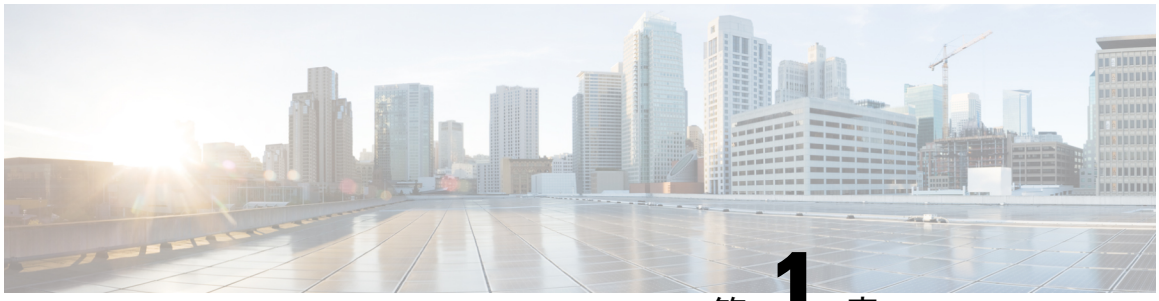
Cisco Secure Cloud Analytics リリースノート

初版：2021 年 1 月 12 日

最終更新：2022 年 8 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

Cisco Secure Cloud Analytics の新機能

新機能

関連情報：Secure Cloud Insights（JupiterOne）リリースノート

2022 年 12 月

デバイスアウトラインの更新：[アラートの詳細（Alert Details）] ページと [デバイスレポート（Device Report）] ページの両方にある [デバイスアウトライン（Device Outline）] パネルが更新され、センサーとエクスポータの参照が含まれるようになりました。センサーとエクスポータのデータが利用可能な場合、それを使用してデバイスがアクティブに通信しているネットワーク部を特定できます。

通知パネル：ポータルのどのページからでも、アクティブなシステム警告と新機能のリリースノートをすばやく表示できるようになりました。ポータルヘッダーの右側にあるメガホンアイコンをクリックして、新しい [通知（Notifications）] パネルを表示します。

可視性評価の更新：可視性評価レポートが更新され、機能が追加されました。表示されているインサイトを明確にするために、更新の説明を使用します。次に、組み込まれたデバイスリンクを使用して調査を続行します。このレポートにアクセスするには、[レポート（Report）] > [可視性評価（Visibility Assessment）] に移動します。

2022 年 11 月

アラートと監視の更新：

- [AWS がAPIエラーを繰り返す（AWS Repeated API Failures）] : AWS CloudTrail ログを監視している場合、この新しいアラートは、ユーザーが複数の API 呼び出しを実行し、権限が不十分なために失敗したことを示します。これは、敵対者が環境に関する情報を取得しようとしたり、列挙を試みたり、永続性を確立したり、権限をエスカレー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。このアラートはデフォルトで無効になっています。

- [クラウドアカウントへのAzureデータ転送（Azure Transfer Data to Cloud Account）] : このAzure アクティビティログアラートは、追加の Azure 仮想ハードドライブのデータ漏洩手法にまで拡張されました。スナップショットの抽出に加えて、URL ベースの抽出についてもアラートが送信されるようになりました。
- [緊急プロファイル（Emergent Profile）] : この既存のアラートは、特定のプロファイルについてクライアント/サーバーの状態を判断できない条件を排除することで改善されました。このアラートは、デバイスに新しいプロファイルに適合するトラフィックがある場合にトリガーされ、デバイスの設定不備または侵害を示している可能性があります。

Cisco Umbrella Investigations の更新：Umbrella Investigations を設定した場合（[設定（Setting）] >[統合（Integrations）]> [Umbrella]）、調査ピボットから、対応する [Umbrella IP 結果（Umbrella IP Results）] ページに直接移動します。Cisco Umbrella Investigation は、任意の外部 IP アドレスのピボットメニューにあります。SecureX と統合すると、SecureX ポータルからオーケストレーションを使用して、Cisco Umbrella およびその他のツールのワークフローを追加できます。

[センサーの詳細（Sensor Details）] ページ：クラウド構成のオンプレミスセンサーを使用している場合、関連するテレメトリ統計にアクセスできます。[設定（Settings）] > [センサー（Sensors）]>[センサーの詳細（Sensor Details）] に移動して、これらのセンサーのボリュームと一般的な使用状況の指標を表示します。

センサー/エクスポーターの詳細：センサーとエクスポーターのコンテキストが利用可能な場合、アラートの詳細とデバイスレポートの両方のデバイスアウトラインに含まれるようになりました。この詳細を使用して、調査中に特定のデバイスが確認された場所のコンテキストを提供します。

セッショントラフィックの更新：セッショントラフィックデータは、オンプレミス センサーフィールドの新しいセンサータイプである Azure for Cloud Provider および Catalyst を反映するようになりました。これらのセンサータイプをポータルに統合している場合、このデータは、[調査（Investigate）]>[イベントビューア（Event Viewer）]>[セッショントラフィック（Session Traffic）] を使用してクエリを実行するときに見つけることができます。

上位の高リスク国の調査：ダッシュボードのリスクの高い国の上位ウィジェットを使用すると、国固有の地理情報ウォッチリストの観測をドリルダウンすることができます。ダッシュボードから、特定の国のインバウンド/アウトバウンドグラフの任意の場所をクリックして、調査を続行します。

2022 年 10 月

アラートと監視の更新：

- [AWS IAM Anywhereトラストアンカー作成（AWS IAM Anywhere Trust Anchor Created）] : AWS CloudTrail ログを監視している場合、この新しいアラートは、最近作成された IAM ロール Anywhere トラストアンカーを通知します。これは、攻撃者がアカウントへの永続的なアクセスを確立しようとしていることを示している可能性があります。このアラートはデフォルトで無効になっています。
- [ハートビートの監視（Heartbeat Observation）] : この既存の監視と関連するアラートは、信頼できる企業としてシスコ （openDNS を含む）を追加することで改善されました。こ

の監視結果は、デバイスがリモートホストとのハートビートを維持していることを示しています。

- [新しいAWS Lambda呼び出しアクセス許可の追加（New AWS Lambda Invoke Permission Added）]：AWS CloudTrail ログを監視している場合、この新しいアラートは、別の AWS サービス、アカウント、または組織から AWS Lambda 関数を呼び出すための新しいアクセス許可が追加されたことを示します。これは、外部の AWS からアカウントへの永続的なアクセスを確立しようとしていることを示している可能性があります。このアラートはデフォルトで無効になっています。
- **新しい高スループット接続の観測**：この既存の監視は、アップロード率とダウンロード率に関連するロジックを追加することによって改善されました。この観察は、デバイスが内部から外部への大量のトラフィックを新しいホストと交換したことを示しています。
- [異常に大きいEC2インスタンス（Unusually Large EC2 Instance）] : AWS CloudTrail ログを監視している場合、この新しいアラートは異常に大きい EC2 インスタンスの作成を通知します。攻撃者がリソースハイジャックの目的で EC2 インスタンスを展開したことを示している可能性があります。このアラートはデフォルトで無効になっています。

クラウド ポスチャ ウォッチリストの更新：[設定（Settings）] > [アラート/ウォッチリスト（Alerts/Watchlists）] > [クラウドポスチャウォッチリスト（Cloud Posture Watchlist）] ページで関連する [クラウドポスチャの再評価（Re-Evaluate Cloud Posture）] オプションを選択することで、GCP フレームワークの再評価を手動でトリガーできるようになりました。

デバイスアウトラインの更新：[アラートの詳細（Alert Details）] ページと [デバイスレポート（Device Report）] ページの両方にある [デバイスアウトライン（Device Outline）] パネルが更新され、使いやすさが向上しました。特定の要素の横にある注アイコンで示されているように、[コピー（Copy）] アイコンを使用して特定のデバイス属性をコピーできるようになりました。[出席（Attendance）] セクションと [オブザベーション（Observations）] セクションの両方が再配置され、全体のデバイスメトリック（現在の日付に固有ではない）であることをより適切に表示できるようになりました。

イベントビューアの更新：センサーおよびエクスポータの詳細列が、プライベート ネットワーク モニタリングの [イベントビューア（Event Viewer）] > [セッショントラフィック（Session Traffic）] テーブルに含まれるようになりました。これらの詳細は、特定のトラフィックがネットワーク上で通過する場所に関するコンテキストを提供します。デフォルトのテーブル列として含まれていないため、これらを追加するには、[列の管理（Manage Columns）] アイコンをクリックする必要があります。

