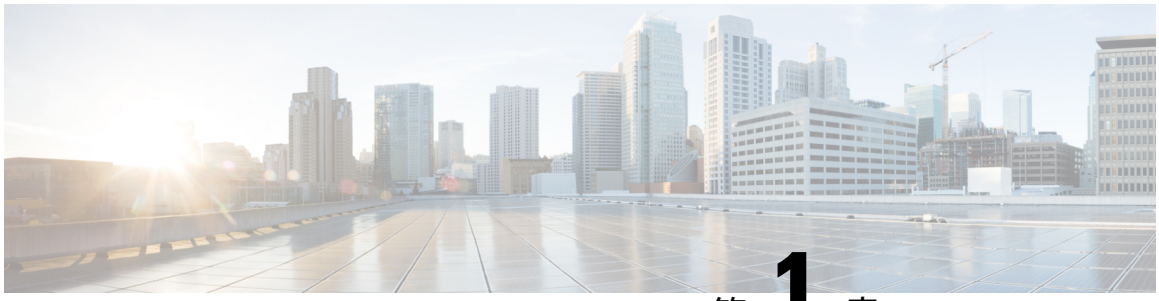
Cisco Cognitive Intelligence ユーザガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

新機能

新機能

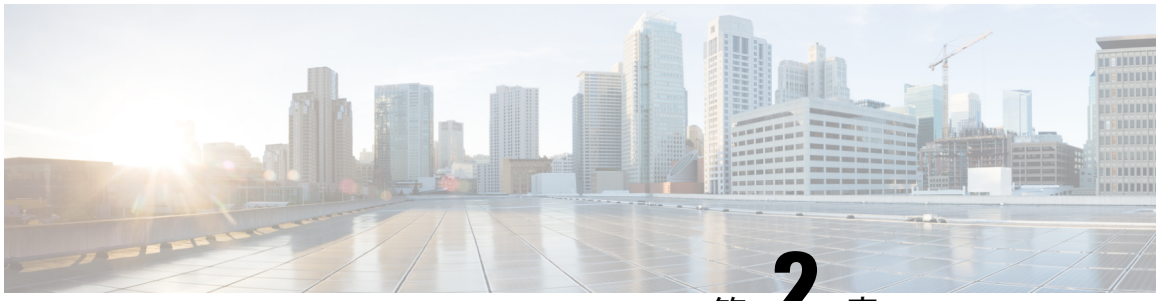
Alert Fusion

Cognitive Intelligence は 2020 年 6 月に Alert Fusion をリリースしました。これは、Cognitive Intelligence の Web ポータルで Early Access を有効にすると、すべてのお客様が利用可能になります。検出された脅威をネットワーク上のリスクを示すセキュリティアラートの優先順位リストに動的にグループ化し、調査の次のステップを容易にします。詳細については、『Cognitive Alert Fusion Early Access Release Notes』を参照してください。

Cognitive Intelligence

2018 年 10 月、Cognitive Threat Analytics（CTA）は Cognitive Intelligence に名称変更されました。これは、AMP for Endpoints、Stealthwatch、Threat Grid など、特化型の複数の Cisco Security 製品から組み込み機能へ進化したものです。

新機能



第 2 章

Web ポータル

概要

Cognitive Intelligence は、すでに進行している攻撃や、お客様のネットワーク環境内で密かにプレゼンスを確立しようとしている高度な攻撃を迅速に検出して対応するのに役立ちます。このソリューションは、不審な Web ベースのトラフィックや悪意のあるトラフィックを自動的に特定して調査します。潜在的な脅威と確認済みの脅威の両方を特定することで、感染を迅速に修復し、攻撃の範囲と損害を軽減できます。これは、既知の脅威キャンペーンが複数の組織に拡散している場合でも、これまでに見たことのない固有の脅威である場合でも同様です。クラウドベースのサービスである Cognitive Intelligence は、ハードウェアやソフトウェアを追加せずに、既存の Web セキュリティソリューションによって生成された情報を分析します。

Cognitive Intelligence は、毎日 100 億を超える Web 要求を自動的に分析します。セキュリティ制御をバイパスし、標準チャネル、暗号化チャネル、匿名チャネルを含む Web ベースの通信を使用して組織を攻撃する悪意のあるアクティビティを防御します。Cognitive Intelligence は、機械学習とネットワークの統計モデリングを使用して、通常のアクティビティのベースラインを作成し、ネットワーク内で発生する異常なトラフィックを特定します。デバイスのふるまいと Web トラフィックを分析して、コマンドアンドコントロール通信とデータ漏洩を特定します。

Cognitive Intelligence は、認識している情報から学習することで、継続的な侵害の特定を可能にし、繰り返し攻撃や継続的な感染のリスクを軽減します。複数の Cisco Security 製品と統合された直感的な Web ベースのポータルを通じて情報を表示するため、次のことが可能になります。

- 侵入の重大度と範囲を評価します。

- 脅威のミッションとその仕組みを理解します。
- すぐにアクションを開始します。

ダッシュボード

[Dashboard] ページには、ネットワークの正常性とそれに影響する脅威の概要が表示されます。

- ヘルスステータス。ネットワークで検出された脅威の全体的な概要をリスクレベル別に表示します。未解決のユーザは、リスクカテゴリ別にグループ化されます。多数の低リスクの脅威は、時間の経過とともにより深刻な脅威につながる可能性があることに注意してください。
- 相対的な脅威の危険性。同じセクター内の他の企業、同規模の企業、および世界中のすべての企業と比較した、インシデントの数とリスクレベルに基づく脅威の危険性。
- 特定の動作。ネットワークで検出された脅威と未解決の動作の高レベルの内訳。
- 最高リスク。現在ネットワークに最も高いリスクをもたらし、早急な対応が必要な未解決のインシデント。
- 上位のリスクエスカレーション。最近リスクが増加している未解決のインシデント。

確認済みの脅威

[Confirmed] ページではネットワークの確認済みの脅威キャンペーンについての情報を表示します。

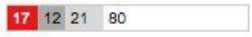
- 複数のユーザ間での脅威
- 違反を 100% 認識、誤検出なし
- 迅速な修復が可能、直接実行可能
- Cisco Collective Security Intelligence、コンテキスト用に提供される追加情報

脅威キャンペーンは、ページの右側にある垂直のパネルに表示されます。

- 脅威リストパネルの上部には次のインシデント状態のチェックボックスがあります。トリアージ、調査中、修復中、解決済み。この4つのチェックボックスを使用して垂直パネルに表示する脅威をフィルタします。たとえば、解決済みのチェックボックスをオフにすると、解決済みのステータスのマークがあるインシデントを含む脅威を非表示にします。
- 脅威は、上が最も高いリスク脅威となるリスクレベルで上から下まで並び替えられます。

脅威をクリックして、垂直パネルの左側に情報を表示します。

- [#Cxxxxx] - 相関動作で検出されたインシデントは脅威クラスタにグループ化されます。各脅威は一意なハッシュタググループ名によって分類されます。
  - [Risk level] - ネットワークに影響を与えている脅威のリスクを、1 から 10 までの数値で表したもの。数字が大きければリスクも高くなります。高リスクの脅威や、低リスクの脅威の前にそこにクラスタ化されたインシデントを調査することで分析を優位付けすることを推奨します。
  - [Confidence] - 検出カテゴリの正確さを表すパーセンテージ。数値が高ければ高いほど、症状が正確に分類されており、インシデントがネットワークに対して実際に脅威となっているという信頼度も高くなります。
  - [Incidents Bar] - 脅威にクラスタ化されたインシデントの数を示す横棒グラフのバー。
    - インシデントの数は 4 つのインシデント状態のボックスのさまざまな明度に対応するインシデント状態ごとに分類されます。
    - たとえば、次のバーでは、17 インシデントが Triage 状態、12 インシデントが Investigating 状態、21 インシデントが Remediating 状態、80 インシデントが Resolved 状態になっています。

    - ステータスのインシデントの情報を含むテーブルを表示するには、クラスタ番号をクリックします。

- [Affecting] - 過去 45 日以内にこの脅威の影響を受けたユーザの数。また、脅威が対象となっているかどうかを判断する手助けになる他の企業で影響を受けたユーザ数を表示します。
- [Occurrence] - この動作が発生した時間、最初に確認された時間、および最後に確認された時間。

