Collect HAR Logs from Cisco Security Cloud Product

Contents

Introduction

This document describes how to collect HTTP Archive (HAR) logs from a browser.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

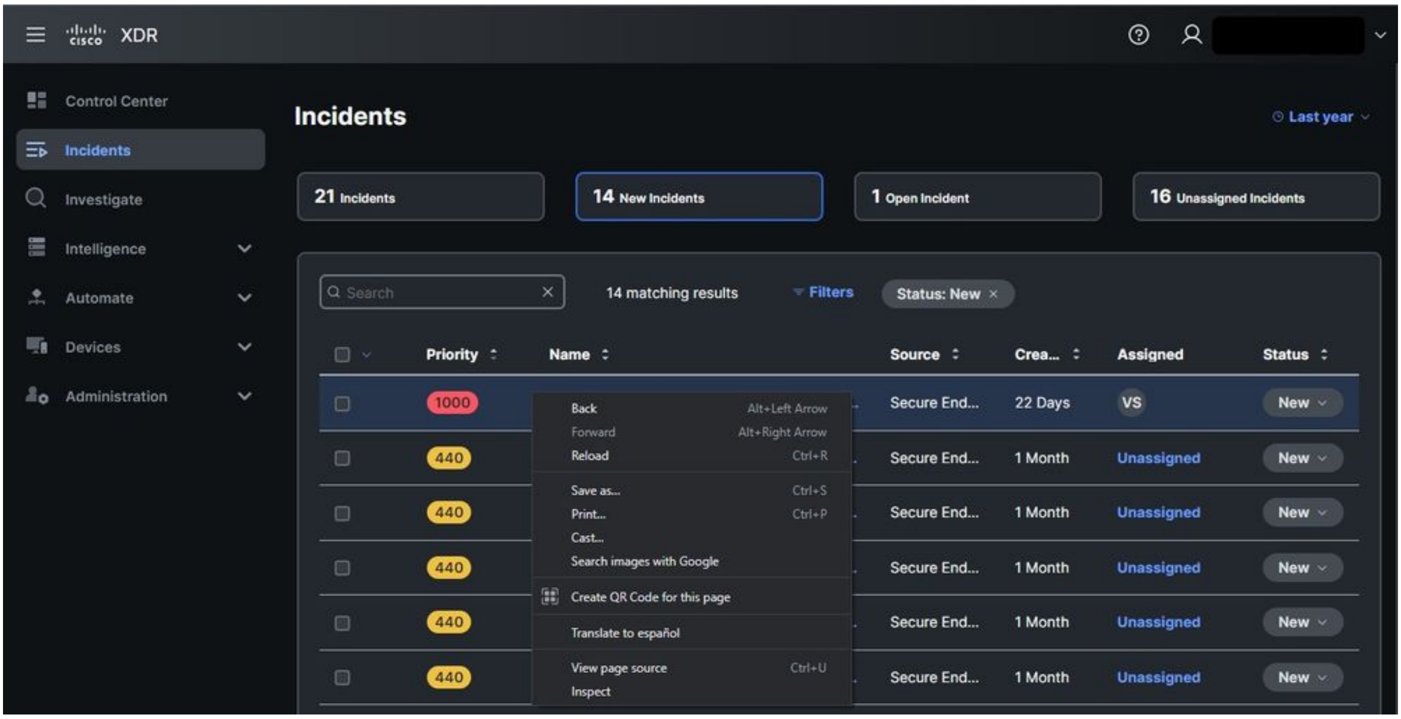
Problem:

TAC uses HAR logs to troubleshoot issues related to Cisco Security Products, such as the XDR console.

With the information in the HAR logs, TAC can review the API queries made to the backend server and isolate an issue efficiently.

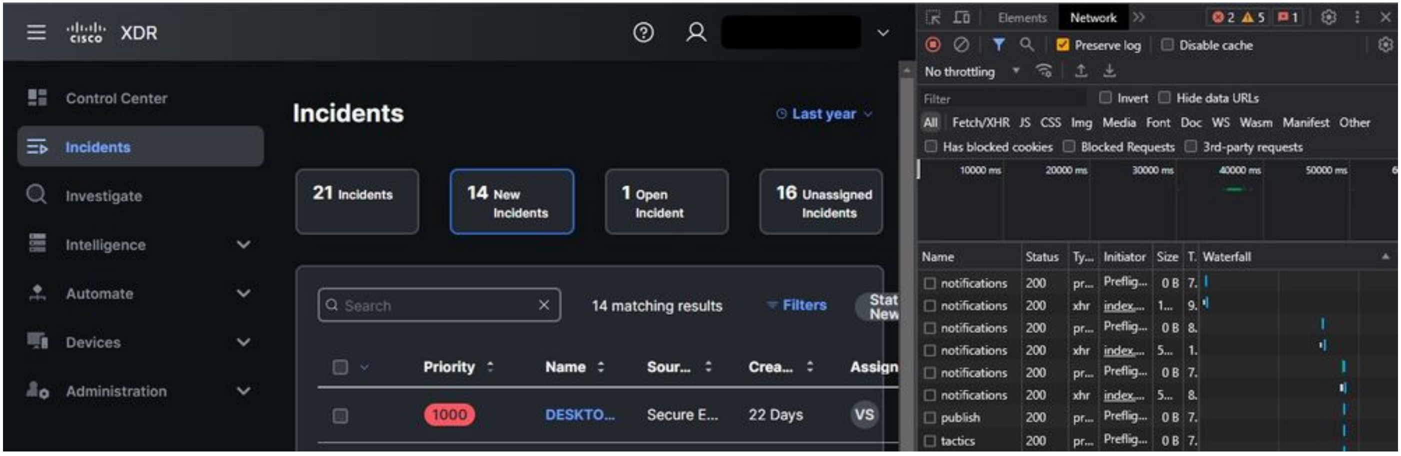
Solution:

Step 1. Navigate to the Cisco Security Cloud Product console, in this example, I used the XDR console.
Step 2. Navigate to the section where the issues are presented and right-click.
Step 3. Select **Inspect.**



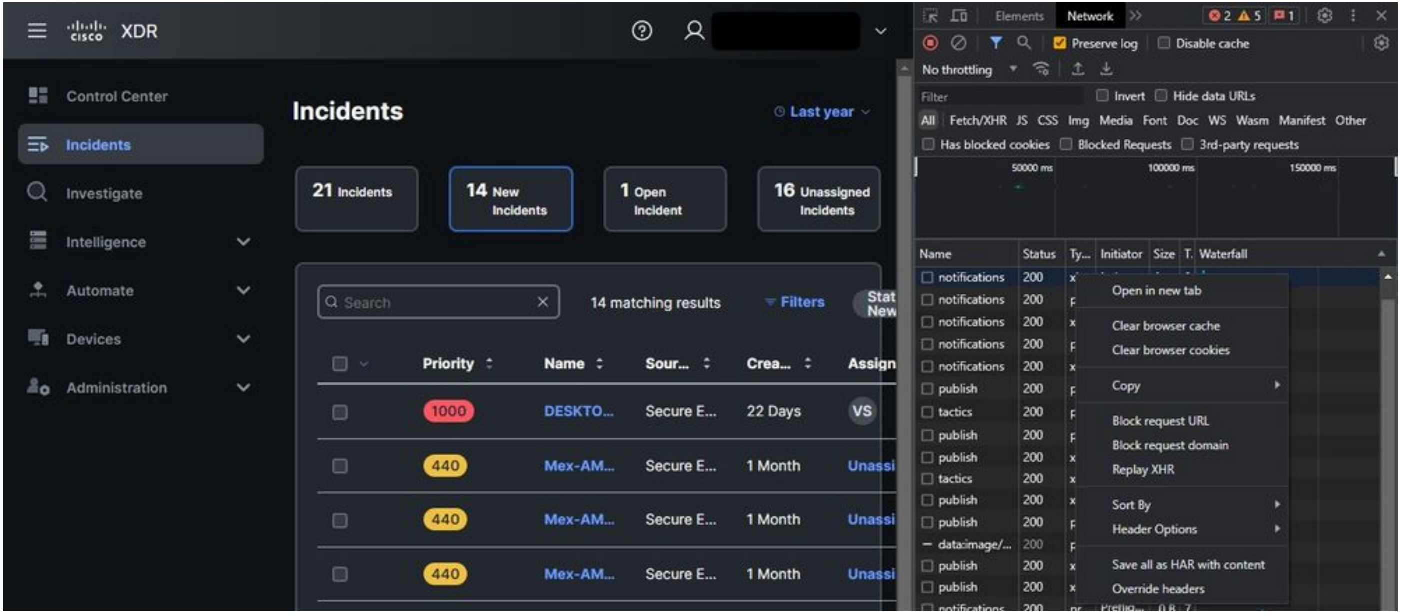
Priority	Name	Source	Crea...	Assigned	Status
1000		Secure End...	22 Days	VS	New
440		Secure End...	1 Month	Unassigned	New
440		Secure End...	1 Month	Unassigned	New
440		Secure End...	1 Month	Unassigned	New
440		Secure End...	1 Month	Unassigned	New
440		Secure End...	1 Month	Unassigned	New

Step 4. Navigate to the **Network** tab.