GCP センサーの制限ステータス：GCP 統合が GCP API の制限に達し始めている場合は、[設定（Setting）] > [センサー（Sensors）] ページに移動すると、影響を受けた特定の GCP センサーのオレンジ色の雲のアイコンが表示されます。

統合ページの更新：次の [設定（Settings）] > [統合（Integrations）] ページは、より一貫したエクスペリエンスのために更新されました。

- **Secure Cloud Insights**
- **Umbrella**
- **SecureX**

サイトナビゲーションの更新：[調査（Investigate）] メニューには、ページ間をすばやくピボットするために左側のサブナビゲーションが含まれるようになりました。この機能は、[イベントビューア（Event Viewer）] および [セッショントラフィック（Session Traffic）] ページにまだ追加されていないことに注意してください。

トラフィックサマリーページの更新：[レポート（Report）] > [トラフィックサマリー（Traffic Summary）] ページの [日付/時刻（Date/Time）] セレクターに検証が追加され、レポートが 8 日間の最大範囲をサポートすることが明確になりました。

アラートの詳細の更新：[アラートの詳細（Alerts Details）] ページには、アラートアクティビティのさまざまな段階を反映する特定のタイムスタンプが含まれます。[アラートルールの詳細（Alert Rules Details）] セクションには、次のタイムスタンプがあります。

- **検出日**
- **最初の観測**
- **前回の観測**

2022 年 9 月

アラートと監視の更新：

- **AWS EC2 起動スクリプトの変更アラート**：AWS 参照の変更を考慮してこのアラートを更新し、インスタンス停止イベントのチェックを追加しました。この改善により、悪意のあるアクティビティを示している可能性のある異常な変更動作がすばやく公開されます。有効性レビューのため、アラートは現在デフォルトで無効になっています。
- **異常な EC2 インスタンスの監視**：異常に大きな EC2 インスタンスが特定のアカウントに展開されたことを示す新しい CloudTrail ベースの観測。
- **AWS の新しいユーザーアクションの監視**：既存の CloudTrail ベースの監視が、より長いルックバック期間に更新されました。この監視は、CloudTrail が初めてアクションを実行する AWS ユーザーを記録したことを示します。結果として得られる観察には、追加のコンテキストの**ユーザー**と**リモート IP** の詳細が含まれます。
- **MITRE ATT&CK の戦術とテクニック**：次のアラートタイプで MITER マッピングが更新されました。
  - **ディスカバリ - ネットワーク サービス ディスカバリ**：新しい IP スキャナ、新しい SNMP スイープ、NetBIOS 接続スパイク、SMB 接続スパイク、および LDAP 接続スパイク。
  - **調査 - アクティブスキャニング**：アウトバウンド LDAP 接続スパイクとアウトバウンド SMB 接続スパイク。

アラートのデモ：アラートのデモに関する新しい動画が 2 つあります。

- AWS ディテクタの変更
- Azure OAuth バイパス

- 新しい AWS リージョン
- 制限の緩い AWS S3 アクセス制限リスト
- 制限の緩い AWS セキュリティグループの作成

パブリッククラウド統合モニタリングの更新：AWS または Azure のモニタリングステータスを表示しているときに、データを CSV ファイルで取得する場合は、[CSV のダウンロード（download CSV）] ボタンをクリックします。モニタリングステータスを表示するには、統合サービスに固有のページを使用します。

- **AWS** - [設定（Settings）] > [統合（Integrations）] > [AWS] > [VPC フローログ（VPC Flow Logs）]
- **Azure** - [設定（Settings）] > [統合（Integrations）] > [Azure] > [ストレージアクセス（Storage Access）]

センサーページの更新：[設定（Settings）] > [センサー（Sensor）] ページで、オンプレミスセンサーのセンサー IP を表示できるようになりました。

2022 年 8 月

アラートと監視の更新：

- **Azure Oauth バイパスアラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、kubeconfig ファイルを変更しようとするアクションを示します。攻撃者が侵害されたクライアントから kubeconfig ファイルにアクセスした場合、それを使用してクラスタにアクセスすることができます。
- **パブリック IP サービスアラート**：このアラートは削除されました。改善後も、この既存アラートは、アクション可能なアラートとして低レベルの有用性を報告し続けました。このアラートは、デバイスが IP サービスドメインの DNS ルックアップをいつ実行したかを示すように設計されています。
- **ISE セッション開始監視**：Cisco Identity Services Engine（ISE）を統合している場合、この新しい監視は、新しく確立された ISE ユーザーセッションを探します。

ダッシュボードの更新：メインダッシュボードにある日次トラフィックグラフは、内部トラフィックと外部トラフィックを区別して、Secure Cloud Analytics によって監視されているトラフィックを把握できるようになりました。

デバイスレポートの更新：あらゆるデバイスまたはデバイス検索からピボットすることでアクセスできるデバイスレポートが更新され、コンテキストと使いやすさが向上しました。レポートには、追加の指標、ハイライト、およびピボットが含まれるようになりました。また、新しい接続の視覚化を [トラフィック接続の視覚化（Traffic Connections Visualization）] タブ内で利用できます。

暗号化されたトラフィックページの更新：[調査（Investigate）] > [暗号化されたトラフィック（ Encrypted Traffic）] ページが、新しい Cisco の外観と操作性に更新されました。

ネットワークテレメトリの機能強化：Cisco Telemetry Broker を Cisco Secure Cloud Analytics のセンサーとして使用できるようになりました。統合すると、Cisco Telemetry Broker はネットワークベースのアラートを有効にします。既存のワークフローを使用して、[調査（Investigate）] > [イベントビューア（Event Viewer）] ページをドリルダウンして、新しい [セッションの詳細（Session Details）] タブにアクセスできます。これにより、これまで以上に完全なネットワークレコードを使用した追加のフォレンジックコンテキストを実現します。Cisco Telemetry Broker とこの統合の詳細については、cs.co/telemetrybroker にアクセスし、『Send On-Premises Flows to Secure Cloud Analytics Configuration Guide』[英語] を参照してください。

エンティティグループ構成の更新：エンティティグループを作成するワークフローが合理化され、使いやすさが向上しました。[設定（Settings）] > [エンティティグループ（Entity Group）] ページを使用して、デバイスグループを作成および管理することにより、デバイスにコンテキストを追加できるようになりました。

監視の詳細の更新：JSON BLOB に含まれる追加のコンテキストを提供する観測を調査する場合、テーブルの左側に矢印アイコンが表示されるようになりました。矢印アイコンをクリックして監視を展開し、JSON コンテキストを読み取り可能な形式で表示できます。展開可能なビューは、アラートの詳細ページと監視固有のレポートにあります。展開したビューを閉じるには、下矢印アイコンをクリックします。

パブリッククラウド統合モニタリングの更新：テーブルフィルタリングを使用して、Azure、AWS、または GCP のモニタリングステータスをより詳細に表示できるようになりました。モニタリングステータスを表示するには、統合サービスに固有のページを使用します。

- **AWS** - [設定（Settings）] > [統合（Integrations）] > [AWS] > [VPC フローログ（VPC Flow Logs）]
- **Azure** - [設定（Settings）] > [統合（Integrations）] > [Azure] > [ストレージアクセス（Storage Access）]
- **GCP** - [設定（Settings）] > [統合（Integrations）] > [GCP] > [クレデンシャル（Credentials）]

センサーオフライン通知の更新：センサーオフライン通知をトリガーするしきい値が、非アクティブ状態の 8 時間から 4 時間に短縮されました。

[センサー（Sensors）] ページの更新：[設定（Settings）] > [センサー（Sensors）] ページをセンサーのステータスでフィルタリングして、特定のセンサーを表示できるようになりました。

2022 年 7 月

アラートと監視の更新：

- **新しいリモートアクセスアラート**：これは、ルックバック期間を延長することによって改善された既存のアラートです。アラートは、最近で初めてデバイスがリモートホストからアクセスされたときに表示されます。これは、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。
- **SMB 接続の外れ値アラート**：これは、有効性レビューを通過した既存のアラートであり、デフォルトで有効になっています。アラートは、デバイスが非常に大規模な SMB ピアの

