存されていたキャプチャ ファイルまたは容量処理ファイルはすべて、マルウェア ストレージ パックに移動します。それ以降デバイスが保存するファイルはすべて、マルウェア ストレージ パックに保存されます。

保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Firepower Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカル ホストにダウンロードし、手動でファイルを分析できます。関連ファイル イベント、マルウェア イベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は [ユーザ設定（User Preferences）] で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを `.zip` パッケージにアーカイブします。`.zip` ファイル名には、ファイルの性質とファイル タイプ（存在する場合）さらに SHA-256 ハッシュ値が含まれます。誤って解凍してしまわないように、`.zip` ファイルをパスワードで保護できます。`.zip` ファイルのデフォルト パスワードは、[ユーザ設定（User Preferences）] で編集または削除できます。

注意 有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

キャプチャされたファイル ワークフローの使用

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	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

管理対象デバイスは、ネットワーク トラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。

（注） デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイル イベント、マルウェアを識別した場合はマルウェア イベントの 2 種類のイベントを生成します。

イベント ビューアでは、テーブルにキャプチャ ファイルを表示できます。また、分析に関連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。キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページ

です。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。

ファイル ポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションを使用してファイルをキャプチャするようにファイル ポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイル ポリシーを更新し、新しい [ファイルの検出（Detect Files）] アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻（Last Changed）] の値を更新します。ただし、別のマルウェア クラウド ルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

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

[分析（Analysis）] > [ファイル（Files）] > [キャプチャ ファイル（Captured Files）]を選択します。

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

関連トピック

キャプチャされたファイルのフィールド （31 ページ）
定義済みキャプチャ ファイルのワークフロー
イベント ビュー設定の設定

キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。

表 *6*: キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ インスペクション ステータス（Archive Inspection Status）	アーカイブ ファイルでの、アーカイブ インスペクションのステータス： • [保留中（Pending）] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。 • [抽出済み（Extracted）] は、アーカイブの内容を抽出し、検査できたことを示します。 • [失敗（Failed）] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [深さ超過（Depth Exceeded）] は、許可されている最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示します。 • [暗号化（Encrypted）] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示します。 • [検査不可（Not Inspectable）] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、イベント ビューアで該当の行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] を選択します。
カテゴリ（Category）	ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。
検出名（Detection Name）	検出されたマルウェアの名前。

フィールド	説明
傾向（Disposition）	ファイルの ネットワーク向け AMP での性質： • [マルウェア（Malware）] は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）] は、ファイルが AMP クラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーン リストに追加したことを示します。 • [不明（Unknown）] は、システムが AMP クラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルが AMP クラウドで正しく分類されていないことを示します。 • [カスタム検出（Custom Detection）] は、ファイルをユーザがカスタム検出リストに追加したことを示します。 • [使用不可（Unavailable）] は、システムが AMP クラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [N/A] は、[ファイルを検出する（Detect Files）] または [ファイルをブロックする（Block Files）] ルールによってファイルが処理され、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
ドメイン	キャプチャされたファイルが検出されたドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

フィールド	説明
動的分析ステータス（Dynamic Analysis Status）	

フィールド	説明
	ファイルが動的分析のために送信されたかどうかを示すものであり、次の値のうちの 1 つ以上が表示されます。 • [分析完了（Analysis Complete）]：ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリー レポートを受け取りました。 • [処理予定の容量（Capacity Handled）]：送信できなかったため、ファイルが保存されました。 • [処理予定の容量（ネットワークの問題）（Capacity Handled (Network Issue)）]：ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。 • [処理予定の容量（レート制限）（Capacity Handled (Rate Limit)）]：最大数に達したことが原因で送信できなかったため、ファイルが保存されました。 • [非アクティブなデバイス（Device Not Activated）]：デバイスがオンプレミスの AMP Threat Grid アプライアンスでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。 • [失敗（分析タイムアウト）（Failure (Analysis Timeout)）]：ファイルが送信されましたが、まだAMPから結果が返されていません。 • [失敗（ファイル実行不可）（Failure (Cannot Run File)）]：ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。 • [失敗（ネットワークの問題）（Failure (Network Issue)）]：ネットワーク接続の問題のため、ファイルが送信されませんでした。 • [分析のための送信なし（Not Sent for Analysis）]：ファイルが送信されませんでした。 • [疑わしくないファイル（分析のための送信なし）（Not Suspicious (Not Sent For Analysis)）]：ファイルがマルウェアではないものとして事前に分類されています。 • [以前に分析済み（Previously Analyzed）]：キャッシュされた脅威スコアがあるファイルをユーザが再び送信しようとしました。 • [分析のために送信（Sent for Analysis）]：ファイルが

フィールド	説明
	マルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。
ダイナミック分析ステータスの変更（Dynamic Analysis Status Changed）	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名（File Name）	ファイルの SHA-256 ハッシュ値に関連した、最後に検出されたファイル名。
最終更新時刻（Last Changed）	このファイルに関連した情報が最後に更新された時刻。
最終送信日時（Last Sent）	ファイルが動的分析のために AMP クラウドに最後に送信された時刻。
ローカル マルウェア分析ステータス（Local Malware Analysis Status）	ローカル マルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。 • [分析完了（Analysis Complete）]：ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。 • [分析失敗（Analysis Failed）]：ローカルマルウェア分析を使用してファイルを検査しようとし、失敗しました。 • [手動による要求の送信（Manual Request Submitted）]：ユーザがローカル マルウェア分析のためにファイルを送信しました。 • [分析なし（Not Analyzed）]：システムでローカル マルウェア分析を使用してファイルが検査されませんでした。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイルイベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージ ステータス（Storage Status）	ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。 • ファイル保存済み（File Stored） • 保存なし（性質分析の保留）（Not Stored (Disposition Was Pending)）

