Cisco Secure Cloud Analytics

観測およびアラートリファレンスガイド

目次

観測とアラートリファレンスの概要

ここでは、Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）で使用可能な観測およびアラートタイプの概要について説明します。

観測とアラート

Secure Cloud 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 Cloud 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、AWS 展開内の Lambda 関数といった、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 Cloud 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 Cloud 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 Cloud 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。

Secure Cloud Analytics Web ポータル UI でアラートを開くと、システムがアラートを生成し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。

マニュアルの概要

このマニュアルでは、Secure Cloud Analytics によって生成される可能性のある観測結果とアラートのタイプを一覧で紹介します。

「アラートの前提条件」では、アラート生成の基本的な前提条件とともに、ベースライン要件を基に並び替えたアラートを表形式で記載します。

「アラートの説明」では、各アラートについて次の情報を記載します。

- アラートタイプ
- 生成の前提条件
- 関連する観測
- 簡単な説明と、これが悪意のある動作を示す可能性がある理由

「観測の説明」では、各観測タイプについて次の情報を記載します。

- 観測タイプ
- 生成の前提条件
- 関連するアラート
- 簡単な説明

アラートの前提条件と MITRE ATT&CK マッピング

次の表では、特定のアラートタイプを生成するためにどれだけの期間の履歴データが必要か、Cisco Secure Cloud Analytics プライベートネットワークのモニタリング（旧 Stealthwatch Cloud プライベート ネットワーク モニターリング）あるいは 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 モニターリング）を使用して生成されるのかどうか、およびアラート生成に追加の制限や前提条件があるのか（AWS との統合が必要など）について簡潔に説明します。また、アラートタイプに関連付けられている MITER ATT&CK の戦術や手法も記載します。

アラート	プライベートネットワークのモニタリング	パブリッククラウドのモニタリング	履歴	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
ユーザーの不正アクション	○	○	36 日間	永続化	正当なアカウント
アンプ攻撃	○	○	0 日	影響	ネットワークサービス拒否
異常な AWS ワークスペース	×	AWS のみ	14 日間		
異常な Mac ワークステーション	○	○	14 日間		
異常な Windows ワークステーション	○	○	14 日間		
アクティティの中断	○	○	14 日間		
AWS API ウォッチリストの IP ヒット	×	AWS のみ	0 日	検出	Cloud Service Discovery
AWS Config ルール違反	×	AWS のみ	0 日		
AWS コンソールへのログイン失敗	×	AWS のみ	0 日	クレデンシャルへのアクセス	総当たり攻撃
AWS ディテクタの変更	×	AWS のみ	0 日	防御の回避	防御の妨害
AWS Inspector の調査結果	×	AWS のみ	0 日		
AWS Lambda 呼び出し回数の急増	×	AWS のみ	14 日間	影響	リソースのハイジャック
AWS ロギングの削除	×	AWS のみ	0 日	防御の回避	防御の妨害
AWS 多要素認証の変更	×	AWS のみ	0 日	永続化	アカウントの不正操作
AWS 重複サブネット	×	AWS のみ	0 日		
AWS ルートアカウントの使用	×	AWS のみ	0 日	永続化	正当なアカウント
AWS 一時的トークンの永続性	×	AWS のみ	0 日	永続化	正当なアカウント
Azure アクティビティログ IP ウォッチリストのヒット	×	Azure のみ	0 日	検出	Cloud Service Discovery
Azure アクティビティ ログ ウォッチリストのヒット	×	Azure のみ	0 日		

アラート	プライベートネットワークのモニタリング	パブリッククラウドのモニタリング	履歴	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
Azure Advisor ウォッチリスト	×	Azure のみ	0 日		
制限の緩い Azure セキュリティグループ	×	Azure のみ	0 日		
制限の緩い Azure ストレージアカウント	×	Azure のみ	0 日		
セキュリティイベント	×	Azure のみ	0 日		
未使用の場所にある Azure 仮想マシン	×	Azure のみ	0 日	影響	リソースのハイジャック
CloudTrail ウォッチリストのヒット	×	AWS のみ	0 日		
脅威ウォッチリストのヒットを確認	拡張 NetFlow が必要	拡張 NetFlow が必要	0 日	指揮統制	アプリケーション層プロトコル
国のセットからの逸脱	○	○	36 日間		
DNS の悪用	○	○	0 日	漏洩	代替プロトコルによるデータ漏洩
ドメイン生成アルゴリズム成功の観測	DNS ログが必要	×	0 日	指揮統制	動的なアドレス解決
電子メールスパムアラート	○	○	36 日間	漏洩	代替プロトコルによるデータ漏洩
新たなプロファイル	○	○	14 日間	漏洩	代替プロトコルによるデータ漏洩
Empire コマンドアンドコントロール	○	○	1 日		
例外的なドメインコントローラ	○	○	7 日間		
過剰アクセス試行回数（外部）	○	○	0 日	クレデンシャルへのアクセス	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		
GCP Cloud 関数呼び出し回数の急増	×	GCP のみ	14 日間	影響	リソースのハイジャック
GCP Stackdriver ロギングウォッチリストのヒット	×	GCP のみ	0 日		
地理的に異常な AWS API の使用	×	AWS のみ	14 日間	検出	Cloud Service Discovery
地理的に異常な Azure API の使用	×	Azure のみ	14 日間	検出	Cloud Service Discovery
地理的に異常なリモートアクセス	○	○	14 日間	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	指揮統制	非アプリケーション層プロトコル

アラート	プライベートネットワークのモニタリング	パブリッククラウドのモニタリング	履歴	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
広帯域幅での単方向トラフィック	○	○	0 日	漏洩	データ自動漏洩
新たな IDS プロファイル	Firepower アプライアンスまたは Suricata IDS とシスコのセキュリティ分析とロギング（SaaS）の連携が必要	Firepower アプライアンスまたは Suricata IDS とセキュリティ分析とロギング（SaaS）の連携 が必要	14 日間		
IDS 通知の急増	Firepower アプライアンスまたは Suricata IDS とセキュリティ分析とロギング（SaaS）の連携 が必要	Firepower アプライアンスまたは Suricata IDS とセキュリティ分析とロギング（SaaS）の連携 が必要	1 日		
インバウンドポートスキャナ	○	○	1 日	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	検出	ネットワークサービスのスキャン
内部接続ウォッチリストのヒット	○	○	0 日		
内部ポートスキャナ	○	○	7 日間	検出	ネットワークサービスのスキャン
マルウェアの急増	Firepower アプライアンスまたは Suricata IDS とシスコのセキュリティ分析とロギング（SaaS）の連携が必要	Firepower アプライアンスまたは Suricata IDS とシスコのセキュリティ分析とロギング（SaaS）の連携が必要	1 日		
Sumo Logic ログの欠落	Sumo Logic が必要	×	0 日		
NetBIOS 接続のスパイク	○	○	7 日間	侵入拡大の動き	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		
ネットワークプリンタの過剰な接続回数	○	○	0 日		
新しい AWS リージョン	×	AWS のみ	0 日	防御の回避	未使用/サポートされていないクラウドリージョン
新しい AWS Route53 ターゲット	×	AWS のみ	0 日		
新しい外部接続	○	○	35 日間		
新しい内部デバイス	○	○	21 日間		
新しい IP スキャナ	○	○	7 日間	検出	ネットワークサービスのスキャン
新たな長時間セッション（地理的）	○	○	2 日間		
新しいリモートアクセス	○	○	36 日間	最初のアクセス	外部リモートサービス

アラート	プライベートネットワークのモニタリング	パブリッククラウドのモニタリング	履歴	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
新しい SNMP スイープ	○	○	7 日間	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		
非サービスポートスキャナ	○	○	9 日間		
アウトバウンド SMB スパイク	○	○	0 日	侵入拡大の動き	リモートサービス
アウトバウンドトラフィックの急増	○	○	14 日間	漏洩	データ自動漏洩
制限の緩い AWS S3 アクセス制限リスト	×	AWS のみ	0 日	収集	クラウド ストレージ オブジェクトからのデータ
制限の緩い AWS セキュリティグループの作成	×	AWS のみ	0 日		
持続的なリモートコントロール接続	○	○	7 日間	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	漏洩	データ自動漏洩
データベース漏洩の疑い	○	○	7 日間	漏洩	代替プロトコルによるデータ漏洩
隠しファイル拡張子の潜在的有害性	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	0 日	実行	ユーザーによる実行
リモート制御プロトコルの潜在的脆弱性	拡張 NetFlow が必要	拡張 NetFlow が必要	1 日		
プロトコル偽造	拡張 NetFlow が必要	拡張 NetFlow が必要	1 日	指揮統制	非標準ポート
プロトコル違反（地理的）	○	○	0 日	指揮統制	アプリケーション層プロトコル
Amazon Route 53 パブリックホストゾーンの作成	×	AWS のみ	0 日		
パブリック IP ウォッチリストとの一致	○	○	0 日		
パブリック IP サービスのルックアップ	Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）またはセキュリティ分析とロギング（SaaS）が必要	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	2 日間		
リモートアクセス（地理的）	○	○	0 日		
ウォッチリスト通信の繰り返し	○	○	0 日	指揮統制	アプリケーション層プロトコル
ロール違反	○	○	0 日	永続化	システムプロセスの作成または変更

アラート	プライベートネットワークのモニタリング	パブリッククラウドのモニタリング	履歴	MITRE ATT&CK の戦術	MITRE ATT&CK の手法
SMB 接続のスパイク	○	○	7 日間	侵入拡大の動き	リモートサービス
古い AWS アクセスキー	×	AWS のみ	30日間		
静的デバイス接続の逸脱	○	○	1 日		
静的デバイスの逸脱	○	○	35 日間		
ボットネット インタラクションの疑い	○	○	1 日	指揮統制	アプリケーション層プロトコル
疑わしい暗号通貨アクティビティ	○	○	0 日	影響	リソースのハイジャック
悪意のあるURLの疑い	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	0 日	最初のアクセス	Web 閲覧による感染
フィッシングドメインの疑い	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	シスコのセキュリティ分析とロギング（SaaS）の連携が必要	0 日	最初のアクセス	Web 閲覧による感染
ポート悪用の疑い（外部）	○	○	1 日	検出	ネットワークサービスのスキャン
Zerologon RBC エクスプロイト試行の疑い	○	○	0 日	特権昇格	特権昇格の悪用
疑わしいドメインルックアップの失敗	DNS ログが必要	×	0 日	指揮統制	動的なアドレス解決
疑わしい SMB アクティビティ	○	○	14 日間	侵入拡大の動き	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	指揮統制	アプリケーション層プロトコル
TrickBot AnchorDNS トンネリング	×	AWS のみ	14 日間		
未使用の AWS リソース	×	AWS のみ	14 日間		
異常な DNS 接続	○	○	1 日		
異常な外部サーバー	○	○	14 日間	指揮統制	アプリケーション層プロトコル
ユーザーウォッチリストのヒット	○	○	0 日		
トランスポート セキュリティ プロトコルの脆弱性	拡張 NetFlow が必要	拡張 NetFlow が必要	1 日		
ウォッチリストのヒット	○	○	0 日		

アラートの説明

ユーザーの不正アクション

説明：通常時にこのユーザーとのセッションが確認されていないエンティティで、ユーザーセッションが作成されました。新しいユーザーセッションは、悪意のあるアクティビティ、または定期的な繰り返しセッションは確立されていないが、予測されるユーザーを示している可能性があります。

前提条件：このアラートでは、エンティティとセッションを確立することが予測される一般的なユーザーであると確定するために、36 日間の履歴が必要です。また、ユーザーの属性値を取得するために、ISE との統合も必要です。

関連する観測：セッションオープンの観測

次の手順：このアラートに関して裏付けとなる観測結果を参照して、どのユーザーアカウントでいつエンティティにログインされたかを特定します。ユーザーに連絡して、ユーザーが実行していたアクションを特定します。不正なアクションの場合は、追加の調査を行います。ユーザー自身がログインしていなかった場合、エンティティが認識されていない場合、または信頼できない外部ネットワークからのログインの場合は、ブロックリストとファイアウォールルールを更新して、悪意のあるユーザーがネットワークにアクセスするのを防ぎます。ユーザーがエンティティに対して行ったアクションを特定し、悪影響の可能性があれば是正処置を講じます。ユーザーによるデータ漏洩の場合は、送信されたデータを特定し、データ損失に関する組織のガイドラインに従います。

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。

関連する観測：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 AWS ワークスペース

説明：AWS 仮想ワークスペース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。

関連する観測：異常なプロファイルの観測

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。

異常な Mac ワークステーション

説明：Apple Mac 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。

関連する観測：異常なプロファイルの観測

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。

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。

関連する観測：異常なプロファイルの観測

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。

アクティビティの中断

説明：このエンティティは、通常は 1 日の大半でアクティブ状態ですが、エンティティのアクティビティが複数のプロファイル（SSH サーバー、FTP サーバーなど）で中断しています。このような動作は、エンティティの計画的なダウンタイムやメンテナンスを示す可能性がありますが、エンティティの機能キャパシティに影響を与えるマルウェア、またはエンティティに何らかの影響を与える他の悪意のある動作を示す可能性もあります。

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。

関連する観測：履歴に基づく異常値の観測

次の手順：裏付けとなる観測結果を参照して、エンティティの役割を特定し、アクティビティの中断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。アクティビティの中断に正当な理由がない場合は、エンティティを調べて、何者かがシャットダウンしたかどうか、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。

AWS API ウォッチリストの IP ヒット

説明：ウォッチリストに登録されている IP から AWS API にアクセスされました。Secure Cloud Analytics ウォッチリスト上のエンティティが AWS 環境の API にアクセスした場合は、リソースに悪意を持ってアクセスを試みたことを示している可能性があり、さらに詳しい調査が必要です。

前提条件：このアラートには、AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS API ウォッチリストのアクセスの観測

次の手順：AWS API にアクセスしたエンティティと、エンティティが呼び出した API 関数を調査します。アクセスにより悪意のあるアクティビティが引き起こされたかどうか、その悪意のあるアクティビティが継続中かどうかを判断し、アクティビティを修正します。AWS のセキュリティ設定を確認し、不正アクセスを防止するための適切な予防措置を講じていることを確認します。悪意のあるアクセスの場合は、ファイアウォールルールを更新してエンティティをブロックします。

AWS Config ルール違反

説明：AWS Config ルールに違反しました。設定変更が AWS の設定ルールに違反している場合は、変更内容を調べ、設定ルールに従って設定を更新する必要があります。

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、AWS との統合、設定変更を SNS トピックにストリーミングするための AWS の設定、設定変更を送信するための SQS キュー、およびメッセージを取得するための Secure Cloud Analytics での追加設定が必要です。

関連する観測：AWS Config 遵守の観測

次の手順：アラートと裏付けとなる観察結果を参照して、どの AWS リソースが設定変更と Config ルール違反の原因であるかを判断します。AWS Config ルールを更新せずに必要な設定変更など、設定の変更がビジネスの過程で予測され、正当であるかどうかを調べます。予期しない変更の場合は、変更を元に戻してログを確認し、どのユーザーまたはセッションが変更したのかを判断します。

AWS コンソールへのログイン失敗

説明：ユーザーが AWS コンソールへのログインを数回試みて失敗しました。ユーザーが AWS コンソールへのログインに繰り返し失敗した場合、権限のないユーザーがアクセスを試みているか、ユーザーがログイン情報を忘れ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、AWS との統合が必要です。また、IAM ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測

次の手順：ログインに失敗したユーザーのアカウントを特定します。裏付けとなる観測結果を参照して、ネットワーク上の認識しているエンティティでログインが実行されたのかを判断します。認識していないエンティティからのログインである場合は、悪意のあるエンティティであるかをさらに調査します。調査結果が出るまでユーザーのログイン情報をリセットまたはロックします。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、悪意のある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。

ログイン要求を送信したエンティティを認識している場合は、ユーザーに連絡して、ログイン情報を忘れていないかを判断します。ログイン情報を忘れた場合はリセットします。ユーザーがログイン情報を忘れておらず、他の誰かがそのユーザーとしてログインを試みている場合は、ユーザーのログイン情報をリセットまたはロックして、ネットワーク上の悪意あるユーザーの特定を試みます。エンティティのネットワークへの接続を切断し、エンティティがマルウェアに感染しているかどうか、あるいは悪意のあるユーザーがマルウェアを介してリモートアクセスしたかどうかを判断します。

AWS ディテクタの変更

説明：AWS GuardDuty ディテクタが削除または無効化されました。このアラートは、悪意のあるアクティビティの検出を回避しようと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。このアラートには AWS との統合、および GuardDuty の有効化が必要です。

関連する観測：AWS CloudTrail イベントの観測

次の手順：GuardDuty ディテクタを再度有効にして、GuardDuty を再度有効にします。ログを確認して、GuardDuty ディテクタがどのように削除または無効化されたかを判断します。これが悪意のある動作によるものである場合は、ファイアウォールルールとセキュリティ設定を更新して、アクセスを防止します。

AWS Inspector の調査結果

説明：AWS Inspector がエンティティに関する重大度の高い調査結果を報告しました。このアラートに必要な履歴期間は、0 日間です。Inspector による重大度の高い調査結果は、できる限り迅速な是正処置を要する重要なセキュリティおよびコンプライアンスの調査結果であることを示しています。

前提条件：このアラートには AWS との統合、および Inspector の有効化が必要です。

関連する観測：Amazon Inspector 調査結果の観測

次の手順：AWS Inspector で調査結果を確認し、適切な是正処置を講じます。

AWS Lambda 呼び出し回数の急増

説明：Lambda 関数が非常に多くの回数呼び出されました。Lambda 関数のアクティビティの急増は、Lambda の設定不備など、悪意のない動作が原因である可能性があります。また、悪意のあるユーザーがリソースを占有するために関数を繰り返し呼び出すなど、悪意のある動作が原因である可能性もあります。

前提条件：このアラートでは、Lambda 関数の実行頻度のメトリックを確立するために 14 日間の履歴が必要です。また、AWS との統合、および AWS に少なくとも 1 つの Lambda 関数も必要です。

関連する観測：AWS Lambda メトリック外れ値の観測

次の手順：Lambda 関数の呼び出し回数が原因でネットワークに問題が発生している場合は、調査結果が出るまで Lambda 関数を一時的に無効にします。

AWS Lambda 関数を呼び出すために必要な条件と、Lambda 関数が複数回トリガーされた理由を確認し、これが繰り返されないように条件を修正します。外部の悪意のあるエンティティによって Lambda 関数がトリガーされた場合は、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、このエンティティがネットワークにアクセスできないようにします。これにより Lambda 関数の欠陥が明らかになった場合は、Lambda 関数のロジックを更新します。

