Solución de problemas y habilitación de NVM para análisis XDR

Contenido

Introducción

Este documento describe cómo resolver problemas de Cisco XDR Analytics para Cisco eXtended Detection and Response (XDR) / Network Visibility Module (NVM)

Prerequisites

Portal de análisis XDR activo con integración XDR

Requirements

Cuenta de XDR Analytics con integración única de XDR

Componentes Utilizados

- Análisis XDR
- XDR
- Sensor NVM
- Secure Client (Versión 5.0+)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

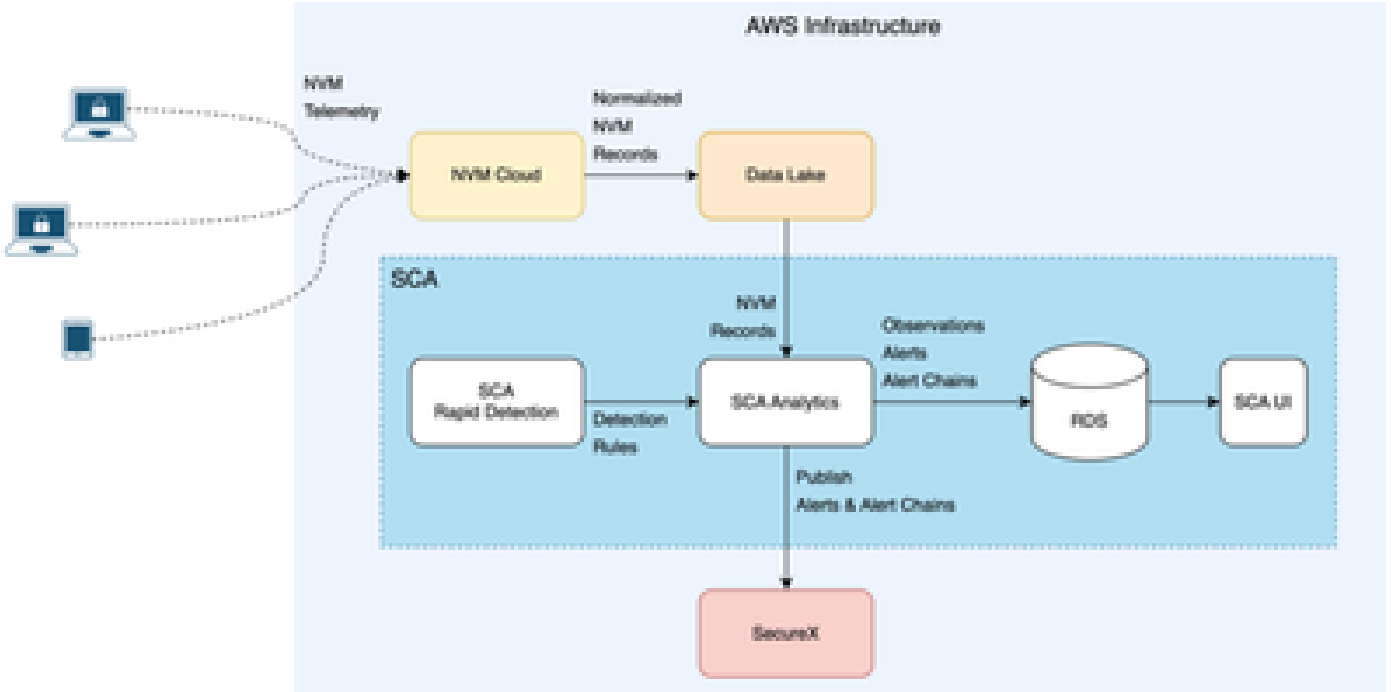
XDR Analytics Flujos de NVM

XDR Analytics utiliza ahora telemetría NVM
La telemetría la genera el componente NVM en Cisco Secure Client.

