

Cisco Stealthwatch 7.0 v1 - インスタント デモ



最終更新日 : 2019 年 9 月 27 日

インスタント デモについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

[インスタント デモについて](#)

[要件](#)

[このソリューションについて](#)

[トポロジ](#)

[はじめに](#)

[シナリオ 1. リアルタイム リスク](#)

[シナリオ 2. ポリシーの検証](#)

[シナリオ 3. データ盗難の調査](#)

[シナリオ 4. コグニティブ分析の統合](#)

[シナリオ 5. ETA 暗号化アシュアランス](#)

[次に必要な作業](#)

要件

次の表に、このデモンストレーションの要件の概要を示します。

| 必須 | オプション |
|--------|-------------------|
| ラップトップ | Cisco AnyConnect® |

このソリューションについて

Stealthwatch システムは、エンタープライズ ネットワーク内部での疑わしいトラフィック パターンを識別して、高度な脅威に対する優れた可視性を提供します。これらの疑わしいパターンに他のデバイスのコンテキスト情報を付加して、全体的な分析精度を高め、アクティビティに関連付けられた特定の脅威レベルを定めます。このソリューションには、次の機能が含まれます。

- 機密情報が失われたり重要なビジネス運営が中断されたりする前に、高度な脅威をすばやく検出し緩和します。
- ネットワーク全体をセンサーにすることで、ネットワーク全体の状況を把握できます。
- ネットワーク全体で高度なマルウェアの伝播を検出します。
- 既存のネットワーク インフラストラクチャ上に、高度な脅威検出および対応機能を構築できます。
- ネットワーク デバイスを通過するトラフィックに対し、エンドツーエンドの可視性を提供します。
- 調査と分析のために、疑わしいトラフィックと通常のトラフィックのトラフィック フローを長期間保存します。
- 暗号化されたトラフィック分析でコンプライアンスを実現し、マルウェアの暗号化された通信の検出を可能にします。

Stealthwatch によって、運営を保護して収益源を保持し、損失と漏洩を回避することでコストを削減し、デジタルエンタープライズに伴うリスクを低減させることが可能になります。

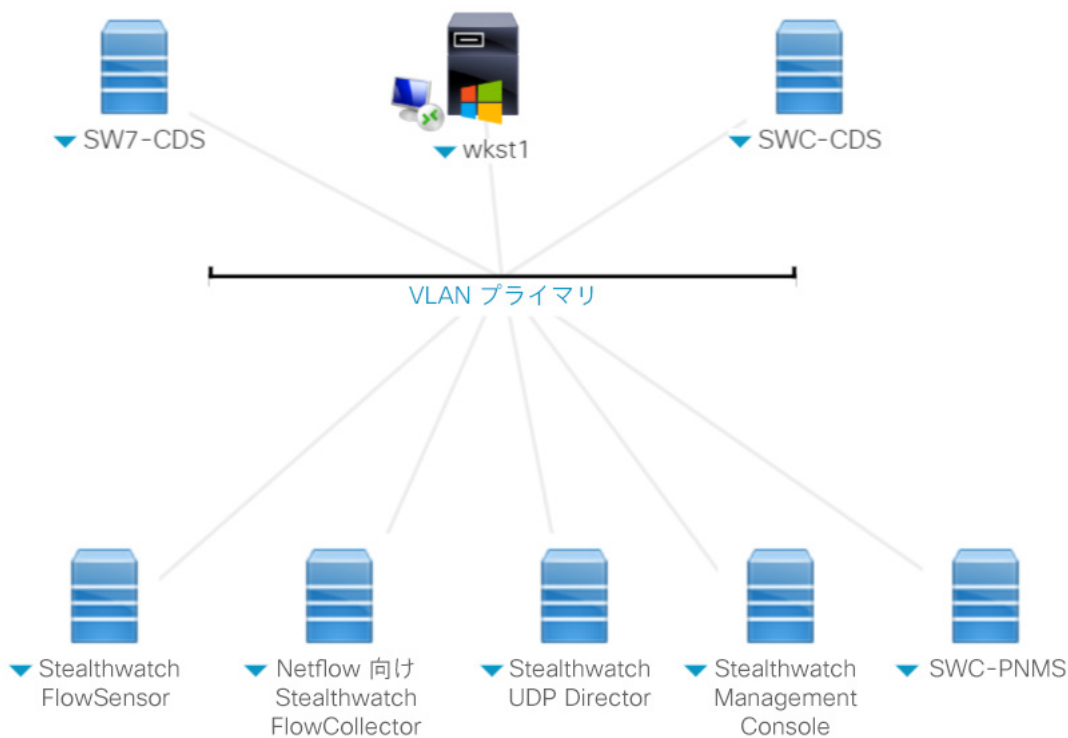
このソリューションの主なコンポーネントは次のとおりです。

- Netflow テレメトリおよびその他のデータを集約および分析して、脅威や異常動作を検出。Stealthwatch システムにより提供されます。
- ネットワーク全体のセキュリティ テレメトリ。Cisco Catalyst® スイッチ、シスコ ルータ、Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス (ASA)、Cisco Netflow Generation Appliance からの Netflow エクスポートにより提供されます。
- 認証、ポストチャ検証、デバイス プロファイリングを含む、ユーザとデバイスのアイデンティティ コンテキスト。Cisco Identity Services Engine (ISE) により提供されます。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザおよびコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブセッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

dCloud のトポロジ



はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

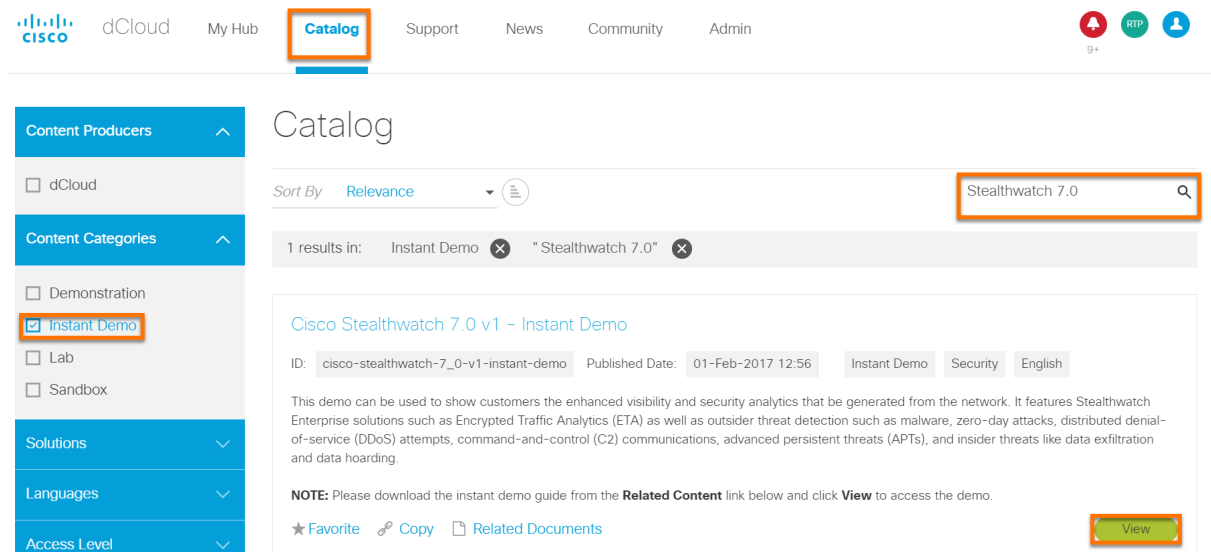
場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ (Catalog)] をクリックして、サイド バーから [インスタントデモ (Instant Demo)] を選択します。これで、すべての dCloud インスタント デモが一覧表示されます。
2. 該当する [表示 (View)] ボタンをクリックします。

注： または、[カタログ検索 (Search Catalog)] ボックスを使用してインスタント デモの名前を検索することもできます。



The screenshot shows the Cisco dCloud interface. At the top, there is a navigation bar with 'dCloud', 'My Hub', 'Catalog' (highlighted with a red box), 'Support', 'News', 'Community', and 'Admin'. On the right, there are user profile icons and a '9+' notification. The main content area is titled 'Catalog'. On the left, there is a sidebar with 'Content Producers' (dCloud) and 'Content Categories' (Demonstration, Instant Demo (checked and highlighted with a red box), Lab, Sandbox). Below the sidebar are filters for 'Solutions', 'Languages', and 'Access Level'. The main search area shows 'Sort By Relevance' and a search box containing 'Stealthwatch 7.0' (highlighted with a red box). Below the search box, it says '1 results in: Instant Demo x "Stealthwatch 7.0" x'. The search result is 'Cisco Stealthwatch 7.0 v1 - Instant Demo'. It includes an ID, published date, and tags like 'Instant Demo', 'Security', and 'English'. A description follows, and a 'NOTE' is provided. At the bottom right of the result card, there is a 'View' button (highlighted with a red box).

