Cisco Secure Network Analytics

Analytics：検出、アラート、および観測 7.4.1

目次

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

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

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

概要

現在、Cisco Secure Network Analytics（以前の Stealthwatch）のアラートを更新しています。新しいアラートは、正確なデータを提供し続けながら、すぐに使用できるより高い価値を持ち、調整や事前構成が少なくて済みます。v7.4.1 では、製品の指定されたスペース内で、これらの新しいアラートと機能の選択への先行アクセスを提供しています。

拡張機能の一部は次のとおりです。

- 自動ロール分類
- 最新の脅威に合わせたアラート
- 「エンティティモデリング」と呼ばれる当社の SaaS 製品（Cisco Secure Cloud Analytics）に現在存在する、通常の動作のベースラインを大幅に強化する独自の機能

新しいアラートを有効にすると、展開内で関連機能がオンになります。これらの追加機能は、既存の検出機能およびインターフェイスと並行して機能します。シスコの新しい実験的な検出機能とインターフェイス機能を活用しながら、アラーム、セキュリティイベント、Manager を引き続き監視できます。

マネージャで新しいアラートを開くと、アラートが生成された原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。

新しいアラートは、追加のシステムリソースを消費します。このオプション機能を有効にする前に、リソースの消費状況を確認してください。新しいアラートの機能セットとその一般提供は、特定のタイプの展開に限定されており、今後のリリースごとに変更される可能性があります。詳細については、「**システム要件**」を参照してください。

新しいアラートをご使用の際には、インライン フィードバック フォームを使用してフィードバックをお寄せください。

- 新しいアラートは、Cisco Secure Network Analytics Data Store ドメインを 1 つだけ含むシステムのみをサポートします。（システムには、Data Store 以外のドメインを 1 つ以上含めることもできます）。最初に Data Store ドメインを 1 つ作成し、後で複数の Data Store ドメインを作成する場合、シスコではこのシナリオはサポートされていないことに注意してください。
- ネットワークに少なくとも 1 つのノードを展開し、1 つ以上の Data Store Flow Collector（NetFlow）を追加するまで、新しいアラートは有効にできません。
- システムで sFlow を使用している場合、検出の精度とシステムのパフォーマンスに影響が出る可能性があります。

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

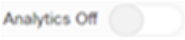
アラートの有効化

1. メインメニューで、[設定（Configure）] > [Analytics] の順に選択します。
   [Analyticsへようこそ（Analytics Welcome）] ページが開きます。
2. ページの右上隅にあるスイッチをクリックすると、次の図のようになります。 

   [アラート（Alerts）] ダッシュボードが開きます。

- 新しいアラートを有効および無効にできるのは、管理者ユーザーのみです。
- アナリスト Web ロールが割り当てられたユーザーは、メニューオプション（[設定（Configure）] > [アラート（Alerts）]）を使用して設定ページにアクセスできません。ただし、すべてのユーザーは、割り当てられたデータロールや機能ロールに関係なく、新しいアラートに関連するすべてのページとデータにアクセスできます。

アラートの無効化

1. メインメニューで、[設定（Configure）] > [Analytics] の順に選択します。
   [Analyticsへようこそ（Analytics Welcome）] ページが開きます。
2. ページの右上隅にあるスイッチをクリックすると、次の図のようになります。 

   [Analyticsへようこそ（Analytics Welcome）] ページは開いたままです。

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

システム要件

新しいアラートの機能セットとその一般提供は、特定のタイプの展開に限定されており、今後のリリースごとに変更される可能性があります。システムが必要な仕様に準拠していることを確認してください。該当する仕様に準拠していないシステムや、高負荷のシステムでは、パフォーマンス、信頼性、保持機能に悪影響が及ぶ可能性があります。

展開のタイプに必要なシステム要件の詳細については、『Virtual Edition Appliance Installation Guide 』の「Resource Requirements」セクションを参照してください。

- 新しいアラートを有効および無効にできるのは、**管理者**ユーザーのみです。
- 新しいアラートをマネージャ（旧 Stealthwatch Management Console）フェールオーバーペアで構成することはできません。

新しいアラートを有効にするには、以下の条件で展開を設定する必要があります

- 任意の数の Flow Collector を備えた仮想またはハードウェア Data Store 展開で設定する。
- Secure Network Analytics Data Store ドメインは 1 つのみ使用する。

アプライアンスをインストールするには、『Virtual Edition Appliance Installation Guide』または『x2xx Series Hardware Appliance Installation Guide』の手順に従います。

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

API

Secure Network Analytics で API を使用する場合は、Cisco Secure Cloud Analytics API ドキュメント [英語] を参照してください。このドキュメントには、Cisco Secure Network Analytics 内の新しいアラートのエンジンで利用できるすべての API エンドポイントと関連ドキュメントが含まれています。

それらの API エンドポイントは、Cisco Secure Network Analytics と Cisco Secure Cloud Analytics の間で共有され、どちらの展開にも使用できます。

それらの API を Secure Network Analytics で使用するには、次のコマンドにある *api_key* を引き続き使用する必要があります。
cat /lancope/var/services/detections/config/api_key

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

アラートと観測の概要

Secure Network Analytics 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の状態を追跡します。Secure Network Analytics のコンテキストにおけるエンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。

この情報から、Secure Network Analytics は次のことを識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メール サーバーに関連付けられるトラフィックを送信する場合、Secure Network Analytics は、そのエンティティに電子メール サーバー ロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。
- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、ウォッチリスト上のエンティティとのやり取り、別のエンティティとの間で確立されたリモートアクセスセッションなど）です。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいて Secure Network Analytics が生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。

アラート前提条件チャート

アラート前提条件チャートには、基準要件でソートされた新しいアラートのリストと、アラートの意味に関する簡単な説明が表示されます。

次の表に、特定のアラートタイプを生成するために必要な履歴の量と、さらなる調査の実施について考えられる理由を示します。調査の理由は、このアラートがリストに挙げられた動作または根拠を示唆することを保証するものではないことに注意してください。これらの理由は、アラートのさらなる調査の際に考慮する必要があります。

また、アラートタイプに関連付けられている MITRE ATT&CK の戦術や手法も示します（該当する場合）。

アラート	履歴	テレメトリ	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
アンプ攻撃	0 日	NetFlow	影響	ネットワークサービス妨害
異常な Windows ワークステーション	14 日間	NetFlow		
国のセットからの逸脱	36 日間	NetFlow		
新たなプロファイル	14 日間	NetFlow	データ漏洩	代替プロトコルによるデータ漏洩

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

アラート	履歴	テレメトリ	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
Empire コマンドアンドコントロール	1 日間	NetFlow	コマンドアンドコントロール	非アプリケーション層プロトコル
例外的なドメインコントローラ	7 日間	NetFlow		
過剰アクセス試行回数（外部）	0 日	NetFlow	ログイン情報へのアクセス	総当たり攻撃
ネットワークプリンタへの過剰な接続回数	0 日	NetFlow		
地理的に異常なリモートアクセス	30日間	NetFlow	最初のアクセス	外部リモートサービス
ハートビート接続の回数	1 日間	NetFlow	コマンドアンドコントロール	非アプリケーション層プロトコル
広帯域幅での単方向トラフィック	0 日	NetFlow	データ漏洩	自動データ漏洩
インバウンドポートスキャナ	1 日	NetFlow	検出	ネットワークサービスのスキャン
内部接続のスパイク	0 日	NetFlow	検出	ネットワークサービスのスキャン
内部ポートスキャナ	7 日間	NetFlow	検出	ネットワークサービスのスキャン
meterpreter コマンドアンドコントロールの成功	1 日	NetFlow	コマンドアンドコントロール	非アプリケーション層プロトコル
NetBIOS 接続のスパイク	9 日間	NetFlow	ラテラルムーブメント	リモートサービス
ネットワーク利用者数のスパイク	36 日間	NetFlow		
ネットワークプリンタの過剰な接続回数	0 日	NetFlow		
新しい内部デバイス	21 日間	NetFlow		
新しい IP スキャナ	9 日間	NetFlow	検出	ネットワークサービスのスキャン
新しいリモートアクセス	36 日間	NetFlow	最初のアクセス	外部リモートサービス

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

アラート	履歴	テレメトリ	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
新しい SNMP スイープ	9 日間	NetFlow	検出	ネットワークサービスのスキャン
新しい異常な DNS リゾルバ	7 日間	NetFlow、パッシブ DNS		
非サービスポートスキャナ	9 日間	NetFlow	検出	ネットワークサービスのスキャン
アウトバウンド SMB スパイク	0 日	NetFlow	ラテラルムーブメント	リモートサービス
持続的なリモートコントロール接続	7 日間	NetFlow	最初のアクセス	外部リモートサービス
データ漏洩の疑い	0 日	NetFlow	データ漏洩	自動データ漏洩
データベース漏洩の疑い	7 日間	NetFlow	データ漏洩	代替プロトコルによるデータ漏洩
プロトコル違反（地理的）	0 日	NetFlow	コマンドアンドコントロール	アプリケーション層プロトコル
リモートアクセス（地理的）	0 日	NetFlow		
ウォッチリスト通信の繰り返し	0 日	ETA、ファイアウォール、NetFlow、パッシブ DNS	コマンドアンドコントロール	アプリケーション層プロトコル
ロール違反	0 日	NetFlow	永続化	システムプロセスの作成または変更
SMB 接続のスパイク	9 日間	NetFlow	ラテラルムーブメント	リモートサービス
ボットネット インタラクションの疑い	1 日間	ETA、ファイアウォール、NetFlow、パッシブ DNS	コマンドアンドコントロール	アプリケーション層プロトコル

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

アラート	履歴	テレメトリ	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
疑わしい暗号通貨アクティビティ	0 日	ETA、ファイアウォール、NetFlow、パッシブ DNS	影響	リソースのハイジャック
ポート悪用の疑い（外部）	1 日	NetFlow	検出	ネットワークサービスのスキャン
疑わしいリモートアクセスツールのハートビート	0 日	NetFlow、パッシブ DNS	コマンドアンドコントロール	非アプリケーション層プロトコル
疑わしい Zerologon RBC エクスプロイトの試行	0 日	NetFlow、パッシブ DNS	特権昇格	特権昇格のエクスプロイト
疑わしい SMB アクティビティ	14 日間	NetFlow	ラテラルムーブメント	リモートサービス
Talos インテリジェンスウォッチリストのヒット	0 日	ETA、ファイアウォール、NetFlow、パッシブ DNS	コマンドアンドコントロール	アプリケーション層プロトコル
異常な DNS 接続	1 日	NetFlow、パッシブ DNS		
異常な外部サーバー	14 日間	ETA、ファイアウォール、NetFlow、パッシブ DNS	コマンドアンドコントロール	アプリケーション層プロトコル
Worm Propagation	9 日間	NetFlow	ラテラルムーブメント	リモートサービスのエクスプロイト

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

アラートの説明

Secure Network Analytics で生成可能なアラートタイプは次のとおりです。このリストには、公開済みのアラートと未公開のアラートの両方が含まれています。

未公開のアラートとは、Secure Network Analytics がまだ実験段階にあると見なされているために、正式に公開されていないアラートです。デフォルトでは [オフ(Off)] になっています。未公開のアラートも、他のアラートと同様に機能します(たとえば、スヌーズして閉じることができます)。また、アラートの優先順位を変更しても、アラートの公開/未公開には影響しません。ただし、単一ノードの展開では正確に動作しなくなります。

未公開のアラートは次のとおりです(以下のアラートリストではアスタリスク(*)で示されています)。

- NetBIOS 接続のスパイク
- 新しい IP スキャナ
- 新しい SNMP スイープ
- アウトバウンド SMB スパイク
- SMB 接続のスパイク
- 疑わしいリモートアクセスツールのハートビート
- Worm Propagation

アンプ攻撃

説明:このエンティティは、アンプ攻撃への参加を示唆するプロファイルでトラフィックを送信しました。アンプ攻撃は、要求に応じて大量のパケットでサーバーを圧倒しようとします。通常、複数のエンティティが要求に応じてトラフィックを送信できるように、スプーフィングされた IP アドレスが使用されます。アンプ攻撃への参加は、エンティティがボットネットマルウェアに感染し、意図せずにパケットを送信していることを示す可能性があります。

前提条件:このアラートに必要な履歴期間は 0 日間です。

関連した観測:トラフィック増幅の観測

次の手順:アラートとサポート観測でエンティティ情報を参照し、外部エンティティがマルウェアの拡散を担っているかどうかを判断します。外部エンティティが原因の場合は、ファイアウォールルールを更新して、外部エンティティからのトラフィックをブロックし、分散型サービス妨害(DDoS)攻撃である場合は他のエンティティからのトラフィックもブロックします。

アンプ攻撃を送信するエンティティがネットワークの内部にある場合は、ネットワークからそのエンティティを隔離し、DDoS 攻撃の場合は他のエンティティも隔離します。エンティティを調べてマルウェアを削除します。

異常な Windows ワークステーション

説明:Windows ワークステーションが新しい異常な動作プロファイルを使用しました(ホストが BitTorrent を介して多数のエンティティに接続された場合など)。このアラートは、異常なプロファイルの観測を使用しており、マルウェアまたは誤使用の兆候である可能性があります。

前提条件:このアラートには、エンティティの通常のアクティビティレベルを確定できるように、14 日間の履歴が必要です。

関連した観測:異常なプロファイルの観測

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

次の手順：裏付けとなる観測結果を参照して、エンティティの役割を特定し、異常な動作に正当なビジネス上の理由があるかどうかを判断します。たとえば、あるエンティティが他のエンティティに接続するために BitTorrent を使用した場合、そのエンティティがテストエンティティだったか、ファイアウォールルールまたは他のセキュリティテストのテストだった可能性があります。異常な動作に正当な理由がない場合は、エンティティを調べて、エンティティが意図したとおりに機能しているかどうか、およびマルウェアがないかどうかを判断します。

国のセットからの逸脱

説明：このエンティティは、通常通信する国のセットから大きく逸脱しています。このアラートに必要な履歴期間は、36 日間です。

前提条件：このアラートには、エンティティが通信する国の通常のセットを確定できるように、36 日間の履歴が必要です。

関連した観測：国のセットからの逸脱に関する観測

次の手順：裏付けとなる観測内容を参照して、このエンティティが接続を確立したエンティティとその地理位置情報を検索します。該当する接続が確立された理由を特定し、悪意のある動作が原因であれば問題を修正します。必要に応じて国のウォッチリストを更新し、悪意のある動作に関与している国を含めます。

新たなプロファイル

説明：非常に機密性の高いエンティティに、新しいプロファイルに適合するトラフィックがあります。たとえば、FTP 接続の受け入れを開始したエンティティが機密データを漏洩している場合があります。

前提条件：このアラートには、エンティティモデルを確定し、予想されるトラフィックプロファイルを判定できるように、14 日間の履歴が必要です。

関連した観測：新しいプロファイルの観測

次の手順：裏付けとなる観測結果でエンティティの新しいトラフィックプロファイルを参照し、特に以前のプロファイルまたはロールに照らして、それが予期されるものかどうかを確認します。たとえば、エンティティが FTP サーバーからメールサーバーに用途変更された場合、この動作の変化は予期されるものとなります。予期されるものではない場合は、エンティティのトラフィックが変更された理由と、それが悪意のあるトラフィックかどうかを調査します。