セットと非常に大量の SMB トラフィックを交換したときに発生します。これは、偵察活動の存在を示している可能性があります。

- **疑わしい DNS over HTTPS アクティビティアラート**：これは、有効性レビューを通過した既存のアラートであり、デフォルトで有効になっています。アラートは、内部サーバーが既知の DNS over HTTPS サーバーとトラフィックを交換していることが判明したときにトリガーされます。これは、DNSベースのセキュリティを回避しようとしていることを示している可能性があります。
- **異常な外部サーバーアラート**：これは、外部サーバーに関連付けられた接続期間に焦点を当てることで改善された既存のアラートです。アラートは、デバイスが新しい外部サーバーと繰り返し通信を行ったことを示しています。これは、マルウェアの存在を示している可能性があります。

アラートのデモ：アラートのデモに関する新しい動画が 2 つあります。

- Permissive AWS Security Group Created Alerts
- New Internal Device Alerts

アラートタイプを SecureX に公開：SecureX と統合する場合は、[アラート（Alerts）] > [優先順位（Priorities）] ページを使用して、SecureX Incident Manager にインシデントとして自動的に公開するアラートタイプを設定します。[Talosインテリジェンスウォッチリストのヒットアラート（Talos Intelligence Watchlist Hits Alert）] タイプがデフォルトで有効になっています。詳細については、『SecureX Integration Guide』を参照してください。

ロールページの更新：[調査（Investigate）] > [アクティブなロール（Active Roles）] ページが [ロール（Roles）] ページになりました。このページには、アクティブなロールの決定方法に関する追加情報、非アクティブなロールタイプのリスト、および各ロールの説明が含まれています。

Cisco Secure Cloud Analytics パブリック IP の API：お使いの環境へのアクセスを動的に制限する必要がある場合に、API エンドポイント（`/api/v3/service/public-ips/`）を使用して、Cisco Secure Cloud Analytics の統合に必要なパブリック IP のリストにアクセスできるようになりました。

SecureX Incident Manager のウェブフック更新：[設定（Settings）] > [ウェブフック/サービス（Webhooks/Services）] > [SecureX Incident Manager] ページを使用して、複数の SecureX のウェブフック統合を管理できるようになりました。

[センサー（Sensors）] ページの更新：[設定（Settings）]>[センサー（Sensors）] ページをセンサー名とセンサータイプでフィルタリングできるようになりました。

サブネットの感度の更新：サブネットの感度に、`None` のオプションが含まれなくなりました。`Low`、`Medium`、または `High` の設定を使用して、サブネットごとにデバイスコンテキストと相対的なアラートの重大度を示します。

2022 年 6 月

アラートと監視の更新：

- **S3バケットのライフサイクル構成済みアラート**：この既存のアラートは、非現行バージョンだけでなくすべてのオブジェクトタイプに拡張することで改善されました。アラートは、バケット内のすべてのファイルの同時永久削除をスケジュールする新しい S3 バケットライフサイクル構成が作成されたことを示しています。これは、データを破壊しようとする試みの存在を示している可能性があります。
- **国のセットからの逸脱アラート**：この既存のアラートの説明が変更され、国のウォッチリストの設定が不要であることが明記されました。この動作アラートは、デバイスが通常通信する国のセットから大幅に逸脱しているときに表示されます。これは、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。

信頼できる企業の更新リスト：信頼できる外部 IP ロジックに、シスコが所有する IP スペースと Mitel 社のクラウドサービスが含まれるようになりました。これにより、こうしたスペースとやり取りする際に異常な外部サーバーやアウトバウンドトラフィックの急増などの選択されたアラートや監視がトリガーされなくなります。信頼できるサードパーティを追加するには、[設定（Settings）] > [サブネット（Subnets）] > [仮想プライベートネットワーク（Virtual Private Networks）] に移動して、追加の VPN サブネットを設定します。

Mitel 社の VoIP クライアントロール：VoIP コールを行うために使用されている Mitel 社のデバイスを識別する、新しいロールが追加されました。

サブネットの感度の更新：アラートの有効性を改善するため、サブネットのデフォルトの感度が Normal/Medium に引き下げられました。さらに、サブネットの感度マトリックスが更新され、デバイス固有のアラートのみに関係するサブネットの感度が明確になりました。設定された感度は、ネットワークタイプのアラートには影響しません。サブネットの感度と設定の詳細については、[設定（Settings）] > [サブネット（Subnets）] に移動してください。

イベントビューアの更新：イベントビューアのリンクが、従来の [セッショントラフィック（Session Traffic）] ページのリンクから [調査（Investigate）] メニューの上部に移動しました。さらに、イベントビューア内のセッション トラフィック テーブルに、トラフィックが生成されたクラウド環境に関連する次の列が含まれるようになりました。

- Cloud_Account
- Cloud_Region
- Cloud_VPC

このデータを使用して、アラートを調査する際に懸念または修復される領域を特定します。新しい列を表示するには、[調査（Investigate）] > [イベントビューア（Event Viewer）] > [セッショントラフィック（Session Traffic）] に移動します。

[アクティブロール（Active Roles）] ページの更新：[調査（Investigate）] > [アクティブロール（Active Roles）] ページに、アクティブロールの決定方法を説明する追加情報と、表示される各ロールタイプの説明が含まれるようになりました。

2022 年 5 月

アラートと監視の更新：

- **疑わしいユーザー エージェント アラート**：Security Analytics and Logging（SaaS）を有効にしている場合、デバイスが疑わしいユーザーエージェント文字列を使用して他のデバイスと通信していることが確認されたデバイスに対して、アラートが送信されるようになりました。検出されたデバイスに、マルウェア（Log4J のエクスプロイトなど）または悪用の兆候があることを示している可能性があります。このアラートはデフォルトで無効になっています。
- **新しい SNMP スイープアラート**：この既存のアラートは、関連するしきい値を調整して有効性を高めることで改善されました。アラートは、デバイスが SNMP を使用して多数のホストに到達しようとしたときに表示されます。これはマルウェアまたは悪用の兆候を示している可能性があります。
- **国のセットからの逸脱アラート**：この既存のアラートは、同様のアラートが発生した場合のアラート量の監視を減らすように調整されています。アラートは、デバイスが通常通信する国のセットから大幅に逸脱していることが確認されたときに表示されます。これは、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。
- **NetBIOS 接続のスパイクアラート**：この既存のアラートは、同じスキャナに対してアラートを追加する頻度を減らすように調整されています。このアラートは、デバイスが NetBIOS を使用して多数のホストに接続しようとしたときに表示されます。これは、マルウェアまたは悪用の兆候を示している可能性があります。
- **パブリック IP サービスアラート**：この既存のアラートは、同じソースに対して追加するアラートの数を減らすように調整されています。アラートには、お使いのセンサーまたは Security Analytics and Logging（SaaS）統合を介したパッシブ DNS のデータが必要です。また、このアラートは、デバイスが IP サービスドメインの DNS ルックアップを実行したことを示しています。
- **新しいファイル拡張子の監視**：この既存の監視機能が改善され、疑わしい拡張子のみが検索されるようになりました。

Nessus スキャナロール：Nessus スキャナを識別する新しいロールが追加されました。

Carbonite プロファイルタグ：既存の Mozy プロファイルタグが更新および拡張され、Carbonite と追加のマッチング動作が反映されるようになりました。

[アラートの優先順位（Alert Priorities）] ページ：

- 対応するテレメトリ要件でタグ付けされた追加のアラートが含まれています。
- [すべてをデフォルトにリセット（Reset All to Defaults）] ボタンで、[優先順位（Priority）] と [有効（Enabled）] の両方の状態をデフォルト設定にリセットするようになりました。

[センサー（Sensors）] ページ：

- [設定（Settings）] > [センサー（Sensors）] ページに、センサーごとに設定された各テレメトリのセンサーのホスト名とステータスのタイムスタンプが反映されるようになりました。
- オフラインになると GCP センサーがメールで通知を行います。

計測レポート：[レポート（Report）] > [計測レポート（Metering Report）] ページに、EMF の傾向線と、ページを月や年でフィルタリングする機能が含まれるようになりました。この機能を使用して、過去のエンドポイントと EMF の傾向を確認できます。

Azure 統合ワークフロー：[設定（Settings）] > [統合（Integrations）] > [Azure] > [バージョン情報（About）] ページが更新され、Azure の統合に必要な更新された言語と手順が反映されました。これは、既存の統合には影響しません。新しい統合では、NSG フローログを有効にする前に、Azure の必須アプリケーションの有効期限要件と、インサイトプロバイダーの登録に留意する必要があります。

Cisco Secure Cloud Analytics パブリック IP：お使いの環境へのアクセスを制限する必要がある場合に、Cisco Secure Cloud Analytics の統合に必要なパブリック IP のリストにアクセスできます。IP のリストは、次のページにあります。

- AWS のバージョン情報（[設定（Settings）] > [統合（Integrations）] > [AWS] > [バージョン情報（About）]）
- Azure のバージョン情報（[設定（Settings）] > [統合（Integrations）] > [Azure] > [バージョン情報（About）]
- GCP のバージョン情報（[設定（Settings）] > [統合（Integrations）] > [GCP] > [バージョン情報（About）]
- センサーインストール（？（ヘルプ）アイコン > [オンプレミスセンサーのインストール（On-Prem Sensor Install）]

エンティティグループ API：エンティティグループの REST API が利用できるようになりました。エンティティグループを使用して、ビジネスコンテキストをデバイスに追加します。Web ポータルを介してエンティティグループを設定および管理するには、[設定（Settings）] > [エンティティグループ（Entity Groups）] に移動するか、API（`https://<portal name>/api/v3/entitygroups/entitygroups/`）を使用します。

2022 年 4 月

アラートと監視の更新：

- **ロール違反アラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、特定のロール（Windows ワークステーションなど）で識別されたデバイスが新しいロール（SSH サーバーなど）で動作していることが確認されたときに通知します。このアラートは、デバイスが侵害されていることを示す可能性があります。
- **Azure 関数呼び出し回数のスパイクアラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、Azure 関数の呼び出し回数が異常に多くなったときに表示されます。これは、運用上の問題またはサービス妨害（DoS）攻撃の発生を示している可能性があります。
- **LDAP 接続回数のスパイクアラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、デバイスが非常に多くの内部 LDAP サー

バーへの接続を試行したときに表示されます。これは、マルウェアまたは悪用を示している可能性があります。

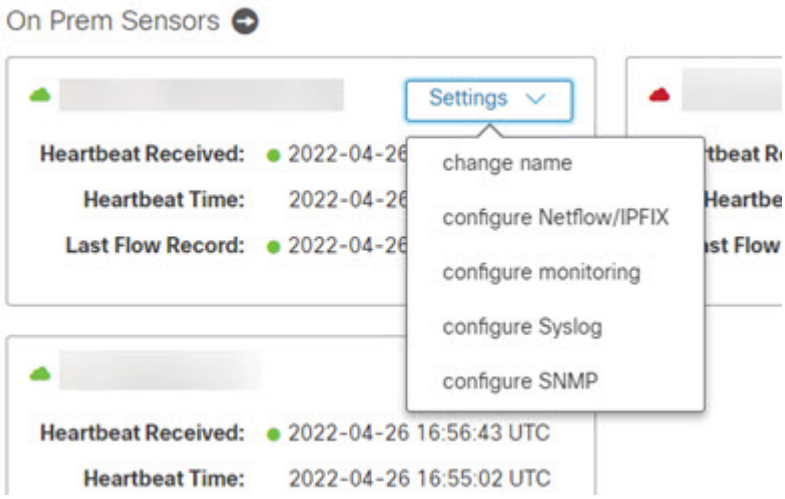
- **アウトバウンド LDAP スパイクアラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、デバイスがLDAPポートを使用して多数の外部ホストと通信しているときに表示されます。これは、ホストが感染したこと、または内部でポートスキャンが開始されたことを示している可能性があります。
- **新しい外部サーバーアラートからの異常なファイル拡張子**：新しい外部サーバーで内部デバイスと新しいファイル拡張子を交換するときに識別を行う、新しいアラートが追加されました。これは、マルウェアがコマンド アンド コントロール センターと通信しようとしていることを示している可能性があります。このアラートには、ファイアウォールデータと Netflow データの両方が必要です。このアラートはデフォルトで無効になっています。
- **疑わしい DNS over HTTPS アクティビティアラート**：内部サーバーで HTTPS 経由で DNS サーバーとトラフィックを交換していることが確認された場合の、新しいアラートが追加されました。これは、DNSベースのセキュリティを回避しようとしていることを示している可能性があります。このアラートはデフォルトで無効になっています。
- **反復的な Cisco Umbrella シンクホール通信アラート**：デバイスが既知の Cisco Umbrella シンクホールとの定期的な接続をいつ確立したかを識別する、新しいアラートが追加されました。これは、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。このアラートはデフォルトで無効になっています。
- **Cisco Umbrella シンクホールヒットの監視**：デバイスが既知の Cisco Umbrella シンクホールと通信するタイミングを特定する、新しい監視機能が追加されました。この監視は、デバイスが既知の不正なドメインと通信しようとしたことを示しています。

ページのルックアンドフィールの更新：[調査（Investigate）] メニューの次のページを更新して、使いやすさを改善しました。

- 外部サービス（External Services）
- IPアドレス別（By IP Address）
- ユーザー アクティビティ（User Activity）

[センサー（Sensors）] ページの更新：[センサー（Sensors）] ページを更新して、使いやすさを改善しました。次の作業に進んでください。

- 各センサーのステータスタイムスタンプを表示する。
- サービスキーとサービスホスト名にアクセスする。
- SPAN/タップによるインターフェイスのモニタリングを有効にする。有効にするには、[設定（Settings）] > [センサー（Sensors）] > [設定（Settings）] > [モニタリングの設定（Configure Monitoring）] に移動します。



- センサーのパブリック IP を設定する。設定するには、[設定（Settings）] > [センサー（Sensors）] > [パブリックIP（Public IP）] に移動します。
- オンプレミスセンサーごとに Netflow/IPFIX プローブを設定する。設定するには、[設定（Settings）] > [センサー（Sensors）] > [選択したNetflow/IPFIX（Selected Netflow/IPFIX）] に移動します。

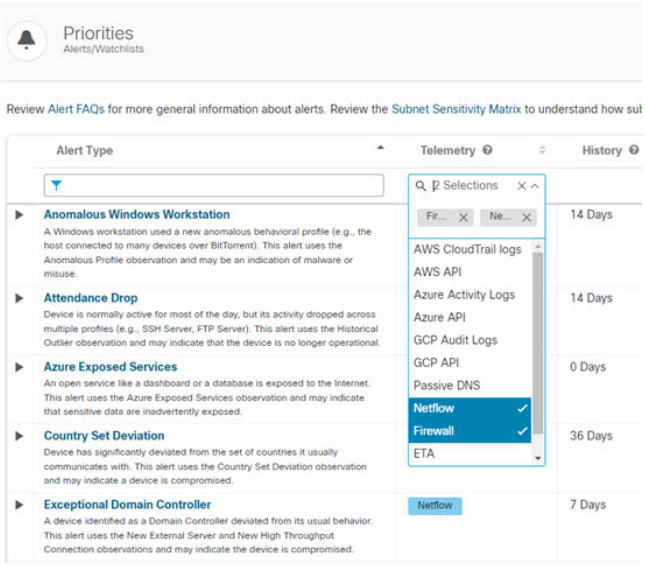
2022 年 3 月

アラートと監視の更新：

- **Azure 関数呼び出し回数のスパイクアラート**：Azure 関数の呼び出し回数が異常に多くなったときに行う、新しいアラートが追加されました。これは、運用上の問題またはサービス妨害（DoS）攻撃の発生を示している可能性があります。このアラートはデフォルトで無効になっています。
- **ICMP 悪用アラート**：異常に大きな ICMP パケットを新しい外部サーバーに送信するデバイスを特定するための、新しいアラートが追加されました。これは、攻撃者が ICMP プロトコルをコバート通信チャネルとして使用してデータを盗み出していることを示している可能性があります。このアラートはデフォルトで無効になっています。
- **クラウドアカウントへの Azure データ転送アラート**：この既存のアラートは有効性レビューを通過し、デフォルトで有効になっています。アラートは、外部からアクセス可能なスナップショットが仮想マシンに作成されたときに通知を行います。これは、データを盗もうとする試みの存在を示している可能性があります。
- **インバウンド ポート スキャナ アラート**：この既存のネットワークタイプアラートによって、優先順位の低いサブネット内で定義したデバイスが無視されるようになります。サブネットの感度は、[設定（Settings）] > [サブネット（Subnets）] に移動して調整できます。
- **疑わしいリモートアクセスツールのハートビートアラート**：RevengeRAT 署名を識別する機能が改善されました。

- **新しいファイル拡張子の監視**：デバイスが新しいファイル拡張子を外部 IP と交換した時期を特定する、新しい監視機能が追加されました。この動作は、他の要因と組み合わされて、マルウェアの存在を示している可能性があります。この監視には、ファイアウォールデータが必要です。
- **Talos の疑わしいアクティビティの監視**：既存の監視機能が更新され、より広範なリモートアクセスツールが識別されるようになりました。
- **異常なパケットサイズの監視**：既存の監視機能が拡張され、エコーパケット内の異常なパケットサイズが識別されるようになりました。

