Cisco Secure Cloud Analytics

サブネット設定ガイド

目次

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

サブネットの監視とアラートの概要

Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）は、ダイナミック エンティティ モデリングを使用してネットワークエンティティを追跡し、トラフィックに関する観測データを作成します。また、この観測データに基づきアラートを生成します。Secure Cloud Analytics のデフォルト設定では、トラフィックを生成する RFC 1918 の IP スペース内にある任意の IP アドレスにエンティティを作成します。Secure Cloud Analytics では監視対象のネットワークとその感度レベルをカスタマイズできます。このガイドでは、ネットワークのポータルを設定する方法について説明します。

ダイナミック エンティティ モデリングとサブネット監視の設定

エンティティモデリングは、ネットワーク上のエンティティの動作を学習するプロセスです。トラフィックを送信するすべての IP アドレスが、監視対象のエンティティと見なされます。IP アドレスがトラフィックを受信するだけで、トラフィックを生成しない場合（ネットワークスキャナが、存在しない IP に対して使用される場合など）、その IP アドレスは監視対象のエンティティとは見なされません。システムのデフォルト動作は以下のとおりです。

RFC 1918 の IP スペースに事前定義された内部サブネット：

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`

たとえば、Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）がデフォルトのサブネットを監視するように設定されているが、`198.51.100.0/24` ではないとします。次の動作が想定されています。

- 定義されたサブネット（`192.168.0.0/16` など）内のエンティティが接続を確立する場合、システムはこれらのエンティティのトラフィックを追跡してモデル化します。各エンティティが一意のエンティティとして追跡されます。
- 定義されたサブネット（`192.168.0.0/16`）内のエンティティが別の定義されたサブネット（`10.0.0.0/8` など）内のエンティティと接続を確立する場合、システムはこれらのエンティティのトラフィックを追跡してモデル化します。
- 定義されたサブネット（`192.168.0.0/16`）内のエンティティが、定義されたサブネット（`198.51.100.0/24`）にリストされていない外部 IP アドレスと接続を確立する場合、システムはトラフィックを追跡しますが、内部エンティティのみをモデル化します。
- 定義されていないサブネット（`198.51.100.0/24` など）内の 2 つの IP アドレスが接続を確立する場合、このサブネットはデフォルトで監視対象ではないため、システムはどちらのエンティティでもモデル化を実行せず、トラフィックも追跡しません。

ダイナミック エンティティ モデリングからのサブネットの除外

サブネットの設定では、デフォルトの RFC 1918 スペースに従うことを推奨します。定義したサブネットは、ネットワークに合わせて変更できます。追加のサブネットをより詳細に定義したり、内部として扱う必要がある外部 IP スペースを追加したりすることもできます。

サブネット設定ページでサブネットを定義することに加えて、センサーでトラフィックを可視化できるようにする必要もあります。

エンティティモデリングからローカルサブネットを除外することが必要になる場合があります。ただし、サブネットがトラフィックを生成していることがシステムで観測され、そのサブネットが RFC 1918 スペース内にある場合、定義されているサブネットから削除しても、Secure Cloud Analytics はエン

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

ティティとしての IP アドレスの追跡を停止しません。この動作はハードコード化されているためです。RFC 1918 内のサブネットを削除するには、除外するサブネットを記載した電子メールを support@obsrvbl.com に送信してください。

> サブネットをアラート対象外にするには、サブネットの感度を指定せずにローカルサブネットとして定義する必要があります。

サブネットとアラートの生成

アラートは、システムによって識別される悪意のある動作の可能性を示す実用的なアイテムです。デフォルトでは、事前定義したすべてのサブネットは [標準(normal)] に設定されます。つまり、優先順位が [標準(normal)] または [高(high)] のアラートタイプがそのサブネットに対してアクティブ化されますが、優先順位が [低(low)] のアラートタイプは、そのサブネットに対してアクティブ化されず、生成されても自動的にクローズします。

サブネットの感度は、[なし(none)]、[低(low)]、[標準(normal)]、[高(high)] に設定できます。サブネットの感度レベルを [なし(none)] に設定すると、アクティブな IP アドレスは引き続きエンティティとして扱われ、モデル化されますが、そのサブネット内のエンドポイントに対してアラートはトリガーされません。[なし(none)] に設定するのは、パブリックにアクセス可能でデバイスの回転率が高い、ゲスト ワイヤレス ネットワークなどのアンマネージドネットワークの場合です。詳細については、以下を参照してください。