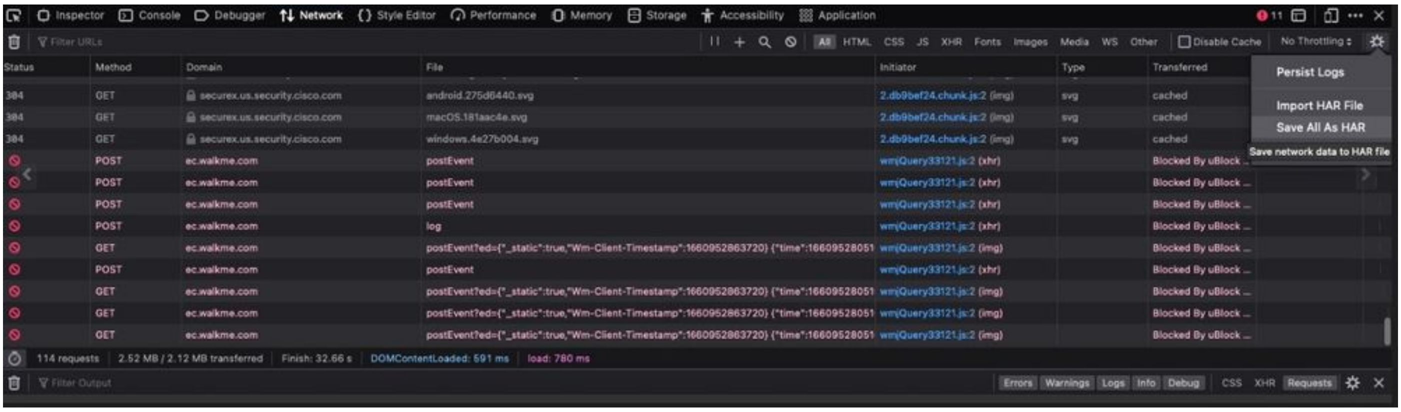
Name	Status	Ty...	Initiator	Size	T.
notifications	200	pr...	Preflig...	0 B	7.
notifications	200	xhr	index....	1....	9.
notifications	200	pr...	Preflig...	0 B	8.
notifications	200	xhr	index....	5....	1.
notifications	200	pr...	Preflig...	0 B	7.
notifications	200	xhr	index....	5....	8.
publish	200	pr...	Preflig...	0 B	7.
tactics	200	pr...	Preflig...	0 B	7.

Step 5. Reproduce the issue or reload the page so that all the queries can be captured in the logs.
Step 6. Right-click and select **Save All as HAR with content** to archive the logs on your computer or select the Engine icon (depending on the browser) in order to visualize the **Save All as HAR with content** option.



Priority	Name	Sour...	Crea...	Assign
1000	DESKTO...	Secure E...	22 Days	VS
440	Mex-AM...	Secure E...	1 Month	Unassi
440	Mex-AM...	Secure E...	1 Month	Unassi
440	Mex-AM...	Secure E...	1 Month	Unassi

Name	Status
notifications	200
notifications	200
notifications	200
notifications	200
notifications	200
publish	200
tactics	200
publish	200
publish	200
tactics	200
publish	200
publish	200
data:image/...	200
publish	200
publish	200



Status	Method	Domain	File	Initiator	Type	Transferred
304	GET	securex.us.security.cisco.com	android.275d6440.svg	2.db9bef24.chunk.js:2 (img)	svg	cached
304	GET	securex.us.security.cisco.com	macOS.181aac4e.svg	2.db9bef24.chunk.js:2 (img)	svg	cached
304	GET	securex.us.security.cisco.com	windows.4e27b004.svg	2.db9bef24.chunk.js:2 (img)	svg	cached
⊘	POST	ec.walkme.com	postEvent	wmjQuery33121.js:2 (xhr)		Blocked By uBlock ...
⊘	POST	ec.walkme.com	postEvent	wmjQuery33121.js:2 (xhr)		Blocked By uBlock ...
⊘	POST	ec.walkme.com	postEvent	wmjQuery33121.js:2 (xhr)		Blocked By uBlock ...
⊘	POST	ec.walkme.com	log	wmjQuery33121.js:2 (xhr)		Blocked By uBlock ...
⊘	GET	ec.walkme.com	postEvent?ed={"_static":true,"Wm-Client-Timestamp":1660952863720} {"time":16609528051	wmjQuery33121.js:2 (img)		Blocked By uBlock ...
⊘	POST	ec.walkme.com	postEvent	wmjQuery33121.js:2 (xhr)		Blocked By uBlock ...
⊘	GET	ec.walkme.com	postEvent?ed={"_static":true,"Wm-Client-Timestamp":1660952863720} {"time":16609528051	wmjQuery33121.js:2 (img)		Blocked By uBlock ...
⊘	GET	ec.walkme.com	postEvent?ed={"_static":true,"Wm-Client-Timestamp":1660952863720} {"time":16609528051	wmjQuery33121.js:2 (img)		Blocked By uBlock ...
⊘	GET	ec.walkme.com	postEvent?ed={"_static":true,"Wm-Client-Timestamp":1660952863720} {"time":16609528051	wmjQuery33121.js:2 (img)		Blocked By uBlock ...

114 requests | 2.52 MB / 2.12 MB transferred | Finish: 32.66 s | DOMContentLoaded: 591 ms | load: 780 ms

Step 7. Once you have the HAR file created, upload the file to the Support Case Manager into your TAC case.

Related Information

- Official XDR Documentation
- **Technical Support & Documentation - Cisco Systems**