暗号化された可視性エンジン

Encrypted Visibility Engine（EVE）は、TLS 暗号化を使用するクライアント アプリケーションとプロセスを識別するために使用されます。可視性を実現し、管理者が環境内でアクションを実行してポリシーを適用できるようにします。EVEテクノロジーは、マルウェアの特定と阻止にも使用できます。

暗号化された可視性エンジン

暗号化された可視性エンジン（EVE）は、復号を必要とせずに暗号化セッションの可視性を高めるために使用されます。暗号化されたセッションに関する洞察は、シスコの脆弱性データベース（VDB）にパッケージ化されているシスコのオープンソースライブラリによって取得されます。ライブラリは、着信暗号化セッションをフィンガープリントして分析し、一連の既知のフィンガープリントと照合します。この既知のフィンガープリントのデータベースも、Cisco VDB で利用できます。

アクセス コントロール ポリシーの [詳細（Advanced）] タブにある [暗号化された可視性エンジン（Encrypted Visibility Engine）] トグルボタンを使用して、EVE を有効または無効にします。Management Center 7.1 では、暗号化された可視性エンジンは、暗号化されたトラフィックの可視性を高めるためにのみ使用されます。そのトラフィックにアクションを強制しません。

Management Center 7.2 では、暗号化された可視性エンジン（EVE）に次の拡張機能があります。

- Management Center 7.2 で EVE を使用するには、デバイスに有効なIPS ライセンスが必要です。IPS ライセンスがない場合、ポリシーによって警告が表示され、展開は許可されません。
- EVEから取得した情報を使用して、トラフィックに対してアクセス コントロール ポリシー アクションを実行できます。
- Cisco Secure Firewall 7.2 に含まれる VDB には、EVE によって高い信頼値で検出された一部のプロセスにアプリケーションを割り当てる機能があります。または、次の目的でカスタム アプリケーション ディテクタを作成できます。

- EVE で検出されたプロセスを新しいユーザー定義アプリケーションにマッピングする。
- EVE で検出されたプロセスにアプリケーションを割り当てるために使用されるプロセス確実性の組み込み値を上書きする。

『Cisco Secure Firewall Device Management Configuration Guide』の「**Application Detection**」の章にあるセクション「**Configuring Custom Application Detectors**」と「**Specifying EVE Process Assignments**」を参照してください。

- EVE は、暗号化されたトラフィックで Client Hello パケットを作成したクライアントのオペレーティングシステムのタイプとバージョンを検出できます。
- EVE は、Quick UDP Internet Connections（QUIC）トラフィックのフィンガープリントと分析もサポートします。Client Hello パケットからのサーバー名は、[接続イベント（Connection Events）] ページの [URL] フィールドに表示されます。

（注） 暗号化された可視性エンジンの機能は、Snort 3 を実行している Management Center の管理対象デバイスでのみサポートされます。この機能は、Snort 2 デバイス、Device Manager の管理対象管理デバイス、または CDO ではサポートされていません。

[暗号化された可視性エンジン（Encrypted Visibility Engine）] トグルボタンが有効になり、アクセス コントロール ポリシーが展開されたら、システムを介してライブトラフィックの送信を開始できます。ログに記録された接続イベントは、[接続イベント（Connection Events）] ページで表示できます。接続イベントにアクセスするには、Management Center で [分析（Analysis）] > [接続（Connections）] > [イベント（Events）] に移動し、[接続イベントのテーブルビュー（Table View of Connection Events）] タブをクリックします。[分析（Analysis）] メニューにある [統合イベント（Unified Events）] ビューアに接続イベントフィールドを表示することもできます。暗号化された可視性エンジンでは、接続を開始したクライアントプロセス、クライアントのOS、そのプロセスにマルウェアが含まれているかどうかを特定できます。

[接続イベント（Connection Events）] ページには、で暗号化された可視性エンジン用の次の列が追加されました。以下の列を明示的に有効にする必要があることに注意してください。