3. [ユーザ名 (User Name)] フィールドに「amdemo1」と入力し、[パスワード (Password)] フィールドに「C1sco12345」と入力して、[サインイン (Sign In)] をクリックします。



Stealthwatch

USER NAME *

amdemo1

This is a Required Field

PASSWORD *

Sign In

シナリオ 1. リアルタイム リスク

価値提案 : Stealthwatch ダッシュボードの概要は、お客様のネットワーク内の脅威環境をリアルタイムに把握するために使用できます。ネットワーク内にどのような脅威が存在しているのかということをお客様が懸念している場合は、ここから始めるのが適切です。

ネットワーク セキュリティは従来、境界上のデバイスに依存してきました。この方法には、ネットワーク内で発生している事象を十分に分析できないという欠点がありました。ネットワーク内のすべてのデバイスで Netflow を有効にし、その情報を Stealthwatch システムに送信することで、ネットワーク全体の脅威に対する可視性が得られ、ネットワーク全体をセキュリティ センサーにすることができます。

課題 - リスクに焦点を当てる

- 境界型セキュリティでは内部の脅威を認識できないため、ネットワークがセキュアであるとは限らない

利点 - リスクの低減に焦点を当てる

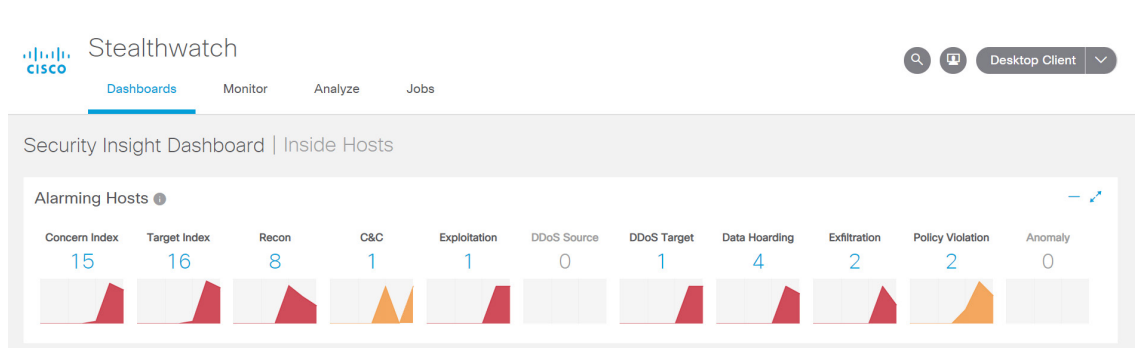
- 環境全体におけるセキュリティ上の脅威と異常な行動について、ネットワーク全体でリアルタイムの可視性が得られるようにする

手順

注 : システムに初めてログインすると、ダッシュボードに現在の脅威環境が表示されます。

- ダッシュボードの上部にある [アラーム受信ホスト (Alarming Host)] ウィジェットには、現在のセキュリティ イベントが表示されます。

注 : イベントは、ポリシー、異常、攻撃、エクスプロイトなど、セキュリティ関連の違反が検出されると生成されます。

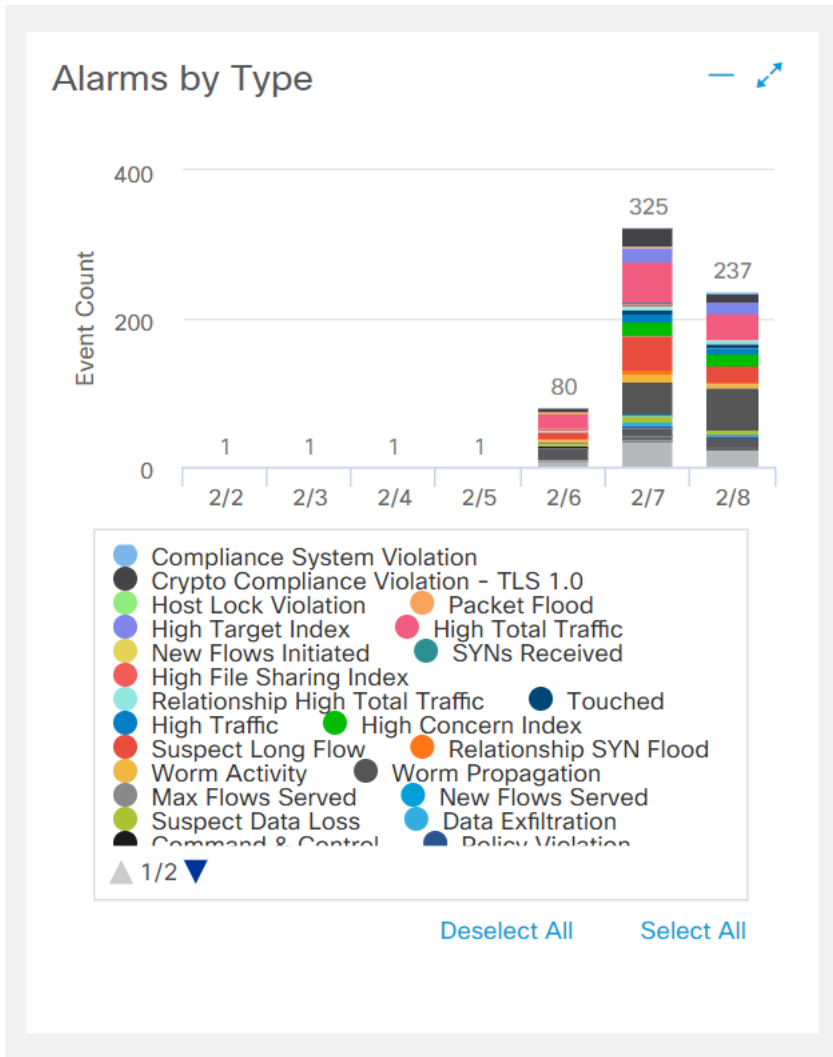


注 : カテゴリ内のトレンドの数字は、定期的に変更され更新されます。これは通常の動作であり、Stealthwatch デモ システム内でリアルタイムに収集されたデータが反映されています。

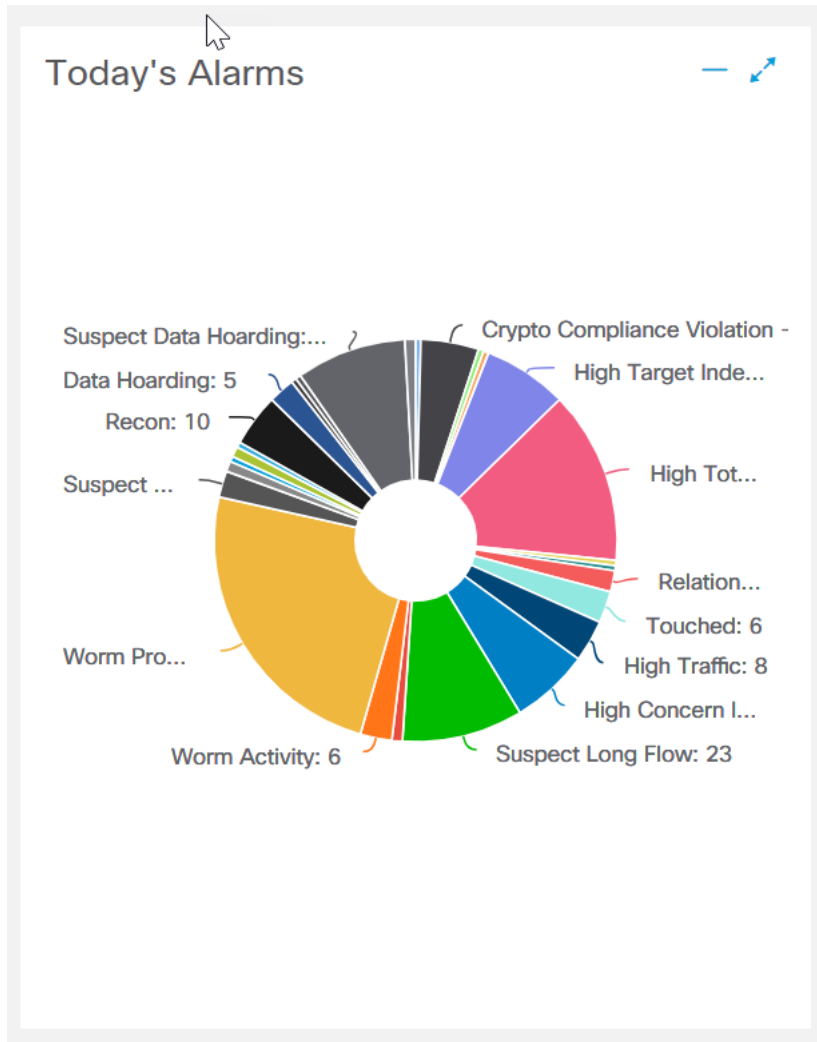
2. アラームには次のカテゴリがあります。

- [懸念インデックス (Concern Index)]- ネットワーク内で攻撃者として行動しているホスト
 - [ターゲット インデックス (Target Index)]- スキャンやその他の悪意ある攻撃のターゲットまたは被害者になっているホスト
 - [Recon]- 悪意のある可能性がある不正なスキャンが TCP または UDP を使用してネットワーク内のホストに対して実行されていることを示します。偵察と呼ばれるこれらのスキャンは、ネットワークに対する攻撃の兆候であり、ネットワークの内部または外部からスキャンが行われている可能性があります。
 - [C&C]- ネットワーク内にボットに感染したサーバまたはホストが存在し、C&C サーバに接続を試みていることを示します。
 - [エクスプロイト (Exploitation)]- ワームの拡散やブルート フォースによるパスワード解読などによる、ホスト相互の直接的な侵害を追跡します。
 - [DDoS ソース (DDoS Source)]- サービス拒否のソースとして動作するホスト
 - [DDoS ターゲット (DDoS Target)]- サービス拒否のターゲットとして動作するホスト
 - [データ ホーディング (Data Hoarding)]- ネットワーク内の 1 つ以上のホストから異常なほど膨大なデータをダウンロードするホスト (East-West)
 - [漏洩 (Exfiltration)]- 異常な量のデータが転送された内部または外部のホストを追跡します (South-North) 。
 - [ポリシー違反 (Policy Violation)]- ポリシー内のルールの違反
 - [異常 (Anomaly)]- ホストの動作が異常であるか、異常なトラフィックを生成しているが、別のカテゴリのアクティビティとは一致しないことを示すイベントを追跡します。
3. 上記の情報は、発生している事態に関する分析を得るために役立ちます。現在のアラームの下にある各種のダッシュボードを見ると、一定期間に存在する脅威を確認できます。