脅威サマリーの下には、選択された脅威の詳細を示す次のセクションがあります。

- 脅威の説明および修復への推奨処置。
- 影響を受けたユーザのリストと経時的に悪意のある動作を示すユーザの数を表示するグラフ。
- ネットワークの脅威の動作を表すサンプル Web 要求。URL にエンコードされた部分が含まれている場合、システムはデコードしたコンテンツをここで表示することを試みます。
- Cisco Cloud Web Security のマルウェアブロックは、この脅威の影響を受けたネットワークのユーザを監視します。
- [AMP Threat Grid Global Intelligence] - 共通エンドポイント コンテンツ セキュリティ シグニチャおよび脅威のグローバル トラフィック サンプルに関連する動作。
  - エンドポイントに存在する可能性があるグローバルな脅威サンプルに現れる共通ファイル、エンドポイントのマルウェアによってこれらのファイルが作成または変更される確率の割合、およびファイルタイプの重大度

- AMP Threat Grid のサンプルで確認された同様の脅威に関連する共通エンドポイントの動作

- Cognitive Intelligence で検出されたインシデントのリストと、この脅威キャンペーンに分類される影響を受けたユーザ。詳細を表示するには、インシデントをクリックします。「インシデントの詳細」を参照してください。

検出済みインシデント

Cognitive Intelligence システムは Web プロキシログを監視しますが、通信の内容は調査しません。Cognitive Intelligence システムは、悪意のある Web 閲覧動作を識別することにフォーカスしており、感染によって動作に現れる症状から生成されたインシデントを示します。[Detected] ページでは、相関性のない Cognitive Intelligence インシデントおよび AMP のレトロスペクティブインシデントを含む、脅威の疑いがある検出されたインシデントの概要を示します。また、[Confirmed] ページで検証済みの脅威にグループ化された、相関性のある Cognitive Intelligence インシデントを表示することもできます。

- [Incident] - リスクと信頼度を含む、個別に検出された主要な動作の種類で、クラスタまたは確認済みの脅威の一部であるかどうかは関係ありません。クラスタは同様のマルウェアの症状があるインシデントの集合です。
  - [Risk] - インシデントのリスクを、1 から 10 までの数値で表したもの。数字が大きければリスクも高くなります。低リスクのインシデントよりも高リスクのインシデントを先に調査し、インシデント分析に優先順位を付けることをお勧めします。
  - [Confidence] - 検出カテゴリの正確さを表すパーセンテージ値。数値が高ければ高いほど、症状が正確に分類されており、インシデントがネットワークに対して実際に脅威となっているという信頼度も高くなります。Cognitive Intelligence インシデントにのみ適用されます。

- [User Identity] - 影響を受けたユーザの ID と IP アドレス。
  - IP アドレスは、経時的に複数のユーザに再割り当てされることがあるため、Cognitive Intelligence システムはユーザ単位でのモデリングを行います。こうした重要なシステム強化により、より一貫性の高い結果がもたらされるようになりました。
  - ユーザには、経時的に 1 つ以上の IP アドレスが割り当てられることがあります。Cognitive Intelligence システムはこれらの割り当てを追跡し、指定された期間内にユーザに割り当てられた IP アドレスをすべて表示します。

- [IP Reputation] - 接続したリモートサーバのレーティングは、各インシデントにおいてユーザが通信した既知のソースの集約情報を表します。レーティングは、Anomaly Detection Engine（異常検出エンジン）が検出を行う際には使用されません。レーティングは、インシデント検出が発生した状況を、セキュリティアナリストが理解しやすくするための情報（グローバルインテリジェンス）として提供されます。
  - 赤 - IP レピュテーション レーティングが低い接続済みリモートサーバ数（-10 ～ -6）。

- オレンジ - グローバル インテリジェンス データベースにレコードが存在しない、または中間レーティングの接続済みリモートサーバ数（-5 ～ +5）。
- 緑 - IP レピュテーション レーティングが高い接続済みリモートサーバ数（+6 ～ +10）。

- [Duration] - この動作が発生した期間および時間。また、[First Seen] および [Last Seen] 列も参照してください。
- [State] - トリアージ、再発中、調査中、修復中、解決済み、誤検出、または無視とマークされたインシデント。
- [Anomaly Types] - リスク要因（重大、高、中、低）を含む、このインシデントで検出された異常のタイプ。各インシデントは多くの異常で形成されます。各異常は、マルウェアの動作の症状を表します。セルの上にカーソルを置くと、そのインシデントに関連するすべての異常タイプがすべて表示されます。異常タイプは、リスク要因によって上から下にソートされ、最も重大なものが一番上になります。
- [Last Updated] - このインシデントが作成された時間、またはいくつかの継続的なトラフィックが最後に追加された時間。

フィルタリングインシデント

インシデントをフィルタ処理して次のように表示することができます。

- 日付選択 - 各フィールドをクリックするとカレンダーが開くので、開始日（[From]）および終了日（[To]）を指定します。
  - デフォルトでは、過去 45 日間が表示されます。
  - 最大の日付範囲は 45 日間です。
  - 指定可能な日付範囲は、過去 45 日間です。
  - また、[1 day]、[3 days]、[7 days]、[30 days]、[45 days] をクイッククリックすることもできます。
- [Search] フィールド - ユーザ名、クライアントの IP アドレス、またはインシデントの名前（正規表現またはワイルドカードなし）を入力して、[Filter] ボタンをクリックします。
- [Show] - AMP および/または Cognitive Intelligence のインシデント、確認済みインシデント、低信頼度のインシデントを表示するチェックボックス、およびインシデントの状態別に表示するタブがあります。
  - [Triage] -（デフォルト）新規または再発し、かつ調査する必要があるインシデント。
  - [Investigating] - 調査中および作業中のインシデント。
  - [Remediating] - 解決中のインシデント、デバイスのクリーニング待ち。
  - **[Resolved]**
    - [Remediated] - 修復されたインシデント、デバイスはクリーニング済み。

- [False Positives] - 誤検出と判断されたインシデント。
- [Ignored] - 無視され調査されていないとマーキングされたインシデント。たとえば、ゲスト Wi-Fi ゾーンのデバイス用のインシデント。

- [All] - 状態またはマーキングを無視したすべてのインシデント。

（注） インシデントは、[Incident Details] ページでドロップダウンリストを使用してマーキングできます。

設定

グローバル設定を構成するには、ページの右上隅にある歯車アイコンのドロップダウンメニューをクリックします。

- [Email Notifications] - 新規および更新されたインシデントのサマリーを送信する電子メールアドレスを 24 時間ごとに入力します。
- [Cisco Threat Response] - セキュリティイベントおよびアラートを一元的に把握し、その他のセキュリティサービスからのデータによってそれらの情報を拡張できます。これにより、インシデントレスポンダと SOC アナリストは、セキュリティイベントの検出、関連付け、および優先順位付けに必要なデータを得られます。事例集やピボットメニューなどの強力なツールが含まれています。Threat Response を有効にするには、Threat Response アカウントリージョンを選択し、[Authorize] をクリックして、Threat Response アカウントにサインインします。AMP for Endpoints のお客様全員に自動的に Threat Response アカウントが付与されます。
- [CTA STIX/TAXII Service] - CTA STIX/TAXII サービスを使用して、さらなる分析、インシデント対応、およびデータアーカイブのための SIEM クライアントまで Cognitive Intelligence で検出されたインシデントの情報を取り出します。「STIX/TAXII サービス」を参照してください。
- [Device Accounts] - 1 つ以上のソースプロキシデバイスから分析用 Cognitive Intelligence システムにログファイルのテレメトリデータをアップロードします。このサービスにアクセスするには、外部テレメトリ機能を有効にして、企業用にプロビジョニングする必要があります。外部テレメトリ機能がない場合は、Cisco Security アカウントチームにお問い合わせください。「プロキシデバイスのアップロード」を参照してください。
- [Ignored Networks] - 無視する IPv4 アドレスとネットワーク範囲をリストしてアラートを非表示にします。これは、ゲストネットワークやその他の重要度の低いネットワークからのアラートなど、不要なアラートをフィルタリングする場合に役立ちます。インシデントのリストから非表示にするホスト、ネットワーク、または IPv4 アドレス範囲の IPv4 アドレス（例：10.100.10.1、10.100.10.0/24、10.100.10.1-10.100.10.254）を入力します。
- [Release Notes] - リリースごとのアップデート、変更、および修正を集約します。

次のテーブルヘッダー内およびグローバル設定メニューボタンの下。

- Download ボタンをクリックして、（表示された現在のフィルタから）デバイスの CSV ファイルにインシデントをエクスポートします。
- ページ設定ボタンをクリックして、どのカラムを表示するかを選択します。
- カラムの見出しのソート矢印をクリックすると、そのカラムの情報に従って表の行がソートされます。
- カラムヘッダーセル間の線をドラッグして、カラム幅を変更します。
- カラムを選択（ヘッダーをクリック）してテーブルカラムの順序を変更し、ポインタが交差矢印に変わったら、カラムのヘッダーをドラッグしてテーブル内の新しい場所にドロップします。

インシデントをさらに詳しく調査するには、そのインシデントの列の上にカーソルを置くと、その行がハイライト表示されます。その行をクリックして、インシデントの詳細ページを開きます。また、インシデントを右クリックし、[Open incident in a new window] を選択すると、新しいウィンドウでインシデントの詳細ページを開くことができます。

インシデントの詳細

インシデントは通常、複数のアクティビティや疑わしい動作のタイプで構成されます。インシデントの詳細ページに 3 つの主要セクションがあります。

インシデントのヘッダー

最初の主なセクションは次のインシデントヘッダーです。

- [Incident Classification] - リスクと信頼度を含む検出された主な動作の種類。
  - [Risk] - ネットワークに影響を与えているインシデントのリスクを、1 から 10 までの数値で表したもの。数字が大きければリスクも高くなります。そのため、低リスクのインシデントよりも高リスクのインシデントを先に調査し、インシデント分析に優先順位を付けることをお勧めします。
  - [Confidence] - 検出カテゴリの正確さを表すパーセンテージ値。数値が高ければ高いほど、症状が正確に分類されており、インシデントがネットワークに対して実際に脅威となっているという信頼度も高くなります。Cognitive Intelligence インシデントにのみ適用されます。
- ドロップダウンリストを使用して、インシデントをトリアージ、調査中、修復中、脅威として解決済み、誤検出として解決済み、または無視として解決済みにマークします。このマーキングは主に 2 つの目的があります。1 つ目は、インシデント管理および分析のワークフローを支援するインシデントを分類します。2 つ目は、コミュニティフィードバックの一部にすることです。シスコはこれを使用し、検出アルゴリズムを向上します。調査後

にインシデントをマークしてください。リストされたインシデントの表では、マーキングは、[State] 列に表示されます。

- [Affecting] - 影響を受けたユーザの ID と IP アドレス。また、オペレーティングシステムおよびインシデントがプロキシに関連しているかどうかも表示します。

（注） テキストが暗号化されている場合、ログファイルが分析のために Cognitive にプッシュされたときに、WSA 11.5 によってフィールド値が匿名化されました。暗号化されたテキストを非匿名化する方法については、「Configure WSA to Upload Log Files to CTA System」を参照してください。

- [Occurrence] - この動作が起こった時期とその履歴。

（注） [View web traffic history] をクリックすると、このユーザの Web 閲覧履歴が Cisco WIRe（Web インテリジェンスレポート）レポートに表示されます。

平行座標

2 つ目の主要なセクションは時間、異常、ドメイン、IP アドレスおよび自律システム間の関係を表示する平行座標グラフです。

- At-a-Glance は、インシデントおよびアソシエーションの異常に関する情報を表示します。
- 相互接続情報を表示するには、折れ線グラフの各座標のノードにカーソルを合わせます。
- 永続的接続のターゲットであるドメインは PERS インジケータと太字で強調されています。
- 詳細については、ドメイン名の横にあるドロップダウンアイコンをクリックします。
- IP アドレスには国の場所と IP レピュテーションが含まれます。
- 詳細については、IP アドレスの横にあるドロップダウンアイコンをクリックします。
- 1 つ以上のノードを選択してクリックすることで、Web フローのフィルタ処理に使用できます。関連 Web フローはグラフの下の表にリストされています。
- 重大、高、中、低を選択して、異常リスク要素でフィルタリングされたフローを表示します。

Web フロー要求

3 つ目の主要なセクションは web フロー要求の詳細をリストする表です。

- [Client IP] - IP クライアントで使用される IP アドレス。
- [Client Port] - クライアントで使用される TCP/UDP ポート。
- [Server IP] - サーバで使用される IP アドレス。サーバの場所がわかっている場合は、その場所の国旗、およびサーバの IP レピュテーションスコアも表示されます。サーバの横の赤のボックスは、そのサーバに対してマイナスの IP レピュテーションがあることを意味します。ドメイン名が含まれています。マイナスの IP レピュテーションは、攻撃者が運営するドメインからの疑わしい通信があったことを示すことがあります。
- [Server Port] - サーバで使用される TCP/UDP ポート。
- [Bytes Up] - サーバに送信されたデータの量。
- [Bytes Down] - サーバから受信したデータの量。
- [Header Content Type] - リモートサーバから送信される HTTP ヘッダーのコンテンツタイプ。
- [Body Content Type] - 応答の本文で検出されたコンテンツタイプ。ヘッダーのコンテンツタイプが異なる場合があります。たとえば、悪意のあるホストがプロキシまたはファイアウォール フィルタリング ルールによって取得を試みる場合などです。
- [URL] - クライアントがアクセスするサーバの URL。URL にカーソルを合わせると、URL にエンコードされた部分が含まれている場合、システムはデコードしたコンテンツをここで表示することを試みます。多くの場合、通過したコマンドとデータが表示されます。
- [Referrer] - リクエストされているリソースにリンクされる URL のアドレスを識別する、HTTP ヘッダーフィールド。
- [HTTP Status] - サーバから返される HTTP ステータスコード。ステータスコードの横にある赤い [x] ボックスは、Web プロキシによってフローがブロックされたことを示します。
- [Timestamp] - 接続が開始した時刻。
- [Duration] - イベントが持続した期間。
- [User Agent] - アクティビティ中に使用されていたブラウザのタイプ。
- [Category] - サイトのカテゴリ（ギャンブルやソーシャルのサイト）。
- [Filename] - ダウンロードされたファイルの名前（AMP 固有のフィールド）。
- [SHA-256] - ファイル用に計算されたセキュア ハッシュ アルゴリズム SHA-256（AMP 固有のフィールド）。

検索フィールドで、クライアント IP アドレス、サーバ IP アドレス、URL、または SHA 値（正規表現またはワイルドカードなし）を入力して、[Filter] ボタンをクリックします。

ページ設定ボタンをクリックして、どのカラムを表示するかを選択します。カラムの見出しのソート矢印をクリックすると、そのカラムの情報に従って表の行がソートされます。ヘッダーをクリック、ドラッグして列を並べ替えます。

表の下のページの下部に選択されたwebフローの次の統計情報の概要を示す1列のフッターがあります。トラフィック量、ブロックされた割合、リクエストの数、合計時間、ユーザエージェント、リファラではない割合、およびHTTPステータスコード。

プロキシデバイスのアップロード

Cisco Webセキュリティアプライアンス（WSA）やBlue Coat ProxySGなどのプロキシデバイスから分析用のCognitive Intelligenceシステムに、ログファイルのテレメトリデータをアップロードします。

ステップ1 ページ右上隅の歯車アイコンをクリックし、[Device Accounts] を選択して設定ウィザードを開きます。

（注） すでに既存のデバイスアカウントが1つ以上ある場合は、設定を省略して [Device Accounts] ページが表示されます。

ステップ2 セットアップウィザードを開始してデバイスアカウントを追加する準備ができたら、[Let's Get Started] をクリックします。

ステップ3 ドロップダウンから自動アップロードまたは手動アップロードのいずれかを選択して、テレメトリデータをデバイスからアップロードする方法を選択します。Cognitive Intelligenceシステムは、一度に1つのアップロード方法のみをサポートします。組み合わせることはできません。