- [暗号化された可視性プロセス名（Encrypted Visibility Process Name）]
- [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）]
- [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）]
- [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）]
- [検出タイプ（Detection Type）]

これらのフィールドの詳細については、『Cisco Firepower Management Center Administration Guide』の「Connection and Security Intelligence Event Fields」の項を参照してください。

（注） プロセスにアプリケーションが割り当てられている場合、[接続イベント（Connection Events）] ページの [検出タイプ（Detection Type）] 列には、クライアント アプリケーションが EVE によって識別されたことを示す [暗号化された可視性エンジン（Encrypted Visibility Engine）] が表示されます。プロセス名へのアプリケーションの割り当てがない場合、[検出タイプ（Detection Type）] 列には、クライアント アプリケーションを識別したエンジンが AppID であることを示す [AppID] が表示されます。

分析情報は 2 つのダッシュボードに表示できます。[概要（Overview）] > [ダッシュボード（Dashboards）] に移動し、[ダッシュボード（Dashboards）] をクリックします。[概要ダッシュボード（Summary Dashboard）] ウィンドウで、スイッチダッシュボードのリンクをクリックし、ドロップダウンボックスから [アプリケーション統計（Application Statistics）] を選択します。[TLSフィンガープリント（TLS Fingerprint）] タブを選択し、次の 2 つのダッシュボードを表示します。

- **[上位の暗号化された可視性エンジンで検出されたプロセス（Top Encrypted Visibility Engine Discovered Processes）]**：ネットワークで使用されている上位の TLS プロセス名と接続数が表示されます。テーブルのプロセス名をクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューはプロセス名でフィルタリングされています。
- **[暗号化可視性エンジンの脅威の信頼度別の接続（Connections by Encrypted Visibility Engine Threat Confidence）]**：マルウェアの確実性レベル（非常に高い、非常に低いなど）別に接続が表示されます。テーブル内の脅威の信頼レベルをクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューは、信頼レベルによってフィルタリングされています。

Management Center 7.2 では、EVE は SSL セッションのオペレーティングシステムのタイプとバージョンを検出できます。アプリケーションやパッケージ管理ソフトウェアの実行など、オペレーティングシステムの通常の使用により、OS 検出がトリガーされる可能性があります。クライアント OS 検出を表示するには、EVE トグルを有効にすることに加えて、[ポリシー（Plicies）] > [ネットワークの検出（Network Discovery）] で [ホスト（Hosts）] を有効にする必要があります。 > ホスト IP アドレスで使用可能なオペレーティングシステムのリストを表示するには、**[分析（Analysis）]** > **[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]** をクリックし、該当するホストを選択します。

Management Center 7.3.0 以降、ホストの暗号化された可視性エンジン検出の侵害の兆候（IoC）イベントにより、非常に高いマルウェアの確実性レベルで、EVE によって報告された接続イベントをチェックできます。IoC イベントは、悪意のあるクライアントを使用してホストから生成された暗号化セッションに対してトリガーされます。悪意のあるホストの IP アドレス、MAC アドレス、OS 情報などの情報と、不審なアクティビティのタイムスタンプを表示できます。

接続イベントで示される、暗号化された可視性脅威の確実性スコアが「非常に高い」となっているセッションは、IoC イベントを生成します。**[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** から [ホスト（Hosts）] を有効にする必要があります。 Management Center では、次の場所から IoC イベントの存在を表示できます。

- **[分析（Analysis）] > [侵害の兆候（Indications of Compromise）]**
- **[分析（Analysis）] > [ネットワークマップ（Network Map）] > [侵害の兆候（Indications of Compromise）] >** チェックする必要があるホストを選択します。

  IoC を生成したセッションのプロセス情報は、以下から表示できます。

  [分析（Analysis）] > [接続イベント（Connection Events）] > [接続イベントのテーブルビュー（Table View of Connection Events）] > [IoC]。暗号化された可視性フィールドと IoC フィールドを手動で選択する必要があることに注意してください。