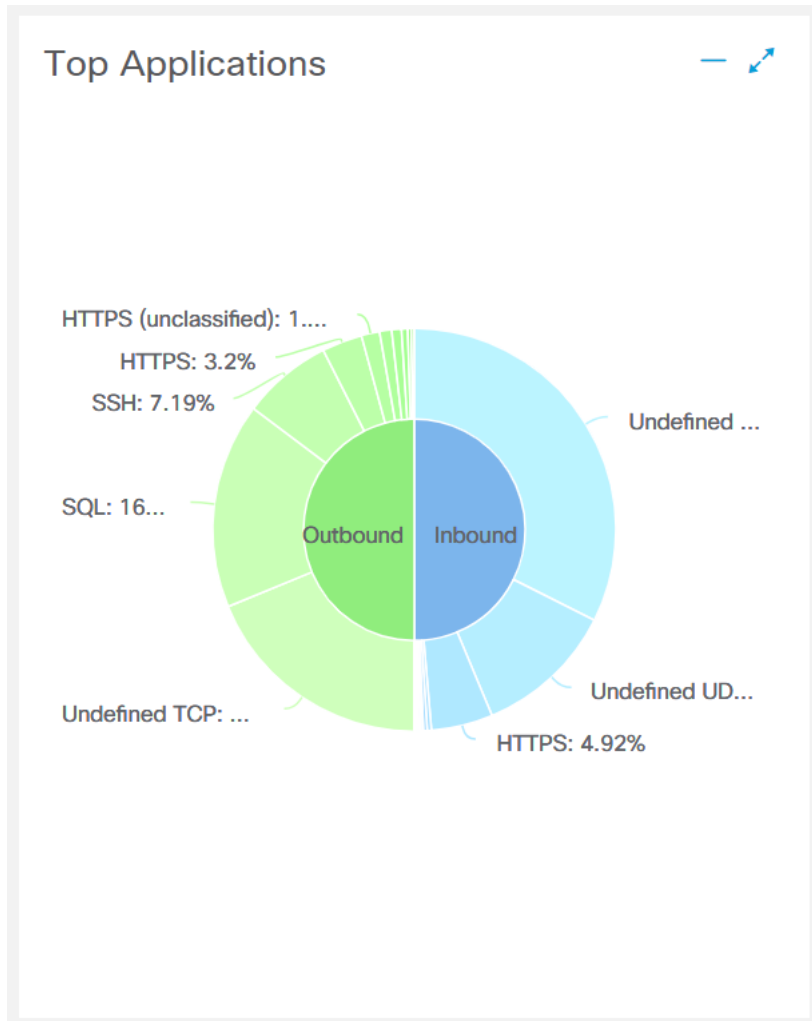
4. [タイプ別アラーム (Alarms by Type)] ウィジェットには、過去 1 週間にわたるすべてのアラームの内訳がタイプと頻度別に示されます。



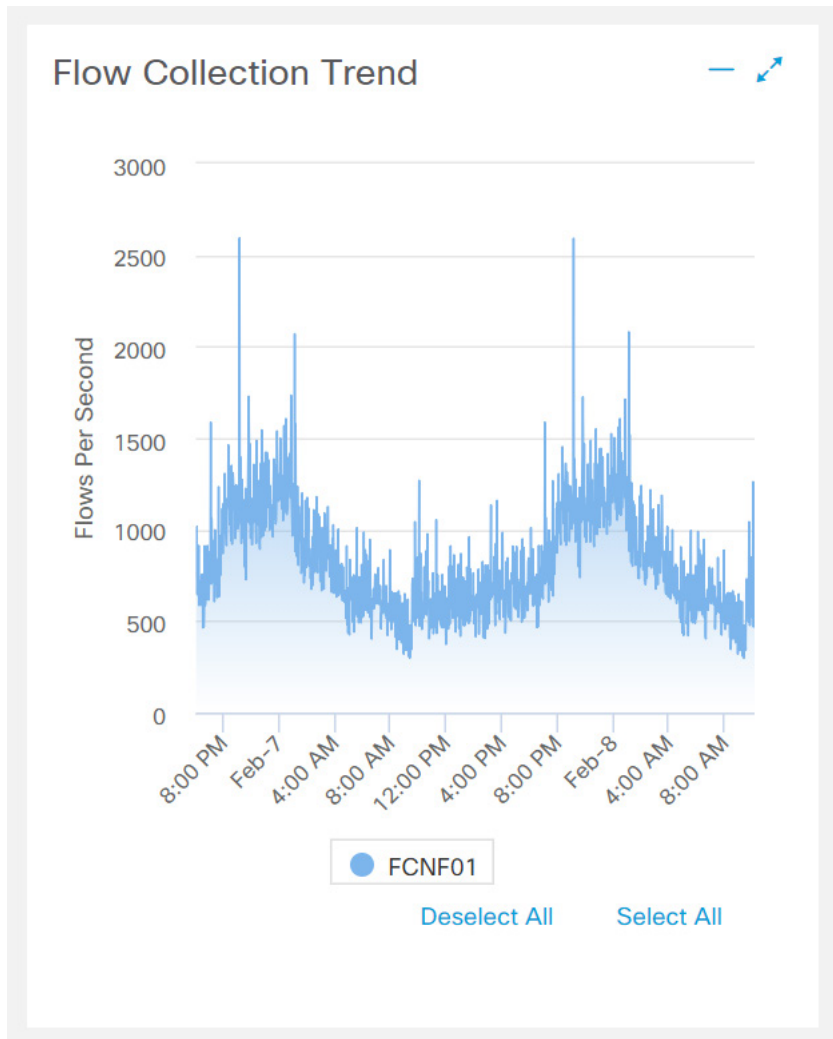
5. [今日のアラーム (Today's Alarms)] ウィジェットには、最後のアーカイブ時間以降に発生したすべてのアラームのスナップショットが表示されます。



6. [ランキング上位のアプリケーション (Top Application)] ウィジェットには、過去 24 時間でランキング上位のアプリケーションが示されます。



7. [フロー収集のトレンド (Flow Collection Trend)] ウィジェットには、過去 48 時間にわたるネットワーク経由のフロー データの総量が示されます。これは、フロー ボリュームの基準となる通常のトレンドを視覚的に確認し、異常な動作を即座に目視するのに役立ちます。



まとめ

多くの組織は、境界ベースのネットワーク セキュリティに投資しています。境界では有効ではあっても、セキュリティはネットワーク境界で終わるものではありません。Stealthwatch システムでは、Netflow から提供された情報が実用的なインテリジェンスに変換され、セキュリティ チームは見えない攻撃者を検出することが可能になります。Stealthwatch では脅威がリアルタイムに検出されるとともに、日次および週次のサマリーも得られます。お客様は即時にデータにアクセスでき、リスクが低減します。

シナリオ 2. ポリシーの検証

価値提案：このシナリオでは、包括的なフロー クエリ ツールを使用して、ホスト デバイス コミュニティ間のネットワークのセグメンテーションを手動で検証します。お客様が、事業部門、製造用装置、IOT センサー、医療機器などが、他の組織やデバイスからセキュアに分離されている状態を維持したいと考えている場合は、このデモによってセグメンテーションの有効性を示すことができます。セキュリティの取り組みの有効性をすばやく見極めるために、どのような手法を今すぐに採用すべきでしょうか。

ネットワーク レベルでセキュリティを考えると、すぐに思いつくのはファイアウォールやアクセス制御リスト、またはその他の静的で複雑な方法によるセキュリティ強化です。VRF のような他の手法によるトラフィックの分離やホスト コミュニティの遮断では、多くの場合、複雑性がさらに高まります。こうした静的な方法では、俊敏性が課題になり、ネットワークにデバイスを追加するたびにセキュリティ コストが増大します。またネットワーク全体で一貫性のあるポリシーを維持しようとするれば、複雑性が高まります。このような問題自体が成功に対する障害になります。さらに、意図した目標の達成において、こうした取り組みが有効かどうかを継続的に検証することにも大きな課題が残ります。

Stealthwatch ではその独自の機能によって、セキュリティ対策の導入前後のネットワークの状況を完全に把握できるため、セキュリティ投資の成果を適切に検証できます。

セグメンテーションや分離は、多くのお客様のセキュリティ フレームワークにとって重要な要素になっています。製造業では、IP 対応のロボット工学やプラント システムを通常のオフィス システムから分離する必要があります。医療分野では、医療機器がネットワークの他の部分から分離されています。多くの場合、デバイス レベルのセグメンテーションを検証するのは困難で、時間もかかります。さらに、完全に自動化されたエンドポイントが、その他の自動化されたエンドポイントのみと通信できる状態にあることを確認することは不可能です。意図したとおりにセキュリティ上の取り組みが機能しているかどうかを確認するには、完全で継続的な可視性が求められます。

検証は、長期的な使用を考慮したポリシー作成によって自動化できます。しかしこのデモンストレーションでは手動による検証を行い、セキュリティ対策の検証に Stealthwatch をどのように使用できるかを示します。この手動による例は、自動化、変更、適応を行うことで継続的な検証が可能になります。

課題 - リスクに焦点を当てる

- セキュリティ ポリシーの適用状況を検証する自動的なメカニズムがない

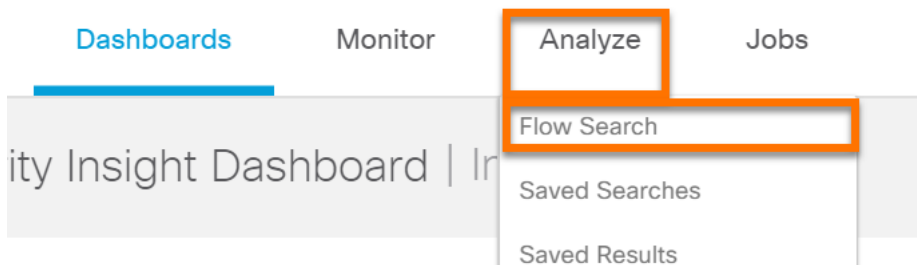
利点 - リスクの低減に焦点を当てる

- 環境全体におけるセキュリティ上の脅威と異常な行動について、ネットワーク全体でリアルタイムの可視性が得られるようにする

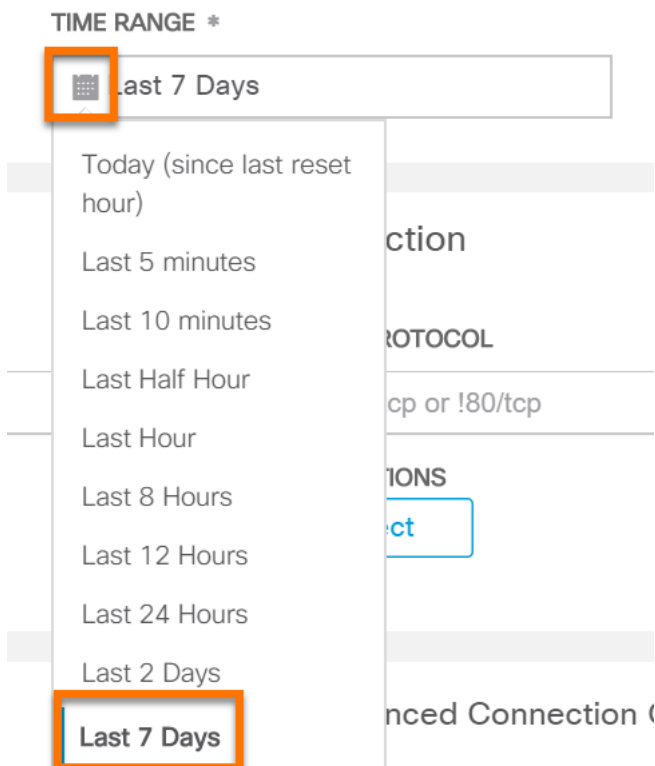
手順

1. 上部のナビゲーション セクションで、[分析 (Analyze)] > [フロー検索 (Flow Search)] に移動します。

Stealthwatch



2. [時間範囲 (Time Range)] ドロップダウンで [過去 7 日間 (Last 7 Days)] を選択すると、過去 7 日間に発生したフローを表示できます。通信の有無や通信の発生時期はわからないため、対象範囲を広くとって、セキュリティ対策が意図したとおりの効果を上げているかどうかを確認します。



