Dépannage et activation de NVM pour XDR Analytics

Table des matières

- Introduction
  - Conditions préalables
    - Exigences
    - Composants utilisés
  - Flux NVM XDR Analytics
    - Flux de données NVM - XDR Analytics
    - État du capteur NVM
    - ID d'organisation NVM
    - État du provisionnement NVM Data Lake
    - Débogage
  - Observations et alertes
    - Alertes NVM
    - Paramètres d'alerte NVM
    - Observations NVM
    - Avertissements relatifs à la détection NVM
  - Conclusion

Introduction

Ce document décrit comment dépanner Cisco XDR Analytics pour Cisco XDR (Extended Detection and Response) / NVM (Network Visibility Module)

Conditions préalables

Portail Active XDR Analytics avec intégration XDR

Exigences

Exécution d'un compte XDR Analytics avec intégration XDR unique

Composants utilisés

- Analyses XDR
- XDR
- Capteur NVM
- Client sécurisé (version 5.0+)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

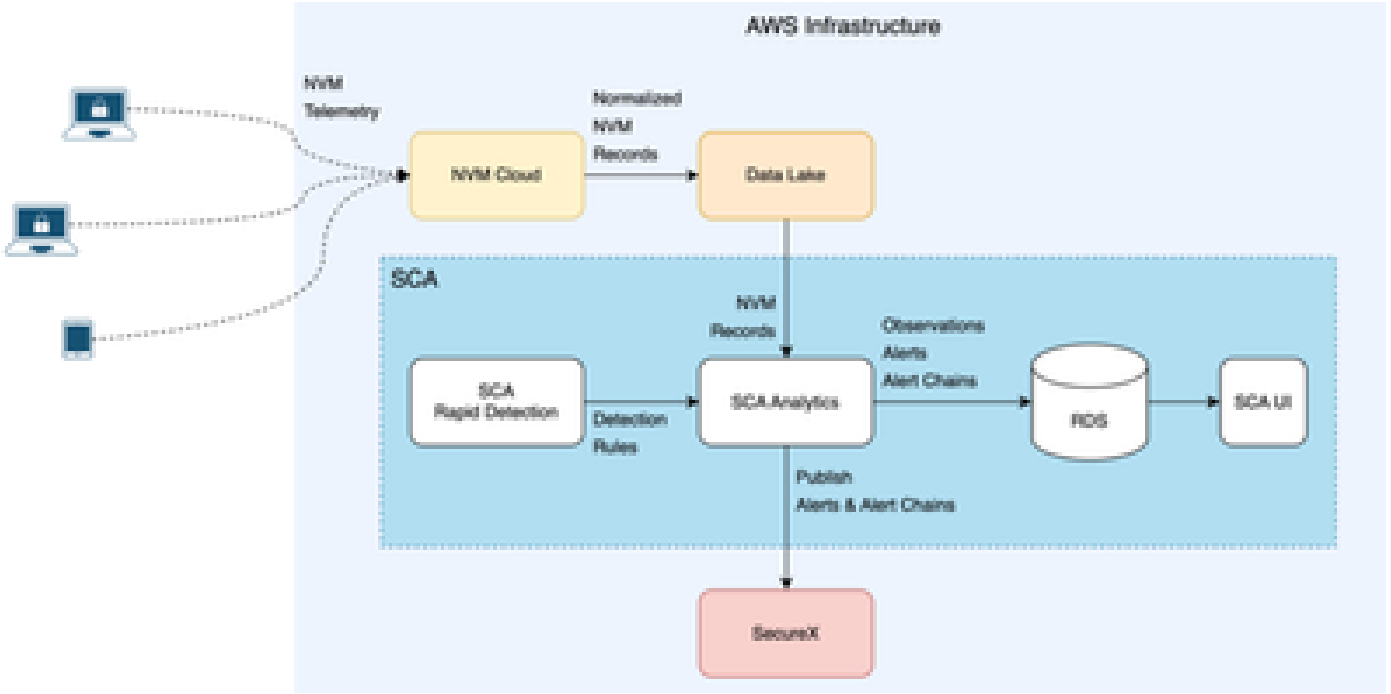
Flux NVM XDR Analytics

XDR Analytics utilise désormais la télémétrie NVM
La télémétrie est générée par le composant NVM dans Cisco Secure Client.

