

Cisco Security Cloud製品からのHARログの収集

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題：](#)

[ソリューション：](#)

[関連情報](#)

はじめに

このドキュメントでは、ブラウザからHTTP Archive(HAR)ロ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ログを使用して、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ログの情報をを使用して、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**.

The screenshot shows the Cisco XDR interface. On the left is a navigation menu with 'Incidents' selected. The main area displays 'Incidents' with summary cards for 21 total, 14 new, 1 open, and 16 unassigned incidents. Below is a table of incidents. A context menu is open over the first incident (Priority 1000, Name 'Back').

Priority	Name	Source	Creation Time	Assigned	Status
1000	Back	Secure End...	22 Days	VS	New
440	Forward	Secure End...	1 Month	Unassigned	New
440	Reload	Secure End...	1 Month	Unassigned	New
440	Save as...	Secure End...	1 Month	Unassigned	New
440	Print...	Secure End...	1 Month	Unassigned	New
440	Cast...	Secure End...	1 Month	Unassigned	New
440	Search images with Google	Secure End...	1 Month	Unassigned	New
440	Create QR Code for this page	Secure End...	1 Month	Unassigned	New
440	Translate to español	Secure End...	1 Month	Unassigned	New
440	View page source	Secure End...	1 Month	Unassigned	New
440	Inspect	Secure End...	1 Month	Unassigned	New

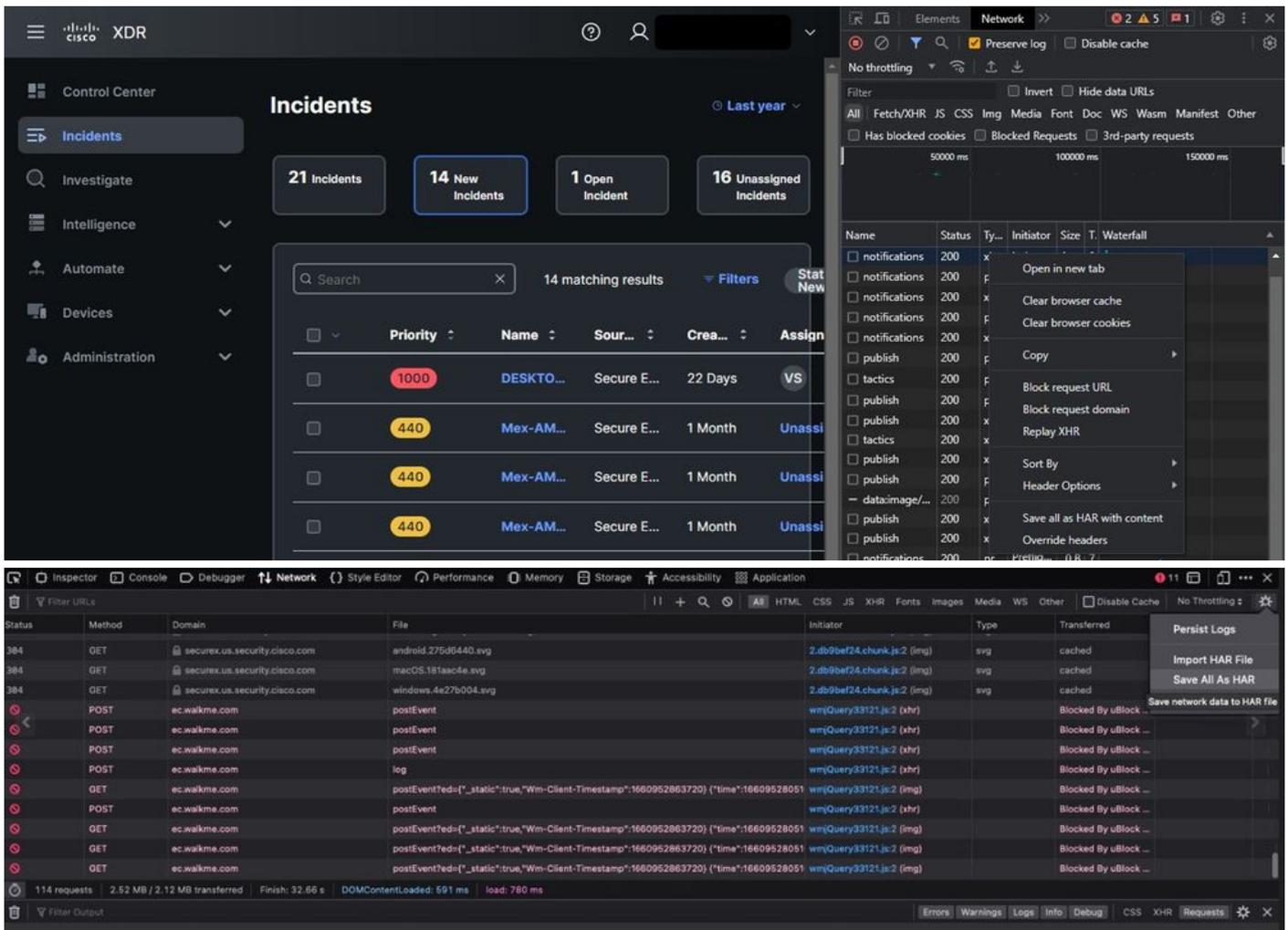
ステップ 4：に移動します。 **Network tab**.

The screenshot shows the same Cisco XDR interface, but with the 'Network' tab open in the developer tools. The 'Network' tab displays a list of network requests with columns for Name, Status, Type, Initiator, Size, and Time. The 'Waterfall' view is visible on the right.

Name	Status	Type	Initiator	Size	Time
notifications	200	pr...	Preflig...	0 B	7.1
notifications	200	xhr	index...	1...	9.1
notifications	200	pr...	Preflig...	0 B	8.1
notifications	200	xhr	index...	5...	1.1
notifications	200	pr...	Preflig...	0 B	7.1
notifications	200	xhr	index...	5...	8.1
publish	200	pr...	Preflig...	0 B	7.1
tactics	200	pr...	Preflig...	0 B	7.1

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。