3. 次に [検索項目 (Search Subject)] がリストされている左側のペインで、[マシン (Machines)] ホスト内のデバイスに検索を絞り込みます。このデモでは、[マシン (Machines)] グループ内の自動化ホストが、ControlSystems グループとのみ通信していることを確認します。

- ここで多少ドリル ダウンする必要があります。Stealthwatch ではホストを階層別に編成できます。[ホストグループ (Host Groups)] ボタンをクリックします。デフォルト設定は [内部ホスト (Inside Hosts)] ですが、これを [ControlSystems] ホストに絞り込みます。このホストグループは、このデモで Stealthwatch 管理コンソール上の IP アドレスによって定義されています。
- ここでは、Control System ホスト以外から [マシン (Machine)] ホストに到達したトラフィックを特定することが目標になります。最も簡単な方法は、ControlSystem グループからのデータを除外した、検索対象ホスト (マシングループ) に対するフロー データをすべて検索することです。

4. [件名 (Subject)] および [ピア (Peer)] セクションで、[選択 (Select)]、[内部ホスト (Inside Hosts)]、[マシン (Machines)]、[適用 (Apply)] の順にクリックします。

注 : [ピア (Peer)] セクションで、上記の手順を繰り返します。

5. [件名 (Subject)] および [ピア (Peer)] セクションのクエリから [Control Systems] グループのフロー データを除外します。そのため、[選択 (Select)]、[除外 (Exclude)]、[ControlSystems]、[適用 (Apply)] の順にクリックします。

注 : [ピア (Peer)] セクションで、上記の手順を繰り返します。

| | | |
|---|---|--|
| <p>Subject</p> <p>HOST IP ADDRESS</p> <input type="text" value="ex. 192.168.10.10 or !192.168.10.10"/> <p>HOST GROUPS</p> <input type="button" value="Select"/> | <p>Connection</p> <p>PORT / PROTOCOL</p> <input type="text" value="ex. 80/tcp or !80/tcp"/> <p>APPLICATIONS</p> <input type="button" value="Select"/> | <p>Peer</p> <p>HOST IP ADDRESS</p> <input type="text" value="ex. 192.168.10.10 or !192.168.10.10"/> <p>HOST GROUPS</p> <input type="button" value="Select"/> |
|---|---|--|

Host Group Selector

Inside Hosts x Machines x !ControlSystems x

Include

Search

- ▼ Inside Hosts
 - Blackhole
 - ▶ Business Units
 - ▶ By Function
 - ▶ By Location
 - Catch All
 - ▶ Cloud Hosts
 - Compliance Systems
 - ControlSystems
 - DMZ Servers
 - Machines

Host Group Selector

Inside Hosts x Machines x !ControlSystems x

Include

Search

- ▼ Inside Hosts
 - Blackhole
 - ▶ Business Units
 - ▶ By Function
 - ▶ By Location
 - Catch All
 - ▶ Cloud Hosts
 - Compliance Systems
 - ControlSystems
 - DMZ Servers
 - Machines

注：[マシン (Machines)]グループとそれ以外のグループとの通信を確認するデバイスを定義したところで、対象とするトラフィックのタイプを指定します。ここではマシンと ControlSystems 間以外のフロー (トラフィック) を検索しているため、さらに検索基準を絞り込む必要はありません。

6. [フロー検索 (Flow Search)]クエリを実行するには、[検索 (Search)]をクリックします。

Flow Search ⓘ

Last 7 Days (Time Range) 2,000 (Max Records) Restore Defaults Load Saved Search Save Search

Subject: Inside Hosts (Host Groups) Machines (Host Groups) By Function (Host Groups) !ControlSystems (Host Groups) Either (Orientation)

Connection: All (Flow Direction)

Peer: Inside Hosts (Host Groups) Machines (Host Groups) !ControlSystems (Host Groups)

注：クエリの実行には多少時間がかかります。過去 1 週間にネットワーク内で発生したすべてのフロー レコードが処理されます。フロー データが多いほど、クエリにかかる時間は長くなります。それでも、存在するワークロードの量に比べて非常に短い時間で完了します。わずかな時間で何千、何百万ものフロー レコードが処理されます。

Flow Search Results (2,000)

Edit Search Last 7 Days (Time Range) 2,000 (Max Records) Save Search Save Results Start New Search

Subject: Inside Hosts (Host Groups) Machines (Host Groups) !ControlSystems (Host Groups) Either (Orientation) 100% Complete Delete Search

Connection: All (Flow Direction)

Peer: Inside Hosts (Host Groups) Machines (Host Groups) !ControlSystems (Host Groups)

| START | DURATION | SUBJECT IP A... | SUBJECT POR... | SUBJECT HO... | SUBJECT BYT... | APPLICATION | TOTAL BYTES | PEER IP ADDR... | PEER PORT/P... | PEER HOST G... | PEER BYTES | ACTIONS |
|--|------------------|-----------------|----------------|--|----------------|-----------------|-------------|-----------------|----------------|---|------------|---------|
| Ex. 06/09/2 | Ex. <-50min4t | Ex. 10.10.10.1 | Ex. 57100/UDI | Ex. "catch All" | Ex. <-50M | Ex. "Corporate" | Ex. <-50M | Ex. 10.255.25. | Ex. 2055/UDP | Ex. "Catch All" | Ex. <-50M | |
| Feb 8, 2019 10:31:19 AM (3d 5hr 18min ago) | 3d 5hr 16min 40s | 10.201.3.20 | 50928/TCP | End User Devices, Desktops, Atlanta, Sales and Marketing | 810.66 K | Undefined TCP | 644.59 M | 10.201.1.51 | 22609/TCP | Atlanta | 643.8 M | |
| Feb 8, 2019 10:31:33 AM (3d 5hr 17min 46s ago) | 3d 5hr 16min 26s | 10.201.3.21 | 57258/TCP | End User Devices, Desktops, Atlanta, Sales and Marketing | 5.81 K | HTTPS | 132.71 M | 10.203.0.212 | 443/TCP | Atlanta, Protected Assets, Casablanca, QA | 132.7 M | |
| Feb 11, 2019 11:12:36 AM (4hr 36min 43s ago) | 4hr 34min 43s | 10.201.3.21 | 58742/TCP | End User Devices, Desktops, Atlanta, Sales and Marketing | 2.61 K | HTTPS | 49.4 M | 10.203.0.202 | 443/TCP | Atlanta, Protected Assets, Casablanca, QA | 49.39 M | |

まとめ

ネットワーク ポリシーが正しく機能していれば、クエリが完了したときにフロー レコードは表示されません。このクエリの一部としてフロー レコードが返された場合、ファイアウォール、セグメンテーション、ACL などの環境にお客様が変更を加えたことがわかります。また、ControlSystems グループがマシン外部のホストとトラフィック フローを送受信しているため、セキュリティに問題が発生していることもわかります。

どの企業でも、セキュリティに自信を持ち、セキュリティ上の取り組みが効果を上げていることを確認したいと考えています。そうした取り組みの有効性について、どれだけの企業がリアルタイムの広範な可視性を確保しているのでしょうか。金銭と労力の両面で、投資がインフラストラクチャのセキュリティにプラスの影響を与えているのでしょうか。Stealthwatch は、デジタル エンタープライズのセキュリティ対策について、可視性が高く実証的な証拠とフィードバックを継続的に提供します。

このフロー クエリは、不要なトラフィックを特定し、Stealthwatch のカスタム セキュリティ イベント機能を使用して自動検出メカニズムに変換することができます。これにより、トラフィックを繰り返し検索することなく、類似のトラフィック違反を自動的に検出できます。自動検出では、応答アクションと関連付けることができるポリシー違反アラームがトリガーされます。

シナリオ 3. データ盗難の調査

価値提案：残念なことに、データ盗難は日々発生しています。攻撃者は従来、主にサービスの中断に集中していました。現在のセキュリティ侵害は窃盗に集中しています。Stealthwatch は一連の攻撃全体に対して機能し、早期に行動を認識して攻撃とセキュリティ侵害を偵察サイクルの早い段階で検出し、進行中の攻撃を特定し、インシデント発生後の調査を可能にします。Stealthwatch と ISE を組み合わせると、インシデント対応を推測ではなくコンテキスト（属性情報）を基に実行でき、ユーザ中心の分析が可能になります。

ネットワーク調査では、機密情報や重要な情報のデータ盗難の兆候を調査します。お客様が機密情報とデータ整合性の保持を求めている場合は、このデモを通じて、Stealthwatch を使用したデータ侵害の追跡を効果的に示すことができます。データ侵害が発生した場合、いつどこで発生したか、どのデバイスを誰がどのような方法で使用したか、どのようにしたら迅速に特定できるでしょうか。

脅威は必ずしも簡単に検出できるものではなく、また悪意のあるトラフィックではない場合もあります。ソーシャルエンジニアリングと有効なトラフィック タイプを組み合わせても、収益や信用の低下に至ることがあります。パートナーやサプライヤの情報などの機密データは、意図的にまたは意図せずに第三者に簡単に開示される可能性があります。ネットワーク調査について、Stealthwatch はどのような面で支援できるでしょうか。

