2022 年 8 月

2022 年 8 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

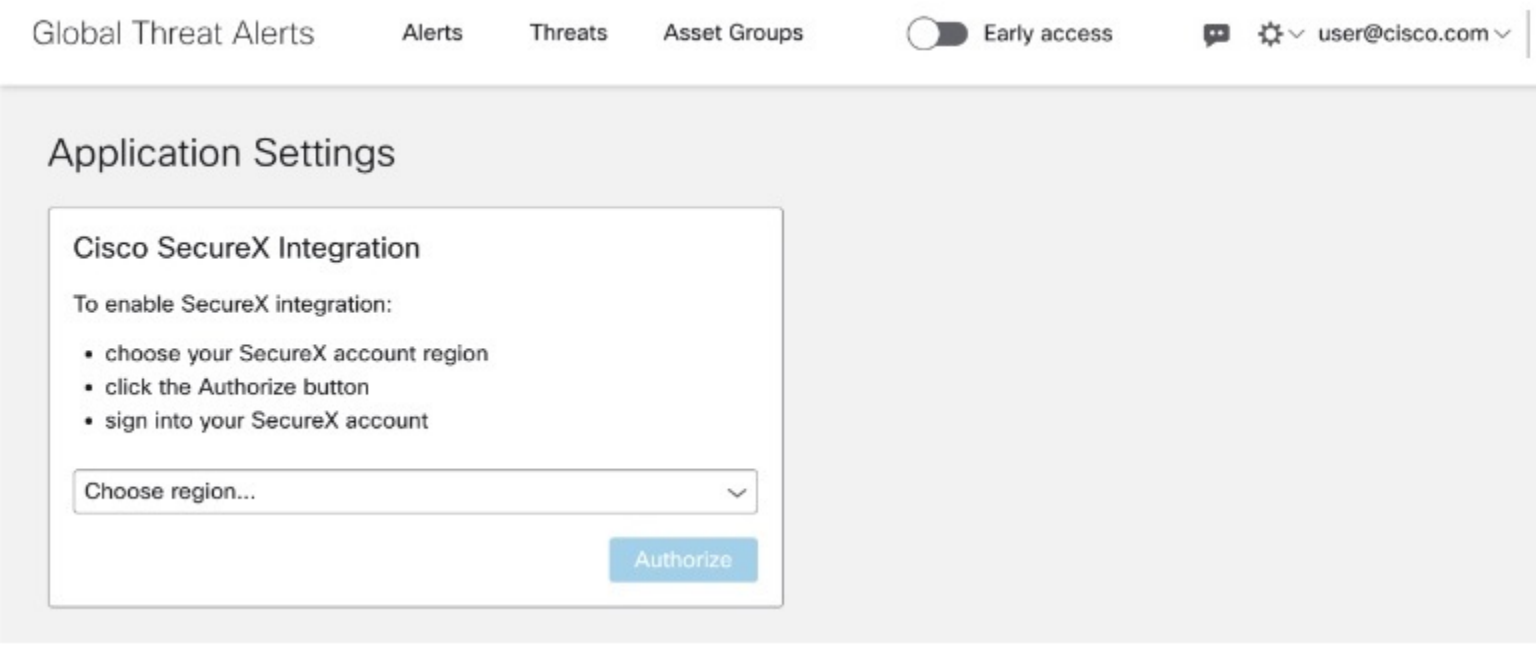
- 改善されたアラートワークフロー （1 ページ）
- 追加の脅威検出 （6 ページ）

改善されたアラートワークフロー

[早期アクセス（Early access）] でアラートを操作する方法を改善し、グローバル脅威アラートでアラートを SecureX incident manager にプロモートする方法を改善しました。