Empire コマンドアンドコントロール

説明：Empire PowerShell コマンド アンド コントロール チャネルの一部であると思われる新しい定期接続をエンティティが確立しました。このアラートは、ハートビートの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。このアラートに必要な履歴期間は、1 日間です。

前提条件：このアラートには、エンティティモデルを確定し、予想されるトラフィックプロファイルを判定できるように、1 日間の履歴が必要です。

関連した観測：ハートビートの観測

次の手順：裏付けとなる観測結果でエンティティのトラフィックを確認し、ハートビート接続を確立しているエンティティを特定し、トラフィックが予期されるものか悪意のあるものかを判断します。悪意のあるものである場合は、ネットワーク上の他のエンティティも同様に影響を受けるかどうかを判断します。エンティティを検疫してマルウェアを削除します。ブロックリストとファイアウォールのルールを更新して、コマンド アンド コントロール サーバーのネットワークへのアクセスを拒否します。

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

例外的なドメインコントローラ

説明：このエンティティは、通常の動作から逸脱したドメインコントローラとして識別されます。これは悪用を示唆している可能性があります。たとえば、エンティティが多数のアウトバウンド接続を確立している場合は、データ漏洩、ボットネットマルウェア、または悪意のある DNS 要求リダイレクトの兆候である可能性があります。

前提条件：このアラートには、通常のエンティティトラフィック プロファイルを確定できるように、7 日間の履歴が必要です。

関連した観測：新しい外部サーバーの観測、例外的なドメインコントローラの観測

次の手順：このアラートと裏付けとなる観測結果から、エンティティのトラフィックプロファイルと他のエンティティとの接続を表示して、送信しているトラフィックのタイプを確認し、悪意のあるトラフィックかどうかを判断します。ネットワークからデータが漏洩したかどうかを確認し、漏洩した場合は、データのタイプと、状況を修復する最適な方法を見極めます。

過剰アクセス試行回数（外部）

説明：このエンティティには、外部エンティティからのアクセス試行の失敗が多数あります。たとえば、リモートエンティティが SSH または Telnet を使用して内部サーバーに繰り返しアクセスしようとすると、このアラートがトリガーされます。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：多数のアクセス失敗の観測

次の手順：裏付けとなる観測結果を参照し、この外部エンティティが異常で予期されないものかどうかを確認します。正常で予期されるものである場合は、ユーザーまたはマシンのログイン失敗が続く理由を確認します（ログイン情報が変更されたのに、更新されたログイン情報がユーザーまたはマシンに提供されなかった場合など）。外部エンティティが不明な場合は、ファイアウォールまたはセキュリティグループルールを更新して、リモート制御プロトコルのアクセスを制限します。エンティティに悪意がある可能性がある場合は、ブロックリストとファイアウォールのルールを更新して、このエンティティのネットワークへのアクセスを拒否します。

ネットワークプリンタへの過剰な接続回数

説明：このエンティティからネットワークプリンタへの接続回数が過剰になっています。この動作は、サービス妨害（DoS）攻撃や、ドキュメントの印刷によるデータ漏洩の試みを示唆する可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：ネットワークプリンタへの過剰な接続回数の観測

次の手順：裏付けとなる観測結果を参照し、エンティティがネットワークプリンタと通信している方法を確認します。通信が悪意のあるものである場合は、エンティティを検疫してマルウェアを削除します。プリンタのジョブキューを調べて、実行されているアクションを確認します。プリンタが機密文書を印刷するように指示されている場合は、キューをクリアします。プリンタが機密情報を外部エンティティに送信するように指示されている場合は、プリンタのインターネットアクセスを切断します。必要に応じて、プリンタからマルウェアを削除します。

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

地理的に異常なリモートアクセス

説明：このエンティティに対して、通常はローカルネットワークにアクセスしない国のリモートホストからのアクセスがありました。たとえば、外部ソースからの SSH 接続を受け入れるローカルサーバーで、このアラートがトリガーされます。異常な地理位置からのリモートアクセスは、悪意のあるアクセスの兆候の可能性があります。

前提条件：このアラートには、十分なトラフィック履歴を確保し、地理位置情報に基づいて通常のトラフィックを判別できるように、30 日間の履歴が必要です。

関連した観測：リモートアクセスの観測

次の手順：裏付けとなる観測結果を参照し、エンティティが実行したアクションと、そのアクションを実行した理由を確認します。エンティティが予期されたものである一方で、想定外の国からインターネットにアクセスしている場合は、ファイアウォールの設定を更新してこのトラフィックを許可します。悪意のあるアクセスの場合は、アクションを修正し、ブロックリストとファイアウォールのルールを更新して、エンティティのネットワークへのアクセスを拒否します。

ハートビート接続の回数

説明：このエンティティは、多くのリモートエンティティとの新しい定期接続を確立しています。これは、不正な P2P トラフィックまたはボットネットアクティビティの兆候である可能性があります。

前提条件：このアラートには、トラフィックモデルを確定できるように、1 日間の履歴が必要です。

関連した観測：ハートビートの観測

次の手順：裏付けとなる観測結果を参照し、影響を受けているエンティティがハートビート接続を確立しているエンティティを特定し、それらのエンティティが想定外のものであることを確認します。定期的な接続の目的を把握し、ファイアウォールとブロックリストのルールを更新して、今後のアクセスを防止します。

広帯域幅での単方向トラフィック

説明：このエンティティは、新しいリモートホストに対する大量のデータの送信を開始しました。これは誤使用または不良構成の兆候である可能性があります。たとえば、マルウェアは、脆弱なサービスに大量のデータを送信するよう特定のホストに指示することにより、感染したホストに Web サイトを攻撃させる場合があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：新しい高スループット接続の観測

次の手順：フローの詳細についての裏付けとなる観測結果を参照し、エンティティが大量のトラフィックを送信している理由を特定します。トラフィックが許可されていない場合は、ホスト上のどのソフトウェアが悪意のあるトラフィックの原因であるかを調査します。

インバウンドポートスキャナ

説明：このエンティティは、外部エンティティによってポートスキャンされました。外部エンティティがネットワーク内部のエンティティをスキャンしている場合、パッチが適用されていない脆弱性や、ネットワーク上のエンティティに侵入する他の方法を把握するためにスキャンしている可能性があります。

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

前提条件：このアラートには、エンティティモデルを確定し、通常の動作を判別できるように、1 日間の履歴が必要です。

関連した観測：外部ポートスキャナの観測

次の手順：裏付けとなる観測結果を参照して、内部エンティティをポートスキャンした外部エンティティを特定します。計画されたペネトレーションテストなどの意図された動作の結果か、それとも悪意のあるものかを判断します。意図されたものだった場合は、IP スキャナを更新し、トラフィックを許可するリストルールを有効にします。意図しないものだった場合は、トラフィックをブロックします。必要に応じて、ポートアクセスを含むファイアウォールルールを更新します。

内部接続のスパイク

説明：このエンティティで内部接続が急増しました。これはスキャンアクティビティを示唆しています。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：異常測定値の観測

次の手順：裏付けとなる観測結果を参照して、エンティティが複数の接続を確立している理由を判断します。ペネトレーションテストなどの許可された目的のためにスキャンアクティビティを実行しているのか、それとも悪意のある動作かを判断します。必要に応じて動作を修正します。

内部ポートスキャナ

説明：このエンティティは、ネットワーク内部のエンティティでポートスキャンを開始しました。内部エンティティがネットワーク内部のエンティティをスキャンしている場合、ネットワーク セキュリティ チームによるペネトレーションテストである可能性があります。あるいは、ネットワーク上のエンティティからの悪意のある動作である可能性もあります。

前提条件：このアラートには、エンティティモデルと通常のエンティティの動作を確定できるように、7 日間の履歴が必要です。

関連した観測：ポートスキャナの観測

次の手順：裏付けとなる観測結果を参照して、スキャンアクティビティのタイプを把握します。スキャンアクティビティは、データや感染させようとする他のホストを検索している侵害されたホストに関係していることがよくあります。より多くのコンテキストを取得するには、システムが同じ時期に記録した、当該エンティティに関連した観測結果（ウォッチリスト インタラクションなど）を検索します。この操作により、調査対象の動作についての追加情報が得られる場合があります。

meterpreter コマンドアンドコントロールの成功

説明：このデバイスは、meterpreter コマンド アンド コントロール チャネルの一部であるように見える、新しい定期的な接続を確立しました。このアラートは、ハートビートの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 1 日間です。

関連した観測：ハートビートの観測

次の手順：裏付けとなる観測結果でエンティティのトラフィックを確認し、ハートビート接続を確立しているエンティティを特定し、トラフィックが予期されるものか悪意のあるものかを判断します。悪意のあるものである場合は、ネットワーク上の他のエンティティも同様に影響を受けるかどうかを判断します。エンティティを検疫してマルウェアを削除します。ブロックリストとファイアウォールのルールを更新して、コマンド アンド コントロール サーバーのネットワークへのアクセスを拒否します。

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

NetBIOS 接続のスパイク *

説明：送信元が NetBIOS を使用して多数のホストに接続しようとしました。これはマルウェアまたは悪用の兆候である可能性があります。

前提条件：このアラートには、エンティティのトラフィックモデルを確定し、通常のトラフィック動作を判別できるように、9 日間の履歴が必要です。

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照してホストを特定し、トラフィックフローの詳細を分析します。NetBIOS は一般的に使用されるプロトコルではないため、どの接続スパイクイベントも悪意のあるものである可能性があります。このイベントが検出された場合は、NetBIOS を使用しているアプリケーションはどれか、そのトラフィックは正当なものかどうかを確認します。正当な場合は、このアラートをホストに対してスヌーズにします。

ネットワーク利用者数のスパイク

説明：記録的な数の IP アドレスとの通信がネットワーク上で観測されました。これは送信元アドレスのスプーフィングまたはスキャンアクティビティの発生を示している可能性があります。

前提条件：このアラートには、ネットワーク上で通信しているエンティティの総数のカウントに十分な日数を確保できるように、36 日間の履歴が必要です。

関連した観測：利用者数スパイクの観測

次の手順：アラートに関連した裏付けとなる観測結果を参照し、IP アドレスが正当なエンティティかどうかを判断します。正当なものでない場合は、スプーフィングされたアドレスの送信元を特定し、必要に応じて修正します。

ネットワークプリンタの過剰な接続回数

説明：このプリンタが開始する接続が多すぎます。これはボットネットマルウェア感染といった悪意のある動作の存在を示す可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：過剰な接続が観測されたネットワークプリンタ

次の手順：確立された接続と、プリンタとの接続を確立したエンティティを確認します。裏付けとなる観測結果を参照して、プリンタによって確立された接続のタイプを確認します。接続状況がプリンタへの侵害を示唆する場合は、プリンタを検疫し、オペレーティングシステムの削除と再インストールを検討してください。

新しい内部デバイス

説明：ルックバック期間には表示されていなかった新しいエンティティが、制限されたサブネット範囲に表示されています。

前提条件：このアラートには、ネットワークで通常表示されるエンティティを把握できるように、21 日間の履歴が必要です。このアラートの場合、[サブネット設定（Subnet Configuration）] ページで [新しい内部デバイス（New Internal Device）] を選択する必要もあります。

関連した観測：新しい内部デバイスの観測

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

次の手順：裏付けとなる観測結果を参照して、このエンティティが想定されていたエンティティかどうか、使用中のネットワークにとって新規であるにすぎないのかどうかを判断します。エンティティが予期されていたもので悪意がない場合は、アラートを閉じます。将来の新しいエンティティによって今後もアラートが生成されます。エンティティが疑わしい場合は、ローカルスイッチにアクセスして MAC アドレスを確認します。

新しい IP スキャナ *

説明：このエンティティは、ローカル IP ネットワークのスキャンを開始しました。これは、たとえば攻撃者による偵察を示している可能性があります。

前提条件：このアラートには、エンティティのトラフィックモデルを確定し、通常のトラフィック動作を判別できるように、9 日間の履歴が必要です。

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照し、外部エンティティがネットワークをスキャンしている理由を調査します。ペネトレーションテストなどの意図された動作の結果か、それとも悪意のあるものかを判断します。意図された動作だった場合は、トラフィックを許可するように IP スキャナとファイアウォールルールを更新します。悪意があると考えられる場合は、マシンを所有するエンティティまたはユーザーに関連した観測結果を検索して、スキャンアクティビティの原因となったソフトウェアを特定します。

新しいリモートアクセス

説明：このエンティティは、最近の履歴の中で初めてリモートホストから（SSH 経由などで）アクセスされました。このリモートアクセスは、特にエンティティが外部エンティティからの接続を受け入れることが想定されていない場合に、悪意のある動作を示している可能性があります。

前提条件：このアラートには、十分なトラフィック履歴を確保するとともに、エンティティモデルを確定できるように、36 日間の履歴が必要です。

関連した観測：リモートアクセスの観測

次の手順：裏付けとなる観測結果を参照して、外部のエンティティがこのエンティティにアクセスしている理由と、それが正当な形式のアクセスであるかどうかを判断します。また、この外部エンティティからのアクセスか別の外部エンティティからのアクセスかを問わず、このアクセスの前に送信元エンティティへの複数のアクセス試行があったかどうかを（観測結果に基づいて）確認します。この情報に基づいて、ファイアウォールとブロックリストのルールを更新します。

新しい SNMP スイープ *

説明：このエンティティは、SNMP を使用して多数のホストへの到達を試みました。これは、悪意のあるソフトウェアによるネットワーク偵察が原因であることを示している可能性があります。悪意のある攻撃者が SNMP スイープを実行すると、ネットワークに関する情報が収集されたり、悪意のあるエンティティ設定が更新されたりする可能性があります。

前提条件：このアラートには、エンティティのトラフィックモデルを確定し、通常のトラフィック動作を判別できるように、9 日間の履歴が必要です。

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照して、エンティティが SNMP を介してネットワークエンティティを追跡するように意図されているかどうか、およびこの動作に悪意があるかどうかを判断します。このアクティビティが計画されたペネトレーションテストまたは意図された動作の一部ではない

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

場合は、エンティティを検疫し問題を修正します。更新された設定や侵害を受けたセキュリティ設定など、いずれかのエンティティが影響を受けているかどうかを判断し、問題を修正します。エンティティが SNMP スイープを実行することが予期されている場合は、エンティティをスキャナホワイトリストに追加します。

新しい異常な DNS リゾルバ

説明：このエンティティは、通常は使用しない DNS リゾルバに接続しました。これは不良構成またはマルウェアの存在を示している可能性があります。たとえば、攻撃者は DNS リゾルバを使用して、人気のある Web サイトから追加のマルウェアを提供するドメインへのリダイレクトを発生させる場合があります。

前提条件：このアラートには、エンティティロールを確定し、通常のトラフィックをモデル化できるように、7 日間の履歴が必要です。

関連した観測：異常な DNS リゾルバの観測

次の手順：エンティティの設定を確認し、適切な DNS 設定が行われていることを確かめます。設定が適切な場合は、DNS ルックアップを実行しているソフトウェアを特定します。トラフィックに悪意があると見なされる場合は、外部 IP アドレスをブロックします。

非サービスポートスキャナ

説明：このデバイスは、通常のサービスに関連付けられていないポートでローカルネットワークのスキャンを開始しました。このアラートは IP スキャナの観測結果を使用しており、攻撃者がネットワーク内に存在し、脆弱性をスキャンしていることを示す可能性があります。