パートナー データやいくつかの機密情報がオフサイトに送信されている、という噂が流れているとします。この時点では 1 つの噂にすぎませんが、調査は必要です。

課題 - リスクに焦点を当てる

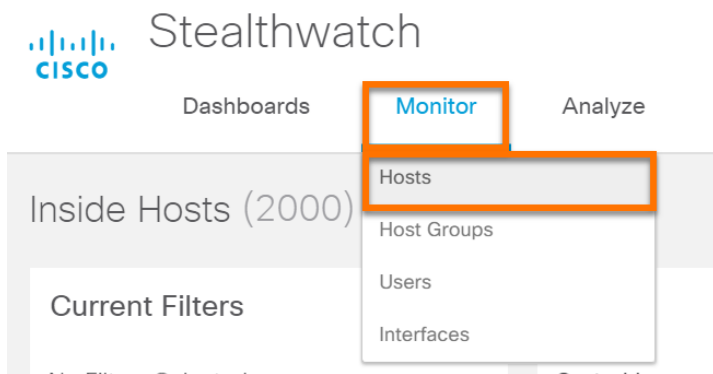
- セキュリティ インシデント中に簡単にデータを収集できる方法がない

利点 - リスクの低減に焦点を当てる

- 異常なトラフィックの検出と、より効果的なフォレンジック調査に向け、すべてのネットワーク トランザクションの監査証拠を漏れなく提供する

手順

1. ナビゲーション ウィンドウから開始し、[モニタ (Monitor)] > [ホスト (Hosts)] をクリックします。



2. [ホスト (hosts)] ビューが表示されます。すべての内部ホストがアラームの重大度に応じてリストされています。重大度は、Stealthwatch が追跡したイベント カテゴリ全体の複合比率によって判定されます。

Inside Hosts (2000)

Current Filters
No Filters Selected
Clear All

Filter Results By:

ALARMS

- Target Index (19)
- Concern Index (16)
- Recon (7)
- Data Hoarding (5)
- Exfiltration (4)
- Exploitation (2)
- Command & Control (1)
- DDoS Target (1)
- Policy Violation (1)
- Anomaly (0)
- DDoS Source (0)
- Select Multiple

HOST GROUPS

- Inside Hosts (3614)

Host

Sorted by overall severity

| Host Address | Host Name | Last Active | CI | TI | RC | C&C | EP | DS | DT |
|--------------|------------------|-----------------|--------|--------|--------|-----|--------|----|------|
| 10.201.3.149 | workstation-149. | 2/11/19 8:03 PM | 1,076% | | 1,586% | 12% | 1% | | |
| 10.201.0.23 | terminal-server. | 2/11/19 8:03 PM | 92% | 7% | 68% | 12% | | | 1% |
| 10.201.3.18 | workstation-018. | 2/11/19 8:03 PM | 63% | | 4,598% | | | | |
| 10.10.30.15 | | 2/11/19 8:03 PM | 24% | 2,156% | 71% | 76% | | | 649% |
| 10.202.1.220 | | 2/11/19 8:03 PM | 1% | 2,353% | 2% | | | | |
| 10.201.0.16 | server-016. | 2/11/19 8:03 PM | 44% | 1,597% | 22% | 78% | | | |
| 10.201.0.15 | server-015. | 2/11/19 8:03 PM | 6% | 1,213% | 76% | 87% | | | |
| 10.10.101.24 | | 2/11/19 8:02 PM | 68% | | 69% | | 1,100% | | |
| 10.240.200.1 | | 2/11/19 8:03 PM | | 913% | | | | | |
| 10.150.1.200 | | 2/11/19 1:14 AM | 100% | 1% | | | | | |
| 10.201.3.83 | workstation-083. | 2/11/19 8:02 PM | 378% | | 183% | | 53% | | |
| 10.50.10.254 | | 2/11/19 3:50 AM | 213% | 111% | 94% | | 101% | | |

3. ホストが最初にネットワークに入った時刻、ネットワークで存在が確認された最後の時刻、発生したイベントやホストとの関連が特定されたイベントのカテゴリなどの詳細も表示されます。色分けされているため、イベントが直ちに対応や介入が必要であるかどうかをすばやく判断できます。
4. [フィルタ条件： (Filter Results By:)] セクションで、[漏洩 (Exfiltration)] を選択します。

注：ここではデータの盗難または漏洩を探しています。噂の調査であるため、いつ発生したかはわかりません。そこで画面の左側を確認すると、サポートされているアラーム タイプのリストが表示されています。過去 24 時間以内に漏洩アラームがトリガーされていることがわかります。ただの噂ではなかった可能性があります。

Filter Results By:

ALARMS

- Concern Index (17)
- Target Index (15)
- Recon (12)
- Data Hoarding (4)
- Exfiltration (2)**
- Policy Violation (2)
- Exploitation (1)
- DDoS Target (1)
- Anomaly (0)
- Command & Control (0)
- DDoS Source (0)
- Select Multiple

5. この漏洩アラームについて、Stealthwatch でどのような情報が得られるかを見てみましょう。
6. ホスト 10.210.7.38 が、アラームをトリガーした可能性があることがわかります。

注：デモ環境では、お客様の実際の環境から事前に取得した Netflow データが使用されています。データは約 24 時間ごとに再生されており、若干の変化があります。そのため 1 つまたは複数のホストで漏洩アラームが生成されている可能性があります。ホスト 10.210.7.38 に漏洩の可能性があります。

7. このデモンストレーションでは 10.210.7.38 にフォーカスを当てますが、実際のネットワークでは、すべてのアラームを調査することを推奨します。
8. 漏洩ポリシーに違反するホストが見受けられることから、何らかの漏洩イベントが発生した疑いがあることを確認できます。ただしそれが正当なデータ転送であるのか、データ盗難であるのかは不明です。さらに詳細が得られるかどうかを確認します。
9. IP アドレス **10.201.3.149** をクリックして、さらに深く調べます。

Host

Sort by overall severity ⓘ

| Host Address | Host Name | Last Active | CI | TI | RC | C&C | EP |
|-----------------------|------------------|------------------|------|----|--------|-----|----|
| 10.150.1.200 ⓘ | | 8/28/19 6:14 AM | 253% | 3% | 2,984% | | |
| 10.201.3.149 ⓘ | workstation-149. | 8/28/19 11:39 AM | 865% | | 2,747% | | |

First Previous 1 Next Last

10. このホストが、[エンド ユーザ デバイス (End User Devices)] ホスト グループ (画面左側にホストの詳細が表示される) に属し、少なくとも 1 日 1 回、中国のホストと通信を行っていることがわかります (画面中央にフロー ピアが表示される)。
11. このホストがどの組織単位に属しているかがわかり、このホストとユーザがアクセスしているデータのタイプと、対応すべきかどうかもわかります。
12. 右上にあるグラフは、過去 7 日間のデータ損失の疑いと漏洩イベントを示しています。
13. 関係する外部ホストでフロー クエリを実行するには、[ピア ホスト グループ別トラフィック (過去 12 時間) (Traffic by Peer Host Group (last 12 hours))] セクションで [エンド ユーザ デバイス (End User Devices)] ホスト ラインをクリックし、[フローの表示 (View Flows)] をクリックします。

Concern Index: 1, Target Index: 0, Recon: 1, C&C: 0, Exploitation: 0, DDoS Source: 0, DDoS Target: 0, Data Hoarding: 2, **Exfiltration: 1**, Policy Violation: 0

Host Summary

Host IP: 10.201.3.149

Flows | History

Status: workstation-149

Hostname: workstation-149

Host Groups: **End User Devices** (Sales and Marketing)

Location: RFC 1918

First Seen: 9/28/18 11:46 AM

Last Seen: 8/28/19 11:43 AM

Policies: Insider Threat Event, Client IP Policy, Inside

Traffic by Peer Host Group (last 12 hours)

10.201.3.149

View Flows | Edit | Top Reports

Subject Host IP: 10.201.3.149

Peer Host Group: End User Devices

from: 08/27 11:47 PM

to: 08/28 11:47 AM

Alarms by Type (last 7 days)

14. フロー検索が終了するのを待ちます (100%)。

15. サマリーとアプリケーショントラフィックを表示するには、[サブジェクトのホスト (Subject Host)] 列で [エンド ユーザ デバイス (End User Devices)] をクリックします。

Flow Search Results (318)

08/27/2019 11:47 PM - 08/28/2019 11:47 AM (Time Range) | 2,000 (Max Records)

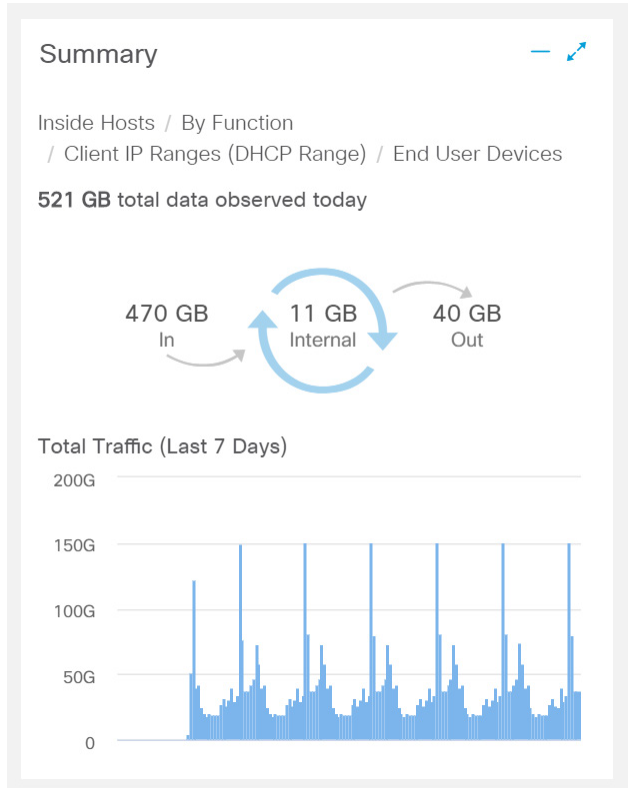
Subject: 10.201.3.149 | Either (Orientation)

Connection: All (Flow Direction)

Peer: End User Devices (Host Groups)

100% Complete

| START | DURATION | SUBJECT IP A... | SUBJECT PO... | SUBJECT HO... | SUBJECT BYT... | APPLICATION | TOTAL BYTES | PEER IP ADDR... | PEER... |
|--|-----------|-----------------|---------------|---|----------------|------------------------|-------------|-----------------|---------|
| Aug 28, 2019 3:55:42 AM (7hr 54min 6s ago) | 55min 56s | 10.201.3.149 | 137/UDP | End User Devices, Desktops, Atlanta, Sales and Marketing | -- | NetBIOS (unclassified) | 1.66 K | 10.201.3.115 | 6235 |



まとめ

Stealthwatch で明らかになった情報に基づいて、ホストの隔離が保証されます。ホストを確実に隔離し、漏洩イベントに関するユーザ名の特定や、データが現行のポリシー ルールに違反してオフサイトに転送されたことを確認できます。

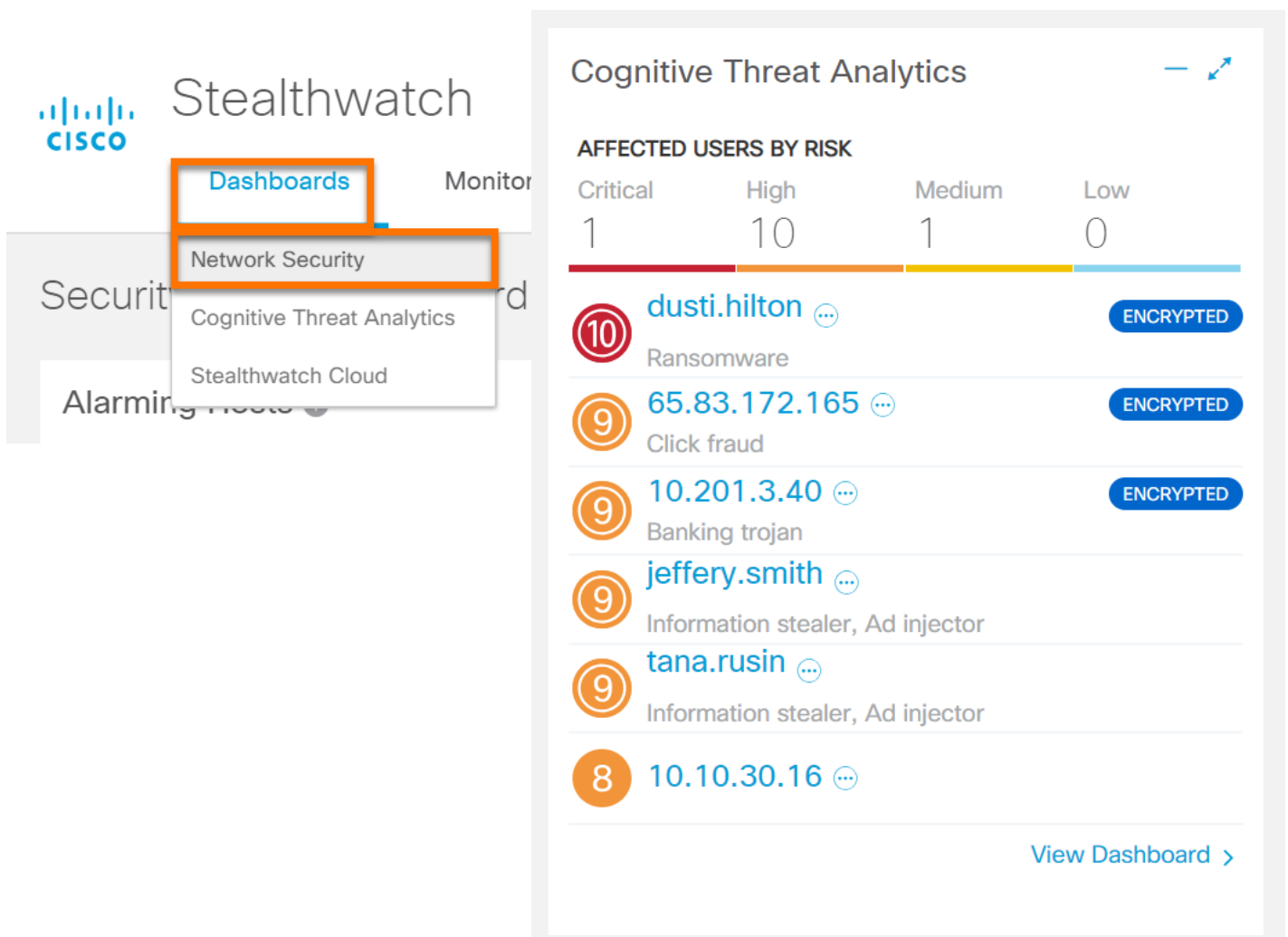
データの整合性に対する脅威は、外部ばかりでなく内部にも存在します。こうした内部の脅威をどのように検出し、場所を特定し、検証できるでしょうか。Stealthwatch は、正当なトラフィックが不正な目的で、または企業のポリシーに違反して使用されたかどうかを確認できます。これは他のシステムでは見逃されてしまうでしょう。また、ユーザとイベントの関連性、調査の証跡機能をすぐに使用できます。従来型の方法で何日も何週間も時間をかける必要はありません。

シナリオ 4. コグニティブ分析の統合

価値提案：この機能では、プロキシ統合機能によって取り込まれた Netflow とプロキシの両方のデータを使用できます。この機能を有効にすると、関連するネットワークトラフィックの詳細が分析のために Cognitive Analytics Cloud に送信されます。検出された脅威は、Stealthwatch SMC に表示されます。コグニティブ分析により、ネットワーク境界を通過するトラフィックに対する、強化された機械学習ベースの動作分析が Stealthwatch に導入されます。

手順

1. [ダッシュボード (Dashboard)] > [ネットワークセキュリティ (Network Security)] に移動し、ページの左下で [認識脅威分析 (Cognitive Threat Analysis)] ウィジェットを確認します。



The screenshot shows the Stealthwatch interface. On the left, a navigation menu is visible with 'Dashboards' highlighted in orange, and a sub-menu showing 'Network Security' also highlighted in orange. The main content area displays the 'Cognitive Threat Analytics' dashboard. At the top right of the dashboard is a minus sign and a refresh icon. Below the title is a section 'AFFECTED USERS BY RISK' with a horizontal bar chart and the following data:

| Critical | High | Medium | Low |
|----------|------|--------|-----|
| 1 | 10 | 1 | 0 |

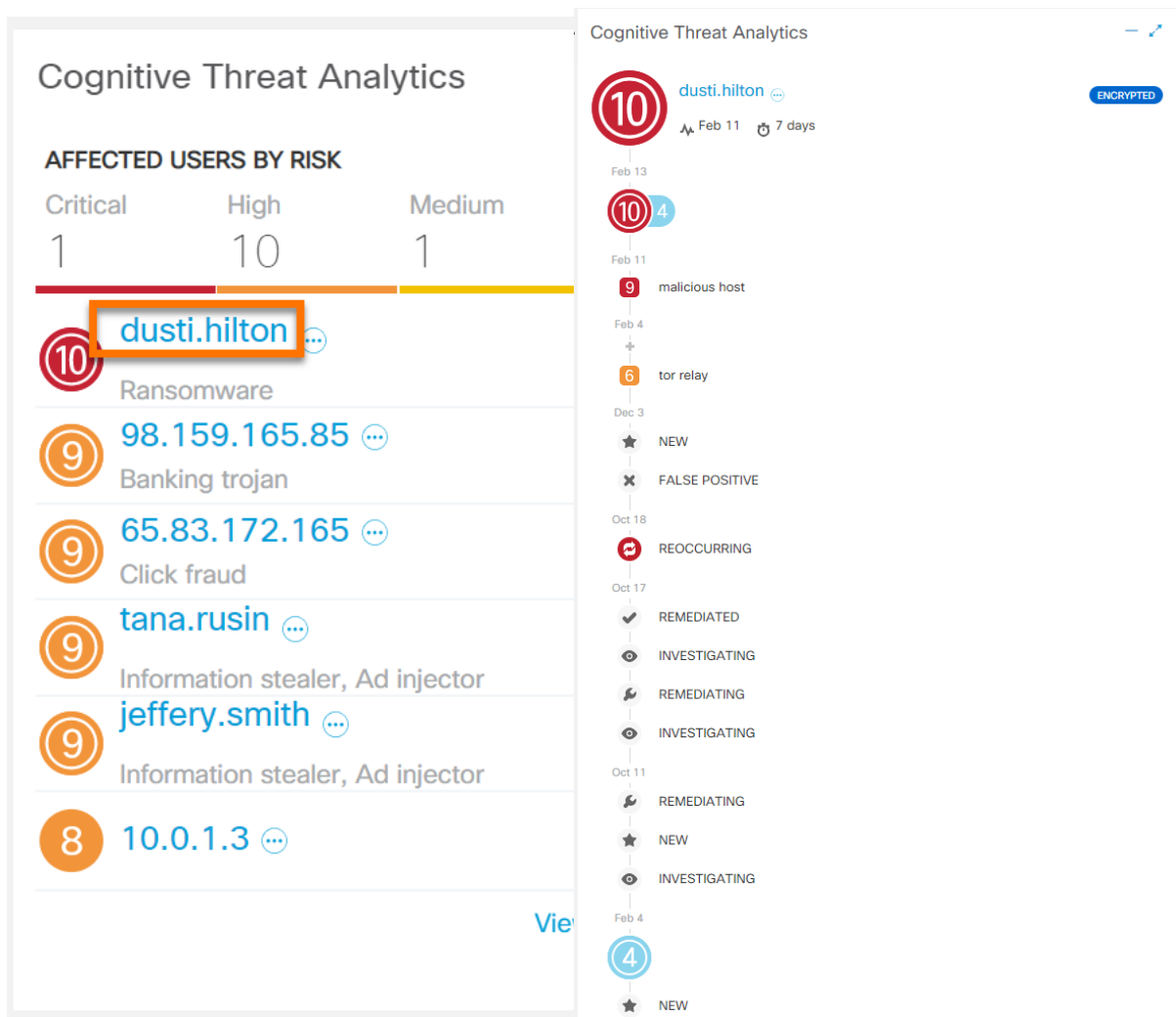
Below the chart is a list of affected users with their risk scores and threat types:

- dusti.hilton** (Risk: 10) - Ransomware (Status: ENCRYPTED)
- 65.83.172.165** (Risk: 9) - Click fraud (Status: ENCRYPTED)
- 10.201.3.40** (Risk: 9) - Banking trojan (Status: ENCRYPTED)
- jeffery.smith** (Risk: 9) - Information stealer, Ad injector
- tana.rusin** (Risk: 9) - Information stealer, Ad injector
- 10.10.30.16** (Risk: 8)

At the bottom right of the dashboard, there is a 'View Dashboard >' link.

2. [ホスト レポート (Host Report)] ページで [認識脅威分析 (Cognitive Threat Analysis)] を確認するには、任意のホストをクリックします。
3. [ホスト レポート (Host Report)] 画面のコグニティブ ウィジェットに、検出された異常または敵対的なアクティビティが (上から順に) 新しいものから表示されます。
4. [ホスト レポート (Host Report)] 画面に表示されるイベントについては、情報パネルに示されるのは TOR リレー アクティビティの初期検出です。初期の脅威分類 (4 ~ 6) が行われ、既知の悪意のあるホストとの通信があれば重大度レベルが 9 に増加します。脅威が特定され、ランサムウェアの脅威として分類されると、10 に昇格されます。この場合、脅威にはワームのような拡散動作があり、ネットワークの他の部分に対する大きな脅威となります。数字にマウス ポインタを合わせると、すべての説明が表示されます。

注：コグニティブ関連の UI のほとんどの部分ではマウスオーバー機能が有効になっていて、要素に関する追加情報が示されます。いざというときには、要素にマウス ポインタを合わせて、表示される説明テキストをご確認ください。



The screenshot displays the 'Cognitive Threat Analytics' interface. On the left, a table titled 'AFFECTED USERS BY RISK' shows the following data:

| Critical | High | Medium |
|----------|------|--------|
| 1 | 10 | 1 |

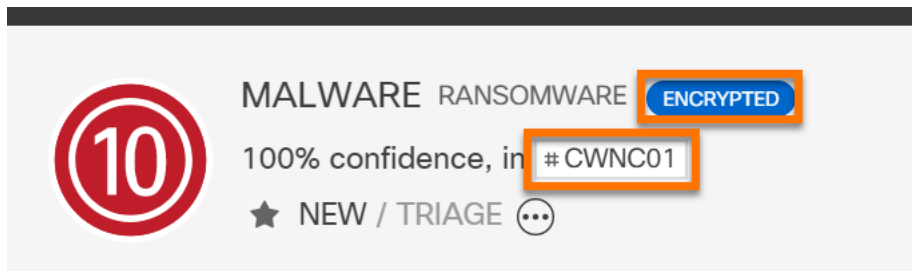
Below the table, a list of affected users is shown with their risk scores and associated threats:

- dusti.hilton** (Risk: 10) - Ransomware
- 98.159.165.85** (Risk: 9) - Banking trojan
- 65.83.172.165** (Risk: 9) - Click fraud
- tana.rusin** (Risk: 9) - Information stealer, Ad injector
- jeffery.smith** (Risk: 9) - Information stealer, Ad injector
- 10.0.1.3** (Risk: 8)

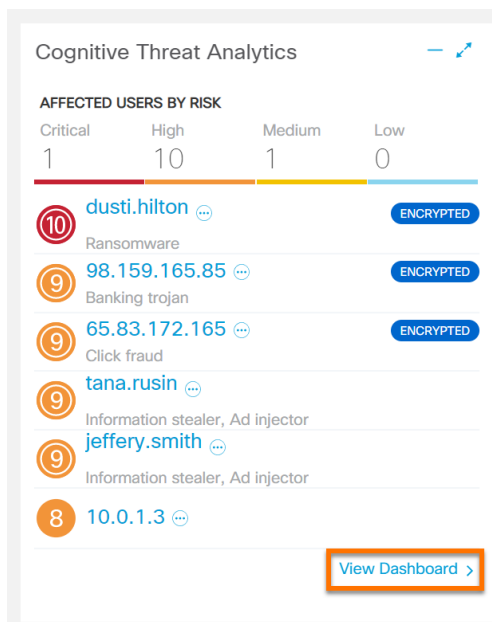
On the right, a vertical timeline titled 'Cognitive Threat Analytics' shows a sequence of events:

- Feb 11: **10** (Risk: 10) - **dusti.hilton** (7 days ago)
- Feb 13: **10** (Risk: 10) - 4
- Feb 11: **9** (Risk: 9) - malicious host
- Feb 4: **6** (Risk: 6) - tor relay
- Dec 3: **NEW** (Risk: 9) - FALSE POSITIVE
- Oct 18: **REOCCURRING** (Risk: 9)
- Oct 17: **REMIEDIATED** (Risk: 9)
- Oct 17: **INVESTIGATING** (Risk: 9)
- Oct 17: **REMIEDIATING** (Risk: 9)
- Oct 17: **INVESTIGATING** (Risk: 9)
- Oct 11: **REMIEDIATING** (Risk: 9)
- Oct 11: **NEW** (Risk: 9)
- Oct 11: **INVESTIGATING** (Risk: 9)
- Feb 4: **4** (Risk: 4) - **NEW**

5. 数値による順位付けでは、観察されたアクティビティの重大度が示されます（1 = マイナー、10 = クリティカル）。
6. 円が付いた数値インジケータは、特定されたキャンペーン（WannaCry など）と、検出された疑わしい動作（TOR リレー、永続的な異常トラフィック、大規模なデータ転送など）を示します。
7. 特定された攻撃キャンペーン（特定のワームやマルウェア感染など）は、#CWNC01 のようなハッシュタグ識別子とともに表示されます。
8. #識別子をクリックすると、検出されたイベントに関する簡潔な英語の説明が表示されます。内容は以下のとおりです。
 - キャンペーンの詳細情報。
 - 脅威を軽減および修復するための方法。
 - エンタープライズ ネットワーク全体で影響を受けるホストの数、および影響を受ける企業とユーザの数に関する主要な傾向。
 - 青い ENCRYPTED というタグが付いたイベントは、暗号化されたトラフィック動作の分析によって検出されています（Stealthwatch FC によって収集された ETA データを使用）。

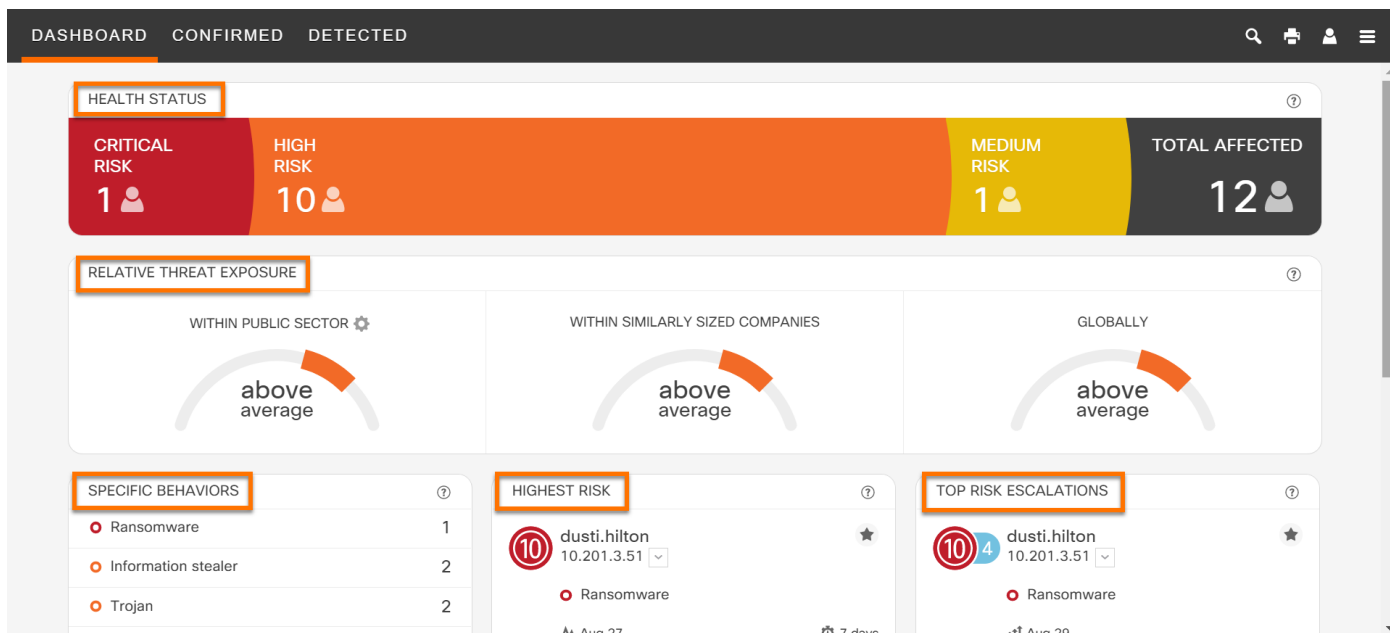


9. [ダッシュボードの表示 (View Dashboard)] を選択すると、クラウドベースの Cognitive ダッシュボードに移動します（新しいタブで開きます）。



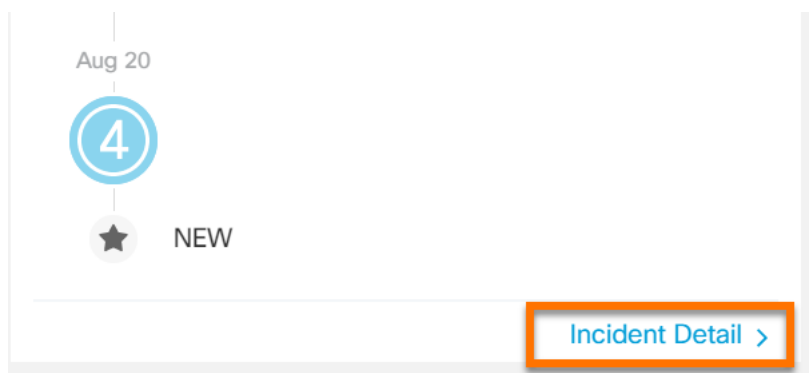
10. すぐに表示される情報 :

- ヘルス ステータス (Health Status) : Cognitive によって検出された、異常な、または脅威となる動作を示すホストの総数。
- 相対的脅威の暴露 (Relative Threat Exposure) : 同種の他の組織と比較した、企業の脅威アクティビティレベルの比較概要。
- 特定の動作 (Specific Behaviors) : ネットワークで検出された脅威タイプ。
- 最高のリスク (Highest Risk) : ネットワークに対して最高のリスクをもたらす動作を示すホスト。
- 上位リスク エスカレーション (Top Risk Escalations) : 全体的な重大度が最近増加しているインシデント。



注 : ダッシュボードのほとんどの要素は、クリックしてドリルダウンできます。

11. [ホスト レポート (Host Report)] ページの [Cognitive Threat Analytics] ウィジェットで、[インシデントの詳細 (Incident Detail)] をクリックするとイベントの詳細が表示されます。



12. 表示される詳細 :