Snort は、EVE に基づいて QUIC セッション内のクライアント アプリケーションを識別できます。QUIC フィンガープリントでは次を実行できます。

- 復号を有効にせずに QUIC でアプリケーションを検出する。
- 復号を有効にせずにマルウェアを特定する。
- サービスアプリケーションを検出する。QUIC プロトコルで検出されたサービスに基づいて、アクセスコントロールルールを割り当てることができます。

[暗号化された可視性エンジン（EVE）（Encrypted Visibility Engine (EVE)）] トグルを有効にすると、その下に次のトグルが表示されます。

- [アプリケーション検出にEVEを使用（Use EVE for Application Detection）]：このトグルはデフォルトで有効になっています。つまり、EVE はクライアント アプリケーションをプロセスに割り当てることができます。

  接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] 列ヘッダーに EVE のフィンガープリント情報が追加されます。収集された EVE データをさらに分析する場合は、フィンガープリント情報を右クリックしてドロップダウンメニューを開くことができます。メニューで、[暗号化された可視性エンジンプロセス分析の表示（View Encrypted Visibility Engine Process Analysis）] をクリックして appid.cisco.com に移動し、フィンガープリント、VDB バージョンなどの詳細を表示します。同じフィンガープリント文字列を持つ異なる行と、それらに関連付けられている潜在的なプロセス名およびその拡散度が表示されます。拡散度は、データ収集システム内の特定のフィンガープリントに関連付けられたプロセスの頻度を示します。プロセス名を選択し、[リクエストの送信（Submit Request）] をクリックすると、EVE のプロセス検出の不一致に関するフィードバックを送信することができます。たとえば、検出されたプロセス名が送信されているトラフィックと一致しない場合や、特定のフィンガープリントについてプロセス名がまったく検出されない場合に、リクエストを送信できます。

  トグルが無効になっている場合、AppID で識別されたクライアントがプロセスに割り当てられ、EVE プロセスとスコアは表示されますが、EVE で検出されたプロセスからアプリケーションへのマッピングはなく、アクションも実行されません。イベントの詳細は、[接続イベント（Connection Events）] または [統合イベント（Unified Events）] で確認できます。接続イベントの違い（アプリケーションの割り当ての有無）を確認するには、[クライアントアプリケーション（Client Application）] 列ヘッダーを確認します。トグルが無効になっている場合、接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] フィールドは空です。

- [EVEスコアに基づくトラフィックのブロック（Block Traffic Based on EVE Score）]：このトグルを有効にすると、EVEの脅威の確実性スコアに基づいてトラフィックをブロックできます。潜在的な脅威である着信トラフィックは、デフォルトでブロックされます。デフォルトのブロックしきい値は 80% で、次のことを意味します。
  - EVE がトラフィックを 80% 以上の確実性でマルウェアであると検出した場合、トラフィックはブロックされます。
  - EVE がトラフィックを 80% 未満の確実性でマルウェアであると検出した場合、何も実行されません。

  EVE がトラフィックをブロックした場合、[接続イベント（Connection Events）] の [理由（Reason）] 列ヘッダーに [暗号化された可視性ブロック（Encrypted Visiblity Block）] が表示されます。
  - [詳細設定（Advanced Settings）]：[EVEスコアに基づくトラフィックのブロック（Block Traffic Based on EVE Score）] で、[詳細モード（Advanced Mode）] トグルを有効にして、EVEでトラフィックをブロックするしきい値をカスタマイズします。スライダを使用して、トラフィックをブロックする割合（しきい値）を調整できます。

注意 最適なパフォーマンスを得るには、しきい値を50%未満に設定しないことをお勧めします。

Client Hello パケットがフラグメント化されている場合、EVE はクライアント情報（クライアントプロセス、クライアント OS、およびマルウェア確実性）を再構成して検出できます。

暗号化された可視性エンジン

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。