

ةفورعم ل Cisco XDR لئاسم

تايوتحم ل

[ةمدقم ل](#)

[ةفورعم ل تالكش ل](#)

[شداو ل](#)

[تاقى قحت ل](#)

[مكحت ل زكرم](#)

[Cisco لمك تاي لمع](#)

[ثلاث ل ف رطل ل لمك تاي لمع](#)

[لوص ل](#)

[XDR ةتم ل](#)

[راعش ت س ل ا ةزوح ل / ةزوح ل](#)

[نم ل ل ل ل](#)

[XDR تال لحت](#)

[اهلح مت لكاش م](#)

ةمدقم ل

Cisco XDR ل ا ل ا ح ةفورعم ل ةينقت ل لكاش م ل ل ا ق م ل ا ذه قثوي

اهنأ رابتع و ا ل ا راطت ناب ، ضارعت س ل ا ديق ، Cisco لبق نم ةينقت ل لكاش م ل رارق نكمي ع قوت م وه امك لمعت

ةفورعم ل تالكش ل

شداو ل

ي ل ا ل ا ت ق و ل ا ي ف ه ذه XDR ةفي طول ةفورعم لكاش م دجوت ال

تاقى قحت ل

ي ل ا ل ا ت ق و ل ا ي ف ه ذه XDR ةفي طول ةفورعم لكاش م دجوت ال

مكحت ل زكرم

ي ل ا ل ا ت ق و ل ا ي ف ه ذه XDR ةفي طول ةفورعم لكاش م دجوت ال

Cisco لمك تاي لمع

1. Cisco XDR - نم ل ل ل ل ا ر ا د ج ل ل م ا ك ل ل ل م ا ك ت ل - Cisco

لدابتو Cisco Defense Orchestrator (CDO) نيب سلسلا لمككتل نامضل :ليصافتلا نمضتت .يوديلا نييعتلا مزلي ،(SAL) ليحستلاو نامألا تاليلحتو (SSX) نامألا تامدخ .ةرورضللا تانييعتلاو تانيوكتلا ذيفنتل Cisco TAC ب لاصلتالا ةيلمعلا هذه

لمككتلا نامضو ةلصللا تاذ تاباسحلا طبري ف ةدعاسم لل TAC ب لصتا :ليدبلا لحلا مطنلل ميلسلا

يدي ب ي ت :عقوتما رارقلا

ثلاثا ف رطلا لمككت تاي لمع

XDR لمككت تاي لمع مادختسا G عون نم صيخارت مهيدل نيذلا Microsoft ءالمعل نكمي ال -1. Microsoft.

ممصم وه امك لمعلا :ةلاحلا

في Microsoft G عون نم تاقاقتسالا لىل لوصول ةيناكما ريفوت متي :ليصافتلا .طقف ةيموكتلا تانايللل اهيف مكحتلا متي يتلا تائيبل

سلجم ةئي ب عم لمككتلا تابللطم مهفل Microsoft عم Cisco لمعت :ةيلاتلا تاوطلخا Microsoft G عون نم تاقاقتسالا ريفوت اهيف متي يتلا Microsoft ل يجيللخا نواعتلا صيخارت عم لمككتلا مزتعي هنإف ،قيبطتلل الباق Cisco نم XDR رادصلإا ناك اذا Microsoft Defender for Endpoint، O365، و EntraID. J Microsoft G-type

[.انـه](#) حاتملا لمككتلا لح مت :عقوتما لحلا

لوصألا

.يلاحلا تقولا في هذه XDR ةفيظول ةفورعم لكاشم دجوت ال

XDR ةتمتأ

.يلاحلا تقولا في هذه XDR ةفيظول ةفورعم لكاشم دجوت ال

راعتستسالا ةزهجأ/ةزهجألا

.يلاحلا تقولا في هذه XDR ةفيظول ةفورعم لكاشم دجوت ال

نمآلا ليمعلا

[.ةلاقملا](#) عابتا يجري ،"نمآلا ليمعلا" ب ةقلعتما تالكشملا لىل عالطالل

XDR تاليلحت

في دحاو زاهج مساب ةددعتما ةفيضملا ةزهجألا ءامسأ وأ/و ةددعتما IP نيوانع نارقإ نكمي - 1. XDR-A