AWS ロギングの削除

説明：AWS VPC フローログまたは CloudTrail ログが削除されました。このアラートは、悪意のあるアクティビティの履歴を削除しようと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。このアラートには AWS との統合、および VPC フローロギングまたは CloudTrail ロギングの有効化が必要です。

関連する観測：AWS CloudTrail イベントの観測

次の手順：ログ情報を削除したユーザーまたはプロセスを特定し、ログ削除の前後にユーザーまたはプロセスが実行した可能性のある他のアクションを特定します。これが悪意のある動作によるものである場合は、ファイアウォールルールとセキュリティ設定を更新して、今後のアクセスを防止します。

AWS 多要素認証の変更

説明：多要素認証がユーザーアカウントから削除されました。多要素認証の削除は、セキュリティのベストプラクティスに違反します。

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 AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測、AWS 多要素認証の変更の観測

次の手順：組織のセキュリティ要件に従い、必要に応じてアカウントを無効にします。多要素認証を削除したユーザーとその理由を特定します。ユーザーが多要素認証デバイスの 1 つを紛失したために削除した場合は、デバイスを交換して多要素認証をリセットします。

悪意のあるユーザーが多要素認証を削除した場合は、アカウントを無効にしてログイン情報をリセットします。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、この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。

AWS 重複サブネット

説明：新しい AWS サブネットには、既存のサブネットと重複する CIDR があります。これは、Amazon のベストプラクティスに違反しています。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測、AWS Config 更新の観測

次の手順：AWS サブネットを更新して、IP アドレスの重複を削除します。

AWS ルートアカウントの使用

説明：AWS ルートアカウントを使用してアクションが実行されました。AWS が推奨するベストプラクティスは、タスクの実行に必要な権限のみをユーザー作成アカウントに割り当てて、不要な場合はルートアカウントを使用しないことです。

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 AWS との統合が必要です。

関連する観測：AWS CloudTrail イベントの観測、AWS ルートアカウント使用の観測

次の手順：ユーザーまたはロールにルートレベルの権限が必要かどうかを判断します。必要ない場合は、設定を更新して AWS ルートアカウントの使用を制限します。

AWS 一時的トークンの永続性

説明：AWS Security Token Service のログイン情報などの一時的なクレデンシャルが、永続化と防御の回避に使用される可能性があります。一時的なクレデンシャルの作成は、AWS サービス自体とユーザーの両方によって実行される非常に一般的で正当なアクションですが、他の一時的なクレデンシャルによって一時的なクレデンシャルが作成された場合は、不正の疑いがあります。また、一時的なクレデンシャルの作成は、ほとんどの AWS 環境であまり一般的ではありません。

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 AWS との統合が必要です。

関連する観測：AWS CloudTrail イベントの観測

次の手順：すべての `sts:*` 権限、特に `AssumeRole` と `GetFederationToken` の IAM ポリシーを確認し、最小権限の原則を適用します。必要に応じて、EC2 および ECS メタデータ API へのアクセスを制限します。

Azure アクティビティログ IP ウォッチリストのヒット

説明：Azure アクティビティログで、ユーザー定義のウォッチリストまたは統合型のウォッチリスト上の IP アドレスによって開始されたイベントが報告されました。これは、権限のないユーザーが Azure にアクセスした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 Azure との統合が必要です。また、Secure Cloud Analytics で Azure アクティビティログのウォッチリストを設定する必要があります。

関連する観測：Azure 異常アクティビティの観測

次の手順：ウォッチリストのエントリが正しいことを確認します。裏付けとなる IP アドレスの観測結果を参照し、悪意のある動作かどうかを判断します。悪意のある動作の場合は、アクティビティを修正します。Azure のセキュリティ設定を確認し、不正アクセスを防止するための適切な予防措置を講じていることを確認します。悪意あるアクセスの場合は、ファイアウォールルールを更新して IP アドレスをブロックします。

Azure アクティビティ ログ ウォッチリストのヒット

説明：Azure アクティビティログで、ユーザー定義のウォッチリスト上のイベントが報告されました。Secure Cloud Analytics ウォッチリスト上のエンティティが Azure 環境にアクセスした場合は、リソースに悪意を持ってアクセスを試みたことを示している可能性があり、さらに詳しい調査が必要です。

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 Azure との統合が必要です。また、Secure Cloud Analytics で Azure アクティビティログのウォッチリストを設定する必要があります。

関連する観測：Azure 異常アクティビティの観測

次の手順：ウォッチリストのエントリが正しいことを確認します。エンティティのトラフィックプロファイルについての裏付けとなる観測結果を参照し、悪意のある動作かどうかを判断します。悪意のある動作の場合は、アクティビティを修正します。Azure のセキュリティ設定を確認し、不正アクセスを防止するための適切な予防措置を講じていることを確認します。悪意のあるアクセスの場合は、ファイアウォールルールを更新してエンティティをブロックします。

Azure Advisor ウォッチリスト

説明：ウォッチリスト上の推奨タイプに対して Azure Advisor の推奨事項が検出されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには Azure との統合、および Azure Advisor が必要です。

関連する観察：Azure Advisor 推奨事項の観測

次の手順：関連する Azure Advisor の推奨事項を確認し、推奨事項に基づいてアクションを実行します。

制限の緩い Azure セキュリティグループ

説明：ネットワーク セキュリティ グループは、Azure Security Center によって許容度が高すぎると判定されました。これは、インバウンドルールで「任意」または「インターネット」範囲からのアクセスが許可されている場合、または許可されたポート範囲が過度に許容的になっている場合に発生する可能性があります。これらのルールを強化すると、攻撃者がリソースを簡単に標的にするのを防ぐことができます。

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 Azure との統合、および少なくとも 1 つのネットワーク セキュリティ グループが必要です。

関連する観測：制限の緩い Azure セキュリティグループの観測

次の手順：Azure のネットワーク セキュリティ グループのアクセス権を調べ、許可されたユーザーまたはドメインのみにアクセス権を制限します。必要に応じてポート範囲を制限します。

制限の緩い Azure ストレージアカウント

説明：Azure Security Center によって、ファイアウォールが設定が無制限のストレージアカウントと識別されました。これは、保存データへの不正アクセスにつながる可能性があります。許可されたネットワークまたは IP アドレス範囲のアプリケーションのみがストレージアカウントにアクセスできるように、ネットワークルールを設定することをお勧めします。

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 AWS との統合、および少なくとも 1 つのストレージアカウントが必要です。

関連する観測：制限の緩い Azure ストレージ設定の観測

次の手順：Azure のストレージアカウントのアクセス権を調べ、許可されたユーザーまたはドメインのみにアクセス権を制限します。必要に応じてポート範囲を制限します。

セキュリティイベント

説明：Azure Security Center によって、重大度が中または高のイベントが報告されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには、Azure との統合、Azure Security Center、標準層、および Azure アクティビティログが必要です。

関連する観測：Azure セキュリティイベントの観測

次の手順：裏付けとなる観測結果を参照して、重要度が中または高のイベントを特定します。Azure Security Center にログインしてイベントを確認し、必要に応じて是正処置を講じます。

未使用の場所にある Azure 仮想マシン

説明：Azure 仮想マシンが、以前に使用されていない場所に作成されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには Azure との統合が必要です。また、Azure サブスクリプションを確認するために、Secure Cloud Analytics にモニターリングリーダーロール権限を付与する必要があります。

関連する観察：未使用の場所における Azure VM の観測

次の手順：裏付けとなる観測結果を確認して、仮想マシンとその場所を特定します。悪意のある仮想マシン作成の可能性がある場合は、仮想マシンをシャットダウンし、必要に応じて是正処置を講じます。

CloudTrail ウォッチリストのヒット

説明：AWS CloudTrail によって、ユーザーが定義したウォッチリスト上のイベントが報告されました。このアラートに必要な履歴期間は、0 日間です。このアラートが生成された場合、AWS アカウントのイベントに焦点を当てるように CloudTrail ウォッチリストをカスタマイズして、追加の調査を実行できます。

前提条件：このアラートには、AWS との統合、CloudTrail ログを読み取るための Secure Cloud Analytics アクセス権の付与、および Secure Cloud Analytics Web UI における AWS CloudTrail ウォッチリストの設定が必要です。

関連する観測：AWS CloudTrail イベントの観測

次の手順：報告されたイベントとアラートの裏付けとなる観測結果を参照します。悪意のある動作かどうかを判断し、さらに調査する必要があります。

脅威ウォッチリストのヒットを確認

説明：このエンティティは、既知の脅威に関係している外部リソースと通信しました。このアラートは暗号化トラフィック分析 機能の一部です。拡張 NetFlow をベースとする脅威インテリジェンスを使用すると、ネットワークへの脅威に関する更なる洞察を得ることができます。

前提条件：このアラートに必要な履歴期間は 0 日間です。脅威インジケーターの一致を確認 – ホスト名の観測および脅威インジケーターの一致を確認 – URL の観測の結果の裏付けには拡張 NetFlow が必要です。詳細については、『Secure Cloud AnalyticsConfiguration Guide for Enhanced NetFlow』を参照してください。

関連する観測：脅威インジケーターの一致を確認 – ホスト名の観測、脅威インジケーターの一致を確認 – IP の観測、脅威インジケーターの一致を確認 – ドメインの観測、脅威インジケーターの一致を確認 – URL の観測

次の手順：既知の脅威のタイプ（ドメイン名、ホスト名、IP アドレス、悪意のある URL）のアラートと裏付けとなる観測結果を参照します。既知の脅威に基づき、必要に応じて是正処置を講じます。ファイアウォールルールを更新して、既知の脅威との間でアクセスを防止します。

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。

関連する観測：対象国の逸脱の観測

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。

DNS の悪用

説明：このエンティティは、非常に大きな DNS パケットを送信しています。これは、データ転送を DNS トラフィックであるかのように偽装している可能性があります。たとえば、マルウェアが原因で、エンティティが攻撃者の制御下にあるリモートサーバーに機密情報を送信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。

関連する観測：異常なパケットサイズの観測

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 DNS パケットを送信している DNS サーバーを特定します。正当な DNS サーバーの場合は、サブネット設定の VPN サブネットに追加して、誤検出アラート数を減らします。エンティティが大量の DNS パケットを送信している理由をさらに調査します。正当でない DNS サーバーの場合は、エンティティのログを確認し、エンティティが DNS パケットを送信している理由と、それが悪意のある動作であるかを判断します。悪意のある動作があれば、是正処置を講じます。また、今後の悪意ある動作を防ぐために、必要に応じてファイアウォールルールを更新します。

ドメイン生成アルゴリズム成功の観測

説明：エンティティは、アルゴリズムによって生成されたドメイン（rgkte-hdvj.cc など）を IP アドレスに正しく解決しました。これは、マルウェア感染、生成されたドメインでコマンドアンドコントロール サーバーを使用したボットネット作成の試み、またはその他のボットネットアクティビティ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、SPAN、ミラーポート、または拡張 NetFlow からの DNS ログが必要です。

関連する観測：ドメイン生成アルゴリズム成功の観測

次の手順：裏付けとなる観測結果に記載されているドメインを参照し、ドメインルックアップが正当な目的か不正目的かを判断します。不正目的の場合は、ルックアップを生成したソフトウェアを特定します。ドメイン生成アルゴリズム成功の観測を確認し、他のエンティティが疑わしい呼び出しを行っているかどうかを判断します。

電子メールスパムアラート

説明：このエンティティと外部メールサーバーとの接続が異常に増加しています。これは、ボットネットマルウェア、データ漏洩の試み、スパムメールを送受信するマルウェアなどの侵害タイプの悪意のある動作を示す可能性があります。

前提条件：このアラートでは、エンティティモデルと予想されるトラフィックプロファイルを確定するために、36 日間の履歴が必要です。

関連する観測：外部メールクライアント接続の観測、履歴に基づく異常値の観測、新しい外部接続の観測

次の手順：裏付けとなる観測結果を参照し、外部メールサーバーが予測された正当なものであるかどうかを判断します。予測された正当なサーバーの場合、エンティティとサーバーとの間でトラフィックが増加した理由を特定します。それ以外の場合は、悪意のある動作の原因を特定します。影響を受けるエンティティを検疫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同様の影響を受けていないかを確認します。

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。

関連する観測：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。

関連する観測：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。

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。

関連する観測：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。

関連する観測：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。

関連する観測：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。

GCP Cloud 関数呼び出し回数の急増

説明：GCP クラウド関数が非常に多くの回数呼び出されました。

前提条件：このアラートでは、関数が呼び出される頻度を判断するために 14 日間の履歴が必要です。また、GCP との統合も必要です。

関連する観測：GCP クラウド関数メトリックの外れ値の観測

次の手順：GCP クラウド関数と目的のコードを確認します。関数が破損しているかどうか、または追加の環境要因によって関数の動作が変化したかどうかを判断します。呼び出しの急増に問題のない場合は、アラートをスヌーズすることをお勧めします。

GCP Stackdriver ロギングウォッチリストのヒット

説明：Google Cloud Platform（GCP）Stackdriver ログで、ユーザ定義のウォッチリスト上のイベントが報告されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには GCP との統合、および Stackdriver ログにアクセスするための Secure Cloud Analytics 権限の付与も必要です。

関連する観測：GCP ウォッチリスト 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確認して、イベントを生成したウォッチリストのエントリを特定し、必要に応じて是正処置を講じます。また、GCP にログインし、必要に応じてウォッチリストを更新します。

地理的に異常な AWS API の使用

説明：AWS AWS に対して、通常はこの API 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、一般的でない海外の IP からクラウドコンソールにアクセスすると、このアラート

がトリガーされます。ユーザーが予期しない地理的場所から AWS API にアクセスしている場合、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：このアラートでは、AWS 環境の API にアクセスする IP アドレスの通常の地理位置情報を確定するために、14 日間の履歴が必要です。また、AWS との統合、および CloudTrail ログを読み取るための Secure Cloud Analytics アクセス権の付与が必要です。

関連する観測：AWS CloudTrail イベントの観測

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。予期されるエンティティであるが、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、ユーザーの ID が侵害されていないことを確認し、そのエンティティが移動している間、エンティティのアラートをスヌーズします。ユーザーの ID が侵害された場合は、そのユーザーアカウントをすぐに無効にします。

地理的に異常な Azure API の使用

説明：Azure API に対して、通常はこの API 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、一般的でない海外の IP から IAM ロールを作成すると、このアラートがトリガーされます。ユーザーが予期しない地理的場所から Azure API にアクセスしている場合、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：このアラートでは、Azure 環境の API にアクセスする IP アドレスの通常の地理位置情報を確定するために、14 日間の履歴が必要です。このアラートには Azure との統合も必要です。

関連する観察：Azure の通常と異なる推奨事項の観測

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。予測されるエンティティの場合、これが 1 回限りのアクセスの場合はアラートを閉じます。通常と異なるアクセスが一定期間予測される場合はアラートをスヌーズします。悪意のあるアクセスの場合は、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更新して、今後のアクセスを防止します。また、システムで実行されたアクションを特定して、是正処置を講じます。

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、14 日間の履歴が必要です。

関連する観測：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。

関連する観測：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。

関連する観測：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。許容範囲内のトラフィックの場合は、このホストのアラートをスヌーズします。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。

新たな IDS プロファイル

説明：このエンティティで新しいタイプのトラフィックが確認されましたが、IDS によって疑わしいトラフィックとしてフラグが付けられています。

前提条件：このアラートでは、エンティティがさまざまなトラフィックタイプの送信を開始するタイミングを判断するのに適したエンティティモデルを確立するために、14 日間の履歴が必要です。このアラートには、次のいずれかが必要です。

- セキュリティ分析とロギング（SaaS）Cisco Defense Orchestrator を介して Firepower アプライアンスと統合された詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。
- Suricata IDS

関連する観測：侵入検知システム通知の観測、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プロファイルの詳細を参照し、新しいトラフィックプロファイルが悪意のあるものかどうかを判断します。悪意のある場合は、ホストを検疫して問題のあるソフトウェアを削除します。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。

IDS 通知の急増

説明：このエンティティにより、IDS での検知数が急激に増加しました。

前提条件：このアラートでは、通常の IDS 報告動作を確定するために、1 日間の履歴が必要です。このアラートには、次のいずれかが必要です。

- セキュリティ分析とロギング（SaaS）Cisco Defense Orchestrator を介して Firepower アプライアンスと統合された詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。
- Suricata IDS
- Zeek IDS

関連する観測：侵入検知システム通知の観測

次の手順：裏付けとなる観測結果を参照して、エンティティとエンティティが多数の通知をトリガーした理由を特定します。IDS 通知を確認して、是正処置を講じます。また、他のエンティティが影響を受ける可能性があるかどうかを判断します。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。

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。

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。

関連する観測：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。

関連する観測：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。

内部接続ウォッチリストのヒット

説明 ：通信すべきではない 2 つの IP アドレスがデータを交換していることが確認されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連する観測：内部接続ウォッチリストの観測

次の手順：裏付けとなる観測結果を参照して一致したウォッチリストルールを特定し、フローの詳細を分析します。許容される接続の場合は、ウォッチリストルールを更新して接続を許可します。

このアラートは、ユーザーがセグメンテーションルールを入力している場合にのみ生成されます。

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。

関連する観測：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。

マルウェアの急増

説明：このエンティティにより、IDS での検知数が急激に増加しました。

前提条件：このアラートでは、通常の IDS 報告動作を確定するために、1 日間の履歴が必要です。また、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合も必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連する観測：マルウェアイベントの観測

次の手順：裏付けとなる観測結果を参照して、エンティティとエンティティが多数のマルウェアイベントをトリガーした理由を特定します。マルウェアイベントを確認して是正処置を講じます。また、他のエンティティが影響を受ける可能性があるかどうかを判断します。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。

Sumo Logic ログの欠落

説明：このロールを持つエンティティに必要な 1 つ以上のログが Sumo Logic データベースで見つかりませんでした。これは、Sumo Logic コレクタの 1 つが正しく設定されていないか、欠落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。また、Sumo Logic の導入が必要です。

関連する観測：Sumo Logic ログの観測

次の手順：Sumo Logic コレクタを調査し、コレクタの設定を確認します。Sumo Logic コレクタをネットワークで検出できない場合は、再導入するか、接続を確認します。

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、7 日間の履歴が必要です。

関連する観測：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。

関連する観測: 利用者数急増の観測

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。

関連する観測: 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: 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 AWS リージョン

説明: 以前に使用されていなかったリージョンで AWS リソースが検出されました。

前提条件: このアラートに必要な履歴期間は 0 日間です。このアラートには AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測: AWS CloudTrail イベントの観測

次の手順: AWS リソースを特定し、それが AWS 環境で予測されているリソースかどうかを判断します。予測されていない AWS リソースの場合は、必要に応じて修正します。AWS CloudTrail イベントの観測結果を参照して、リソースを作成および設定したユーザーに関する詳細を確認します。

新しい AWS Route53 ターゲット

説明: 新しい AWS Route53 リソースレコードが、これまで Route53 リソースレコードに関連付けられていなかったエンティティに割り当てられました。このアラートに必要な履歴期間は、0 日間です。新しい Route53 リソースレコードは、エンティティのトラフィックを悪意を持ってリダイレクトしようと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 0 日間です。このアラートには AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測: AWS CloudTrail イベントの観測

次の手順: アラートと裏付けとなる観測結果を参照して、エンティティに関する情報を収集し、ネットワーク上の意図されたイベントかどうかを確認します。AWS のログを確認して、エンティティが示している動作を特定します。予測されたエンティティの場合は、エンティティを許可するように設定を更新します。

新しい外部接続

説明: ベースライン期間中、エンティティは組織外で双方向に通信することはありませんでしたが、ベースライン期間後に初めて双方向通信を行いました。これは、逸脱動作です。

前提条件: このアラートでは、トラフィックモデルを確定し、予測されるトラフィック動作を判別するために、35 日間の履歴が必要です。

関連する観測：新しい外部接続の観測

次の手順：裏付けとなる観測結果とトラフィックフローの詳細を参照して、正当なトラフィックかどうかを判断します。一部の非常に静的なエンティティは、外部 IP を呼び出すことがあります（ソフトウェアの更新をチェックするプリンターなど）。この場合、アラートをスヌーズするか、その外部 IP 範囲を VPN サブネットに追加します。

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。

関連する観測：新しい内部デバイスの観測

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、7 日間の履歴が必要です。

関連する観測：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。

新たな長時間セッション（地理的）

説明：このエンティティは、ウォッチリストに登録された国と長時間にわたって接続を確立しました。この接続は、ウォッチリストに登録された国のユーザーによる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：このアラートでは、長時間にわたり確立された接続を確定するために、2 日間の履歴が必要です。Secure Cloud Analytics Web ポータル UI で、国のウォッチリストに追加する国を設定できます。

関連する観測：長時間セッションの観測

次の手順：裏付けとなる観測結果を参照して、トラフィックフローの詳細を確認します。IP アドレスのメニューから **Talos Intelligence** と **AbuseIPDB** を選択して、外部 IP アドレスのレピュテーションを調査します。外部 IP に悪意があると思われる場合は、ホストマシンを調査するか、セキュリティグループまたはファイアウォールルールを使用してトラフィックをブロックします。

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。

関連する観測：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、7 日間の履歴が必要です。

関連する観測：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ウォッチリストに追加するかアラートをスヌーズします。

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。

関連する観測：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。悪意のあるトラフィックと判断した場合は、外部 IP アドレスをブロックします。予想されるトラフィックの場合はアラートをスヌーズします。

非サービスポートスキャナ

説明：デバイスが、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、攻撃者がネットワーク内に存在し、脆弱性を探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、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、9 日間の履歴が必要です。

関連する観測：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。

関連する観測：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。

アウトバウンドトラフィックの急増

説明：観測対象が、以前よりもはるかに大量のトラフィックを外部の接続先に送信し始めました。これまで見られなかった大量トラフィックの急増は、データ漏洩などの悪意のある動作を示す可能性があります。この動作に悪意がない場合でも、調査が必要になる場合があります。

前提条件：このアラートでは、このエンティティが送信するトラフィックの通常レベルを示すのに十分な情報量を持つエンティティモデルを確立するために、14 日間の履歴が必要です。

関連する観測：履歴に基づく異常値の観測、異常測定値の観測、レコードプロファイルの異常値の観測、新しい大規模接続（外部）の観測

次の手順：裏付けとなる観測結果を参照して、トラフィックの性質と送信先を判断します（例：大規模な Dropbox アップロード）。疑わしいトラフィックの場合は、ユーザーまたはマシンの所有者に連絡して、トラフィックが外部に移動した理由を特定し、必要に応じて境界でトラフィックをブロックします。

制限の緩い AWS S3 アクセス制限リスト

説明：新しく作成された ACL は、S3 バケットへのアクセス権の制限が緩くなっています。これは設定不備の可能性があり、保存されたデータへの不正アクセスにつなが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 AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測

次の手順：**アクセス制御リスト**を調べて、S3 バケットへのアクセス権が適切に制限されているかを判断します。設定に不備がある場合は、エントリを修正します。

制限の緩い AWS セキュリティグループの作成

説明：新しく作成された AWS セキュリティグループは、安全でないポート上のホストからのアクセスを許可しています。保護されておらず安全でないポートが設定された VPC セキュリティグループはセキュリティ問題の原因となるため、そうしたポートを保護する必要があります。

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 AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測

次の手順：AWS コンソールまたは AWS 視覚化ページを使用して AWS セキュリティグループの設定を調べ、必要に応じてアクセスを制限します。

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。

関連する観測：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。

関連する観測：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。

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。

関連する観測：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。

隠しファイル拡張子の潜在的有害性

説明：このエンティティで、潜在的に有害性のある隠し拡張子を持つファイルが検出されました。このアラートでは、複数のファイル拡張子の観測結果が使用されます。注：このアラートには、Cisco Defense Orchestrator から提供される URL データが必要です。潜在的に有害性のある隠し拡張子を持つファイルがマルウェアを構成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。また、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合も必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連する観測：複数のファイル拡張子の観測

次の手順：裏付けとなる観測結果を参照して、ファイルがマルウェアであるかどうか、または拡張子が非表示になっている理由を判断します。ファイルがネットワーク上のどこに転送されたか、どのエンティティがマルウェアに感染している可能性があるかを把握します。影響を受けるエンティティを隔離し、マルウェアを排除します。

潜在的なランサムウェア アクティビティ

説明：このエンティティは、共有ディレクトリの不正な変更や、ランサムウェアの疑いのあるコマンドアンドコントロール サーバーとの通信により、ランサムウェアに感染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。

関連する観測：パブリック IP ウォッチリストとの一致の観測、ウォッチリスト インタラクションの観測、ウォッチリスト ルックアップの観測

次の手順：エンティティがランサムウェアに感染しているかどうかを確認し、感染している場合はネットワークから隔離します。ネットワーク上の他のエンティティが同様にランサムウェアに感染しているかどうかを判断し、それらも隔離します。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。

リモート制御プロトコルの潜在的脆弱性

説明：このエンティティで古いバージョンのリモート制御アプリケーション（OpenSSH など）が使用されていることが確認されました。既知のセキュリティ脆弱性により、エンティティが危険にさらされる可能性があります。

前提条件：このアラートでは、リモート制御アプリケーションを使用するエンティティを確定するために、1 日間の履歴が必要です。Cognitive Intelligence が使用されます。

関連する観測：安全でないトランスポートプロトコルの観測

次の手順：裏付けとなる観測結果を参照して、エンティティで使用されているアプリケーションを特定し、どのエンティティとどのような接続が確立されたのかを判断します。組織で許可されているリモート制御アプリケーションの場合は、アプリケーションを最新バージョンに更新し、組織の使用ポリシーに従ってエンティティのセキュリティ設定を更新します。組織で許可されていないリモート制御アプリケーションが場合は、承認を得たユーザーまたは承認を得ていないユーザーによってインストールされたかのかをを判断し、アプリケーションを削除します。

プロトコル偽造

説明：このエンティティが、制限されている可能性のあるサービス（SSH など）を非標準ポートで実行していることが確認されました。これは、セキュリティコントロールの回避を示す可能性があります。

前提条件：このアラートでは、エンティティモデルを確定し、どのエンティティが制限されている可能性のあるサービスを使用しているのかを判断するために、1 日間の履歴が必要です。このアラートには 暗号化トラフィック分析 機能も必要です。

関連する観測：安全でないトランスポートプロトコルの観測

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プロトコルとポートの一般的ではない組み合わせを使用して通信した理由を特定します。セキュリティリスクがあると判断した場合は、ファイアウォールとブロックリストルールを更新し、今後はこのプロトコルとポートの組み合わせを使用してアクセスできないようにします。

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。

関連する観測：不正なプロトコルの観測

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。

Amazon Route 53 パブリックホストゾーンの作成

説明：Amazon Route 53 パブリックホストゾーンが作成されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートには AWS との統合が必要です。また、CloudTrail ログを読み取るために Secure Cloud Analytics のアクセス権を付与する必要があります。

関連する観測：AWS CloudTrail イベントの観測

次の手順：パブリックホストゾーンが作成されていなかった場合、これは、AWS でホストされているリソースから意図しない外部リソースにユーザーをリダイレクトしようとする悪意のある試みの可能性があります。AWS Cloudtrail イベントの観測を確認して、新しいゾーンを調査します。

