

تاديدهتلا ةكبش و CTR جمد

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ديدهتلا ةكبش لةيطمنلا ةدحو لا نيوكت - CTR مكحتلا ةدحو](#)

[ةباجتساللا لىلا لوصولاب تاديدهتلا ةكبش لءامسلا - تاديدهتلا ةكبش يف مكحتلا ةدحو تاديدهتلا](#)

[ةحصللا نم ققحتلا](#)

ةمدقملا

ةباجتسم عم (CTR) Cisco تاديدهتلا ةباجتساللا جمدل ةمزاللا تاوطخلال دنتسملا اذه فص ي CTR تاقىقحت ءارج لءا نم (TG) تاديدهتلا ةكبش

Cisco نم TAC يس دنهم ،زيشناس نيءلاري لبق نم ررحو ،زىنيترام ريي فاخ عوسى هب مهاس

ةيساسألا تابلطتملا

تابلطتملا

ةيلاللا عيضاوملاب ةفرعم كيدل نوكت نأ Cisco ي صوت

- Cisco نم ةياملال تاديدهت ةباجتسلا
- تاديدهت ةكبش

ةمدختسملا تانوكملا

ةيلاللا ءماربال تارادصلا لىلا دنتسملا اذه يف ةءراول تامولعملال دنتست

- (لوؤسملا قوقح عم مدختسملا باسح) CTR مكحت ةدحو
- (لوؤسملا قوقح عم مدختسملا باسح) تاديدهتلا ةكبش مكحت ةدحو

ةصاخ ةيلمعم ةئيب يف ةءوجوملا ءزهءال نم دنتسملا اذه يف ةءراول تامولعملال ءاشنإ مت تناك اذا .(يضارتفا) ءوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ءزهءال عيمء آءب رما يال لمءمءلا ريثاثلل كمءف نم ءكأءف ،ليءشءلا ءي قكءكءبش

ةيساسأ تامولعم

لليءلءل يءاقولءو روطءم يساسأ ماظن نع ءرابع يه Cisco نم ةياملال تاديدهت ةكبش نكمي شيء ،ءراضلا ءماربال تاديدهت لوء ءيرابءءسالا تامولعملال ءينقءو ءراضلا ءماربال

مدخستسملا ةئيب ىلع ريثأتلا نود بيولا تاهجو وأ ةببملا تافلما ريحفت

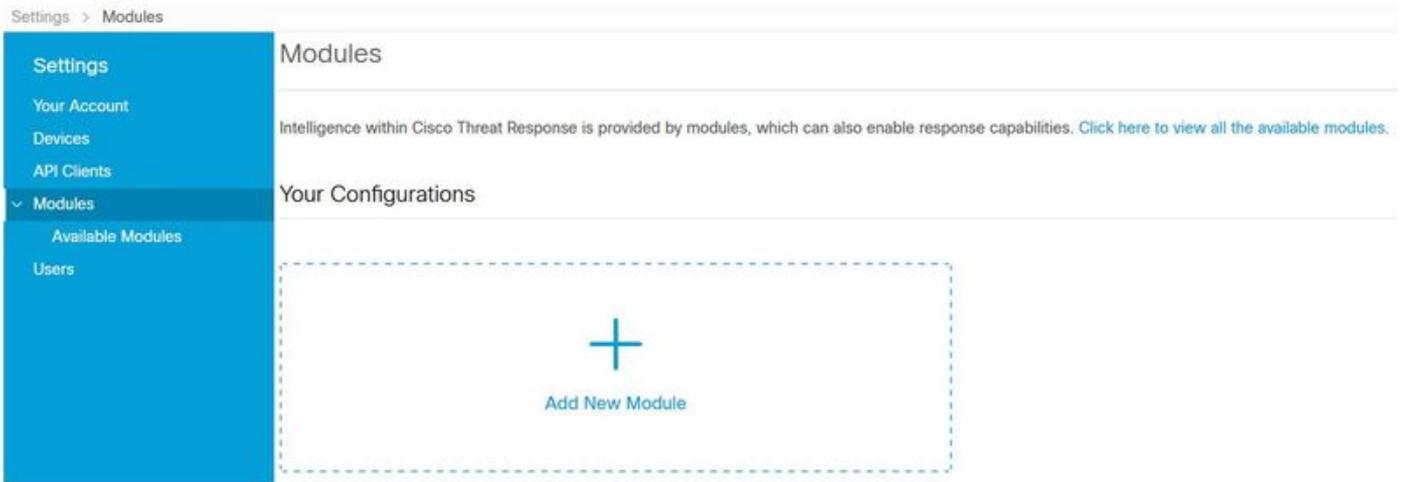
ىلع ةردقلا رفوتو ةيغرم ةدحو "تاديدهتلا ةكبش" دعت Cisco Threat Response عم جمدا ي ةئجت لوح ةيفاضا ةيتارابختسا تامولعم عمجل "تاديدهتلا ةكبش" ةبواب لوح نارودلا تاديدهتلا ةكبش فراعم نزخم في URLs و تاقاطنلا و IPs و تافلما