（注） 自動から手動にアップロード方法を切り替えるには、まず、すべてのプロキシデバイスを自動アップロード設定から削除する必要があります。

ステップ4 自動アップロード方式を選択した場合は、[SCP] または [HTTPS] のいずれかを選択して、ログファイルの転送に使用するプロトコルを選択します。

a) このデバイスの名前を入力し、[Add Account] をクリックします。

b) SCPを選択した場合：

- Cisco WSAの設定に情報（ホスト、ポート、ディレクトリ、ユーザ名）をコピーします。セキュリティ上の理由により、情報は1度しか表示されません。
- Cisco WSAの設定方法の詳細については、Cisco WSAの設定ガイドを参照してください。
- Cisco WSA管理コンソールがSSH公開キーを返したら、このSSH公開キーをデバイスアカウントにコピーして貼り付けます。
- [Finish] をクリックします。
- また、[Device Accounts] ページに移動してデバイスをクリックすると、SSH公開キーを後で入力できます。

c) HTTPSを選択した場合：

- 情報（ホスト、ポート、パス、ユーザ名、パスワード）をコピーしてBlue Coat ProxySG設定に貼り付けます。

- Blue Coat ProxySG の設定方法の詳細については、Blue Coat ProxySG の設定ガイドを参照してください。
- [Finish] をクリックします。

ステップ 5 手動アップロード方式を選択した場合：

a) ログファイルの形式を検証します。次の準備ガイドラインに従ってください。

- Cisco WSA および Blue Coat プロキシで作成された W3C ログファイルはサポートされています。
- すべてのログファイルは GZip（*.gz）形式で圧縮する必要があります。
- 各ログファイルは 1 GB 未満にする必要があります。1 GB を超えるログファイルは、複数の小さいファイルに分割する必要があります。それぞれの間隔が重複していないこと、すべてのファイルに同一の適切なヘッダーが含まれていることを確認します。
- ログファイルに必要な間隔の合計は 2 日以上です。
- 各ログファイルの間隔は、固有で重複しないようにする必要があります。
- 各ログファイルには、時間の昇順（古いエントリが前、新しいエントリが後）にログエントリを含める必要があります。
- ログファイルはアルファベット順/数字順にソートし、時間に応じた順序でアップロードする必要があります。古いファイルを新しいファイルの前にアップロードする必要があります。1回のアップロードの中では、アップロードコンポーネントが自動的にファイルをソートします。複数回アップロードする場合は、常に以前よりも新しいデータをアップロードしてください。プロキシログファイルでデフォルトで使用される命名規則が保持されている場合、ファイル名はすでに正しくソートされています。
- 前にアップロードしたデータよりも古いデータは処理されません。
- ログファイルの内容は、アップロードに有効な特定の基準に一致する必要があります。
  - シスコは、アップロード前にログファイルを確認するためのログ検証ツールを提供しています。
  - ログファイルの先頭の 20 行をコピーしてログ検証ツールに貼り付け、エラーをチェックします。
  - エラーが表示されたら、ユーザがそのエラーを修正すると同時に、ツールはエラーのチェックを自動的に継続します。

b) [Add files] をクリックしてアップロードするログファイルを選択するか、ログファイルをアップロードボックスにドラッグアンドドロップします。

（注） [Clear files] をクリックして、アップロードボックスに追加されたすべてのファイルをクリアします。

c) [Start upload] をクリックすると、選択したログファイルが解析用 Cognitive Intelligence システムにアップロードされます。Cognitive Intelligence システムが結果を表示するまでしばらくかかります。

（注） データをドロップするリスクを最小限に抑えるため、Cognitive Intelligence システムは 5 時間後にアップロードされたデータの処理を開始します。これにより、処理が開始される前にすべてのアップロードを完了して、すべてが適切な順序で配置されるようにできます。

注意 手動から自動に切り替えると、すべてのアップロードが中止し、アップロードデータの処理が停止されます。アップロードしたデータはすべて廃棄されます。

（注） ページを閉じたり、ページから移動したりすると、現在のファイルアップロードが停止されます。

（注） 最初にすべての手動アップロードを停止するまで、自動アップロードを使用することはできません。すべてのデータが処理される前に切り替えると、移行の際に一部の分析データが消失する場合があります。システムがデータをドロップしないようにするには、最後の手動アップロードから 24 時間後に切り替えを実行します。

次のタスク

[Device Accounts] ページには、プロキシデバイスとその情報が一覧で表示されます。[Status] 列には、各デバイスのステータスが表示されます。

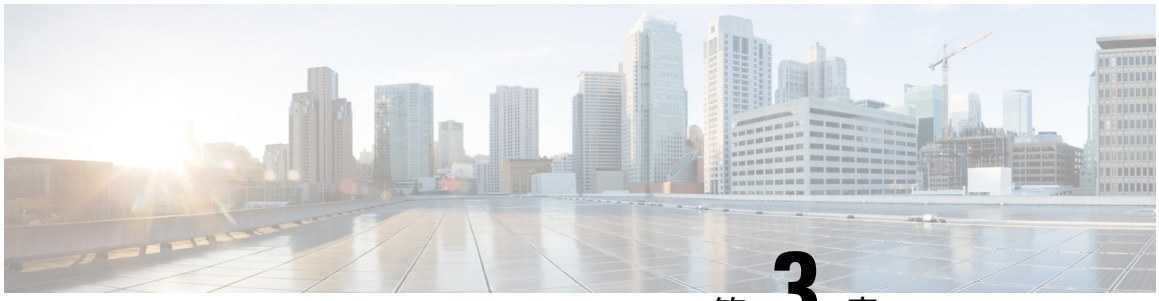
- New - SCP の設定が未完了で、SSH 公開キーが消失している場合があります
- Provisioning - プロビジョニング中のアカウントの準備がまだできていません
- Ready - アカウントが正常に作成されました
- Error - ステータスにカーソルを合わせると、エラーを説明するポップアップメッセージが表示されます

この概要ページから、別のデバイスアカウントの追加、削除するデバイスの選択、SSH 公開キーの入力、トラブルシューティングを行うことができます。

複数のデバイス間またはアップロードプロセス間でアカウントを共有できますが、各デバイスに個別のアカウントを使用し、ファイル名の競合の可能性を最小限に抑え、アップロード問題のトラブルシューティングを簡単にすることを推奨します。

デバイスアカウントの準備が完了したら、クリックして [Confirmed] ページまたは [Detected] ページを表示し、ネットワーク内の疑わしいアクティビティを確認します。

（注） 通常、データは、プロビジョニングの完了後 2 ～ 3 日以内に利用可能になります。



第 3 章

インシデント調査

概要

信頼度とリスクレベルに基づいて次のようにインシデントに対応します。

- **高いリスクと高い信頼度。**エンドポイントは、署名やルールベースのエンドポイントセキュリティを回避した高度な脅威により危険にさらされています。エンドポイントのクリーニングツールで脅威を削除できる見込みはありません。ユーザのプロファイルを完全にバックアップせずに、ドキュメントのみをバックアップして、エンドポイントを再イメージ化または再構築します。Cognitive Intelligence がアクティブなマルウェア感染を検出すると、通常は SOC とデスクトップチームからの手動操作が必要です。
- **中程度の信頼度または中程度のリスク。**エンドポイントには、エンドポイントのクリーニングツールで除去できるマルウェアが含まれています。選択したエンドポイントスキャンおよびアンチウイルスのクリーニングツールを実行します。発見した感染を除去し、エンドポイントを監視します。問題があれば、ユーザのプロファイルを完全にバックアップせずに、ドキュメントのみをバックアップして、エンドポイントの再イメージ化および再構築を実行します。
- **その他のすべて（低い信頼性および低いリスク）。**エンドポイントが感染しているかどうかは不明です。アラートは、スパムやフィッシング URL に従いユーザをリンクさせる可能性があります。通常のスキャンを実行し、発見された感染を除去します。何も見つからない場合、マルウェアの進行を防ぐために、すべてのエスカレーションのエンドポイントを監視します。