Los NVM proporcionan una mayor visibilidad de la red, incluidos los comportamientos de los usuarios, las comunicaciones de red y los procesos, lo que reduce el tiempo de investigación de incidentes y llena las lagunas en la visibilidad de los terminales

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

Flujos de datos de NVM - XDR Analytics

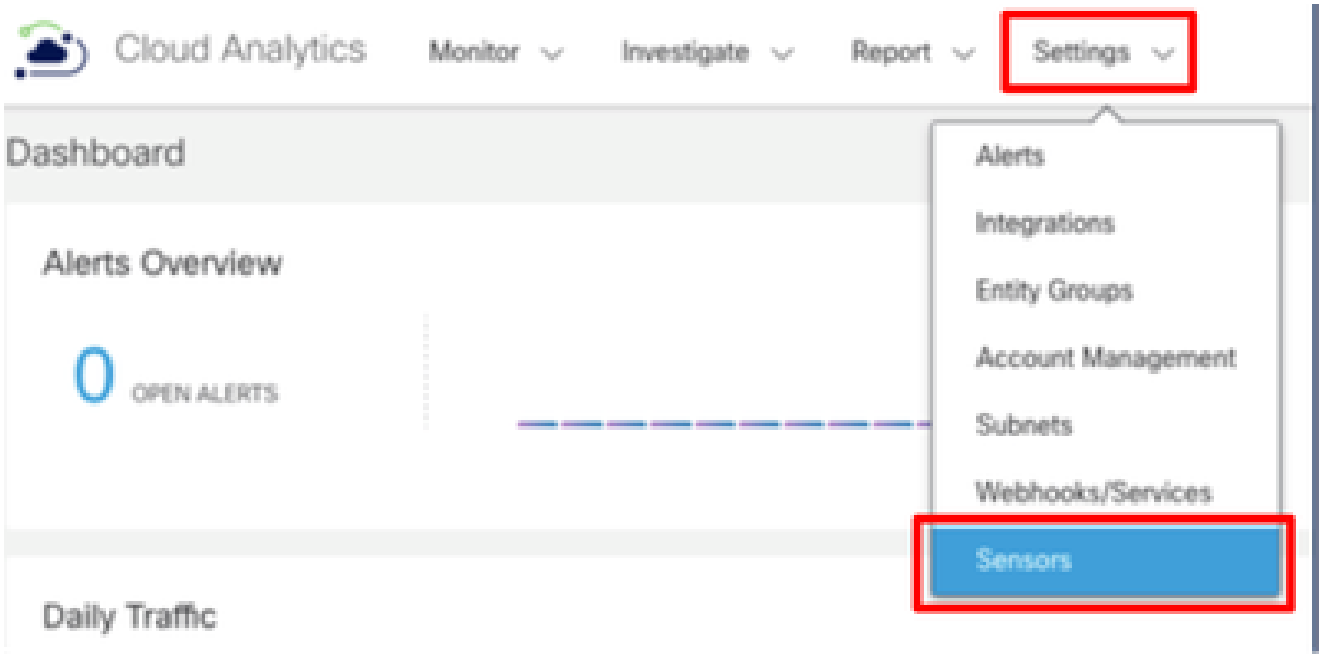


- Siempre recomendamos mantenerse al día con sus versiones de Secure Client, este flujo de trabajo requiere que utilice Secure Client versión 5.0 o posterior : https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Mantener una actualización actualizada de Secure Client versión e Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud gestiona el volumen de telemetría y lo pone a disposición de la ingesta Data Lake ingiere la telemetría y la normaliza para un almacenamiento eficiente