アラートの優先順位をテレメトリでフィルタリング：[アラートの優先順位（Alert Priorities）] ページを 1 つ以上のテレメトリタイプでフィルタリングできるようになりました。このビューをフィルタリングして、どのアラートタイプがどのタイプのテレメトリを必要とするか、およびテレメトリタイプを Cisco Secure Cloud Analytics に統合することによって得られる可能性のある追加のアラートについて理解します。



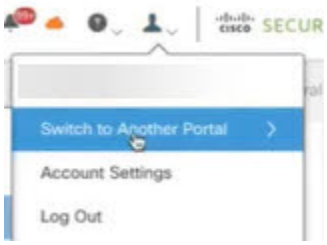
Azure 統合の更新：Azure `Network Contributor` ロールの割り当てが不要になりました。このロールは [Azure統合（Azure Integrations）] ページから削除されており、Azure インスタンスから安全に削除できます。

Azure ログ分析ウェブフック：Azure ログ分析をサポートされるウェブフックの対象として設定できるようになりました。これを使用してアラートを Azure に投稿し、Azure Sentinel にルーティングできます。詳細については、[設定（Settings）] > [Webhook/サービス（Webhooks/Services）] > [Azureログ分析（Azure Log Analytics）] に移動してください。

GCP ステータスのモニタリング：[GCPログイン情報（GCP Credentials）] ページを使用して、プロジェクトおよびリージョンごとに GCP 統合のステータスをモニタリングできるようになりました。モニタリングの詳細は、[設定（Settings）] > [統合（Integrations）] > [GCP] > [ログイン情報（Credentials）] に移動すると表示されます。

ISE 統合ガイド：ISE セットアップ手順が改善されました。これらの手順は、[設定（Settings）] > [統合（Integrations）] > [ISE] で確認できます。

ポータル選択メニュー：複数のポータル/テナントにアクセスできる場合、ログアウトせずにビューを変更できるようになりました。ログインした状態でユーザーアイコンをクリックし、[別のポータルに切り替える（Switch to Another Portal）] に移動して、表示するポータルを選択します。



センサーパッケージの更新：センサーがより多くの Palo Alto ファイアウォールをサポートするために、NetSA パッケージの新しいバージョンを利用できます。『Private Network Monitoring Advanced Configuration Guide』の手順を使用してセンサーを更新するか、次の手順を使用してパッケージを個別に更新できます。

1. 以下のコマンドを入力します。

```
curl -o netsa-pkg.deb --location
https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.deb
sudo apt-get install libsnappy1v5
sudo systemctl stop obsrvbl-ona.service
sudo dpkg -i netsa-pkg.deb
sudo systemctl start obsrvbl-ona.service
```

2. ona サービスが再起動するまで数分待ちます。
3. ポータル Web UI にログインします。
4. [設定（Settings）] > [センサー（Sensors）] を選択します。リストにセンサーが表示されていることを確認します。

2022 年 2 月

アラートと監視の更新：

- 39 の追加アラートを MITRE ATT&CK の戦術とテクニックにマッピングしました。これにより、アラートの詳細と [設定（Settings）]>[アラート（Alerts）]>[優先順位（Priorities）] ページ内に追加のコンテキストが提供されます。
- **LDAP 接続スパイクアラート** ：デバイスが異常に多数の内部 LDAP サーバーへの接続を試みた場合の新しいアラートを追加しました。このアラートはデフォルトで無効になっています。
- **アウトバウンド LDAP 接続スパイクアラート**：デバイスが LDAP ポートを使用して多数の外部ホストと通信している場合の新しいアラートが追加されました。このアラートはデフォルトで無効になっています。

- **異常なユーザーエージェントの監視**：デバイスに異常なユーザーエージェント文字列がある場合の新しい監視が追加されました。

IP スキャナルールの一括削除：API エンドポイント `ip_scanner_allowlist/bulk/` を使用して、特定のルール ID またはすべてを指定して、IP スキャナ許可リストから IP スキャナルールを一括削除できるようになりました。

新しい役割：セキュリティ分析およびロギング（SaaS）を有効にしている場合、Linux デバイスと Sony PlayStation が [役割（Roles）] ページで識別されるようになりました。

新しいプロファイルタグ：

- **ShoreTel プロファイルタグ**：ShoreTel VoIP テレフォニーアプライアンスを識別するための新しいプロファイルタグが追加されました。
- **TikTok プロファイルタグ**：TikTok と通信するデバイスを識別するための新しいプロファイルタグが追加されました。

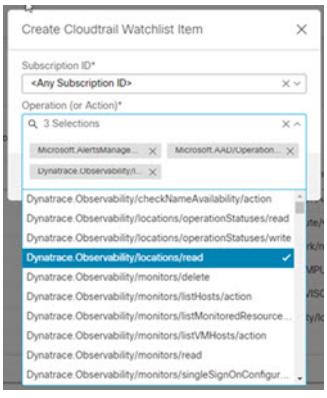
SecureX 統合の強化：SecureX のインスタンスを統合するプロセスがより合理化されました。詳細については、『SecureX Integration Guide』を参照してください。

2022 年 1 月

AWS ECS 統合の改善：コンテナ化された環境のモデリングを改善するために、AWS 統合に権限が追加されました。要求された新しい権限を追加するには、IAM ロールポリシードキュメントを更新する必要があります。詳細については、[設定（Settings）] > [統合（Integrations）] > [AWS] > [バージョン情報（About）] に移動します。

Azure アクティビティ ログ ウォッチリストの改善：[Cloudtrail ウォッチリストアイテムの作成（Create Cloudtrail Watchlist Item）] メニューに次のものが含まれました。

- 提案された操作/アクションのリスト。
- 複数の操作/アクションを同時に作成する機能。



アラートの更新：AWS Elastic Load Balancer の誤検出を防ぐために、国のセットからの逸脱アラートが改善されました。

2021 年 12 月

アラートの更新：ポート悪用の疑い（外部）の動作を改善し、説明を更新しました。

GitHub プロファイルタグで使用されるピア IP のセットを更新しました。

2021 年 11 月

Cisco Stealthwatch Cloud 製品のブランド名を Cisco Secure Cloud Analytics に変更しました。

Cisco Secure Cloud Insights との統合：

- Secure Cloud Insights API を使用して、Secure Cloud Insights データベースに IP アドレスとデバイス情報をクエリします。
- 詳細については、ポータルで [設定（Settings）] > [統合（Integrations）] > [Cisco Secure Cloud Insights] に移動します。