前提条件：このアラートには、エンティティロールを確定し、通常のトラフィックをモデル化できるように、9 日間の履歴が必要です

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照し、外部エンティティがネットワークをスキャンしている理由を調査します。ペネトレーションテストなどの意図された動作の結果か、それとも悪意のあるものかを判断します。意図された動作だった場合は、トラフィックを許可するように IP スキャナとファイアウォールルールを更新します。悪意があると考えられる場合は、マシンを所有するエンティティまたはユーザーに関連した観測結果を検索して、スキャンアクティビティの原因となったソフトウェアを特定します。

アウトバウンド SMB スパイク＊

説明：このエンティティは、SMB ポートを使用して多数の外部ホストと通信しています。これは、感染が疑われるホスト、外部で開始された悪用（スプーフィング攻撃など）、または内部で開始されたポートスキャンを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照し、送信元エンティティがトラフィックを送信しているエンティティ、トラフィックのタイプを特定し、エンティティのロールまたは責任の更新なのか、それとも意図されていないものなのかを判断します。意図されていないものだった場合は、問題を修正します。ファイアウォールとブロックリストのルールを更新して、このアクセスを防止します。

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

持続的なリモートコントロール接続

説明：このエンティティは、リモートデスクトップや SSH などのリモート制御プロトコルを使用して、新しいホストから持続的な接続を受信しています。これは、ファイアウォールルールまたは ACL が過度に許容的になっていることを示す可能性があります。

前提条件：このアラートには、トラフィックモデルを確定し、通常のトラフィック動作を判別できるように、7 日間の履歴が必要です。

関連した観測：新しい外部サーバーの観測、持続的な外部サーバーの観測

次の手順：ファイアウォールまたはセキュリティグループのルールを調整して、エンティティへの悪意のあるアクセス試行が繰り返されることを防止します。リモートアクセスの観測結果やエンティティをチェックして、ローカルエンティティが侵害されていないことを確認します。

データ漏洩の疑い

説明：このエンティティは、定期的に通信していない内部エンティティから大量のデータをダウンロードしました。その後まもなく、エンティティは外部エンティティにほぼ同じ量のデータをアップロードしました。これは、情報の不正な転送などの悪意のある動作を示唆する可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：データ転送の可能性の観測

次の手順：裏付けとなる観測結果を参照して、トラフィックの量とクライアントエンティティを特定し、新たにスケジュールされたバックアップのように、この動作が通常のビジネスの過程で予期されるものなのかどうかを判断します。悪意のある動作だった場合は、何が転送されたかを特定します。データ漏洩に関する組織のガイドラインに従ってください。

データベース漏洩の疑い

説明：統計的に異常な量のデータがデータベースサーバーからクライアントに転送されました。これは、情報の不正な転送などの悪意のある動作を示唆する可能性があります。

前提条件：このアラートには、通常はデータベースとして機能するエンティティと、通常のトラフィックプロファイルを確定できるように、7 日間の履歴が必要です。

関連した観測：新しい高スループット接続の観測

次の手順：クライアントエンティティを調べて、新たにスケジュールされたバックアップのように、この動作が通常のビジネスの過程で予期されるものなのかどうかを判断します。悪意のある動作だった場合は、何が転送されたかを特定します。データ漏洩に関する組織のガイドラインに従ってください。

プロトコル違反（地理的）

説明：このエンティティは、不正なプロトコル/ポートの組み合わせ（ポート 22 での UDP など）でウォッチリストに登録された国のホストとの通信を試みました。

前提条件：このアラートに必要な履歴期間は 0 日間です。少なくとも 1 つの国を含む国のウォッチリストを設定する必要があります。

関連した観測：不正なプロトコルの観測

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

次の手順：裏付けとなる観測結果を参照し、このエンティティが異常なプロトコル/ポートの組み合わせを使用してウォッチリストに登録された国のエンティティと通信した理由を特定します。通信で転送されたものを特定します。悪意があると判断された場合は、ファイアウォールとブロックリストのルールを更新して、このプロトコル/ポートの組み合わせ、およびこの地理位置情報を使用した今後のアクセスを（許可すべきビジネス上の理由がない限り）防止します。

API を使用してウォッチリストを設定する方法

現在、Manager にウォッチリストまたはブロックリストを設定する機能はありません。そのため、以下で説明するように、バックエンド（オンサイト）に対して API コールを実行する必要があります。たとえば、ある国（「CN」：この例では中国）のウォッチリストを設定するには、マネージャで次のコールを実行して、その国をウォッチリストに追加します。

> 次の両方のコマンドでは、最初の行に続く各行の最初の文字が、直前行の最終文字の直後に続きます。

ここから API キーを取得するには、次の手順を実行します。

`cat /lancope/var/services/detections/config/api_key`（**次のコマンドに渡すキーをメモします**）。

1. 次のコマンドを入力します。

```
curl -X POST -d '{"identifier":"US", "list_on":"watchlist"}' -v
-H 'Content-Type:application/json' -H 'Authorization:ApiKey _
customer_01-api[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

2. 次のコマンドを入力して確認します。

```
curl -X GET -v -H 'Content-Type:application/json' -H
'Authorization:ApiKey _customer_01-api:[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

リモートアクセス（地理的）

説明：このデバイスは、ユーザーが指定したウォッチリストの国のリモートホストからアクセスされました。このアラートは、リモートアクセスの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには、少なくとも 1 つの国を含む国のウォッチリストを設定することが必要です。

関連した観測：リモートアクセスの観測

次の手順：裏付けとなる観測結果を参照して、外部エンティティを特定し、外部エンティティが内部エンティティと対話した方法を確認します。動作が悪意のあるものかどうか、データが漏洩したかどうか、および内部エンティティでどのようなアクションが実行されたかを確認します。必要に応じて、ファイアウォールまたはセキュリティグループルールを追加し、今後のアクセスを防止します。

API を使用してウォッチリストを設定する方法

現在、Manager にウォッチリストまたはブロックリストを設定する機能はありません。そのため、以下で説明するように、バックエンド（オンサイト）に対して API コールを実行する必要があります。たとえ

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

ば、ある国(「CN」:この例では中国)のウォッチリストを設定するには、マネージャで次のコールを実行して、その国をウォッチリストに追加します。

> 次の両方のコマンドでは、最初の行に続く各行の最初の文字が、直前行の最終文字の直後に続きます。

ここから API キーを取得するには、次の手順を実行します。

```
cat /lancope/var/services/detections/config/api_key
```
(次のコマンドに渡すキーをメモします)。

1. 次のコマンドを入力します。

```
curl -X POST -d '{"identifier":"US", "list_on":"watchlist"}' -v
-H 'Content-Type:application/json' -H 'Authorization:ApiKey _
customer_01-api[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

2. 次のコマンドを入力して確認します。

```
curl -X GET -v -H 'Content-Type:application/json' -H
'Authorization:ApiKey _customer_01-api:[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

ウォッチリスト通信の繰り返し

説明:このエンティティは、ウォッチリストに登録された IP との定期的な接続を確立しました。これは、ネットワークにマルウェアや侵害されたエンティティが存在することを示している可能性があります。

前提条件:このアラートに必要な履歴期間は 0 日間です。

関連した観測:ウォッチリスト インタラクションの観測およびハートビートの観測

次の手順:裏付けとなる観測結果を参照して、影響を受けるエンティティとログ情報を調べます。エンティティが定期的な通信を確立している理由を特定し、状況を修復します。必要に応じて、状況を修復するためのアドバイスを得るため、またはエンティティが現在はマルウェアに感染していないことを確認するために、特定のウォッチリストを管理している組織に連絡してください。

ロール違反

説明:このエンティティは、特定のロール(ユーザーエンティティなど)で識別されますが、ロールの通常の動作とは異なる動作をしていることが確認されました(SSH サーバーなど)。エンティティがロールを変更した場合、マルウェアがエンティティの機能を変更するなど、悪意のある動作を示唆している可能性があります。

前提条件:このアラートに必要な履歴期間は 0 日間です。

関連した観測:ロール違反の観測

次の手順:裏付けとなる観測結果を参照し、新しいロールの動作が意図されたもので、通常のビジネスの過程に含まれるかどうかを判断します。そうでない場合は、エンティティを検疫します。意図されたものである場合は、アラートをスヌーズにします。

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

SMB 接続のスパイク＊

説明：このエンティティは、非常に多くの SMB サーバーへの接続を試みました。これはマルウェアまたは悪用の兆候である可能性があります。SMB は主にファイル共有に使用されますが、ネットワークプリンタへのアクセスや、ネットワーク上の他のホストを参照する目的にも使用できるため、この状況はデータ漏洩やネットワークリソースの不正使用の存在を示唆している可能性があります。

前提条件：このアラートには、エンティティのトラフィックモデルを確定し、通常のトラフィック動作を判別できるように、9 日間の履歴が必要です。

関連した観測：IP スキャナの観測

次の手順：裏付けとなる観測結果を参照して、エンティティが複数の SMB サーバーとの接続を確立している理由、エンティティが実行しているアクションのタイプを確定し、悪意のある動作かどうかを判断します。データが漏洩した場合は、データ漏洩に対処するための組織のガイドラインに従ってください。必要に応じて、エンティティを検疫しマルウェアを削除します。

ボットネット インタラクションの疑い

説明：このエンティティは、ボットネットに関連付けられた IP アドレスとトラフィックを交換したか、ボットネットに関連付けられたドメイン名を解決しようとしました。

前提条件：このアラートには、エンティティモデルを確定できるように、1 日間の履歴が必要です。

関連した観測：ウォッチリスト インタラクションの観測

次の手順：エンティティを検疫して、すべてのマルウェアを削除します。ブロックリストとファイアウォールのルールを更新して、ボットネットエンティティがネットワークにアクセスできないようにします。裏付けとなる観測結果を参照して、ネットワーク上の他のエンティティも感染しているかどうかを確認します。この確認はエンティティが確立した可能性のある通信に基づいて実行し、必要に応じて修復します。

疑わしい暗号通貨アクティビティ

説明：送信元は、Talos インテリジェンスに基づいて、暗号通貨ノードを運用していることで知られる複数のアドレスや他の送信元と大量のトラフィックを交換しました。この動作は、エンティティが暗号通貨のマイニングに使用されていることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：ウォッチリスト インタラクションの観測

次の手順：エンティティを検疫し、マルウェアかユーザーがインストールしたものかにかかわらず、すべての暗号通貨マイニングソフトウェアを削除します。

ポート悪用の疑い（外部）

説明：このエンティティは、通常とは異なる範囲のポートで外部ホストと通信しています。これは、外部で開始された悪用（スプーフィング攻撃など）または内部で開始されたポートスキャンを示している可能性があります。

前提条件：このアラートには、エンティティモデルを確定できるように、1 日間の履歴が必要です。

関連した観測：ポートスキャナの観測、外部ポートスキャナの観測

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

次の手順：裏付けとなる観測結果を参照して、エンティティのアクティビティを確認し、計画されたペネトレーションテストと一致しているかどうか、あるいは悪意のある動作かを判断します。悪意のある動作の原因を特定し、問題を修正します。必要に応じて、ファイアウォールとブロックリストのルールを更新します。

疑わしいリモートアクセスツールのハートビート *

説明：リモートアクセスツール（RevengeRAT など）に一致する署名を持つトラフィックがこのデバイスで確認されました。このアラートは、疑わしいネットワークアクティビティの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：疑わしいネットワークアクティビティの観測

次の手順：このデバイスに最新のセキュリティ更新が適用されていることを確認し、侵害の兆候がないか調べます。

疑わしい Zerologon RBC エクスプロイトの試行

説明：Zerologon RPC エクスプロイトと一致する署名を持つトラフィックがこのデバイスで確認されました。このアラートは、疑わしいネットワークアクティビティの観測結果を使用しており、デバイスがエクスプロイトの対象になっていることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：疑わしいネットワークアクティビティの観測

次の手順：このデバイスに最新のセキュリティ更新が適用されていることを確認します。CVE-2020-1472 を参照して、軽減手順を実行します。

疑わしい SMB アクティビティ

説明：複数の新しい SMB サーバーが一般的な SMB ピアと通信しました。これはマルウェアまたは悪用の兆候である可能性があります。

前提条件：このアラートに必要な履歴期間は 14 日間です。

関連した観測：疑わしい SMB アクティビティの観測

次の手順：裏付けとなる観測結果を参照して、エンティティのトラフィックプロファイルを調べ、ボットネットアクティビティや他の悪意のある動作のさらなる証拠があるかどうかを判断します。同様の動作を示している可能性があるネットワーク上の他のエンティティを確認し、修正します。

Talos インテリジェンス ウォッチリストのヒット

説明：このエンティティは、Cisco Talos IP ブロックリスト記載の複数のアドレスと大量のトラフィックを交換しました。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連した観測：ウォッチリスト インタラクションの観測

次の手順：エンティティを検疫して、すべてのマルウェアを削除します。メニューから [Talosインテリジェンス（Talos Intelligence）] を選択して外部 IP アドレスを調査し、トラフィックが示唆する事柄を確認して、適切な修復アクションを実行します。

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

異常な DNS 接続

説明：このエンティティは、異常な DNS リゾルバに接続し、リモートエンティティとの定期的な接続を確立しました。この動作は、トラフィックの悪意のあるリダイレクト、またはエンティティのマルウェア感染を示している可能性があります。

前提条件：このアラートには、エンティティモデルを確定できるように、1 日間の履歴が必要です。

関連した観測：異常な DNS リゾルバの観測とハートビートの観測

次の手順：裏付けとなる観測結果を参照して、この動作が悪意のあるものかどうかを判断し、マルウェアが存在する場合は削除します。ブロックリストとファイアウォールのルールを更新して、アクセスを拒否します。

異常な外部サーバー

説明：このエンティティは、疑わしいトラフィックプロファイルを持つ新しい外部サーバーと繰り返し通信しています。これは、たとえば syslog や TeamViewer などの外部エンティティに対するサーバーとして機能している新しいソフトウェアの存在を示している可能性があります。

前提条件：このアラートには、通常のトラフィックパターンを確定し、予想される外部エンティティトラフィックを判別できるように、14 日間の履歴が必要です。

関連した観測：新しい外部サーバーの観測、持続的な外部サーバーの観測、ウォッチリストルックアップの観測、ウォッチリスト インタラクションの観測

次の手順：裏付けとなる観測結果を参照して、エンティティのトラフィックプロファイルを調べ、トラフィックの性質とトラフィックが許可されているかどうかを判断します。エンティティを検疫し、問題のあるソフトウェアを削除します。ネットワーク上の他のエンティティが同様の動作を示すかどうかを確認し、その動作を修正します。

ワームの伝播 *

説明：以前スキャンされたデバイスがローカル IP ネットワークのスキャンを開始しました。このアラートは、ワーム伝達の監視を使用しており、ワームがネットワーク内でそれ自体を伝達していることを示している可能性があります。

前提条件：このアラートに必要な履歴期間は 9 日間です。

関連した観測：ワームの伝播の観測

次の手順：裏付けとなる観測結果を参照し、内部エンティティがネットワークをスキャンしている理由を調査します。ペネトレーションテストなどの意図された動作の結果か、それとも悪意のある動作なのかを判断します。意図された動作だった場合は、トラフィックを許可するように IP スキャナとファイアウォールルールを更新します。悪意があると考えられる場合は、マシンを所有するエンティティまたはユーザーに関連した観測結果を検索して、スキャンアクティビティの原因となったソフトウェアを特定します。

