

مهفل ةنمآلا ةكبشلا تاليلحت ليلد ةيجراخلا تالاصتالا

تايوتحملا

[ةمدقملا](#)

[ةيجراخلا تالاصتالا](#)

[ةيفاضا تامولعم](#)

[Cisco نم \(SSE\) ةنمآلا تامدخل الاداب](#)

[ني فيض ملاءة قطنملا](#)

[\(BETA\) قرشابملا جماربلا تاليننت](#)

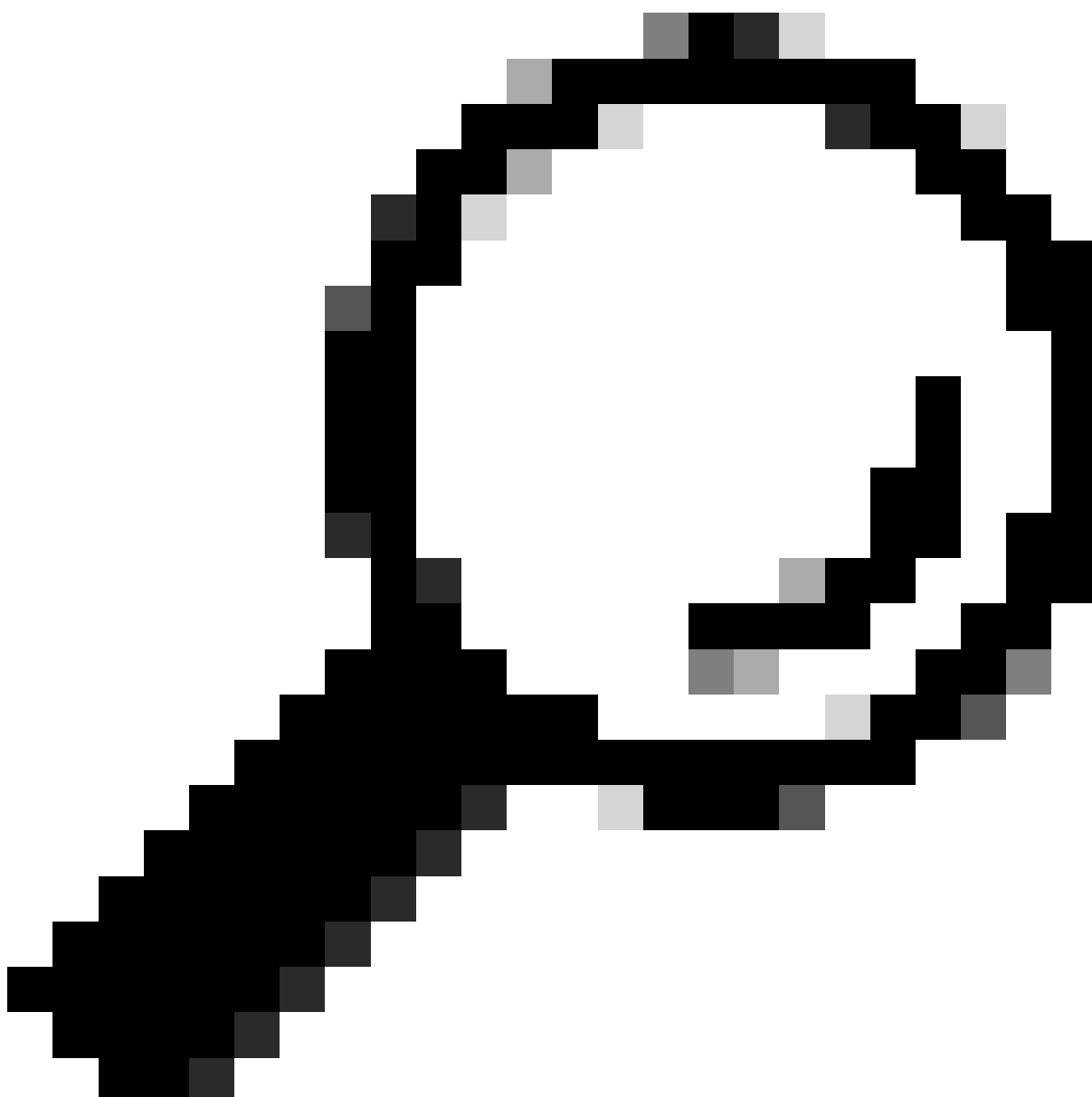
[Miter ATT&CK® لمع راطا](#)