- イベントの分類 (Event classification) : #HASHTAG 識別子 (利用可能な場合) をクリックすると、検出されたイベント キャンペーンに関する簡潔な英語の説明が表示されます。
- 影響 (Affecting) : ネットワーク環境内で影響を受けるホストの詳細。
- 発生 (Occurrence) : インシデントがネットワーク上でアクティブになっている期間。
- 重大度フィルタ (Severity Filter) : 検出されたイベントのアクティビティやフローを重大度別にフィルタリングできます (アクティブになっている各種の番号をクリックします) 。
- アクティビティとフロー (Activities and Flows) : アラームをトリガーした、疑わしい、または悪意のあるアクティビティを視覚的に表示します。アクティビティ、連絡先ドメイン、GeoIP データを持つドメインの IP アドレス、IP アドレスを所有する登録済みシステムが示されます。
- アラームをトリガーした上記のネットワーク アクティビティの詳細なリスト : 左側にある [タイプ (Type)] 列で注目すべきは、横に **E** と表示されている通信は、Stealthwatch の解析暗号化 (ETA) データによって提供されるデータを使用して暗号化および分析されているということです。[タイプ (Type)] 列の **N** は分析された Netflow 接続を示し、**W** は Web プロキシ ログを示します。

The screenshot displays the Cisco dCloud interface for an event. At the top, there are several status indicators: a red circle with '10', 'MALWARE RANSOMWARE ENCRYPTED', '100% confidence, in CWNC01', 'NEW / TRIAGE', 'AFFECTING dusti.hilton 10.201.3.51', and 'OCCURRENCE 7 days Feb 4 - Feb 11'. Below this is a section titled 'ACTIVITIES AND FLOWS' with a 'SEVERITY FILTER' set to 9. The main area shows a flow diagram with nodes for 'Activities (1 out of 3)', 'Domains (1 out of 6)', 'IPs (1 out of 6)', and 'Autonomous systems (1 out of 5)'. A flow is shown from a 'malicious host' to a domain, then to an IP (104.17.41.137), and finally to 'Cloudflare Inc'. Below the flow diagram is a table with columns for UPLOAD, DOWNLOAD, REQUESTS, DURATION, USER AGENTS, NO REFERRER, and HTTP. The table contains four rows of data, all with a type of 'N'.

| TYPE | TIMESTAMP | CLIENT IP | SERVER IP | SER | URL | BYTES UP | BYTES DOWN |
|------|---------------------------------|-------------|---------------|-----|-----|----------|------------|
| N | Jan 18, 2019 16:06:09 GMT-06:00 | 10.201.3.51 | 104.17.41.137 | 80 | | 1,628 | 1,248 |
| N | Jan 18, 2019 16:06:09 GMT-06:00 | 10.201.3.51 | 104.17.41.137 | 80 | | 1,628 | 1,248 |
| N | Jan 18, 2019 16:06:09 GMT-06:00 | 10.201.3.51 | 104.17.41.137 | 80 | | 1,628 | 1,248 |
| N | Jan 18, 2019 16:06:09 GMT-06:00 | 10.201.3.51 | 104.17.41.137 | 80 | | 1,628 | 1,248 |

シナリオ 5. ETA 暗号化アシュアランス

価値提案 : Stealthwatch は、観察されたネットワーク接続の暗号化関連の属性を保持し、それを SMC に表示して、暗号化の監査とアシュアランスの使用例を実現できます。Cognitive は必要ありません。

手順

1. フローで ETA によって提供された暗号の詳細を表示するには、上部のナビゲーション パネルで [分析 (Analyze)] > [フロー検索 (Flow Search)] に移動し、次のように入力します。
 - a. [時間範囲 (Time Range)] ドロップダウンで、[過去 8 時間 (Last 8 Hours)] をクリックします。
 - b. [件名 (Subject)] セクションの [ホスト IP アドレス (Host IP Address)] フィールドに、**10.201.3.51** と入力します。
 - c. [接続 (Connection)] セクションの [ポート/プロトコル (Port/Protocol)] フィールドに、**443/tcp** と入力します。
 - d. [接続 (Connection)] セクションで、[拡張接続オプション (Advanced Connection Options)] をクリックします。
 - e. 下にスクロールして、[暗号化 (Encryption)] にある [選択 (Select)] ボタンをクリックします。

注 : [選択 (Select)] オプションをクリックすると、左側にパネルが表示されます。

- f. 左側の [暗号化 (Encryption)] パネルで、[暗号化 TLS/SSL バージョン (Encryption TLS/SSL Version)] フィールド内をクリックします。
- g. これにより、検索をフィルタリングするためのバージョンが表示されます。[TLS 1.0] を選択し、[適用 (Apply)] をクリックします。

注 : これにより結果がフィルタリングされ、TLS 1.0 を使用するフローのみが表示されます。

2. 上にスクロールし、[検索 (Search)] をクリックします。

3. フローの結果がロードされたら、関連する ETA 列を追加する必要があります (デフォルトでは表示されません)。[列の管理 (Manage Columns)] をクリックし、[接続 (Connection)] セクションで [暗号化 (Encryption)] 列オプションをすべて選択して、[設定 (Set)] をクリックします。

Flow Search Results (8)

Edit Search | Last 8 Hours (Time Range) | 2,000 (Max Records) | Save Search | Save Results | Start New Search

Subject: 10.201.3.51 | Ether (Orientation) | 100% Complete | Delete Search

Connection: All (Flow Direction) | TLS 1.0 (Encryption TLS/SSL Version)

Manage Columns | Summary | Export

| START | DURATION | SUBJECT IP A... | SUBJECT PO... | SUBJECT HO... | SUBJECT BYT... | APPLICATION | TOTAL BYTES | PEER IP ADDR... | PEER PORT/P... | PEER HOST G... |
|---|----------------|-----------------|---------------|---|----------------|-------------------------|-------------|-----------------|----------------|-----------------|
| Ex. 06/09/2 | Ex. <=<50min4s | Ex. 10.10.10.1 | Ex. 57100/UDP | Ex. "catch All" | Ex. <=<50M | Ex. "Corporate" | Ex. <=<50M | Ex. 10.255.255 | Ex. 2055/UDP | Ex. "Catch All" |
| Aug 27, 2019 10:53:40 PM (6hr 51min 8s ago) | 4s | 10.201.3.51 | 49319/TCP | End User Devices, Desktops, Atlanta, Sales and Marketing | 5.47 K | HTTPS (unclassified) | 17.12 K | 185.103.97.174 | 443/TCP | United Kingdom |
| Aug 27, 2019 | 4s | 10.201.3.51 | 49319/TCP | End User Devices, | 5.47 K | HTTPS | 17.12 K | 185.103.97.174 | 443/TCP | United Kingdom |

☰ Flow Table Columns

| Connection | Subject | Peer | General |
|---|---------|---|--------------------------------------|
| <input checked="" type="checkbox"/> Start | | <input type="checkbox"/> Flow Action | <input type="checkbox"/> SRT Maximum |
| <input type="checkbox"/> End | | <input type="checkbox"/> MPLS Label | <input type="checkbox"/> SRT Minimum |
| <input checked="" type="checkbox"/> Duration | | <input type="checkbox"/> Packet Rate | <input type="checkbox"/> VLAN ID |
| <input type="checkbox"/> Appliance | | <input type="checkbox"/> Protocol | |
| <input checked="" type="checkbox"/> Application | | <input type="checkbox"/> Service | |
| <input type="checkbox"/> Application (Flow Sensor) | | <input type="checkbox"/> TCP Connections | |
| <input type="checkbox"/> Application (NBAR) | | <input type="checkbox"/> TCP Retransmissions | |
| <input type="checkbox"/> Application (PacketShaper) | | <input checked="" type="checkbox"/> Total Bytes | |
| <input type="checkbox"/> Application (Palo Alto Networks) | | <input type="checkbox"/> TCP Retransmission Ratio | |
| <input type="checkbox"/> Byte Rate | | <input type="checkbox"/> Total Packets | |
| <input checked="" type="checkbox"/> Encryption TLS/SSL Version | | <input type="checkbox"/> Total Traffic (Bps) | |
| <input checked="" type="checkbox"/> Encryption Key Exchange | | <input type="checkbox"/> RTT Average | |
| <input checked="" type="checkbox"/> Encryption Authentication | | <input type="checkbox"/> RTT Maximum | |
| <input checked="" type="checkbox"/> Encryption Algorithm | | <input type="checkbox"/> RTT Minimum | |
| <input checked="" type="checkbox"/> Encryption Algorithm And Key Length | | <input type="checkbox"/> SRT Average | |
| <input checked="" type="checkbox"/> Encryption MAC | | | |

Select All Deselect All Restore Defaults

4. 結果を降順に並べ替える（下向き矢印）には、[暗号化 MAC (Encryption MAC)] 列の見出しを 2 回クリックします。

Flow Search Results (8)

Edit Search | Last 8 Hours (Time Range) | 2,000 (Max Records) | Save Search | Save Results | Start New Search

Subject: 10.201.3.51 | Ether (Orientation) | 100% Complete | Delete Search

Connection: All (Flow Direction) | TLS 1.0 (Encryption TLS/SSL Version)

| APPLICATION | TOTAL BYTES | ENCRYPTION ... | ENCRYPTION KEY ... | ENCRYPTION AUT... | ENCRYPTION ALG... | ENCRYPTION MAC | PEER IP ADDR... | PEER PORT/P... | PEER HOST G... |
|----------------------|-------------|----------------|--------------------|-------------------|-------------------|----------------|-----------------|----------------|----------------|
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |
| HTTPS (unclassified) | 17.12 K | TLS 1.0 | ECDHE | RSA | AES_256_CBC/256 | SHA | 185.103.97.174 | 443/TCP | United Kingdom |

50 items per page | 1 - 8 of 8 items

まとめ

この Stealthwatch の機能は、Cisco Catalyst 9000 スイッチ、ASR、ISR、CSR ルータ、およびバージョン 7.1 の Stealthwatch フロー センサーの ETA 機能に基づいていて、コグニティブ インテリジェンス クラウドにフロー データを送信する必要はありません。この例では、TLS 1.0 トラフィック フローが検出されました。TLS 1.0 は、PCI や NIST などのさまざまな機関によって推奨されておらず、信頼性の高いプロトコルとして承認されていません。この機能は暗号化コンプライアンスの検証に役立ち、Heartbleed、Poodle、Beast などの TLS 1.0 に関連する危険な攻撃を回避するためにより高いレベルの TLS を必要とする場所を示します。



次に必要な作業

デモゾーンの関連情報を確認します。

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2019 年 9 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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