

اهنيكمت واهالصل او NVM ءاطخأ فاشكتسأ XDR تاليلحتل

تايوتحمل

[قمدملا](#)

[فيساسألا تابلطتملا](#)

[تابلطتملا](#)

[قمدمتسملا تانوكملا](#)

[تاقفدتلا XDR NVM تاليلحت](#)

[XDR تاليلحت - NVM تانايب تاقفدت](#)

[NVM رعشتسم قلاخ](#)

[NVM قسسؤم فرع](#)

[NVM Data Lake دادملا قلاخ](#)

[ءاطخألا جيحصت](#)

[تاهيبتنلاو تاطخالمل](#)

[NVM تاهيبتن](#)

[NVM هيبتن تادادع](#)

[قینطولا دصرلا قیلأ تاشب تاطخالمل](#)

[NVM فاشكتا تاراركت](#)

[بارقلا](#)

قمدملا

Cisco تاليلحتل اهالصل او Cisco XDR ءاطخأ فاشكتسأ ةيفيك دنتسملا اذه فصي (NVM) ةكبشلل ةيؤر ةيناكل ةيظمنلا ةدحول / (XDR) eXtended Detection and Response

ةفيساسألا تابلطتملا

XDR لماكتم عم طشنلا XDR تاليلحت لخدم

تابلطتملا

دحو XDR لماكتم مادختساب XDR تاليلحت باسح ليغشت

قمدمتسملا تانوكملا

- XDR تاليلحت
- XDR
- NVM رعشتسم
- (5.0+ رادصلال) نمالال ليمعلا

عصاخ ةي لمعم ةئي ب ي ف ةدوچومل ةزهجال نم دنن سمل اذه ي ف ةدراول تامولعمل عاشن ا م تناك اذا .(يضا رتفا) حوسمم نيوكتب دنن سمل اذه ي ف ةمدختسمل ةزهجال ا عي مج تادب رمل ا ل م حمل ري ثا تلل كمهف نم دكا تف ،لي غشتل دي ق ك تكبش