[بيدهتلا ةيذغت](#)

[مع دلاب لاصتالا](#)

ةمدقملا

تاليلحت نم ةنيعم تازيمل ةبولطملا ةيجراخلا تالاصتالا ةعجارمل ليلدل اذه مدختسا طاقن و تالاجم ةيجراخلا تالاصتالا هذه نوكت نا نكمي . ةعرسب لمعلل ةنمآلا ةكبشلا و بيولا عقاوم ةداع ، تنرتنإلا ىلع دراوملا فيرعتل مدختست عامسا يه تالاجملا . ةياهن اذهل زيكرتل نا امب . ةكبش ربع لصتت ةيلعف دقع و ازهجا يه ةياهنلا طاقنو ؛ تامدخل لودجل درس ي . URL نيوانع ةئييه ىلع تامدخل هذه ضرع متيس ، بيولا تامدخ وه ليلدل اذيجبالا بيترتلل بسح يجرخلا لاصتالا اب ةصاخلا URL نيوانع .



بېترتال بسح ځراځال لاصتالاب ؤصاځال URL نږوانع لودځال درسي :ځملت
ځدځبال

ؤځراځال لاصتالاب

ضرغال	ځراځال لاصتالاب URL ناونع
مدختسي ؤطساوب تالځلت ؤنمآلؤكېشال تانايب لدابتل دعبنع سايقلا تامدخ مادختساب	https://analytics.int.obsrvbl.com

	تالېلحت ةنمآلةباحسلا
https://api.apj.sse.itd.cisco.com	Cisco نم بولطم تانايبل لقنل بيولا تامدخ ىلإ Amazon في ةقطنمل (AWS) طيحمل او ايسآ نابايلاو ئداهلا نصللاو دنع مدختسي هيجوت ةداعإ ىلإ تاهيبننتلا Cisco نم XDR اضياو ةمدخ سيياقملا ءالمعلا.
https://api.eu.sse.itd.cisco.com	Cisco نم بولطم تانايبل لقنل بيولا تامدخ ىلإ Amazon في ةقطنمل (AWS) ابوروا (EU). دنع مدختسي هيجوت ةداعإ ىلإ تاهيبننتلا Cisco نم XDR اضياو ةمدخ سيياقملا ءالمعلا.
https://api-sse.cisco.com	Cisco نم بولطم تانايبل لقنل بيولا تامدخ ىلإ Amazon في ةقطنمل (AWS) ةدحتملا تايالولا مدختسي (US). هيجوت ةداعإ دنع ىلإ تاهيبننتلا Cisco XDR ةمدخل اضياو سيياقم/ءالمعلا حاجنلا.
https://apix.cisco.com	نم مدختسي تالېلحت لبق ةنمآلةكبشلا تاليزنت "ةزيملا

	جماربلا "ةرشابملا".
https://dex.sse.itd.cisco.com	لاسريال بولطم حاجن سيياقم ءالمعلا اهعي مچتو
https://est.sco.cisco.com	لاسريال بولطم حاجن سيياقم ءالمعلا اهعي مچتو
https://eventing-ingest.sse.itd.cisco.com	لاسريال بولطم حاجن سيياقم ءالمعلا اهعي مچتو
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	لبق نم بولطم بيو بيو زجوم صاخلا يذلاو، ديهتلاب همادختسا متي تاهي بنتلل ناطحال مل او ةصاخلا تاليحتب ،ةنمالة كبشلا نيكمت دنع تاليحتلا.
https://id.cisco.com	نم مدختسي تاليحت لبق ةنمالة كبشلا تالي زنت "ةزيمل جماربلا "ةرشابملا".
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	لبق نم بولطم بيو بيو زجوم صاخلا يذلاو، ديهتلاب همادختسا متي تاهي بنتلل ناطحال مل او ةصاخلا تاليحتب ،ةنمالة كبشلا نيكمت دنع تاليحتلا.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	لبق نم بولطم بيو بيو زجوم