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

観測の説明

Secure Network Analytics が生成可能な観測のタイプを次に示します。

異常なプロファイルの観測

説明：1 つまたは複数のエンティティが初めてプロファイルを使用しましたが、ネットワークで見られる一般的な動作とは異なる動作でした（異常に多くのエンティティが初めてそのプロファイルを使用して異常なトラフィックを送信した場合など）。

前提条件：なし。

関連したアラート：異常な Windows ワークステーションアラート

不正なプロトコルの観測

説明：エンティティが標準ポートで非標準プロトコルを使用しました（ポート 22 で UDP を使用するなど）。

前提条件：なし。

関連したアラート：プロトコル違反（地理的）アラート

国のセットからの逸脱の観測

説明：1 つのエンティティが、通常とは異なる一連の国々と通信しました。

前提条件：なし。

関連したアラート：国のセットからの逸脱アラート

例外的なドメインコントローラの観測

説明：ドメイン コントローラ エンティティが、通常とは異なる外部ポートと通信しました。

前提条件：なし。

関連したアラート：例外的なドメイン コントローラ アラート

ネットワークプリンタへの過剰な接続回数の観測

説明：1 つのエンティティがネットワークプリンタへの接続を過剰な回数開始しました。

前提条件：なし。

関連したアラート：ネットワークプリンタへの過剰な接続回数アラート

外部ポートスキャナの観測

説明：ローカルネットワーク上の 1 つのエンティティがリモート IP アドレスをスキャンしました（またはリモート IP アドレスによりスキャンされました）。

前提条件：なし。

関連したアラート：インバウンド ポート スキャナ アラート、ポート悪用の疑い（外部）アラート

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

ハートビートの観測

説明：1 つのエンティティがリモートホストとのハートビートを維持しました。

前提条件：なし。

関連したアラート：Empire コマンド アンド コントロール アラート、ハートビート接続回数アラート、異常な DNS 接続アラート、meterpreter コマンドアンドコントロールの成功

内部ポートスキャナの観測

説明：1 つのエンティティが多数のポートをスキャンしました。

前提条件：なし。

IP スキャナの観測

説明：1 つのエンティティが多数のエンティティをスキャンしました。

前提条件：なし。

関連したアラート：NetBIOS 接続のスパイクアラート、新しい IP スキャナアラート、新しい SNMP スイープアラート、アウトバウンド SMB スパイクアラート、SMB 接続のスパイクアラート

多数のアクセス失敗の観測

説明：1 つのエンティティがアプリケーション（FTP、SSH、RDP など）へのアクセス試行に何度も失敗しました。

前提条件：なし。

関連したアラート：過剰アクセス試行回数（外部）アラート

ネットワークプリンタの過剰な接続回数の観測

説明：ネットワークプリンタが他のエンティティへの接続を過剰な回数開始しました。

前提条件：なし。

関連したアラート：ネットワークプリンタの過剰な接続回数アラート

新しい外部サーバーの観測

説明：1 つのエンティティが外部サーバーとの通信を開始しました。

前提条件：なし。

関連したアラート：例外的なドメイン コントローラ アラート、持続的なリモートコントロール接続アラート、異常な外部サーバーアラート

新しい高スループット接続の観測

説明：1 つのエンティティが新しいホストと大量のトラフィックを交換しました。

前提条件：なし。

関連したアラート：広帯域幅での単方向トラフィックアラート、データベース漏洩の疑いアラート

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

新しい内部デバイスの観測

説明：ルックバック期間には表示されていなかった新しいエンティティが、ネットワーク上に表示されています。

前提条件：なし。

関連したアラート：新しい内部デバイスアラート

新しいプロファイルの観測

説明：1 つのエンティティが、最近まで一致していなかったプロファイルタグ（FTP サーバーなど）と一致しています。

前提条件：なし。

関連したアラート：新たなプロファイルアラート

持続的な外部サーバーの観測

説明：このエンティティは、同じ外部サーバー（FTP、SSH など）と定期的に通信しています。

前提条件：なし。

関連したアラート：持続的なリモートコントロール接続アラート、異常な外部サーバーアラート

利用者数スパイクの観測

説明：記録的な数の IP アドレスとの通信がローカルネットワーク上で観測されました。

前提条件：なし。

関連したアラート：ネットワーク利用者数のスパイクアラート

ポートスキャナの観測

説明：1 つのエンティティが多数のポートをスキャンしました。

前提条件：なし。

関連したアラート：内部ポートスキャナアラート

データ転送の可能性の観測

説明：内部データソースからこのエンティティへの転送（「ダウンロード」）と、その後実行されたこのエンティティから外部データシンクへの転送（「アップロード」）で、ほぼ同じサイズのタイミングの近いデータ転送が検出されました。

前提条件：なし。

関連したアラート：データ漏洩の疑いアラート

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

異常測定値の観測

説明：1 つのエンティティが記録的な量のトラフィックを送信または受信しました。

前提条件：なし。

関連したアラート：内部接続のスパイクアラート、アウトバウンドトラフィックのスパイクアラート

リモートアクセスの観測

説明：1 つのエンティティがリモートソースからアクセスされました。

前提条件：なし。

関連したアラート：地理的に異常なリモートアクセスアラート、新しいリモートアクセスアラート、リモートアクセス（地理的）アラート

ロール違反の観測

説明：1 つのエンティティに、そのロールに適合しない新しいトラフィックがあります（ポート 80 で通信する FTP サーバーなど）。

前提条件：なし。

関連したアラート：ロール違反アラート

疑わしいネットワークアクティビティの観測

説明：Talos シグネチャに一致する疑わしいアクティビティが検出されました。

前提条件：なし。

関連したアラート：疑わしいリモートアクセスツールのハートビート

疑わしい SMB アクティビティの観測

説明：複数のエンティティが SMB プロトコルを使用して初めて異常なアクティビティを実行しました。

前提条件：なし。

関連したアラート：疑わしい SMB アクティビティアラート

トラフィック増幅の観測

説明：1 つのエンティティのアウトバウンドトラフィックとインバウンドトラフィックが、使用していたプロファイルに関連付けられている一般的な比率と一致しませんでした。これはアンプ攻撃への参加を示している可能性があります。アンプ攻撃は、要求に応じて大量のパケットでサーバーを圧倒するもので、スプーフィングされた IP アドレスや他の識別情報が関係しています。また、アンプ攻撃への参加は、エンティティがボットネットマルウェアに感染し、意図せずにパケットを送信していることを示す可能性もあります。

前提条件：なし。

関連したアラート：アンプ攻撃アラート

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

異常な DNS リゾルバの観測

説明：1 つのエンティティが異常な DNS リゾルバと通信しました。

前提条件：なし。

関連したアラート：新しい異常な DNS リゾルバアラート、異常な DNS 接続アラート

ウォッチリスト インタラクションの観測

説明：1 つのエンティティが、ウォッチリストに記載されている IP アドレスと（明示的に、またはドメイン名を介して暗黙的に）通信しました。

前提条件：なし。

関連したアラート：ウォッチリスト通信の繰り返しアラート、ボットネット インタラクションの疑いアラート、疑わしい暗号通貨アクティビティアラート、Talos インテリジェンス ウォッチリストのヒットアラート、異常な外部サーバーアラート、ユーザー ウォッチリスト ヒット アラート、ウォッチリスト ヒット アラート

ワームの伝播

説明：以前スキャンされたデバイスがローカル IP ネットワークのスキャンを開始しました。

前提条件：なし

関連したアラート：ワームの伝播

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

[アラート(Alerts)] ダッシュボード

[アラート(Alerts)] ダッシュボードには、フィルタ設定に従ってシステムで生成されたアラートが表示されます。システムは、次のようなネットワークに関するさまざまな情報の分析に基づいて、潜在的な悪意のあるアクティビティを示すアラートを生成します。

- モニター対象のエンティティのロールと、それらのエンティティについてログに記録された観測内容
- アラートタイプの優先順位
- IP スキャナのルール

> [ホストグループ管理(Host Group Management)] を使用して、既知の有効な IP スキャナをデフォルトのネットワーク スキャナ グループ(ホストグループ ID:48)に追加します。追加するスキャナは、単一のカンマ区切りの IP または CIDR 表記で一覧表示する必要があります。既知のスキャナを追加することで、それらのスキャナが外部ホストや内部ホストをスキャンする際にアラートが発生するのを防止できます。

[アラート(Alerts)] ダッシュボードを開く

メインメニューから、[モニター(Monitor)] > [アラート(Alerts)] の順に選択します。

または

[アラートの詳細(Alert Details)] ページの [裏付けとなる観測内容(Supporting Observations)] セクションで、目的のデバイスのドロップダウンリストから [アラート(Alerts)] を選択します。

[アラート(Alerts)] ダッシュボードが開き、そのデバイスに関連するすべてのアラートのリストが表示されます。

[アラート(Alerts)] ダッシュボードの概要

> このページの使用方法の詳細については、「**アラートの調査**」を参照してください。

アラートテーブルのフィルタ処理

さまざまな設定のフィルタ処理方法については、次の情報を参照してください。ページの左上隅にある [フィルタ(Filters)] フィールドで、▶(右向き三角形)アイコンをクリックして、[検索(Search)] フィールドと [時間範囲(Time Range)] フィールドを表示します。

検索(Search) [検索(Search)] フィールドに、テーブルをフィルタ処理するエントリを入力します。アラートタイプ、ソースタイプ、時間など、いずれかのテーブルの列に表示される可能性のあるコンテンツでフィルタ処理できます。終了したら、[時間範囲(Time Range)] フィールドの右側にある [適用(Apply)] をクリックします。

時間範囲(Time Range) 日付と時間でフィルタ処理するには、[日付の選択(Select Date)] ドロップダウン矢印をクリックします。左の列にあるエントリから選択するか、カスタムエントリを設定できます。[開始日時(From Date/Time)] カレンダーと [終了日時(To Date/Time)] カレンダーの両方で同じ日付をクリックしたり、別の日付を選択したりできます。スクロールリストを使用して時刻を指定します。終了したら、ダイアログの右下隅にある [範囲の選択(Select range)] をクリックし、[時間範囲(Time Range)] フィールドの右側にある [適用(Apply)] をクリックします。保存せずに終了するには、ページ上でカレンダーの外側にある空白部分をクリックします。

ステータス別にアラートを設定する(Set alerts by status) このフィールドで目的のオプションをクリックし、すべてのアラートを表示するか、[オープン(Open)]、[スヌーズ(Snoozed)]、[未公開

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

(Unpublished)]、または [クローズド(Closed)] アラートのみを表示するかを選択できます。デフォルトでは、[すべて(All)] ステータスが割り当てられているアラートがテーブルに表示されます。

- スヌーズされたアラート:アラートを閉じるときに(「**アラートテーブルエントリの編集**」を参照)、[アラートを閉じる(Close Alert)] ダイアログが開きます。このダイアログで、アラートを一定期間スヌーズするかどうかを指定できます。
- 未公開のアラートとは、Secure Network Analytics がまだ実験段階にあると見なされているために、正式に公開されていないアラートです。デフォルトでは [オフ(Off)] になっています。未公開のアラートも、他のアラートと同様に機能します(たとえば、スヌーズして閉じることができます)。また、アラートの優先順位を変更しても、アラートの公開/未公開には影響しません。ただし、単一ノードの展開では正確に動作しなくなります。

  未公開のアラートを識別するには、「**アラートの説明**」を参照してください。

アラートテーブルの表示

アラートテーブルに次の情報が表示されます。

フィールド	説明
アラート(Alert)	生成されたアラートタイプ。 • アラートの説明を表示するには、説明にカーソルを合わせます。 • アラートの [アラートの詳細(Alert Details)] ページにアクセスするには、アラートをクリックします。[アラートの詳細(Alert Details)] ページについては、「**アラートの詳細**」を参照してください。 [フィルタ(Filter)] ドロップダウンリストを使用して、特定のアラートタイプでフィルタ処理します。
送信元(Source)	アラートを生成したソースエンティティ。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス(ネットワーク)(Device (Network))] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス(Device)] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート(Alerts)] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート(Alerts)] ダッシュボードにアクセスします。 [アラート(Alerts)] ダッシュボードの詳細については、「**[アラート(Alerts)] ダッシュボード**」を参照してください。 • [観測(Observations)] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測(Observations by Device)] ページにアクセスします。 [デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。

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

	• [フロー分析(Flow Analysis)] を選択して、送信元に関連するフロー情報を含む [フロー検索結果(Flow Search Results)] ページにアクセスします。 [フロー検索結果(Flow Search Results)] ページの詳細については、「**フロー検索結果:概要**」を参照してください。
時刻(Time)	アラートが最後に更新された時刻。
タグ(Tags)	タグは、アラートに追加する任意のタイプのラベルまたはテキストであり、ラベルまたはテキストでアラートをフィルタ処理できるようになります。 [タグ(Tags)] ドロップダウンリストを使用して、特定のタグでフィルタ処理します。
担当者(Assignee)	アラートに割り当てられたユーザー。 [担当者(Assignee)] ドロップダウンリストを使用して、[任意の担当者(Any Assignee)] または [担当者なし(No Assignee)] でフィルタ処理します。

アラートテーブルエントリの編集

[アクション(Actions)] フィールド(アラートテーブルのすぐ上)のドロップダウンリストを使用して、特定のアラートにタグとユーザーを割り当てたり、アラートのステータスを変更したりできます。

1. [アラート(Alerts)] テーブルで、1 つ以上の変更を行う各アラートの横にあるチェックボックスをオンにします。複数のアラートをオンにした場合、行った変更は選択したすべてのアラートに均一に適用されます。
2. [アクション(Actions)] フィールドで、次のいずれかのドロップダウンリストから一度に 1 つずつ選択します。
   - タグの割り当て(Assign Tag)
   - ステータスの変更(Change Status)

   > 現在、[ユーザーの割り当て(Assign User)] ドロップダウンリストは無効になっています。

   ステータスは、[オープン(Open)]、[クローズ(Close)]、または [スヌーズ解除(Unsnooze)] に変更できます。アラートを閉じるときに、[アラートを閉じる(Close Alert)] ダイアログが開きます。このダイアログで、アラートを一定期間スヌーズするかどうかを指定できます。アラートをスヌーズした後で開き直す場合は、そのアラートの [スヌーズ解除(Unsnooze)] オプションを選択します。

   特定のドロップダウンリストから一度に複数のオプションを選択するには、Shift キーを押しながら各オプションをクリックします。選択解除するには、もう一度クリックします。
3. オプションを保存するには、ページ上でドロップダウンリストの外側にある空白部分をクリックします。

   テーブル内の該当するエントリが、選択内容を反映して変更されます。

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

関連する設定ページの表示

ページの右上隅にある Related Config Links ([関連する設定リンク(Related Config Links)]) アイコンをクリックし、適切なオプションをクリックして、[アラートの優先順位設定(Alert Priorities Configuration)] ページまたは [アラートの国のウォッチリスト設定(Alerts Country Watchlist Configuration)] ページにアクセスします。

.CSV ファイルのダウンロード

利用可能なすべての観測値または現在フィルタ済みのビュー(テーブルがすでにフィルタ処理されている場合)のみのいずれかを含む .csv ファイルをダウンロードするには、ページの右上隅にある CSV ([CSVのダウンロード(Download CSV)]) アイコン をクリックし、適切なオプションをクリックします。