NVM offre une meilleure visibilité sur le réseau, notamment sur les comportements des utilisateurs, les communications réseau et les processus, réduisant ainsi le temps d'investigation des incidents et comblant les lacunes en matière de visibilité sur les terminaux

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

Flux de données NVM - XDR Analytics



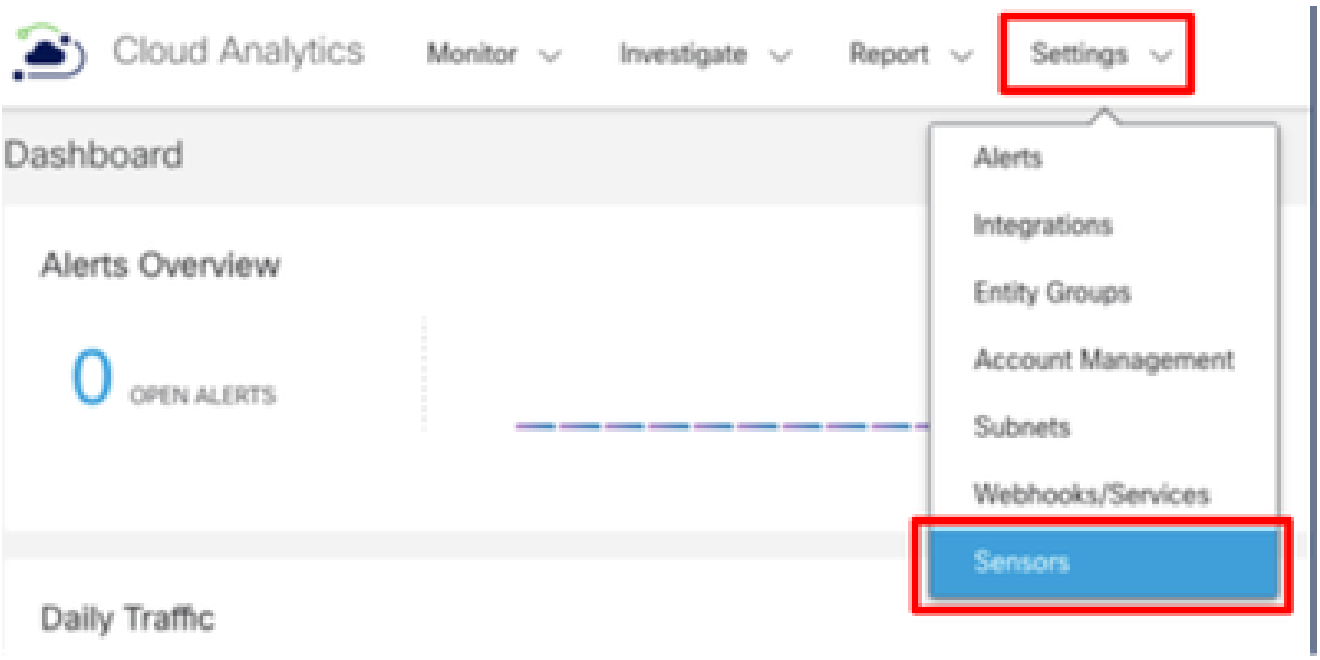
- Nous vous recommandons de toujours rester à jour avec vos versions Secure Client. Ce workflow nécessite que vous utilisiez Secure Client version 5.0 ou ultérieure : https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Mettre à jour la version Secure Client et Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud gère le volume de télémétrie et le rend disponible pour l'acquisition de données. Data Lake l'acquiert et le normalise pour un stockage efficace
- XDR Analytics traite les enregistrements NVM à intervalles réguliers (10 minutes) pour