	صاخال يذلاو، ديدهتلاب همادختسا متي تاهي بننتلل ناطحال مل او ة صاخال تالي لحتب ،ةنم آلا ةكبشلا نيكمت دنع تالي لحتلا.
https://lancopex.net/operations/control/Incp/LancopexDownload	لبق نم بولطم تالي لحت" "ةنم آلا ةكبشلا تامولعم زجوم يذلاو، ديدهتلاب همادختسا متي نام آلا ثادحل تالي لحتو ةنم آلا ةكبشلا اذه بلطتي زجوم صيخرت تالي لحت بيو تاديدهت ةنم آلا ةكبشلا.
https://mx*.sse.itd.cisco.com	لاسرا ل بولطم حاجن سيياقم ءالمعلا اهعيميحتو
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	لوصولاب حمسي تامولعم يلا MITER دنع تاهي بننتلل نيكمت تالي لحتلا.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	لوصولاب حمسي تامولعم يلا MITER دنع تاهي بننتلل نيكمت تالي لحتلا.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	لوصولاب حمسي تامولعم يلا MITER دنع تاهي بننتلل نيكمت تالي لحتلا.

https://s3.amazonaws.com/onconfig/global-blacklist	بې وزوم ديده تل يذالو، بول طم ل هم ادخ تس ا مت ي تاهي بن تل ل تا طحال م ل او ة صا خ ل ا تالي لحت ب ،ة م آ ل ا ك ب ش ل ا ن ي ك م ت د ن ع تالي لحت ل ا.
https://sensor.anz-prod.obsrvbl.com	Cisco ن م بول طم تاناي ب ل ل ق ن ل بي و ل ا تام د خ ي ل ا ف Amazon ة ق ط ن م ل (AWS) طي ح م ل او اي س آ ن اب اي ل او ئ دا ه ل ا ن ي ص ل او د ن ع م د خ ت س ي ه ي ج و ت ة دا ع ا ي ل ا تاهي بن تل ل Cisco ن م XDR اض ي او ة م د خ س ي ي اق م ل ء ا ل م ع ل ا.
https://sensor.eu-prod.obsrvbl.com	Cisco ن م بول طم تاناي ب ل ل ق ن ل بي و ل ا تام د خ ي ل ا ف Amazon ة ق ط ن م ل (AWS) (EU). ا ب و ر و ا د ن ع م د خ ت س ي ه ي ج و ت ة دا ع ا ي ل ا تاهي بن تل ل Cisco ن م XDR اض ي او ة م د خ س ي ي اق م ل ء ا ل م ع ل ا.
https://sensor.ext.obsrvbl.com	Cisco ن م بول طم تاناي ب ل ل ق ن ل بي و ل ا تام د خ ي ل ا ف Amazon ة ق ط ن م ل (AWS) ة د ح ت م ل ا تاي ال و ل ا م د خ ت س ي (US) ه ي ج و ت ة دا ع ا د ن ع

	ىلإ تاهي بننتلا Cisco نم XDR اضى أو ةمدخ سيي اقم ءالمعلا.
smartreceiver.cisco.com	مدختسي ىلإ لوصولل جمارب صيخرت Cisco Smart. عجرا ليلد" ىلإ صيخرتلا لوصحلل "يكلذل ليصافت ىلع صيخرت رفوتسي نود ليدب ناك اذا ،لاصتا الضفم كلذل تاظحالم ىلإ عجرا رادصلا ىلع لوصولل ليصافتلا.
https://software.cisco.com	نم مدختسي تاليلحت لبقي ةنمآلا ةكبشلا تاليزنت" ةزيم جماربال ةرشابملا.
https://www.cisco.com	لاجل بولطم متي يذلاو ،Cisco همادختسا تارابتخال يكلذل صيخرتلا ةباحسلا ليك وو رادل لاصتاو ةياملحلا.