نيوكتلا

ديدهتلا ةكبش ل ةيطمنلا ةدحو نيوكت - CTR مكحتلا ةدحو

لوؤسملا دامتعا تانايب مادختساب Cisco [تاديدهت ةباجتسا](#) ىلا لوخدلا لفس 1. ةوطخلا

ةيطمن ةدحو ةفاضلا > ةيطمن تادحو دحو، ةيطمن تادحو بيوتلا ةمالع ىلا لقتنا 2. ةوطخلا ةروصلا في حضوم وه امك، ةديج



ةدحو ءزج في ةديج ةيطمن ةدحو ةفاضلا دحو، ةحاتملا ةيطمنلا تادحو ءحفص في 3. ةوطخلا ةروصلا في حضوم وه امك، ديدهتلا ةكبش ل ةيطمنلا



ةروصلا في حضوم وه امك جذومنلا لمكأ. ةديج ةيطمن ةدحو ةفاضلا جذومن حتفي 4. ةوطخلا

- كل ىنعم اذ امسا لخدأ وأ يضا رتفالا مسالا كرتأ - ةيطمنلا ةدحو امسا
- باسح هيلا دننسي يذلا عقوملل بسانملا URL رتخأ، ةلدسنملا ةمئاقلا نم - URL ي. لالحا تقولا في رخآلا راخلا لهاجت. (ابوروا وأ ةيلا مشلا الكيرمأ) تاديدهتلا ةكبش

Add New Threat Grid Module

Module Name*

Threat Grid

URL*

https://panacea.threatgrid.com

Save Cancel

تاديدهت الة ك بشل لة ط م ن الة د ح و الة ني و ك ت ل ا م ك ا ل ظ ف ح د د ح . 5 ة و ط خ ل ا

ة ح ف ص ي ف ك ب ة ص ا خ ل ا ت ا ن ي و ك ت ل ا ل ف س ا ن ا ل ا " ت ا د ي د ه ت ل ا ة ك ب ش " ض ر ع م ت ي . 6 ة و ط خ ل ا
ة ر و ص ل ل ا ي ف ح ض و م و ه ا م ك ة ط م ن ل ا ت ا د ح و الة

(تاديدهت الة ي ف ق ي ق ح ت ل ا ن ي س ح ت ل ة ل ا ح ال ر ت ا ف د ي ف و ي ر و ح م ال م ئ ا و ق م ن T G ر ف و ت ي).

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

Settings > Modules

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Tg Threat Grid
Threat Grid

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

Edit Learn More

ى ل ا ل و ص و ل ا ب ت ا د ي د ه ت ل ا ة ك ب ش ل ح ا م س ل ا - ت ا د ي د ه ت ل ا ة ك ب ش ي ف م ك ح ت ل ا ة د ح و
ت ا د ي د ه ت ل ل ة ب ا ج ت س ا ل ا

ل و و س م ال د ا م ت ع ا ت ا ن ا ي ب م ا د خ ت س ا ب [ديدهت الة ك ب ش](#) ى ل ا ل و خ د ل ا ل ج س . 1 ة و ط خ ل ا

ة ر و ص ل ل ا ي ف ح ض و م و ه ا م ك ، ي ب ا س ح م س ق ى ل ا ل ق ت ن ا . 2 ة و ط خ ل ا



وه امك تاديدهت لل ةباحتسالا لي صوت را يخ ددحو تالاصتالا مسق ىلإ لقتنا 3. ةوطخلا ةروصلال ي ف حضورم.

Connections

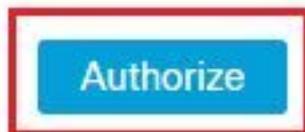


تاديدهت ةباحتسالا لىلإ لوصولاب ديدهتالا ةكبشلال حامسلال لي وختلا را يخ ددح 4. ربم ت بس ةروصلال ي ف حضورم وه امك، Cisco.

Authorize Threat Grid to Access Threat Response

Authorization will allow Threat Grid to access Threat Response threat intelligence and enrichment capabilities.

If you've never accessed Threat Response, simply click the Authorize button and log in to Threat Response using your Threat Grid or AMP for Endpoints credentials.



ي ف حضورم وه امك، قي بطتالا لىلإ لوصولال حن مل تاديدهت ةكبشلال لي وخت را يخ ددح 5. ةوطخلا ةروصلال.

Grant Application Access

The application **Threat Grid** (panacea.threatgrid.com) would like access to your Cisco Threat Response account.

Specifically, **Threat Grid** is requesting the following:

- **casebook**: access and modify your casebooks
- **enrich**: query your configured modules for threat intelligence (*enrich:read*)
- **global-intel**: query AMP Global Intelligence
- **inspect**: extract observables and data from text (*inspect:read*)
- **integration**: manage your integration modules configuration (*integration:read*)
- **private-intel**: access Private Intelligence
- **profile**
- **registry** (*registry/user/ribbon*)
- **response**: list and execute response actions using configured modules
- **telemetry** (*telemetry:write*)
- **users** (*users:read*)

Authorize Threat Grid

Deny

اهي دل تاديدهت الة ك ب ش نأ ن م ق قحتت لوصول لاهب حرصم الة لاسرلنا ودي 6 ة وطلخا
ديدهت الة ل ع درل ديهت ب قلعتت عارثا تاردقو ة تارابختس ا تامولعم الة لوصول ة ناكم ا
ة روصول يف حصوم وه امك

Access Authorized

Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

Increase and improve the threat intelligence that Threat Response provides by **configuring modules** such as AMP for Endpoints, Umbrella, and Virus Total.

ة حصلنا نم ق قحتلنا

حېحص لكش ب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

عيمج رهظت ام دنع ،CTR م كحت ةدحو ىلع قيقحت عارجا ك نكمي ،TG و CTR لم اكات نم ققحتلل ةروصلال يف حضورم وه امك ،ديدهتلا ةكبش راىخ ةيؤر ك نكمي ،قيقحتلل لىصاف

Investigation 1 of 1 enrichments complete

ad...2b

Investigate Clear Reset What can I search for?

Relations Graph - Filters: Show All, Expanded - Showing 8 nodes

Malicious SHA-256 Hash
ad59bca10a3056571d65ffb6...

ad...
Malicious SHA-256
Copy to Clipboard
Create Judgement
Add to New Case
Threat Grid
Browse ad...b...
Search ad...b6...

ةكبش ةباوب ىلإ ههيجوت ةداعإو ديهتلا ةكبش يف شحب وأ ضارعتسا راىخ ديدحت ك نكمي نيوانع / تالاجملا / ip / ةئزجتلا / تافلما لوح ةيضا ةي تارابختسا تامولعم عمجل ديهتلا ةروصلال يف حضورم وه امك ،ديدهتلا ةكبش تامولعم نزخم يف URLs

Threat Grid Submit Sample Dashboard Samples Reports Indicators Administration

Search / Samples

Query: ad... X

Match By: SHA-256

Date Range: Start date End date

Scope: All My Organization My Samples

Access: All Private Public

Search

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Access	Status
F...	Q,a...		#test	Windows 7 64-bit					
ad...	Q,a...		amptoolbox	Windows 7 64-bit	Random Cursor Movem...				
F...	Q,a...			Windows 7 64-bit					
ad...	Q,a...		amptoolbox	Windows 7 64-bit	Random Cursor Movem...				

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنل دن تسمل