générer des détections - Observations et alertes

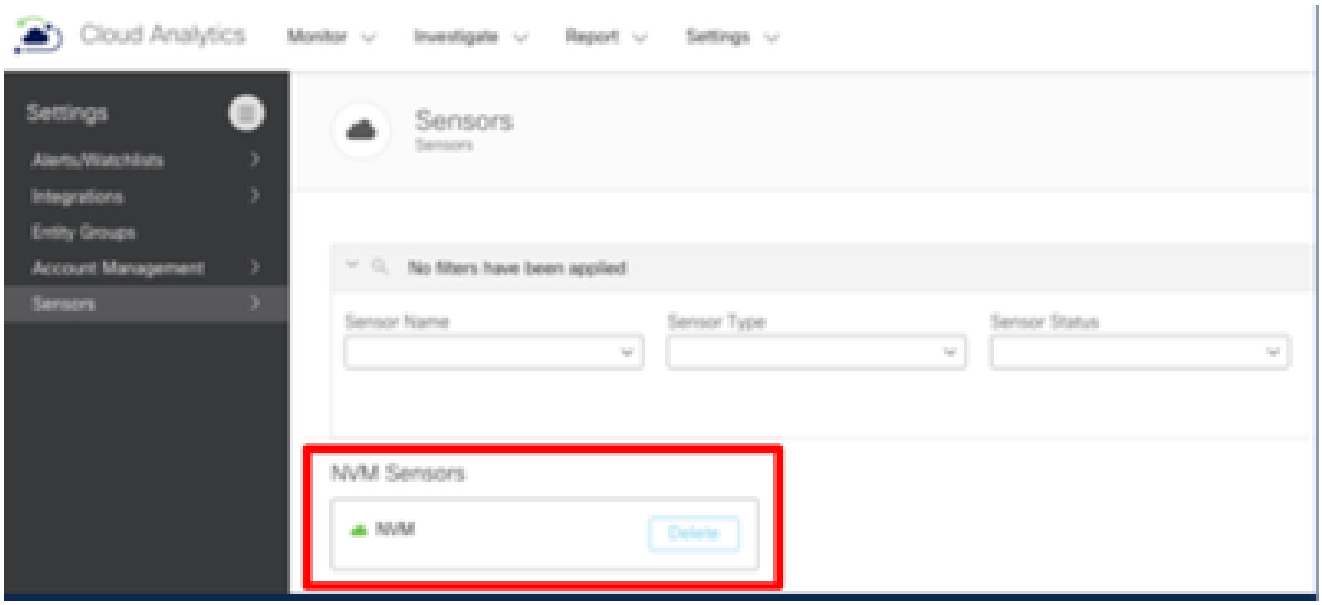
- Les détections rapides permettent d'ajouter rapidement des observations et des alertes simples à l'aide des configurations
- XDR Analytics met en corrélation les alertes avec les chaînes d'attaque (anciennement Chaînes d'alerte)
- L'utilisateur peut publier des chaînes d'alerte et d'attaque sur XDR.

