StealthWatch および Cognitive Threat Analytics コンフィギュレーション ガイド

（Stealthwatch System v6.9.1 用）

はじめに

Cisco Cognitive Threat Analytics（CTA）は、疑わしい Web トラフィックや NetFlow 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 CTA が有効になると、StealthWatch は分析のために NetFlow データを CTA クラウドに送信します。NetFlow と Web トラフィック データの両方を使用すると、CTA によるより詳細な分析と検出が実現します。CTA に NetFlow データを送信するために追加のライセンスは必要ありませんが、StealthWatch システムから CTA に Web トラフィック データを送信するには StealthWatch ProxyWatch 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、このマニュアルの最後にある「関連資料」を参照してください。

注：StealthWatch Management Console およびフロー コレクタは、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。CTA システムは、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 システムは SOCKS プロキシをサポートしていません。

データ

境界 NetFlow および Web ログの 2 種類のデータが、SCP と HTTPS 経由でロンドンの CTA データセンターに送信されます。Web ログ データは、StealthWatch ProxyWatch が使用されている場合にのみ送信されます。

NetFlow データ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
- ペイロード
- 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
- フロー コレクタの 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

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

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

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。
    a. cognitive.cisco.com - 108.171.128.81

       注：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. [アプライアンスの管理（Administer Appliance）] に移動します。
4. [設定（Configuration）] > [システム時刻と NTP（System Time and NTP）] をクリックします。[Network Time Protocol の有効化（Enable Network Time Protocol）] チェックボックスがオンになっていることを確認します。

   注：システムに正確な NTP 時刻が設定されていない場合、アプライアンスは CTA に正しく接続できません。
5. [ホーム（Home）] をクリックします。[Docker サービス（Docker Services）] で、[Cognitive Threat Analytics ダッシュボードコンポーネント（Cognitive Threat Analytics Dashboard Component）] の [設定（Configure）] をクリックします。
6. [ダッシュボードコンポーネント（Dashboard Component）] チェック ボックスをオンにして、セキュリティ インサイト ダッシュボードおよびホスト レポートで CTA コンポーネントを有効にします。
7. （省略可）CTA 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。

   注：自動更新では、主に CTA クラウドのセキュリティ修正と小規模な機能拡張がカバーされます。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、フロー コレクタでも有効にする必要があります。
8. [適用（Apply）] をクリックします。

   注：Docker サービスが更新され、セキュリティ インサイト ダッシュボードおよびホスト レポートに CTA コンポーネントが表示されるまでには数分かかります。

フロー コレクタの設定

フロー コレクタで CTA コンポーネントを設定するには、次の手順を実行します。

注：正確な結果を得るには、各フロー コレクタで CTA データ アップローダーを設定する必要があります。

1. フロー コレクタから次の 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。
    a. etr.cloudsec.sco.cisco.com - 108.171.128.86
    b. cognitive.cisco.com - 108.171.128.81

        注：パブリック DNS が許可されていない場合は、フロー コレクタでローカルに解決方法を設定する必要があります。
2. フロー コレクタにログインします。
3. [設定（Configuration）] > [システム時刻と NTP（System Time and NTP）] をクリックします。[Network Time Protocol の有効化（Enable Network Time Protocol）] チェックボックスがオンになっていることを確認します。

    注：システムに正確な NTP 時刻が設定されていない場合、アプライアンスは CTA に正しく接続できません。
4. [ホーム（Home）] をクリックします。[Docker サービス（Docker Services）] で、[Cognitive Threat Analytics データアップローダー（Cognitive Threat Analytics Data Uploader）] の [設定（Configure）] をクリックします。
5. [データアップローダー（Data Uploader）] チェック ボックスをオンにして、フロー コレクタから CTA エンジンにデータを送信できるようにします。
6. （省略可）CTA 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。

    注：自動更新では、主に CTA クラウドのセキュリティ修正と小規模な機能拡張がカバーされます。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。フロー コレクタ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。
7. [適用（Apply）] をクリックします。

検証

CTA の Docker サービス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。

注：CTA を無効にするには、[設定（Configure）] をクリックしてチェック ボックスをオフにします。[停止（Stop）] をクリックすると、Docker コンテナは停止しますが、フロー コレクタを再起動した場合は CTA が再度有効になります。

1. StealthWatch Management Console およびフロー コレクタで、Docker サービスが [有効（Enabled）] と表示されていることを確認します。
2. CTA コンポーネントがセキュリティ インサイト 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 Threat Analytics] をクリックします。[CTA ダッシュボード（CTA Dashboard）] 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。設定されている各フロー コレクタにアカウントが存在し、データがアップロードされていることを確認します。

注：設定後、CTA 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。

関連資料

- CTA 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 利用規約については、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。
- 包括的なオファーの説明については、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 ProxyWatch および Web プロキシの詳細については、StealthWatch カスタマー コミュニティ（https://lancope.force.com/Customer）にアクセスして、[製品マニュアル（Product Documentation）] をクリックします。

  注：サイトへの初回アクセス時に、アカウントの作成を求められます。

お問い合せ先

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