أستكشاف أخطاء NVM وإصلاحها وتمكينها لتحليلات XDR

المحتويات

المقدمة

يصف هذا المستند كيفية أستكشاف أخطاء Cisco XDR وإصلاحها لتحليلات Cisco eXtended Detection and Response (XDR) / الوحدة النمطية لإمكانية رؤية الشبكة (NVM)

المتطلبات الأساسية

مدخل تحليلات XDR النشط مع تكامل XDR

المتطلبات

تشغيل حساب تحليلات XDR باستخدام تكامل XDR واحد

المكونات المستخدمة

- تحليلات XDR
- XDR
- مستشعر NVM
- العميل الآمن (الإصدار 5.0+)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

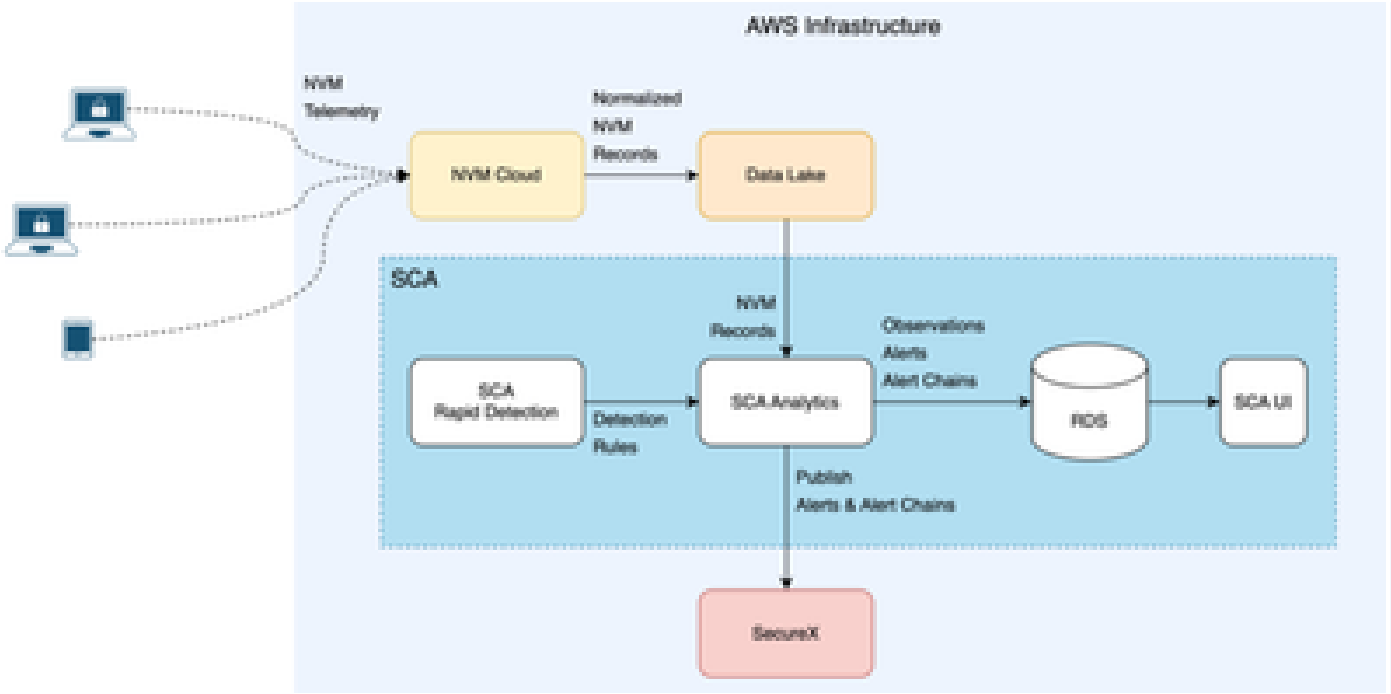
تحليلات XDR NVM التدفقات

تستهلك تحليلات XDR الآن بيانات تتبع NVM
يتم إنشاء بيانات تتبع الاستخدام بواسطة مكون NVM في Cisco Secure Client.

