Cisco Stealthwatch

Stealthwatch v7.3 および Cognitive Intelligence 構成ガイド

目次

はじめに

Cisco Cognitive Intelligence は、疑わしい Web トラフィックや Stealthwatch フローレコードを迅速に検出し、環境内でのプレゼンス確立の試みや、すでに発生中の攻撃に対処します。Stealthwatch システム上で Cognitive Intelligence が有効になると、Stealthwatch は分析のためにフローレコードを Cognitive Intelligence クラウドに送信します。デフォルトでは、Cognitive Intelligence は、内外のホストグループトラフィックおよび DNS 要求の Stealthwatch フローレコードを処理します。内部トラフィックをモニタするには、追加のホストグループを指定できます。Cognitive Intelligence は、暗号化トラフィック分析（ETA）を使用して、暗号化されたトラフィック内の悪意のあるパターンも検出します。

Cognitive Intelligence は Stealthwatch と連携して、フローレコードとネットワークアドレス変換（NAT）を分析します。Stealthwatch フローレコードを Cognitive Intelligence に送信するために追加のライセンスは必要ありませんが、Web トラフィックデータを Stealthwatch から Cognitive Intelligence に送信するには、インターネット境界 NAT データが必要です。これらの製品に関する詳細情報へのリンクについては、このドキュメントの最後にある「**関連資料**」を参照してください。

> Cognitive Intelligence は Amazon Web Services（AWS）クラウドに移行し、URL と IP アドレスが新しくなりました。詳細については、次のフィールド通知を参照してください。
>
> フィールド通知：2018 年 5 月
> フィールド通知：2018 年 10 月

Stealthwatch サポート

- StealthWatch Management Console および Flow Collector は、プロキシ サーバ経由でインターネットに接続するように設定できます。詳細については、「**プロキシ設定**」を参照してください。
- Cognitive Intelligence は、Stealthwatch 内のデフォルトドメインまたはサイトでのみ使用可能です。複数のドメインおよびサイトはサポートされません。
- Cognitive Intelligence は、Flow Collector sFlow ではサポートされていません。
- FIPS暗号化ライブラリが有効になっている場合、Cognitive Intelligenceは使用できません。

ETA のサポート

Cognitive Intelligence は、ETA 対応のスイッチとルータがある場合、ETA 情報のみを検出できます。StealthWatch および ETA の詳細については、暗号化トラフィック分析ホワイト ペーパー [英語] および暗号化トラフィック分析導入ガイド [英語] を参照してください。

ユーザとデータロール

次のユーザが	次のデータロールを使用する場合	アクセス可能なもの
プライマリ Admin	すべてのデータ（読み取りおよび書き込み）	• Cognitive ダッシュボード • Cognitive コンポーネント
パワーアナリスト（Power Analyst）		
設定マネージャ（Configuration Manager）	すべてのデータ（読み取り専用）*	• Cognitive ダッシュボード
アナリスト（Analyst）		

* Configuration Manager と Analyst のデータロールを変更すれば、Cognitive への全面的なアクセスを付与できます。詳細については、*ユーザ管理の設定*に関するヘルプトピックを参照してください。

データ

次の 2 つのカテゴリのデータがダブリンの AWS データセンターに送信されます。

- 次のいずれかの条件を満たす StealthWatch フロー レコード:
  - 内部/外部ホスト グループのトラフィックのレコード
  - 特定の内部ホスト グループのトラフィックのレコード(**内部ホスト**)
  - サーバポートが 53 の場合の DNS 要求レコード
  - ETA が有効になっているスイッチとルータがある場合の暗号化トラフィック分析のレコード
- Web ログ データ(StealthWatch プロキシ ログがある場合)

StealthWatch フロー レコード

StealthWatch フロー レコードには以下が含まれます。

- ホスト エンドポイントの IP アドレス
- TCP ポートまたは UDP ポート
- mac アドレス
- プロトコル データ*
- 期間ごとの送信時のバイトおよびパケットの数
- FIN パケット数
- フロー ID
- サービス ID
- Palo Alto アプリケーション ID
- ユーザ名
- MPLS ラベル
- ラウンドトリップ時間
- 開始時刻
- ポート範囲
- グループ ID
- SYN パケット数
- TrustSec セキュリティ グループ タグの ID と名前
- 既知のサービス ポート
- アプリケーション ID
- フロー センサー アプリケーション ID
- VLAN ID(Admin. VLAN ID)
- 再送信数
- エクスポータのリスト
- Flow Collector の IP アドレス
- 最終アクティブ時刻
- 自律システム番号
- VM ID
- RST パケット数
- フロー開始以降のバイトとパケットの合計数
- プロトコル
- パケット シェーパー アプリケーション ID
- NBAR アプリケーション ID
- 接続数
- サーバ応答時間
- フロー シーケンス番号
- SVRD メトリック

* プロトコルデータフィールドには、URL、SSL 証明書、ヘッダーデータ用の特殊文字などのその他の情報が含まれます。

ETA フローレコード

ETA フローレコードは、ETA が有効になっているスイッチとルータがある場合にのみ送信されます。StealthWatch および ETA の詳細については、暗号化トラフィック分析ホワイト ペーパー [英語] および暗号化トラフィック分析導入ガイド [英語] を参照してください。

StealthWatch フローレコードには以下が含まれます。

- 初期データパケット(IDP)*
- TLS セッション UD
- パケットの長さと時間のシーケンス(SPLT)
- 選択した暗号スイート
- Transport Layer Security (TLS) バージョン

* 初期データパケット(IDP)には、サーバ名表示(SNI)、プロトコルバージョン、提供および選択された暗号スイートと HTTP ヘッダーフィールド(暗号化されていない HTTP トラフィックの場合)など、プロトコル関連のデータとヘッダーがほとんど含まれています。HTTPS/HTTP 以外のプロトコルの場合は、クライアント/サーバ通信の最初の 1500 バイトのプロトコルヘッダーが含まれています(通常は、データの残りの部分を復号することなく、プロトコルレベルで暗号化されます)。

Web ログ データ

Web ログデータの目的の 1 つは、NAT を介してルーティング不可能な内部 IP とルーティング可能な外部パブリック IP の間の変換を提供することです。

> Stealthwatch でサポートされているプロキシログ設定については、『Stealthwatch proxy log Configuration Guide』を参照してください。

Web ログ データには以下が含まれます。

- タイムスタンプ
- サーバ IP アドレス
- クライアント TCP ポート
- クライアントからサーバに転送されたバイト数
- HTTP Referrer ヘッダー
- user-agent 文字列
- 経過時間
- クライアント ユーザ名(オプション)
- サーバ TCP ポート
- サーバからクライアントに転送されたバイト数
- HTTP 応答ステータスコード
- 応答 MIME タイプまたはコンテンツ タイプ
- クライアント IP アドレス
- サーバ名
- 要求された URL/URI
- HTTP 要求メソッド
- HTTP Location ヘッダー
- Web セキュリティプロキシによって実行されるアクション

StealthWatch Management Console の設定

ダッシュボード コンポーネント

Stealthwatch Management Console で Cognitive Intelligence コンポーネントを設定するには、次の手順を実行します。

> Cognitive Intelligence に接続するには、すべてのアプライアンスのクロックを NTP サーバを使用して同期する必要があります。

> デュアル SMC のペアでは、設定後にセカンダリ SMC は Cognitive Intelligence に接続されません。これは、Flow Collector がデータを受信することを妨げず、プライマリ SMC が Cognitive に接続し、ウィジェットを適切に表示します。プライマリ SMC に障害が発生すると、セカンダリ SMC が Cognitive に接続し、ウィジェットを表示します。元のプライマリ SMC が稼働状態に戻ると、両方の SMC が Cognitive に正常に接続します。

> 少なくとも 1 つの SMC にインターネットアクセスが必要です。プロキシ設定も必要な場合は、「**プロキシ設定**」で詳細を確認してください。

1. StealthWatch Management Console から次の IP アドレスおよびポート 443 への通信を許可するように、ネットワークのファイアウォールを設定します。

AWS の Elastic IP	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105
シスコの合理化 IP	• 146.112.59.0/24 • 208.69.38.0/24

> パブリック DNS が許可されていない場合は、StealthWatch Management Console でローカルに解決方法を設定する必要があります。

2. StealthWatch Management Console にログインします。
3. ⚙ ([グローバル設定(Global Settings)]) アイコン をクリックします。[集中管理(Central Management)] を選択します。
4. SMC の [アクション(Actions)] 列の下にある ••• ([省略記号(Ellipsis)]) アイコン をクリックします。[アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
5. [全般(General)] タブをクリックします。
6. 外部サービスの [Cognitive Intelligenceの有効化(Enable Cognitive Intelligence)] チェックボックスをオンにして、[セキュリティ分析(Security Insight)] ダッシュボードおよびホストレポートの Cognitive Intelligence コンポーネントを有効にします。

7. （省略可）Cognitive Intelligence がクラウドから自動的にアップデートを送信できるようにするには、[自動更新（Automatic Updates）] チェックボックスをオンにします。

   自動更新には、主に Cognitive Intelligence クラウド向けのセキュリティ修正と小規模な機能拡張が含まれます。これらの更新は、通常の StealthWatch リリースプロセスでも利用可能です。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。StealthWatch Management Console で自動更新を有効にした場合は、Flow Collector でも有効にする必要があります。

8. [設定の適用（Apply settings）] をクリックします。

   [セキュリティ分析（Security Insight）] ダッシュボードおよびホストレポートでサービスが Cognitive Intelligence コンポーネントを更新し、表示するには数分かかります。

9. （省略可）インターネットプロキシをアップロードするには、[ネットワークサービス（Network Services）] に移動します。[インターネットプロキシ（Internet Proxy）] セクションまでスクロールダウンし、[有効（Enable）] チェックボックスをオンにします。フォームに入力してから、[設定の適用（Apply Settings）] をクリックします。

内部ホスト

デフォルトでは、Cognitive Intelligence は、内外のホストグループトラフィックおよび DNS 要求の Stealthwatch フローレコードを処理します。分析用にクラウドに送信するデータを追加するには、StealthWatch フローレコードを送信する内部ホストグループを設定します。特定のホストグループを Cognitive Intelligence モニタリングに追加する方法は、企業の内部サーバ（メールサーバ、ファイルサーバ、Web サーバ、認証サーバなど）に使用されます。これらのサーバにエンドユーザからのトラフィックを追加すると、該当のデバイスで実行されているマルウェアによって悪用される可能性があるデータの露出の可視性を改善できます。データを送信するホストグループをすべて選択するのではなく、内部サーバを表すホストグループのみを選択してください。

Cognitive Intelligence が内部ホストのトラフィックをモニタできるようにするには、次の手順を実行します。

1. SMC にログインします。
2. [設定（Configure）] > [ホストグループ管理（Host Group Management）] に移動します。
3. 該当する内部ホストグループをクリックし、[Cognitive Intelligenceにフローを送信する（Send flows to Cognitive Intelligence）] チェックボックスをオンにします。

> この機能により、選択した親ホストグループの下にあるすべてのホストグループのトラフィックのモニタリングが有効になります。潜在的なパフォーマンスの問題を避けるため、このオプションは子ホストグループでのみ有効にすることをお勧めします。

4. **[保存（Save）]**をクリックします。

Flow Collector の設定

Flow Collector NetFlow で Cognitive Intelligence コンポーネントを設定するには、次の手順を実行します。

> Cognitive Intelligence に接続するには、すべてのアプライアンスのクロックを NTP サーバを使用して同期する必要があります。

> 正確な結果を得るには、各 Flow Collector で Cognitive Intelligence を設定する必要があります。

> 設定後、Cognitive Intelligence エンジンがネットワークの動作を学習するのに 2 日間かかります。

1. Flow Collector から次の IP アドレスおよびポート 443 への通信を許可するように、ネットワークのファイアウォールを設定します。

AWS の Elastic IP	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105	• 34.251.210.21 • 34.255.162.33 • 54.194.49.205
シスコの合理化 IP	• 146.112.59.0/24 • 208.69.38.0/24	

> パブリック DNS が許可されていない場合は、Flow Collector でローカルに解決方法を設定する必要があります。

2. StealthWatch Management Console にログインします。
3. ⚙ ([グローバル設定(Global Settings)]) アイコン をクリックします。[集中管理(Central Management)] を選択します。
4. Flow Collector NetFlow の [アクション(Actions)] 列の下にある ••• ([省略記号(Ellipsis)]) アイコン をクリックします。[アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
5. [全般(General)] タブをクリックします。
6. 外部サービスの [Cognitive Intelligenceの有効化(Enable Cognitive Intelligence)] チェックボックスをオンにして、Flow Collector から Cognitive Intelligence エンジンにデータを送信できるようにします。
7. (省略可) Cognitive がクラウドから自動的にアップデートを送信できるようにするには、[自動更新(Automatic Updates)] チェックボックスをオンにします。

自動更新には、主に Cognitive Intelligence クラウド向けのセキュリティ修正と小規模な機能拡張が含まれます。これらの更新は、通常の StealthWatch リリースプロセスでも利用可能です。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。Flow Collector で自動更新を有効にした場合は、StealthWatch Management Console でも有効にする必要があります。

8. [設定の適用(Apply settings)]をクリックします。

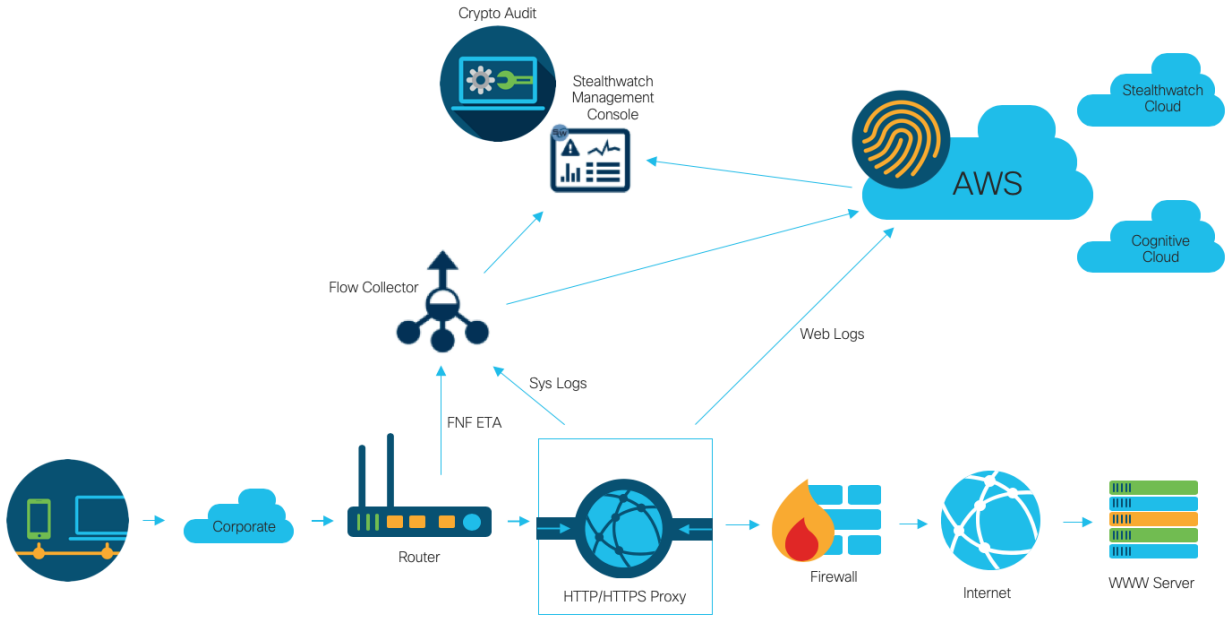
プロキシ設定

これを可能にするには、StealthWatch Management Console および Flow Collector を設定し、プロキシサーバ経由でインターネットに接続できるようにします。Cognitive Intelligence は、SSL インスペクションが無効になっている HTTP/HTTPS プロキシをサポートします。StealthWatch は SOCKS プロキシをサポートしていません。

Web プロキシの設定方法の詳細については、このドキュメントのセクション「**StealthWatch Management Console の設定**」を参照してください。プロキシログの設定の詳細については、『Stealthwatch proxy Log Configuration』を参照してください。

セットアップの設定については、次の図を参照してください。

> この設定では、WSA のプロキシを透過モードにする必要があります。詳細については、「Configure WSA to Upload Log Files to Cognitive System」を参照してください。



次の場合、プロキシを使用して Cognitive の最適な結果を得ることができます。

- Flow Collector は、プロキシの前にフローを収集します。
- プロキシログはクラウドに直接送信されます。

次の場合、プロキシを使用して、Stealthwatch Enterprise から最適な結果を得ることができます。

- プロキシログは、Flow Collector に直接送信されます。
- ETA を有効にする

プロキシをクラウドに直接接続する方法の詳細については、次を参照してください。

Configure Blue Coat ProxySG to Upload Log Files to Cognitive System

Configure McAfee Web Gateway to Upload Log Files to Cognitive System

Configure WSA to Upload Log Files to Cognitive System

検証

Docker サービス

Cognitive Intelligence が適切に設定されていることを確認するには、次の手順を実行します。

> Cognitive Intelligence を無効にするには、[集中管理(Central Manager)] > [アプライアンス設定の編集(Edit Appliance Configuration)] > [General(全般)] の順に移動し、各 SMC および Flow Collector NetFlow の [Cognitive Intelligenceの有効化(Enable Cognitive Intelligence)] チェックボックスをオフにします。

1. Cognitive Intelligence が SMC および Flow Collector で有効になっていることを確認します。
2. Cognitive Intelligence コンポーネントが [セキュリティ分析(Security Insight)] ダッシュボードおよびホストレポートに表示されていることを確認します。
3. ナビゲーションメニューで [ダッシュボード(Dashboard)] > [Cognitive Intelligence] をクリックします。[Cognitive Intelligence] ダッシュボードページが開きます。ページの右上にあるメニューから [デバイスアカウント(Device Accounts)] をクリックします。設定されている各 Flow Collector のアカウントでデータがアップロードされていて、準備ステータスであることを確認します。

ETA の統合

Cognitive Intelligence は、暗号化トラフィック分析(ETA)ソリューション内にマルウェア検出機能を実装しています。ETA ソリューションが正しく設定されていることを確認するために、Cognitive で特定のテストサイトドメインを使用して ETA テストインシデントを生成できます。これらのテストインシデントを生成するには、HTTPS セッションが ETA 対応スイッチおよびルータを通過するホストを使用して、次のテストサイトのいずれかを参照します。

- マルウェア : https://examplemalwaredomain.com
- ボットネット : https://examplebotnetdomain.com
- フィッシング : https://internetbadguys.com

> 最初は検出結果にリスクレーティング 5 と表示されます。上記の複数の URL にアクセスしたり、同じ URL に繰り返しアクセスしたりといった不正または反復的な動作が行われると、リスクレーティングが増大する可能性があります。

- TOR 検出 : TOR ブラウザをダウンロードしてインストールし(https://www.torproject.org/projects/torbrowser.html.en)、いくつかのウェブサイトにアクセスしてください。
- TOR 検出は、リスクレーティング 4 の「TORリレー(TOR relay)」または「潜在的に望ましくないアプリケーション(Possibly Unwanted Application)」と表示されます。

既知の問題

このセクションでは、このリリースに存在する既知の問題（バグ）について概要を示します。可能な場合には、回避策も示しています。参照用に問題番号が示されています。

問題番号	説明	回避策
CHOPIN-25314	Stealthwatch ユーザの権限が昇格または降格された場合（例：読み取り専用から読み取り/書き込みへ、またはその逆）、Cognitive Intelligence システムに変更が伝わるまでに最大 30 分かかります。	現在使用可能なものはありません。
SWD-13834	設定の復元を実行すると、Cognitive Intelligence が無効になります。	これを克服するには、バックアップの復元プロセス後に手動で Cognitive を有効にします。
NA	ユーザが複数の Stealthwatch システムにログインすると、Cognitive Intelligence 内の 2 番目のシステムにログインできなくなります。	この問題を解決するには、次の手順に従います。 • 最初のログインが期限切れになるまで 30 分待機します。 • 最初のシステムで Cognitive Intelligence からログアウトします。

関連資料

- Cognitive Intelligence の詳細については、製品の Web サイト（https://cognitive.cisco.com）にアクセスするか、http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011110.html にある製品マニュアルを参照してください。
- すべてのシスコ クラウド製品のクラウド利用規約とオファーの説明については、http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html を参照してください。
- Cisco Universal Cloud 契約については、http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf を参照してください。
- オファー全般については、http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/omnibus-cloud-security.pdf を参照してください。
- Stealthwatch プロキシログおよび Web プロキシの詳細については、https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html を参照してください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先：
  - Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
  - 電子メールでケースを開く場合：tac@cisco.com
  - 電話でサポートを受ける場合：800-553-2447（米国）
  - ワールドワイド サポート番号：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

著作権情報