Cisco Secure Cloud Analytics

内部接続ウォッチリスト クイック スタート ガイド

目次

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

内部接続ウォッチリストの概要

Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）は、オンプレミスとクラウド内の両方の IT 環境で脅威を検出して対応する SaaS ベースのセキュリティサービスです。このガイドでは、ポリシーおよびセグメンテーションの監査ツールとして Secure Cloud Analytics を使用する方法について説明します。

内部接続ウォッチリストから許可ルールと一致ルールを作成できます。一致ルールをトリガーし、ファイアウォールおよびセグメンテーションポリシーに違反する接続がエンティティで確立されると、一致するトラフィックの詳細が記載された内部接続ウォッチリスト ヒット アラートが生成されます。一致ルールのトリガー対象となる特定のトラフィックを許可する場合は、特定のエンティティ向けに細かくカスタマイズした許可ルールを例外として作成できます。

サブネット設定

ローカル、仮想クラウド、および VPN サブネット内のエンティティに対するアラートの生成方法を設定できます。また、エンティティグループに設定済みのサブネットを追加して、エンティティグループにエンティティの範囲を一度に追加することもできます。設定とサブネットタイプに基づいて、サブネットの感度を設定できます。これにより、サブネットの設定に基づいてシステムが生成するアラートが調整されます。サブネット範囲内の新しいエンティティを検出した場合にシステムがアラートを生成するかどうかも設定できます。詳細については、次の各項を参照してください。

サブネットタイプ	設定オプション	推奨されるサブネット範囲
ローカル（Local）	• サブネット範囲 • アラート生成の相対しきい値 • サブネット内で IP アドレスが静的または動的に割り当てられるかどうか • サブネット範囲内で検出された新しいエンティティに対してアラートを生成するかどうか	• オンプレミスネットワーク展開のローカルエンティティ • 制御対象のオンプレミスネットワーク展開の外部にあるエンティティ
仮想クラウド（AWS および GCP）	• サブネット範囲 • アラート生成の相対しきい値 • サブネット範囲内で検出された新しいエンティティに対してアラートを生成するかどうか	• クラウドベースのネットワーク展開のクラウドエンティティ
VPN	• サブネット範囲	• 追跡対象ではない、重複が原因でネットワーク変換が必要な VPN 内のエンティティ • サードパーティによって制御される、ネットワーク展開の外部にあるエンティティ

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ローカル サブネット アラート設定の指定

ローカルサブネットは、主にオンプレミス展開用に設定します。具体的には、オンプレミスネットワークに対してローカルなエンティティ、または制御対象のオンプレミスネットワークの外部にあるエンティティのローカルサブネットを設定できます。一度に 1 つのエントリを追加することも、複数のエントリをカンマ区切り値（CSV）ファイルでアップロードすることもできます。

ローカルサブネットを追加する際に、次のローカルサブネットのアラート設定を行うことができます。

パラメータ	説明
プレフィックス（Prefix）	IPv4 形式のサブネットプレフィックス。
長さ	CIDR 表記のサブネット長（1 ～ 32）。詳細については、https://tools.ietf.org/html/rfc4632 を参照してください。
デフォルトのエンドポイント感度	生成可能なアラートに影響するデフォルトのサブネット感度： • [高（high）]：システムは、[低（low）]、[通常（normal）]、および [高（high）] 優先度のアラートを生成できます。 • [通常（normal）]：システムは、[通常（normal）] および [高（high）] 優先度のアラートを生成できます。 • [低（low）]：システムは、[高（high）] 優先度のアラートを生成できます。
説明	インターフェイスに表示されるローカルサブネットの説明。