توفر NVM إمكانية رؤية محسنة للشبكة، بما في ذلك سلوكيات المستخدم واتصالات الشبكة والعمليات، وبالتالي تقليل وقت التحقيق في الحوادث وسد الثغرات في رؤية نقطة النهاية

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

تدفقات بيانات NVM - تحليلات XDR



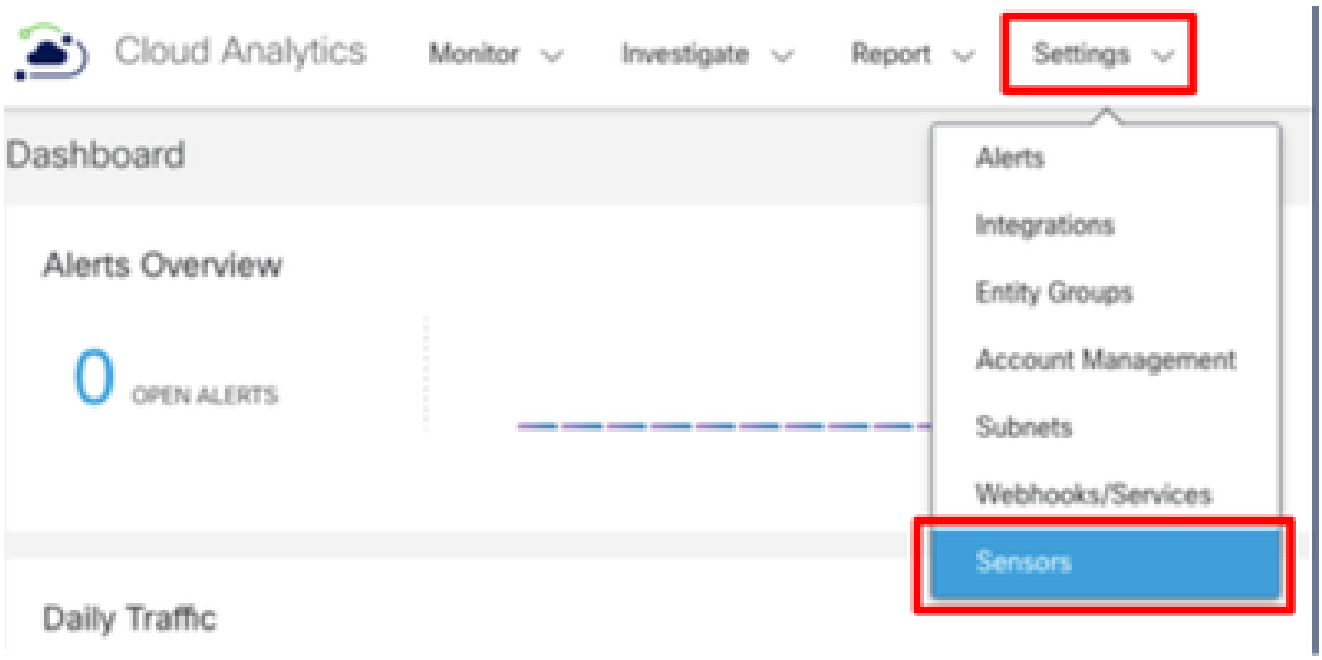
- نوصي دائما بالتحديث مع إصدارات Secure Client الخاصة بك، يتطلب سير العمل هذا إستخدام الإصدار 5. 0 من Secure Client أو إصدار أحدث : https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- الاحتفاظ بتحديث حتى تاريخ ل Secure Client الإصدار و Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- تقوم سحابة NVM بمعالجة حجم بيانات القياس عن بعد وتجعلها متوفرة لأحدث إصدارات Data Lake للقياس عن بعد وتطبيعها لتخزين فعال
- تعمل تحليلات XDR على معالجة سجلات NVM على فترات زمنية منتظمة (10 دقائق)

لإنشاء عمليات الكشف - عمليات المراقبة والتنبيهات

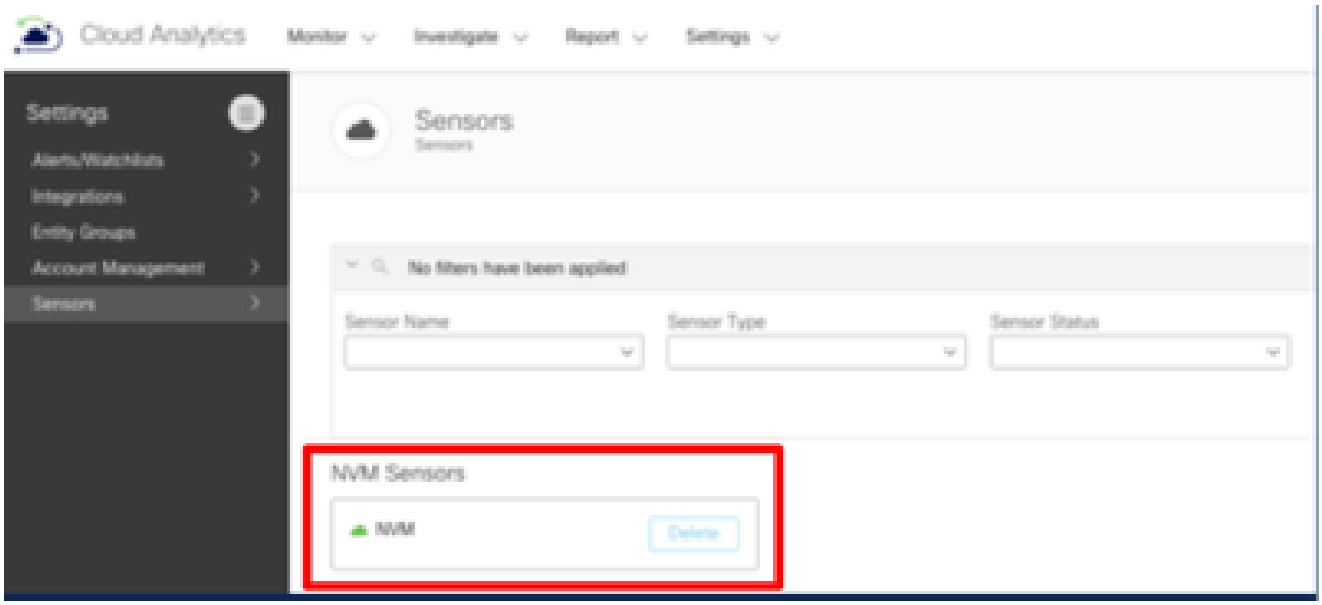
- تساعد عمليات الكشف السريع على إضافة ملاحظات وتنبيهات بسيطة بسرعة باستخدام عمليات التهيئة
- تقوم تحليلات XDR بربط التنبيهات في سلاسل الهجمات (سلاسل التنبيه سابقا)
- يمكن للمستخدم نشر سلاسل التنبيه والهجمات إلى XDR.

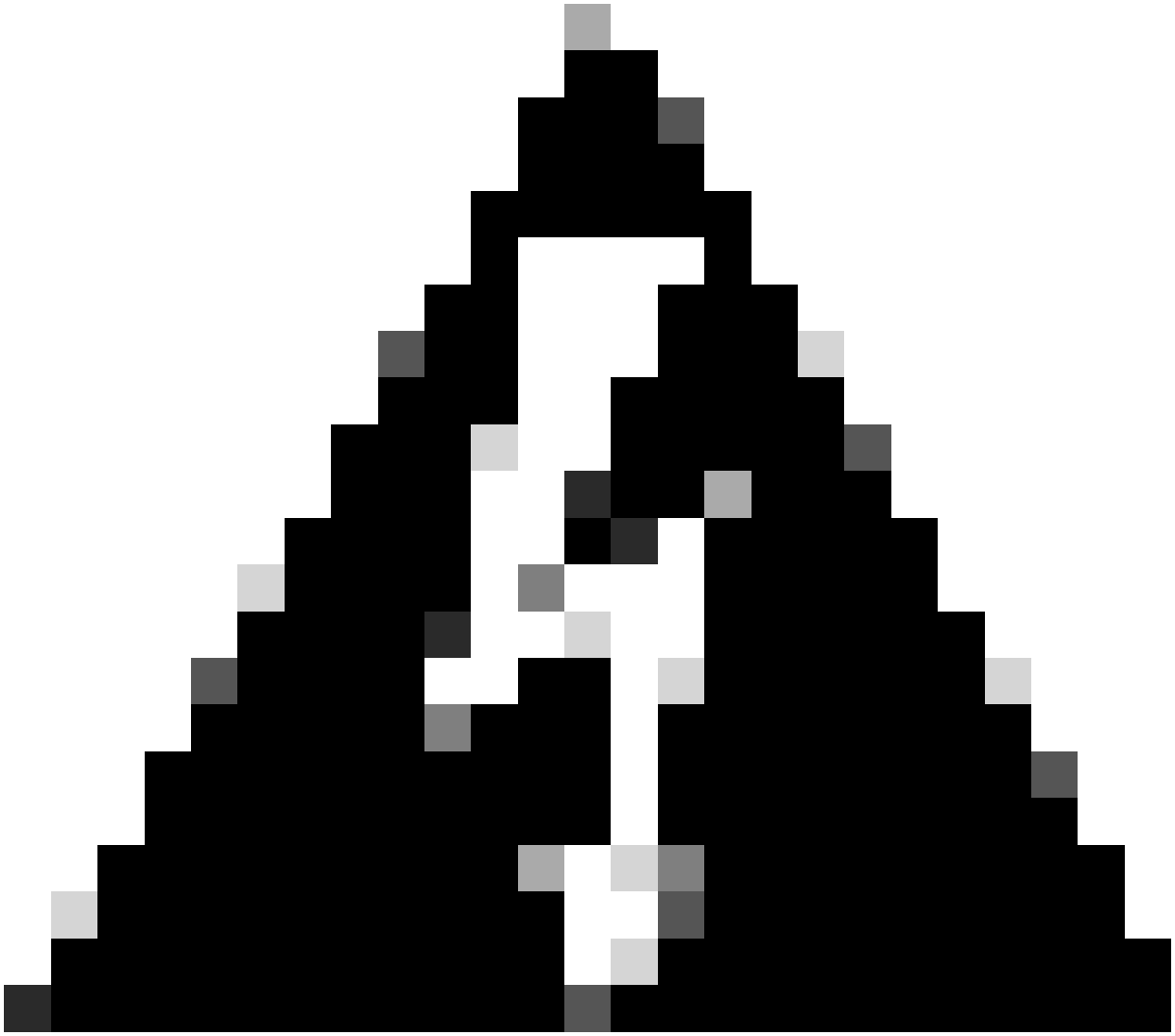
حالة مستشعر NVM

- التأكد من إنشاء مستشعر NVM:- من لوحة معلومات تحليلات XDR، انتقل إلى الإعدادات > أجهزة الاستشعار



- ثم تأكد من توفر مستشعر NVM في قائمة المستشعر





تحذير: يجب أن يكون لمدخل تحليلات XDR على الأكثر مستأجر/مؤسسة XDR واحدة مقترنة به.

معرف مؤسسة NVM

- تأكيد أن عملاء NVM لديهم عرض معرف المؤسسة نفسه في نقطة نهاية API : https://XDR Analytics_portal_url/api/v3/integration/securex/orgs/

حالة إمداد NVM Data Lake

- نقاط النهاية لواجهة برمجة التطبيقات للتأكد من وجود بحيرة البيانات على السطح بشكل صحيح، يمكن تأكيد الارتباط باستخدام نقطة نهاية واجهة برمجة التطبيقات هذه :https://XDRAnalytics_portal_url/api/v3/integration/securex/orgs/on_datalake/

- يمكن لجميع المستخدمين الذين تم منحهم حق الوصول من خلال البوابة الوصول إلى نقاط النهاية هذه (مسؤول المدخل و TAC و Engineering)

تصحيح الأخطاء

- رموز الاستجابة للتصحيح:

رمز الاستجابة	الإجراء مطلوب
تم توفير DataLake بنجاح	التحقق من صحة تدفقات NVM عبر عارض الأحداث
تعذر توفير بحيرة البيانات، لم يتم الكشف عن مؤسسة XDR	أستخدم دمج XDR بنقرة واحدة لتوصيل تحليلات XDR و XDR
تعذر توفير DataAlke، تم الكشف عن مؤسسات XDR متعددة	الاتصال ب TAC للمساعدة

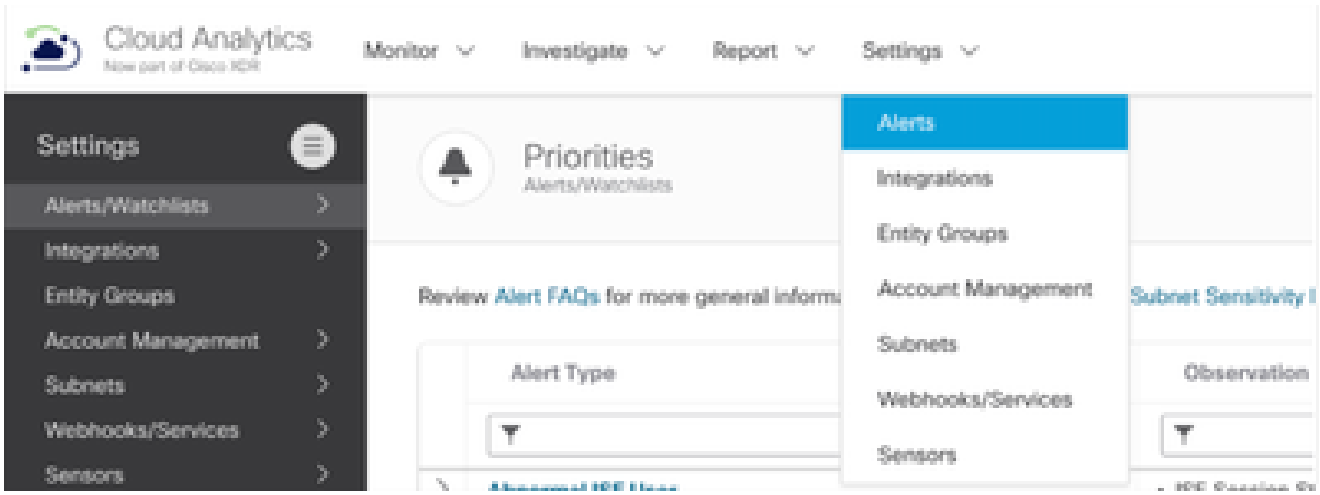
- في حالة فشل أي من هذه الخطوات، قم بتشغيل "أداة التشخيص وإعداد التقارير للعملاء الآمنين (DART)" من واجهة "العميل الآمن" لتشخيص المشكلة (اطلب دائما تشغيل DART كمسؤول)
تجميع حزمة DART للعميل الآمن

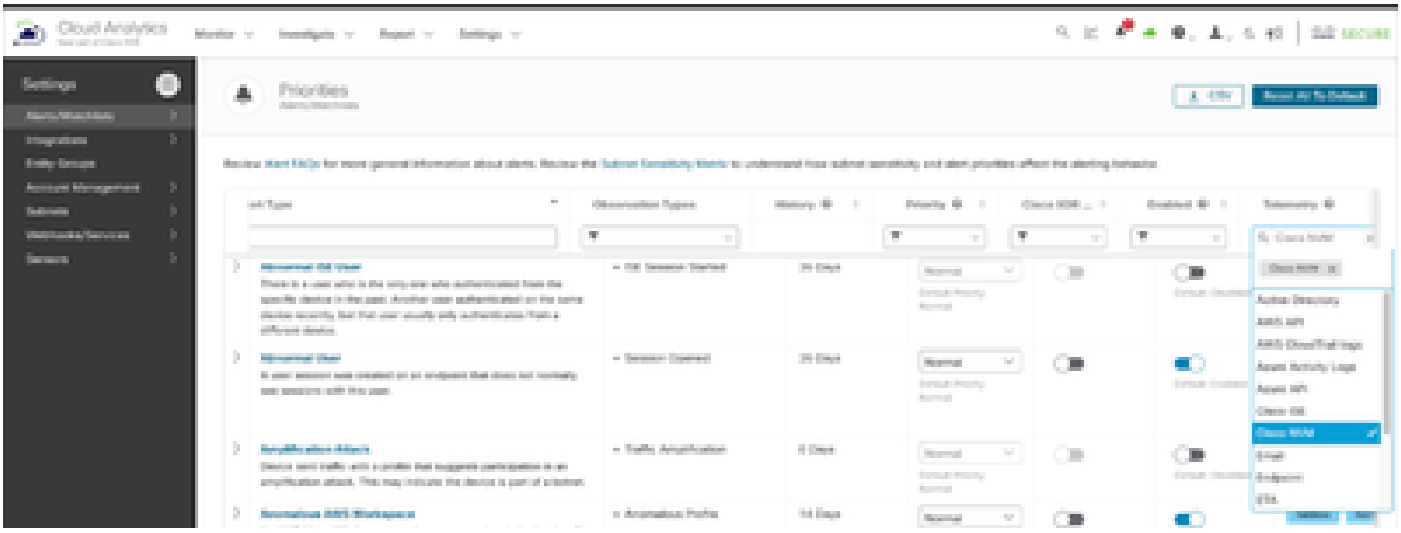
الملاحظات والتنبيهات

تنبيهات NVM

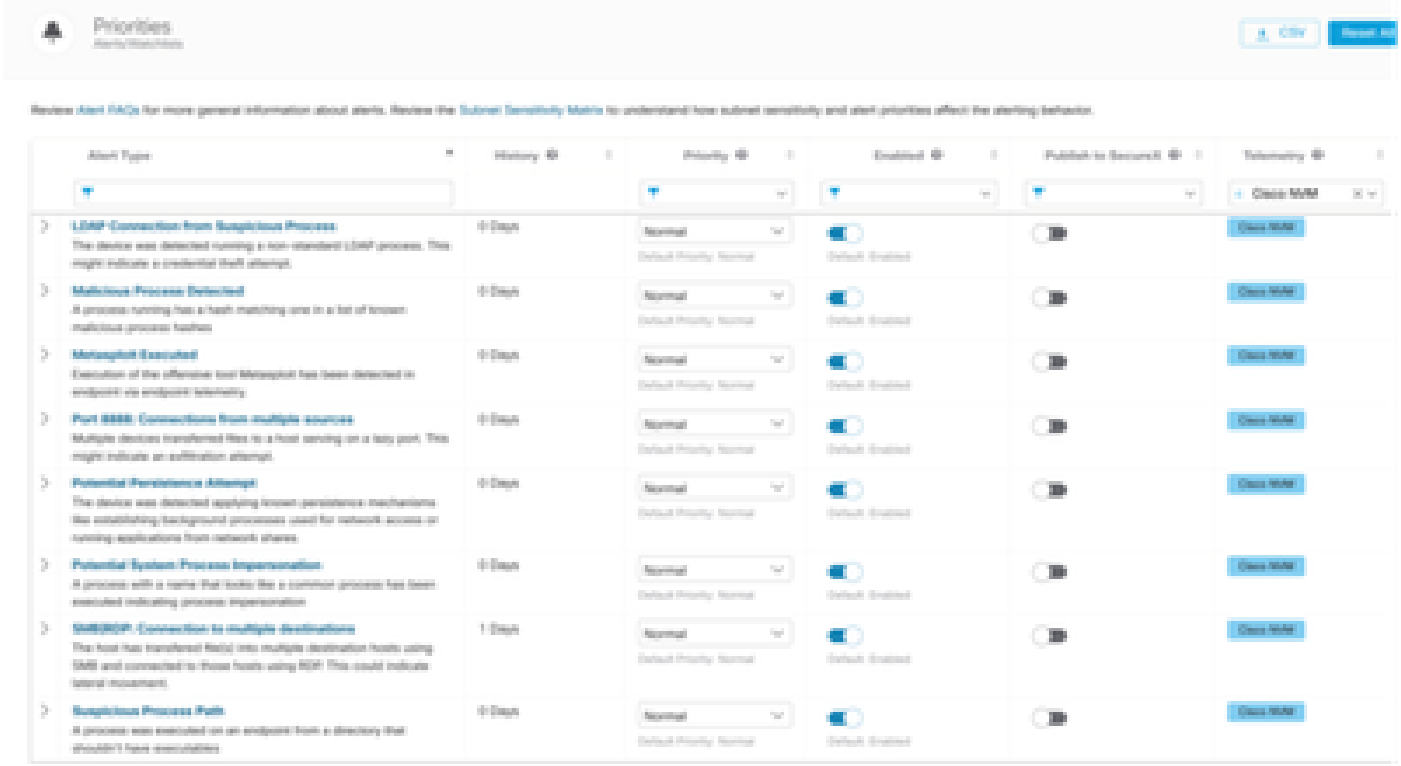
- تسجيل الدخول إلى مدخل تحليلات XDR
- إعدادات > AlertsTelemetry > Cisco NVM

- القياس عن بعد > Cisco NVM



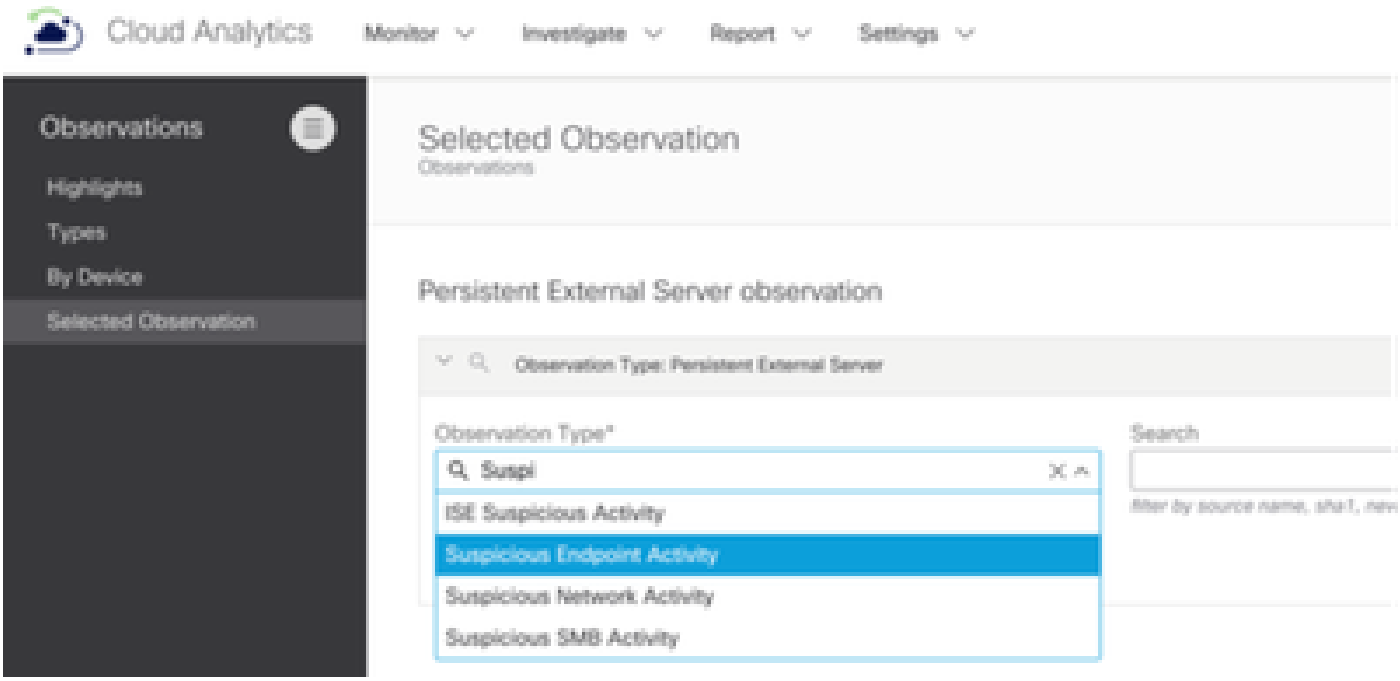


إعدادات تنبيه NVM



ملاحظات بشأن آلية الرصد الوطنية

- نشاط نقطة نهاية مشكوك فيه
- مدخل تحليلات XDR
- شاشة > ملاحظات
- ملاحظة مختارة
- تصفية نشاط نقطة النهاية المريب



تكرارات اكتشاف NVM

- يلتقط NVM العمليات وبيانات التدفق التي لها اتصال شبكة مرتبط فقط
- يتم تكوين NVM للإبلاغ عن بيانات التدفق فقط في نهاية التدفق بشكل افتراضي

القرار

تساعدك هذه الخطوات في التنقل عبر تحليلات XDR لتمكين الملاحظات والتنبيهات باستخدام معلومات NVM واستكشاف سير العمل وإصلاحها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).