AWS CloudTrail ウォッチリスト ドロップダウン セレクタ：複数のアカウントにわたる選択が改善されました。

アラートの更新：meterpreter コマンドおよびコントロールの成功 が公開されました。

2021 年 10 月

全体としてのサービスへのアプリケーションに対する論理的な可視性をコントローラによって監視することにより、Kubernetes の検出を強化しました。

VPC モニタリングステータスとカバレッジのギャップを可視化するための AWS VPC Cloud カバレッジレポート。

構成を簡単にするために、スキャナルールの検索とフィルタ処理が更新されました。

デバイスアウトラインパネル：アラートの詳細ページで、別のパネルに追加のデバイスコンテキストが表示されるようになりました。

アラートの更新：DNSやその他の信頼できるサービスの誤検出を防ぐために、潜在的なデータ漏洩が改善されました。

2021 年 9 月

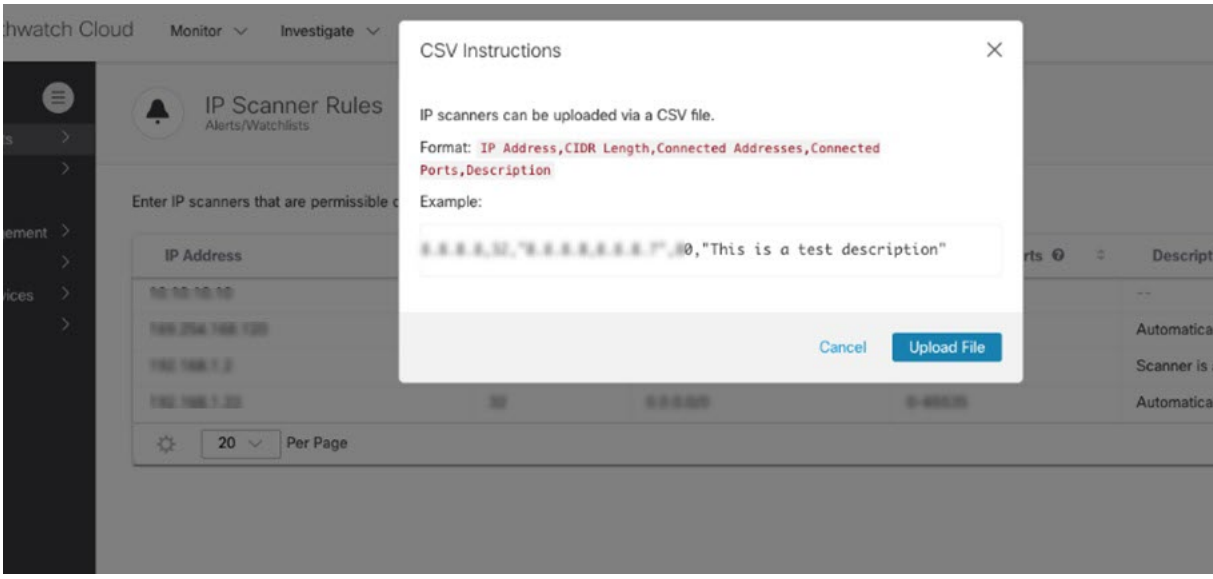
アラートの優先順位による電子メールの頻度のカスタマイズ：[設定（Settings）] > [アカウント管理（Account Management）] > [電子メール（Email）] に移動し、[アラートの更新（Alert Updates）] セクションを使用して、アラートの優先順位に基づいて電子メールの頻度を調整します。

AWS VPC モニタリングステータス：提供された AWS ログイン情報から取得されたすべての VPC のテーブルが表示され、モニタリングステータスが表示されます。[アカウント設定（Account Settings）] > [統合（Integrations）] > [AWS] > [VPC フローログ（VPC Flow Logs）] を選択します。

AWS EC2 起動スクリプトの変更アラート：AWS EC2 インスタンスの起動スクリプトが変更されました。このアラートは AWS CloudTrail イベント監視を使用しており、悪意のある実行者による永続化の確立または悪意のあるコードの実行の試みを示している可能性があります。

ワーム伝達のアラート：以前に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。アラートはさらに調査と改良が行われており、現在デフォルトで無効になっています。

スキャナルールを構成するための IP スキャナの一括インポートが追加されました。

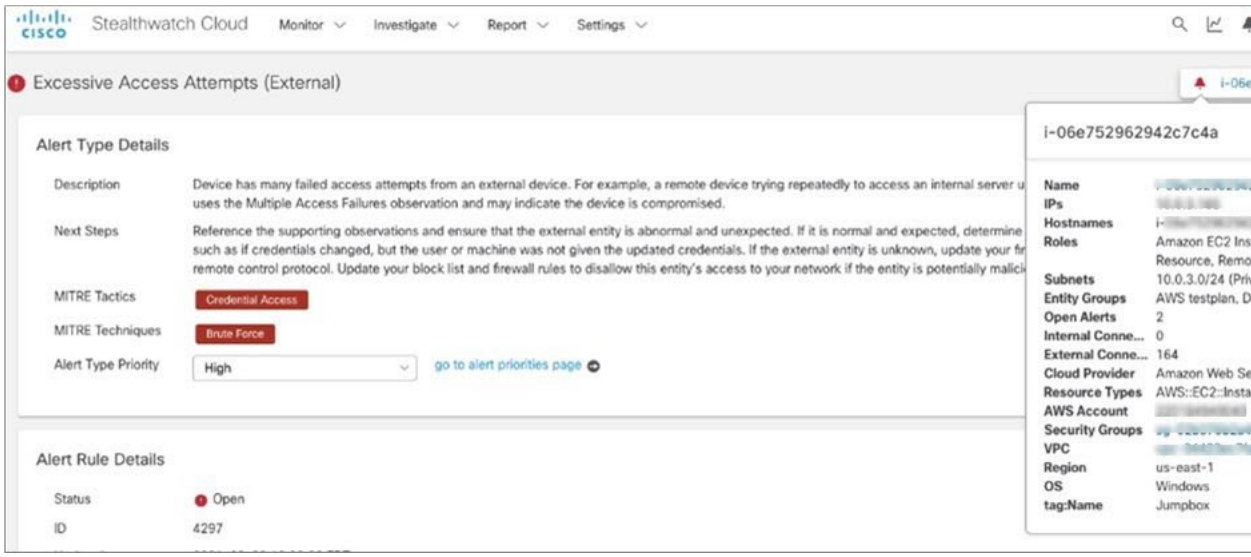


アラートの詳細ページに [デバイスの概要（Device Outline）] セクションを追加し、アラートのトリアージ中に追加のデバイスコンテキストをすぐに利用できるようにしました。

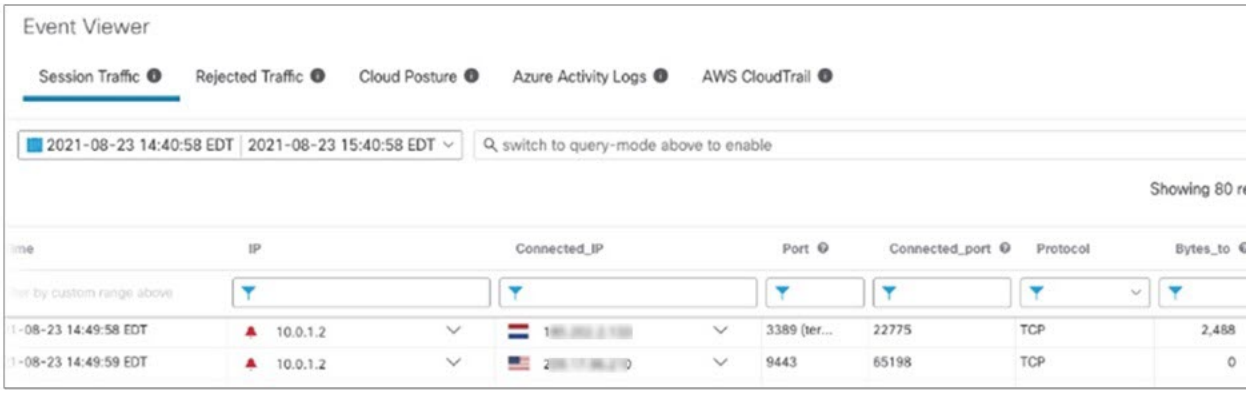
2021 年 8 月

キーローテーションのために複数の API キーを管理する機能が追加されました。

[デバイスの詳細（Details for Device）] に AWS リンクが追加されました。



イベントビューアにすべてのフィールドをダウンロードするオプションが追加されました。



新しいアラート（デフォルトではオフ）：

- S3 バケットのライフサイクル構成済みアラートが追加されました。

  バケット内のすべてのファイルの同時永久削除をスケジュールする新しい S3 バケットライフサイクル構成が作成されました。このアラートは AWS CloudTrail イベント監視を使用しており、データ廃棄の試みを示している可能性があります。

- meterpreter コマンドおよびコントロールの失敗アラートが追加されました。

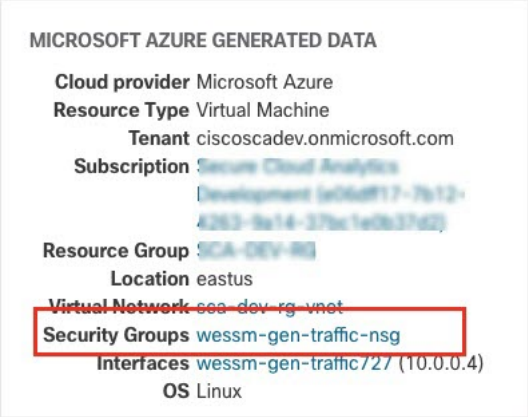
  デバイスは、meterpreter コマンドおよびコントロールチャネルの一部であるように見える新しい定期的な接続を確立しようとしました。このアラートは、ハートビートの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。