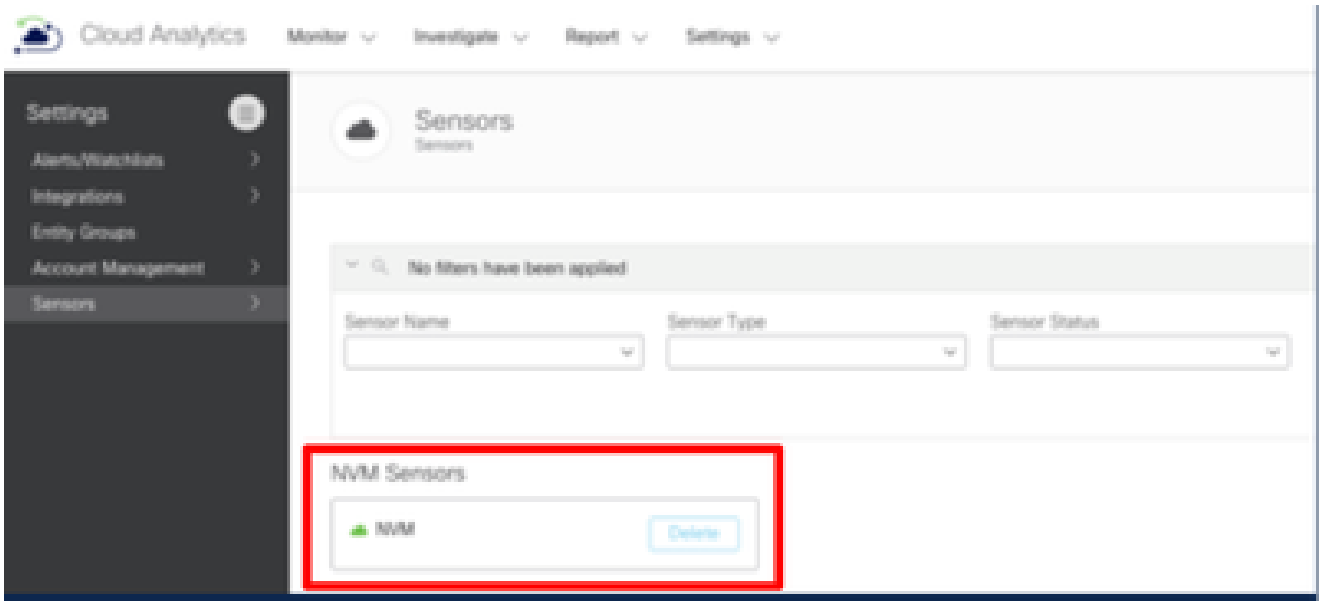
- XDR Analytics procesa registros NVM a intervalos regulares (10 minutos) para generar detecciones - Observations & Alerts
- Las detecciones rápidas ayudan a agregar rápidamente observaciones y alertas sencillas mediante configuraciones
- El análisis XDR correlaciona las alertas con las cadenas de ataque (anteriormente, cadenas de alerta)
- El usuario puede publicar cadenas de alertas y ataques en XDR.