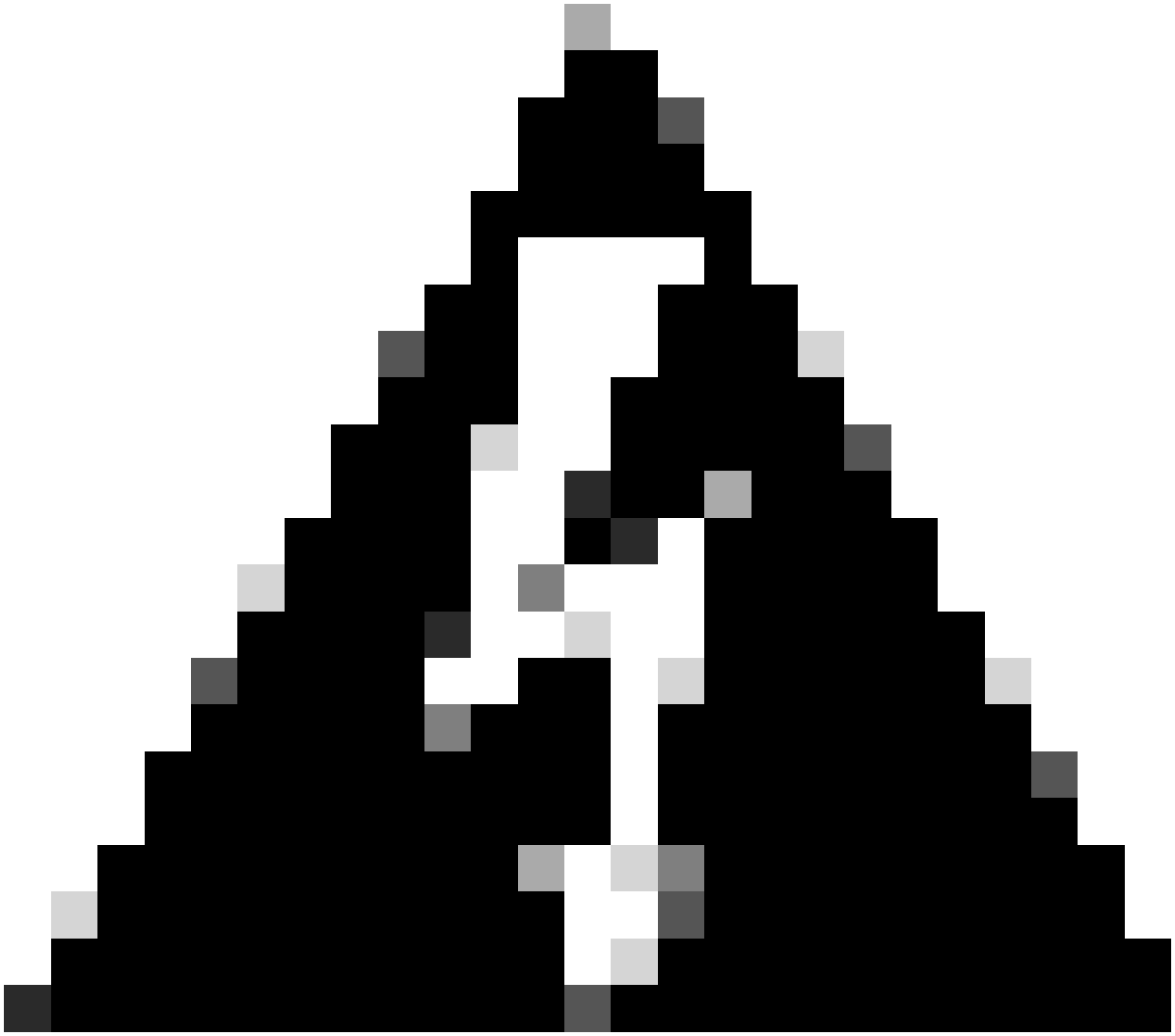
État du capteur NVM

- Vérification de la création du capteur NVM :- Dans le tableau de bord XDR Analytics, accédez à settings > Sensors



- Vérifiez ensuite que le capteur NVM est disponible dans la liste des capteurs





Avertissement : Le portail XDR Analytics doit être associé à un seul locataire/organisation XDR au maximum.

ID d'organisation NVM

- Vérifiez que les clients NVM ont le même ID d'organisation que celui affiché dans le point de terminaison API :
  https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/



État du provisionnement NVM Data Lake

- Points de terminaison API pour garantir l'intégration correcte du lac de données, l'association peut être confirmée à l'aide de ce point de terminaison API :https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/



- Tous les utilisateurs autorisés à accéder au portail peuvent accéder à ces terminaux (administrateurs du portail, TAC, ingénierie)

Débogage

- Codes de réponse de débogage :

Code réponse	Mesure à prendre
DataLake provisionné avec succès	Valider les flux NVM via l'Observateur d'événements
Impossible de mettre en service le lac de données, aucune organisation XDR détectée	Utilisez l'intégration XDR en un clic pour connecter XDR et XDR Analytics
Impossible de mettre en service le DataAlake, plusieurs organisations XDR détectées	Contactez le TAC pour obtenir de l'aide

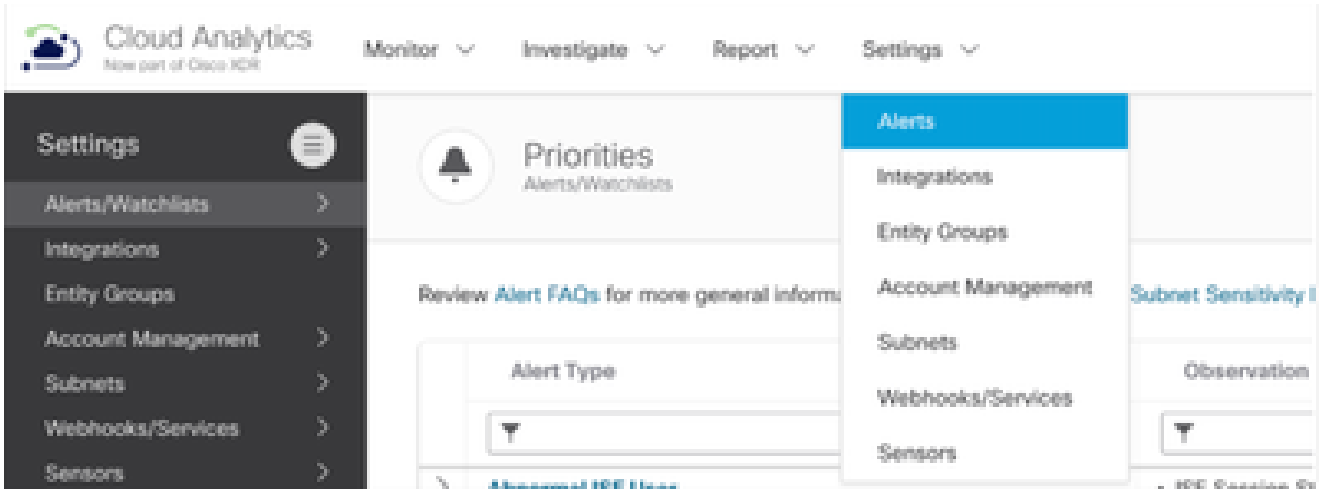
- Si l'une de ces étapes échoue, exécutez l'outil Secure Client Diagnostics And Reporting Tool (DART) à partir de l'interface Secure Client pour diagnostiquer le problème (demandez toujours à ce que DART soit exécuté en tant qu'administrateur)
  Collecter l'offre groupée DART pour client sécurisé

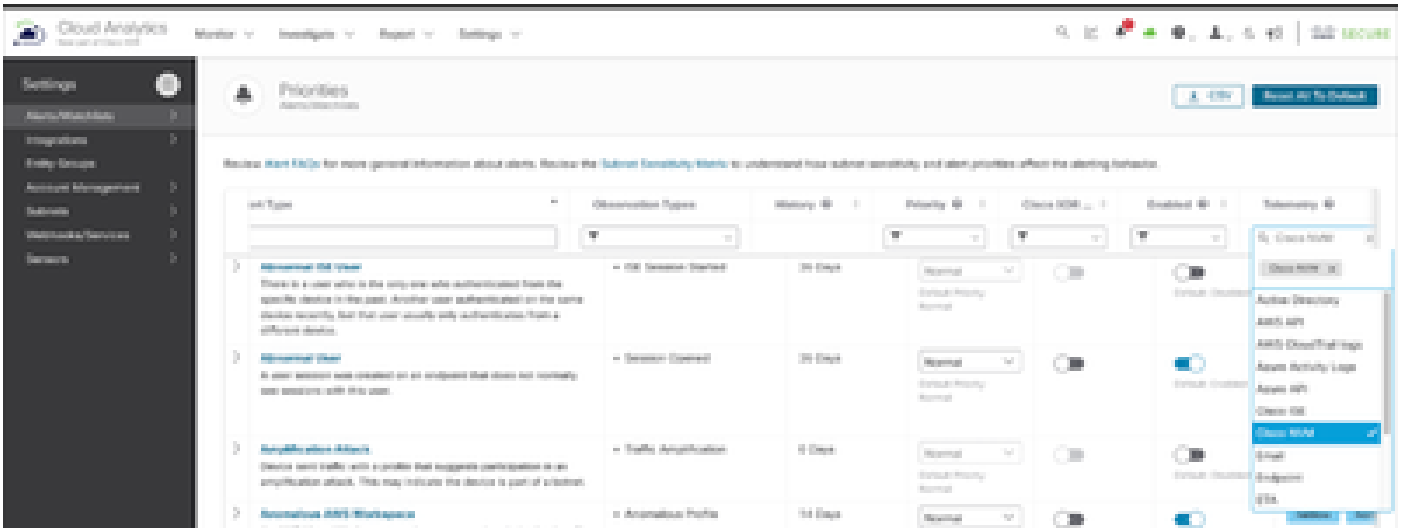
Observations et alertes

Alertes NVM

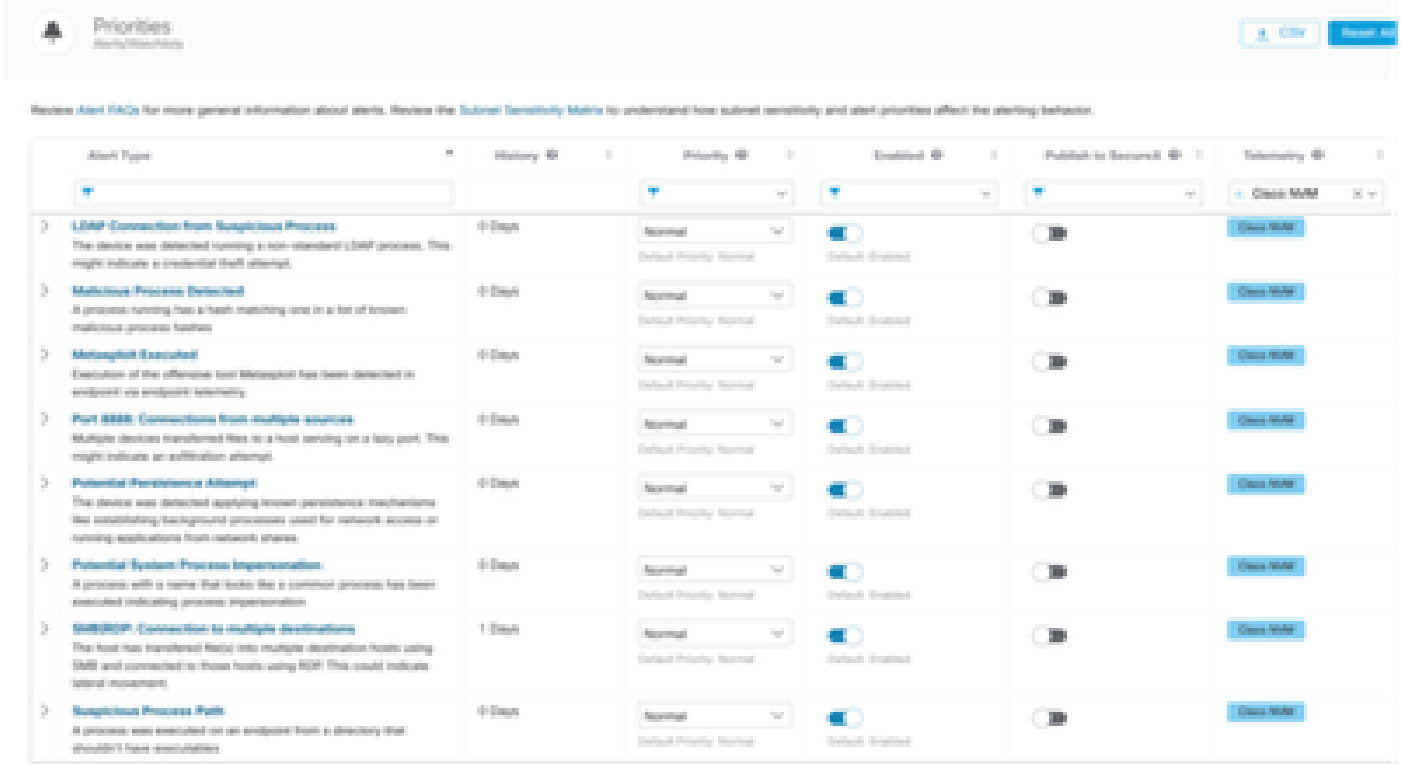
- Connexion au portail XDR Analytics
- Paramètres > AlertesTélémétrie > Cisco NVM