ローカルサブネットを追加した後、次のアラート生成設定を行うことができます。

パラメータ	説明
[機密性（Sensitivity）]	サブネットの感度は、生成可能なアラートに影響します。 • [高（high）]：システムは、[低（low）]、[通常（normal）]、および [高（high）] 優先度のアラートを生成できます。 • [通常（normal）]：システムは、[通常（normal）] および [高（high）] 優先度のアラートを生成できます。 • [低（low）]：システムは、[高（high）] 優先度のアラートを生成できます。
[静的（Static）]	エンティティに、このサブネット内の IP アドレスが静的に割り当てられているのか、DHCP などによって動的に割り当てられているのか。このサブネット内のエンティティが、静的に割り当てられた IP アドレスを受信すると、システムは、IP アドレスが常に同じエンティティと相関すると見なします。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

[新しいデバイスのアラート（New Device Alerts）]	このサブネットに新しいデバイスが出現した場合に、システムがこのサブネットに関してアラートを生成するかどうか。 このサブネットの静的 IP 割り当ても有効にする場合にのみ、このパラメータを有効にすることをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

ローカルサブネットアラート設定へのエントリの追加

1. [設定（Settings）] > [サブネット（Subnets）] > [オンプレミス（On-Premises）] を選択します。
2. [オンプレミスサブネットの作成（Create On-Premises Subnet）] をクリックします。
3. CIDR ブロックの**プレフィックス**を IPv4 アドレスとして入力します。
4. CIDR ブロック**長**（1 ～ 32）を入力します。
5. エントリの**説明**を入力します。
6. 次の選択肢があります。
   - 静的に IP アドレスを割り当てるサブネットを識別するには、[静的（Static）] をオンにします。
   - IP アドレスを動的に割り当てるサブネットを識別するには、[静的（Static）] をオフにします。
7. 次の選択肢があります。
   - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート（New Device Alerts）] を選択します。
   - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート（New Device Alerts）] を選択します。
8. [作成（Create）] をクリックします。
9. ドロップダウンリストから [感度（Sensitivity）] を選択します。
   - [低（low）]：システムはアラートを生成するために高い相対しきい値を必要とします。
   - [通常（normal）]：システムはアラートを生成するために中程度のしきい値を必要とします。
   - [高（high）]：システムはアラートを生成するために低いしきい値を必要とします。

ローカルサブネットアラート設定エントリの検索

1. [設定（Settings）] > [サブネット（Subnets）] > [オンプレミス（On-Premises）] を選択します。
2. **サブネットプレフィックス**を入力し、[適用（Apply）] をクリックして、ローカルサブネットアラート設定エントリを見つけます。

ローカルサブネットアラート設定エントリの変更

1. [設定（Settings）] > [サブネット（Subnets）] > [オンプレミス（On-Premises）] を選択します。
2. 既存のエントリについて、ドロップダウン リストから [機密性（Sensitivity）] を選択します。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. 次の選択肢があります。
    - IP アドレスを静的に割り当てるサブネットを識別するには、[静的(Static)] をオンにします。
    - IP アドレスを動的に割り当てるサブネットを識別するには、[静的(Static)] をオフにします。
4. 次の選択肢があります。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。

ローカル サブネット設定ファイルのアップロード

複数のローカル サブネット エントリ(1 行に 1 エントリずつ)を含むコンマ区切り値ファイルをアップロードできます。各行は次の形式である必要があります。

```
<cidr-prefix>,<cidr-length>,<description>,[sensitivity],[static-ip-assign],[new-device-alerts]
```

詳細については、次の各項を参照してください。

パラメータ	必須	使用可能な値
`<cidr-prefix>`	はい	IPv4 アドレス。
`<cidr-length>`	はい	1 ～ 32 の整数。
`<description>`	はい	任意の英数字。
`[sensitivity]`	いいえ	次のいずれかです。 • [低(low)]:システムはアラートを生成するために高い相対しきい値を必要とします。 • [通常(normal)]:システムはアラートを生成するために中程度のしきい値を必要とします。 • [高(high)]:システムはアラートを生成するために低いしきい値を必要とします。
`[static-ip-assign]`	いいえ	次のいずれかです。 • [真(true)]:サブネット内のエンティティは静的に割り当てられた IP　アドレスを受け取ります。 • [偽(false)]:サブネット内のエンティティは動的に割り当てられた IP　アドレスを受け取ります。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