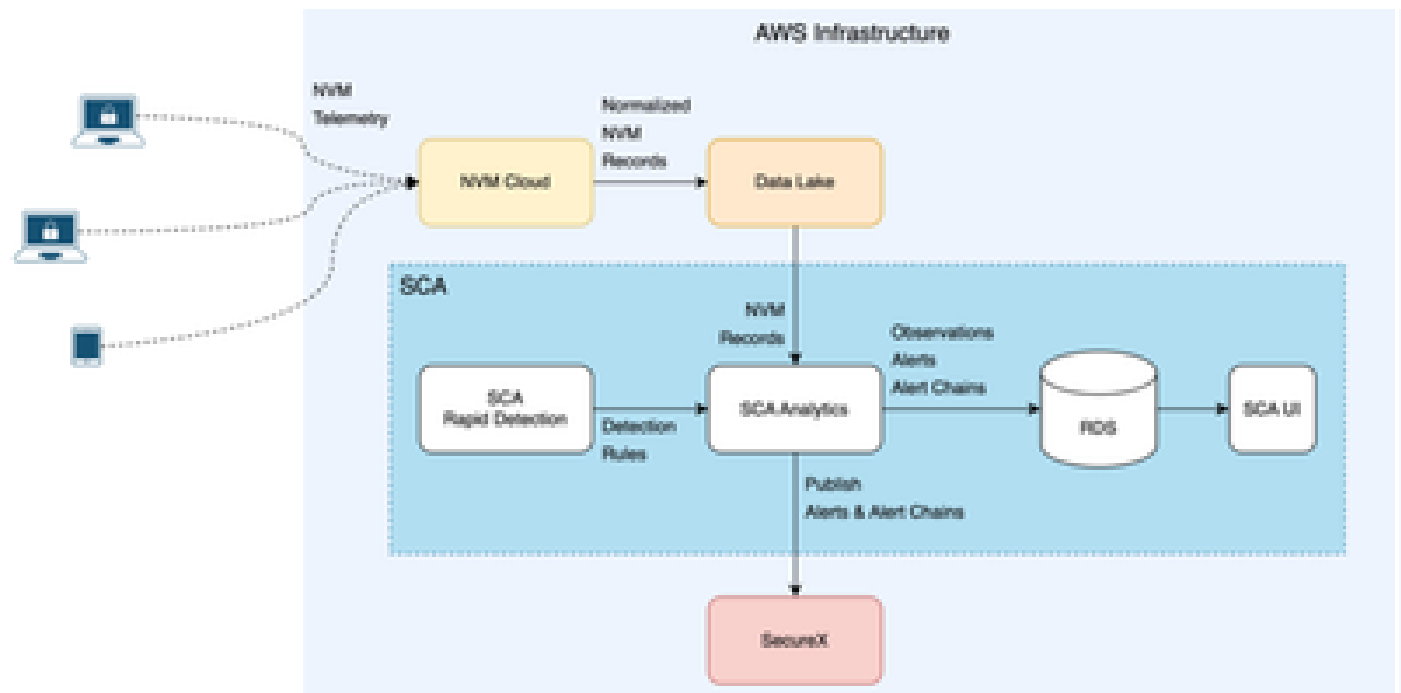
تاقف دتلل XDR NVM تاليلحت

NVM عبتت تانايب نال XDR تاليلحت كلهتست
Cisco Secure Client ي ف NVM نوكم ةطساوب مادختسال عبتت تانايب عاشن ا م تي

تالاصتاو مدختسمل تاياكولس كلذ ي ف امب ،ةكبشلل ةنسح م ةيؤر ةيناكم ا NVM رفوت ةيؤر ي ف تارغلثال دسو ثداوخل ي ف قي قحتل تاقوليلقت يلاتلابو ،تايلعملالو ةكبشلال ةيانهلل ةطقن

<https://docs.xdr.security.cisco.com/Content/Help-Resources/nvm-resources.htm>

XDR تاليلحت - NVM تانايب تاقف دتل



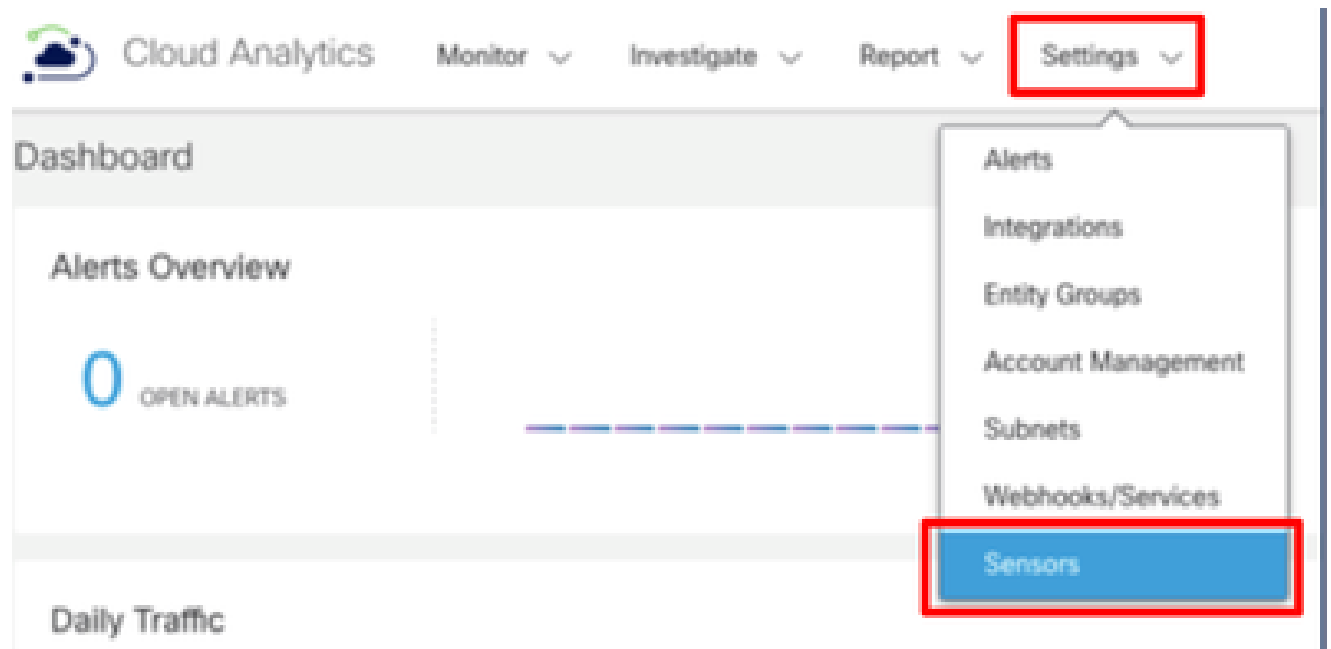
- اذه لمعمل ريس بلطتي ،كب ةصاخال Secure Client تارادصل عم شي دحتلاب امئاد ي صون :
ثدحا رادصل او Secure Client نم 5.0 رادصل ا مادختس
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Deployment و رادصل ال Secure Client ل مخيرات يتح شي دحتب ظافتحال
Profile: <https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm>
- ثدحال ةرفوتم اهل عجتو دعب نع سايقلا تانايب مجح ةجالعمب NVM ةباحس موقت
لاعل ني زختل اهعيبطتو دعب نع سايقلا Data Lake تارادصل
- قئاقد 10 ةمظتنم ةينمز تارفت يلعل NVM تالاجس ةجالعم يلعل XDR تاليلحت لمعت

تاهي بنت لاو ب قارم لا تاي لمع - فشك لا تاي لمع عاشن إل

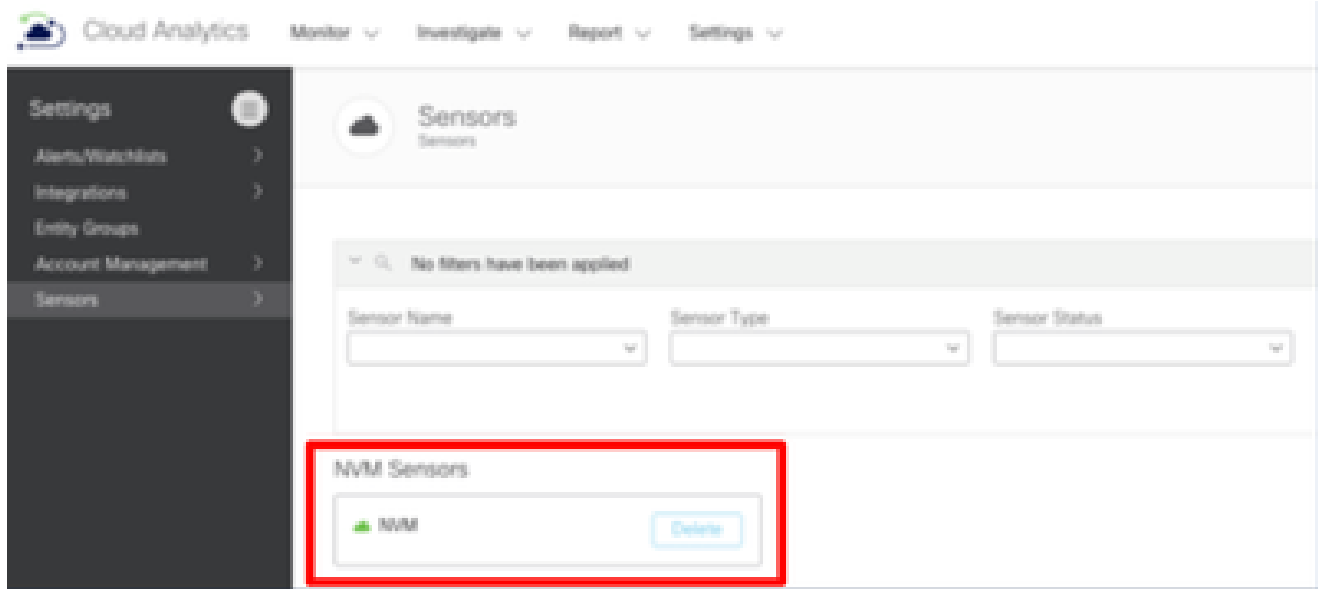
- عرسب ة طيسب تاهي بنت و تاظالم ة فاضا إل ع عرسلا فشك لا تاي لمع دعاست ة ئهتلا تاي لمع مادختساب
- هيبنتلا لسالس) تامجهلا لسالس في تاهي بنتلا طبرب XDR تاي لحت موقت (اقباس
- XDR إل تامجهلا و هيبنتلا لسالس رشن مدختسم لل نكمي