信頼度レベル：

- 高い（100 % ー 95 %）
- 中程度（94 % ー 85 %）
- 低い（84 % ー 0 %）

リスクレベル：

- 重大（10）
- 高い（9、8）
- 中程度（7、6）
- 低い（5、4、3、2、1）

詳細

ステップ 1 [Dashboard] タブをクリックします。

a) ヘルスステータス。ネットワークで検出された脅威の全体的な概要をリスクレベル別に表示します。未解決のユーザは、リスクカテゴリ別にグループ化されます。多数の低リスクの脅威は、時間の経過とともにより深刻な脅威につながる可能性があることに注意してください。

b) 相対的な脅威の危険性。同じセクター内の他の企業、同規模の企業、および世界中のすべての企業と比較した、インシデントの数とリスクレベルに基づく脅威の危険性。

c) 特定の動作。ネットワークで検出された脅威と未解決の動作の高レベルの内訳。

d) 最高リスク。現在ネットワークに最も高いリスクをもたらし、早急な対応が必要な未解決のインシデント。

e) 上位のリスクエスカレーション。最近リスクが増加している未解決のインシデント。

ステップ 2 [Confirmed] タブをクリックします。

a) このセクションでは、ネットワーク上で確認された脅威および侵害（100%の信頼レベルのインシデント）とその関連情報について示します。

b) 相関動作とともに検出されたインシデントは、脅威キャンペーンにグループ化され、各脅威キャンペーンは一意のハッシュタググループ名によってラベル付けされます。

c) 脅威キャンペーンは、ページの右側にある垂直のパネルに表示されます。状態ボックスをチェックして、どの脅威キャンペーンをパネルに表示するのかフィルタすることができます。

d) リスクの数字が大きければ、ネットワークに影響を与えるリスクが高い脅威であることを示します。クラスタ化されたインシデントを含む、より高いリスクの脅威を調査することで、分析の優先順位付けをします。

e) 調査に多くの時間を必要としないインシデントについては、迅速な対処が必要です。Cognitive Intelligence の結果に対してワークフローを調整するため、リカバリプロセスを設定します。

f) 脅威に固有の説明を確認し、対象をより明確にした修復のために推奨されるアクションを確認します。

ステップ 3 [Detected] タブをクリックします。

a) このセクションでは、相関性のない Cognitive Intelligence インシデントおよび AMP のレトロスペクティブ インシデントを含む、検出されたインシデントの概要を示します。また、[Confirmed] セクションの脅威にグループ化された、相関性のある Cognitive Intelligence インシデントを表示することもできます。

b) AMPやCognitive Intelligenceを選択し、日付選択、検索フィールド、環境設定、および状態を調整することで、どのインシデントが示されるかをフィルタすることができます。
c) [Email Notifications] ページを使用して電子メールアドレスを入力し、24 時間おきに新しい更新されたインシデントのサマリーが送信されるようにします。

ステップ 4 インシデントの調査を開始するには、そのインシデントをクリックして、その詳細を見直します。リスクと信頼性の高いものを優先してインシデントを調査します。インシデントは通常、複数のアクティビティや疑わしい動作のタイプで構成されます。

ステップ 5 影響を受けているデバイスまたはサーバを識別します。

ステップ 6 インシデント内の異常について情報を一覧できる並行座標グラフを調査します。相互接続情報を表示するには、折れ線グラフの各座標のノードにカーソルを合わせます。

a) リスク要因が最も高いものから開始し、低い方へと進みます。
b) [Time] 列の情報に注意します。マルウェアの活動がレポートされている時間の長さを確認します。高度なマルウェアの活動の特徴の 1 つは、通信が長期にわたって持続することです。インシデントが数日または数週間レポートされている場合は、高度なマルウェアによってインシデントが引き起こされている可能性が高まります。
c) 最近継続している活動を識別します。過去 48 時間の間に発生した異常に焦点を当てます。
d) 並行して発生する異常を探します。異常のシーケンスは、使用中のコマンドアンドコントロール通信チャネルを示唆する場合があります。
e) 接続された行を確認します。ドメインはまとまって成立していますか?それらが関連付けられていますか?IPアドレスが変わるのは、疑わしいドメインです。ドメインがデータを転送しているかどうかを判断するために、Web フローテーブルに関連付けます。
f) 多くの場合、より多くのマルウェアトラフィックが含まれているため、最も高いリスク要因に関連する異常を確認します。
g) 異常は、同じ AS、または異なる所有者および異なる場所の異なるシステムに結びついたものですか?ハッキングされ、攻撃元として使用されたシステムであることを示している可能性があります。

ステップ 7 Webフローをフィルタリングするには、グラフを使用できます。1つ以上のノードを選択してクリックし、関連する Web フローを表示します。

a) サーバの横のボックスに注意してください。赤のボックスは、そのサーバに対してマイナスの IP レピュテーションがあることを意味します。ドメイン名が含まれています。マイナスの IP レピュテーションは、攻撃者が運営するドメインからの疑わしい通信があったことを示すことがあります。
b) サーバから返される HTTP ステータスコードに注意してください。ステータスコードの横にある赤い [x] ボックスは、Webプロキシによってフローがブロックされたことを示します。ブロックされていないために、マルウェアの動作を許してしまっている、少なくとも 1 つのコマンドアンドコントロール（C&C）チャネルを持つインシデントに焦点を当てます。

ステップ 8 検出されたインシデントは、100%未満の信頼レベルです。実際のインシデントの詳細に基づいて、次の要因は、報告されたリスクを低減する、または増加する可能性があります。

リスクの低減	リスクの増加
レポートされた活動はプロキシですでにブロックされています。	レポートされた活動はプロキシでまだブロックされていません。

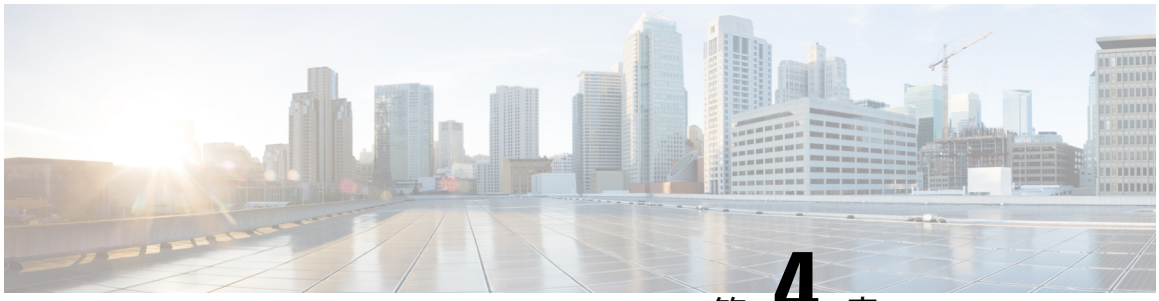
リスクの低減	リスクの増加
インシデントの特性（アクセスされた URL など）は、1 つのインシデントのみに固有です。	インシデントの特性（アクセスされた URL など）は、多くのユーザに繰り返されています。
インシデントの総量は、複数の要求を伴う 1 つの活動です。	インシデントの詳細は、長期にわたって、負荷が高く、永続的な動作を示します。
インシデントの詳細には、少量のデータ転送が表示されます。	インシデントの詳細には、大量のデータ転送、特にアップロードが表示されます。

次のタスク

収集した情報を分析して、このインシデントがネットワークに対して脅威であるかどうかを結論付けます。インシデントの詳細ページで、インシデントが脅威として解決されたか、誤検出として解決されたか、または無視として解決されたかをマークします。

脅威を緩和するため、組織の標準によるインシデント対応手順に従ってください。内部システムから脅威インテリジェンスより多くを収集することは、何らかのアクションを行う前の適切な慣行です。攻撃サイクルの侵害後のフェーズで運用をおこなっていることを、念頭に置いてください。これは、このフェーズ中に従来のセキュリティ対策が成功せず、脅威を完全に取り除くことができず、影響を受けたエンドポイントのイメージを再作成する必要性を意味します。

（注） 誤検出の数を減らすには、すべてのインシデントが事前にすぐにブロックされるわけではありません。異常は調査対象のインシデントとして検出およびレポートされます。分析、モニタリング、および時間追跡の後、脅威がブロックされたことを確認します。ただし、モーフィングマルウェアなどの脅威は検出を避けるために動作を変更できます。そのため、Cognitive Intelligence では時間経過とともに継続的にファイルを分析し、SenderBase に情報を送信し、Web-Based Reputation Score（WBRS）を更新しています。Cisco Security 製品は、次に脅威をブロックしますが、これが最終処理の包括的ソリューションであると見なすべきではありません。Cisco Security 製品が行うブロックは、通信の一部のみを対象としている場合があります。たとえば、Cisco Security 製品で保護されていない場所から接続した場合、マルウェアは、データを隠し、後からこっそり持ち出す可能性があります。完全なものにするには、感染したデバイスのイメージを作成し直します。