`[new-device-alerts]`	いいえ	次のいずれかです。 • [真(true)]:システムはサブネット内で検出された新しいデバイスに関してアラートを生成します。 • [偽(false)]:システムはサブネット内で検出された新しいデバイスに関してアラートを抑制します。 `[static-ip-assign]` も true に設定する場合にのみ、このパラメータを `true` に設定することをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

サブネットアラート設定ファイルのアップロード

1. [設定(Settings)]>[サブネット(Subnets)]>[オンプレミス(On-Premises)]を選択します。
2. [CSV のアップロード(Upload CSV)]をクリックします。
3. [ファイルのアップロード(Upload File)]をクリックして、アップロードするファイルを選択します。

仮想クラウド サブネット設定の変更

提供されているデフォルトのポリシー設定を使用してクラウドベース環境向けに Cisco Secure Cloud Analytics パブリッククラウドのモニタリング(旧 Stealthwatch Cloud パブリック クラウド モニータリング)を設定すると、Secure Cloud Analytics では、設定済みの権限を介してクラウドサブネット情報が取得されます。

エントリを検出した後、仮想クラウドサブネットに関して次のアラート生成設定を指定できます。

パラメータ	説明
[機密性(Sensitivity)]	サブネットの感度は、生成可能なアラートに影響します。 • [高(high)]:システムは、[低(low)]、[通常(normal)]、および [高(high)] 優先度のアラートを生成できます。 • [通常(normal)]:システムは、[通常(normal)] および [高(high)] 優先度のアラートを生成できます。 • [低(low)]:システムは、[高(high)] 優先度のアラートを生成できます。
[静的(Static)]	エンティティに、このサブネット内の IP アドレスが静的に割り当てられているのか、DHCP などによって動的に割り当てられているのか。このサブネット内のエンティティが、静的に割り当てられた IP アドレスを受信すると、システムは、IP アドレスが常に同じエンティティと相関すると見なします。
[新しいデバイスのアラート(New Device	このサブネットに新しいデバイスが出現した場合に、システムがこのサブネットに関してアラートを生成するかどうか。 このサブネットの静的 IP 割り当ても有効にする場合にのみ、このパラメータを

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Alerts)]	有効にすることをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

システムが仮想クラウドサブネットを追加した後、エントリを検索できます。

仮想クラウドサブネットアラート設定エントリの検索

1. [設定(Settings)] > [サブネット(Subnets)] を選択します。
2. [Amazon Web Services]、[Google Cloud Platform]、または [Microsoft Azure] を選択します。
3. **サブネットプレフィックス**を入力し、[適用(Apply)] をクリックして、仮想クラウドサブネットアラート設定エントリを見つけます。

仮想クラウドサブネットアラート設定エントリの変更

1. [設定(Settings)] > [サブネット(Subnets)] を選択します。
2. [Amazon Web Services]、[Google Cloud Platform]、または [Microsoft Azure] を選択します。
3. 既存のエントリについて、ドロップダウン リストから [機密性(Sensitivity)] を選択します。
4. 次の選択肢があります。
   - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。
   - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。

VPN サブネット アラート設定の指定

VPN サブネットは、信頼できるサードパーティの関係会社など、管理対象ネットワークの拡張と見なされる外部 IP アドレススペースを識別します。これらのサブネットは、追跡対象でないサードパーティによって制御される外部エンティティに設定できます。

VPN サブネットを追加する際に、次の VPN サブネットアラート設定を構成できます。

パラメータ	**説明**
プレフィックス(Prefix)	IPv4 形式のサブネットプレフィックス。
長さ	CIDR 表記のサブネット長(1 ～ 32)。詳細については、https://tools.ietf.org/html/rfc4632 を参照してください。
説明	インターフェイスに表示されるローカルサブネットの説明。