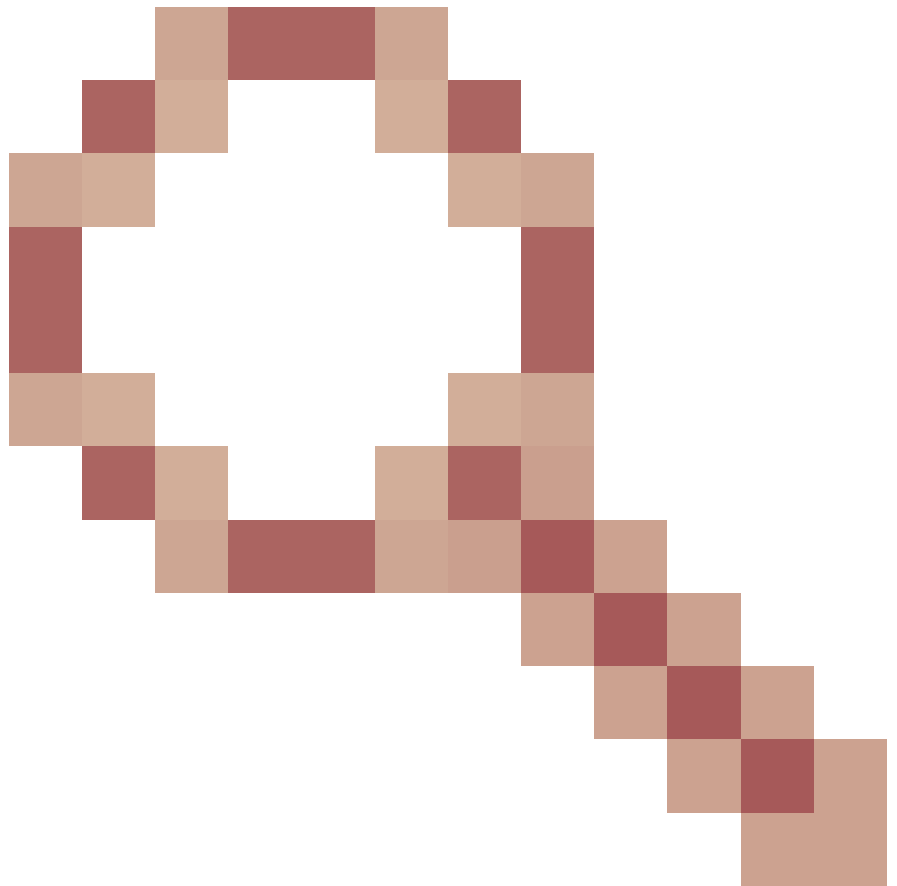
لجؤم/موسحم ريغ :ةلاحلا

SNA/XDR-A. ةبابوب لخاد دحاو زاهجب ةطشنل IP نيوانع نم ديدعل طبر نكمي :لليصافتلا
ىلع اضيا ةزهجالا ضعب يوتحت NVM ريغو NVM ةزهجا نم الك كلذ نمضتي نا نكميو
نوكي نا ىلا ةزهجالا ليحست يدؤي دق ،يلالحا ذيفنتلا ساسا ىلع .ةددعت متويب عامسا
ةيلزنملا ةكبشلا نم هذه IP نيوانع ضعب نوكي دق .(عقوم) دحاو IP ناوانع نم رثكا زاهجل
ةسسؤملا ةكبش ي IP نيوانع مدطصي دقو مدختسملل

يف ةدوجوم ةلكشملا لازت الو ،تقولا اذه يف ةلكشملا هذه لوح لمع دجوي ال :لحلا
لبقتسملا يف لصفأ وحن ىلع ةلأسملا هذه جلاعت نا يف لامآ ةمئو .ةيلالحا ةينبلا
و ONA نياردصملا الك نم ةكبشلا ةطشنا عيبطتت حمست ةديج ةينب ذيفنت درجمب
اعم اعمج و NVM

رفوتم ريغ :ةيلاتلا تاوطخلا

TBD / لبقتسملا :حوضولا ةقد



بقعتلا ةقاطب : [CSCwo67299](https://www.cisco.com/c/en-us/support/docs/cscwo67299.html)

اهلح مت لكاشم

1.- Cisco XDR ةبابوب ىلع Cisco نم ةنمآلا ةياهنلا ةطقن لمكث طابترا لمعي ال - Cisco XDR