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによって生成されるアラートのデフォルトステータスは [オープン(Open)] になります。当面注意が必要となるため、[アラートの詳細(Alert Details)] ページにすべてのオープンアラートがデフォルトで表示されます。

[アラート(Alerts)] ダッシュボードを確認する際は、初期トリアージとしてステータスを更新できます。フィルタ機能と検索機能を使用して特定のアラートを検索したり、さまざまなステータスのアラートまたはさまざまなタグや担当者のアラートを表示したりできます。

> アラートを閉じるときに、アラートのステータスを [スヌーズ(Snoozed)] に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。また、アラートから [スヌーズ(Snoozed)] ステータスを削除して、再びオープンアラートとして表示されるようにできます。

アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

[アラート(Alerts)] ページでアラートをクリックすると、アラートの詳細を確認できます。このページで、アラートに関連付けられたデバイスをクリックできます。

この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。Manager 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートに残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを [クローズ(Closed)] に更新できるため、デフォルトでオープンアラートとして表示されなくなります。

アラートに関するよくある質問

特定のアラートが無効になっている理由は何ですか。

最も広範な顧客に影響を与える可能性が高いアラートのみが有効になっているため、特定のアラートはデフォルトで無効になっています。ユーザーは、ネットワークのニーズ(特に展開の微調整など)に応じてアラートを有効にできます。

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

アラートのステータスにはどんな意味がありますか。

アラートのワークフローは、そのステータスに基づいて異なります。システムによって生成されるアラートのデフォルトステータスは [オープン(Open)] であり、ユーザーは割り当てられません。当面注意が必要となるため、[アラート(Alerts)] ページにすべてのオープンアラートがデフォルトで表示されます。

[アラート(Alerts)] ダッシュボードを確認する際は、初期トリアージとしてアラートにステータスを割り当て、タグ付けし、ステータスを更新できます。フィルタ機能と検索機能を使用して特定のアラートを検索したり、さまざまなステータスのアラートまたはさまざまなタグや担当者のアラートを表示したりできます。アラートを閉じるときに、アラートのステータスを [スヌーズ(Snoozed)] に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ(Snoozed)] ステータスを削除し、再びオープンアラートとして表示することもできます。

分析が完了したら、ステータスを [クローズ(Closed)] に更新できるため、デフォルトでオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

サブネットの機密性はアラートにどのように影響しますか。

現在、この機能が適用されるのは次の Secure Network Analytics サブネットのみです。

- 10.0.0.0/8(デフォルト RFC1918)
- 172.16.0.0/12(デフォルト RFC1918)
- 192.168.0.0/16(デフォルト RFC1918)
- fc00::/7(デフォルト RFC4193)

デフォルトでは、これらのサブネットの機密性タイプは中(Medium)です。

サブネットの機密性とアラートの優先順位タイプによって、特定のサブネットのトラフィックに基づいた特定のアラートの生成タイミングが決まります。アラートの優先順位タイプは、サブネットトラフィックの監視の程度に影響します。

前述のサブネットのアラートを生成するサブネットの機密性とアラートの優先順位タイプの組み合わせについては、次のマトリックスを参照してください。

サブネットの機密性ステータス	アラートの優先順位タイプ		
	低(Low)	中規模	高(High)
低(Low)	オープンアラートは生成されません。	オープンアラートは生成されません。	オープンアラートが生成されます。
中(Medium)	オープンアラートは生成されません。	オープンアラートが生成されます。	オープンアラートが生成されます。
高(High)	オープンアラートが生成されます。	オープンアラートが生成されます。	オープンアラートが生成されます。

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

アラートの調査

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Secure Network Analytics はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

> これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

オープンアラートのトリアージ

オープンアラートのトリアージは、特に複数の調査が必要な場合に役立ちます。

[アラート(Alerts)] ダッシュボードの [ステータス別にアラートを表示(See alerts by status)] フィールドで [開く(Open)] をクリックし、[オープン(Open)] ステータスでフィルタ処理します。

次の質問に答えてください。

- このアラート タイプを優先度の高いものとして設定しましたか。
- 影響を受けるサブネットに高い機密性を設定しましたか。
- この異常な動作はネットワーク上の新しいエンティティによるものですか。
- エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
- これは、このエンティティの通常の動作からの例外的な逸脱ですか。
- ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
- 保護されたデータや機密データが侵害を受けるリスクがありますか。
- この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
- 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。
- これが優先度の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を閉じることを検討してください。

アラートをスヌーズする

1. [アラート(Alerts)] ダッシュボードの [アラート(Alerts)] テーブルで、該当するアラートの横にあるチェックボックスをオンにします。
2. テーブルの右上隅にある [ステータスの変更(Change Status)] ドロップダウンリストで、[閉じる(Close)] を選択します。
3. [アラートを閉じる(Close Alert)] ダイアログで、ドロップダウンリストからスヌーズ期間を指定し、[送信(Submit)] をクリックします。

スヌーズしたアラートのスヌーズを解除する

スヌーズしたアラートを確認する準備ができたら、スヌーズを解除できます。解除すると、アラートのステータスが [オープン(Open)] に設定されます。

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

1. [アラート(Alerts)] ダッシュボードの [アラート(Alerts)] テーブルで、該当するアラートの横にあるチェックボックスをオンにします。
2. テーブルの右上隅にある [ステータスの変更(Change Status)] ドロップダウンリストで、[スヌーズ解除(Unsnoozed)] を選択します。

アラートを閉じる

調査が終了したら、アラートは閉じることができます。

1. [アラート(Alerts)] ダッシュボードの [アラート(Alerts)] テーブルで、該当するアラートの横にあるチェックボックスをオンにします。
2. テーブルの右上隅にある [ステータスの変更(Change Status)] ドロップダウンリストで、[閉じる(Close)] を選択します。
3. [アラート(Alerts)] ダッシュボードの [アラート(Alerts)] テーブルで、アラートが実際に閉じていることを確認します。

クローズドアラートを再度開く

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを [オープン(Open)] に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

1. アラートリストをフィルタ処理して、クローズドアラートをすべて表示します。
2. 再度開く必要があるアラートを検索してクリックし、詳細を表示します。
3. テーブルの右上隅にある [ステータスの変更(Change Status)] ドロップダウンリストで、[開く(Open)] を選択します。

アラートの更新

初期トリアージに基づいて、次の 1 つ以上の手順を実行します。

- [アラート(Alerts)] ダッシュボードで、テーブルの右上隅にある [アクション(Actions)] フィールドのアラートにタグを追加します。タグを追加することで、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンを確立したりできます。
- [アラートの詳細(Alert Details)] ページの下部にある [コメント(Comments)] テキストボックスに、アラートに関するコメントを入力します。

アラートの確認

割り当てられたアラートを確認する際は、アラートの詳細情報を確認して、Secure Network Analytics がアラートを生成した理由を把握してください。

確認するには、次のいずれかまたは両方を実行します。

- [観測(Observations)] ダッシュボードで、観測タイプの横にある (右矢印)アイコン をクリックすると、そのタイプの記録されたすべての観測内容が表示されます。
- [アラートの詳細(Alerts Details)] ページに、このアラートのソースエンティティについて記録されたすべての観測内容が表示されます。

以下は、確認時の推奨事項です。

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

- 裏付けとなる観測内容を確認し、それらの観測内容がソースに対して持つ意味を理解します。ソースの観測内容をすべて表示して、一般的な動作やパターンを理解し、このアクティビティがより長いトレンドの一部になっている可能性を確認します。
- 裏付けとなる観測内容を確認します。これらの観測内容がソース エンティティに対して持つ意味を理解します。
- 該当するソースの観測内容をすべて表示して、一般的な動作やパターンを理解し、このアクティビティがより長いトレンドの一部になっている可能性を確認します。
- 観測内容から、ソースに関連する追加コンテキスト(関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているフロートラフィックのタイプなど)を表示します。この動作が悪意のある動作を示しているかどうかを判断してください。ソース エンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか(それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど)を確認します。
- 観測内容から、ソースが接続を確立したエンティティのコンテキストを確認します。地理位置情報を調査し、いずれかの地理位置情報データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

裏付けとなる観測結果とコンテキスト詳細の確認

ソースエンティティ

裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。ソースエンティティの動作が悪意のある動作を示しているかどうかを判断してください。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか(それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど)を確認します。ソースエンティティに関連する追加コンテキスト(関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、送信しているフロートラフィックのタイプなど)を表示します。

観測内容では、次のオプションがあります。

[デバイス(Device)] ドロップダウンリストから、次の手順を実行します。

- [アラート(Alerts)] を選択して、エンティティに関連するすべてのアラートを表示します。
- [観測(Observations)] を選択して、エンティティに関連するすべての観測内容を表示します。
- [デバイス(Device)] を選択して、デバイスに関する情報を表示します。
- [フロー分析(Flow Analysis)] を選択して、このエンティティに関連するフロートラフィックを表示します。

IP アドレスまたはホスト名のドロップダウンリストから、次の手順を実行します。

- [コピー(Copy)] アイコン をクリックして、IP アドレスまたはホスト名をコピーします。

外部エンティティ

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データによって悪意のあるエンティティが特定されるかどうかを確認します。これら

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

のエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。ソースエンティティが接続を確立したエンティティのコンテキストを確認します。

観測内容では、次のオプションがあります。

IP アドレスまたはホスト名のドロップダウンリストから、次の手順を実行します。

- [コピー(Copy)] アイコン を選択して、IP アドレスまたはホスト名をコピーします。
- [複数日のIPを検索(Find IP on multiple days)] を選択して、対応するエンティティとの間で送受信されたトラフィックの量と、前日、当日、および翌日に関連付けられた接続の数を表示します。[日(Day)] 列の日付をクリックすると、そのエンティティに関連付けられた日のトラフィック関連情報を追加で表示できます。
- [IPトラフィック(IP Traffic)] を選択して、このエンティティの最近のトラフィック情報を表示します。
- [フロー分析(Flow Analysis)] を選択して、このエンティティのフロー検索結果を表示します。
- [IPをウォッチリストに追加(Add IP to watchlist)] を選択して、このエンティティをウォッチリストに追加します。
- [AbuseIPDB] を選択して、AbuseIPDB の Web サイト上でこのエンティティに関する情報を表示します。
- IP アドレスまたはホスト名のドロップダウンから [Cisco Umbrella] を選択し、Cisco Umbrella の Web サイト上でこのエンティティに関する情報を表示します。
- [Google検索(Google Search)] を選択し、Google でこの IP アドレスを検索します。
- [Talos Intelligence] を選択し、Talos の Web サイト上でこの情報に関する情報を表示します。

エンティティと関連ユーザーの調査

ソースエンティティと、このアラートに関与した可能性のあるすべてのユーザーに関する追加のコンテキストを収集します。

- このエンティティのログ ファイルを見つけます。それがネットワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。
- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更(組織によって承認されていない USB スティックなど)を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況(解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど)が発生したかどうかを確認します。

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

- 確認した内容についてコメントを入力します。[アラートの詳細(Alert Details)] ページの下までスクロールし、[コメント(Comment)] テキストボックスに入力します。完了したら、[コメント(Comment)] をクリックします。

問題の修正

悪意のある動作によってアラートが発生した場合は、悪意のある動作を修正します。

- 悪意のあるエンティティまたはユーザーがネットワーク外からのログインを試みた場合は、ファイアウォール ルールを更新して、それらのエンティティまたはユーザーがネットワークにアクセスできないようにします。
- 脆弱性またはエクスプロイトを特定した場合は、影響を受けるエンティティを更新したり、それらにパッチを適用して脆弱性を削除するか、ファイアウォール設定を更新して不正アクセスを防止します。ネットワーク上の他のエンティティが同様に影響を受ける可能性があるかどうかを判断し、それらのエンティティに同じ更新またはパッチを適用します。現時点で脆弱性またはエクスプロイトを修正する手段がない場合は、該当するベンダーに連絡し、それらを通知してください。
- マルウェアを特定した場合は、エンティティを隔離してマルウェアを削除します。ネットワーク上の他のエンティティが危険にさらされているかどうかを判断し、エンティティまたはセキュリティ ソリューションを更新して、このマルウェアが広がることを防止します。このマルウェアまたはこのマルウェアの原因となったエンティティに関する情報によってセキュリティ情報を更新してください。必要に応じてベンダーに通知してください。
- 悪意のある動作によってデータが漏洩した場合は、許可されていないソースに送信されたデータの性質を確認します。不正なデータ漏洩に関する組織の規定に従ってください。
- 確認した内容についてコメントを入力します。[アラートの詳細(Alert Details)] ページの下までスクロールし、[コメント(Comment)] テキストボックスに入力します。完了したら、[コメント(Comment)] をクリックします。

Secure Network Analytics 設定の微調整

アラートと修正に基づいて、今後のこの動作の識別に役立つように Secure Network Analytics の設定を更新します。

- 外部エンティティが悪意のある動作を引き起こした場合は、それらをウォッチリストに追加します。
- ある国の複数のエンティティによって悪意のある動作が引き起こされた場合は、その国を国のウォッチリストに追加します。
- 特定のサブネットがターゲットになっている場合は、サブネットの機密性を更新します。
- 特定のアラートが懸念される場合は、アラート タイプの優先順位設定を更新します。
- 既知の正常なスキャナを、デフォルトのネットワーク スキャナ ホスト グループ(ID 48)に追加します。

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

アラートの詳細

このページの使用方法の詳細については、「**アラートの調査**」を参照してください。

アラートの詳細には、システムによって報告されたアラートの概要が表示されます。特定のテキストを検索したり、ステータス、タグ、または担当者でフィルタリングしたりできます。また、関連するデバイス情報だけでなく、影響を受けるエンティティに関して生成されたすべての観測結果を表示することもできます。

[アラートタイプの詳細(Alert Type Details)] セクションに、次の情報が表示されます。

アラートの詳細を開く

[アラート(Alerts)] ダッシュボードで、アラートをクリックします。

選択したアラートの [アラートの詳細(Alert Details)] ページが開きます。

アラートタイプの詳細を表示する

フィールド	説明
説明(Description)	アラートの説明。
次の手順(Nest Steps)	アラートを調査するために実行する必要がある次の手順。
MITRE 戦術(MITRE Tactics)	アラートに関連付けられた MITRE 戦術。この戦術の [MITRE(Mitre)] ページにアクセスするには、[MITRE戦術(Mitre Tactic)] エントリをクリックするか、エントリにカーソルを合わせて、開いたポップアップウィンドウで [次で詳細情報を参照(See Full Details at)] リンクをクリックします。
MITRE 手法(MITRE Techniques)	アラートに関連付けられた MITRE 手法。この手法の [MITRE(Mitre)] ページにアクセスするには、[MITRE手法(Mitre Technique)] エントリをクリックするか、エントリにカーソルを合わせて、開いたポップアップウィンドウで [次で詳細情報を参照(See Full Details at)] リンクをクリックします。
アラートタイプの優先順位(Alert Type Priority)	アラートの優先順位:低、通常、高。

アラートルールの詳細を表示する

[アラートルールの詳細(Alert Rule Details)] セクションに、アラートに関連する追加情報を表示できます。

[アラートルールの詳細(Alert Rule Details)] セクションには、次の情報が表示されます。

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

フィールド	説明
ステータス（Status）	アラートのステータス：[オープン（Open）]、[クローズド（Closed）]、または [スヌーズ（Snoozed）]
ID	アラート ID 番号。
更新時刻（Updated）	アラートが最後に更新された時刻。既存のアラートが新しい観測結果を保存すると、システムはこのフィールドを更新します。
作成時刻（Created）	アラートが作成された時刻。
担当者（Assignee）	アラートに割り当てられたユーザー。
タグ（Tags）	タグは、アラートに追加する任意のタイプのラベルまたはテキストであり、ラベルまたはテキストでアラートをフィルタ処理できるようになります。
アラートを閉じる（Close Alert）	アラートを閉じるには、[アラートを閉じる（Close Alert）] をクリックします。

裏付けとなる観測内容テーブルの説明を表示する

アラートの詳細には、このアラートが生成される原因となった観測結果のリストが表示されます。このアラートの原因となったネットワークの動作の詳細については、これらの情報を参照してください。

> このテーブルに表示されるフィールドは、テーブルが関連付けられているアラートによって異なります。

オプション名	説明
影響を受けるリソース（Affected Resource）	影響を受けるリソース。
影響を受けるリソースの種類（Affected Resource Type）	影響を受けるリソースの種類。
異常（Anomaly）	検出された異常のタイプ。
受信バイト数（Bytes In）	特定の時点までにデバイスで受信したトラフィックの量（バイト単位）。

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

オプション名	説明
送信バイト数（Bytes Out）	特定の時点までにデバイスから送信されたトラフィックの量（バイト単位）。
[CIDR範囲（CIDR Range）]	CIDR 表記によるおおよそのスキャン範囲（実際の範囲はもっと小さくなる場合があります）。
接続デバイス（Connected Device）	エンドポイントまたは送信元で接続を確立したデバイス。
接続済み IP（Connected IP）	この送信元が通信を行った IP。
接続済みポート（Connected Ports）	このポートが通信を行ったポート。
対応するポート（Corresponding Ports）	通信で使用されたポート。
データシンク IP（Data Sink IP）	データがアップロードされた外部デバイスの IP アドレス。
データシンクプロファイル（Data Sink Profile）	データシンクにアップロードするときの観測ソース（このデバイス）のローカルプロファイル。
データ ソース（Data Source）	データのダウンロード元となる内部デバイス。
データソース IP（Data Source IP）	データのダウンロード元となる内部デバイスの IP アドレス。
データソースプロファイル（Data Source Profile）	データソースからダウンロードするときの観測ソース（このデバイス）のローカルプロファイル。
デバイス（Device）	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連する

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

オプション名	説明
	[アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。 • [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。
ドメイン/URL（Domain/URL）	NGFW 接続イベントまたはパッシブ DNS に基づくドメイン/URL。
ダウンロード（秒）（Download Sec）	ダウンロードが完了するまでに必要な時間。
ダウンロード速度（bps）（Download Speed bps）	bps 単位のダウンロード速度。
ダウンロード開始（Download Start）	外部データシンクのダウンロードが開始された時刻。
外部 IP（External IP）	外部 IP アドレス。
失敗した試行（Failed Attempts）	エンティティがデバイスへの接続の確立を試行した回数。
ハートビート間隔（秒）（Heartbeat period (Seconds)）	ハートビートの間隔。
履歴の長さ（日）（History Length (Days)）	標準セットの計算に使用された履歴日数。
内部ポートセット（Internal Port Set）	ポートセットのタイプ。たとえば、「接続済み内部（connected internal）」は、内部接続に使用される接続済みポートのセットです。

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

オプション名	説明
最後のアクティブ（Last Active）	観測が最後にアクティブだった時刻。
ローカルデバイス（Local Device）	通信に使用されたローカルデバイス。
ローカル ポート（Local Port）	デバイスに接続されたエンドポイントまたは送信元のポート。
ルックバック日数（Lookback Days）	標準セットの計算に使用された履歴日数。
喪失したポートセット（Lost Port Sets）	この日付に使用されなくなったポート。
一致するウォッチリスト（Matching Watchlists）	ウォッチリストがドメインベースの場合、一致するドメイン名がここにリストされます。
メトリック（Metric）	この外れ値のメトリック。たとえば、内部の「受信バイト数（Bytes In）」の外れ値は、デバイスへの内部ネットワークトラフィック（インターネットがない場合）が急増したことを示します。
新しい接続（New Connections）	ルックバック期間には存在しなかった、この日付の新しい接続。
新しいポートセット（New Port Set）	この日付に使用され、ルックバック期間には使用されなかったポート。
新しいプロファイル（New Profile）	以前の動作とは異なる新しいデバイスプロファイル。
標準の接続セット（Normal Connection Set）	ルックバック期間中に検出された接続。
標準のポートセット（Normal Ports Set）	ルックバック期間に使用されたポート。
ハートビート数（Number of Heartbeats）	この観測されたイベント中にサーバーが接続された回数。
パケット入力（Packets In）	送信元が受信したパケット。

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

オプション名	説明
パケット出力（Packets Out）	送信元から送信されたパケット。
ポート（Port）	観測されたイベントで使用された送信元ポート。
ポート範囲（Port Ranges）	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。一般的な対象に、Web サーバーの対象が含まれる場合があります。
確率（Probability）	この外れ値が表示される確率。
プロファイル（Profile）	デバイスが接続されているエンドポイントまたは送信元に関連付けられたロール。
パブリック IP（Public Facing IP）	ウォッチリストで検出されたパブリック IP アドレス。
リモート デバイス（Remote Device）	この送信元が通信を行ったデバイス。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。 [アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。 • [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。
リモートIP（Remote IP）	この送信元が通信を行った IP アドレス。

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

オプション名	説明
リモート ポート（Remote Port）	この送信元が通信を行ったポート。
リソース（Resource）	影響を受けるリソース。
サンプル サイズ（Sample Size）	この計算で使用された履歴サンプルの数。
スキャンされたデバイス（Scanned Device）	スキャンされたデバイスの IP アドレスまたはホスト名。
スキャンされたポート（Scanned Ports）	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。
スキャナデバイス（Scanner Device）	スキャンを実行したデバイスの IP アドレスまたはホスト名。
重大度（Severity）	報告されたイベントの重大度。
送信元（Source）	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。 [アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。 • [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。

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

オプション名	説明
ソース IP（Source IP）	イベントが観測されたときの送信元 IP。
送信元ポート（Source Port）	イベントが観測されたときの送信元ポート。
疑わしい接続（Suspect Connections）	異常な外部ソースへの新しい接続、または異常なポート上の接続。
時刻（Time）	観測が行われた時刻。
時間枠（Time Window）	イベントが共有された期間。
転送サイズ（Transfer Size）	転送されたバイト数。
アップロード開始（Upload Start）	外部データシンクへのアップロードの開始時間。
アップロード（秒）（Upload Sec）	アップロードの期間。
アップロード速度（bps）（Upload Speed bps）	bps 単位のアップロード速度。
ユーザー（User）	観測されたイベントに関連付けられたユーザーアカウント。
違反ポート（Violating Port）	送信元によって使用されたポート。
違反プロトコル（Violating Protocol）	送信元によって使用されたネットワークプロトコル（TCP など）。
違反タイプ（Violating Type）	違反のタイプ。

[アラートの詳細（Alert Details）] ページからアクセスできるその他のページ

アラートの優先順位設定

[アラートの優先順位設定（Alerts Priorities Configuration）] ページにアクセスするには、[アラートタイプの詳細（Alert Type Details）] セクションの下部にある [アラートの優先順位ページに移動（Go to Alert Priorities page）] リンクをクリックします。

[アラートの優先順位設定（Alert Priorities Configuration）] ページが開きます。

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

フロー検索結果

裏付けとなる観測内容テーブルに表示されている特定の時間の [フロー検索結果(Flow Search Results)] ページにアクセスするには、[時間(Time)] 列の該当するエントリをクリックします。

または

裏付けとなる観測内容テーブルから、該当するデバイスのドロップダウンリストをクリックし、表示されるメニューで [フロー分析(Flow Analysis)] を選択します。

[フロー検索結果(Flow Search Results)] ページが表示されます。

[フロー検索結果(Flow Search Results)] ページの詳細については、「**フロー検索結果:概要**」を参照してください。

デバイスレポート

裏付けとなる観測内容テーブルに表示された特定のデバイスのデバイスレポートにアクセスするには、該当するデバイスのドロップダウンリストをクリックし、表示されるメニューで [デバイス(Device)] を選択します。

デバイスレポートが開きます。

[デバイス(Device)] ページの詳細については、「**デバイスレポート**」を参照してください。

[アラート(Alerts)] ダッシュボード

裏付けとなる観測内容テーブルに表示された、特定のデバイスに関連するすべてのアラートのリストが含まれる [アラート(Alerts)] ダッシュボードにアクセスするには、該当するデバイスのドロップダウンリストをクリックし、表示されるメニューで [アラート(Alerts)] を選択します。

[アラート(Alerts)] ダッシュボードが開き、そのデバイスでフィルタ処理されます。

[アラート(Alerts)] ダッシュボードの詳細については、「**[アラート(Alerts)] ダッシュボード**」を参照してください。

デバイス別の観測

裏付けとなる観測内容テーブルに表示された、特定のデバイスに関連するすべての観測内容のリストが含まれる [デバイス別の観測(Observations by Device)] ページにアクセスするには、該当するデバイスのドロップダウンリストをクリックし、表示されるメニューで [観測(Observations)] を選択します。

[デバイス別の観測(Observations by Device)] ページが開き、そのデバイスでフィルタ処理されます。

[デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。

アラートのコメントを入力する

1. ページ下部の [コメント(Comments)] テキストボックスに、適切なコメントを入力します。
2. [コメント(Comment)] をクリックします。

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

デバイスレポート

デバイスレポートでは、ネットワーク内のエンティティに関する動作情報を提供します。

- アラートに関する追加のコンテキストを表示するには、[アラートの詳細(Alert Details)] ページからデバイスレポートにアクセスします。
- 観測に関する追加のコンテキストを表示するには、次のセクションにリストされている [観測(Observation)] ページのいずれかからこのレポートにアクセスします。

デバイスレポートを開く

次のいずれかのページで、該当するテーブルに表示されている目的のデバイスのドロップダウンリストをクリックし、表示されるメニューで [デバイス(Device)] を選択します。

- アラート詳細(Alert Details)
- 観測ハイライト
- デバイス別の観測
- 選択された観測結果

デバイスレポートが開きます。

デバイスレポートの概要

このページでは次の情報を確認できます。

- 日次のデバイスメトリックの履歴。この情報は、[履歴(History)] セクションに表示されます(このトピックの「履歴」セクションを参照)。
- システムによって保存されるエンティティのモデルの概要。この情報は、[概要(Summary)] タブに表示されます(このトピックの「概要」セクションを参照)。
- エンティティと関連する接続との間で送受信されるトラフィックの量。この情報は、[トラフィック(Traffic)] タブに表示されます(このトピックの「トラフィック」セクションを参照)。
- ロール関連の情報。この情報は、[プロファイリング(Profiling)] タブに表示されます(このトピックの「プロファイリング」セクションを参照)。

時間範囲の編集

デフォルトでは、[概要(Summary)]、[トラフィック(Traffic)]、[プロファイリング(Profiling)] および [IP(IPs)] タブに当日の情報が表示されます。ただし、過去 1 日の情報を表示する選択もできます。これを行うには、次の手順を実行します。

1. 履歴グラフのすぐ下にある [選択した日付(Selected Date)] ドロップダウンリストから、左右の矢印を使用して目的の月に移動します。
2. 目的の日付をクリックします。
3. [日付の選択(Select Date)] をクリックします。
4. [選択した日付(Selected Date)] セクションの右側にある [適用(Apply)] をクリックします。

履歴

[履歴(History)] 折れ線グラフには、エンティティとの間で送受信されるトラフィックの量とエンティティが関与した接続の数が 1 日間隔で表示されます。グラフにカーソルを合わせると、その日のエ

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

ンティティのトラフィックに関する詳細情報が表示されます。

概要

[概要(Summary)] タブには、システムに保存されているエンティティのモデルの概要が表示されます。

- [アラート(Alerting)] セクションで、次の手順を実行します。
  - [アラートを開く(Open Alerts)] をクリックして [アラート(Alerts)] ダッシュボードにアクセスし、開いているすべてのアラートを表示します。
  - [クローズドアラート(Closed Alerts)] をクリックして [アラート(Alerts)] ダッシュボードにアクセスし、すべてのクローズドアラートを表示します。
  - [観測(Observations)] をクリックして、[デバイス別の観測(Observations by Device)] ページにアクセスします。

[概要(Summary)] タブに表示されるフィールドの説明については、次の表を参照してください。

エンティティ概要フィールド

フィールド	説明
参加者(Attendance)	
通常アクティブ(Normally Active)	このエンティティが通常アクティブである期間。
IP アドレス(IP Addresses)	エンティティの IP アドレス。
接続	
接続(Connections)	このエンティティが関与していた接続の数。
内部接続(Internal Connections)	このエンティティが関与していた内部エンティティとの接続数。
外部接続(External Connections)	このエンティティが関与していた外部エンティティとの接続数。
上位内部接続	
上位内部接続(Top Internal Connections)	送信されたトラフィックの合計数に基づく、エンティティが接続を確立した上位 5 つの内部エンティティ。
上位外部接続(Top External Connections)	
上位外部接続(Top External Connections)	送信されたトラフィックの合計数に基づく、エンティティが接続を確立した上位 5 つの外部エンティティ。

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

トラフィック	
受信バイト数（Bytes In）	エンティティが受信したトラフィックの量。
送信バイト数（Bytes Out）	エンティティが送信したトラフィックの量。
合計バイト数（Bytes Total）	エンティティが送信したトラフィックの合計。
内部トラフィック	
受信バイト数（Bytes In）	エンティティが内部エンティティから受信したトラフィックの量。
送信バイト数（Bytes Out）	エンティティが内部エンティティに送信したトラフィックの量。
外部トラフィック	
受信バイト数（Bytes In）	エンティティが外部エンティティから受信したトラフィックの量。
送信バイト数（Bytes Out）	エンティティが外部エンティティに送信したトラフィックの量。
DNS 名	
DNS 名（DNS name）	エンティティに関連付けられた DNS ドメイン名。
アラート	
オープンアラート（Open Alerts）	このエンティティに関連付けられているすべての（当日だけでなく）オープンアラート。
クローズドアラート（Closed Alerts）	このエンティティに関連付けられているすべての（当日だけでなく）クローズドアラート。
オブザベーション（Observations）	このエンティティに関連付けられたすべての（当日だけでなく）観測結果。
ロール	
ロール（Roles）	このエンティティに関連付けられているロール。
プロファイル	
プロファイル（Profiles）	リストされたプロファイルに対応してエンティティが動作した時間の割合。

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

トラフィック

[トラフィック(Traffic)] 折れ線グラフには、エンティティとの間で送受信されるトラフィックの量とエンティティが関与した接続の数が 10 分間隔で表示されます。エンティティが関与した接続に関する情報も確認できます。

- [トラフィック(Traffic)] グラフのさまざまな線にカーソルを合わせると、エンティティのトラフィックの詳細が 10 分間隔で表示されます。
- グラフをフィルタ処理するオプションは次のとおりです。
    - このエンティティが接続を確立したすべてのエンティティに関する情報を表示するには、[すべて(All)] をクリックします。
    - このエンティティが接続を確立した内部エンティティに関する情報を表示するには、[内部(Internal)] をクリックします。
    - このエンティティが接続を確立した外部エンティティに関する情報を表示するには、[外部(External)] をクリックします。