NVM رعشتسم ةلاح

- تادادع إل إل لقتنا، XDR تاي لحت تامولعم ةحول نم :- NVM رعشتسم عاشن نم دكأتلا راعشتسالا ةزهجاً >



- رعشتسم لا ةمئاق في NVM رعشتسم رفوت نم دكأت مث



ەدحاو XDR ەسسۇم/رجأتسم رثكألإ ىلع XDR تاليلحت لخدمل نوکي نأ بجي :ريذحت
هه ەنرتقم.

NVM ةسسؤم فرع م

- API ةياهن ةطقن يف هسفن ةسسؤم الفرع ضرع مهيدل NVM ءالمع نأ ديكأت :
https://XDR Analytics_portal_url/api/v3/integration/securex/orgs/

```
pretty_print(  
{"meta":{"limit":1000,"next":null,"offset":0,"previous":null,"total_count":1},"objects":[{"org_id":"XXXXXXXXXXXXXXXXXXXX","org_name":"Cisco"}]}
```

NVM Data Lake دادم ةلاح

- حطسلا ىلع تانايبلا ةريحب دوجو نم دكأتلل تاقيبطتلا ةجمر رب ةهجاول ةياهنلا طاقن تاقيبطتلا ةجمر رب ةهجاو ةياهن ةطقن مادختساب طابترا لا ديكأت نكمي ،جحص لكشب هذه :
https://XDRAnalytics_portal_url/api/v3/integration/securex/orgs/on_datalake/

```
Pretty print ☐  
"DataLake provisioned successfully"
```

- ىلإ لوصول ةباوبلا لالخنم لوصول قح مهحنم مت نيذل ني مدختسملا عيمجل نكمي (Engineering و TAC و لخدملا ولوؤسم) هذه ةياهنلا طاقن

ءاطخالا جحصت

- جحصت لل ةباجتسالا زمر :

