Cisco Security Cloud製品からのHAR口グの収集

内容

はじめに

このドキュメントでは、ブラウザからHTTP Archive(HAR)口グを収集する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題：

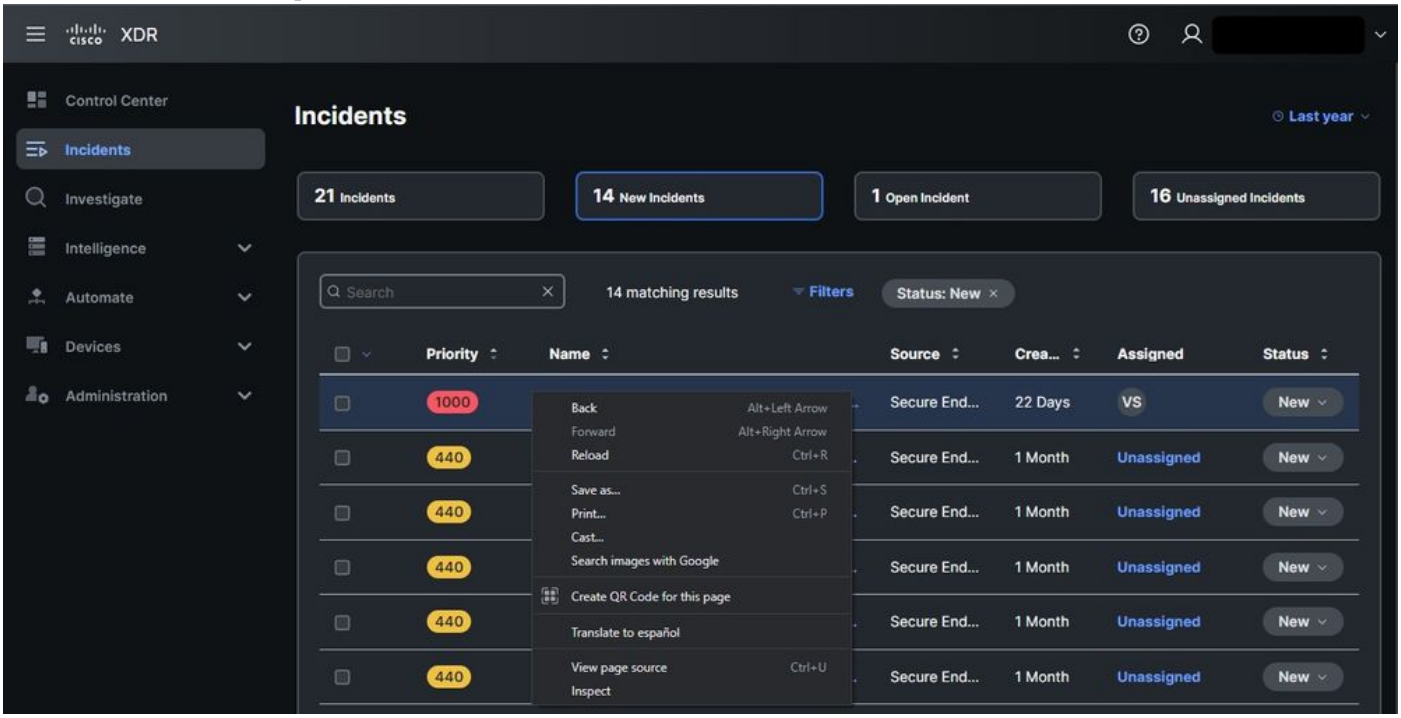
TACはHAR口グを使用して、XDRコンソールなどのシスコセキュリティ製品に関連する問題をトラブルシューティングします。

TACはHAR口グの情報を使用して、バックエンドサーバに対して行われたAPIクエリを確認し、問題を効率的に切り分けることができます。

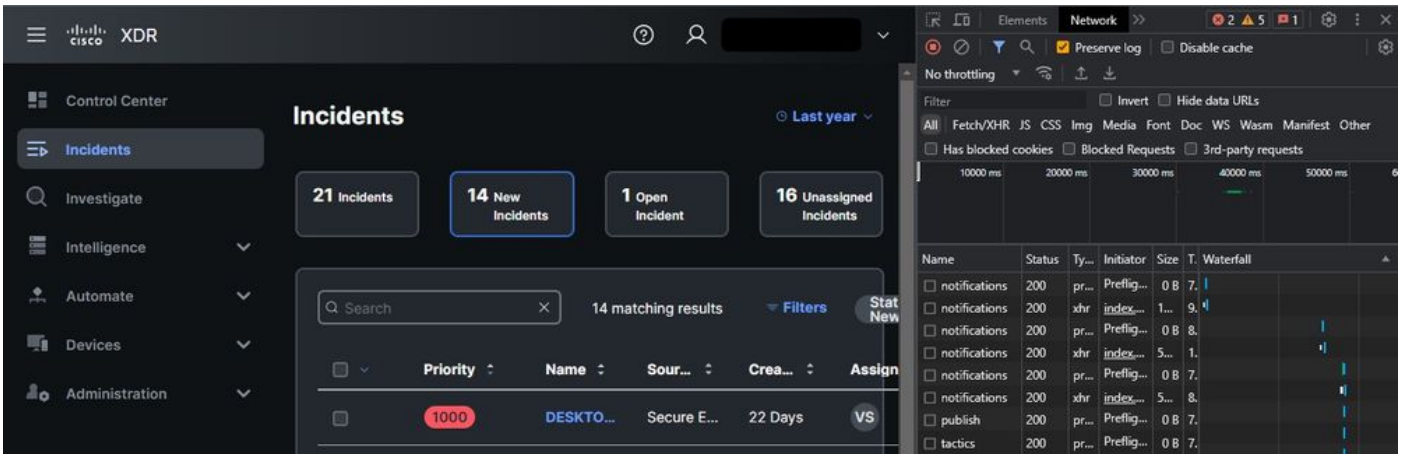
ソリューション：

ステップ 1：Cisco Security Cloud製品コンソールに移動します。この例では、XDRコンソールを

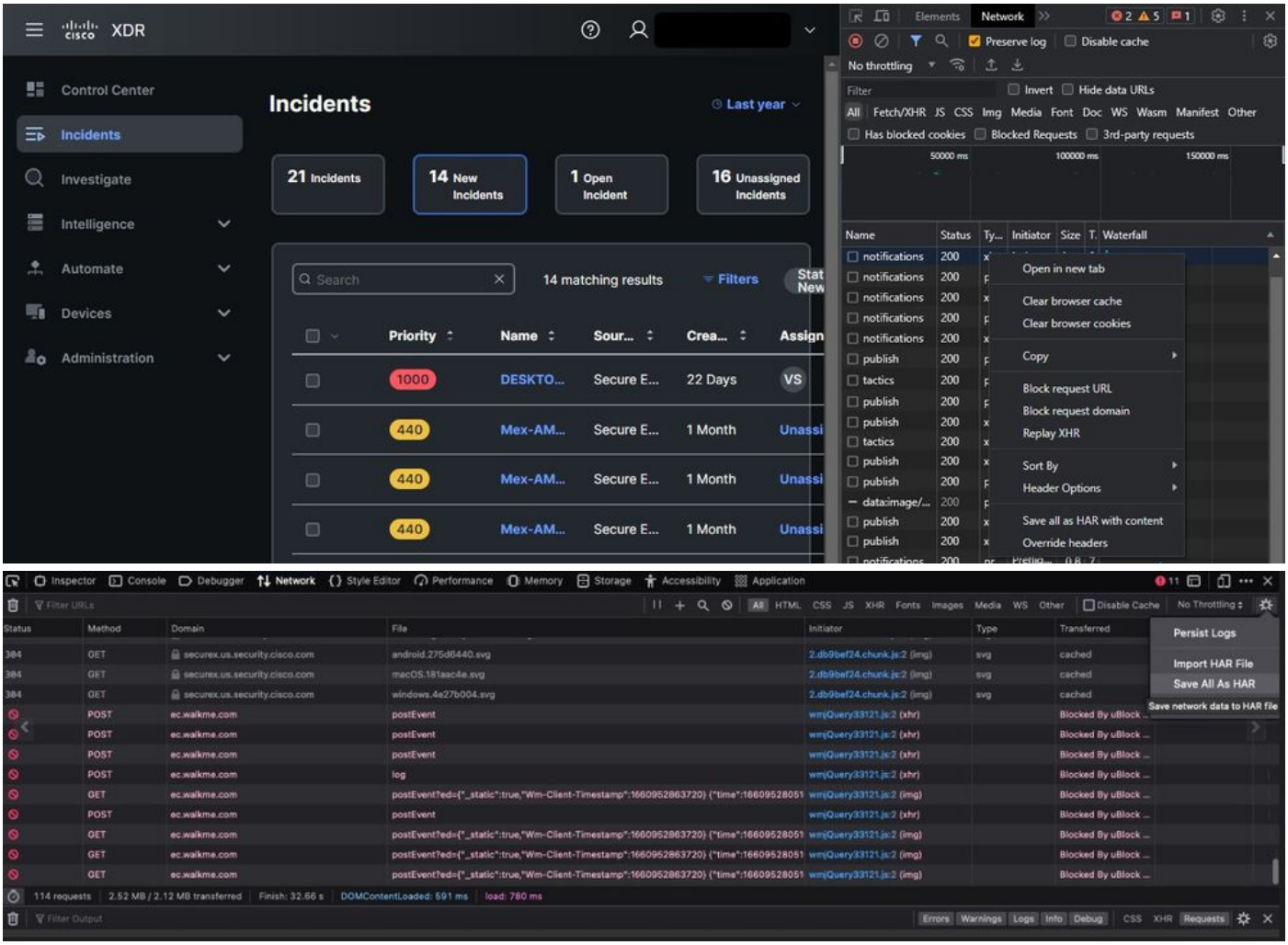
使用しました。
ステップ 2：問題が表示されているセクションに移動し、右クリックします。
ステップ 3：選択 **Inspect.**



ステップ 4：に移動します。 **Network** tab.



ステップ 5：問題を再現するか、ページをリロードして、すべてのクエリをログにキャプチャできるようにします。
手順 6：右クリックして、 **Save All as HAR with content** コンピュータ上のログをアーカイブする場合、またはエンジンアイコン（ブラウザによって異なります）を選択して、Save All as HAR with contentオプションを表示します。



手順 7：HARファイルを作成したら、そのファイルを Support Case Manager お客様のTACケースに組み込みます。

関連情報

- XDRの公式ドキュメント
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。