フィールド	説明
脅威スコア（Threat Score）	このファイルに関連付けられている最新の脅威スコア。 動的分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ（Type）	ファイルのタイプ（HTML や MSEXE など）。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストおよびユーザやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、ネットワーク向け AMP と AMP for Endpoints の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイル トラジェクトリ リスト（Network File Trajectory List）] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルの SHA-256 のハッシュ値、名前、タイプ、現在のファイルの性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256 ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストの IP アドレスによってファイルを見つけることができます。ファイルを見つけた後、[ファイル SHA256（File SHA256）] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

ネットワーク ファイル トラジェクトリの詳細ビュー

詳細なネットワーク ファイル トラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルの SHA 256 値を検索するか、[ネットワーク ファイル トラジェクトリ（Network File Trajectory）] リスト内の [ファイルの SHA 256（File SHA 256）] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイル トラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリ ページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間と表示したユーザ、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データ ポイント間の縦線は、ホスト間のファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に応じたホストのファイルアクティビティを示します。

  また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。このパスにより、関与するユーザが識別されます。
- 関連イベント：[イベント（Events）] テーブルに、マップ内の各データ ポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイルイベント、このファイルを転送または受信したネットワーク上のホストとユーザ、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。

ヒント 関連するファイルイベントを表示するには、フィールド値のリンクをクリックします。ファイルイベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 7: ネットワーク ファイル トラジェクトリのサマリー情報フィールド

[名前（Name）]	説明
アーカイブ コンテンツ（Archive Contents）	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。

[名前（Name）]	説明
現在の性質（Current Disposition）	次のいずれかの ネットワーク向け AMP ファイルの性質です。 • マルウェア（Malware）：ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。 • [クリーン（Clean）]：AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • [不明（Unknown）]：システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。 • カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。 • 利用不可（Unavailable）：システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [該当なし（N/A）]：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
検出名（Detection Name）	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント（Event Count）	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
ファイル カテゴリ（File Category）	ファイル タイプの一般的なカテゴリ（Office Documents や System Files など）。

[名前（Name）]	説明
ファイル名（File Names）	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名が SHA-256 ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細（more）] をクリックすると、これが展開されて、残りのファイル名が表示されます。
ファイル SHA256（File SHA256）	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
ファイル サイズ（File Size）（KB）	ファイルのサイズ（KB 単位）。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
最初の確認日時（First Seen）	ネットワーク向け AMP または AMP for Endpoints による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、および関与するユーザの識別情報。
最終表示（Last Seen）	ネットワーク向け AMP または AMP for Endpoints による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、および関与するユーザの識別情報。
親アプリケーション（Parent Application）	エンドポイント向け AMP による検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。
送受信ホスト数（Seen On）	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[送受信ホスト数の内訳（Seen On Breakdown）] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
送受信ホスト数の内訳（Seen On Breakdown）	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名（Threat Name）	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。

[名前（Name）]	説明
脅威スコア（Threat Score）	ファイルの脅威スコア。

ネットワーク ファイル トラジェクトリ マップと関連イベント リスト

ファイル トラジェクトリ マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、レトロスペクティブ イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA-256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて矢印アイコン（）が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。

デフォルトの [File Events（ファイル イベント）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイントベースのマルウェア イベントが表示されない場合、[マルウェア イベント（Malware Events）] テーブルに切り替えて、それらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック（Malware Block）] イベント アイコンは、[悪意のある性質（Malicious Disposition）] アイコンと [ブロック イベント（Block Event）] アイコンを結合したものです。

エンドポイントベースのマルウェア イベントには 1 つアイコンが含まれます。レトロスペクティブ イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付けられている IP アドレスが関係するエンドポイントベースのマルウェア イベント
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係する場合、その他方の IP アドレスが関係するエンドポイントベースのマルウェア イベント

強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

ネットワーク ファイル トラジェクトリの使用

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	サポートされるドメイン	アクセス（Access）
マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin/Any Security Analyst

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 **[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）]**を選択します。

ヒント また、ファイル情報を使用して、コンテキストエクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

ステップ 2 リストの [ファイル SHA 256（File SHA 256）] リンクをクリックします。

ステップ 3 オプションで、追跡するファイルの完全な SHA-256 ハッシュ値、ホスト IP アドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

ヒント 1 つの結果だけが一致する場合、そのファイルの [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] ページが表示されます。

ステップ 4 [サマリー情報（Summary Information）] セクションでは、以下を実行できます。

- ファイル リストにファイルを追加する：クリーン リストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、編集アイコン（  ）をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、ファイルのダウンロード アイコン（  ）をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このアイコンは淡色表示されます。

- レポートする：脅威スコア アイコンをクリックすると、動的分析サマリー レポートが表示されます。
- 動的分析のために送信する：AMP クラウド アイコン（）をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、このアイコンは淡色表示されます。
- アーカイブの内容を表示する：アーカイブ ファイルの内容に関する情報を表示するには、表示アイコン（）をクリックします。
- ファイル構成を表示する：ファイルの構成を表示するには、ファイル リスト アイコン（）をクリックします。システムがファイル構成レポートを生成していなければ、このアイコンは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコア リンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

（注） シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ステップ 5 トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IP アドレスをクリックして、IP アドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[イベント（Events）] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。
- 非表示のイベントを表示する：矢印アイコンをクリックすると、[ファイル サマリー（File Summary）] イベント ビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：イベント アイコン（）の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベント サマリー情報リンクをクリックすると、デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、そのファイル タイプのすべての余分のイベントが表示されます。[ファイル サマリー（File Summary）] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

ステップ 6 [イベント（Events）] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイルイベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。