第 4 章

STIX/TAXII サービス

概要

Cognitive Intelligence では、詳細な相関分析およびアーカイブのために、検出されたインシデントの情報をクライアントに取り込むことができます。このサービスは、Security Information and Event Management（SIEM）システムとの統合のため、MITRE の Trusted Automated eXchange of Indicator Information（TAXII）標準をサポートしています。TAXII 標準は、システム間のサイバー脅威情報の共有に使用される転送メカニズムを指定するものです。

TAXII の詳細については、次を参照してください。

TAXII MITRE 組織

TAXII プロジェクト GitHub

各インシデントの情報は、Structured Threat Information eXpression（STIX）言語形式を使用して表されます。STIX はサイバー脅威情報を表す構造化言語であるため、一貫した方法で共有、保存、および分析できます。STIX 形式を使用すると、Cognitive Intelligence が階層形式での侵害検出の調査結果を示すことができます。TAXII サービスは、Cognitive Intelligence が検出したインシデントの記述に STIX 言語のサブセットを使用します。現在サポートされているオブジェクトは次のとおりです。

- キャンペーン - 確認された脅威カテゴリ（利用できる場合）
- インシデント - 異常な活動
- TTP - 戦術、手法、手段
- 監視 - Web 要求
- インジケータ - 観察可能な条件を識別するパターン

STIX の詳細については、次を参照してください。

https://stix.mitre.org/

ポーリングサービス

ポーリングサービスは、標準化された TAXII 転送メカニズムを使用して Cognitive Intelligence から TAXII 規格をサポートするクライアントにインシデント情報を送信します。インシデント情報を取得するには、TAXII クライアントは TAXII ポーリングサービスにポーリング要求を送信します。承認されたユーザだけにアクセスを制限するため、HTTP 基本認証が使用されます。次に、TAXII ポーリングサービスは、Cognitive Intelligence から TAXII クライアントにインシデント情報を送信することで応答します。すべてのデータ転送を保護するために HTTPS プロトコルが使用されます。

SIEM やその他のセキュリティ ワークフロー システムは、ネイティブで STIX/TAXII をサポートしている必要があります。サードパーティの TAXII クライアントが定期的に TAXII ポーリングサービスにポーリングを実行するように構成します。

- アカウント情報を取得するには、STIX/TAXII サービスを要求します。
  - 右上隅にあるグローバル設定の歯車アイコンをクリックします。
  - [CTA STIX/TAXII API] をクリックします。
  - [Add account] ボタンをクリックします。
  - アカウントを特定する名前を入力し、[Add account] ボタンをクリックします。
- プロビジョニングプロセスが完了したら、アカウント情報が表示されます。ウィンドウを閉じる前に、安全な場所にこのアカウント情報をコピーします。

（注） セキュリティ上の理由により、シークレットパスワードは 1 度しか表示されません。シークレットパスワードを失くした場合は、既存のシークレットパスワードを廃止し、新しいシークレットパスワードを生成する必要があります。

- 固有の属性をサードパーティの TAXII クライアントにコピーするには、次のものを使用します。
  - pollEndpoint またはフィードサービス URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
  - ユーザ名
  - パスワード
  - コレクション名またはフィード名

（注） Cognitive Intelligence（旧 Cognitive Threat Analytics または CTA）は、2018 年 8 月に Amazon Web Services の新しい場所への移行を開始したため、サービスにアクセスして使用するための新しい IP アドレスと追加の URL があります。サービスへのアクセスを維持するには、アウトバウンド ファイアウォール ルールの更新が必要な場合があります。2018 年 11 月のスイッチオーバー後は、古いデータ取得サービスの IP アドレスにデータを正常に送信できなくなります。必要な変更およびその他の重要な情報の詳細については、「Field Notice」を参照してください。

（注） シスコでは、サードパーティ製品または SIEM デバイスを構成するためのテクニカルサポートを提供していません。問題発生時には、ベンダー固有のサポートチームに問い合わせてください。

または、シスコから TAXII クライアント例をダウンロードして使用できます。SIEM または他のセキュリティシステムがネイティブで STIX/TAXII をサポートしていない場合、シスコは軽量な Java TAXII Log Adapter を提供します。これは、SIEM の最も近くにある Linux または Windows の仮想マシン環境に配備できます。セットアップ手順を表示するために提供されているリンクをクリックします。アダプタは、TAXII API を使用して、新しいインテリジェンスの定期的ポーリングを実行し、データを STIX メッセージで提供します。STIX メッセージは、アダプタによって、一般的な SIEM システムで受け入れられる他の形式に変換されます。

ポーリングサービスの安定性、パフォーマンス、および可用性をサポートするには、次を行います。

- 1 つの TAXII クライアントに許容されるポーリングは、10 分ごとに 1 回だけです。それ以外の場合、このエラーを示すステータスメッセージが返されます。
- ポーリング要求は、最大で 3 日までインシデント情報を取得できます。
- インシデント情報は、30 日間取得できるように保存されます。

