Cisco Security Cloud製品からのHARログの収集

内容 <u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンボーネント</u> 問題: <u>ソリューション:</u> 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.

Ξ	uliulii XDR								<u>م</u> @	· · · · · · · · · · · · · · · · · · ·
55	Control Center		Incidents							⊙ Last year ∽
Ià	Incidents									
Q	Investigate		21 Incidents		14 New Incidents		1 Open Incident		16 Una	essigned Incidents
C800 C800 C800	Intelligence	~								
•	Automate	~	Q Search		× 14 matching res	ults 🗢 Filters	Status: New ×			
ų,	Devices	~	<u> </u>	Priority 🗘	Name ‡		Source 🗘	Crea ‡	Assigned	Status 🗧
å,	Administration	*		1000	Back Forward	Alt+Left Arrow	Secure End	22 Days	VS	New ~
				440	Reload		Secure End	1 Month	Unassigned	New ~
				440	Save as Print Cast		Secure End	1 Month	Unassigned	New ~
				440	Search images with Google		Secure End	1 Month	Unassigned	New ~
				440	Translate to español	ige -	Secure End	1 Month	Unassigned	I New ~
				440	View page source Inspect		Secure End	1 Month	Unassigned	New y

ステップ4:に移動します。 Network tab.

=				୭			K LO Ele	ments N	etwork >>	🙁 2 🔺 5	💷 🕸 i					
=	cisco ADR				Ū	\sim			0017	Q 🗹	Preserve log 📗 🗏	Disable cache		۲		
14-142									No throttling		t ±					
	Control Center		Incidente			O Lastware -			Filter Invert Hide data URLs							
6			incluents				O Last ye	201	All Fetch/XHR	JS CSS Ir	ng Media Font	Doc WS Wasm	Manifest Other	r		
≡₽	Incidents								Has blocked	cookies 🔲	Blocked Request	s 🔲 3rd-party req	uests			
Q	Investigate		21 Incidents	14 New Incide	ents 1 op	en ident	16 Unass Incide	ligned	10000 ms	20000 r	ns 30000 m	s 40000 ms	50000 ms			
	Intelligence	~							Name	Status T	y Initiator Siz	e T. Waterfall				
	Automate	~							notifications	200 p	r Preflig 0	в 7. <mark>I</mark>				
ete.	Automate		Q Search		× 14 match	ing results	= Filters	Stat	notifications	200 x	hr <u>index</u> 1	. 9. 1				
105	Devices	~							notifications	200 p	r Preflig 0	B 8.				
	Devices			Priority *	Nama * S	our 1	Crea *	Accian	notifications	200 x	hr <u>index</u> 5		1			
1.	Administration	~		Phoney	Hame - C		Ciea ·	Assidi		200 p	r Pretlig ()	B 7.				
- •	Administration			1000	DESKTO	Secure F	22 Davs	VS		200 x	nr <u>index</u> S • Preflin 0	. 8. p.7				
						Cours L				200 1	r Preflig 0	B 7.				

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。

≡	cisco XDR					@ A				ments Q	Network	e log 🔲 Disable cache	s 😐 1 🛞 🗄		
								1	No throttling						
22	Control Center								Filter Invert I Hide data URLs						
			Incidents				O Last ye	iar ~	All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other						
≣₽	Incidents								Has blocked	d Requests 🔲 3rd-party	requests				
										50000 ms		100000 ms	150000 ms		
Q	Investigate		21 Incidents	14 New Incident	14 New Incidents Incident		16 Unassigned Incidents								
	Intelligence	~							Name	Status	Ty Ini	tiator Size T. Waterfall			
									notifications	200	×				
	Automate	Ť	Q Search		× 14 r	matching results	= Filters	Stat	notifications	200		Open in new tab		- 1	
10G	Devices	~							notifications	200		Clear browser cache		_	
-10	Devices			Priority *	Name :	Sour :	Crea :	Assian	notifications	200	F	Clear browser cookies		- 1	
20	Administration	~								200		Сору		_	
				1000	DESKTO	Secure E	22 Davs	vs		200	1				
								~	publish	200	-	Block request URL		- 1	
		A40 May AM Casura E			1 Month United		🗆 publish	200		Block request domain		_			
				440	Mex-MM	Secure E	rmonth	Unassi	□ tactics	200		Replay XHR		-	
				-				V1000 000	🗆 publish	200		Sort By		_	
				440	Mex-AM	Secure E	1 Month	Unassi	publish	200		Header Options		- 1	
									- dataimage/	200				_	
				440	Mex-AM	Secure E	1 Month	Unassi		200		Save all as HAR with conte	nt	_	
								_		200	x pr P0	Overnde headers		- 1	
G 0	Inspector D Consol	e 🖸 Debugger 1	Network {} Style Ec	litor O Performance	I Memory	🗄 Storage 🔺 Ac	cessibility 🚟 App	lication					0 11 日 日・	•• ×	
n v	Filter URLs					11	+ 9 9 4		JS XHR Fonts	Images	Media W	S Other Disable Cach	e No Throttling a	*	
Status	Method	Domain		File				Initia	tor		Type	Transferred	Download I women	-	
				State of the second second				0.000	Contraction of the			10000	Persist Logs		
384 384		A secure us securi	ty.cisco.com	marOS 181aacda svo				2.001	Herza, chunk js 2 (ing		svg	cached	Import HAR Fi	ile	
384	GET	A securex.us.securi	ty.cisco.com	windows.4e27b004.svg				2.dbi	bef24.chunk is 2 (img)		5VG	cached	Save All As HA	AR	
	POST	ec.walkme.com		postEvent					m(Query33121.js/2 (xhr)			Blocked By uBlock	ave network data to l	HAR file	
	POST	ec.walkme.com		postEvent					uery33121.js:2 (xhr)			Blocked By uBlock			
	POST	ec.walkme.com		postEvent					uery33121.(s.2 (shr)			Blocked By uBlock			
	POST	ec.walkme.com		log					rm(Query33121.js:2 (xhr)			Blocked By uBlock			
	GET	ec.walkme.com		postEvent1ed={"_static":true,"Wm-Client-Timestamp":1660952863720} {"time":16609528051					m(Query33121.js:2 (img)			Blocked By uBlock			
	POST	ec.walkme.com		postEvent				winjG	uery33121.js:2 (xhr)			Blocked By uBlock			
	OET	ec.walkme.com		postEvent?ed={*_static	rent?ed=("_static":true,"Wm-Client-Timestamp":1660952863720) ("time":16609528051 un							Blocked By uBlock			
	GET	ec.waikme.com		nt-Timestamp* 16609528	63720) ("time":16609	528051 Wm(0	uery33121.js:2 (mg)			Blocked By uBlock		-			
0	GET	ec.waikme.com	Eleich 22.66 a DOMOLO	postEvent7ed=("_static	true, wm-Clier	nt-i mestamp": 16609528	63720) ("time":16609	528051 Wim(C	/wery3/3121-jac2 (mg)			Blocked By uBlock _			
10 11 10 11	riquests 2.52 MB/2.	rz. mo transferred	einish: 32.66 s DOMCon	entroaded: 591 ms los	la: 780 ms				Line	202221 1922	222625227 1993		vuo inconstati e	1e v	
0 4									195	(1409 - 1408	Lo Lo	an inno inggun css	and [methoday] >	~ ^	

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

関連情報

- ・ <u>XDRの公式ドキュメント</u>
- ・ 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。