パブリック IP ウォッチリストとの一致

説明：ネットワーク内のパブリック IP が、ウォッチリスト上で（明示的にまたはドメイン名を介して暗黙的に）検出されました。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連する観測：パブリック IP ウォッチリストとの一致の観測

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。エンティティが脅威インテリジェンス ウォッチリストに追加される原因となったマルウェアやアクティビティを特定し、是正処置を講じます。

パブリック IP サービスのルックアップ

説明：デバイスは、パブリック IP サービスドメインの DNS ルックアップを実行しました。このアラートは、パブリック IP サービスのドメイン検索の観測結果を使用します。パッシブ DNS データまたは Cisco Defense Orchestrator によって提供されるデータを収集するように センサー を設定する必要があります。

前提条件：このアラートに必要な履歴期間は 2 日間です。このアラートでは、パッシブ DNS 情報を収集するように センサー を設定するか、Cisco Defense Orchestrator を介して セキュリティ分析とロギング（SaaS）を Firepower アプライアンスと統合する必要があります。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging を参照してください。

関連する観測：パブリック IP ルックアップサービスを使用したデバイスの観測

次の手順：裏付けとなる観測結果に記載されているドメインを参照し、ドメインルックアップが正当な目的か不正目的かを判断します。不正目的の場合は、ルックアップを生成したソフトウェアを特定します。「デバイスで使用されたパブリック IP ルックアップサービスの観測」を確認し、他のエンティティが疑わしい呼び出しを行っているかを判断します。

高速ログイン

説明：ユーザーが短期間に複数のマシンにアクセスしました。

前提条件：このアラートに必要な履歴期間は 0 日間です。このアラートでは、ユーザーデータを取得するために ISE と連携する必要があります。

関連する観測：高速ログインの観測

次の手順：裏付けとなる観察結果を参照し、ユーザーのログイン試行が正当であるかを判断します。正当でない場合は、ユーザーのアクセスを無効にするか、クレデンシャルをリセットします。可能であれば、クレデンシャルがハイジャックされた方法を特定します。

リモートアクセス（地理的）

説明：このエンティティは、ウォッチリスト上の国のリモートホストからアクセスされました。

前提条件：このアラートに必要な履歴期間は 0 日間です。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。

関連する観測：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。

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。

関連する観測：ウォッチリスト インタラクションの観測、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。

関連する観測：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。

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、7 日間の履歴が必要です。

関連する観測：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。

古い AWS アクセスキー

説明：AWS IAM アクセスキーが設定可能な期間を超えました。これは、ベストプラクティスに違反します。

前提条件：このアラートに必要な履歴期間は 30 日間です。このアラートには AWS との統合も必要です。

関連する観察：AWS アーキテクチャ コンプライアンスの観測

次の手順：IAM ユーザーアカウントに引き続きアクセスできることを確認します。IAM ポリシーを調整して、キーがより定期的にローテーションされるようにします。

静的デバイス接続の逸脱

説明：このデバイスは通常、ネットワーク上で静的です。毎日、同様のトラフィックパターンで、同じデバイスと通信します。最近、このデバイスの動作が標準から逸脱（新しい外部ホストとの通信など）しています。このアラートは誤用または侵害を示す可能性があります。

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

関連する観測：履歴に基づく異常値の観測、新しい外部接続の観測

次の手順：裏付けとなる観測結果を参照して、エンティティの通常の通信を把握します。無害な逸脱か、あるいは悪意のある動作かを判断し、悪意のある動作があれば、是正処置を講じます。

静的デバイスの逸脱

説明：このエンティティは通常、ネットワーク上で静的です。毎日、同様のトラフィックパターンで、同じポートまたは同じエンティティと通信します。最近、このエンティティが標準から逸脱しており、これは誤用の兆候の可能性があります。

前提条件：このアラートには、エンティティモデルを確定し、通常のトラフィック量と動作を判別できるように、35 日間の履歴が必要です。

関連する観測：履歴に基づく異常値の観測、静的接続設定からの逸脱の監視、静的ポート設定からの逸脱の監視

次の手順：裏付けとなる観測結果を参照して、エンティティの通常の通信を把握します。無害な逸脱か、あるいは悪意のある動作かを判断し、悪意のある動作があれば、是正処置を講じます。

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。

関連する観測：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。

関連する観測：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。

悪意のあるURLの疑い

説明：エンティティが悪意が疑われる URL と通信しました。これは、悪意のあるアクセスやエンティティの侵害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。また、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合も必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連する観測：悪意のある URL の疑いの観測

次の手順：裏付けとなる観測結果を参照して、エンティティがアクセスしている URL を特定します。エンティティが侵害されているかどうかを判断し、感染している場合はエンティティからマルウェアを削除します。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 URL へのアクセスを防止します。

フィッシングドメインの疑い

説明：エンティティは、フィッシングの疑いのあるドメインの DNS ルックアップを正常に実行しました。

前提条件：このアラートに必要な履歴期間は 0 日間です。また、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合も必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連する観測：疑わしいフィッシングドメインの観測

次の手順：裏付けとなる観測結果を参照して、エンティティと接続先のドメインを特定します。これがマルウェアや悪意のある動作によるものかを判断し、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。

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。

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。

関連する観測：ポートスキャナの観測、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、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。

Zerologon RBC エクスプロイト試行の疑い

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。

関連する観測：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。

疑わしいドメインルックアップの失敗

説明：このエンティティは、アルゴリズムによって生成された複数のドメイン（rgkte-hdvj.cc など）を IP アドレスに解決しようとしました。これは、マルウェア感染、または生成されたドメインでコマンドアンドコントロール サーバーを使用したボットネット作成の試み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、SPAN またはミラーポートの DNS ログが必要です。

関連する観測：ドメイン生成アルゴリズムの観測

次の手順：裏付けとなる観測結果を参照し、エンティティがマルウェアに感染しているかどうか、またはドメインルックアップの原因を特定します。必要に応じて、問題のあるソフトウェアを削除します。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。

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。

関連する観測：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。

関連する観測：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。

TrickBot AnchorDNS トンネリング

説明：デバイスは、AnchorDNS（TrickBot マルウェアで使用されるトンネリング方式 ）で使用されるアルゴリズムが一致するドメインを検索しました。このアラートは、マルウェア感染またはボットネットアクティビティを示している可能性があります。

前提条件：このアラートでは、通常の AWS リソース動作を確定するために、14 日間の履歴が必要です。このアラートには AWS との統合も必要です。

関連する観測：TrickBot AnchorDNS トンネリングアクティビティの観測

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。

未使用の AWS リソース

説明：この AWS リソースの最近のアクティビティが確認されていません。リソースが関連しなくなったための予期される動作の可能性があります。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連する観測：未使用の AWS リソースの観測

次の手順：この AWS リソースが必要かどうか、または削除できるかどうかを判断します。動作している、またはアクティビティを示していると思われる場合は、AWS リソースを確認し、非アクティブになっている理由を特定します。必要に応じて是正処置を講じます。

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。

関連する観測：異常な DNS リゾルバの観測、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。

関連する観測：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。

ユーザーウォッチリストのヒット

説明：このエンティティは、ユーザーが定義したウォッチリスト上の IP アドレスとトラフィックを交換したか、ユーザーが定義したウォッチリスト上のドメイン名を解決しようとしました。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連する観測：ウォッチリストルックアップの観測およびウォッチリスト 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、悪意のある動作であるかどうかを判断します。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。

トランスポート セキュリティ プロトコルの脆弱性

説明：このエンティティは、安全でない SSL/TLS プロトコルバージョンを使用していることが確認されました。

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。拡張 NetFlow が使用されます。

関連する観測：安全でないトランスポートプロトコルの観測

次の手順：裏付けとなる観察結果を参照し、安全でないトランスポートプロトコルを使用しているアプリケーションを確認します。ローカルアプリケーションの場合は、安全なバージョンに更新します。アプリケーションがネットワークの外部にある場合は、セキュリティリスクの存在を示しているかどうかを判断し、ファイアウォールルールを使用して必要に応じてアクセスをブロックします。

ウォッチリストのヒット

説明：このエンティティは、ウォッチリスト上の IP アドレスとトラフィックを交換したか、ウォッチリスト上のドメイン名を解決しようとしました。Secure Cloud Analyticsエンジンには、いくつかのウォッチリストが組み込まれています。

前提条件：このアラートに必要な履歴期間は 0 日間です。

関連する観測：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、悪意のある動作であるかどうかを判断します。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。

観測の説明

追加の観測

説明：観測対象に関する追加情報。

前提条件：なし。

デバイスがパブリック IP ルックアップサービスを使用しました。観測

説明：デバイスが使用したパブリック IP ルックアップサービスは、マルウェアによって使用されています。

前提条件：なし。

関連するアラート：パブリック IP サービス ルックアップ アラート

Amazon GuardDuty による DNS リクエスト調査結果の観測

説明：Amazon GuardDuty が不審な DNS リクエストを報告しました。

前提条件：この観測には AWS との統合、および GuardDuty の有効化が必要です。

Amazon GuardDuty によるネットワーク接続の調査結果の観測

説明：Amazon GuardDuty が不審なネットワーク接続を報告しました。

前提条件：この観測には AWS との統合、および GuardDuty の有効化が必要です。

Amazon Inspector による調査結果の観測

説明：AWS リソースについての調査結果が報告されました。

前提条件：この観測には AWS との統合、および Inspector の有効化が必要です。

関連するアラート：AWS Inspector の調査結果アラート

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。

関連するアラート：AWS ワークスペースの異常検知アラート、Mac ワークステーションの異常検知アラート、Windows ワークステーションの異常検知アラート

AWS API ウォッチリストアクセスの観測

説明：ウォッチリストに登録されている IP から AWS API にアクセスされました。ウォッチリスト上のエンティティから API にアクセスがあった場合、悪意のある動作の可能性について調査が必要になる場合があります。

前提条件：この観測には、AWS との 統合および CloudTrail の有効化が必要です。

関連するアラート：AWS API ウォッチリスト IP ヒットアラート

AWS アーキテクチャ コンプライアンスの観測

説明: AWS の「Well-Architectured」ガイドラインに違反している可能性のある AWS リソースが検出されました。

前提条件: この観測には AWS との統合が必要です。

関連するアラート: 古い AWS アクセスキー使用アラート

AWS CloudTrail イベントの観測

説明: エンティティに関する AWS CloudTrail イベントが報告されました。

前提条件: この観測には、AWS との 統合および CloudTrail の有効化が必要です。

関連するアラート: AWS コンソールへのログイン失敗アラート、AWS ディテクタの変更アラート、AWS ロギング削除アラート、AWS 重複サブネットアラート、AWS ルートアカウント使用アラート、AWS 一時トークン永続性アラート、地理的に異常な AWS API 使用アラート、新しい AWS リージョンアラート、新しい AWS Route53 ターゲットアラート、制限の緩い AWS S3 アクセス制限リスト使用アラート、制限の緩い AWS セキュリティグループ作成アラート、Amazon Route 53 パブリックホストゾーン作成アラート

AWS Config コンプライアンスの観測

説明: AWS に関する設定コンプライアンスが報告されました。

前提条件: この観測には、AWS との 統合、設定変更を SNS トピックにストリーミングするための AWS の設定、設定変更を送信するための SQS キュー、およびメッセージを取得するための Secure Cloud Analytics での追加設定が必要です。

関連するアラート: AWS Config ルール違反アラート

AWS Config 更新の観測

説明: AWS リソースに関する設定の更新が報告されました。

前提条件: この観測には、AWS との 統合、設定変更を SNS トピックにストリーミングするための AWS の設定、設定変更を送信するための SQS キュー、およびメッセージを取得するための Secure Cloud Analytics での追加設定が必要です。

関連するアラート: AWS 重複サブネットアラート

AWS Lambda メトリックの外れ値の観測

説明: AWS Lambda 関数で、メトリックの 1 つに異常なアクティビティ（呼び出し回数が多いなど）ありました。

前提条件: この観測には AWS との統合、および少なくとも 1 つの Lambda 関数が必要です。

関連するアラート: AWS Lambda 呼び出し回数急増アラート

AWS 多要素認証の変更の観測

説明: 多要素認証がユーザーアカウントから削除されました。

前提条件: この観測には、AWS との 統合および CloudTrail の有効化が必要です。

関連するアラート: AWS 多要素認証の変更アラート

AWS 新規ユーザーアクションの観測

説明：CloudTrail が初めてアクションを実行する AWS ユーザーを記録しました。

前提条件：この観測には、AWS との 統合および CloudTrail の有効化が必要です。

AWS ルートアカウント使用の観測

説明：AWS ルートアカウントを使用してアクションが実行されました。

前提条件：この観測には、AWS との 統合および CloudTrail の有効化が必要です。

関連するアラート：AWS ルートアカウント使用アラート

Azure Advisor 推奨事項の観測

説明：Azure Advisor が Azure Resource Manager（ARM）リソースに関する推奨事項を生成しました。

前提条件：この観測には Azure との統合、および少なくとも 1 つのネットワーク セキュリティ グループまたはストレージアカウントが必要です。

関連するアラート：Azure Advisor ウォッチリストアラート

制限の緩い Azure セキュリティグループの観測

説明：ネットワーク セキュリティ グループに関連するセキュリティルールで、アクセス権の制限が非常に緩く設定されています。許可される IP アドレスが明示的に示されておらず、インターネット全体（例：*、0.0.0.0、:0/0）へのアクセスが許可されています。

前提条件：この観測には Azure との統合、および少なくとも 1 つのネットワーク セキュリティ グループが必要です。

関連するアラート：制限の緩い Azure セキュリティグループ アラート

制限の緩い Azure ストレージ設定の観測

説明：Azure ストレージ設定が過度に許容的になっています。

前提条件：この観測には Azure との統合、および 少なくとも 1 つのストレージアカウントが必要です。

関連するアラート：制限の緩い Azure ストレージアカウントアラート

Azure セキュリティイベントの観測

説明：Azure Security Center アラートが生成されました。

前提条件：この観測には Azure との統合、Azure Security Center、標準層、および Azure アクティビティログが必要です。

関連するアラート：Azure セキュリティ イベント アラート

Azure 異常アクティビティの観測

説明：Azure アクティビティログで異常なアクティビティが検出されました

前提条件：この観測には Azure との統合が必要です。

関連するアラート：Azure アクティビティログ IP ウォッチリスト ヒット アラート、Azure アクティビティ ログ ウォッチリスト ヒット アラート、地理的に異常な Azure API 使用アラート

未使用の場所における Azure VM の観測

説明：Azure Security Center アラートが生成されました。

前提条件：この観測には Azure との統合が必要です。また、Azure サブスクリプションを確認するために、Secure Cloud Analytics にモニターリングリーダーロール権限を付与する必要があります。

関連するアラート：未使用の場所における Azure 仮想マシン検知アラート

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。

関連するアラート：プロトコル違反（地理的）アラート

クラスター変更の観測

説明：エンティティのプロファイルセットが、最近関係していない他のエンティティのプロファイルセットに類似しています。

前提条件：なし。

コンプライアンス判定サマリーの観測

説明：コンプライアンスフレームワークの推奨事項に違反するクラウドリソースが検出されました。

前提条件：この観測には、クラウドポスチャ管理対応のクラウドプロバイダーとの連携が必要です。

脅威インジケーターの一致を確認 – ドメインの観測

説明 ：エンティティが既知の脅威の IOC としてリストされているドメインを解決しました。

前提条件：なし。

関連するアラート：脅威ウォッチリスト ヒット アラート

脅威インジケーターの一致を確認 – ホスト名の観測

説明：エンティティが、既知の脅威の IOC としてリストされているホストと通信しました。この観測では、拡張 NetFlow からの情報が使用されます。

前提条件：この観測には、拡張 NetFlow が必要です。詳細については、『Secure Cloud AnalyticsConfiguration Guide for Enhanced NetFlow』を参照してください。

関連するアラート：脅威ウォッチリスト ヒット アラート

脅威インジケータの一致を確認 – IP の観測

説明：エンティティが、既知の脅威の IOC としてリストされている IP アドレスと通信しました。

前提条件：なし。

関連するアラート：脅威ウォッチリスト ヒット アラート

脅威インジケータの一致を確認 – URL の観測

説明：エンティティが、既知の脅威の IOC としてリストされている URL と通信しました。この観測では、拡張 NetFlow からの情報が使用されます。

前提条件：この観測には、拡張 NetFlow が必要です。詳細については、『Secure Cloud AnalyticsConfiguration Guide for Enhanced NetFlow』を参照してください。

関連するアラート：脅威ウォッチリスト ヒット 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。

関連するアラート：通常とは異なる国との通信アラート

ドメイン生成アルゴリズムの観測

説明：エンティティが、アルゴリズムによって生成されたドメイン（qhjvd-hdvj.cc など）に接続しようとしました。

前提条件：なし。

関連するアラート：不審なドメインルックアップ失敗アラート

ドメイン生成アルゴリズム成功の観測

説明：エンティティは、アルゴリズムによって生成されたドメイン（rgkte-hdvj.cc など）を IP アドレスに正しく解決しました。

前提条件：なし。

関連するアラート：ドメイン生成アルゴリズムによるルックアップ成功アラート

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。

関連するアラート：ドメインコントローラの例外的通信アラート

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。

関連するアラート：ネットワークプリンタへの過剰な接続回数アラート

外部メールクライアント接続の観測

説明：1 つのエンティティが複数の外部メールサーバーと通信しました。

前提条件：なし。

関連するアラート：電子メールスパムアラート

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。

関連するアラート：着信ポートスキャナアラート、ポート悪用（外部）の疑いアラート

GCP クラウド関数メトリックの外れ値の観測

説明 : GCP クラウド関数のメトリックの 1 つで異常なアクティビティがありました。

前提条件: この観測には、Google Cloud Platform（GCP）との統合が必要です。

関連するアラート: GCP クラウド関数の呼び出し回数急増アラート

GCP ウォッチリスト アクティビティの観測

説明: GCP Stackdriver ログでウォッチリスト アクティビティが検出されました。

前提条件: この観測には Google Cloud Platform（GCP）との統合、および Stackdriver ログにアクセスするための Secure Cloud Analytics の権限が必要です。

関連するアラート: GCP Stackdriver ロギング ウォッチリスト ヒット アラート

地理情報ウォッチリストの観測

説明: エンティティがウォッチリスト上の地域と通信しました。

前提条件: なし。

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。

関連するアラート: 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

外れ値の履歴の観測

説明: 観測対象のメトリックの 1 つが、過去の基準から大幅に逸脱しています。この観測結果は、予測内または意図されたものである可能性がありますが、悪意のある動作を示している可能性もあります。

前提条件: なし。

関連するアラー: アクティティ中断アラート、電子メールスパムアラート、アウトバウンドトラフィック急増アラート、静的デバイス接続の逸脱アラート、および静的デバイスの逸脱アラート

安全でないトランスポートプロトコルの観測

説明: 暗号化トラフィック分析機能を備えたネットワークリソースによって、観測対象が安全でないトランスポートプロトコルを使用していることが確認されました。

前提条件: この観測には、暗号化トラフィック分析が必要です。

関連するアラート: リモート コントロール プロトコルの潜在的脆弱性アラート、プロトコル偽装アラート、トランスポート セキュリティ プロトコルの脆弱性アラート

内部接続ウォッチリストの観測

説明: 2 つの内部 IP エンドポイント間で、禁止されている通信が検出されました。

前提条件: なし。

関連するアラート: 内部接続ウォッチリストアラート

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。

侵入検知システム通知の観測

説明：IDS が疑わしい署名に一致するトラフィックを検出しました。

前提条件：この観測には、次のいずれかが必要です。

- セキュリティ分析とロギング（SaaS） Cisco Defense Orchestrator を介して Firepower アプライアンスと統合された詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。
- Suricata IDS
- Zeek IDS

関連するアラート：新たな IDS プロファイルアラート、IDS 通知急増アラート

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。

関連するアラート：NetBIOS 接続回数の急増アラート、新しい IP スキャナアラート、新しい SNMP スイープアラート、非サービスのポートスキャナアラート、SMB 接続回数の急増アラート

長時間セッションの観測

説明：エンティティが外部 IP アドレスと長時間セッションを継続しました。

前提条件：なし。

関連するアラート：新たな長時間セッション（地理的）アラート

マルウェアイベントの観測

説明：エンティティでマルウェアアクティビティが検出されました

前提条件：この観測には、マルウェアイベントを生成するための Cisco ファイアウォールが必要です。

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。

関連するアラート：過剰アクセス試行回数（外部）アラート

複数のファイル拡張子の観測

説明：このエンティティは、複数の拡張子でファイルを交換しました。

前提条件：この観測には、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合が必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連するアラート：隠しファイル拡張子の潜在的有害性アラート

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。

関連するアラート：ネットワークプリンタの過剰な接続回数アラート

リソースの新たなコンプライアンス違反の観測

説明：コンプライアンス フレームワークの推奨事項に前日まで遵守していたクラウドリソースで、違反が検出されました。

前提条件：この観測には、クラウドポスチャ管理対応のクラウドプロバイダーとの連携が必要です。

新しい外部接続の観測

説明：通常は予測可能なローカルエンティティが外部エンティティと通信しました。

前提条件：なし。

関連するアラート：新しい外部接続アラート、静的デバイス接続の逸脱アラート

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。

関連するアラート：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。

関連するアラート：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

新しい内部接続の観測

説明：通常は予測可能なローカルエンティティが新しい内部エンティティと通信しました。

前提条件：なし。

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。

関連するアラート：新しい内部デバイスアラート

新しい大規模接続（外部）の観測

説明：エンティティが非常に大量のデータを外部ホストと交換しました。

前提条件：なし。

関連するアラート：アウトバウンドトラフィックの急増アラート

新しい大規模接続（内部）の観測

説明：エンティティが非常に大量のデータを内部ホストと交換しました。

前提条件：なし。

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。

関連するアラート：電子メールスパムアラート、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。

関連するアラート：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。

関連するアラート：ネットワーク利用者数の急増アラート

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。

関連するアラート：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。

関連するアラート：データ漏洩の疑いアラート

Amazon Route 53 パブリックホストゾーン作成の観測

説明：Amazon Route 53 パブリックホストゾーンが作成されました。

前提条件：この観測には AWS との統合が必要です。

パブリック IP ウォッチリストとの一致の観測

説明：ネットワーク内のパブリック IP が、ウォッチリスト上で（明示的にまたはドメイン名を介して暗黙的に）検出されました。

前提条件：なし。

関連するアラート：パブリック IP ウォッチリストとの一致アラート

高速ログインの観測

説明：ユーザーが短期間に多数のエンティティにログインしました。

前提条件：なし。

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。

関連するアラート：内部接続の急増アラート、アウトバウンドトラフィックの急増アラート

レコードプロファイルの外れ値の観測

説明：エンティティは、Facebook クライアントなどの既知のプロファイルに一致するトラフィックを大量に送信または受信しました。

前提条件：なし。

関連するアラート：アウトバウンドトラフィックの急増アラート

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。

関連するアラート：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。

関連するアラート：ロール違反アラート

スキャン結果の観測

説明：アクティブなスキャナー（例：nmap ）がエンティティの動作を検出しました。

前提条件：なし。

セッションクローズの観測

説明 ：ユーザーセッションが閉じられました。

前提条件：この観測には、OSSEC、Sumo Logic、または Active Directory の導入が必要です。

セッションオープンの観測

説明：ユーザーセッションが開かれました。

前提条件：なし。

関連するアラート：ユーザーの不正アクションアラート

静的接続設定からの逸脱の観測

説明：通常は一連の静的な（内部または外部）エンティティと通信するエンティティが、最近、新しいまたは通常のエンティティとの通信を開始または停止しました。

前提条件：なし。

関連するアラート：静的デバイスの逸脱アラート

静的ポートセットの逸脱の観測

説明：エンティティは通信（内部または外部）用に、通常は一連の静的ポート（ローカルポートまたは接続されたポート）を使用しますが、ポートを追加または削除したことが確認されました。

前提条件：なし。

関連するアラート：静的デバイスの逸脱アラート

Sumo Logic ログの観測

説明：エンティティが Sumo Logic によって記録されたログに関係している可能性があります。

前提条件：この観測には Sumo Logic の導入が必要です。

関連するアラート：Sumo Logic ログの欠落アラート

悪意のある URL の疑いの監視

説明：ホストが疑わしい URL と通信しました。

前提条件：この監視には、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合が必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連するアラート：悪意のある URL の疑いアラート

フィッシングの疑いのあるドメインの監視

説明：ホストがフィッシングの疑いのあるドメインと通信しました。

前提条件：この観測には、Cisco Defense Orchestrator を介した セキュリティ分析とロギング（SaaS）との統合が必要です。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Loggingを参照してください。

関連するアラート：フィッシングドメインの疑いアラート

疑わしいネットワークアクティビティの観測

説明：既知の攻撃者の戦術、技術、および手順に関連付けられてい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。

関連するアラート：Zerologon RPC エクスプロイト試行の疑い アラート

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。

関連するアラート：不審な 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。

関連するアラート：アンプ攻撃アラート

TrickBot AnchorDNS トンネリングアクティビティの観測

説明：デバイスが TrickBot Anchor_DNS トンネリングメソッドを使用して C&C サーバーと通信しました。

前提条件：なし。

関連するアラート：TrickBot AnchorDNS トンネリングアラート

未使用の AWS リソースの観測

説明：AWS リソースの最近のアクティビティが確認されていません。

前提条件：この観測には AWS との統合が必要です。

関連するアラート：AWS リソース未使用アラート

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。

関連するアラート：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

異常なパケットサイズの観測

説明：エンティティが特定のプロファイルに対して異常なサイズのパケットを送信または受信しました。

前提条件：なし。

関連するアラート：DNS 悪用アラート

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。

関連するアラート: 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

ウォッチリストのルックアップの観測

説明: エンティティがウォッチリストに記載されているドメインを検索しました。

前提条件: なし。

関連するアラート: 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

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。

変更履歴

リビジョン	改訂日	説明
1.0	2020 年 4 月 3 日	最初のバージョン。
1.1	2020 年 9 月 4 日	次のアラートと観測タイプを追加。 • 異常な AWS ワークスペースアラート • 異常な Mac ワークステーションアラート • Empire コマンドアンドコントロール アラート • マルウェア急増アラート • 異常なプロファイルの観測 次のアラートと観測タイプを更新。 • 電子メールスパムアラート • 履歴に基づく異常値の観測 • 新しいプロファイルの観測 また、セキュリティ分析とロギング（SaaS）に関する詳細情報を追加し、誤字を訂正。
2.0	2021 年 10 月 25 日	製品のブランド名を更新。 次のアラートと観測タイプを追加。 • AWS ディテクタの変更アラート • AWS ロギング削除アラート • AWS 一時的トークンの永続性アラート • Azure Advisor ウォッチリストアラート • 非サービスのポートスキャナアラート • パブリック IP サービスのルックアップアラート • 静的デバイス接続の逸脱アラート • Zerologon RBC エクスプロイト試行の疑いアラート • TrickBot AnchorDNS トンネリングアラート • デバイスで使用されたパブリック IP ルックアップサービスの観測 • 制限の緩い Azure セキュリティグループの観測 • 制限の緩い Azure ストレージ設定の観測 • コンプライアンス判定サマリーの観測 • リソースの新たなコンプライアンス違反の観測 • TrickBot AnchorDNS トンネリングアクティビティの観測

		次のアラートを削除。 • 潜在的なランサムウェア アクティビティのアラート • 高速ログインアラート

著作権情報