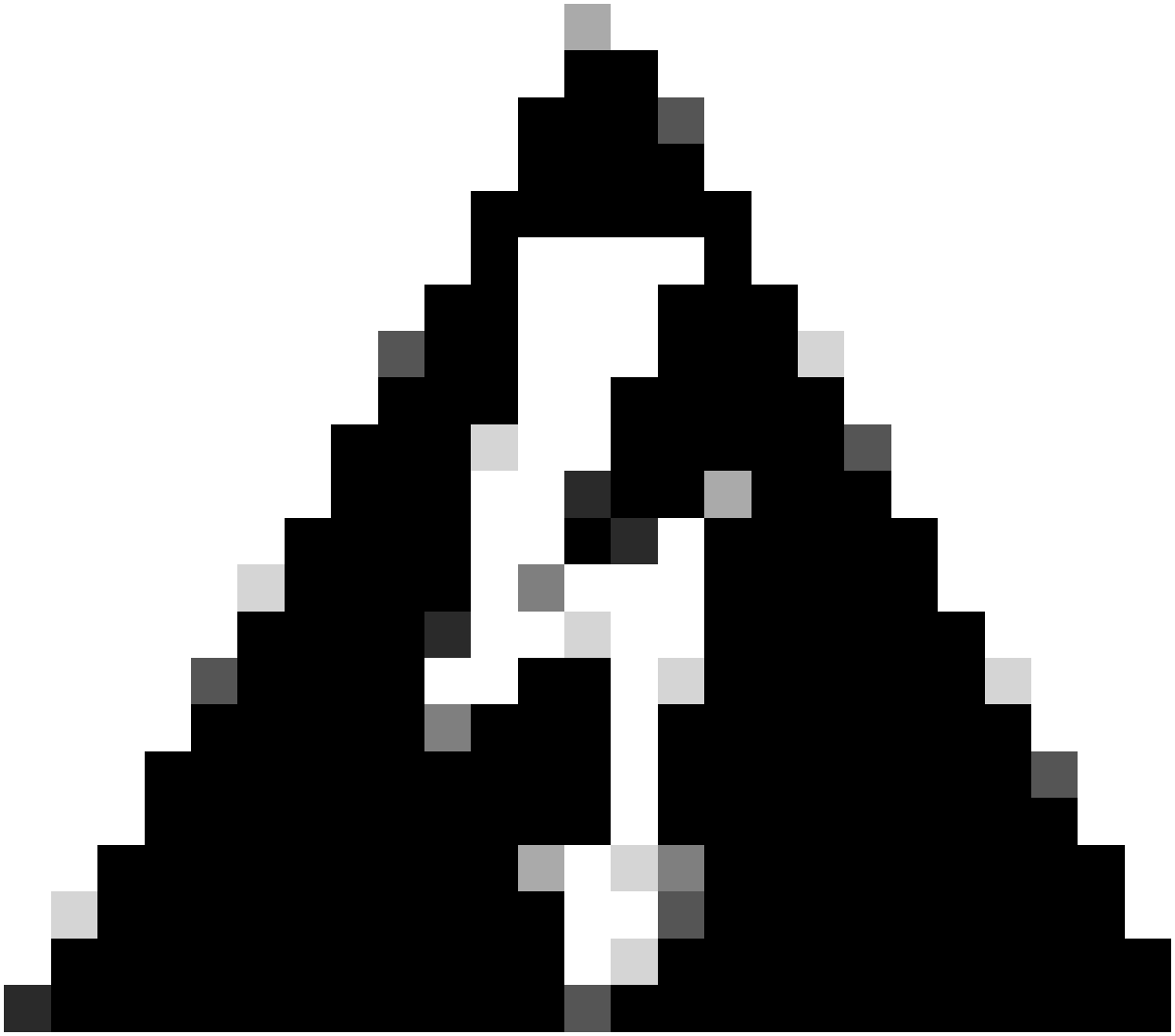
Estado del sensor NVM

- Cómo garantizar la creación del sensor NVM: En el panel de análisis de XDR, acceda a Ajustes > Sensores



- A continuación, confirme que el sensor NVM está disponible en la lista de sensores





Advertencia: El portal de análisis XDR debe tener como máximo un único arrendatario/organización XDR asociado.

ID de organización de NVM

- Confirme que los clientes NVM tengan el mismo ID de organización que se muestra en el terminal API : https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/

Estado del aprovisionamiento de NVM Data Lake

- Los terminales de la API para garantizar que el lago de datos se incorpora correctamente, la asociación se puede confirmar mediante este terminal de la API:https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/

- Todos los usuarios a los que se concede acceso a través del portal pueden acceder a estos terminales (administradores del portal, TAC, ingeniería)

Depuración

- Depuración de códigos de respuesta:

Código de respuesta	Acción requerida
DataLake aprovisionado correctamente	Validar flujos de NVM a través del visor de eventos
No se puede aprovisionar el lago de datos, no se ha detectado ninguna organización XDR	Utilice la integración XDR one-click para conectar análisis XDR y XDR
No se puede aprovisionar el lago de datos, se han detectado varias organizaciones XDR	Comuníquese con el TAC para obtener asistencia