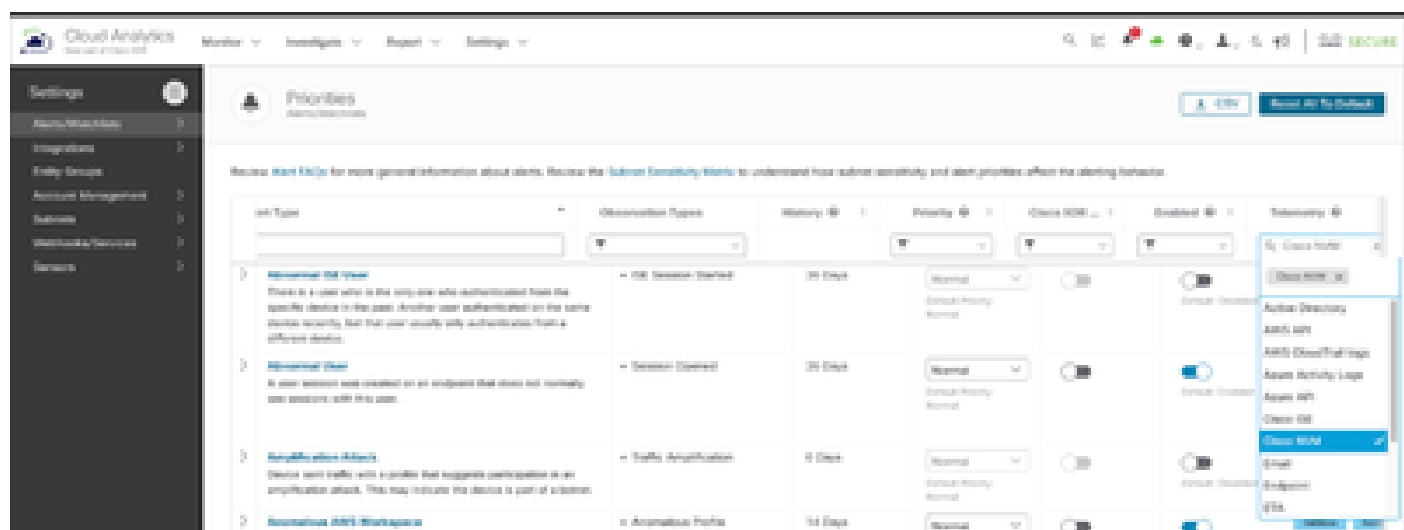
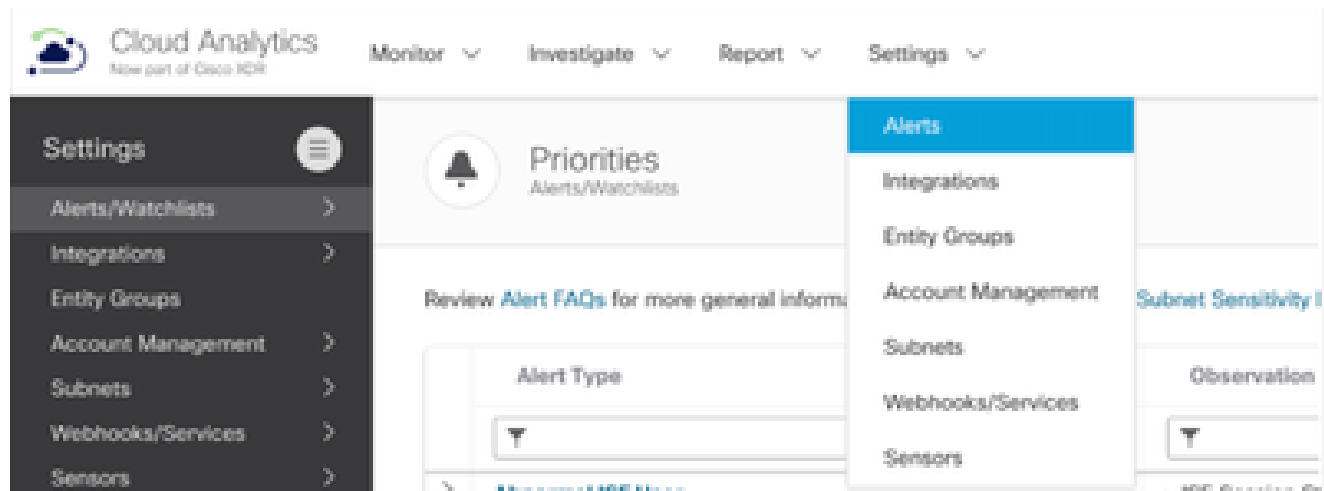
بولطم ءارجالا	ةباجتسالا زمر
ضراع ربع NVM تاقفدت ةحص نم ققحتلا ثادحالا	حاجنب DataLake ريفوت مت
ليصوتل ةدحاو ةرقنب XDR جمدمدختسأ XDR و XDR تاليلحت	م تي مل ، تانايبلا ةريحب ريفوت رذعت XDR ةسسؤم نع فشكال
ةدعاسم لل TAC ب لاصتالا	نع فشكال مت ، DataLake ريفوت رذعت ةددعتم XDR تاسسؤم

- ريراقتلا دادعاو صيخشتل ةادأ" ليغشتب مق ، تاوطخل هذه نم يأ لشف ةلاح يف امئاد بلطا) ةلكشملا صيخشتل "نمآلا ليمعلا" ةهجاو نم "(DART) نينمآلا ءالمع لل (لوؤسمك DART ليغشت
[نمآلا ليمعلا DART ةمزح عيمجت](#)

تاهي بننلاو تاظالملا

NVM تاهي بنت

- XDR تالېلحت لخدم ىل ل لودل لېجست
- AlertsTelemetry > Cisco NVM > تادادع
- Cisco NVM > دع ب نع سايقلا



NVM ھېسابت تادادغا

Priorities						Clear All	Reset All
Review Alert FAQs for more general information about alerts. Review the Subnet Sensitivity Matrix to understand how subnet sensitivity and alert priorities affect the alerting behavior.							
Alert Type	History	Priority	Enabled	Published to Secured	Subnetting		
LDP-Connection from Suspicious Process This device was detected running a non-standard LDP process. This might indicate an credential theft attempt.	0 Days	Normal	☒	☐	☐	Close Modal	
Malicious Process Detected A process running has a hash matching one in a list of known malicious process hashes	0 Days	Normal	☒	☐	☐	Close Modal	
Metasploit Executed Execution of the offensive tool Metasploit has been detected in endpoint's endpoint telemetry	0 Days	Normal	☒	☐	☐	Close Modal	
Port 8888: Connections from multiple sources Multiple devices transferred files to a host serving on a busy port. This might indicate an exfiltration attempt.	0 Days	Normal	☒	☐	☐	Close Modal	
Potential Persistence Attempt This device was detected applying known persistence mechanisms like establishing background processes used for network access or running applications from network shares	0 Days	Normal	☒	☐	☐	Close Modal	
Potential System Process Impersonation A process with a name that looks like a common process has been executed indicating process impersonation	0 Days	Normal	☒	☐	☐	Close Modal	
SMB(SMB): Connection to multiple destinations The host has transferred files to multiple destination hosts using SMB and connected to those hosts using RDP. This could indicate lateral movement.	1 Days	Normal	☒	☐	☐	Close Modal	
Suspicious Process Path A process was executed on an endpoint from a directory that shouldn't have executables	0 Days	Normal	☒	☐	☐	Close Modal	

هين طولا دصرلا ةيلآ ناشب تاظحالم

- هيف لكوشم ةياهن ةطقن طاشن -
- XDR تاليلحت لخدم -
- تاظحالم > ةشاش -
- قراتخم ةظحالم -
- بيرمل ةياهنلا ةطقن طاشن ةيفصت -

Cloud Analytics

Monitor
Investigate
Report
Settings

Observations
Highlights
Types
By Device
Selected Observation

Selected Observation

Observations

Persistent External Server observation

Observation Type*

Suspi

ISE Suspicious Activity

Suspicious Endpoint Activity

Suspicious Network Activity

Suspicious SMB Activity

Search

Filter by source name, sha1, net

NVM فاشتك تاراركت

- طقف طبترم ةكبش لاصتا اهل يتلا قفدتلا تانايبو تايلمعل NVM طقتلي -
- يضارتفا لكشب قفدتلا ةياهن يف طقف قفدتلا تانايب نع غالبلا NVM نيوكت متي -

رارقلا

تاهي بنتلاو تاظحالملا نيكمتل XDR تاليلحت ربع لقننتلا يف تاوطلخال هذه كدعاست
اهالصل او لمعل ريس فاشكتساو NVM تامولعم مادختساب

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