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。「CTA STIX/TAXII Service」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。