[トラフィック(Traffic)] タブに表示されるフィールドの説明については、次の表を参照してください。

エンティティトラフィック フィールド

フィールド	説明
接続済み IP(Connected IP)	このエンティティが接続を確立した IP アドレス。
ホスト名/ PDNS レコード (Hostname/PDNS Record)	この IP アドレスのホスト名(使用可能な場合)。
受信バイト数(Bytes In)	接続されたエンティティからエンティティが受信したバイト数。
送信バイト数(Bytes Out)	エンティティによって接続されたエンティティに送信されたバイト数。
合計バイト数(Bytes Total)	この接続のエンティティによって送信された合計バイト数。
最初の接続時間 (Time of First Connection)	接続された IP との、この日の最初の接続時刻。
最終接続時刻 (Time of Last Connection)	接続された IP との、この日の最後の接続時刻。

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

プロファイリング

[プロファイリング（Profiling）] タブには、このエンティティに関連付けられているロールと、各ロールに関連付けられているトラフィックに関する情報が表示されます。

円グラフにカーソルを合わせると、そのプロファイルと一致する、エンティティの確立された合計接続の割合が表示されます（グラフには上位 8 つのプロファイルが表示されます）。

[プロファイリング（Profilinf）] タブに表示されるフィールドの説明については、次の表を参照してください。

エンティティ プロファイル フィールド

フィールド	説明
名前	エンティティに関連付けられているプロファイルの名前。
参加者（Attendance）	このプロファイルと一致する、このエンティティがアクティブであった 1 日の時間の割合。
受信バイト数（Bytes In）	このプロファイルと一致する、エンティティが受信したバイト数。
送信バイト数（Bytes Out）	このプロファイルと一致する、エンティティによって送信されたバイト数。
合計バイト数（Bytes Total）	このプロファイルと一致する、エンティティによって送信された合計バイト数。
接続（Connections）	このプロファイルと一致する、このエンティティが関与していた接続の数。

IP

[IP（IPs）] タブには、関連付けられた日付ごとにデバイスに関連付けられた IP のリストと、過去 30 日間にデバイスに関連付けられたすべての IP の統合リストが表示されます。また、これらの各 IP がデバイスに関連付けられて最後にアクティブになった日付も表示されます。

フィールド	説明
IPs	デバイスに関連付けられた IP。
[最後のアクティブ（Last Active）]	デバイスに関連付けられた IP が最後にアクティブだった日付。

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

[観測(Observations)] ダッシュボード

- [観測タイプ(Observation Types)] ページの詳細については、「**観測タイプ**」を参照してください。
- [デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。
- [選択された観測内容(Selected Observations)] ページの詳細については、「**選択された観測内容**」を参照してください。

[観測(Observations)] ダッシュボードを開く

メインメニューから、[モニター(Monitor)] > [観測(Observations)] の順に選択します。

[観測(Observations)] ダッシュボードが開きます。

観測ハイライトの概要

観測とは、ネットワーク上でのエンティティの動作に関する事実(外部 IP アドレスとのハートビート接続、ウォッチリスト上のエンティティとのやり取り、別のエンティティとの間で確立されたリモートアクセスセッションなど)です。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートは、観測データを組み合わせて生成されます。単独の観測データが必ずしも悪意のある動作を示すものではありません。最近の観察結果自体が、ネットワークにおける悪意のある動作の存在を必ずしも意味するものではありません。アラートを確認して、悪意のある可能性のある動作の全体像を把握します。

システムがトラフィックを検査すると、ネットワーク上のエンティティについての観察内容(事実)がログに記録されます。観測データはエンティティごとに記録されるため、合理的なレビュー量を超える観測データがネットワークで生成される可能性があります。システムは、ネットワークについて記録された最も注目すべき観測データのサブセットを提示します。これらを確認してフィルタリングすることで、アラートが生成される可能性のある動作のタイプをより深く理解することができます。

観測データが多いほどアラート数が多いとは限りません。たとえば、観測データの多いエンティティでは、さまざまなトラフィックが大量に通過している可能性がありますが、ダイナミック エンティティ モデリングは、この動作が正常であり、このエンティティの予測範囲内と判断した可能性があります。同様に、観測データが少なければ、アラートが生成されないとは限りません。たとえば、エンティティで検出された唯一のアクティビティが、不適切なクレデンシャルを使用したサーバーへの継続的なログインである場合、観測データが比較的少なくても、複数回のログイン試行の失敗を通知するアラートが生成される可能性があります。

観測ハイライトを表示する

ドリルダウンして、そのタイプのすべての観測内容を表示できます。ドリルダウンすると、このページに新しいタブが開き、それらの観測内容が表示されます。別の観察内容タイプを選択してドリルダウンすると、その新しいタブがそれらの観察内容で更新されます。

- 特定のタイプの観測内容をすべて表示するには、該当する観測タイプの横にある (右矢印)アイコン をクリックします。

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

[選択された観測内容(Selected Observations)] ページが開きます。デフォルトでは、過去 24 時間以内に行われた、選択したタイプの観測内容をすべて含むテーブルが表示されます。[選択された観測内容(Selected Observations)] ページの詳細については、「**選択された観測内容**」を参照してください。

- 特定のタイプの観測内容をすべて含む .csv ファイルをダウンロードするには、関連するテーブルの右上隅にある 

([CSVのダウンロード(Download CSV)]) アイコン をクリックします。

観測ハイライトテーブルの説明を表示する

ハイライトテーブルに表示されるフィールドは、各テーブルが関連付けられている観測内容によって異なります。

オプション名	説明
影響を受けるリソース(Affected Resource)	影響を受けるリソース。
影響を受けるリソースの種類(Affected Resource Type)	影響を受けるリソースの種類。
異常(Anomaly)	検出された異常のタイプ。
受信バイト数(Bytes In)	特定の時点までにデバイスで受信したトラフィックの量(バイト単位)。
送信バイト数(Bytes Out)	特定の時点までにデバイスから送信されたトラフィックの量(バイト単位)。
[CIDR範囲(CIDR Range)]	CIDR 表記によるおおよそのスキャン範囲(実際の範囲はもっと小さくなる場合があります)。
接続デバイス(Connected Device)	エンドポイントまたは送信元で接続を確立したデバイス。
接続済み IP(Connected IP)	この送信元が通信を行った IP。
接続済みポート(Connected Ports)	このポートが通信を行ったポート。
対応するポート(Corresponding Ports)	通信で使用されたポート。
データシンク IP(Data	データがアップロードされた外部デバイスの IP アドレス。

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

オプション名	説明
Sink IP）	
データシンクプロファイル（Data Sink Profile）	データシンクにアップロードするときの観測ソース（このデバイス）のローカルプロファイル。
データ ソース（Data Source）	データのダウンロード元となる内部デバイス。
データソース IP（Data Source IP）	データのダウンロード元となる内部デバイスの IP アドレス。
データソースプロファイル（Data Source Profile）	データソースからダウンロードするときの観測ソース（このデバイス）のローカルプロファイル。
デバイス（Device）	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。 [アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。 • [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。
ドメイン/URL（Domain/URL）	NGFW 接続イベントまたはパッシブ DNS に基づくドメイン/URL。

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

オプション名	説明
ダウンロード（秒）（Download Sec）	ダウンロードが完了するまでに必要な時間。
ダウンロード速度（bps）（Download Speed bps）	bps 単位のダウンロード速度。
ダウンロード開始（Download Start）	外部データシンクのダウンロードが開始された時刻。
外部 IP（External IP）	外部 IP アドレス。
失敗した試行（Failed Attempts）	エンティティがデバイスへの接続の確立を試行した回数。
ハートビート間隔（秒）（Heartbeat period (Seconds)）	ハートビートの間隔。
履歴の長さ（日）（History Length (Days)）	標準セットの計算に使用された履歴日数。
内部ポートセット（Internal Port Set）	ポートセットのタイプ。たとえば、「接続済み内部（connected internal）」は、内部接続に使用される接続済みポートのセットです。
最後のアクティブ（Last Active）	観測が最後にアクティブだった時刻。
ローカルデバイス（Local Device）	通信に使用されたローカルデバイス。
ローカル ポート（Local Port）	デバイスに接続されたエンドポイントまたは送信元のポート。
ルックバック日数（Lookback Days）	標準セットの計算に使用された履歴日数。
喪失したポートセット（Lost Port Sets）	この日付に使用されなくなったポート。
一致するウォッチリスト（Matching Watchlists）	ウォッチリストがドメインベースの場合、一致するドメイン名がここにリストされます。

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

オプション名	説明
メトリック（Metric）	この外れ値のメトリック。たとえば、内部の「受信バイト数（Bytes In）」の外れ値は、デバイスへの内部ネットワークトラフィック（インターネットがない場合）が急増したことを示します。
新しい接続（New Connections）	ルックバック期間には存在しなかった、この日付の新しい接続。
新しいポートセット（New Port Set）	この日付に使用され、ルックバック期間には使用されなかったポート。
新しいプロファイル（New Profile）	以前の動作とは異なる新しいデバイスプロファイル。
標準の接続セット（Normal Connection Set）	ルックバック期間中に検出された接続。
標準のポートセット（Normal Ports Set）	ルックバック期間に使用されたポート。
ハートビート数（Number of Heartbeats）	この観測されたイベント中にサーバーが接続された回数。
パケット入力（Packets In）	送信元が受信したパケット。
パケット出力（Packets Out）	送信元から送信されたパケット。
ポート（Port）	観測されたイベントで使用された送信元ポート。
ポート範囲（Port Ranges）	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。一般的な対象に、Web サーバーの対象が含まれる場合があります。
確率（Probability）	この外れ値が表示される確率。
プロファイル（Profile）	デバイスが接続されているエンドポイントまたは送信元に関連付けられたロール。
パブリック IP（Public Facing IP）	ウォッチリストで検出されたパブリック IP アドレス。
リモート デバイス	この送信元が通信を行ったデバイス。

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

オプション名	説明
(Remote Device)	ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス(ネットワーク)(Device (Network))] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス(Device)] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート(Alerts)] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート(Alerts)] ダッシュボードにアクセスします。 [アラート(Alerts)] ダッシュボードの詳細については、「**[アラート(Alerts)] ダッシュボード**」を参照してください。 • [観測(Observations)] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測(Observations by Device)] ページにアクセスします。 [デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析(Flow Analysis)] を選択して、送信元に関連するフロー情報を含む [フロー検索結果(Flow Search Results)] ページにアクセスします。 [フロー検索結果(Flow Search Results)] ページの詳細については、「**フロー検索結果:概要**」を参照してください。
リモートIP(Remote IP)	この送信元が通信を行った IP アドレス。
リモート ポート(Remote Port)	この送信元が通信を行ったポート。
リソース(Resource)	影響を受けるリソース。
サンプル サイズ(Sample Size)	この計算で使用された履歴サンプルの数。
スキャンされたデバイス(Scanned Device)	スキャンされたデバイスの IP アドレスまたはホスト名。
スキャンされたポート(Scanned Ports)	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。
スキャナデバイス(Scanner Device)	スキャンを実行したデバイスの IP アドレスまたはホスト名。

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

オプション名	説明
重大度(Severity)	報告されたイベントの重大度。
送信元(Source)	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス(ネットワーク)(Device (Network))]を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス(Device)]ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート(Alerts)]を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む[アラート(Alerts)]ダッシュボードにアクセスします。 [アラート(Alerts)]ダッシュボードの詳細については、「**[アラート(Alerts)]ダッシュボード**」を参照してください。 • [観測(Observations)]を選択して、送信元に関連するすべての観測内容のリストを含む[デバイス別の観測(Observations by Device)]ページにアクセスします。 [デバイス別の観測(Observations by Device)]ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析(Flow Analysis)]を選択して、送信元に関連するフロー情報を含む[フロー検索結果(Flow Search Results)]ページにアクセスします。 [フロー検索結果(Flow Search Results)]ページの詳細については、「**フロー検索結果:概要**」を参照してください。
ソース IP(Source IP)	イベントが観測されたときの送信元 IP。
送信元ポート(Source Port)	イベントが観測されたときの送信元ポート。
疑わしい接続(Suspect Connections)	異常な外部ソースへの新しい接続、または異常なポート上の接続。
時刻(Time)	観測が行われた時刻。
時間枠(Time Window)	イベントが共有された期間。
転送サイズ(Transfer Size)	転送されたバイト数。

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

オプション名	説明
アップロード開始（Upload Start）	外部データシンクへのアップロードの開始時間。
アップロード（秒）（Upload Sec）	アップロードの期間。
アップロード速度（bps）（Upload Speed bps）	bps 単位のアップロード速度。
ユーザー（User）	観測されたイベントに関連付けられたユーザーアカウント。
違反ポート（Violating Port）	送信元によって使用されたポート。
違反プロトコル（Violating Protocol）	送信元によって使用されたネットワークプロトコル（TCP など）。
違反タイプ（Violating Type）	違反のタイプ。

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

観測タイプ

観測タイプを開く

1. メインメニューから、[モニター(Monitor)] > [観測(Observations)] の順に選択します。
2. [観測(Observations)] ダッシュボードで、[観測(Observations)] サイドメニューから [タイプ(Type)] を選択します。

   [観測タイプ(Observation Types)] ページが開きます。

観測タイプを表示する

観測タイプの説明を読み取るには、次の手順を実行します。

表示する観測タイプの横にある (右矢印)アイコン をクリックします。

[選択された観測内容(Selected Observations)] ページが開きます。デフォルトでは、過去 24 時間以内に行われた、選択したタイプの観測内容をすべて含むテーブルが表示されます。[選択された観測内容(Selected Observations)] ページの詳細については、「**選択された観測内容**」を参照してください。

観測タイプのリストには、ログに記録できるすべての観測タイプが、説明、およびログに記録された観測数とともに表示されます。

ドリルダウンして、そのタイプのすべての観測内容を表示できます。ドリルダウンすると、このページに新しいタブが開き、それらの観測内容が表示されます。別の観察内容タイプを選択してドリルダウンすると、その新しいタブがそれらの観察内容で更新されます。

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

デバイス別の観測

デバイス別の観測を開く

1. メインメニューから、[モニター(Monitor)] > [観測(Observations)] の順に選択します。
2. [観測(Observations)] ダッシュボードで、[観測(Observations)] サイドメニューから [デバイス別(By Device)] を選択します。

または

[アラートの詳細(Alert Details)] ページの [裏付けとなる観測内容(Supporting Observations)] テーブルで、目的のデバイスのドロップダウンリストから [観測(Observations)] を選択します。

[デバイス別の観測(Observations by Device)] ページが開き、そのデバイスに関連するすべての観測内容のリストが表示されます。

デバイス別の観測を表示する

このページを使用して、最も多くの観測内容が関連付けられているデバイスを表示できます。

フィールド	説明
デバイス	観測に関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス(ネットワーク)(Device (Network))] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス(Device)] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート(Alerts)] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート(Alerts)] ダッシュボードにアクセスします。 [アラート(Alerts)] ダッシュボードの詳細については、「**[アラート(Alerts)] ダッシュボード**」を参照してください。 • [観測(Observations)] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測(Observations by Device)] ページにアクセスします。 [デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析(Flow Analysis)] を選択して、送信元に関連するフロー情報を含む [フロー検索結果(Flow Search Results)] ページにアクセスします。 [フロー検索結果(Flow Search Results)] ページの詳細については、「**フロー検索結果:概要**」を参照してください。

