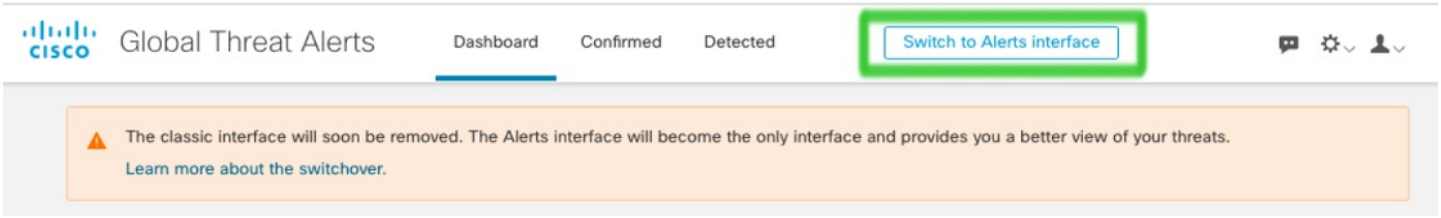
2021 年 8 月

2021 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。

廃止された従来のインターフェイス

6 月に、従来のインターフェイスからアラートインターフェイスに切り替えることをお勧めしました。

図 *1 :*



古い従来のインターフェイスは廃止され、新しいアラートインターフェイスが唯一のインターフェイスになり、ネットワーク上の脅威の拡張表示を提供します。

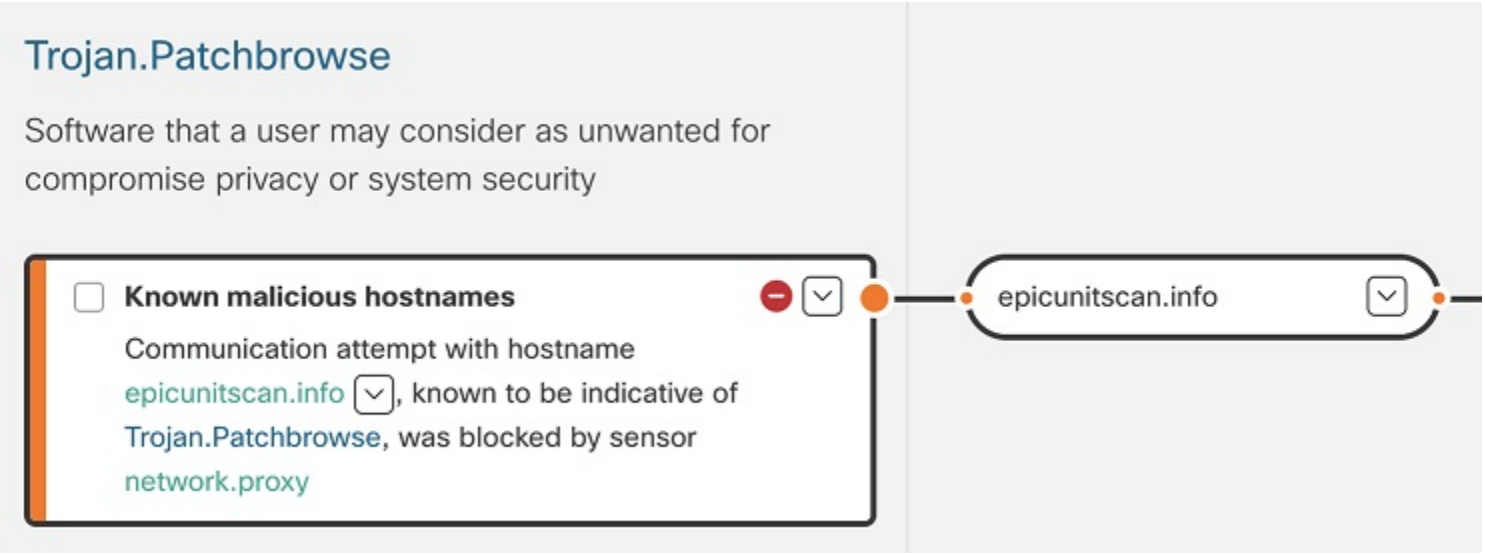
スキャンとブロックされた通信の処理の改善

誤検知の数を減らすために、グローバル脅威アラートは、水平スキャン通信によってトリガーされる脅威検出を抑制できるようになりました。また、感染の初期段階でプロキシでブロックされた通信の脅威検出を抑制することもできます。

ケースの視覚化を改善するため、感染がエンドポイントで持続し、アウトバウンド通信の一部がプロキシ（または他のアウトバウンド制御プロセス）によってブロックされている場合、グローバル脅威アラートは脅威検出の一部として提示される特定のセキュリティイベントを説明します。

この例では、（トロイの木馬に感染していることがわかっている）ホストと通信しようとすると、プロキシセンサーによってブロックされます。セキュリティイベントは、このソフトウェアがユーザーのプライバシーまたはシステムのセキュリティを危険にさらす可能性があるため、望ましくないと見なされると通知します。

図 *2:* 例：通信がプロキシによってブロックされたことを通知するセキュリティイベント



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。