اهلح راطتنابو ةلأسملا ديدحت :ةلالحا

ةطقنل "enable" طابترا عطق متي ،Admin > Integration بيوبت تامالع يف :لليصافتلا
ةحفص ىلا هيحوتلا ةداعا نألا متي ،نكمتلا رز ىلع طغضلا درجمب .ةنمآلا ةياهنلا
ىلا لاقتنالا نم الدب XDR org دجم ةحفص ىلا اهراركت متيو "تاديدهتلا ةباجتسالا"
ةنمآلا ةيفرطلا ةطقنلا مكحت ةدحو

Cisco نم ةنمآلآ ةياهنللا ةطقن ةباوب نم لمككتللا ذيفنت نكمي: لجلل

ةلكشملا هذه حالصا ذيفنت ىلع Cisco لمعت: ةيللاتلا تاوطخل

ةلكشملا هذه لح مت: ةقوتم لح

XDR ةركاذي في لآلآ جمدلاب ةصاخلا ثداوحلل ىئاقللللا لىغشتلا دعاوق لىغشت فقوت 2-
ةقوتم ريغ لكش

قللعملل لجلل او ةددحمللا ةلكشملا: ةلاجل

تايللمع ةطساوب اهليغشت متي يتلا ثداوحلا ةتمتأ دعاوق لىغشت فقوت: لىصافتلا
مدختسم ةهجاو في كلذل ىلإ ةراشإلا متي ال. ةقوتم ريغ لكشب تالغشملاو لمعملل ريس
يريس، كلذب مايقللا دنع. تقولا رورم عم لمعملل ريس سييأقم ةعجارم دنع ال، XDR،
ةلكشملا رارمتسا ىدمل اقفو كلذو، لمعت ال وأ لقأ لمع ريس تايللمع ءالمعل

ططخت. اهلل ىلع لمعتو XDR ةيفلللل نمض ةلكشمك اذه Cisco تددح: ةيللاتلا تاوطخل
في ةلكشملا هذه ثودح بنجتل ةيفاضا ةلاح عبتتو ةبقارم تازيم ذيفنتل اضيأ Cisco
لبلقتسملا.

لمعملل ريس ةدعاوق لىغشت ةداعا ءدبل اهنىكمت ةداعاو ةدعاوقلا لىطعتب مق: لىدبلل لجلل
ةجللعملل او اهذيفنت متي يتلا.

لجلل مت: ةقوتم ةقد

ىلإ ريشي أطخ دوجو عم ةيرهاظلا تائيبلا في ONA تيبتت لشف - Cisco XDR-Analytics - 3.
"يرابتللا عومحملل نم ققحتلل لشف"

قللعملل لجلل او ةددحمللا ةلكشملا: ةلاجل

لامكإ في ISO لشف في، ةيضارتفا ئيب في ONA رعشتسم رشن دنع: لىصافتلا
ءاطخلال ثدحيو تيبتتلا ةيللمع

تاوطخ عبتاو Ubuntu ISO عم لقتسم لكشب Ubuntu Server 24.04 تيبتتب مق: لجلل
U2 7.0 عم قفاوتلل مدختسا. ةمدخل ONA لىغشتل [مدقتملل تيبتتلل](#)

رفوتم ريغ: ةيللاتلا تاوطخل

ONA رعشتسم نم رادصا ثدحأ في ةلكشملا هذه لح مت: ةقدلل

مادختساب اهلل مت يتلا ثداوحلل ةقيقد ريغ اماقراً مكحتلل زكرم ىلع ةطالبل رهظي MTTR-4.
هرىغ وأ دكؤملا ديهتلا: قلغم"، "بذاك بجوم: قلغم" لثم ةديجللا تالاجلل ىدحإ

اهلل راطتئابو ةلأسملل دىحت: ةلاجل

ذخأت الوريانى / يئانللا نوناك 15 في ثداحلل ةديجل تالاج لاخدا مت دقو: لىصافتلا
ئاوىتحت كلذللو، راج لمع هنا ىلع دىجلل رارقلا رسفيو. رابتللا في لودلا كلت ةطالبل
ايراج الممع ربتعي هنا، ةديجللا تايللولا ىدحإ مادختساب قلاغأ دق ثداحلا اذه ناك

ءيش ال: لىدبلل لجلل

ءيش ال: ةيللاتلا تاوطخل

لحل المت: عقوتم الارق

[طابترال](#) اذه ف ةدراول تاميلعتلابتاف Cisco، معدب لاصتالالى ةجاحب تنك اذا

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 ط 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