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

メンバー数（Count）	関連付けられたデバイスで行われた観測の数。
時刻（Time）	関連付けられたデバイスの観測内容が最後に記録された時刻。

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

選択された観測内容

選択された観測内容を開く

1. メインメニューから、[モニター(Monitor)] > [観測(Observations)] の順に選択します。
2. [観測(Observations)] ダッシュボードで、[観測(Observations)] サイドメニューから [選択された観測内容(Selected Observation)] を選択します。

   [選択された観測内容(Selected Observation)] ページが開きます。

選択された観測内容を表示する

[選択された観測内容(Selected Observation)] ウィンドウから、特定のタイプの観測内容がすべて表示されます。これにより、ネットワークトラフィックに基づいて Secure Network Analytics がログに記録している観測データを確認できます。過去 24 時間以内に行われたすべての観測内容が表示されます(この時間範囲は [時間(Time)] フィールドを使用して変更できます)。

選択した観測内容を表示するには、次の手順を実行します。

1. ▶(**右向き三角形**)アイコンをクリックして、ページ上部の [フィルタ(Filters)] ペインを展開します。
2. [観測タイプ(Observation Type)] ドロップダウンリストから、[観測タイプ(Observation Type)] を選択します。
3. [検索(Search)] フィールドにフィルタ値を入力します。
4. 時間範囲を設定するには、[時間(Time)] ドロップダウン矢印をクリックします。時間は、ブラウザのタイムゾーンに従って表示されます。

   [カレンダー(Calendar)] ダイアログが表示されます。

   事前定義された時間範囲を使用する場合は、左パネルのメニューから適切なオプションを選択します。

   カスタム時間範囲を定義する場合は、次のいずれかを実行できます。

   a. [開始日時(From Date/Time)] セクションで、スピンリストを使用して希望の開始日を選択します。
   b. [終了日時(To Data/Time)] セクションで、スピンリストを使用して希望の終了日を選択します。この 2 つの日付の間の期間は灰色で強調表示されます。
   c. [範囲を選択(Select range)] をクリックして変更を保存します。

> このテーブルに表示されるフィールドは、テーブルが関連付けられている観測内容によって異なります。

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

選択された観測内容テーブルの説明を表示する

オプション名	説明
影響を受けるリソース（Affected Resource）	影響を受けるリソース。
影響を受けるリソースの種類（Affected Resource Type）	影響を受けるリソースの種類。
異常（Anomaly）	検出された異常のタイプ。
受信バイト数（Bytes In）	特定の時点までにデバイスで受信したトラフィックの量（バイト単位）。
送信バイト数（Bytes Out）	特定の時点までにデバイスから送信されたトラフィックの量（バイト単位）。
[CIDR範囲（CIDR Range）]	CIDR 表記によるおおよそのスキャン範囲（実際の範囲はもっと小さくなる場合があります）。
接続デバイス（Connected Device）	エンドポイントまたは送信元で接続を確立したデバイス。
接続済み IP（Connected IP）	この送信元が通信を行った IP。
接続済みポート（Connected Ports）	このポートが通信を行ったポート。
対応するポート（Corresponding Ports）	通信で使用されたポート。
データシンク IP（Data Sink IP）	データがアップロードされた外部デバイスの IP アドレス。
データシンクプロファイル（Data Sink Profile）	データシンクにアップロードするときの観測ソース（このデバイス）のローカルプロファイル。
データ ソース（Data Source）	データのダウンロード元となる内部デバイス。
データソース IP（Data Source IP）	データのダウンロード元となる内部デバイスの IP アドレス。

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

オプション名	説明
データソースプロファイル（Data Source Profile）	データソースからダウンロードするときの観測ソース（このデバイス）のローカルプロファイル。
デバイス（Device）	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。 [アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。 • [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。
ドメイン/URL（Domain/URL）	NGFW 接続イベントまたはパッシブ DNS に基づくドメイン/URL。
ダウンロード（秒）（Download Sec）	ダウンロードが完了するまでに必要な時間。
ダウンロード速度（bps）（Download Speed bps）	bps 単位のダウンロード速度。
ダウンロード開始（Download Start）	外部データシンクのダウンロードが開始された時刻。
外部 IP（External IP）	外部 IP アドレス。

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

オプション名	説明
失敗した試行（Failed Attempts）	エンティティがデバイスへの接続の確立を試行した回数。
ハートビート間隔（秒）（Heartbeat period (Seconds)）	ハートビートの間隔。
履歴の長さ（日）（History Length (Days)）	標準セットの計算に使用された履歴日数。
内部ポートセット（Internal Port Set）	ポートセットのタイプ。たとえば、「接続済み内部（connected internal）」は、内部接続に使用される接続済みポートのセットです。
最後のアクティブ（Last Active）	観測が最後にアクティブだった時刻。
ローカルデバイス（Local Device）	通信に使用されたローカルデバイス。
ローカル ポート（Local Port）	デバイスに接続されたエンドポイントまたは送信元のポート。
ルックバック日数（Lookback Days）	標準セットの計算に使用された履歴日数。
喪失したポートセット（Lost Port Sets）	この日付に使用されなくなったポート。
一致するウォッチリスト（Matching Watchlists）	ウォッチリストがドメインベースの場合、一致するドメイン名がここにリストされます。
メトリック（Metric）	この外れ値のメトリック。たとえば、内部の「受信バイト数（Bytes In）」の外れ値は、デバイスへの内部ネットワークトラフィック（インターネットがない場合）が急増したことを示します。
新しい接続（New Connections）	ルックバック期間には存在しなかった、この日付の新しい接続。
新しいポートセット（New Port Set）	この日付に使用され、ルックバック期間には使用されなかったポート。
新しいプロファイル（New Profile）	以前の動作とは異なる新しいデバイスプロファイル。

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

オプション名	説明
標準の接続セット（Normal Connection Set）	ルックバック期間中に検出された接続。
標準のポートセット（Normal Ports Set）	ルックバック期間に使用されたポート。
ハートビート数（Number of Heartbeats）	この観測されたイベント中にサーバーが接続された回数。
パケット入力（Packets In）	送信元が受信したパケット。
パケット出力（Packets Out）	送信元から送信されたパケット。
ポート（Port）	観測されたイベントで使用された送信元ポート。
ポート範囲（Port Ranges）	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。一般的な対象に、Web サーバーの対象が含まれる場合があります。
確率（Probability）	この外れ値が表示される確率。
プロファイル（Profile）	デバイスが接続されているエンドポイントまたは送信元に関連付けられたロール。
パブリック IP（Public Facing IP）	ウォッチリストで検出されたパブリック IP アドレス。
リモート デバイス（Remote Device）	この送信元が通信を行ったデバイス。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。 [アラート（Alerts）] ダッシュボードの詳細については、「**[アラート（Alerts）] ダッシュボード**」を参照してください。

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

オプション名	説明
	• [観測（Observations）] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測（Observations by Device）] ページにアクセスします。 [デバイス別の観測（Observations by Device）] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析（Flow Analysis）] を選択して、送信元に関連するフロー情報を含む [フロー検索結果（Flow Search Results）] ページにアクセスします。 [フロー検索結果（Flow Search Results）] ページの詳細については、「**フロー検索結果：概要**」を参照してください。
リモートIP（Remote IP）	この送信元が通信を行った IP アドレス。
リモート ポート（Remote Port）	この送信元が通信を行ったポート。
リソース（Resource）	影響を受けるリソース。
サンプル サイズ（Sample Size）	この計算で使用された履歴サンプルの数。
スキャンされたデバイス（Scanned Device）	スキャンされたデバイスの IP アドレスまたはホスト名。
スキャンされたポート（Scanned Ports）	この範囲に含まれるデバイスによってスキャンされたポート、および場合によっては他のポート。
スキャナデバイス（Scanner Device）	スキャンを実行したデバイスの IP アドレスまたはホスト名。
重大度（Severity）	報告されたイベントの重大度。
送信元（Source）	関連付けられたエンドポイントまたは送信元。 ドロップダウンリストをクリックして、次のオプションにアクセスします。 • [デバイス（ネットワーク）（Device（Network））] を選択して、送信元別にフィルタ処理されたデバイスレポートにアクセスします。 [デバイス（Device）] ページの詳細については、「**デバイスレポート**」を参照してください。 • [アラート（Alerts）] を選択して、そのアラートの送信元に関連するすべてのアラートのリストを含む [アラート（Alerts）] ダッシュボードにアクセスします。

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

オプション名	説明
	[アラート(Alerts)] ダッシュボードの詳細については、「**[アラート(Alerts)] ダッシュボード**」を参照してください。 • [観測(Observations)] を選択して、送信元に関連するすべての観測内容のリストを含む [デバイス別の観測(Observations by Device)] ページにアクセスします。 [デバイス別の観測(Observations by Device)] ページの詳細については、「**デバイス別の観測**」を参照してください。 • [フロー分析(Flow Analysis)] を選択して、送信元に関連するフロー情報を含む [フロー検索結果(Flow Search Results)] ページにアクセスします。 [フロー検索結果(Flow Search Results)] ページの詳細については、「**フロー検索結果:概要**」を参照してください。
ソース IP(Source IP)	イベントが観測されたときの送信元 IP。
送信元ポート(Source Port)	イベントが観測されたときの送信元ポート。
疑わしい接続(Suspect Connections)	異常な外部ソースへの新しい接続、または異常なポート上の接続。
時刻(Time)	観測が行われた時刻。
時間枠(Time Window)	イベントが共有された期間。
転送サイズ(Transfer Size)	転送されたバイト数。
アップロード開始(Upload Start)	外部データシンクへのアップロードの開始時間。
アップロード(秒)(Upload Sec)	アップロードの期間。
アップロード速度(bps)(Upload Speed bps)	bps 単位のアップロード速度。
ユーザー(User)	観測されたイベントに関連付けられたユーザーアカウント。
違反ポート(Violating	送信元によって使用されたポート。

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

オプション名	説明
Port）	
違反プロトコル（Violating Protocol）	送信元によって使用されたネットワークプロトコル（TCP など）。
違反タイプ（Violating Type）	違反のタイプ。

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

優先順位の設定

- [アラートの有効期限設定(Alerts Expiration Configuration)] ページの詳細については、「**有効期限の設定**」を参照してください。
- [アラート:国のウォッチリストの設定(Alerts Country Watchlist Configuration)] ページの詳細については、「**国のウォッチリストの設定**」を参照してください。

アラートステータスの詳細については、「**アラートに関するよくある質問**」を参照してください。このページの詳細については、 ([ユーザー(User)]) アイコンをクリックし、[ヘルプ(Help)] を選択してヘルプにアクセスしてください。

アラートの優先順位設定を開く

メインメニューで、[設定(Configure)] > [アラート(Alerts)] の順に選択します。

または

[アラートの詳細(Alert Details)] ページで、[アラートタイプの詳細(Alert Types Details)] セクションの下部にある [アラートの優先順位ページに移動(Go to Alert Priorities page)] リンクをクリックします。

[アラートの優先順位設定(Alert Priorities Configuration)] ページが開きます。

アラートの優先順位を設定する

このページに表示されるフィールドの説明については、次の表を参照してください。

アラートの詳細については、「**アラートに関するよくある質問**」を参照してください。

フィールド	説明
[アラートタイプ(Alert Type)]	([フィルタ(Filter)]) アイコンをクリックし、アラートのフィルタリングに使用する次のオプションのいずれかを選択します。[次を含む(Contains)]、[次で始まる(Starts with)]、[次で終わる(Ends with)]
履歴(History)	アラートタイプを生成するために必要なデータ収集日数(「ソーク時間」とも呼ばれます)。

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

プライオリティ	アラートはデフォルトで [低(Low)] または [通常(Normal)] に設定されます。アラートの優先順位はアラートタイプによって決まります。[プライオリティ(Priority)] ドロップダウンリストから、任意のアラートタイプを [低(low)]、[通常(normal)]、または [高(high)] に設定できます。また、[優先順位(Priority)] 列ヘッダーの [フィルタ(Filter)] アイコンを使用して、[アラート設定(Alert Settings)] ページを優先順位別にフィルタ処理できます。14 日後にそのアラートに対するアクティビティが発生しない場合、アラートは自動的に閉じます。 アラートの優先順位を変更しても、アラートの公開/未公開には影響しません。未公開のアラートの詳細については、「**[アラート(Alerts)] ダッシュボード**」の「アラートテーブルのフィルタ処理」セクションを参照してください。
有効(Enabled)	アラートを有効にするには、  ([トグル(Toggle)]) アイコンをクリックして、バーを青色()で表示します。
テレメトリ(Telemetry)	[テレメトリ(Telemetry)] 列に、アラートのテレメトリソースが表示されます。観測、ロールなどのテレメトリソースを結合した 1 つ以上のテレメトリソースが含まれている場合があります。アラートは、環境が統合され、そのテレメトリソースを使用している場合にのみ起動されます。
MITRE ATT&CK の戦術(Mitre ATT&CK Tactics)	アラートに関連付けられた MITRE 戦術。この戦術の [MITRE(Mitre)] ページにアクセスするには、[MITRE戦術(Mitre Tactic)] エントリをクリックするか、エントリにカーソルを合わせて、開いたポップアップウィンドウで [次で詳細情報を参照(See Full Details at)] リンクをクリックします。
MITRE ATT&CK の手法(Mitre ATT&CK Techniques)	アラートに関連付けられた MITRE 手法。この手法の [MITRE(Mitre)] ページにアクセスするには、[MITRE手法(Mitre Technique)] エントリをクリックするか、エントリにカーソルを合わせて、開いたポップアップウィンドウで [次で詳細情報を参照(See Full Details at)] リンクをクリックします。

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

有効期限の設定

アラートの有効期限の設定を開く

1. メインメニューで、[設定（Configure）] > [アラート（Alerts）] の順に選択します。

   [アラートの優先順位設定（Alert Priorities Configuration）] ページが開きます。

2. [アラートの優先順位設定（Alert Priorities Configuration）] ページで、[設定（Settings）] サイドメニューから [有効期限（Expiration）] を選択します。

   [アラートの有効期限設定（Alerts Expiration Configuration）] ページが開きます。

アラートの有効期限を設定する

[アラートの有効期限までの日数（Days before alerts expire）] ドロップダウンリストを使用して、アラートが期限切れとしてタグ付けされるまで任意のテーブルに保持される日数を指定します。

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

国のウォッチリストの設定

アラートの国のウォッチリスト設定を開く

1. メインメニューで、[設定（Configure）] > [アラート（Alerts）] の順に選択します。

   [アラートの優先順位設定（Alert Priorities Configuration）] ページが開きます。

2. [アラートの優先順位設定（Alert Priorities Configuration）] ページで、[設定（Settings）] サイドメニューから [国のウォッチリスト（Country Watchlist）] を選択します。

   [アラートの国のウォッチリスト設定（Alerts Country Watchlist Configuration）] ページが開きます。

監視対象国の表示

国のウォッチリストを使用して、このページにリストされている国のアラートをトリガーします。

国のウォッチリストに追加する国ごとに  （[トグル（Toggle）]）アイコンをクリックして、青色のバー（  ）が表示されるようにします。

すべての優先順位をデフォルト設定に戻すには、ページの右上隅にある [すべてをデフォルトにリセット（Reset All to Default）] をクリックします。

© 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。
- シスコサポートにご連絡ください。
- 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

© 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.