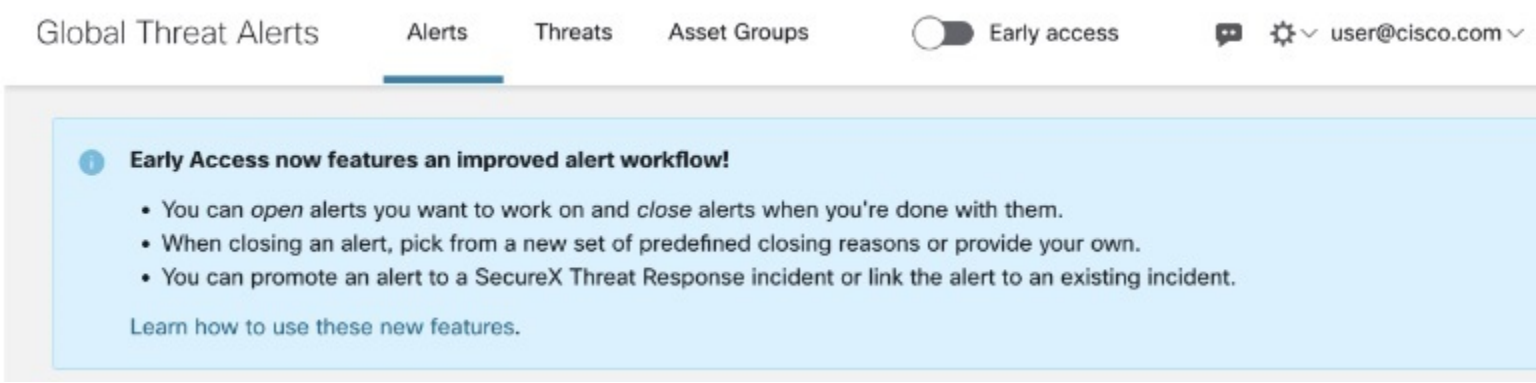
SecureX incident manager との統合のメリットを享受するには、グローバル脅威アラートコンソールの**アプリケーション設定**で SecureX の統合を有効にします。

図 *1* : アプリケーション設定で ***SecureX*** の統合を承認



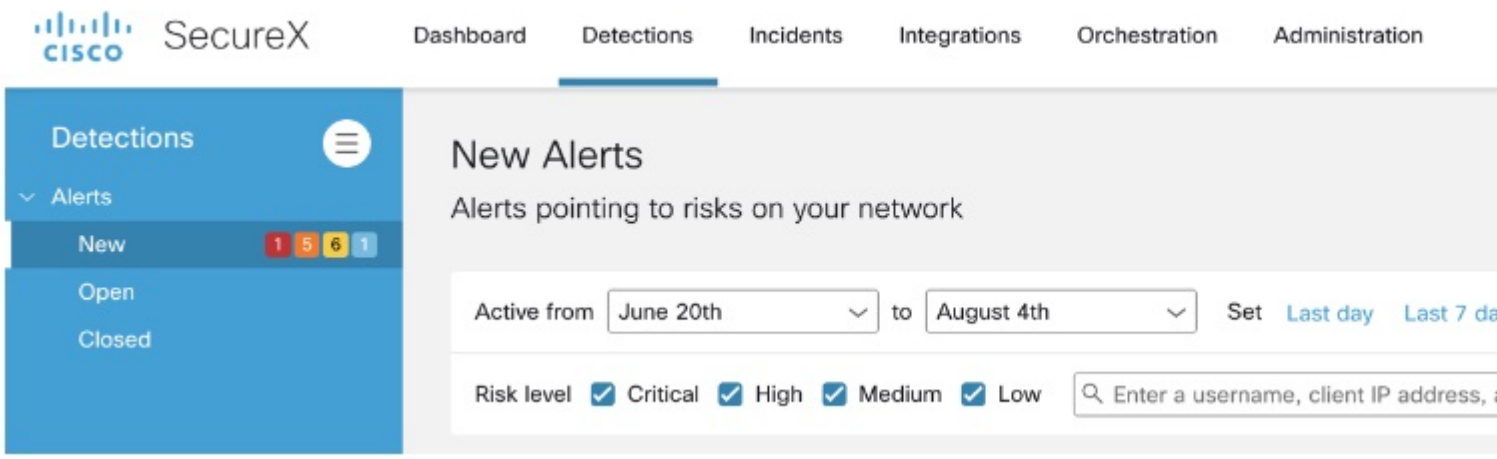
グローバル脅威アラートコンソールのヘッダーで、[早期アクセス（Early access）] をクリックして有効にします。

