ユーザーおよびエンティティの行動分析

ユーザーおよびエンティティの行動分析に関する情報

ユーザーおよびエンティティの行動分析（UEBA）は、異常が発生したときにネットワーク内の潜在的な脅威や標的型攻撃を特定するために、ユーザーとデバイスの動作をプロファイリングおよび追跡できる多くのセキュリティ技術を備えたソリューションです。

たとえば、企業の従業員は、バックドアや企業秘密の漏洩を含む可能性のある悪意のあるソフトウェアを意図せずにダウンロードすることがあります。これは、確立された基準と比較して、ネットワーク内の 1 つ以上のデバイスやユーザーからの通信パターンの変化によって検出されます。

ユーザーおよびエンティティの行動分析は、次の 2 つの方法を使用して展開できます。

- ユーザー データグラム プロトコル（UDP）コレクタ（Cisco Digital Network Architecture（DNA）Center は UDP コレクタです）。
- Stealthwatch Cloud（SwC）：組み込みワイヤレスコントローラ（EWC）は、データを SwC に直接アップロードします。

ユーザーおよびエンティティの行動分析の設定（UDP コレクタを使用）

Cisco DNA Center ベースの展開では、コントローラは、Cisco DNA Center に送信される NetFlow 情報のコレクタとして機能します。次に、Cisco DNA Center は SwC の情報を圧縮します。コントローラは、アクセスポイント（AP）で Application Visibility and Control（AVC）を有効にし、Cisco DNA Center との通信チャネルを維持します。

EWC では、UDP を介して FnFv9 データを UDP コレクタに送信することもできます。

Cisco DNAC ベース以外の展開では、FnF フローレコードはコントローラから SwC に直接送信されます。

ユーザーおよびエンティティの行動分析の設定（Stealthwatch Cloud を使用）

後続の各項では、Stealthwatch Cloud（GUI および CLI）を使用したユーザーおよびエンティティの行動分析ソリューションの設定に関する情報を提供します。

Stealthwatch Cloud を使用したユーザーおよびエンティティの行動分析の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Threat Defense] を選択します。

ステップ 2 [Cisco StealthWatch Integration] をクリックします。

ステップ 3 [Stealthwatch] ページの [Service Key] フィールドに、Stealthwatch Cloud サービスキーを入力します。

ステップ 4 クラウドアイコンをクリックして、Stealthwatch の詳細な統計を表示します。

ステップ 5 [Sensor Name] フィールドに、Stealthwatch Cloud 登録用のセンサー名を入力します。

ステップ 6 [URL] フィールドに、Stealthwatch Cloud サーバーの URL を入力します。

ステップ 7 [Apply] をクリックします。

ステップ 8 （任意）[Unconfigure StealthWatch] をクリックして、Stealthwatch Cloud の設定を解除します。

次のタスク

Stealthwatch Cloud の正常性ステータスは、[Stealthwatch Health Status] で確認できます。

Stealthwatch Cloud の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**stealthwatch-cloud-monitor** 例： `Device(config)# stealthwatch-cloud-monitor`	Stealthwatch Cloud モニターを設定します。Stealthwatch Cloud モニター コンフィギュレーション モードを開始します。
ステップ 3	**service-key** *swc-service-key* 例： `Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`	（任意）Stealthwatch Cloud サービスキーを設定します。サービスキーは、SwC ポータルによって提供されます。サービスキーの代替策として、IP アドレス許可リストを使用した認証があります。サービスキーと許可リストの詳細については、適切な SwC ガイドを参照してください。
ステップ 4	**sensor-name** *swc-sensor-name* 例： `Device(config-stealthwatch-cloud-monitor)# sensor-name swc-sensor-name`	（任意）Stealthwatch Cloud 登録のセンサー名を指定します。デバイスのシリアル番号がデフォルト値です。
ステップ 5	**url** *SwC-server-url* 例： `Device(config-stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com`	Stealthwatch Cloud サーバーの URL を設定します。

フロー測定への Stealthwatch Cloud のマッピング

Stealthwatch Cloud をフロー測定にマッピングするオプションには、フローエクスポータ構成とフローモニター構成の 2 つがあります。

（注） 任意の時点で、アクティブなフローエクスポータは内部と外部でそれぞれ 1 つのみ存在できます。アクティブなフローエクスポータは、ワイヤレス プロファイルにバインドされているフローモニターにバインドされているエクスポータです。

Stealthwatch Cloud のフローエクスポータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow exporter** *flow-exporter-name* 例： `Device(config)# flow exporter flow-exporter-name`	フローエクスポータを定義すします。 （注） 任意の時点で、アクティブなフローエクスポータは内部と外部でそれぞれ 1 つのみ存在できます。アクティブなフローエクスポータは、ワイヤレスプロファイルにバインドされているフローモニターにバインドされているエクスポータです。
ステップ 3	**destination stealthwatch-cloud** 例： `Device(config-flow-exporter)# destination stealthwatch-cloud`	フロー情報を Stealthwatch Cloud にエクスポートします。

Stealthwatch Cloud のフローモニターの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor** *flow-monitor-name* 例： `Device(config)# flow monitor flow-monitor-name`	フローモニターを定義します。
ステップ 3	**exporter** *flow-exporter-name* 例： `Device(config-flow-monitor)# exporter flow-exporter-name`	フロー情報をエクスポータにエクスポートします。

	コマンドまたはアクション	目的
ステップ 4	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	基本の IPv4 ワイヤレス AVC テンプレートを使用してフローレコードを指定します。
ステップ 5	**end** 例： `Device(config-flow-monitor)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例：Stealthwatch Cloud の設定

次の例は、Stealthwatch Cloud の完全な CLI 設定を示しています。

```
stealthwatch-cloud-monitor
  service-key XXXXXXXXXXXXXXXXXXXXXXXXXXXX
  sensor-name ewc-sensor
  url https://sensors.eu-2.obsrvbl.com

flow exporter fexp-swc
 destination stealthwatch-cloud

flow monitor fm-avc-swc
 exporter fexp-swc
 record wireless avc basic

wireless profile policy swc-policy-profile
 ipv4 flow monitor fm-avc-swc input
 ipv4 flow monitor fm-avc-swc output
 ipv6 flow monitor fm-avc-swc input
 ipv6 flow monitor fm-avc-swc output

wlan my-wlan 1 my-wlan

wireless tag policy swc-policy-tag
 wlan my-wlan policy swc-policy-profile

ap 0000.0000.0001
 policy-tag swc-policy-tag
```

Stealthwatch Cloud の詳細の確認

Stealthwatch Cloud の状態と統計を確認するには、**show stealthwatch-cloud wireless-shim** コマンドを使用します。

```
Device# show stealthwatch-cloud wireless-shim
Stealthwatch-Cloud wireless shim

Total
 RX records        : 15
 RX bytes          : 2345
```

```
 TX records        : 10
 TX bytes          : 1234
 TX batches        : 1
 Failed batches    : 0
 Non-SWC records   : 5

Buffers
 Status        : TX
 Size          : 1272000
 Compressed    : 8
 Uncompressed  : 0
 Records       : 8

 Status        : Filling
 Size          : 1272000
 Compressed    : 2
 Uncompressed  : 0
 Records       : 2
```

Stealthwatch Cloud 接続の詳細を確認するには、**show stealthwatch-cloud connection** コマンドを使用します。

```
Device# show stealthwatch-cloud connection
Stealthwatch-Cloud details
  Registration
    #ID         : 0xe6000001
    URL         : https://sensors.eu-2.obsrvbl.com
    Service Key : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Sensor Name : ewc-sensor
    Registered  : Yes
  Connection
    Status               : UP
    Last status update   : 03/17/2020 21:44:55
    # Flaps              : 0
    # Heartbeats         : 9
    # Lost heartbeats    : 1
    Total RX bytes       : 4567
    Total TX bytes       : 1234
    Upload Speed (B/s)   : 247
    Download Speed (B/s) : 269
    # Open sessions      : 0
    # Redirections       : 0
    # Timeouts           : 0

  HTTP Events
    GET response                  : 1
    GET request                   : 1
    GET Status Code 2XX           : 1
    PUT response                  : 1
    PUT request                   : 1
    PUT Status Code 2XX           : 1
    POST response                 : 12
    POST request                  : 12
    POST Status Code 2XX          : 11
    POST Status Code 4XX          : 1
API Events
    Abort                         : 1

  Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
03/21/2020 10:42:06.161 9        HEARTBEAT_OK         0
```

```
03/20/2020 06:49:05.717 1        HEARTBEAT_FAIL       0 HTTPCON_EV_TIMEOUT (6)

03/20/2020 06:47:05.717 1        SEND_START           0 ID:0001
03/20/2020 06:49:05.717 3        SIGNAL_DATA_FAIL     0 ID:0001, attempt : 3
03/18/2020 09:23:39.375 1        REGISTER_OK          0

03/18/2020 09:23:13.276 1        REGISTER_SEND        0

03/18/2020 09:23:12.154 1        SEND_ABORT_ALL       0 config change

03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 URL
https://sensor.staging.obsrvbl.com
03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 Service-key
XXXXXXXXXXXXXXXXXXXXXXXX
03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 Host ewc-sensor => reset

03/18/2020 09:23:12.154 1        OPTIONS_CONFIG       0 cfg-mode manual => reset
```