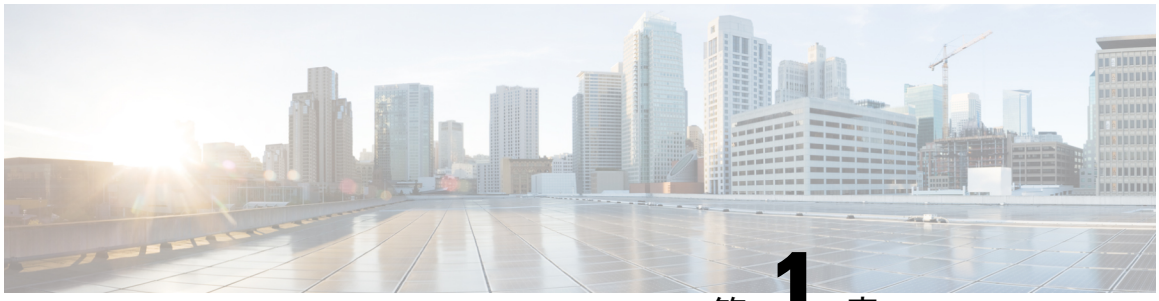
Cisco Secure Cloud Analytics リリースノート

初版：2021 年 1 月 12 日

最終更新：2023 年 3 月 1 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

新機能および改善点

お知らせ

Cisco Secure Cloud Analytics リリースノートは、Cisco XDR ヘルプポータルからのみ入手できるようになりました。Cisco XDR および Cisco Secure Cloud Analytics リリースノートはいずれもこちらからご確認ください。

（注） **Cisco Attack Surface Management**：Cisco Secure Cloud Insights が新たに Cisco Attack Surface Management となり、Cisco Secure Cloud Analytics の Web ポータル内にあるすべての関連資料が更新されました。詳細については、「Cisco Attack Surface Management」にアクセスするか、『Cisco Attack Surface Management (JupiterOne) Release Notes』を参照してください。

2024 年 3 月

アラートと観測の更新

ハートビートの観測：この観測は、Azure インフラストラクチャからの不審なアクティビティを検出するように改善されました。これまでは、Azure アクティビティは信頼できると見なされ、ハートビートの観測から除外されていました。

2024 年 2 月

お知らせ

Cisco Secure Email Threat Defense の統合：Cisco XDR に移行した場合、または Cisco XDR の Advantage もしくは Premier ライセンス階層の利用資格がある場合は、Cisco Secure Email Threat Defense サービスを Cisco XDR で利用できるようになりました。Cisco Secure Email Threat Defense の検出結果では、Cisco XDR 内で相関するインシデントとワークフローを生成し、それらに寄

与することができます。詳細については、『Cisco XDR Third-Party Integrations』を参照してください。

Cisco XDR 統合の一覧表示/削除：Cisco XDR に移行した場合、XDR Analytics 内で統合された XDR 組織を一覧表示または削除するオプションが利用できるようになりました。XDR 組織を表示するには、[設定（Settings）] > [統合（Integrations）] > [XDR] に移動します。特定の組織を一覧表示または削除するために必要な XDR Analytics サイトマネージャ権限があることを確認してください。

GCP Pub/Sub フローログ収集のパフォーマンス：パブリッシャ（Pub）とサブスクライバ（Sub）を使用して Google Cloud Platform（GCP）フローを取得し処理するプロセスが改善されました。

アラートと観測の更新

AWS AppStream イメージ共有アラート：この新しいアラートは、Amazon Web Services（AWS）Appstream イメージが別の AWS アカウントと共有されたことを示します。これは AppStream が提供する正当な機能ですが、Cisco Talos の調査では、データ漏えいや永続化に利用される可能性もあることが示されています。

Azure Anomalous RunCommand アラート：この新しいアラートは、Azure 仮想マシンが実行コマンドをリモートで予期せず実行したことを示します。このアラートは Advanced Persistent Threat（APT）28 または APT 29 を示している可能性があり、組織にとっては異常事態であるため、調査する必要があります。このアラートは、過去 7 日以内に発生した異常に対してのみ表示されます。

2024 年 1 月

お知らせ

Cisco XDR と Microsoft（MS）Defender for Endpoint の統合：Cisco XDR に移行した場合、または Cisco XDR の Advantage または Premier ライセンス階層の利用資格がある場合は、Cisco XDR と MS Defender for Endpoint の統合サービスを利用できるようになりました。MS Defender の検出結果では、Cisco XDR 内で相関するインシデントとワークフローを生成し、それらに寄与することができます。詳細については、『Cisco XDR Third-Party Integrations』を参照してください。

Cisco Secure Cloud Analytics 内では、MS Defender の検出結果は、攻撃者の戦術カテゴリに合わせて不審なエンドポイントアラートとして表示されます。これには、MS Defender 独自の戦術による不審なエンドポイントの検出という新たなアラートが含まれます。

エンドポイントベースのアラートの詳細については、[設定（Settings）]>[アラート（Alerts）] に移動し、[テレメトリ（Telemetry）] 列を [エンドポイント（Endpoint）] でフィルタ処理します。

機能の更新

電子メール管理：**サイトマネージャ**ロールを持つユーザーは、すべてのユーザーのシステム電子メール通知を有効または無効にできるようになりました。[設定（Settings）] > [アカウント管理（Account Management）] > [ユーザー管理（User Management）] に移動し、[電子メール通知（Email Notifications）] トグルを使用して、特定のユーザーアカウントの電子メールを無効にします。

Cisco Meraki タグ：非標準ポートで NetFlow を送信する Cisco Meraki デバイスの適切なアカウントに、新しい Cisco Meraki Netflow コレクタプロファイルタグが追加されました。この新しいタグは、Netflow エクスポータロールに寄与します。

セッショントラフィック ピボット：セッショントラフィック レコードを調査するときに、**[イベントビューア（Event Viewer）]** をクリックして、クエリをイベントビューアに移行できるようになりました。クエリをセッショントラフィックから [イベントビューア（Event Viewer）] > [セッショントラフィック（Session Traffic）] に移行すると、7 日以上経過したレコードを検索できます。

アラートと観測の更新

- **追加のエンドポイントベースの検出**：Cisco XDR に移行しており、エンドポイント ソリューションと統合している場合は、エンドポイントの検出結果にマッピングされる次の 3 つのアラートが追加されています。
  - 調査による不審なエンドポイントの検出
  - リソース開発による不審なエンドポイントの検出
  - 戦術のない不審なエンドポイントの検出
- **MS Defender 独自の戦術による不審なエンドポイントの検出アラート**：この新しいアラートは、そのエンドポイントで検出された、MS Defender 独自の戦術にマッピングされている動作を識別します。
- **不審なプロセスの実行アラート**：Metasploit の実行アラートは、不審なプロセスの実行アラートという名前になりました。

2023 年 12 月

お知らせ

AWS CloudTrail スケーリング：AWS CloudTrail ログと統合すると、AWS S3 ストレージを使用してログを直接収集できるようになりました。API 統合ではなく S3 統合を使用すると、大規模な環境で発生する AWS API スロットリングを修正するのに役立ちます。[設定（Settings）] > [統合（Integrations）] > [AWS] > [CloudTrail] に移動し、S3 を使用して AWS CloudTrail ログ収集を設定します。

Cisco XDR の移行：Cisco XDR への移行を検討している場合、Cisco XDR への参照が統合とワークフローを示すポータル全体に表示されるようになりました。相互接続を管理するには、[Integrations（統合）] > [Cisco XDR とウェブフック（Cisco XDR and Webhooks）] > [Cisco XDR] に移動します。調査中に、SCA と Cisco XDR の間で移行できます。コンテキストメニュー内から、**[Cisco XDRでさらに実行（More with Cisco XDR）]** を選択して Cisco XDR に切り替えます。[アラート（Alert）] > [Cisco XDR にポスト（Post to Cisco XDR）] または [アラートの優先順位（Alert Priorities）] > [XDR に公開（Publish to XDR）] に移動することもできます。

信頼できる外部ネットワーク：サブネット VPN 機能は、**信頼できる外部ネットワーク**に名前が変更されました。関連するサブネットを設定すると、システムでその信頼できるサブネットを管理対象ネットワークの一部のように扱うことができます。

2023 年 11 月

お知らせ

Cisco XDR と CloudStrike の統合：Cisco XDR に移行した場合、または Cisco XDR の Advantage または Premier ライセンス階層の利用資格がある場合は、CrowdStrike Falcon Endpoint Detection and Response（EDR）サービスを Cisco XDR と統合できるようになりました。CloudStrike 統合セキュリティイベントでは、Cisco XDR 内で相関するインシデントとワークフローを生成し、それらに寄与することができます。詳細については、『Cisco XDR Third-Party Integrations』を参照してください。

アラートと観測の更新

- **ハートビート接続回数アラート**：この既存のアラートは、サービス プロバイダー ネットワークで一般的に見られるノイズを排除するために変更されました。このアラートは、多数のリモートデバイスとの新しい定期的な接続を確立したデバイスを識別します。この動作は、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を示している可能性があります。
- **データベースのデータ漏えい疑いアラート**：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。このアラートは、データベースサーバからクライアントに転送された、統計的に異常な量のデータのトラフィックを評価します。この動作は、データ漏洩を示している可能性があります。
- **不審な Curl 動作アラート**：Cisco AnyConnect セキュアモビリティ Network Visibility Module（NVM）をモニターする際に、この新しいアラートは、CVE-2023-38545 のエクスプロイトを示す可能性のある不審な Curl 動作を探します。このアラートはデフォルトで無効になっています。
- **不審なエンドポイントアラート**：Cisco Secure Cloud Analytics 内では、CloudStrike 統合セキュリティイベントは、攻撃者の戦術カテゴリに合わせて不審なエンドポイントアラートとして表示されます。これらのアラートの詳細については、[設定（Settings）] > [アラート（Alerts）] に移動し、[テレメトリ（Telemetry）] 列を [エンドポイント（Endpoint）] でフィルタ処理します。
  - **収集による不審なエンドポイントの検出アラート**：そのエンドポイントで収集の MITRE 戦術にマッピングされている不審な動作が検出されました。
  - **コマンドアンドコントロールによる不審なエンドポイントの検出アラート**：そのエンドポイントでコマンドアンドコントロールの MITRE 戦術にマッピングされている不審な動作が検出されました。
  - **ログイン情報へのアクセスによる不審なエンドポイントの検出アラート**：そのエンドポイントでログイン情報へのアクセスの MITRE 戦術にマッピングされている不審な動作が検出されました。
  - **CrowdStrike 独自の戦術による不審なエンドポイントの検出アラート**：MITRE 戦術にマッピングされていないエンドポイントで不審な動作が検出されました。
  - **防御回避による不審なエンドポイントの検出アラート**：そのエンドポイントで防御回避の MITRE 戦術にマッピングされている不審な動作が検出されました。

- **ディスカバリによる不審なエンドポイントの検出アラート**：そのエンドポイントでディスカバリの MITRE 戦術にマッピングされている不審な動作が検出されました。
- **実行による不審なエンドポイントの検出アラート**：そのエンドポイントで実行の MITRE 戦術にマッピングされている不審な動作が検出されました。
- **データ漏えいによる不審なエンドポイントの検出アラート**：そのエンドポイントでデータ漏えいの MITER 戦術にマッピングされている不審な動作が検出されました。
- **影響による不審なエンドポイントの検出アラート**：そのエンドポイントで影響の MITER 戦術にマッピングされている不審な動作が検出されました。
- **初期アクセスによる不審なエンドポイントの検出アラート**：そのエンドポイントで初期アクセスの MITRE 戦術にマッピングされている不審な動作が検出されました。
- **ラテラルムーブメントによる不審なエンドポイントの検出アラート**：そのエンドポイントでラテラルムーブメントの MITRE 戦術にマッピングされている不審な動作が検出されました。
- **永続化による不審なエンドポイントの検出アラート**：そのエンドポイントで永続化の MITRE 戦術にマッピングされている不審な動作が検出されました。
- **特権昇格による不審なエンドポイントの検出アラート**：そのエンドポイントで特権昇格の MITRE 戦術にマッピングされている不審な動作が検出されました。
- **不審なエンドポイントセキュリティ検出観測**：これは上記のすべての不審なエンドポイントアラートに関する観測です。

2023 年 10 月

お知らせ

観測タイプのフィルタ処理：最も関連性の高いユースケースに基づいて観測タイプをフィルタ処理できるようになりました。[モニター（Monitor）] > [観測（Observations）] > [タイプ（Types）] に移動し、結果をフィルタ処理するためのキーワードを [観測名（Observation Name）]、[カテゴリ（Categories）]、または [テレメトリ（Telemetry）] 列に入力します。たとえば [観測名（Observation Name）] 列でフィルタ処理するには、「エンドポイント（endpoint）」などのキーワードを使用できます。

ユーザー時間設定：アラートを調査する際に、設定した新しいグローバル時間設定が関連する観測に反映されるようになりました。デフォルトの時間設定を行うには、[設定（Settings）] > [アカウント管理（Account Management）] > [時間（Time）] の順に選択し、使用するタイムゾーンを選択します。

アラートと観測の更新

ISE ベースのアラートの調査：Cisco Identity Service Engine（ISE）を統合しており、ISE に基づいてアラートを調査している場合は、関連するユーザーセッションの概要からピボットして、追加の ISE セッションの詳細を表示できるようになりました。たとえば、新しい内部デバイスアラートなどのアラートの詳細を表示する場合は、[ユーザーセッション（User Session）] セク

ションに移動して、[その他のアクション（More Actions）] 列の [イベントビューアでセッションを表示（View Sessions in Event Viewer）] オプションを選択します。新しいブラウザタブが開き、[イベントビューア（Event Viewer）] > [ISE] タブに、関連するユーザーとタイムフレームを含めるようにフィルタ処理されたセッションデータが表示されます。

2023 年 9 月

お知らせ

Cisco ISE のホスト名：Cisco Identity Service Engine（ISE）と統合すると、ISE セッションがホスト名データの追加ソースとして使用されます。ISE ユーザー認証セッション内にホスト名が存在する場合、そのホスト名が UI 全体に反映されます。

アラートと観測の更新

アラートリストの更新：アラートリストをトリアージするときに、確認に役立つ追加のコンテキストが表示されるようになりました。[モニター（Monitor）] > [アラート（Alerts）] の順に選択し、[優先度（Priority）] または [MITRE ATT&CKの戦術（MITRE ATT&CK Tactics）] に基づいてアラートリストを表示およびフィルタリングします。

不審なプロセスの実行アラート：既存のエンドポイントをベースにした Metasploit の実行アラートの名前が変更され、不審なプロセスの動作をより適切に示すようになりました。Cisco AnyConnect セキュア モビリティ クライアントの Network Visibility Module（NVM）をモニターしている場合、このアラートは、エンドポイントで現在 Metasploit が実行中であると検出されたことを示します。将来的には、同じような疑わしいプロセスの動作も検出される予定です。

2023 年 8 月

アラートと観測の更新

- **[AWS ドメインのテイクオーバー（AWS Domain Takeover）] アラート**：この既存のアラートが変更され、状況をより頻繁に評価するようになりました。特定されたアクティビティはドメインを乗っ取ろうとしている可能性があり、将来の攻撃で使用されたり、ランサムウェア攻撃用にドメインを保持したりする可能性があります。
- **[Azure異常アクティビティ（Azure Unusual Activity）] アラート**：次の Azure アクティビティベースのアラートが改善され、正常に実行されたと報告されたアクティビティのみをアラートするようになりました。
  - Azure Firewall の削除
  - Azure Key Vault の削除
  - Azure Network Security Group の削除
  - Azure OAuth バイパス
  - Azure リソースグループの削除
  - クラウドアカウントへの Azure データ転送

- **[GCP Cloud関数呼び出し回数の急増（GCP Cloud Function Invocation Spike）] アラート**：この既存のアラートが、同じ条件のインスタンスを集約するように変更されました。このアラートでキャプチャされたアクティビティは、運用上の問題またはサービス妨害（DoS）攻撃の発生を示す可能性があります。

機能の更新

攻撃チェーンの詳細を更新：詳細ページの [アラートの内訳（Alert Breakdown）] タブを選択すると、攻撃チェーンに関する詳細な調査を実行できます。アラートの詳細とともに、関連する観測、特にアラート動作に寄与した観測の展開可能なリストが表示されます。

NVM CMID コンテキスト：Cisco XDR への移行が完了し、Cisco AnyConnect セキュア モビリティ クライアントの Network Visibility Module（NVM）と統合している場合は、NVM レコードの調査中にコンテキストのエンドポイント情報を表示できます。[調査（Investigate）] > [イベントビューア（Event Viewer）] > [NVMフロー（NVM Flow）] タブを使用して返されたレコードの場合、CMID 値にカーソルを合わせると、関連するエンドポイントのホストとデバイスの情報が表示されます。

Cisco XDR 更新への攻撃チェーンの投稿：Cisco XDR への移行が完了している場合、SCA でクローズされた攻撃チェーンを Cisco XDR インシデントとして昇格できるようになりました。詳細ページの [インシデントとして投稿（Post as Incident）] ボタンをクリックして、攻撃チェーンを Cisco XDR に昇格させます。

メニューとページの更新

ダークモードのテーマ：Cisco Secure Cloud Analytics（SCA）Web ポータルで、ライトビューモードとダークビューモードを切り替えられるようになりました。ポータルヘッダーの右側のセクションで、**月**のアイコンをクリックしてビューを変更します。

グローバルな時刻設定：デフォルトのタイムゾーンと時刻の表示形式を設定できるようになりました。[設定（Settings）] > [アカウント管理（Account Management）] > [時刻（Time）] の順に移動し、時刻形式と優先タイムゾーンを選択します。

2023 年 7 月

お知らせ

攻撃チェーン：より大きな脅威の一部となる可能性があるアラートを関連付けて構築される攻撃チェーンを使用できるようになりました。攻撃チェーンにより、攻撃の早期兆候となる可能性のある潜在的なリスクを調査する時間が短縮されます。抽出されたアラートのメタデータを使用して、アラートに共通するもの（共通インジケータ）を判断します。共通インジケータには、デバイス、IP アドレス、ホスト名、およびユーザー名が含まれます。

次に、MITRE ATT&CK® フレームワークに従って、戦術、手法、および手順（TTP）をさらに詳しく特定し、意図された攻撃の早期兆候を示すアクションと脅威挙動の順序をモデル化します。評価された脅威レベルにより、各攻撃チェーンのシビラティ（重大度）ランキングが次の項目に基づいて割り当てられます。

- 特定された MITRE ATT&CK の戦術
- 関連するデバイスのサブネット感度

- 攻撃チェーン内のアラートの優先度（低/中/高）
- 攻撃チェーン内のアラートの数

また、攻撃チェーンは低/中/高としてランク付けされていることに注意してください。これにより、すぐに調査する必要がある攻撃チェーンを優先させることができます。SecureX がインストールされている場合、高ランクの攻撃チェーンは、インシデントとして SecureX に自動的に昇格されます。

[モニター（Monitor）] > [攻撃チェーン（Attack Chains）] の順に移動して、ネットワークで検出された攻撃チェーンにアクセスします。詳細については、Cisco.com の『Attack Chain Guide』を参照してください。

（注） Cisco Extended Detection and Response（XDR）に移行すると、高ランクの攻撃チェーンは、インシデントとして XDR に自動的に昇格されます。

[NVMフロー（NVM Flow）] タブ：Cisco XDR への移行が完了している場合は、Cisco Secure Cloud Analytics の [NVMフロー（NVM Flow）] タブから Cisco AnyConnect セキュア モビリティ クライアントの Network Visibility Module（NVM）に対するクラウドデータにアクセスできるようになりました。データは、イベントビューアと同様の方法で表示されます。NVM は、AnyConnect VPN が信頼ネットワークに接続し直すたびにエンドポイントからフロー情報を収集します。これにより、リモートデバイスの可視性が向上します。ユーザーが管理対象外デバイスを使用する状況が増加しているため、管理者はネットワーク内外の状況を把握しにくくなっています。NVM は、ネットワークに接続されたデバイスとユーザーの動作を可視化します。

[NVMフロー（NVM Flow）] タブを使用する利点は次のとおりです。

- AnyConnect NVM フィールドの保存
- OS バージョン、OS 名、Mac アドレスなどのエンドポイントフィールドの可視化
- NVM フローからの既存のポリシー違反ルールのトリガー

アラートと観測の更新

- **攻撃チェーンを含むアラートリスト**：[モニター（Monitor）] > [アラート（Alerts）] リストに、関連する攻撃チェーンが含まれるようになりました。アラートのリストを確認すると、攻撃チェーンの一部であるアラートが [攻撃チェーン（Attack Chain）] 列に表示されます。
- **攻撃チェーンを含むアラートの詳細**：攻撃チェーンに含まれるアラートでは、調査している特定の [アラートの詳細（Alert Details）] ページの [アラートタイプの詳細（Alert Types Details）] セクション内にチェーンがリンクされます。
- **エンドポイントベースのアラート**：Cisco XDR への移行が完了し、Cisco AnyConnect セキュア モビリティ クライアントの Network Visibility Module（NVM）と統合している場合は、次のアラートを使用できます。

- **不審な LDAP 接続アラート**：非標準の LDAP プロセスを実行しているデバイスが検出されました。これは、ログイン情報の盗難を試み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。
- **悪意のあるプロセスの検出アラート**：実行中のプロセスに、既知の悪意のあるハッシュリストに含まれるハッシュがあります。
- **Metasploit の実行アラート**：攻撃的なツールである Metasploit の実行が、エンドポイントテレメトリによってエンドポイントで検出されました。
- **ポート8888**：**複数の送信元からの接続アラート**：このアラートは、デバイスとホストが内部の場合にのみ適用されます。主に、複数の内部デバイスが遅延ポートでサービスを提供する内部ホストにファイルを転送する場合を指します。これは、データ漏洩を試みている可能性があります。
- **潜在的な永続化の試行アラート**：ネットワークアクセスに使用されるバックグラウンドプロセスの確立やネットワーク共有からのアプリケーションの実行など、既知の永続メカニズムを適用するデバイスが検出されました。このアラートはデフォルトで無効になっています。
- **潜在的なシステムプロセス偽装アラート**：一般的なプロセスのように見える名前のプロセスが実行されました。これは、プロセスの偽装を示しています。
- **SMB|RDP**：**複数の宛先への接続アラート**：ホストがSMBを使用して複数の宛先ホストにファイルを転送し、RDP を使用してそれらのホストに接続しました。
- **不審なプロセスパスアラート**：実行可能ファイルを持たないディレクトリからエンドポイントでプロセスが実行されました。

- [無効なMacアドレスアラート（Invalid Mac Address Alert）]：Cisco Identity Service Engine（ISE）をSCAと統合している場合、この新しいアラートは、CiscoISEテレメトリを使用して検出された未登録のMacアドレスの組織固有識別子（OUI）がデバイスにあることを示します。これは、Macアクセス制御（Macフィルタリング）をバイパスする、中間者攻撃（Adversary-in-the-Middle）手法を実行する、または他の防御機能を損なうといった試みを示します。このアラートはデフォルトで無効になっています。

ページとメニューの更新

[優先度アラート/ウォッチリスト（Priorities Alerts/Watchlists）] ページの更新：[設定（Settings）] > [アラート/ウォッチリスト（Alerts /Watchlists）] > [優先度（Priorities）] の順に移動して、[優先度アラート/ウォッチリスト（Priorities Alerts/Watchlists）]ページにアクセスします。このページに、アラートタイプから観測タイプへのマッピングが追加されました。[観測タイプ（Observations Types）] 列を使用して、依存関係をフィルタリングして表示します。

[設定（Settings）] メニューの更新：ポータルアカウント関連のメニュー名が更新され、関連するコントロールが明確に示されるようになりました。[設定（Settings）] > [アカウント管理（Account Management）]（以前は [アカウント設定（Account Settings）]）には、特定のユーザーの個々のアカウント設定に関連するページが含まれています。[サイト管理者（Site Admin）] ユーザーの場合、[設定（Settings）] > [アカウント管理（Account Management）] > [ユーザー管

理（User Management）]（以前は [アカウント管理（Account Management）]）で、ポータルのユーザーアクセスを管理できます。

その他の更新

90 日レポートの抽出：[調査（Investigate）] > [イベントビューア（Event Viewer）] を使用すると、最大 90 日前の結果について任意のデータタイプをクエリできるようになりました。クエリをさらに絞り込む場合は、検索条件と調査する時間の範囲を必ず絞り込んでください。

IP スキャナルールの編集：既存の IP スキャナルールを最初の作成後に変更できるようになりました。[設定（Settings）] > [アラート（Alerts）] > [アラート/ウォッチリスト（Alerts/Watchlists）] > [IPスキャナルール（IP Scanner Rules）] の順に移動して既存のルールを編集し、変更する IP スキャナルールで編集（鉛筆）アイコンをクリックします。

セッション接続グラフのデバイスコンテキスト：[調査（Investigate）]>[セッショントラフィック（Session Traffic）] > [セッション接続グラフ（Session Connections Graph）] を使用して IP 接続を調査するときに、デバイス情報の初期セットが含まれるようになりました。コンテキストメニューに情報を表示するには、グラフ内の IP アドレスをクリックします。

TCP フラグレポートの更新：[調査（Investigate）] > [イベントビューア（Event Viewer）] を使用してセッション トラフィック データを調査する場合、[列の管理（Manage Columns）] メニューから使用可能な TCP フラグ情報にアクセスできます。**TCP_Flags** 列と **TCP_Connected_Flags** 列には、セッショントラフィックの検索結果に関する追加情報が表示されます。

2023 年 6 月

アラートと観測の更新

- **[AWSロギングの障害（AWS Logging Impairment）] アラート**：**AWS CloudTrail** ログをモニタリングする場合、この新しいアラートで **AWS CloudTrail** または **VPC フロー**のいずれかのログが削除されたか、収集を停止したことを示します。これは、環境内で防御の回避が試みられていることを示している可能性があります。
- **[Azure Firewallの削除（Azure Firewall Deleted）] アラート**：このアラートは、正常に削除されたファイアウォールに焦点を当てるように改善されました。Azure Firewall が正常に削除されるということは、ネットワーク防御の妨害が試みられていることを示している可能性があります。
- **[新しいAWS Route53ターゲット（New AWS Route53 Target）] アラート**：この CloudTrail アラートが改善され、新しい Route53 の関連付けに関連しない条件が排除されました。このアラートは、悪意のあるトラフィックのリダイレクトを試みる可能性があることを示します。
- **[デフォルトで有効になっているアラートの追加（Additional Alerts Enabled By Default）] アラート**：多くの追加アラートが有効性レビューを通過し、デフォルトで有効になりました。更新されたアラートは次のとおりです。
  - リスクにさらされている Azure サービスアラート
  - 国の設定からの逸脱アラート

- データ漏洩の疑いアラート
- 静的デバイスの逸脱アラート
- 未使用の AWS リソースアラート

- **信頼できる企業のアラート/観測の例外に関する更新**：Cisco Secure Cloud Analytics は、特定のアラートと観測の除外として、考慮、検証、および信頼される企業のリストを保持します。この例外リストが信頼できるグローバル企業リストとなり、次のアラートで動作が変更されます。
  - 国の設定からの逸脱アラート
  - 例外的なドメイン コントローラ アラート
  - ハートビート接続回数アラート
  - ICMP 不正使用アラート
  - 持続的なリモートコントロール接続アラート
  - プロトコル偽造アラート
  - プロトコル違反（地理的）アラート
  - 新しい外部接続アラート
  - 新しい異常な DNS リゾルバアラート
  - 新たな長時間セッション（地理的）アラート
  - 静的デバイス接続の逸脱アラート
  - 異常な外部サーバーアラート
  - 新しい外部サーバーからの異常なファイル拡張子アラート

カスタムテーブルの設定：お使いの Web ポータルで、選択したテーブルのいくつかの設定オプションを調整できるようになりました。テーブルの左下にある**歯車**アイコンを使用して、表示される行数の調整や列の管理を行ったり、長いバイト数を MB/GB に短縮したりできます。

月次フローレポート：日次の有効なフローカウントを可視化するために使用される月次フローレポートに、データをより適切に視覚化するためのテーブルが含まれるようになりました。

2023 年 5 月

アラートと観測の更新

- **Azure アクティビティ ログ ウォッチリストの更新**：関連する検出をトリガーするログ条件を精査することで、Azure アクティビティ ログ ウォッチリスト アラートが改善されました。更新されたアラートは次のとおりです。
  - [Azure Firewallの削除（Azure Firewall Deleted）] アラート

- [Azure Key Vaultの削除（Azure Key Vaults Deleted）] アラート
- [Azure Network Security Groupの削除（Azure Network Security Group Deleted）] アラート
- [Azure OAuthバイパス（Azure OAuth Bypass）] アラート
- [Azure リソースグループの削除（Azure Resource Group Deleted）] アラート
- [クラウドアカウントへのAzureデータ転送（Azure Transfer Data to Cloud Account）] アラート

- **オープンアラート数**：[モニター（Monitor）] > [アラート（Alerts）] ページを使用してアラートリストに移動しているときに、オープンアラートの数が表示されなくなりました。オープンアラートの数を表示するには、画面の右上に表示される**ベル**アイコンにカーソルを合わせます。

2023 年 4 月

アラートと観測の更新

- **ドライブバイダウンロードの観測**：この既存の観測が、外部ホストとの接続によって詳しく焦点を当てるように強化されました。この観測により、リモートホストとの最初の接続後にリモートホストから大量のデータをダウンロードするデバイスが特定されます。これは、悪意のあるペイロードが誤ってダウンロードされたことを示している可能性があります。

AWS 可視化レポートの更新：[レポート（Report）] > [AWS可視化（AWS Visualizations）] の順に移動して表示されるAWS可視化レポートが強化され、使いやすさが向上し、一貫したルックアンドフィールを提供するようになりました。フォーム入力時の一貫性を改善し、関連するグラフが更新されました。

観測の詳細を更新：観測を調査するときに、観測によってキャプチャされたすべてのデータ要素を表示できるようになりました。[アラートの詳細（Alert Details）] ページや [モニター（Monitor）] > [観測（Observations）] ページなどの観測ページ内にある観測テーブルでは、観測の任意のインスタンスをクリックして、すべてのコンテキストデータの行を展開します。

セッショントラフィックの更新：[調査（Investigate）] > [セッショントラフィック（Session Traffic）] ページと、関連するサブタブが強化され、使いやすさが向上し、一貫したルックアンドフィールを提供するようになりました。既存のバグを解決し、フォーム入力時の一貫性が改善され、関連するグラフが更新されました。

2023 年 3 月

アラートと観測の更新

- **[AWSドメインのテイクオーバー（AWS Domain Takeover）] アラート**：**AWS CloudTrail** ログをモニタリングしている場合、この新しいアラートで、AWS ドメインの 1 つが別のアカウントに転送されたことを示します。これは、ドメインのハイジャックが試みられているか、またはセキュリティポリシーの違反を示している可能性があります。

- **[AWS IAMユーザーのテイクオーバー（AWS IAM User Takeover）] アラート**：**AWS CloudTrail** ログをモニタリングしている場合、この新しいアラートで、現在のユーザーが別のユーザーのログイン情報を作成したことを示します。これは、攻撃者が環境内で追加の永続性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。
- **[AWSスナップショットの漏洩（AWS Snapshot Exfiltration）] アラート**：この既存の **AWS CloudTrail** アラートが、追加された一般的な動作をフィルタリングすることで改善されました。このアラートは、EC2 スナップショットが別のアカウントからアクセスできるように変更されたことを示します。これは、攻撃者がデータを盗み出そうとしている兆候である可能性があります。
- **[新たな長時間セッション（地理的）（New Long Sessions (Geographic)）] アラート**：この既存のアラートは、デバイスが国内のウォッチリスト内にあるホストとの長時間の接続を確立したことを示します。追加の信頼ネットワークを除外することで、このアラートが改善され、内部デバイスの動作ベースラインを確立できるようになりました。

イベントビューアクエリのコピー：イベントビューアレポートにつながる調査中に、現在のクエリと、関連するすべてのアクティブなフィルタをコピーして、後で使用したり、チームの他のユーザーと共有したりできるようになりました。[調査（Investigate）] > [イベントビューア（Event Viewer）] ページで結果を表示またはフィルタリングする場合は、[コピー（Copy）] アイコンを使用して、現在の日時、インライン、またはクエリモードのフィルタを URL としてコピーします。その後、URL をブラウザに直接貼り付けることができます。

最初の方向のコンテキスト：イベントビューアでセッション トラフィック レコードを分析する場合は、[最初の方向（First Direction）] フィールドを使用して、トラフィックが観測されたときの方向性に関するコンテキストを確認します。[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）] の順に移動し、[列の管理（Manage Columns）] ボタンをクリックして、[最初の方向（First Direction）] 列をビューに追加します。

Observation.CSV のエクスポート：オフライン調査のために観測リストをダウンロードする場合、**.CSV** ファイルに関連する内部デバイスの IP またはホスト名が含まれるようになりました。[アラートの詳細（Alert Details）] ページまたは任意の観測ページ（[モニター（Monitor）] > [観測（Observations）] > [選択された観測結果（Selected Observations）] など）からダウンロードしたファイル内で **Source.name** を検索します。

上位の高リスク国の調査：メインダッシュボードの [上位の高リスク国（Top High Risk Countries）] マップを確認するときに、関心のある国の関連する観測結果に対して調査を続行できるようになりました。観測で強調表示されている国をクリックすると、その選択した国の [地理情報ウォッチリストの観測（Geographic Watchlist Observations）] にリダイレクトされます。

2023 年 2 月

アラートと観測の更新

- **[ISEユーザーの不正アクション（Abnormal ISE User）] アラート**：この既存のアラートは、関連するアクティビティの時間枠を増やすことで改善されました。Cisco ISE と統合さ

れている場合、このアラートは、通常のデバイスではなく、別のユーザーに関連付けられているデバイスでユーザーが認証されたことを示します。これは、クレデンシャルの侵害または不正な内部関係者を示している可能性があります。

- **[AWS ECSログイン情報へのアクセス（AWS ECS Credential Access）] アラート**：この既存の **AWS CloudTrail** ログベース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。このアラートは、ECS タスク定義が AWS インスタンス メタデータ サービスからログイン情報を取得するコンテナコマンドで登録されたことを示しています。このアクティビティは、攻撃者がサービスログイン情報を取得しようとしていることを示している可能性があります。

- **[AWS IAM Anywhereトラストアンカー作成（AWS IAM Anywhere Trust Anchor Created）] アラート**：この既存の **AWS CloudTrail** ログベース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。このアラートは、新しい IAM Roles Anywhere トラストアンカーの作成を示します。このアクティビティは適切な場合もありますが、攻撃者が AWS の外部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もあります。

- **[AWS Lambda永続化（AWS Lambda Persistence）] アラート**：この既存の **AWS CloudTrail** ログベース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。このアラートは、新しい AWS Lambda 関数が作成されたことを示します。これは、新しく作成されたリソースにバックドアを追加して永続化を試みていることを示す可能性があります。

- **[AWS重複サブネット（AWS Overlapping Subnet）] アラート**：このアラートは削除されています。このアラートは、同じ **AWS VPC** 内で重複するサブネットを示すために使用されていましたが、AWS では設定できなくなくなりました。

- **ドライブバイダウンロードの観測**：この新しい観測は、外部ホストの最初のアクセス後に、デバイスがリモートホストから大量のデータをダウンロードしたことを示します。これは、悪意のあるペイロードが誤ってダウンロードされたことを示している可能性があります。

- **[ジェイルブレイク済みデバイス（Jailbroken Device）] アラート**：Cisco ISE と統合されている場合、Cisco ISE がデバイスを「ジェイルブレイク」として検出したときにアラートを受け取ることができるようになりました。このようなデバイスは、脅威に対して脆弱であり、組織のリスクが増加する可能性があるため、安全ではないと考える必要があります。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AWS Lambda呼び出し許可通知（New AWS Lambda Invoke Permission Added）] アラート**：この既存の **AWS CloudTrail** ログベースのアラートは、追加された有効な AWS アクションを除外することで改善されました。このアラートは、別の AWS サービス、アカウント、または組織でアクションを実行するために新しい呼び出し権限が作成されたことを示します。この動作は、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。

アラートの優先順位をダウンロード：[アラートの優先順位（Alert Priorities）] ページに、Cisco Secure Cloud Analytics の検出スイートに関する貴重な情報をダウンロードするオプションが追加されました。[設定（Settings）]>[アラート（Alerts）]>[優先度（Priorities）] の順に移動し、

[CSV] をクリックして、MITRE ATT&CK マッピング、依存観測、現在のアラート設定などが含まれたファイルをダウンロードします。この情報は、統合計画や外部レビューなどのタスク、またはプレイブックの作成時に使用できます。

ASN 説明コンテキストの更新：自律システム番号（ASN）の説明がすべての外部 IP で使用できるようになりました。この ASN の説明に関する参照情報では、Cisco Talos Threat Intelligence チームによって確立された一般的なシスコのデータセットを使用します。この情報は、すべての外部 IP 参照の左側にあるコンテキストメニューを使用して、調査中に検索できます。ASN CIDR、リージョン、DNS といった外部 IP のより完全な分類については、[設定（Settings）] > [統合（Integrations）] > [Umbrella] にある Cisco Umbrella Investigate 統合を引き続き使用してください。

地理的コンテキストの更新：外部 IP を国にマッピングするために Cisco Secure Cloud Analytics で使用する地理的データセットが更新されました。この地域 IP の参照情報で、Cisco Talos Threat Intelligence チームによって確立された一般的なシスコのデータセットが使用されるようになりました。

セッション詳細の更新：Cisco Telemetry Broker をオンプレミスセンサーとして使用している場合、[調査（Investigate）] > [イベントビューア（Event Viewer）] ページ内のいくつかの [セッション詳細（Session Details）] フィールドに表示される名前が改善または変更されました。

2023 年 1 月

アラートと監視の更新：

- **[ISEユーザーの不正アクション（Abnormal ISE User）] アラート**：Cisco ISE と統合されている場合、別のユーザーに関連付けられている新しいデバイスでユーザーが認証されたときにアラートを受け取ることができるようになりました。これは、クレデンシャルの侵害または不正な内部関係者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。
- **地理情報ウォッチリストの観測に関する検索**：**地理情報ウォッチリストの観測**を調査する場合、国コードに加えて国名で観測のリストをフィルタリングできるようになりました。このフィルタは、[観測内容（Observations）] > [選択された観測内容（Selected Observation）] ページで、地理情報ウォッチリストの観測をピボットした後、または直接調査した後にドリルダウンする場合に使用します。
- [ISEセッション開始観測（ISE Session Started Observation）]：この新しい観測は、新しいセッションが作成されたことを示します。この観測には Cisco ISE との統合が必要です。
- **ISE の疑わしいアクティビティの観測**：この既存の観測は、Cisco ISE を使用して疑わしいアクティビティが検出されたことを示します。この観測が拡張され、ISE によって「ジェイルブレイク」と報告されたデバイスを検索できるようになりました。このようなデバイスは、脅威に対してより脆弱になる可能性があるため、安全ではないと考える必要があります。

AWS 統合の更新：[設定（Settings）] > [統合（Integrations）] > [AWSの概要（AWS About）] ページが更新され、パフォーマンスが向上し、AWS S3 のコストを最小限に抑えるためのオプションが追加されました。Cisco Secure Cloud Analytics との統合のために VPC フローログのみ

を保存する場合は、『Amazon Web Services Integration Quick Start Guide』で、不要になったログを削除する方法の手順を参照してください。

AWS リージョンコンテキスト：**AWS CloudTrail** ベースのアラートを調査するときに、アクティビティが発生した特定の AWS リージョンのコンテキストを検索できるようになりました。関連する **AWS CloudTrail** 観測、または [イベントビューア（Event Viewer）] > [AWS CloudTrail] ログ内で関心のある行を展開し、応答要素で公開されているリージョンを検索できます。

追加のコンテキストピボット：[調査（Investigate）] > [IP別（by IP）] ページと外部 **IP トラフィック**のドリルダウンを使用して IP トラフィックを調査する場合、要約されたメトリックから関連トラフィックまで調査をより簡単に続行できるようになりました。ドリルインするデータの行を特定したら、テーブルの最後の列にある [イベントビューアで会話を表示（See Conversation in Event Viewer）] ピボットを使用します。これらのコンテキストピボットにより、[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、対応する結果を表示できます。

アラート優先順位の更新：[設定（Settings）] > [アラートの優先順位（Alerts Priorities）] および [観測（Observation）] > [タイプ（Types）] ページに、追加のテレメトリタイプとして Cisco ISE が示されるようになりました。このタイプでフィルタ処理して、統合時に使用可能な追加の検出を特定します。Cisco ISE とお使いのポータルの統合に関する詳細については、[設定（Settings）] > [統合（Integrations）] > [ISE] を参照してください。

デバイスの概要更新：[デバイスの概要（Device Outline）] > [プロファイル（Profiles）] セクションは、[アラートの詳細（Alert Detail）] ページとデバイスレポートのパフォーマンスを向上させるために最適化されました。このセクションを使用して、既知の動作に一致するデバイスアクティビティの 7 日間の概要を取得します。

オープンソースソフトウェア：Cisco Secure Cloud Analytics チームが提供するオープンソースソフトウェアが、新しいリポジトリに再配置されました。シスコのオープンソースツールへのリンクがある場合は、ブックマークを更新して反映してください。https://github.com/obsrvbl-oss/

レポートのサイドバー：一貫したエクスペリエンスを提供するために、[レポート（Report）] メニューセクション内のすべてのレポートに左側のナビゲーションメニューが追加されました。

可視性アセスメントの更新：[レポート（Report）] > [可視性アセスメント（Visibility Assessment）] の [リスクの高い国へのトラフィック（Traffic to High-Risk Countries）] セクションに、このセクションで提供される情報の使用方法に関する詳細が追加されました。**地理情報ウォッチリストの観測に関する検索**を使用して、調査を続行します。

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）] アラート**：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 コールを実行したが、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）] アラート**：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）] アラート**：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）] アラート**：AWS CloudTrail ログをモニタリングしている場合、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）] アラート**：AWS CloudTrail ログをモニタリングしている場合、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）] アラート**：AWS CloudTrail ログをモニタリングしている場合、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。

- **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。
- **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。

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：

- **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。
- **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。

[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。

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。

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。

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。

2022 年 5 月

アラートと監視の更新：

- **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。
- **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。
- **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。
- **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。
- **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。

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：

- **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。
- **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。
- **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。
- **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。

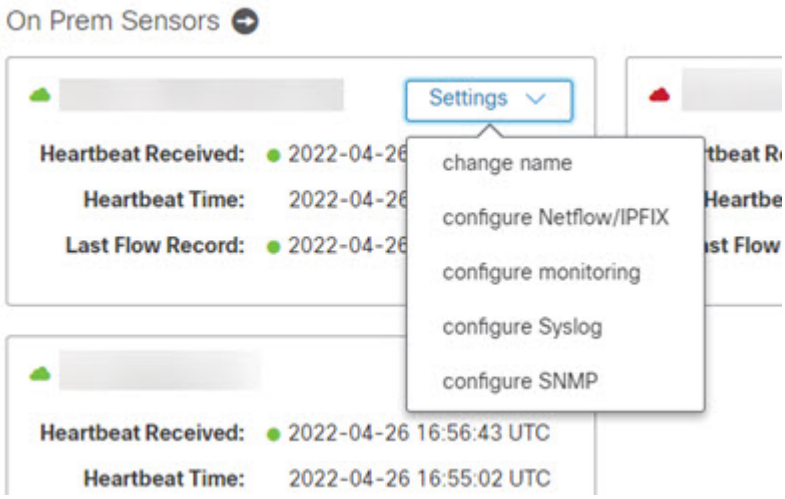
- **Cisco Umbrella シンクホールヒットの監視**：デバイスが既知の Cisco Umbrella シンクホールと通信するタイミングを特定する、新しい監視機能が追加されました。この監視は、デバイスが既知の不正なドメインと通信しようとしたことを示しています。
- **新しい外部サーバーアラートからの異常なファイル拡張子**：新しい外部サーバーで内部デバイスと新しいファイル拡張子を交換するときに識別を行う、新しいアラートが追加されました。これは、マルウェアがコマンド アンド コントロール センターと通信しようとしていることを示している可能性があります。このアラートには、ファイアウォールデータと 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。

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。

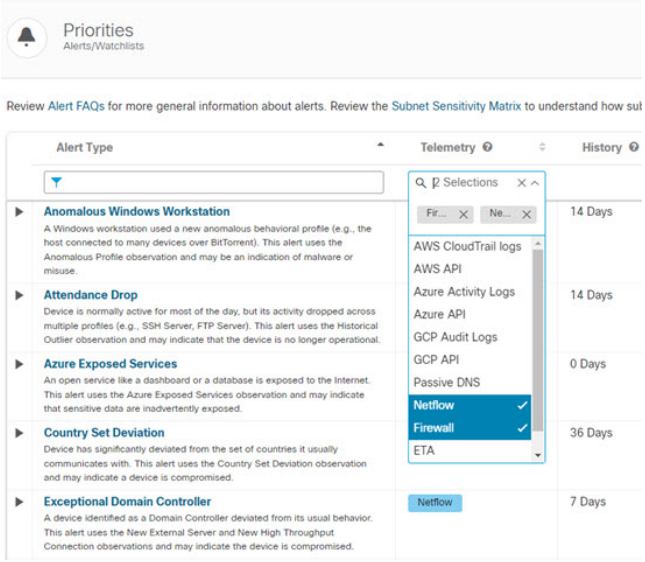
- オンプレミスセンサーごとに Netflow/IPFIX プローブを設定する。設定するには、[設定（Settings）] > [センサー（Sensors）] > [選択したNetflow/IPFIX（Selected Netflow/IPFIX）] に移動します。

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。
- **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。
- **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。
- **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。
- **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。
- **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。
- **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。



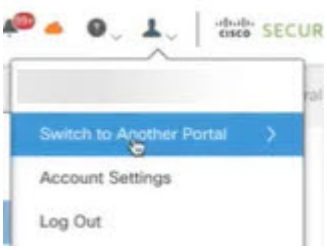
Azure 統合の更新：Azure `Network Contributor` ロールの割り当てが不要になりました。このロールは [Azure統合（Azure Integrations）] ページから削除されており、Azure インスタンスから安全に削除できます。

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：

- **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。
- **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。
- 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。

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。

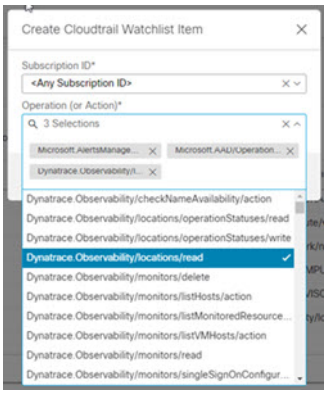
SecureX 統合の強化 ：SecureX のインスタンスを統合するプロセスがより合理化されました。詳細については、『SecureX Integration Guide』を参照してください。

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

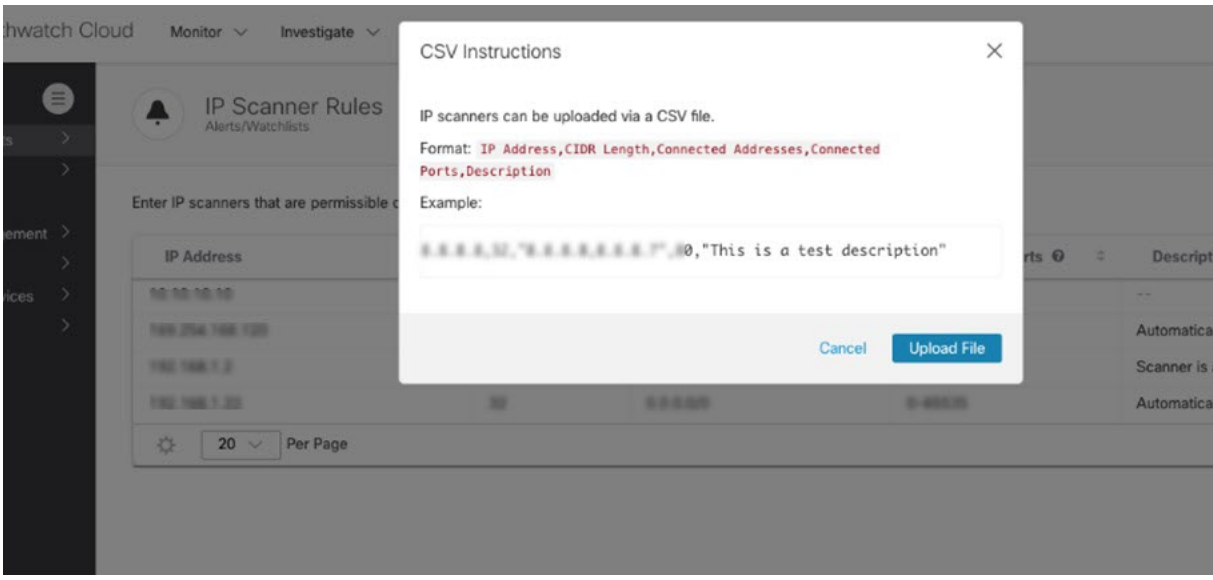
アラートの優先順位による電子メールの頻度のカスタマイズ：[設定（Settings）] > [アカウント管理（Account Management）] > [電子メール（Email）] に移動し、[アラートの更新（Alert Updates）] セクションを使用して、アラートの優先順位に基づいて電子メールの頻度を調整します。

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）] に移動します。

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。

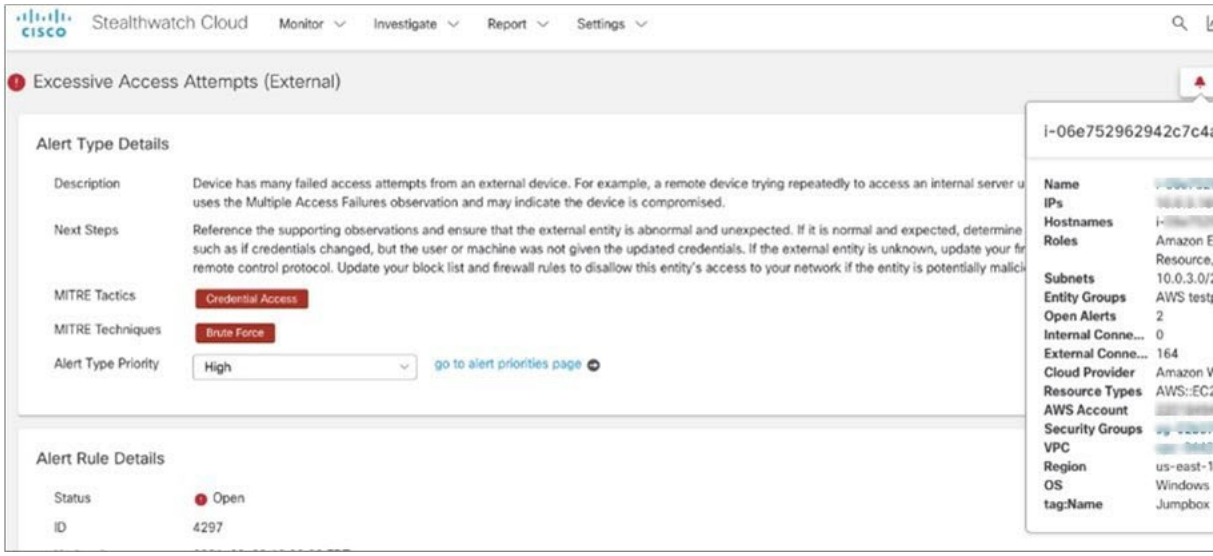


アラートの詳細ページに [デバイスの概要（Device Outline）] セクションを追加し、アラートのトリアージ中に追加のデバイスコンテキストをすぐに利用できるようにしました。

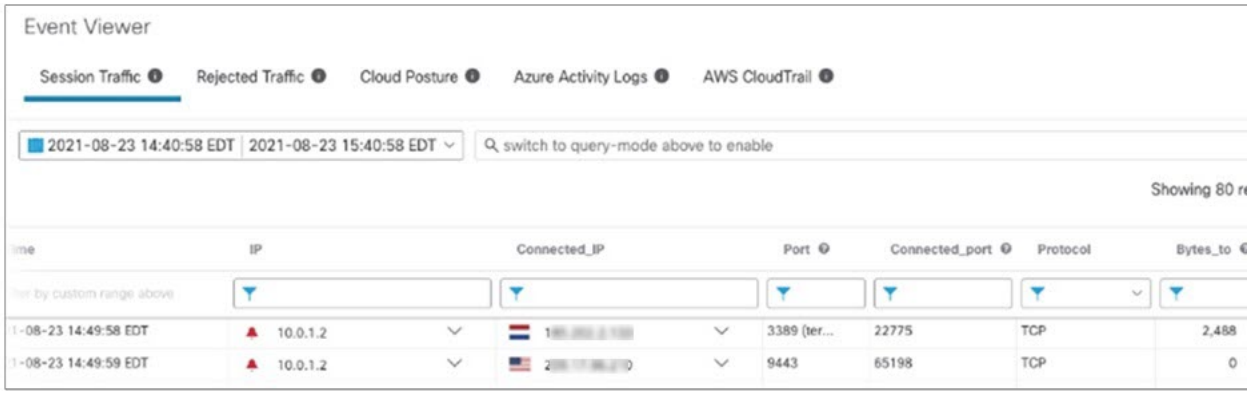
2021 年 8 月

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。

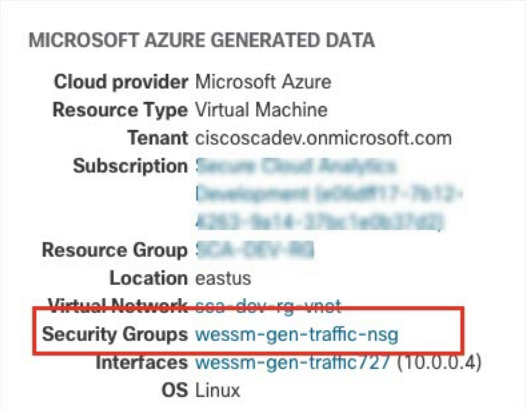
  デバイスは、meterpreter コマンドおよびコントロールチャネルの一部であるように見える新しい定期的な接続を確立しようとしました。このアラートは、ハートビートの観測結果を使用しており、デバイスが侵害されていることを示している可能性があります。

- 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。

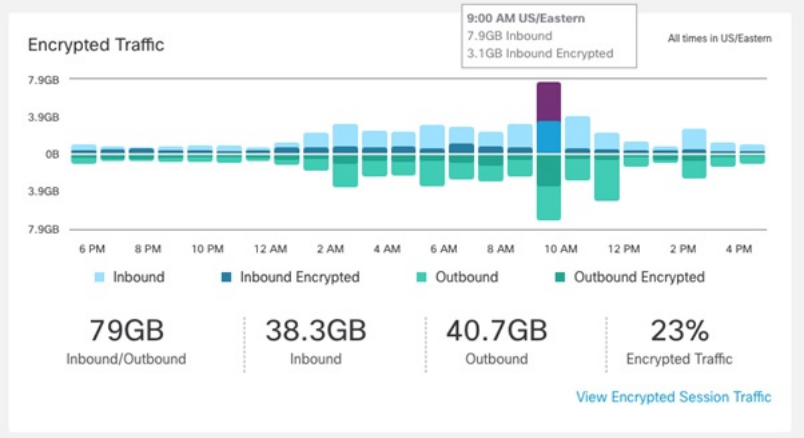
- AWS Lambda 永続化アラートが追加されました。

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。

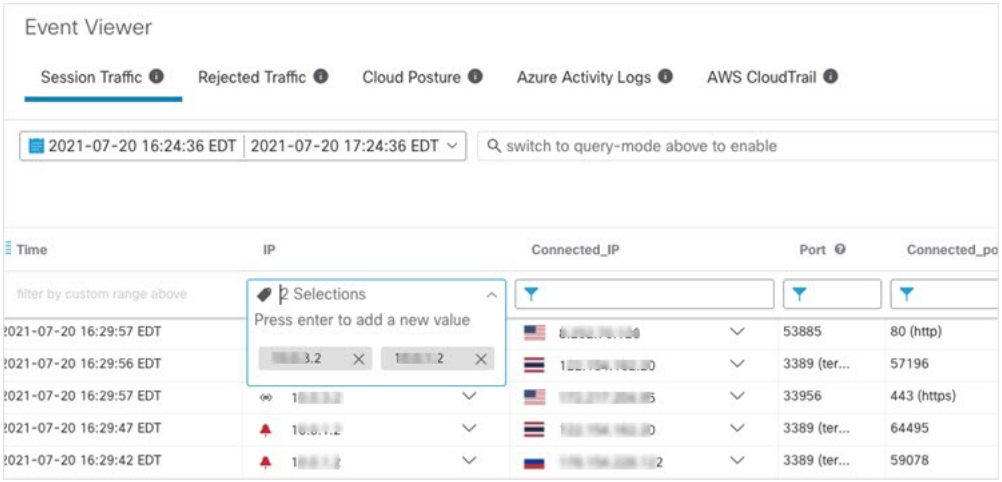


2021 年 7 月

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。

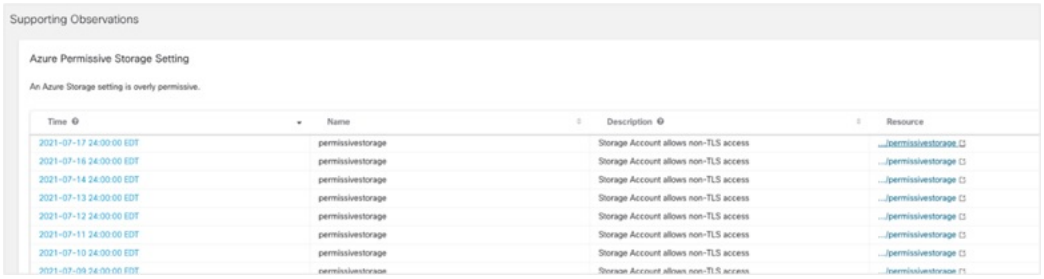


監視タイプにテレメトリソースが追加されました。

イベントビューアでの永続的な列のサイズ変更。

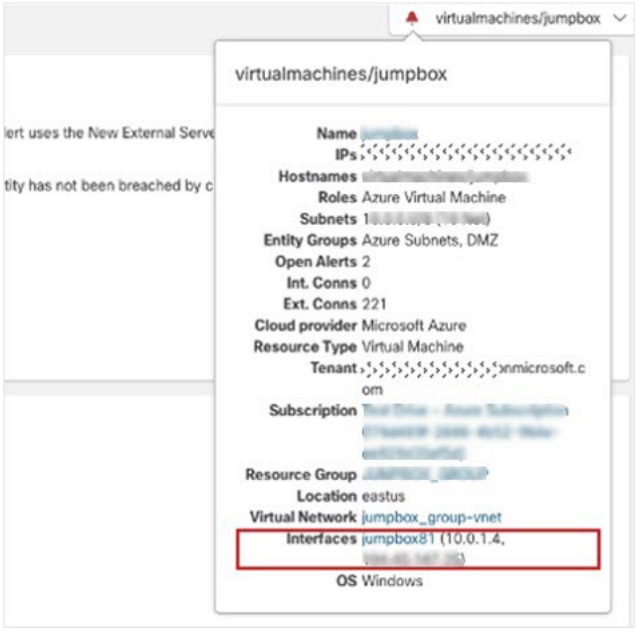
API で利用可能な監視のためのネットワークセッション情報がサポートされています。

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。

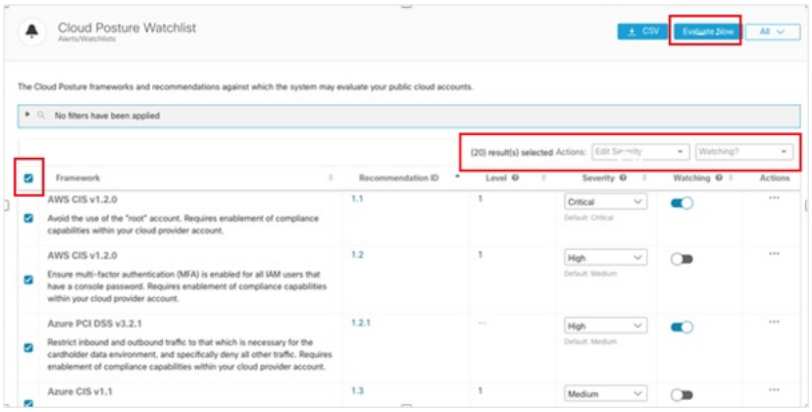


2021 年 6 月

[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。



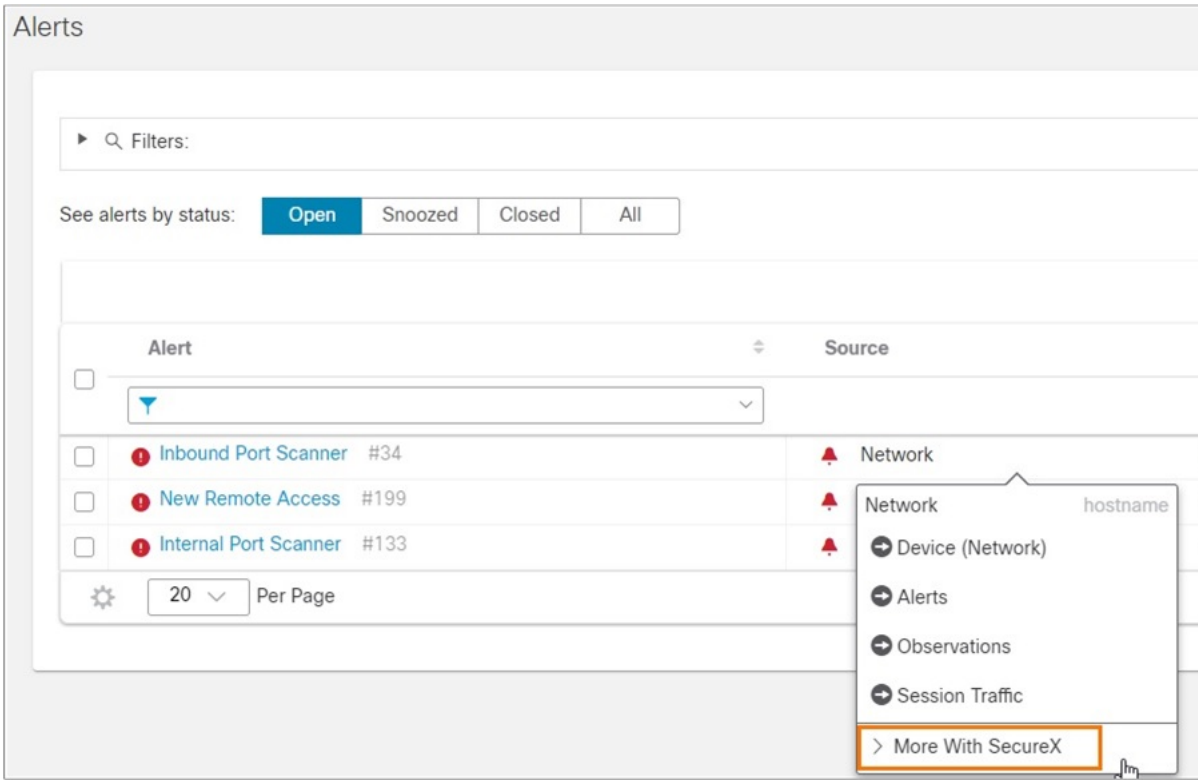
Cloud Posture のオンデマンド ウォッチリスト チェックと一括ウォッチリスト編集。



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。