図 *2* : *[*早期アクセス（***Early access***）*]* をオンにして新機能を有効化



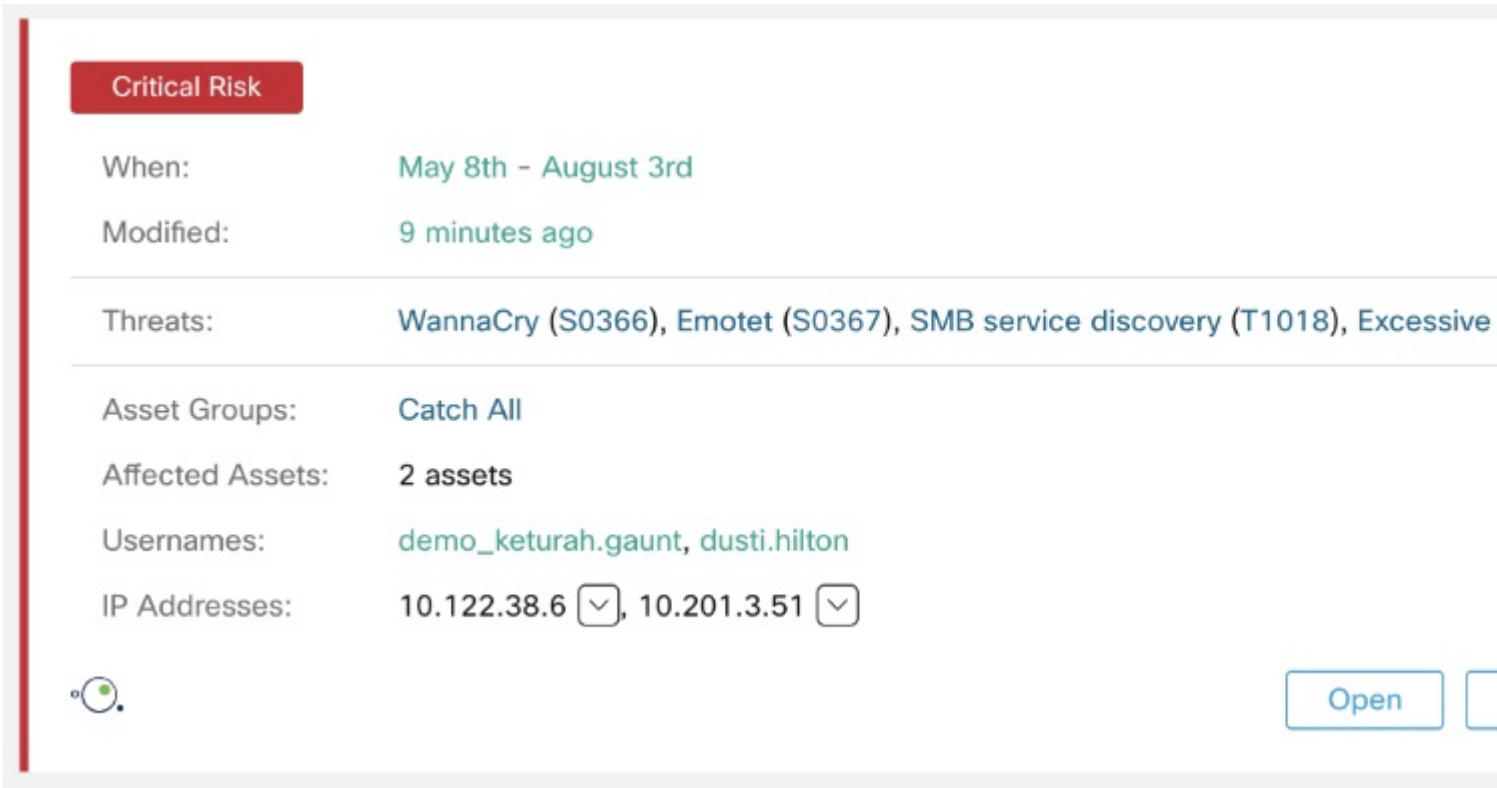
[早期アクセス（Early access）] を有効にすると、アラートは [新規（New）]、[オープン（Open）]、または [終了（Closed）] に分類されます。