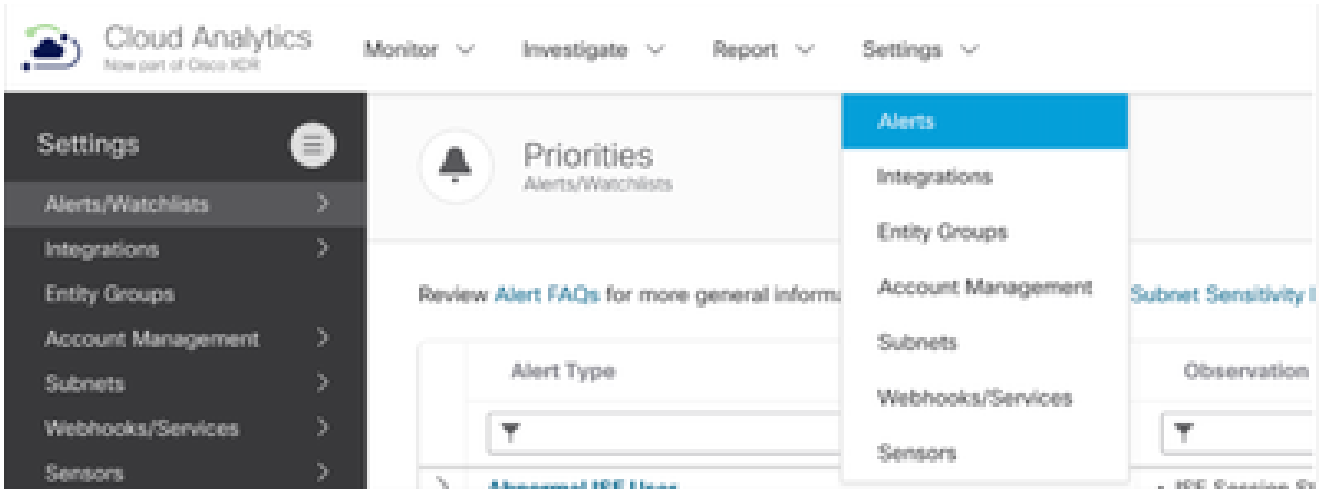
- Si cualquiera de estos pasos falla, ejecute la herramienta Secure Client Diagnostics And Reporting Tool (DART) desde la interfaz de Secure Client para diagnosticar el problema (solicite siempre que DART se ejecute como administrador) Recopile el paquete DART para Secure Client

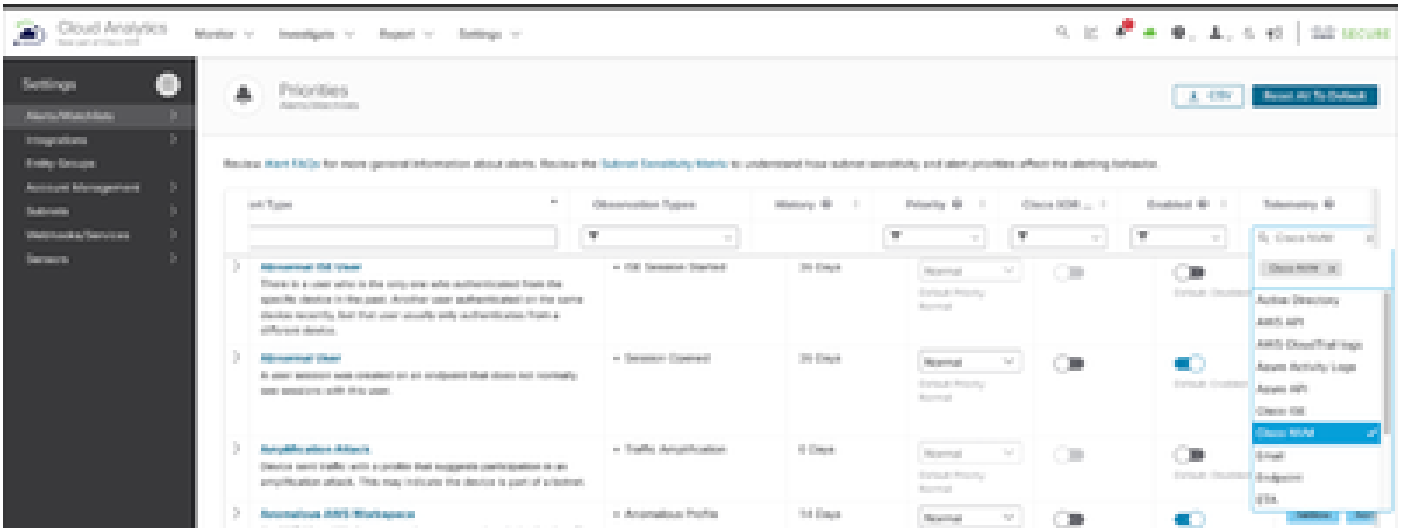
Observaciones y alertas

Alertas de NVM

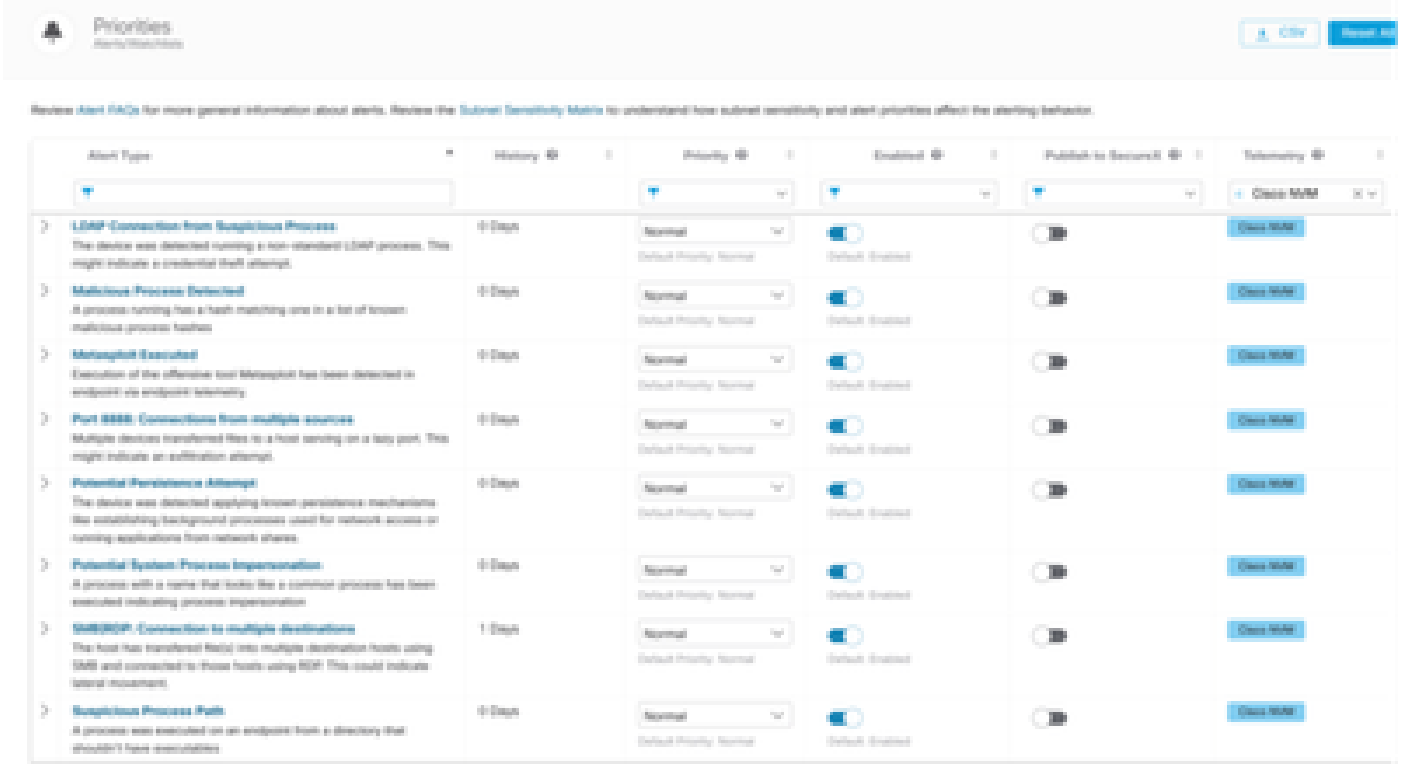
- Iniciar sesión en el portal de análisis XDR
- Configuración > AlertasTelemetría > Cisco NVM