ポーリング要求

TAXII クライアントから TAXII ポーリングサービスへのポーリング要求の例を次に示します。

メソッドは POST です。

HTTP 要求ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

要求本文：

```
<taxii_11:Poll_Request
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                            message_id=" " collection_name=" ">

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

サポートされる要求パラメータ	説明
Poll_Request	
message_id	TAXII 仕様に従って、各要求に対してランダムに生成された文字列。要求ごとに一意の文字列を再生成します。
collection_name	Cognitive Intelligence サービスから抽出または取得されるコレクションの名前。この属性は、Cisco によってプロビジョニングプロセスの完了後に提供されます。
Exclusive_Begin_Timestamp	時間枠に応じてこの値を調整します。
Inclusive_End_Timestamp	時間枠に応じてこの値を調整します。
Poll_Parameters	
allow_asynch	この属性は常に false に設定します。

（注） **Exclusive_Begin_Timestamp** と **Inclusive_End_Timestamp** の間でサポートされる最大の差は 3 日です。差がこれを超えている場合、返される結果は **Inclusive_End_Timestamp** から 3 日前までに制限されます。

ポーリング応答

TAXII ポーリングサービスから TAXII クライアントへのポーリング応答の例を次に示します。

HTTP 応答ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

応答本文：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Poll_Response xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                 xmlns:c="http://cybox.mitre.org/cybox-2"
                 xmlns:cc="http://cybox.mitre.org/common-2"
                 xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
                 xmlns:coa="http://stix.mitre.org/CourseOfAction-1"
                 xmlns:sc="http://stix.mitre.org/common-1"
                 xmlns:ind="http://stix.mitre.org/Indicator-2"
                 xmlns:ttp="http://stix.mitre.org/TTP-1"
                 xmlns:inc="http://stix.mitre.org/Incident-1"
                 xmlns:s="http://stix.mitre.org/stix-1"
                 collection_name=" " more="true"
                  result_id=" " result_part_number="1"
                  in_response_to="generatedMessageID" message_id="responseMessageID">
    <t:Exclusive_Begin_Timestamp>2015-01-17T15:11:00.648Z</t:Exclusive_Begin_Timestamp>
    <t:Inclusive_End_Timestamp>2015-01-20T15:11:00.649Z</t:Inclusive_End_Timestamp>
    <t:Content_Block>
      <t:Content_Binding binding_id="STIX_XML_1.1"/>
      <t:Content>
        <s:STIX_Package xmlns:cta="http://cisco.com/td/cta"
               id="cta:package-1412045744-66911c07-c9b8-4389-8888-00e438f58c2e"
               timestamp="2015-01-20T15:11:02.766Z" version="1.1.1">
          <s:STIX_Header>
            <s:Package_Intent>Incident</s:Package_Intent>
              <s:Information_Source>
                <sc:Identity id="cta:customer-1234567890"/>
                <sc:Tools>
                   <cc:Tool id="cta:tool-cta">
                       <cc:Name>Cognitive Threat Analytics</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
                   <cc:Tool id="cta:tool-amp">
                       <cc:Name>Advanced Malware Protection</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
                </sc:Tools>
             </s:Information_Source>
          </s:STIX_Header>
          <s:Incidents>
            <s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="inc:IncidentType"
                    id="cta:incident-1412045744_f8bae03fb2ff7d6185907ae3240d_ITMAL1">
             <inc:Title>malware|using automatically generated domain (DGA)</inc:Title>
             <inc:Victim>
                 <sc:Name>JohnDoe</sc:Name>
             </inc:Victim>
              <inc:Related_Indicators>
               <inc:Related_Indicator>
                <sc:Indicator xsi:type="ind:IndicatorType"

id="cta:indicator-1412045744_1421623800000_f8bae03fb2ff7d6185907ae3240d_0">
                 <ind:Observable>
                  <c:Observable_Composition operator="AND">
                    <c:Observable>
                     <c:Object>
                      <c:Properties xsi:type="co:CustomObjectType">
                       <cc:Custom_Properties>
                        <cc:Property name="timestamp">1421623882432</cc:Property>
                        <cc:Property name="xElapsedTime">1810</cc:Property>
                        <cc:Property name="scHttpStatus">0</cc:Property>
                        <cc:Property name="csContentBytes">622</cc:Property>
                        <cc:Property name="scContentBytes">907</cc:Property>
```

```
                                    <cc:Property name="csUrl"></cc:Property>
                                    <cc:Property name="sIP">195.22.26.231</cc:Property>
                                    <cc:Property name="cIP">33.196.39.11</cc:Property>
                                    <cc:Property name="cUsername">JohnDoe</cc:Property>
                                    <cc:Property name="sReputation">-580</cc:Property>
                                    <cc:Property name="sCategory">unclassified</cc:Property>
                                   </cc:Custom_Properties>
                                  </c:Properties>
                                 </c:Object>
                                </c:Observable>
                                <c:Observable>
                                 <c:Object>
                                  <c:Properties xsi:type="co:CustomObjectType">
                                   <cc:Custom_Properties>
                                    <cc:Property name="timestamp">1421623896635</cc:Property>
                                    <cc:Property name="xElapsedTime">1942</cc:Property>
                                    <cc:Property name="scHttpStatus">0</cc:Property>
                                    <cc:Property name="csContentBytes">361</cc:Property>
                                    <cc:Property name="scContentBytes">582</cc:Property>
                                    <cc:Property name="csUrl"></cc:Property>
                                    <cc:Property name="sIP">195.22.26.231</cc:Property>
                                    <cc:Property name="cIP">33.196.39.11</cc:Property>
                                    <cc:Property name="cUsername">JohnDoe</cc:Property>
                                    <cc:Property name="sReputation">-580</cc:Property>
                                    <cc:Property name="sCategory">unclassified</cc:Property>
                                   </cc:Custom_Properties>
                                  </c:Properties>
                                 </c:Object>
                                </c:Observable>
                               </c:Observable_Composition>
                              </ind:Observable>
                              <ind:Indicated_TTP>
                               <sc:TTP xsi:type="ttp:TTPType">
                                <ttp:Title>communication to automatically generated domain
(DGA)</ttp:Title>
                               </sc:TTP>
                              </ind:Indicated_TTP>
                             </sc:Indicator>
                            </inc:Related_Indicator>
                           </inc:Related_Indicators>
                           <inc:Discovery_Method>Log Review</inc:Discovery_Method>
                           <inc:COA_Requested>
                            <inc:Course_Of_Actionxsi:type="coa:CourseOfActionType">
                             <coa:Stage>Remedy</coa:Stage>
                             <coa:Type>Eradication</coa:Type>
                           <coa:Parameter_Observablescybox_major_version="2"cybox_minor_version="1">

                              <c:Observable_Package_Source>
                               <cc:Time>
                                <cc:Produced_Time>2016-08-15T17:02:02.616Z</cc:Produced_Time>
                               </cc:Time>
                              </c:Observable_Package_Source>
                              <c:Observable>
                               <c:Object>
                                <c:Propertiesxsi:type="user:UserAccountObjectType">
                                 <user:Username>JohnDoe</user:Username>
                                </c:Properties>
                               </c:Object>
                              </c:Observable>
                              <c:Observable>
                               <c:Object>
                                <c:Propertiesxsi:type="addr:AddressObjectType"category="ipv4-addr">
                                 <addr:Address_Value>33.196.39.11</addr:Address_Value>
                                </c:Properties>
```

```
                    </c:Object>
                   </c:Observable>
                  </coa:Parameter_Observables>
                 </inc:Course_Of_Action>
                </inc:COA_Requested>
                <inc:Confidence>
                 <sc:Value>Low</sc:Value>
                </inc:Confidence>
                <inc:Information_Source>
                    <sc:Tools>
                        <cc:Tool idref="cta:tool-cta"/>
                    </sc:Tools>
                </inc:Information_Source>
            </s:Incident>
          </s:Incidents>
         </s:STIX_Package>
        </t:Content>
    </t:Content_Block>
</t:Poll_Response>
```

（注） `Poll_Reponse` では、これ以上脅威項目がない場合、`more` と `result_id` の 2 つの属性はありません。`more=true` が指定されている場合は、`Poll_Fulfillment` を使用して応答の次のページを要求できます。

サポートされる応答オブジェクト	フィールドの説明
Poll_Response	
collection_name	Cognitive Intelligence サービスから抽出または取得されるコレクションの名前。この属性は、Cisco によってプロビジョニングプロセスの完了後に提供されます。
result_id	この値をポーリング履行要求にコピーします。
Exclusive_Begin_Timestamp	このポーリング応答によって対応する時間範囲の最初（この値を含まない）。このフィールドがない場合は、ポーリング応答がこの TAXII データフィードの最も早い時間に対応することを示します。
Inclusive_End_Timestamp	このポーリング応答によって対応する時間範囲の最後（この値を含む）。
Content_Block	返されたコンテンツ。
Content_Binding	
Content	
STIX_Package	STIX 言語に関する情報。

サポートされる応答オブジェクト	フィールドの説明
STIX_Header	STIX コンテンツのこのパッケージに関する情報。
Incidents	1 つ以上のインシデント。
Incident	1 つのインシデントに関する情報。
Title	このインシデントを説明するタイトル。
Victim	このインシデントの被害者に関する情報。
Related_Indicators	このインシデントに関連するインジケータを識別します。
Related_Indicator	このインシデントに関連する 1 つのインジケータを識別します。
Indicator	特定の観察可能な条件を識別するパターン、パターンの意味に関するコンテキスト情報、パターンのアクションの方法およびタイミングなどで構成されるインジケータ。
Observable	このインジケータに関連する監視。
Observable_Composition	他の監視の論理的な組み合わせを作成することで、高次の複合監視を指定できます。
Observable	単一の監視を表します。
Object	特定のオブジェクト（ファイル、レジストリキー、プロセス）の特性を識別します。
Properties	オブジェクトの操作の結果として列挙されたプロパティ。
Custom_Properties	既存の Properties スキーマで定義できない一連のカスタムオブジェクトのプロパティを指定することができます。
Property	オブジェクトの操作の結果として列挙された単一のプロパティ。
Indicated_TTP	このインジケータが示す、関連する戦術、手法、手段（TTP）を指定します。
Discovery_Method	コードを検出するために使用される手法やツールに関する情報。

サポートされる応答オブジェクト	フィールドの説明
COA_Requested	このインシデントに推奨される一連のアクション。
Confidence	このインシデントの特性で保持されている信頼性のレベルに関する情報。
Information_Source	このインシデントのソースに関する情報。
Tools	
Tool	Cognitive Intelligence と AMP のどちらのツールが、このインシデントを検出したか。

エラーが発生した場合、エラー メッセージが返されます。次に例を示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Status_Message
          xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1"
          xmlns:c="http://cybox.mitre.org/cybox-2"
          xmlns:cc="http://cybox.mitre.org/common-2"
          xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
          xmlns:sc="http://stix.mitre.org/common-1"
          xmlns:ind="http://stix.mitre.org/Indicator-2"
          xmlns:ttp="http://stix.mitre.org/TTP-1"
          xmlns:inc="http://stix.mitre.org/Incident-1"
          xmlns:s="http://stix.mitre.org/stix-1"
                status_type="FAILURE" in_response_to="23537"
                message_id="16ed0b75-2af6-4537-b71c-da00e0a0c419">
   <t:Message>An error occurred during request processing.</t:Message>
</t:Status_Message>
```

TAXII status_type	エラーの説明
	ユーザは認証されておらず、HTTP 応答ステータスコードが 404 です。
DENIED	ユーザは認証されておらず、HTTP 応答ステータスコードが 401 です。
BAD_MESSAGE	無効な要求メッセージです。`Message` パラメータを参照してください。
FAILURE	未指定のエラーです。`Message` パラメータを参照してください。

ポーリング履行

TAXII クライアントから TAXII ポーリングサービスへのポーリング履行要求の例を次に示します。

メソッドは POST です。

HTTP 要求ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

要求本文：