	アラートタイプの優先順位「低」	アラートタイプの優先順位「中」	アラートタイプの優先順位「高」
サブネットアラート感度なし	アラートなし	アラートなし	アラートなし
低いサブネットアラート感度	アラートなし	アラートなし	アラート
通常のサブネットアラート感度	アラートなし	アラート	アラート
高いサブネットアラート感度	アラート	アラート	アラート

追加のサブネット設定

Secure Cloud Analytics では、次の 3 つのサブネットカテゴリを定義できます。

- オンプレミス環境のエンティティを含むローカルサブネット
- クラウドベースの環境のエンティティを含む仮想クラウドサブネット
- 信頼できるが管理対象外のサードパーティエンティティを含む VPN サブネット

通常、CSV ファイルをインポートして、ローカルサブネットと VPN サブネットを手動で編集します。対照的に、Secure Cloud Analytics ではクラウドプロバイダー(AWS および GCP)から仮想クラウドサブネットが直接取得されます。

> Secure Cloud Analytics はサードパーティの IP 管理ツールと統合されていません。

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

VPN サブネットは、エンドポイントが定期的に通信するパートナーなどの外部の信頼できるエンティティに使用され、他の外部 IP アドレスよりも信頼されます。

感度レベルに加えて、サブネットごとに 2 つのオプションを設定できます。

- [静的(Static)]:サブネット上の IP アドレスが主に静的であり、変更されない場合は、これを有効にします。
- [新しいデバイスのアラート(New Device Alerts)]:これを有効にすると、サブネット範囲で新しいエンティティが検出されるたびにアラートが生成されます。これにより、多くのアラートが生成される可能性があるため、非常に機密性の高いサブネット範囲にのみ使用する必要があります。

サブネット設定

サブネットの監視とアラートを設定するには、次の手順を実行します。

1. センサーの設定にサブネットを追加するには、「Sensorの監視設定」を参照してください。
2. 次を参照してください。
    - サブネット設定の概要:「 サブネット設定」
    - ローカルサブネットの追加およびサブネット感度の調整:「 ローカルサブネットのアラート設定」
    - 仮想クラウドサブネットの変更およびサブネット感度の調整:「 仮想クラウドサブネット設定の変更」
    - サブネットの追加:「 VPN サブネットアラートの設定」
3. アラートタイプの優先順位を変更するには、「アラート優先順位の更新」を参照してください。

Sensorのモニターリング設定

Secure Cloud Analytics Web UI では、センサーがモニターするサブネットを設定できます。また、パッシブ DNS を使用する場合は、キャプチャする 1 秒あたりのパケット数を設定できます。センサーの設定からサブネット範囲を削除すると、そのサブネットから送信されたパケットを無視するようにセンサーに指示されます。

センサーのモニター対象ネットワークにリストされていない IP アドレスに対してなぜエンティティが作成されるのか、混乱が生じます。これは、モニター対象範囲にリスト**されている**エンティティが、リストされていない範囲と通信しているためです。

たとえば、`192.168.0.0/24` の範囲だけをモニターするように設定されたセンサーがあるとします。システムは、その範囲のトラフィックを送信する IP アドレスをエンティティと見なします。さらに、`192.168.0.0/24` の範囲内のエンティティが `10.0.0.0/8` の範囲内の IP アドレスと通信していることが確認された場合、`192.168.0.0/24` はモニター対象範囲と見なされるため、センサーはそのトラフィックをモニターします。次の理由により、システムはモニター対象でない `10.0.0.0/8` の範囲にある他の IP アドレスのエンティティも作成します。

- `10.0.0.0/8` の範囲は RFC 1918 スペースの一部である、および
- その範囲の IP アドレスがモニター対象の IP アドレスと通信していることが確認された。

センサーによるモニターリング用に `10.0.0.0/8` の範囲が定義されておらず、`10.0.0.0/8` サブネット内の 2 つの IP アドレスが相互に通信するだけの場合、どちらも定義されたサブネットと直接通信していないため、どちらもエンティティとは見なされません。

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

センサーのモニタリングの設定

手順

1. [設定（Settings）] > [Sensor（Sensors）] > [Sensorリスト（Sensor List）] を選択します。
2. 設定するセンサーについて、[設定の変更（Change Settings）] をクリックします。
3. [モニターリング（Monitoring）] タブを選択します。
4. 1 つ以上の CIDR ブロックを [モニターするネットワーク（Networks to monitor）] フィールドに 1 行に 1 つずつ追加します。
5. **PDNS に関してキャプチャする 1 秒あたりのパケット数**を選択します。
6. **[保存（Save）]**をクリックします。

