Cisco Secure Network Analytics

v7.4 アラーム抑制

目次

概要

アラーム属性に基づいて、悪意のないことが予想される既知のデバイス間の既知の通信に対してルールを設定できます。通信がルール基準（ポート、プロトコル、IP アドレスなど）に一致すると、Analytics で通常生成されるアラームが抑制され、ノイズが少なく効果的なシステムになります。

Analytics では、設定ファイルを処理するたびに、前のファイルが上書きされます。このアクションはマネージャ（旧 Stealthwatch Management Console）に限定されているため、Flow Collector の同期は発生しません。

使用可能なアラームのうち、任意のドメインに対して 23 個のアラームを抑制できます。

- Analytics では、Cisco Secure Network Analytics（旧 Stealthwatch）バージョン 7.4.0 のアラーム抑制をサポートしています。
- 応答管理用の Syslog は送信されません。
- 抑制のログは保持されますが、監査ログには記録されません。
- 設定のバックアップを実行する場合は、アラーム抑制ファイルを含める必要があります（このファイルを正常に処理したことがある場合のみ）。ただし、Manager でこのファイルの設定のバックアップを作成することを推奨します。

抑制できるアラーム

次のアラームを抑制できます。

アラームタイプ（アラーム ID）	抑制できるアラーム属性
Addr（アドレス）Scan/tcp（276） 送信元ホストが同じポート上でナチュラル クラス C ネットワーク（/24）内の複数のホストと（TCP を使って）通信しようと試みており、ほとんどの接続試行が拒否されているか（TCP リセット）、またはターゲット ホストが全く応答していません。この状況は、[ワームアクティビティ（Worm Activity）] アラームと [ワームの伝播（Worm Propagation ）] アラームのトリガーに使用されます。こうした状況は、一般的にネットワークのスキャン中または列挙中に発生します。	• source_ip • source_groups • プロトコル • destination_ip_range • destination_port
Addr（アドレス）Scan/udp（286） 送信元ホストが同じポート上でナチュラル クラス C ネットワーク（/24）内の複数のホストと（UDP を使って）通信しようと試みており、ほとんどの接続試行が拒否されているか（ICMP ポート到達不能）、またはホストが全く応答していません。こうした状況は、一般的にネットワークのスキャン中または列挙中に発生します。この状況は、[ワームアクティビティ（Worm Activity）] アラームと [ワームの伝播（Worm Propagation ）] アラームのトリガーに使用されます。	• source_ip • source_groups • プロトコル • destination_ip_range • destination_port

アラームタイプ（アラーム ID）	抑制できるアラーム属性
ホストに対してビーコンを実行（39） 内部ホストと外部ホスト間の IP 通信（一方向のトラフィックのみによる）が、[フローを長期間として認定するために必要な秒数（Seconds required to qualify a flow as long duration）] 設定を超えています。	• source _ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
[ボット感染ホスト：試行されたC&Cアクティビティ（Bot Infected Host – Attempted C&C Activity）]（41） 送信元ホストが、C&Cサーバーリストに記載されているポートを使用して、コマンドアンドコントロール（C&C）サーバーに接続しようとしています。この通信は一方向のみであり、C&Cサーバーが応答していないことを示しています。内部ホストは、イニシエータとして、懸念インデックス（CI）ポイントの累積を行います。接続を試みられている C&C サーバーも内部ホストである場合、その C&C サーバーはターゲット インデックス（TI）ポイントの累積を行います。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
[ボット感染ホスト：成功したC&Cアクティビティ（Bot Infected Host – Successful C&C Activity）]（42） 送信元ホストが、C&Cサーバーリストに記載されているポートを使用してC&Cサーバーに接続しました。通信は双方向であり、C&Cサーバーが応答したことを示しています。内部ホストは、イニシエータとして、懸念インデックス（CI）ポイントの累積を行います。接続先のC&Cサーバーも内部ホストである場合は、そのC&Cサーバーがターゲットインデックス（TI）ポイントを累積します。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
ブルートフォースログイン（58） ホストがログインの繰り返しによるブルートフォース パスワード クラッキングの試行と一致する短い TCP 接続の繰り返しを検出しました。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル

アラームタイプ（アラーム ID）	抑制できるアラーム属性
高 SMB ピア（60） このセキュリティ イベントは、ホストで、ワームの拡散と一致する、外部へのサーバ メッセージ ブロック（SMB）セッションが多数発生していることを示します。	• source_ip • source_groups • source_port • プロトコル • flows_count
高トラフィック（30） 5 分間のホスト トラフィック レートの平均が、許容可能なトラフィック値の制限を上回りました。	• source_ip • source_groups • bytes_ per_second
ICMP フラッド（7） 送信元ホストは、5 分間に過剰な数の ICMP パケットを送信しました。	• source_ip • source_groups • パケット
パケットフラッド（8） 送信元ホストが、ターゲット ホストに過大な数のショートパケットを送信しました。このセキュリティ イベントは、ブルート フォース攻撃、DoS 攻撃、ネットワーク アプリケーションの不具合によるものと考えられます。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
特大サイズの Ping パケット（278） 送信元ホストが、90 データ バイトを超える ICMP エコー要求または返信を送信しました。これらのイベントは無害なネットワーク ヘルス チェックである可能性もありますが、隠されたデータ チャネルが含まれている場合もあります。	• source_ip • source_groups • destination_ip • destination_groups • プロトコル
ping スキャン（277） 送信元ホストは、ナチュラル クラス C ネットワーク（/24）範囲のアドレスを使用して、多数のホストにエコー要求パケットを送信しています。これは多くの場合、ネットワーク上のアクティブ ホストを識別するために実行されます。	• source_ip • source_groups • プロトコル • destination_ip_range

アラームタイプ（アラーム ID）	抑制できるアラーム属性
ポートスキャン（55） ソース IP からターゲット IP の多数のポートへの接続が試行されました。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
スキャナ通信（63） このセキュリティ イベントは、ネットワークをスキャンしていたホストが、スキャンしたいずれかのターゲット ホストと双方向の対話を行っていることを示します。これは、内部ホスト ポリシーと外部ホストポリシーでデフォルトで有効になっています。ただし、ネットワーク管理およびスキャナ ロールのポリシーではデフォルトで無効になっています。	• source_ip • source_groups • source_ports • destination_ip • destination_group • destination_port • プロトコル
SSH リバースシェル（61） リバース シェルに見える SSH セッションを検出します。外部ホストに送信されるデータが、受信するデータを上回っています。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
ステルススキャン/TCP（272） 送信元ホストが、同じ送信元ポートを使用して、ターゲット ホスト上の複数のポートに同時に接続していました。この動作は、raw ソケットを使用して TCP または UDP 接続を確立するアプリケーションがあることを示しています。このセキュリティ イベントでは、セキュリティ イベントが認識される前に最後にアクセスしたターゲット ポートが示されます。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル

アラームタイプ（アラーム ID）	抑制できるアラーム属性
ステルススキャン/UDP（271） 送信元ホストによるポート番号の再利用を伴う、細工された UDP スキャン。これは多くの場合、攻撃対象のホストを探しているスキャン元のホストが「パケット クラフティング」を実行していることを示します。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル
データ蓄積の疑い（315） 送信元ホストは、1 つ以上のホストから異常な量のデータをダウンロードしました。	• 送信元 IP アドレス • 送信元グループリスト • bytes
データ損失の疑い（40） 内部のホストが異常なデータ量を外部のホストにアップロードしたことを示します。	• source_ip • source_groups • bytes
疑わしい UDP アクティビティ（24） 送信元ホストが、UDP ポートで複数のホストをスキャンしていることが特定され、サイズの大きい UDP パケットを以前スキャンした別のホストに送信しました。このタイプの動作は、「SQL Slammer」や「Witty」など、多くのシングルパケット UDP ベースのワームの特徴に合致しています。このセキュリティ イベントの調査をただちに行ってください。	• source_ip • source_groups • source _port • destination_ip • destination_groups • destination_port • プロトコル
SYN フラッド（5） 送信元ホストは過剰な数の TCP 接続要求（SYN パケット）を 5 分間送信しました。これは DoS 攻撃または非ステルス性のスキャン アクティビティであることを示している可能性があります。	• source_ip • source_groups • パケット
UDP フラッド（6） 送信元ホストは、5 分間に過剰な数の UDP パケットを送信しました。これは DoS 攻撃または非ステルス性のスキャン アクティビティであることを示している可能性があります。	• source_ip • source_groups • パケット

アラームタイプ(アラーム ID)	抑制できるアラーム属性
ワームの伝播(36) ホストが複数のサブネットを越えて特定のポート上でスキャンし、接続しました。このホストは、以前、[ワーム アクティビティ(Worm Activity)] アラームが発生したホストによってスキャンされ、接続されたことがあります。	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • プロトコル • initial_infected_host

これらのアラームの詳細については、「**セキュリティイベント一覧**」を参照してください。

ルール設定

アラーム抑制ルールを設定するには、API を使用する必要があります。各 API には、次のエンドポイントが含まれています。

- **Get**:現在の抑制設定が表示されます。
- **Put**:アラームを抑制するルールをアップロードし、設定します。
- **Delete**:すべての抑制設定を削除します。

> 管理者ユーザーとプライマリ管理者ユーザーの両方がアラーム抑制ルールを設定できます。

例: 次に、アラームタイプルールの例を示します。ルールの定義は、「400 または 401 に対応するデバイス ID、300 または 301 以外のドメイン ID、22、23、24 に対応する送信元グループ、および 1.1.1.1 または 1.1.1.2 に対応する送信元 IP を持つアドレススキャン TCP アラームの場合」です。

```
{
"rules": [
{
"type": 276,
"filters": [
{ "field": "device_id", "operator": "In", "value": [400, 401] }

,
{ "field": "domain_id", "operator": "NotIn", "value": [300, 301] }

,
{ "field": "source_groups", "operator": "In", "value": [22,23,24] }

,
{ "field": "source_ip", "operator": "In", "value": ["1.1.1.1", "1.1.1.2"] }

]
}
]
}
```

ルールのプロパティ

ルールを設定する場合は、次のガイドラインを参照してください。

- アラームタイプに複数のルールがある場合、それらのルールのいずれか（ルール間の OR 演算）によってアラームが抑制されることがあります。
- 発生したアラームは、抑制する特定のアラームタイプのルールで定義されているすべての属性と一致する必要があります。
- 値に演算子「IN」が使用されている場合、その式内のいずれかの値が true になります（式内の値の OR 演算）。
- 同じアラームタイプに複数のルールを設定できます。
- アラームタイプに関係なく、最大 500 のルールを設定できます。

次に、アドレススキャン TCP の 2 つのルールを示します。ルールの完全なセットに対する JSON は、以下の 2 つのルールに示されています。ルールの定義は次のとおりです。

「（ID が 123、およびデバイス ID が 12 のドメイン内にあるアドレススキャン TCP アラームの場合）

または

（ID が 234、およびデバイス ID が 432 のドメイン内にあるアドレススキャン TCP アラームの場合）」。

```
{
"rules": [
{
"type": 276,
"filters": [
{ "field": "domain_id", "operator" : "Equal", "value": 123}
,
{ "field": "device_id", "operator" : "Equal", "value": 12}
]
},
{
"type" : 276,
"filters": [
{ "field": "domain_id", "operator" : "Equal", "value": 234}
,
{ "field": "device_id", "operator" : "Equal", "value": 432}
]
}
]
}
```

1 つのホストが複数のポートを持つ同じサブネット上でアドレススキャン（TCP/UDP）を実行すると、多数のセキュリティイベントが生成されますが、生成条件は 1 つのみで、1 つのアラームがマネージャの host_alarm データベースに記録されます。

この種類のアラームを抑制するには、次のルールを使用します。

Option 1: Give one port per expression

```
{
"rules" : [ {
"type" : 276,
"filters" : [
{ "field" : "destination_port", "operator" : Equal, "value" : 2049}
]
}, {
"type" : 276,
"filters" : [
{ "field" : "destination_port", "operator" : Equal, "value" : 2055}
,
```

Option 2: Give additional criteria (be more granular). See example below for available attributes

```
{
"type": 276,
"filters": [
{ "field": "device_id", "operator": "Equal", "value": 301 }
,
{ "field": "domain_id", "operator": "Equal", "value": 301 }
,
{ "field": "source_groups", "operator": "In", "value": [65534] }
,
{ "field": "source_ip", "operator": "In", "value": ["10.1.0.9", "10.1.0.8", "10.1.0.7", "10.1.0.6","10.1.0.5"] }
,
{ "field": "destination_ip_range", "operator": "In", "value": ["10.10.0.0"] }
,
{ "field": "protocol", "operator": "In", "value": ["tcp"] }
,
{ "field": "destination_port", "operator": "In", "value": [50] }
]
}
```

属性の詳細

アラームで抑制できる属性は、次の属性タイプのいずれかに分類されます。ルールの作成時に、特定の属性タイプに一致するいずれかの演算子を使用できます。以下の属性は、アラーム間で共通な場合と共通でない場合があります。

> エントリの大文字と小文字は区別されません。たとえば、プロトコルの属性には TCP、tcp、TcP などを使用でき、すべて有効なエントリです。

属性	タイプ	演算子	説明
bytes	長整数型	Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	0 ～ 4294967296 の正の整数。
bytes_per_second	長整数型	Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	0 ～ 4294967296 の正の整数。
device_id （これはフローコレクタ ID です）。	整数または Set<Integer>	整数の場合：Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	正の整数。
		Set<Integer> の場合：In、NotIn	[ ] で囲まれた最大 100 個の整数のセット。
destination_ip	Set<IPAddress>	In、NotIn	[ ] で囲まれた最大 100 個の IP アドレスのセットまたはサブネットアドレス範囲。
destination_ip_range	Set<IPAddress>	In、NotIn	[ ] で囲まれた最大 100 個のサブネットアドレスのセット。
destination_groups	Set<Integer>	In、NotIn	[ ] で囲まれたホストグループ ID を表す整数のセット。

属性	タイプ	演算子	説明
destination_port	整数または Set<Integer>	整数の場合：Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	正の整数。
		Set<Integer> の場合：In、NotIn	[ ] で囲まれた最大 100 個の整数のセット。
domain_id	整数または Set<Integer>	整数の場合：Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	正の整数。
		Set<Integer> の場合：In、NotIn	[ ] で囲まれた最大 100 個の整数のセット。
flows_count	長整数型	Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	0 ～ 4294967296 の正の整数。
initial_infected_host	Set<IPAddress>	In、NotIn	[ ] で囲まれた最大 100 個の IP アドレスのセット。
パケット	長整数型	Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	0 ～ 4294967296 の正の整数。
プロトコル	プロトコルまたは Set<Protocol>	プロトコルの場合：Equal、NotEqual	二重引用符で囲まれた単一の有効なプロトコル名 例：["TCP"]。
		Set<Protocol> の場合：In、NotIn	[ ] で囲まれた最大 100 個の有効なプロトコル名のセット 例：["TCP"、"UDP"]。

属性	タイプ	演算子	説明
source_ip	Set<IPAddress>	In、NotIn	[ ] で囲まれた最大 100 個の IP アドレスのセットまたはサブネットアドレス範囲。
source_groups	Set<Integer>	In、NotIn	[ ] で囲まれた最大 100 個のホストグループ ID を表す整数のセット。
source_port	整数または Set<Integer>	整数の場合：Equal、NotEqual、GreaterThan、GreaterThanEqual、LessThan、LessThanEqual	正の整数。
		Set<Integer> の場合：In、NotIn	[ ] で囲まれた最大 100 個の整数のセット。

API の例

エンドポイントを含む API の概要を要求および応答スキーマとともに確認するには、次のいずれかを実行します。

オプション 1

1. 次の URL を入力します。**https://[manager_ip_address]/api-docs**
2. [API] セクションで [アラームの抑制API（Alarm Suppression API）] というタイトルのリンクまでスクロールして、リンクをクリックします。

   対応するページが開きます。

オプション 2

次の URL を入力します。**https://[manager_ip_address]/legacy-detections/v1/docs**

対応する APIドキュメントが表示されます。

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。
- シスコサポートの連絡先
- 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：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報