```
<taxii_11:Poll_Fulfillment
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                           message_id=" " collection_name=" "
                           result_id=" " result_part_number="2" />

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

サポートされる要求パラメータ	説明
Poll_Request	
message_id	TAXII 仕様に従って、各要求に対してランダムに生成された文字列。要求ごとに一意の文字列を再生成します。
collection_name	Cognitive Intelligence サービスから抽出または取得されるコレクションの名前。この属性は、Cisco によってプロビジョニングプロセスの完了後に提供されます。
result_id	ポーリング応答からこの値を貼り付けます。
result_part_number	ポーリング応答の値からこの値を 1 増やします。
Exclusive_Begin_Timestamp	時間枠に応じてこの値を調整します。
Inclusive_End_Timestamp	時間枠に応じてこの値を調整します。
Poll_Parameters	
allow_asynch	この属性は常に false に設定します。

（注） **Exclusive_Begin_Timestamp** と **Inclusive_End_Timestamp** の間でサポートされる最大の差は 3 日です。差がこれを超えている場合、返される結果は **Inclusive_End_Timestamp** から 3 日前までに制限されます。

共通のクエリ

このセクションでは、詳細な調査に向けて結果に優先度を設定するため、Cisco STIX/TAXII API で使用される共通のクエリの一部について説明します。クエリ例で使用する構文は、SPLUNK の統合に基づいており、象徴的なものです。特定のフィールドや値はローカルの統合によって異なる可能性がありますが、クエリの意味は SIEM システムおよび統合に広く適用されます。

ヒント SPLUNK に他のデータを収集している場合、ホスト、インデックス、またはソース名の先頭にクエリを追加して Cognitive Intelligence データのみを介して検索します。

Users Affected by Confirmed Threats

このクエリは確認済みの脅威を持つすべてのユーザを返します。また、デスクトップ修復のための Incident Response Team に報告することができます。これらのインシデントもリスクが高い場合は、影響を受けるデバイスの再イメージングを検討します。このクエリは、影響を受けるユーザ名およびキャンペーン名を持つテーブルを作成します。次のようにして空でないキャンペーン名を検索し、username+campaign ペアの重複を排除します。

```
campaign!="" | table cUsername campaign | dedup cUsername campaign | sort + cUsername
```

または、次のようにキャンペーン名の複数値のフィールドを使用します。

```
campaign!="" | transaction cUsername | table cUsername campaign | sort + cUsername
```

Users Affected by Confirmed Threats Within a Timeframe

このクエリには、最初に表示された列および最後に表示された列も含まれています。空でないキャンペーンを検索し、username+campaign ペアで集約し、Web フローのタイムスタンプの最小値および最大値を計算します。結果はエポックミリ秒単位ですが、必要に応じて、カレンダー時間に変換できます。

```
campaign!="" | stats min(timestamp) max(timestamp) by cUsername campaign
```

または、strftime 関数を使用してエポックの変換を含めます。次の例では、ミリ秒を削除するため、タイムスタンプを 1000 で割っています。

```
campaign!="" | stats min(timestamp) as oldest max(timestamp) as newest by cUsername
campaign |
  eval oldest_time=strftime(oldest/1000,"%m/%d/%y %H:%M:%S") |
```

```
eval newest_time=strftime(newest/1000,"%m/%d/%y %H:%M:%S") |
table cUsername, campaign, oldest_time, newest_time
```

Users Affected by High Risk and High Confidence Incidents

このクエリは、確認されたキャンペーンの有無にかかわらず、高いリスクおよび高い信頼性を持つユーザの優先順位リストのテーブルを生成します。高いリスクと高い信頼性を検索し、ユーザ名の重複を排除します。これらすべてのインシデントは高いリスクかつ高い信頼性であるため、影響を受けるデバイスの再イメージングを検討します。

```
confidence="High" risk="High" | dedup cUsername | table cUsername campaign
```

Users Affected by Campaign

このクエリは、感染したユーザ数について、時間の経過とともにキャンペーンで分割したグラフを生成します。空でないキャンペーンを検索し、1 日の期間で bin を実行し、その bin 内のユーザ名の明確な数を計算します。

```
campaign!="" | timechart dc(cUsername) span=1d by campaign
```

（注） SPLUNK では、タイム チャート ショートカットを使用できます。

Command and Control Servers

このクエリは、確認されたカテゴリで検出されたすべてのコマンドおよび制御（C&C）サーバのリストを生成します。サーバの IP アドレスとキャンペーンを表示する一方で、空でないキャンペーンを探して、サーバ IP アドレスの重複を排除します。検索の結果、C&C の通信を維持するために感染したデバイスで使用される C&C 宛先 IP アドレスをリストします。各 C&C IP アドレスごとに、どの脅威キャンペーンに含まれているのかも分かります。より多くのインテリジェンスの他のシステムを照会し、セキュリティ侵害の指標（IOC）を提供し、感染したエンドポイントの悪意のあるプロセスとアプリケーションを特定するために使用できます。

```
campaign!="" | table sIP campaign | dedup sIP
```

Cisco ISE との統合

Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。Cisco ISE はポリシーデシジョンポイントとして動作し、企業におけるコンプライアンスの遵守、インフラストラクチャのセキュリティの向上、およびサービスオペレーションの合理化を可能にします。企業は、Cisco ISE を使用して、ネットワーク、ユーザ、およびデバイスから状況情報をリアルタイムで収集できます。その後、その情報を使用して、ネットワーク内のさまざまな要素にアイデンティティを関連付けることで、プロアクティブなガバナンスの判断を行うことができます。

Cognitive Intelligence は Cisco ISE と統合され、ネットワークレベルの隔離を提供します。この機能は、感染したデバイスをネットワークから切断する機能を備えており、機密データをそれ以上漏洩できないようになっています。Cognitive Intelligence と Cisco ISE の統合では、STIX / TAXII を使用します。システムが個々のユーザに感染したと見なすことができる重大レベルのリスクが検出された場合、Cisco ISE は Requested Course of Action（要求された一連のアクション）を受信します。これにより Cisco Rapid Threat Containment フレームワークの一部である Threat Centric Network Access Control（TC-NAC）検疫が提案されます。 Requested Course of Action は、感染に関連するリスクに応じて、モニタリング、根絶、内部ブロック、またはその組み合わせになります。内部ブロッキングは、TC-NAC のブロッキングポリシーで使用することを目的とした一連のアクションです。詳細については「Cisco Rapid Threat Containment」を参照してください。

Cisco ISE と、Cognitive STIX / TAXII サービスによって提供されるデータフィードを使用して、独自のソリューションを開発できます。データフィードには、感染したデバイスの識別と実行するアクションに関する情報が含まれています。Cognitive STIX / TAXII フィードの推奨事項に基づいて、Cisco ISE で検疫ポリシーを定義できます。Cisco ISE で Cognitive アダプタを設定する方法については、『Cisco ISE Administrator Guide, Release 2.2』を参照してください。

（注） Cognitive Intelligence は Web プロキシログにクライアント IP アドレスまたはユーザ名としてリストされているユーザ ID を処理します。具体的には、IP アドレスの場合、プロキシログで使用可能な IP アドレスが、企業内部ネットワークの（別のデバイスの）IP アドレスと競合する IP アドレスである可能性があります。たとえば AnyConnect 経由で接続するローミングユーザと、インターネットに直接接続するスプリットトンネルが自宅で獲得するローカル IP アドレス（例：10.0.0.x）が、企業内部ネットワークで使用されている重複するプライベート範囲の IP アドレスと競合することがあります。Rapid Threat Containment ポリシーを定義する場合は、不適合デバイスに検疫アクションが適用されないように、論理ネットワークアーキテクチャを考慮してください。