- meterpreter コマンドおよびコントロールの成功アラートが追加されました。

  デバイスは、meterpreter コマンドおよび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。

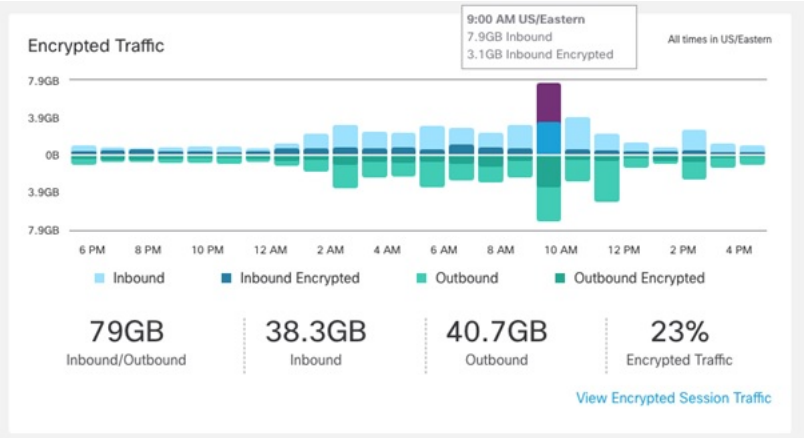
- AWS Lambda 永続化アラートが追加されました。

Azureデバイスコンテキストの更新：アラートリストのホバーとアラートの詳細ページにセキュリティグループを追加しました。

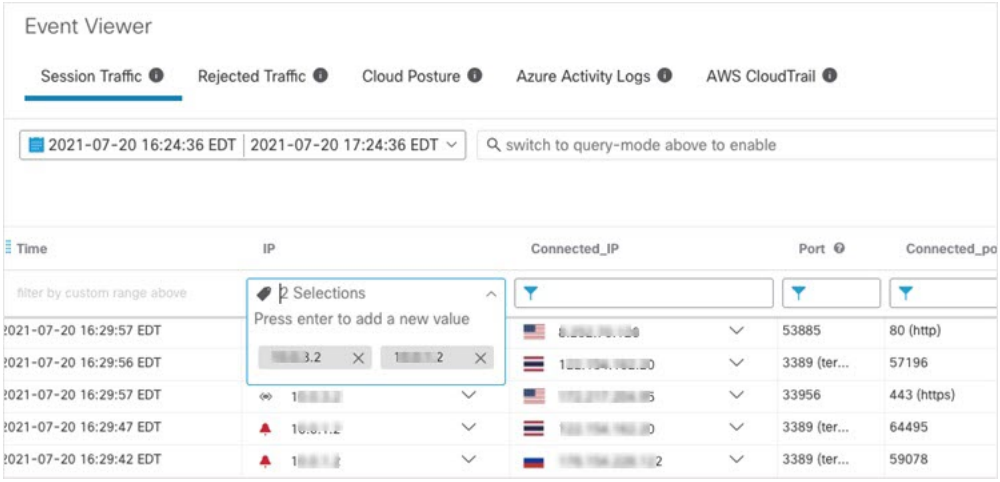


2021 年 7 月

フィルタ処理されたセッショントラフィックにリンクする棒グラフをクリックするトラフィックウィジェット機能が暗号化されました。



イベントビューアに IP とポートの複数選択エントリまたは一括コピーおよび貼り付けによる挿入が追加されました。

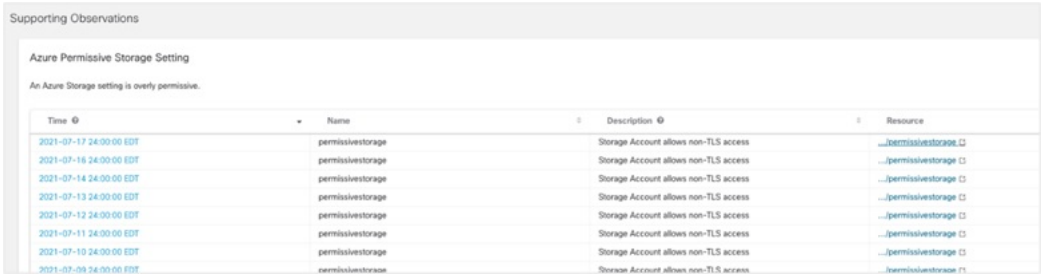


監視タイプにテレメトリソースが追加されました。

イベントビューアでの永続的な列のサイズ変更。

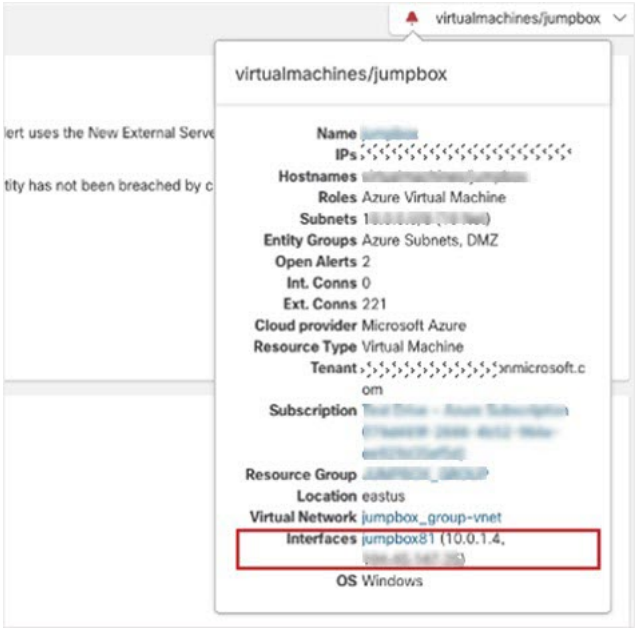
API で利用可能な監視のためのネットワークセッション情報がサポートされています。

Azure ベースの監視では、影響を受けるリソースの Azure ポータルへのリンクが提供されます。

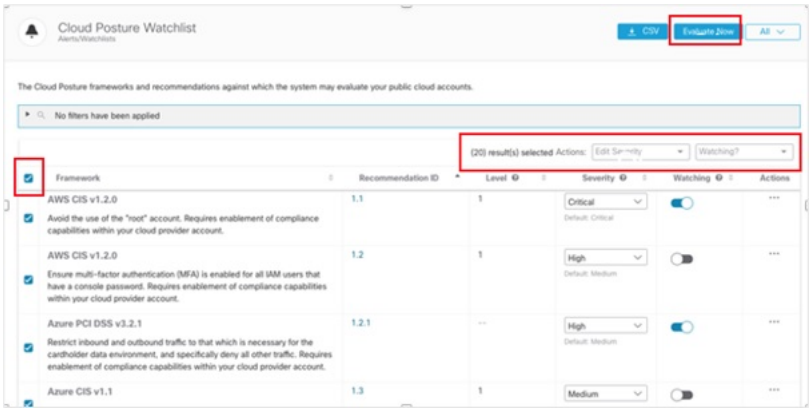


2021 年 6 月

[デバイス情報（Device Info）] で Azure ネットワーク インターフェイスを利用できるようになりました。



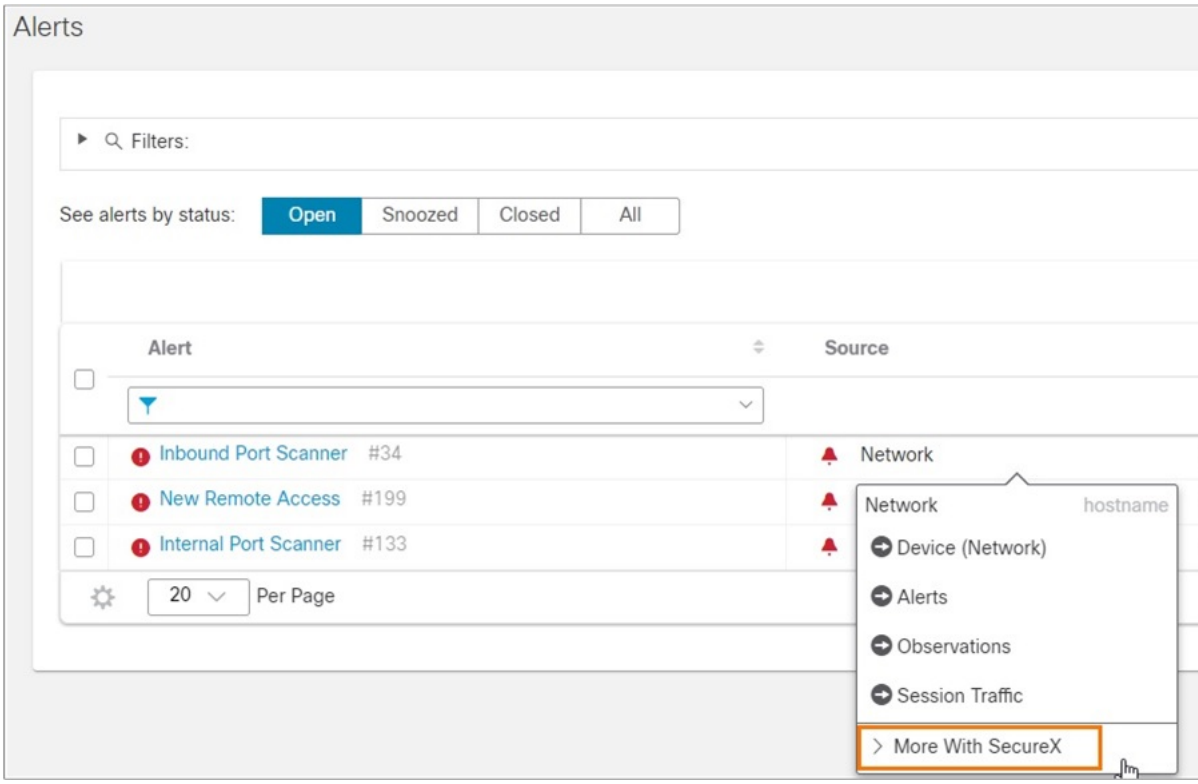
Cloud Posture のオンデマンド ウォッチリスト チェックと一括ウォッチリスト編集。



SecureX 脅威対応では、アラートや監視を含む、外部 IP に関する Secure Cloud Analytics からの目撃情報が表示されるようになりました。

[モニタ（Monitor）] > [アラート（Alerts）] の更新：

- [未割り当て（Not Assigned）] でフィルタ処理する機能。
- [ソース（Source）] ピボットメニューに SecureX リンクが追加されました。



2021 年 5 月

ISE の統合

- テレメトリを Secure Cloud Analytics に送信する ISE を簡単に設定します。
- イベントビューアでデータを表示、クエリ、およびレポートします。
- ISE テレメトリからの追加のコンテキストは、アラートワークフローで利用可能になります（最終リリース日はベータ結果待ち）。

Azure

- 自動展開のセットアップスクリプトをサイトマネージャが利用できるようになりました。
- Azure 関連のアラートまたはデバイスは、Azure アカウントのデバイスへの直接リンクを提供するようになりました。

デバイスのコンテキスト

- 仮想ネットワークの名前、サブスクリプション名、ID（パブリック クラウド アカウントの場合）など、アラートワークフローで提供される追加のデバイスコンテキスト。

DNA Center の統合

- DNA Center 2.2.2.0 以降、ユーザーはフローテレメトリを大規模に Secure Cloud Analytics へ直接送信するように Catalyst デバイスを構成できます。スイッチのコマンドラインで手動で構成する必要はありません。

2021 年 4 月

Cisco Catalyst 9k シリーズとの直接クラウド統合。

スイッチング プラットフォームでコンテナとして Sensor を利用できるため、センサーの追加の展開やインストールを行うことなく、デバイスからクラウドへのテレメトリを簡単に構成できます。

2021 年 3 月

SecureX の機能強化：

- インシデントマネージャの統合 – より詳細な調査のために SecureX にアラートを発行します。
- 新しい 5 つのオーケストレーション ワークフロー。

デバイス情報に、固有の内部および外部ピアが含まれるようになりました。

2021 年 2 月

アラートと監視ページの機能強化：

- 新しい外観。
- 関連するクラウドアカウントに関する追加のコンテキスト。
- 利用可能な新しいフィルタを使用して一括アクションを実行するための更新されたワークフローが含まれています。

クラウドデータストアが東京地域で利用できるようになりました。

AWS CloudTrail と Azure のアクティビティログがイベントビューアで利用できるようになりました。

2021 年 1 月

クラウドポスチャ管理

Secure Cloud Analytics では、追加のセキュリティとコンプライアンスのベストプラクティスに対する AWS または Azure の展開の評価がサポートされるようになりました。イベントビューアの [クラウドポスチャ（Cloud Posture）] タブを使用して、クラウドアセットに関連する最終的な推奨事項の判定を行います。AWS または Azure 内でネイティブ コンプライアンス チェックを有効にした場合、クラウドポスチャには、クラウドプロバイダーからの追加の推奨事項と推奨事項の判定が表示されることがあります。

すでに Secure Cloud Analytics を AWS と統合している場合は、AWS の IAM ポリシーの権限を更新して、AWS のクラウドポスチャレポートを有効にする必要があります。Secure Cloud Analytics の [AWS の概要（AWS About）] ページに、「`"Sid": "CloudCompliance"`」で始まる JSON オブジェクトの必要な権限が一覧表示されます。これらの追加の権限を付与しない場合は、クラウドポスチャレポートを使用できません。

既に Secure Cloud Analytics を Azure と統合している場合は、Azure のクラウドポスチャレポートを有効にするために権限を更新する必要はありません。

2020 年 10 月

エンティティグループ

Secure Cloud Analytics では、組織内外のエンティティのサブセットをより適切に追跡するために、定義できるエンティティの論理グループであるエンティティグループがサポートされるようになりました。エンティティグループは、Secure Cloud Analytics 内部のユーザー定義サブネットと CIDR ブロックに基づいて定義できます。

CIDR ブロックの追加に加えて、エンティティグループを参照するように内部接続ウォッチリストを構成できるようになりました。内部接続ウォッチリストエントリは、内部エンティティ間のトラフィックが検出されたときにアラートを生成するか、しないかのいずれかにすることができ、ネットワーク内の通信をより適切に監視できます。

アラートの優先順位

[アラートの優先順位設定（Alert Priorities Settings）] ページが更新され、より直感的なナビゲーションのために再編成されました。

このページには、アラートタイプと関連する MITRE ATT&CK の戦術とテクニックとの間のマッピングが反映されるようになったため、アラートタイプをよりよく理解し、組織のニーズに基づいて適切な優先順位を割り当てることができます。

更新されたサイトナビゲーション

ユーザーのフィードバックに基づいて、Secure Cloud Analytics の高レベルのポータルナビゲーションが更新され、一般的なワークフローに適切に対処できます。メニューオプションは次のとおりです。

- モニタ（Monitor） - ネットワークの状態を確認し、Secure Cloud Analytics によってログに記録された監視とアラートを表示します。[ダッシュボード（Dashboard）]、[アラート（Alerts）]、および [監視（Observations）] が含まれます。
- 調査（Investigate） - ネットワークの状態に関するコンテキストと情報を収集し、アラートの考えられる根本原因を調査します。[セッショントラフィック（Session Traffic）]、[外部サービス（External Services）]、[デバイス（Device）]、[IP またはドメイン（IP or Domain）]、[暗号化されたトラフィック（Encrypted Traffic）]、[ユーザーアクティビティ（User Activity）]、[アクティブロール（Active Roles）] が含まれます。
- レポート（Report） - ネットワークに関する情報が一目でわかるレポートを生成します。[AWS の可視化（AWS Visualizations）]、[計測レポート（Metering Report）]、[月次フロー

レポート（Monthly Flows Report）]、[サブネットレポート（Subnet Report）]、[トラフィックサマリー（Traffic Summary）]、[可視性アセスメント（Visibility Assessment）] が含まれます。

- 設定（Settings） - Secure Cloud Analytics ポータルを構成およびカスタマイズします。[アラート（Alerts）]、[統合（Integrations）]、[エンティティグループ（Entity Groups）]、[アカウント管理（Account Management）]、[サブネット（Subnets）]、[ウェブフック/サービス（Webhooks/Services）]、および [センサー（Sensors）] が含まれます。
- [エンティティ検索（Entity Search ）] フィールド - エンティティを検索します。
- [ダッシュボード（Dashboard ）] アイコン - ダッシュボードを表示します。
- [アラート（Alerts ）] アイコン - アラートの概要を表示します。
- [Cisco Secure Cloud Analytics センサー（Secure Cloud Analytics sensors ）] アイコン - センサーリストを表示します。
- [ヘルプ（Help）] アイコン - Secure Cloud Analytics の構成および使用方法に関するドキュメントを検索し、オープンソースライセンスとデータプライバシーに関する情報を表示します。[新機能（What's New?）]、[よくある質問（FAQs）]、[API ドキュメント（API Docs）]、[製品ドキュメント（Product Documentation）]、[オンプレミスセンサーのインストール（On-Prem Sensor Install）]、[オープンソースライセンス（Open Source Licensing）]、[プライバシー（Privacy）] が含まれます。
- [ユーザー（User）] アイコン - アカウントのユーザー設定を確認します。[アカウント設定（Account Settings）] と [ログアウト（Log Out）] が含まれます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。