- Télémétrie > Cisco NVM



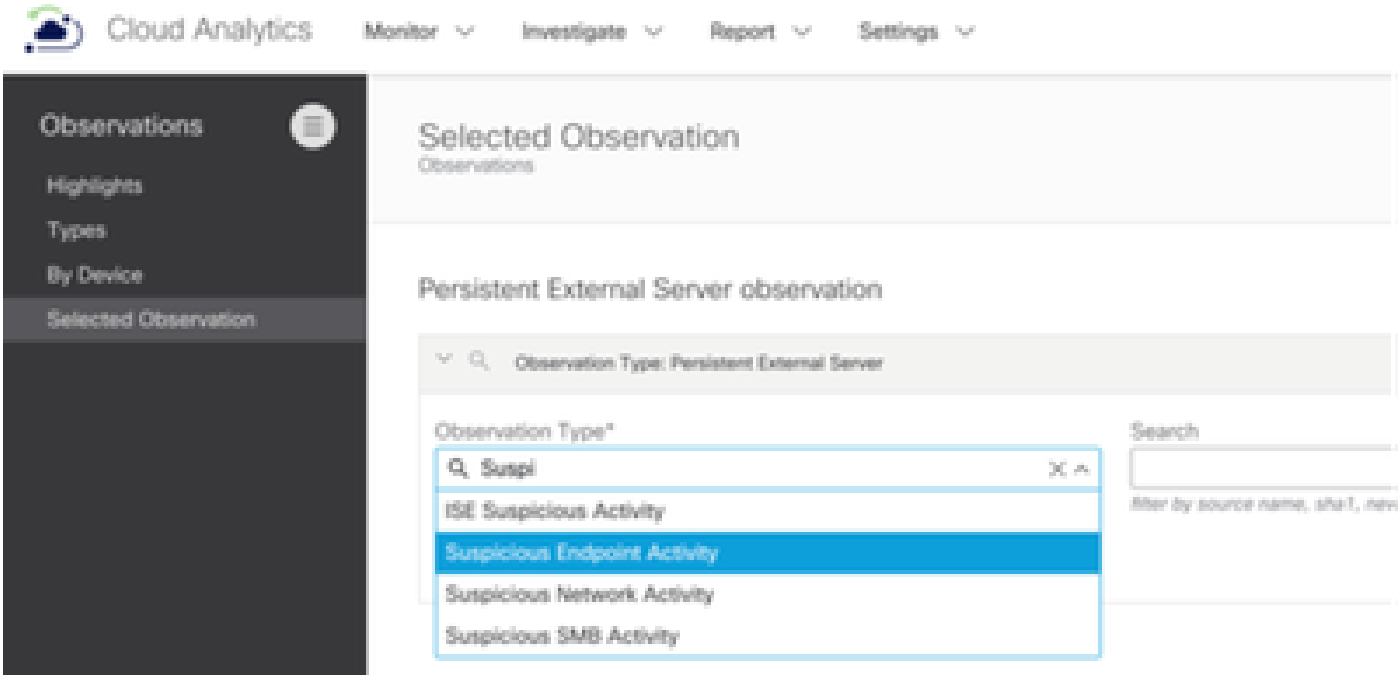


Paramètres d'alerte NVM



Observations NVM

- Activité sur les terminaux suspects
- Portail XDR Analytics
- Surveillance > Observations
- Observation sélectionnée
- Filtrer les activités suspectes sur les terminaux



Avertissements relatifs à la détection NVM

- NVM capture uniquement les processus et les données de flux associés à une connexion réseau
- NVM est configuré par défaut pour rapporter les données de flux uniquement à la fin du flux

Conclusion

Ces étapes vous aident à naviguer dans XDR Analytics pour activer les observations et les alertes à l'aide des informations NVM et du dépannage du workflow.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.