図 *3 : [*新規（***New***）*]*、*[*オープン（***Open***）*]*、*[*終了（***Closed***）*]* のステータスのカテゴリのアラート



[新規（New）] アラートのステータスは、[開く（Open）] または [閉じる（Close）] ボタンを使用して変更できます。

図 *4 :* アラートの開閉

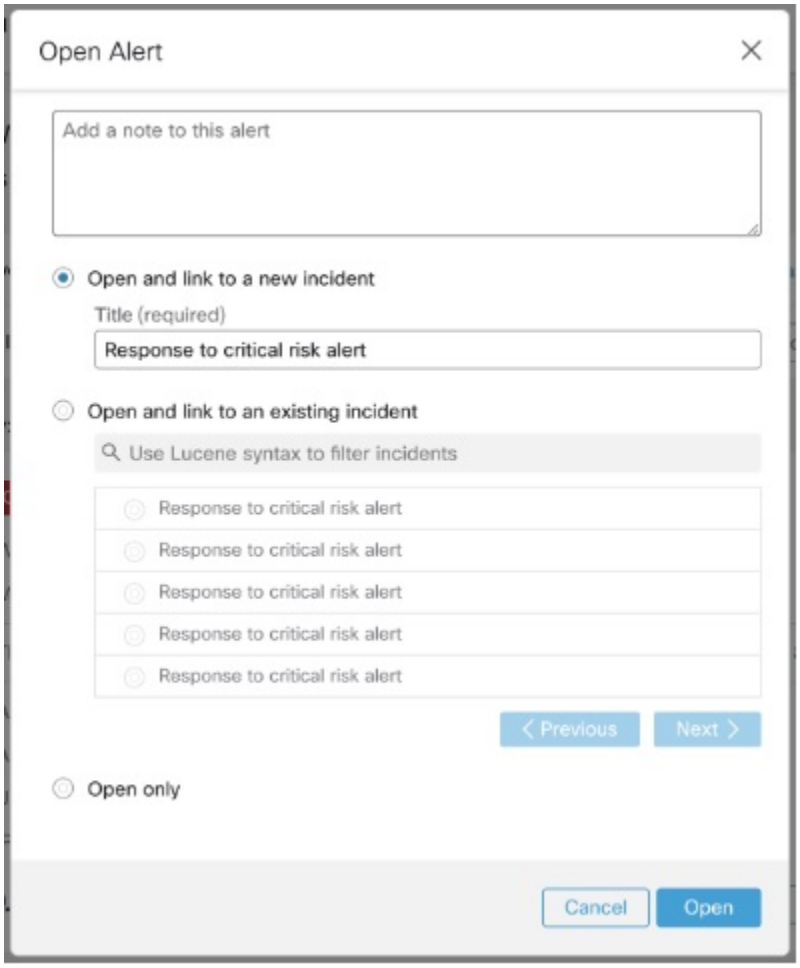


グローバル脅威アラートは、拡張された検出や効率的なアラートトリアージなどのコアコンピテンシーに引き続き重点を置いていますが、現在は SecureX エコシステムとより緊密に統合され、ワンクリックで SecureX のインシデント対応ワークフローへ検出をプロモートします。

アラートが開かれると、以下のオプションが用意されています。

- アラートを開いて新しいインシデントにリンク
- アラートを開いて既存のインシデントにリンク
- 開くのみ

図 *5:* インシデントにリンクするオプション付きのアラートを開く

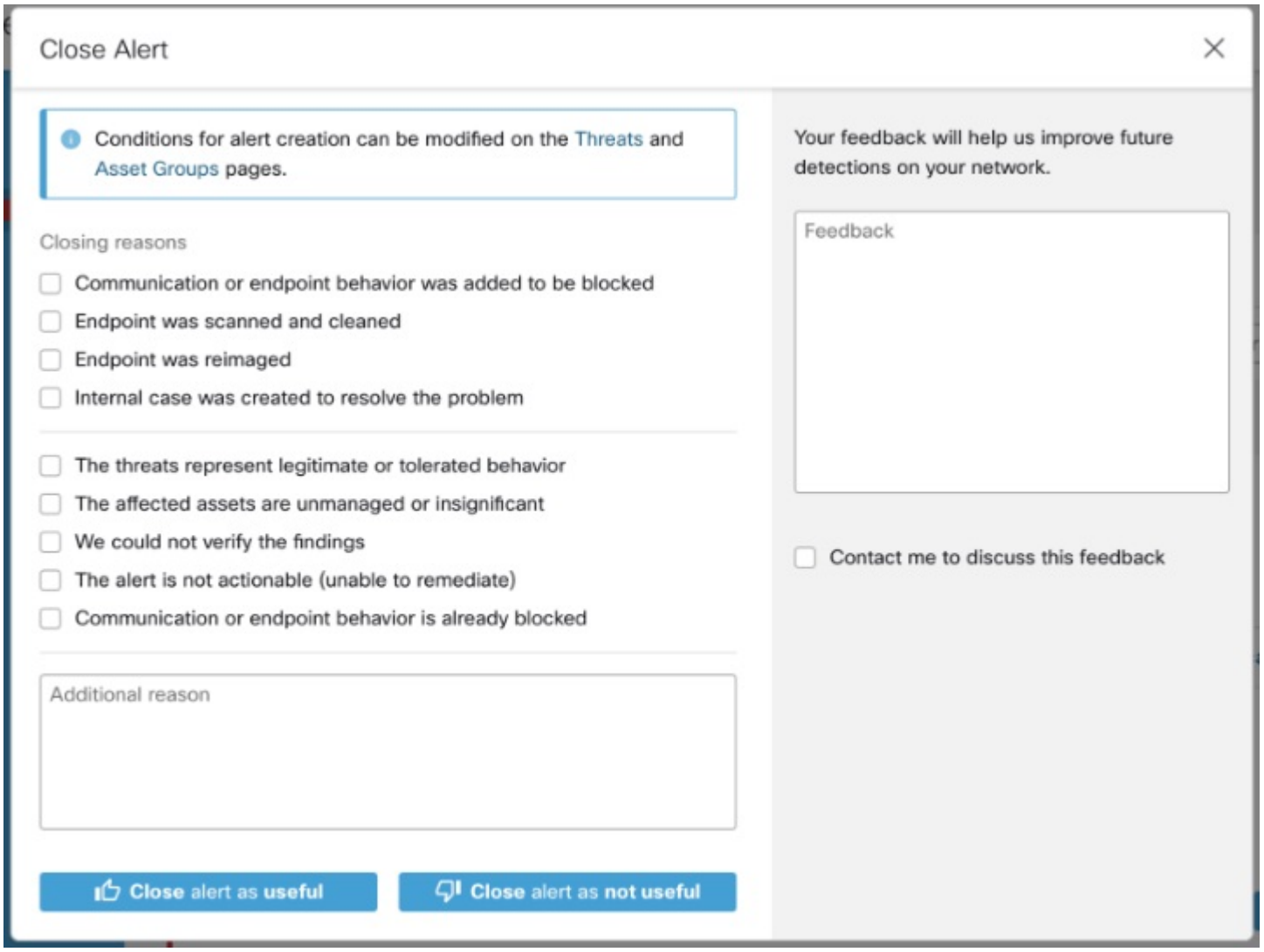


SecureX incident manager では、インシデントには、[概要（Summary）] や、元のアラートからのすべてのセキュリティ [イベント（Events）] と [監視対象（Observables）] などの詳細が含まれています。その後、調査、エンリッチメント、オーケストレーションといった SecureX の機能を使用して、より詳細に調査して対応することができます。

アラートをインシデントとしてプロモートすることが望ましくない場合でも、グローバル脅威アラートコンソールでのみ [開くのみ（Open only）] を実行でき、作業を追跡できます。

どちらの場合も、完了後はアラートを [閉じる（Close）] ことができます。アラートを閉じるときは、定義されている新しい一連の [閉じる理由（Closing reasons）] から選択するか、自身で理由を指定します。

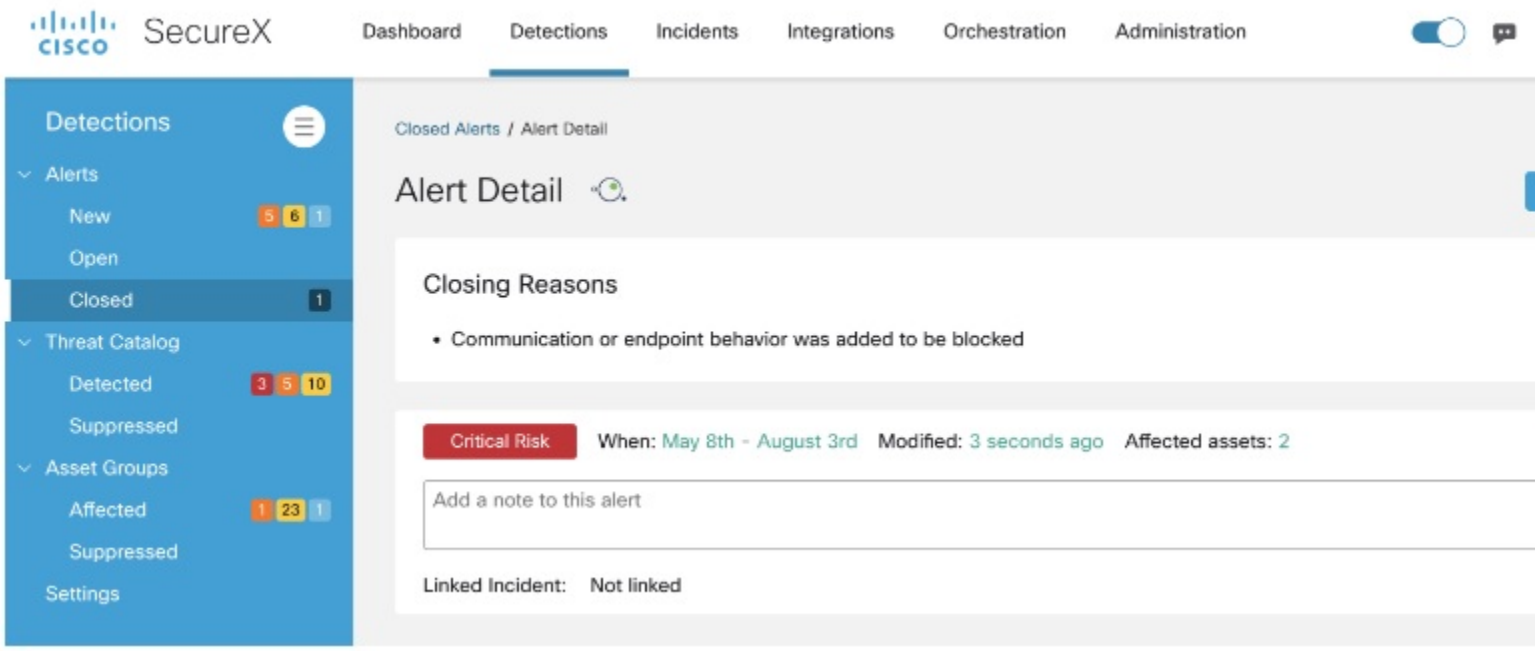
図 *6* : 閉じる理由を使用してアラートを閉じる



アラートを閉じるときは、[有用（useful）] または [有用でない（not useful）] として閉じることができます。アラートに関する追加のフィードバックをシスコのチームに提供することもできます。貴重なフィードバックは、今後の検出の改善に活用されます。

閉じる理由は、後で参照できるようにアラートの一部として記録されます。

図 7: アラートの詳細ページに表示される閉じる理由



閉じたアラートを開くことができます。アラートを再び開くと、閉じる理由はすべて削除されます。また、以前にリンクされたSecureXインシデントへの参照も削除されます。ただし、以前と同じSecureXインシデントであっても、アラートを再度リンクすることを選択できます。

追加の脅威検出

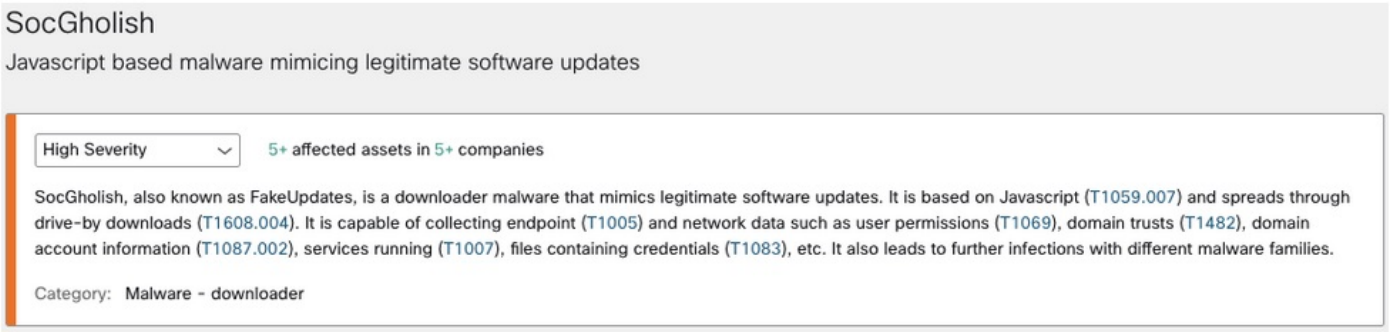
新しい脅威検出、SocGholishをポートフォリオに追加しました。また、既存の脅威検出のインジケーターを更新しました。

SocGholish

FakeUpdates とも呼ばれる SocGholish は、正規のソフトウェアアップデートを模倣するダウンローダーマルウェアです。これは Javascript（T1059.007）に基づいており、ドライブバイダウンロード（T1608.004）を介して展開します。エンドポイント（T1005）と、ユーザー許可（T1069）、ドメイン信頼（T1482）、ドメインアカウント情報（T1087.002）、実行中のサービス（T1007）、資格情報を含むファイル（T1083）などのネットワークデータを収集できます。また、異なるマルウェアファミリによるさらなる感染につながります。

お使いの環境で SocGholish が検出されたかどうかを確認するには、[SocGholish脅威の詳細（SocGholish Threat Detail）]https://cta.eu.amp.cisco.com/ui/threats/74536f03-a984-4a28-8dfa-a415f2d56cc5 をクリックして、グローバル脅威アラートで詳細を表示します。

図 *8 :*


SocGholish
Javascript based malware mimicing legitimate software updates
High Severity
5+ affected assets in 5+ companies
SocGholish, also known as FakeUpdates, is a downloader malware that mimics legitimate software updates. It is based on Javascript (T1059.007) and spreads through drive-by downloads (T1608.004). It is capable of collecting endpoint (T1005) and network data such as user permissions (T1069), domain trusts (T1482), domain account information (T1087.002), services running (T1007), files containing credentials (T1083), etc. It also leads to further infections with different malware families.
Category: Malware - downloader

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。