ةيفاضا تامولعم

ةياهن ةطقنو لاجم تالاصتا مادختسا ببسو ةيفيكل مبيقتلا نم ديزم ىلع لوصولل
ةيلاتلا تاعوضوملا ىلإ عجرا ،ةنيعم

- [Cisco نم \(SSE\) ةنمآلا تامدخلا لدابت](#)
- [\(BETA\) ةرشابملا جماربال تاليزنت](#)

- [Miter ATT&CK® لمع رابطا](#)
- [ديدهتلا ةيذغت](#)

Cisco نم (SSE) ةنمآلا تامدخلا لدابت

ةطساوب ، Amazon (AWS) بيوتامدخلى إ تانايبلا لقنل SSE ةياهنلا طاقن مادختسا متي Cisco إلهيبتنلا هيوت ةداع دنع اهمادختسا متي امك ، ءالمعلا ةمدخ سيياقم Cisco XDR. ةفلتخملا عاونألا هذه لكشب هذه ةياهنلا طاقن فاشتكا متي . ةفيضملا ةزهجألاو ةقطنملا إلهيبتنلا تايلمع رشن دنع SSE. لصوم اهرفوي يتلا ةمدخلا فاشتكا ةيلا مادختساب يكيمايد "xdr-data-" ناونعب ةمدخ فاشتكا "ةنمآلا ةكبشلا تاليلحت" لواح Cisco XDR، إلهيبتنلا فاشكلا "ثادحألا" اهب ةصاخلا API ةياهن ةطقنو "xdr-data-platform".

ني فيضملاو ةقطنملا

يلي امك ةفيضملا تائيبل نوكت ، جاتنإلا تائيب في ةقطنملا بسح

ةدحتملا تايالول:

- <https://api-sse.cisco.com>
- <https://sensor.ext.observbl.com>

EU :

- <https://api.eu.sse.itd.cisco.com>
- <https://sensor.eu-prod.observbl.com>

ةكرتشملا ةدعاسملا زكرم

- <https://api.apj.sse.itd.cisco.com>
- <https://sensor.anz-prod.observbl.com>

(BETA) ةرشابملا جماربلا تاليزنت

"ةرشابملا جماربلا تاليزنت" ةزيم لبق نم ةيلاتلا تالاصتالا مادختسا متي

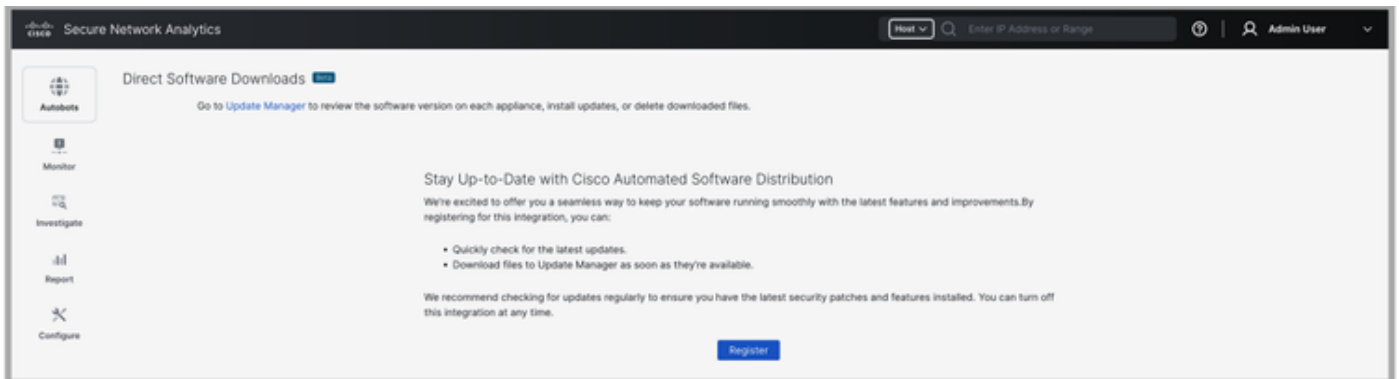
- <https://apix.cisco.com>
- <https://software.cisco.com>
- <https://id.cisco.com>

إلهيبتنلا جمارب ثي دحت تافلومو جماربلا ليزنتلا ةديدل ةزيملا هذه مادختسالا (CCOID) cisco.com مدمختسملا فرعم مادختساب ليچستلاب تمق كنأ نم دكأت ، ثي دحتلا ريديم

1. ريديملا إلهيبتنلا لوخدلا لچس .
2. ةيزكرملا ةرادإلا > ماع > نيوكترتخأ ، ةيسيئرلا ةمئاقلا نم .
3. Update Manager بيوبتلا ةمالع قوف رقنا .
4. ءحفص حتفل (ةرشابملا جماربلا ليزنت) Direct Software Downloads طابترالا قوف رقنا .