VPN サブネットを追加したら、エントリを検索できます。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ローカルサブネットアラート設定とは対照的に、機密性や IP アドレス割り当て、または VPN サブネットに関して新しいエンティティが検出されたときにアラートが生成されるかどうかを変更することはできません。インターフェイスに表示される説明のみを変更できます。

VPN サブネットアラート設定へのエントリの追加

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. [VPNサブネットの作成(Create VPN Subnet)] をクリックします。
3. CIDR ブロックの**プレフィックス**を IPv4 アドレスとして入力します。
4. CIDR ブロック**長**(1 ～ 32)を入力します。
5. エントリの**説明**を入力します。
6. [作成(Create)] をクリックします。

VPN サブネットアラート設定エントリの検索

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. **サブネットプレフィックス**を入力し、[検索(Search)] をクリックして、VPN サブネットアラート設定エントリを見つけます。

VPN サブネットアラート設定エントリの変更

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. [編集(Edit)] アイコンをクリックします。
3. [説明(Description)] を更新します。
4. [更新(Update)] をクリックします。

エンティティグループの設定

ユーザー定義のサブネットと CIDR ブロックをグループ化する、Secure Cloud Analytics 展開のエンティティグループを設定できます。その後、内部接続ウォッチリストエントリにこれらのグループを使用して、エンティティごとに個別のエントリを作成するのではなく、複数のエンティティまたは特定のブロックの IP アドレスの可能なエンティティをモニターできます。

サブネットを追加するには、まず [サブネット(Subnets)] 設定でサブネットを設定します。詳細については、「サブネットの設定」を参照してください。

CIDR ブロックを追加するには、それらを個別に定義するか、複数の CIDR ブロックを含むカンマ区切り値(CSV)ファイルをアップロードします。ファイル内の各エントリは、`prefix,length` 形式に従う必要があり、1 行につき最初のエントリのみがアップロードされます。システムが重複 CIDR ブロックを検出した場合、重複ブロックはエンティティグループに追加されません。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

エンティティグループの設定

エンティティグループの作成:

手順

1. [設定(Settings)]>[エンティティグループ(Entity Groups)]を選択します。
2. [新しいエンティティグループ(New Entity Group)]をクリックします。
3. エンティティグループの[名前(Name)]と[説明(Description)]を入力します。
4. [次へ(Next)]をクリックします。

   [サブネット(Subnets)]タブが表示されます。
5. サブネットを追加する場合は、次のオプションがあります。
   - [サブネットを追加(Add Subnets)]ペインから1つ以上のサブネットを選択し、[選択したものをグループに追加(Add Selected to Group)]をクリックしてエンティティグループに追加します。
   - [現在グループ内にある(Currently In Group)]ペインから1つ以上のサブネットを選択し、[選択したものを削除(Delete Selected)]をクリックしてエンティティグループから削除します。

   サブネットの作成についての詳細は、「サブネットの設定」を参照してください。
6. [CIDRs]タブを選択します。
7. CIDRブロックを追加する場合は、次のオプションがあります。
   - [CIDRプレフィックス(CIDR Prefix)]と[長さ(Length)]を入力し、[追加(Add)]をクリックして1つのCIDRブロックをエンティティグループに追加します。表示されるIPアドレスだけをモニターする場合は、[長さ(Length)]に「32」と入力し、より大きなCIDRブロック値をモニターするには、異なる値を入力します。
   - [参照(Browse)]をクリックし、`prefix,length`の形式でCIDRブロックを含むCSVファイルを1行に1エントリずつ選択し、[アップロード(Upload)]をクリックして各行の最初のCIDRブロックをエンティティグループに追加します。
8. [作成(Create)]をクリックします。

エンティティグループの変更:

手順

1. [設定(Settings)]>[エンティティグループ(Entity Groups)]を選択します。
2. 既存のエンティティグループの[編集(Edit)]をクリックします。
3. エンティティグループに異なる[名前(Name)]と[説明(Description)]を入力します。
4. [サブネット(Subnets)]タブを選択します。
5. 次の選択肢があります。
   - [CIDRプレフィックス(CIDR Prefix)]と[長さ(Length)]を入力し、[追加(Add)]をクリックして1つのCIDRブロックをエンティティグループに追加します。表示されるIPアドレスだけをモニターする場合は、[長さ(Length)]に「32」と入力し、より大きなCIDRブロック値をモニターするには、異なる値を入力します。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- [参照(Browse)]をクリックし、`prefix,length` の形式で CIDR ブロックを含む CSV ファイルを 1 行に 1 エントリずつ選択し、[アップロード(Upload)]をクリックして各行の最初の CIDR ブロックをエンティティグループに追加します。

6. [CIDRs]タブを選択します。
7. 次の選択肢があります。
   - [サブネットを追加(Add Subnets)]ペインから 1 つ以上のサブネットを選択し、[選択したものをグループに追加(Add Selected to Group)]をクリックしてエンティティグループに追加します。
   - [現在グループ内にある(Currently In Group)]ペインから 1 つ以上のサブネットを選択し、[選択したものを削除(Delete Selected)]をクリックしてエンティティグループから削除します。

   サブネットの作成についての詳細は、「サブネットの設定」を参照してください。
8. [完了(Done)]をクリックして変更を保存します。

エンティティグループの削除

手順

1. [設定(Settings)]>[エンティティグループ(Entity Groups)]を選択します。
2. 既存のエンティティグループの削除アイコンをクリックし、選択を確認します。

アラート向けの一般的なプロトコルとプログラム

ポートの包括的なリストについては、https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml を参照してください。

> 信頼できるホストに対して特定のプロトコルを介したトラフィックを許可する場合は、広範な一致ルールと組み合わせて、細かくカスタマイズした許可ルールを作成します。

プロトコルまたはプログラム	関連するポート
Domain Name Service(DNS)	53/TCP、53/UDP
サーバーメッセージブロック(SMB)/Samba	445/TCP
NetBIOS 経由の SMB/Samba	137/TCP、137/UDP、138/UDP、139/TCP
SSH	22/TCP
TeamViewer	5938/TCP、5938/UDP
telnet	23/TCP、23/UDP
Virtual Network Computing(VNC)	5800/TCP、5900/TCP(デフォルト)
Windows リモートデスクトップ	3389/TCP、3389/UDP

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ポリシー違反ルールの作成

ポリシー違反ルールを作成する際、次の点に注意してください。

- Secure Cloud Analytics はトラフィックフローに影響を与えないため、許可ルールと一致ルールはファイアウォールルールとして機能しません。トラフィックがこれらのルールに一致し、システムがアラートを生成した場合でも、トラフィックを直接許可またはブロックすることはありませんが、アラートとトラフィックに関係するエンティティを調査できます。
- デフォルトでは、内部接続ウォッチリストに追加したルールは、一致ルールになります。許可ルールを作成するには、[許可された接続(Connections are Allowed)] を有効にします。一般的には、許可ルールをより広範な一致ルールと組み合わせて使用して、信頼できるホストの正当なトラフィックを許可し、そのタイプの他のすべてのトラフィックに対して一致ルールをトリガーします。
- 1 つの監視対象または接続先エンティティでアラートを作成する場合、CIDR の**ブロックサイズ**を 32 にします。CIDR ブロック境界と指定する CIDR ブロック内の IP アドレスについては、https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#IPv4_CIDR_blocks を参照してください。
- 特定のプロトコルまたはプログラムを使用して監視対象エンティティにアラートを送信する場合、**宛先 IP** には 0.0.0.0、**宛先ブロックサイズ** には 0 を入力します。また、プロトコルまたはプログラムに関連付けられた**宛先ポート**を入力します。

ポリシー違反ルールの作成:

はじめる前に

- Web ポータル UI にログインします。

手順

1. [設定(Settings)] > [アラート(Alerts)] > [内部接続ウォッチリスト(Internal Connections Watchlist)] を選択します。
2. [新しいウォッチリスト項目(New Watchlist Item)] をクリックします。
3. ウォッチリストエントリの [ルール名(Rule Name)] と [説明(Description)] を入力します。
4. このエントリに一致する接続で観測内容やアラートが生成されないようにするには、[許可(Allowed)] の [接続ルールタイプ(Connection Rule Type)] を選択します。このエントリに一致する接続で観測内容やアラートが生成されるようにするには、[不可(NOT Allowed)] を選択します。

   [許可(Allowed)] ルールを追加する前に、少なくとも 1 つの [不可(NOT Allowed)] ルールを内部接続ウォッチリストに追加する必要があります。
5. ドロップダウンリストから [プロトコル(Protocol)] を選択します。
6. [送信元(Source)] を選択してフィールドを展開します。
7. 次の選択肢があります。

   [CIDR] を選択し、[IPアドレス(IP Address)] と [バイト/長さ(Bytes/Length)] を入力して、送信元 CIDR ブロックを定義します。表示される IP アドレスだけをモニターする場合は、[バイト/長さ(Bytes/Length)] に「32」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

[エンティティグループ(Entity Groups)]を選択し、[エンティティグループを追加(Add Entity Group(s))]をクリックして 1 つ以上のエンティティグループを選択し、[送信元に追加(Add to Source)]をクリックします。

8. 送信元を特定のポートに制限する場合は、個別の送信元**ポート**またはポート範囲を入力します。
9. [宛先(Destination)]を選択してフィールドを展開します。
10. 次の選択肢があります。

    [CIDR]を選択し、[IPアドレス(IP Address)]と[バイト/長さ(Bytes/Length)]を入力して、宛先 CIDR ブロックを定義します。表示される IP アドレスだけをモニターする場合は、[バイト/長さ(Bytes/Length)]に「`32`」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。

    [エンティティグループ(Entity Groups)]を選択し、[エンティティグループを追加(Add Entity Group(s))]をクリックして 1 つ以上のエンティティグループを選択し、[宛先に追加(Add to Destination)]をクリックします。

11. 宛先を特定のポートに制限する場合は、個別の宛先**ポート**またはポート範囲を入力します。
12. [保存(Save)]をクリックします。

ポリシー違反アラートの表示

トラフィックによっていずれかの一致ルールがトリガーされると、内部接続ウォッチリストの観測結果が自動的に生成されます。また、内部ウォッチリスト接続ヒットアラートも生成されます。複数の観測結果により発信される他のアラートとは異なり、観測機能に関連付けられたトラフィックが一致ルールの 1 つをトリガーすると、システムは 1 つの観測結果のみで内部接続ウォッチリスト ヒット アラートを生成します。ただし、複数の観測結果によって一致ルールの 1 つがトリガーされた場合、システムはアラートを生成して、アラート内に監視対象のすべてを一覧表示します。

アラートリストをフィルタリングして、ポリシー違反アラートのみを表示することができます。

ポリシー違反アラートの表示

はじめる前に

- Web ポータル UI にログインします。

手順

1. [モニター(Monitor)]>[アラート(Alerts)]を選択します。
2. フィルターフィールドに `internal connection watchlist hit` を入力し、🔍 **(虫眼鏡)**アイコンをクリックしてアラートリストを並べ替えます。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

関連リソース

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html を参照してください。
- 60 日間の無料トライアルに登録するには、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html にアクセスしてください。
- ドキュメントリソースについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html を参照してください。
- Secure Cloud Analytics 初期導入ガイドなど、インストールおよびコンフィギュレーション ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html を参照してください。

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
  swatchc-support@cisco.com

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコ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。（1721R）

© 2022 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.