- Telemetría > Cisco NVM



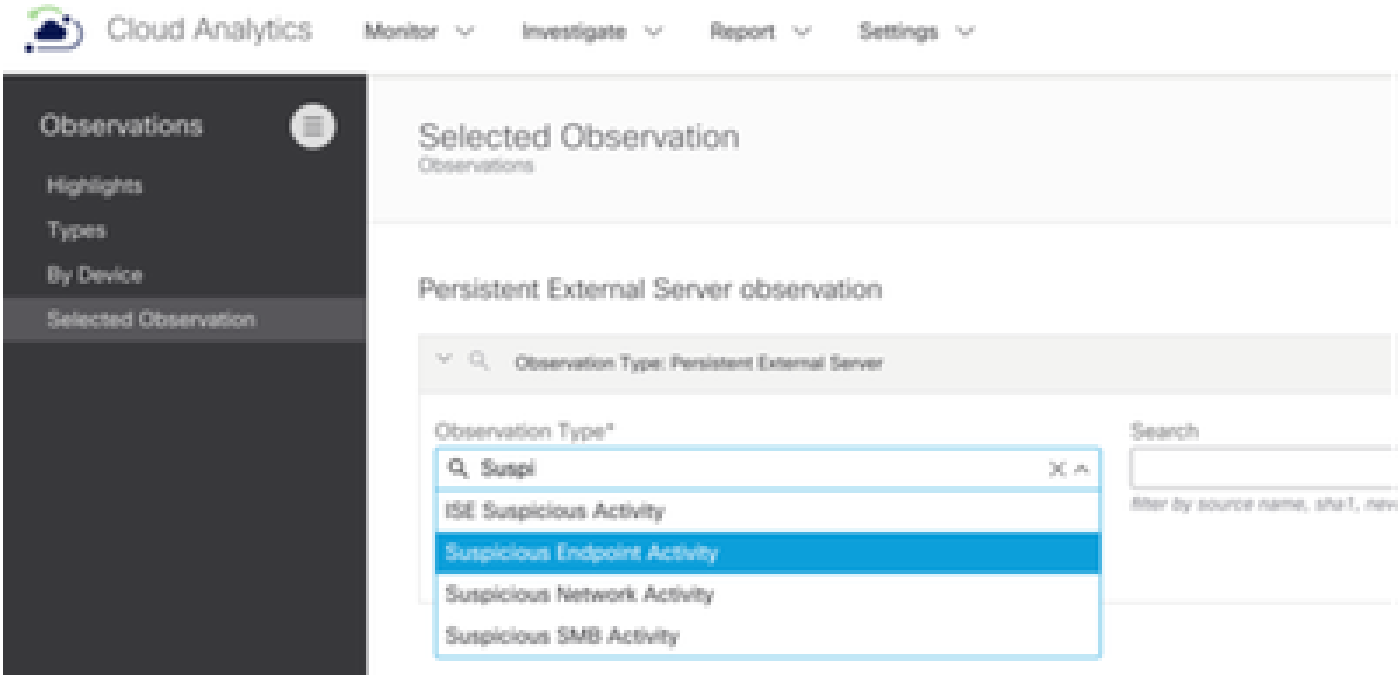


Configuración de alertas de NVM



Observaciones de NVM

- Actividad de terminal sospechosa
- Portal de análisis XDR
- Supervisar > Observaciones
- Observación seleccionada
- Filtrar actividad de terminales sospechosos



Advertencias de detección de NVM

- El NVM sólo captura procesos y flujos de datos que tienen una conexión de red asociada
- El sistema NVM está configurado de forma predeterminada para informar de flujos de datos sólo al final del flujo

Conclusión

Estos pasos le ayudarán a navegar por XDR Analytics para habilitar las observaciones y alertas con información de NVM y solucionar problemas del flujo de trabajo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).