ليجستال.

ليجستال ليلعلم عدبل ليجستال رزلا قوف رونا 5.



6. رفوتمال طابترالا قوف رونا.

7. عباتملل يلاتال قوف رونا. كزاه طيشنت ءحفص ىل كلقن مئيس.

8. cisco.com (CCOID) ىلع كب صاخال مدختسمال فرعم مادختساب لوخذال لجس.

9. طيشنتال لامتكأ درجمب "زاهال طيشنت" ءلاسرى قىلتت فوس.

10. عباتم قوف روناو Manager في "ءرشابمال جامربال تاليزنت" ءحفص ىل دع.

11. ءارقول (K9) و (EULA) صرفال وفاق يققافتاب ءصاخال تالصولا قوف رونا - ءعباتم قوف رونا، طورشلال لوبق درجمب. اهلوبقو طورشلال

Cisco مءدب لصتا، جامربلل رشابمال ليزنتال لوح تامولعلمال نم ديزم ىلع لوصحلل

مير ATT&CK® لمع راطا

تاكيتكت نع روهمللل ءحاتم ءفرعم ءءاق لكشي Miter ATT&CK® ءكرش لمع راطا نا
لخا تاليلحتال نيكمت دنع. يقيققحال ملالاعال تاطحال م ىلع ءمئاقال مصخال تالينقتو
تاليدته فاشكتسا في MITER تالينقتو تاكيتكت ءعاست، ءنمآل ءكبشل تاليلحت
امل ءباجتسال او افاشتكاو ينورتكلال نامال.



To make sure Analytics is enabled, choose **Configure > Detection > Analytics** from the main menu, then click **Analytics On** .

MITER تامولعلم ىل لوصولا ءنمآل ءكبشل تاليلحت ءيلاتال تالاصتال ءيتت
ت:ءايبنتلل

- <https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json>
- <https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json>
- <https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json>

ءيدهتال ءيذغت

ءاكذ تامولعلم زجوم مساب اقباس فورعلمال Cisco Secure Network Analytics Threat Feed رفوي
ىل تاليدتهتال لوح ءيملالاعال ءياملحال تاليدتهت زجوم نم تاناي (Stealthwatch) تاليدتهت
ذفانمال ماقراو IP نينوانع نمضتيو رركتم لكشب بيول زجوم شيءت مئي. كتكبش

راض الطاشنلل مدختست اهنأب ةفورعمل URL نيوانعو فيضم المامسأو تالوكوتوربل او ةزهألا، مكحتل او مكحتل تامداخ: زجوملا في ةللالتل فيضم المامسأو مضمضت متي تاهجوملاو.

تاميلعتل في ةدراول تاميلعتل عبتا، ةزكرملا ةرادإلا في ديدعتل ةيذغت نيكمتل

1. يساسألا ريذمل إلى لوخذل لجس.
2. ةزكرملا ةرادإلا > ماع > نيوكت ددح.
3. تاميلعت ددح. (تاميلعت) ةنوقيأ رقنا.
4. ديدعتل بيو زجوم > زاهجل نيوكت ددح.



Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

[مماظنلل نيوكت ليلد](#) إلى عجرا، ديدعتل بيو زجوم لوح تامولعمل نم ديزم إلى لوصحلل

معذلابل لاصتالا

ةللالتل رومألا دحأب مايقلل يجر في، ينم معد إلى ةجاحب تنك اذا:

- كيدل يلمحمل Cisco كي رشب لصتا
- Cisco معدب لصتا
- بيلول ربع ةلأحتفل: <http://www.cisco.com/c/en/us/support/index.html>
- (ةدحتمل تايلالول) 1-800-553-2447: فتاهل ربع معذل إلى لوصحلل
- ةيملاعل معذل ماقرأل:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا