ةياەنلا ةطقنو Cisco XDR معدلا دعاسم دادتما ةنمآلا

تايوتحملا

قماع قرظن مادختسال ا تال اح مادختسال ا تال اح قرحلم توبيثت :1 قوطخل ا قرحلمل ا طوشيت :2 قوطخل ا قرحلمل ا تانوم مادختس ا :3 قوطخل ا معد قل اح حتف م معمد قل اح حتف بو معمد موج - موج ال ال اس را :4 قوطخل ا معرامل ا :5 قوطخل ا

ةماع ةرظن

معدلا ةبرجت نيسحتو ميظنتل <u>Cisco Support Assistant Chrome</u> قرلم ميمصت مت ايليصفت ارامت ليلدلا اذه رفوي .(قعسوملا ةباجتسالاو فشكلا) Cisco XDR يمدختسمل ليجست ،معدلا تالاح حتف لثم هتازيمم مادختساو ،هتقداصم ،قحلملا تيبثتل ةوطخب ةوطخ نكمي ،تاميلعتلا هذه عابتا لالخ نم .ضرعتسملاب ةصاخلا HAR تالجس عمجو ،تاشاشلا ةدعاسملا زكرم عم ةءافكو ةعرسب اهتكراشمو ةيرورضلا تامولعملا طاقتلا نيمدختسمل

ىلع فرعت .ەاندأ تاوطخلاو ەذە مادختسالا تالاحل ةيليصفتلا تاريسفتلا فشكتسا ا<u>انە</u> ديزملا.

مادختسالا تالاح

2 و 1 تاوطخلا ةءارق ىجريف ،لبق نم "Cisco ل معدلا دعاسم قحلم" تمدختسأ دق نكت مل اذإ ءدبلا ةيفيك ةفرعمل 3 ةوطخلا ىلإ ةرشابم لقتنا ،ةربخلا يوذ نيمدختسملل .هاندأ ةموعدملا تاقحلملا تازيم مادختساب.

Chrome قحلم تيبثت :1 ةوطخلا

- 1. رجتم نم Chrome Assistant ق<u>حلم</u> ليزنتب مق :تيبثتو ليزنت Cisco Support Chrome Assistant وجتم نم Chrome من المريفي قحلم رفوت نمضي امم ،هتيبثتل "Chrome ىلإ ةفاضإ" قوف رقناو <u>بيولا علع</u> يروفلا مادختسالل ضرعتسملا
- ةمئاق نم ققحتلا لالخ نم ەنيكمت نم دكأت ،قحلملا تيبثت درجمب :قحلملا نيكمت .2 .طشن Cisco معد دعاسم نأ ديكأتو Chrome يف تاقحلملا

قحلملا طيشنت :2 ةوطخلا

- الثم ،موعدم Cisco کا لقتنا Sisco XDR: حتفا Cisco XDR: حتفا Cisco XDR: الثم ،موعدم Cisco کرا لقتنا. طيشنتارا قيلمع عدبال.
- قَتْبِنِم ارصنع ىرتس ،موعدملاً جَتَنِملاً مَحْفَص مَرايز دنع :مَقَتْبِنِملاً تَاراطإلاً طَيْشنت طيشنتب مقو TAC قيبطتل نييضارتفالاً نيدعاسملاً مَوقل نانعلاً قلطاً" :لوقي معد دعاسم قرحلم



- 1. المع ريس ليغشتل قثبنم مالعإ ىلع رقنا :طيشنتلل رقنا Cisco.com. المع ريس ليغشتل من المع ريس المع ريس المع
- دامتعالا تانايب لاخدا لالخ نم Cisco.com ىلع ةقداصملا ةيلمع لمكأ :ةقداصملا 2. كتيوه نم ققحتلاو.
- كمسا رەظيسو ،"ليغشت" ك ەزييمت مت قحلملا نأ ىرتس ،قيدصتلا درجمب :ديكأتلا .3 تاودأ طيرش يف قحلملا ةنوقيأ ىلع رقنت امدنع Chrome.



Ct

े 🗘

ÓМ

Cisco Support Assistant Extension

Welcome back Nik Kale



Enabled on this URL

Ð			P
Open	Record	Collect	Submit
Cisco	Screen	HAR	Feedback
Support		Logs	
Case			

: تاوطخلا لالخ كدشرتس يتلاو ،ةديدج معد ةلاح حتفل رايخلا رتخأ ،قحلملا ةهجاو يف ةيرورضلا.

- طاقتلال يرايتخإ لكشب ةشاشلا ليجست ةزيم مادختسإ كنكمي :لجسلا ةلكشم .3 معدلا قيرفل ةياغلل اديفم نوكي نأ نكمي ام وهو ،ايهفشو ايرصب اهحرشو كتلكشم (4 ةوطخلا يف ةلصفم تاداشرا).
- ،ةلصلا تاذ تامولعملاو ةلكشملا فصو لثم ،ةبولطملا ليصافتلا ألما :ةلاحلا لاسرا .4 قحلملا ةهجاو لالخ نم كب ةصاخلا معدلا ةلاح لاسرا مث

كتشاش ليجست .ب

ةشاش" رايخ ددحو Chrome تاودأ طيرش يف قحلملا ةنوقيأ ىلع رقنا :ليجستلا ءدب .1



ةشاشلا ليجست ةيلمع ءدبل "ليجستل.

بيوبت ةمالع ليجست ديرت تنك اذإ ام ديدحت كنم بلطيس :ليجستلا ةحاسم رتخأ .2 اهلمكأب بتكملا حطس ةشاش وأ ،اهلمكأب ضرعتسملا ةذفان وأ ،ةنيعم Chrome



💳 ليجستلا حوضو نيسحت ىلع لمعي امم ،كتلكشمل يتوص حرش ريفوتل كب

عم ،ةشاشلا ليجسّت عدبل ةشّاشلا يلع رَهُظت يتلا تاميلغتا عبّتاً :ليجسّتلا عدبً .4 ةلصلا تاذ تامولعملاو تاءارجإلا عيمج طاقتلا.

cisco XDR		xdr.us.security.cisco.com says		▼ ⑦ ♀ ♀ A Daniel Benitez XDR BETA - TAC Org ~
≡	Devices	shared content. Double-click to take a screenshot of the visible area on the browser page.		
Control Center >	Source health 27.369 D	Cancel	os	View all 13 Operation Systems
Incidents	Asset Inventory Sources Ty	pes Status		
-Q Investigate		Server (25)	20,83	33 Windows
Statelligence >	78%	Desktop (20,747)	Managed (0)	Unknown
+ 🔂 Automate >		Virtual (65)	Unmanaged (27,369)	UBURU
📑 Assets >		Mobile (0)	2	Network Gateway
्रि Client Management >				
20 Administration >	Text search Saved filt Q User, IP, hostname Devices Selected Indiate Value	v Thefare Lands	Filters 27,369 matching results	C. Export to (SV)
		Copulate Cablers Concentrations (Numes		
	Device name COS	OS version OS support Users seen	Sources	Managed ① Compromised ① Labe @
	☐ 192.168.1.100 ⓒ ⁹ 2' Ne Gatew	work	Secure Endpoint - Jocreek Org	No
	□ 192.168.10.5 ⓒ 😵 Ne Gatew	work _	Secure Endpoint - Jocreek Org	
	220-mail2.e2e.test 🛇 Unknow	vn —	Microsoft Defender for Endpoint	
	☐ Alex2 ⓒ 왕 Wir	dows 1703	Microsoft Defender for Endpoint	
cote XDR		dows 1703	Microsoft Defender for	No

<u>ةفاضإل </u>ةشاش يأ ىلع جودزملا رقنلا ليجستلا ءانثأ كنكمي :ةشاش تاطقل ةفاضإ .5

📰 🛄 ويديفلا ليجست عم معدلا ةلاح يف اەنيمضت متيس يتلاو ،ةشاش ةطقل

- مئاعلا طيرشلا يف "فاقيإ" رايخلا قوف رقنا ،ليجستلا فاقيإل :ليجستلا فاقيا .6 ليجستلا فاقيإ رز ددحو قحلملا ةنوقيا قوف رقنا وأ ةشاشلا لفسأ يف.
- ىلإ ويديفلا ليمحت رايخ كيدل نوكيس ،ليجستلا فاقيإ درجمب :ليمحتلا ليجست .7 ةلاح حتف وأ ماقرأ ةعست نم فلؤملا (SR) ةمدخلا بلط مقر لاخدا لالخ نم ةدوجوم ةلاح ةديدج.



HAR تالجس عمج - ميج

تالجس عيمجت" رايخلا ددحو Cisco معد دعاسم قحلم زمر قوف رقنا :لجسلا طاقتلاا ءدب .1



■■.لجسلا تانايب طاقتلا ءدبل "HAR

ةداعإو ةفلتخم تاحفص لالخ لقنتلا ىل كدشري قثبنم راطإ رهظي :لقنتلا تاداشرا ِ .2



.ةلصلا تاذ HAR تالجس طاقتلاب قحلملل حمسي امم ،ةلكشملا جاتنا

- لجس طاقتلاا ةيلمع ءدبل ةقثبنملا ةمئاقلا يف "قفاوم" ىلع رقنا :طاقتلالا ءدب .3 HAR.
- ،ةيرورضلا تانايبلا طقتلتو رادصإلا جاتنا ةداعإب موقت نأ درجمب :طاقتلالا فاقيإ .4 تباثلا لجسلا طاقتلا فاقيإل رزلا سفن رقنا.
- ةلاح ىلإ اهعيمجت مت يتلا تالجسلا ليمحت رايتخإ كلذ دعب كنكمي :تالجسلا ليمحت .5 رمألا مزل اذإ ةديدج ةلاح حتف وأ ماقرأ ةعست نم فلؤملا SR مقر لاخدا لالخ نم ةدوجوم معد.

-ili-ili- cisco	Cisco XDR						o (2)	Q A Daniel Benitez XDR BETA - TAC Org
			Devices					
55	Control Center							
Ō	Incidents		Source health	27,369 Devices	Status		os	View all 13 Operating Systems
₽Ω	Investigate			Serve	er (25)		20,833	Windows
Ø	Intelligence		78%	Upload to Case		× aged (0)	6,524	Unknown
÷Ð	Automate		10 /0	Do you want to upload	your recording to an existing	case or anaged (27,369)	9	Ubuntu
	Assets	>		Existing Case Op	en New Case		2	Network Gateway
Ę,	Client Management			Case Number: 6889453	575			
2o	Administration	ministration > Text search Save Submit Q User, IP, hostname Set						
			0 Devices Selected Upda	ate Value 🗸 Update Labels	✓ 🖉 Edit Labels Rule	15		Export to CSV
			Device name	CS OS version	OS support Users se	een Sources	Managed (Compromised 🛈 Labe 🛞
			192.168.1.100 ⊙	양 Network — Gateway —		Secure Endpoin Jocreek Org	nt - No	
			□ 192.168.10.5 ⊙	్లి Network Gateway		Secure Endpoin Jocreek Org	it - No	
			220-mail2.e2e.test 📀) Unknown —		Microsoft Defer Endpoint	nder for No	
			Alex2 📀	88 Windows 1703		Microsoft Defer Endpoint	nder for No	
-4)-4)- 6969	XDR			0 89 Mindawa 1700		Microsoft Defer	nder for	

TAC ىلإ تامولعملا لاسرإ :4 ةوطخلا

بلط مقر لخدأف ،ةدوجوم ةلاح ىلإ تامولعملا ليمحتب موقت تنك اذإ :ةدوجوملا ةلاحلا .1 ةلاحلاب تاليجستلا وأ تالجسلا قافرا نامضل ماقرأ ةعست نم فلؤملا (SR) ةمدخلا .ةحيحصلا

- ةنيعم تامولعم ءلم ىلإ قحلملا يدؤيسف ،ةديدج ةلاح حتفب موقت تنك اذإ :ةديدج ةلاح .2 لجسلا طاقتلا ةيلمع ءانثأ اهذيفنت متي يتلا ةطشنألا ىلإ ادانتسا قبسم لكشب .ةيقبتملا ليصافتلا لامكإب كبلاطيس امم ،ةشاشلا ليجست وأ تباثلا
- دكؤت ينورتكلإلاا ديربلاا ربع تاراطخإ ىقلتت فوس ،تامولعملا لاسرا دعب :ديكأتلاا .3 تانايبلا عيمج هيدل TAC قيرف نأ نمضي امم ،ةديدجلا ةلاحلا اعاشنا وأ تافلملا ليمحت كب ةصاخلا ةلكشملا ىلع لمعلا عدبل ةمزاللا.

ةعباتملا :5 ةوطخلا

- لوصولا لواحي دقو ةمدقملا تامولعملا ضارعتساب TAC قيرف موقيس :TAC ىلع درلا ءاطخألا فاشكتسأ ةيلمع يف ءدبلل كلذو ،رمألا مزل اذإ ةيفاضإ ليصافت ىلإ . قلكشملا لحو امحالصإو
- دق امم ،ةرفوتملا تانايبلا ىلإ ادانتسا ةلكشملا لح ىلع TAC لمعيس :تالكشملا لح ،ةدراولا ينورتكلإلا ديربلا لئاسر وأ ةيفاضإلا Webex تاعامتجإ ىلإ ةجاحلا نم للقي لحلا ةيلمع عيرست يلاتلابو.

دادتمال ةلماكلا فئاظولا نم ةدافتسالا نيمدختسملل نكمي ،تاوطخلا هذه عابتا لالخ نم Cisco XDR. عم ةءافكو ةيلاعف رثكأ معد ةيلمع نمضي امم ،Cisco Support Assistant Chrome

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما