Fehlerbehebung und Aktivierung von NVM für XDR-Analysen

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Cisco XDR-Analysen für Cisco Xtended Detection and Response (XDR)/Network Visibility Module (NVM) beschrieben.

Voraussetzungen

Aktives XDR-Analyseportal mit XDR-Integration

Anforderungen

Ausführung des XDR-Analytics-Kontos mit einer einzigen XDR-Integration

Verwendete Komponenten

- XDR-Analysen
- XDR
- NVM-Sensor
- Sicherer Client (Version 5.0+)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

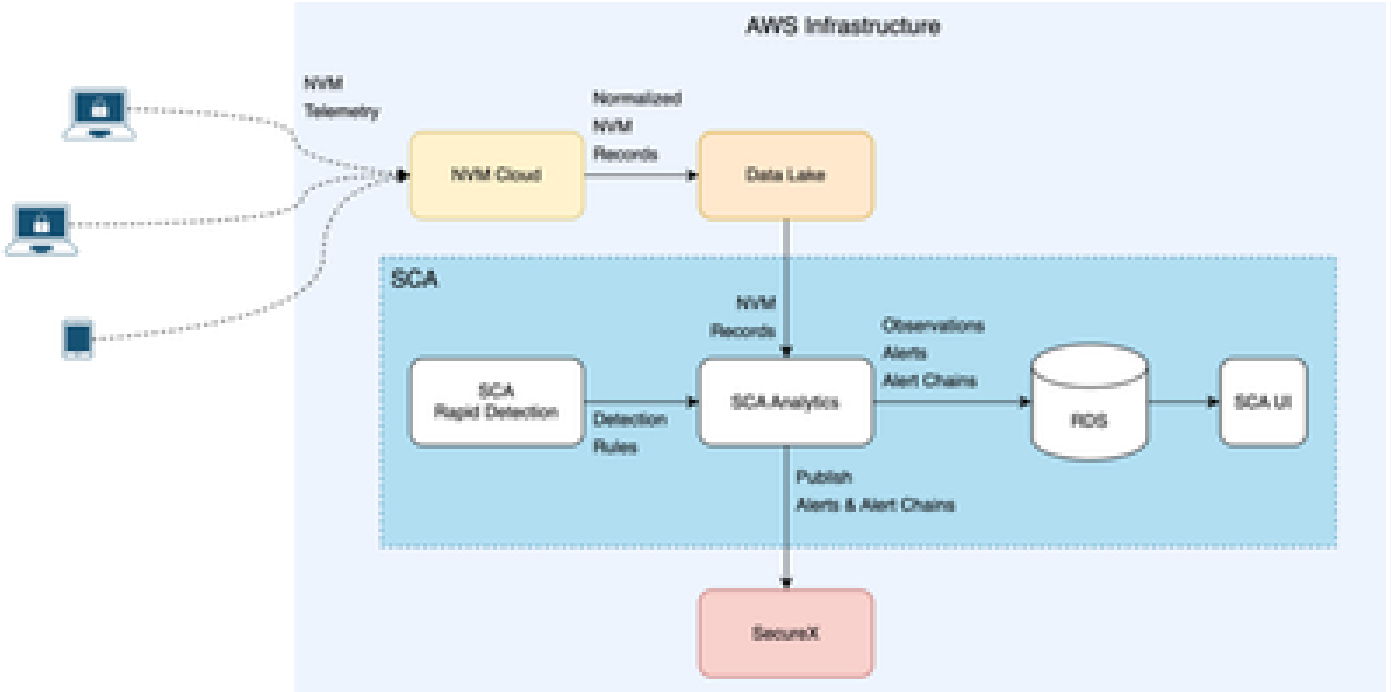
XDR-Analysen NVM-Datenflüsse

XDR Analytics nutzt jetzt NVM-Telemetrie
Die Telemetrie wird von der NVM-Komponente des Cisco Secure Client generiert.

Die NVM bietet eine verbesserte Netzwerktransparenz, einschließlich des Benutzerverhaltens, der Netzwerkkommunikation und der Prozesse, wodurch der Zeitaufwand für die Vorfalluntersuchung reduziert wird und Lücken in der Endpunkttransparenz geschlossen werden.

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

NVM-Datenflüsse - XDR-Analysen



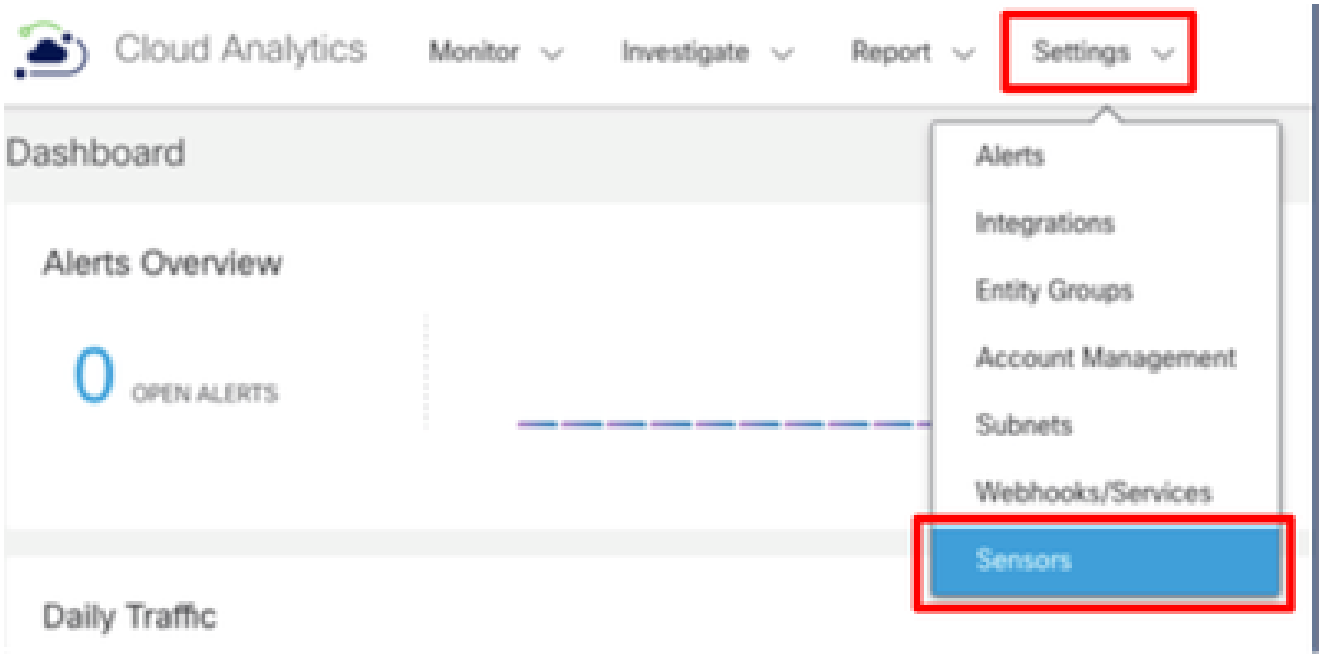
- Wir empfehlen stets, die aktuellen Versionen von Secure Client zu verwenden. Für diesen Workflow ist Secure Client Version 5.0 oder höher erforderlich: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Aktualisieren Sie Ihr System auf die aktuelle Version von Secure Client und Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud verarbeitet das Telemetriemetriematerial und stellt es für die Erfassung zur Verfügung. Data Lake nimmt die Telemetriedaten auf und normalisiert sie für eine effiziente

Speicherung.

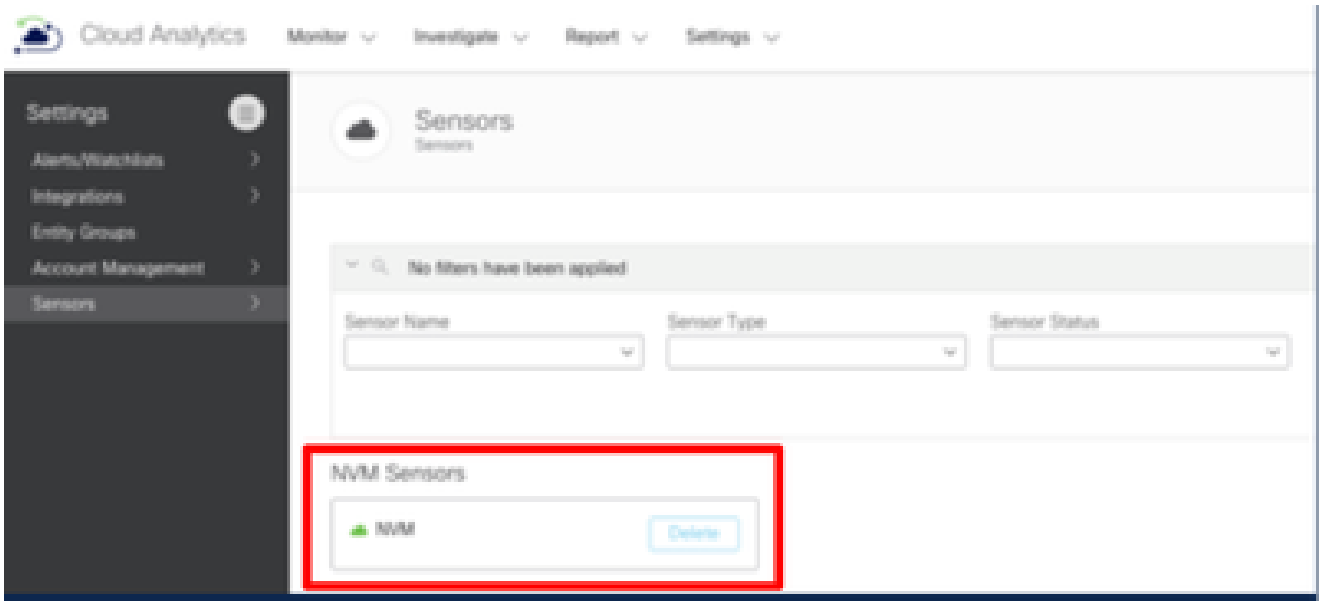
- XDR Analytics verarbeitet NVM-Datensätze in regelmäßigen Abständen (10 Minuten), um Erkennungen zu generieren - Beobachtungen und Warnungen
- Schnelle Erkennung ermöglicht schnelles Hinzufügen einfacher Beobachtungen und Warnungen mithilfe von Konfigurationen
- XDR-Analytik korreliert Warnungen mit Angriffsketten (ehemals Warnketten)
- Benutzer können Warn- und Angriffsketten auf XDR veröffentlichen.

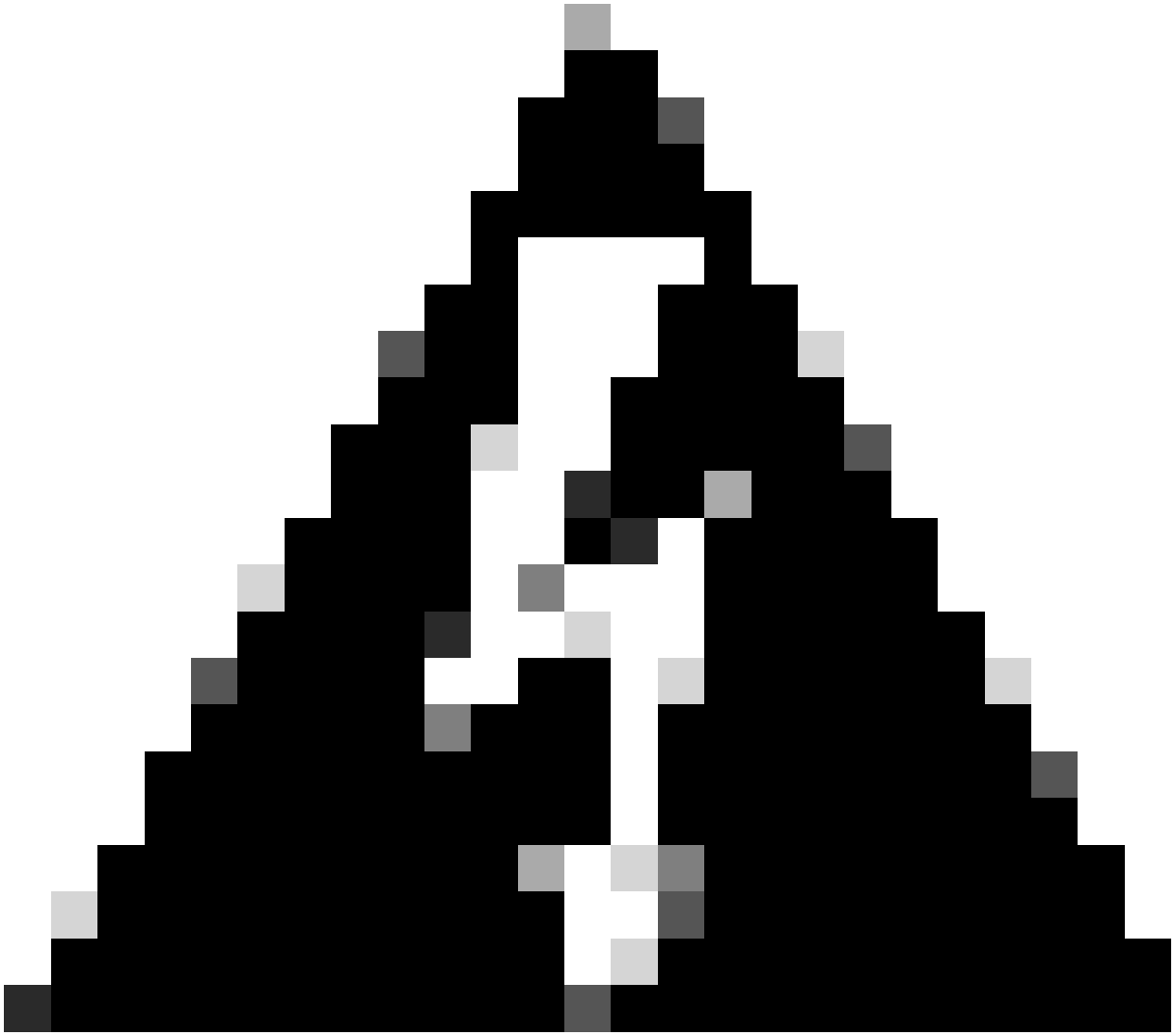
NVM-Sensorstatus

- Sicherstellen, dass der NVM-Sensor erstellt wurde:- Navigieren Sie im XDR-Analyse-Dashboard zu "Einstellungen > Sensoren".



- Bestätigen Sie anschließend, dass der NVM-Sensor in der Sensorliste verfügbar ist.





Warnung: Dem XDR-Analytikportal muss maximal ein einzelner XDR-Tenant/eine einzelne Organisation zugeordnet sein.

NVM-Org-ID

- Vergewissern Sie sich, dass die NVM-Clients die gleiche im API-Endpunkt angezeigte Organisations-ID aufweisen:
  https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/

NVM Data Lake-Bereitstellungsstatus

- Die API-Endpunkte, um sicherzustellen, dass der Datensee ordnungsgemäß integriert ist, kann die Zuordnung mithilfe dieses API-Endpunkts bestätigt werden:https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/

- Alle Benutzer, denen Zugriff über das Portal gewährt wird, können diese Endpunkte erreichen (Portal-Administratoren, TAC, Techniker)

Debuggen

- Debugging-Antwortcodes:

Antwortcode	Aktion erforderlich
DataLake erfolgreich bereitgestellt	Validierung von NVM-Flows über die Ereignisanzeige
Datensee kann nicht bereitgestellt werden, keine XDR-Organisation erkannt	XDR und XDR Analytics mit einem Klick integrieren
Datenpakete können nicht bereitgestellt werden. Mehrere XDR-Organisationen wurden erkannt.	TAC-Unterstützung kontaktieren

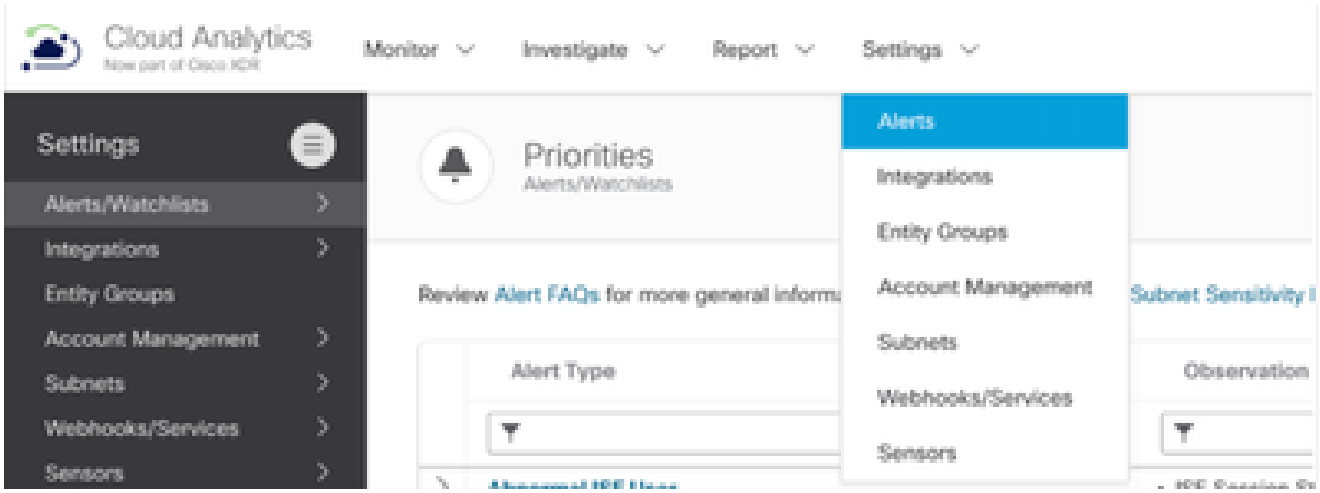
- Wenn einer dieser Schritte fehlschlägt, führen Sie das Secure Client Diagnostics And Reporting Tool (DART) über die Secure Client-Schnittstelle aus, um das Problem zu diagnostizieren (fordern Sie DART immer als Administrator an).
  Sammeln Sie DART-Pakete für sichere Clients

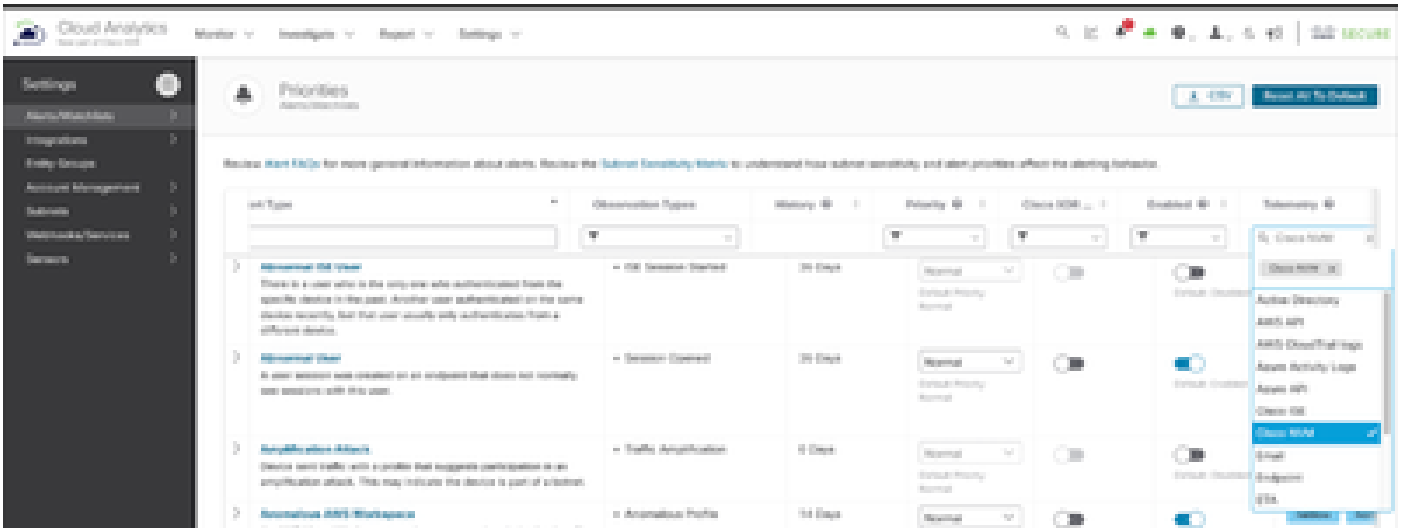
Beobachtungen und Warnungen

NVM-Warnungen

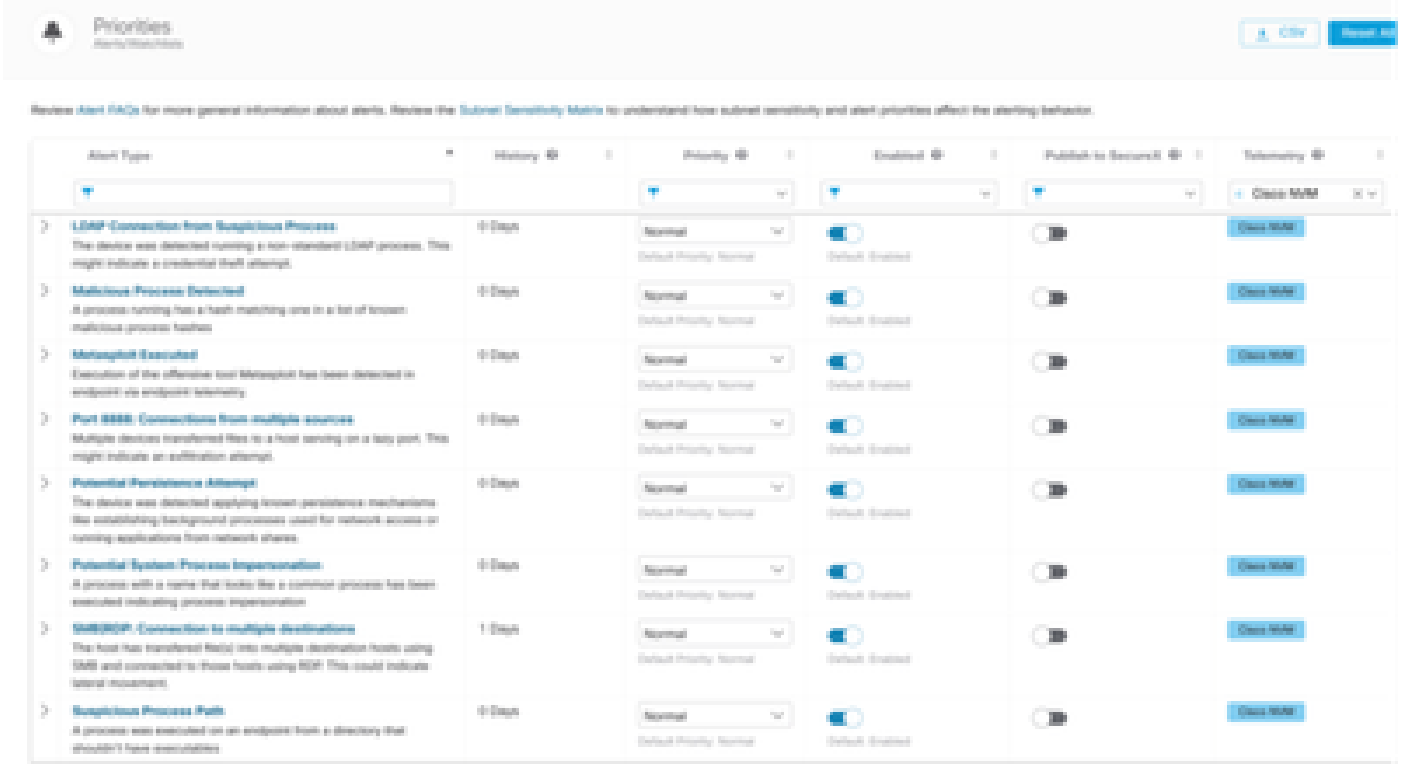
- Anmeldung beim XDR Analytics-Portal
- Einstellungen > WarnmeldungenTelemetrie > Cisco NVM

- Telemetrie > Cisco NVM



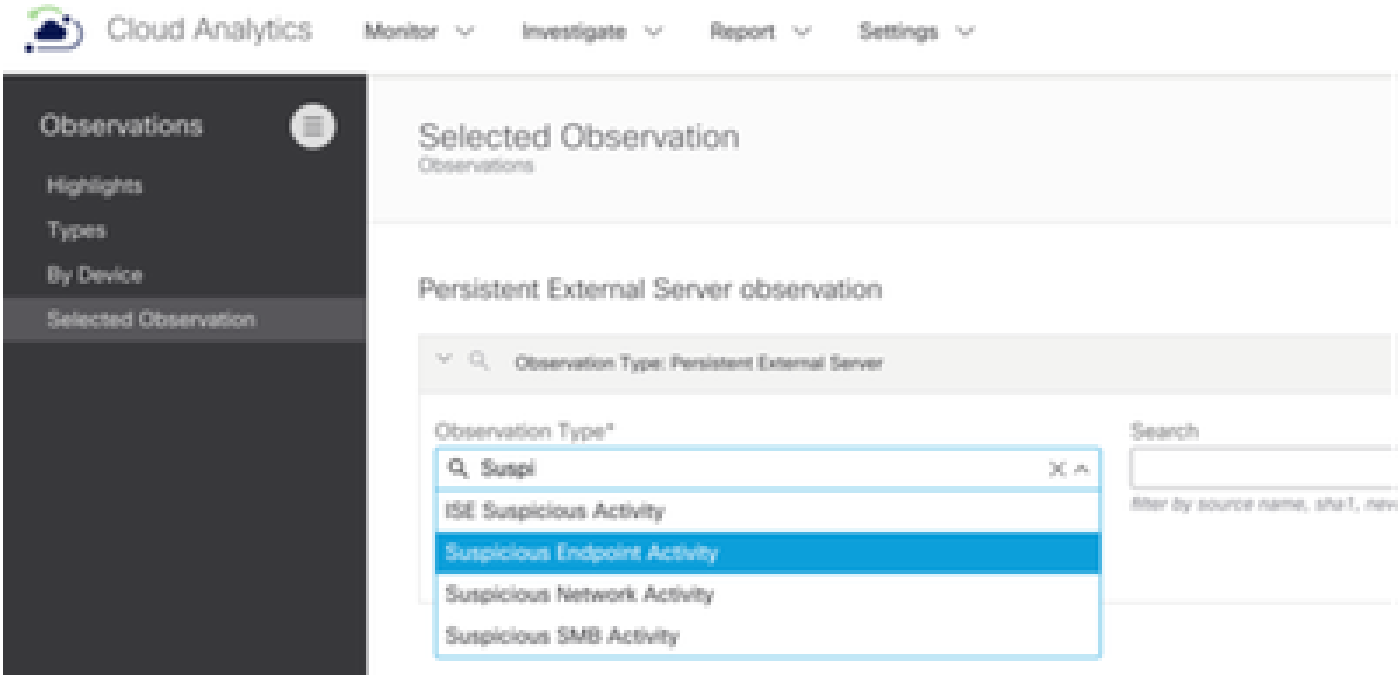


NVM-Warnmeldungseinstellungen



NVM-Beobachtungen

- Verdächtige Endpunktaktivität
- XDR Analytics-Portal
- Überwachen > Beobachtungen
- Ausgewählte Beobachtung
- Filtern verdächtiger Endpunktaktivitäten



Hinweise zur NVM-Erkennung

- NVM erfasst nur Prozesse und Flow-Daten, mit denen eine Netzwerkverbindung besteht.
- NVM ist so konfiguriert, dass Flow-Daten standardmäßig nur am Ende des Flow gemeldet werden

Schlussfolgerung

Diese Schritte helfen Ihnen, durch XDR-Analysen zu navigieren, um Beobachtungen und Warnungen mithilfe von NVM-Informationen zu aktivieren und den Workflow zu beheben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.