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	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。 • [なし（none）]：システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
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。

Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）のモニターリング設定からデフォルトの内部サブネットを削除しても、システムは引き続きこれらのサブネット内のエンティティに対して動的エンティティモデリングを実行します。これらのエンティティでアラートの受信を停止するには、サブネットをローカルサブネットとして明示的に追加し、感度を [なし（none）] に設定する必要があります。

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

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。 • [なし（none）]：システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
[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 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：

手順

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。
   - 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。
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。

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

- 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。
    - [なし(none)]:システムでアラートが生成されません。
    - [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:

手順

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:

手順

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。
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。

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

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。 • [なし(none)]:システムでアラートが生成されません。 • [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。
`[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 [真(true)] に設定する場合にのみ、このパラメータを [真(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。

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

サブネット アラート設定ファイルのアップロード:

手順

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。 • [なし(none)]:システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
[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 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。

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。

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

仮想クラウドサブネットアラート設定エントリの検索：

手順

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：

手順

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	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。

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。

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

VPN サブネット アラート設定へのエントリの追加:

手順

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:

手順

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:

手順

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。

サブネット レポート

[サブネットレポート(Subnet Report)] ページには、トラフィックを送信したものとしてシステムが検出したサブネットが含まれます。レポートには、次の概要が含まれます。

- すべてのアクティブなサブネット
- これらのサブネットが生成するトラフィック
- サブネット内のアクティブな IP アドレスの数
- サブネット間で送信されるトラフィックを表示するテーブル

デフォルトでは、レポートには過去 24 時間分のトラフィックが表示されます。システムに表示されるサブネットのタイムスタンプと、それらのサブネットに関連する情報を変更できます。レポートからの情報を含むカンマ区切りファイルをダウンロードすることもできます。

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

サブネットレポートの表示

[サブネットレポート(Subnet Report)] ページには、トラフィックを送信したものとしてシステムが検出したサブネットが含まれます。レポートには、次の概要が含まれます。

- すべてのアクティブなサブネット
- これらのサブネットが生成するトラフィック
- サブネット内のアクティブな IP アドレスの数
- サブネット間で送信されるトラフィックを表示するテーブル

デフォルトでは、レポートには過去 24 時間分のトラフィックが表示されます。システムに表示されるサブネットのタイムスタンプと、それらのサブネットに関連する情報を変更できます。レポートからの情報を含むカンマ区切りファイルをダウンロードすることもできます。

サブネットレポートの表示:

手順

- [レポート(Report)] > [サブネットレポート(Subnet Report)] を選択します。

サブネットレポートに表示される期間の変更:

手順

1. フィルターペインを展開します。
2. 新しい**開始日**と**開始時刻**を入力します。
3. 新しい**終了日**と**終了時刻**を入力します。
4. **[更新(Update)]** をクリックします。

レポート情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の下にある [CSV] をクリックします。

アラート優先順位設定

アラート タイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は [低(low)] または [通常(normal)] にデフォルト設定されます。そのアラート タイプの優先順位も [低(low)]、[通常(normal)]、または [高(high)] に設定できます。

アラートの優先度は、アラートが自動的に閉じるかどうかを決定するためにサブネットの感度と組み合わせて使用されます。たとえば、[過剰アクセス試行回数(外部)(Excessive Access Attempts (External))] アラート タイプの優先順位はデフォルトで [低(low)] に設定されます。このアラートは、[高(High)] に設定されていないサブネットに対しては自動的にクローズされます。

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

アラート優先順位の更新

手順

1. 次の選択肢があります。
    - [設定（Settings）] > [アラート（Alerts）] > [優先順位（Priorities）] を選択します。
    - [モニター（Monitor）] > [アラート（Alerts）] を選択し、次に [関連する設定リンク（Related Config Links）] > [アラートの優先順位（Alert Priorities）] を選択します。
2. アラートタイプには、ドロップダウンからアラートの**優先順位**を選択します。

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

その他のリソースおよびサポート

さらにサポートが必要な場合は、support@obsrvbl.com まで電子メールでお問い合わせください。

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 無料トライアルのガイドなど、インストールおよび設定ガイドについては、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.

変更履歴

リビジョン	改訂日	説明
1.0	2019 年 5 月 14 日	最初のバージョン。
1.1	2020 年 10 月 15 日	UI の更新に基づく更新。
2.0	2021 年 11 月 3 日	製品のブランド名を更新。

© 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.