Troubleshoot and Enable NVM for XDR Analytics

Contents

Introduction

This document describes how to troubleshoot Cisco XDR Analytics for Cisco eXtended Detection and Response (XDR) / Network Visibility Module (NVM)

Prerequisites

Active XDR Analytics portal with XDR integration

Requirements

Running XDR Analytics account with single XDR integration

Components Used

- XDR Analytics
- XDR
- NVM Sensor
- Secure Client (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. If your network is live, ensure that you understand the potential impact of any command.

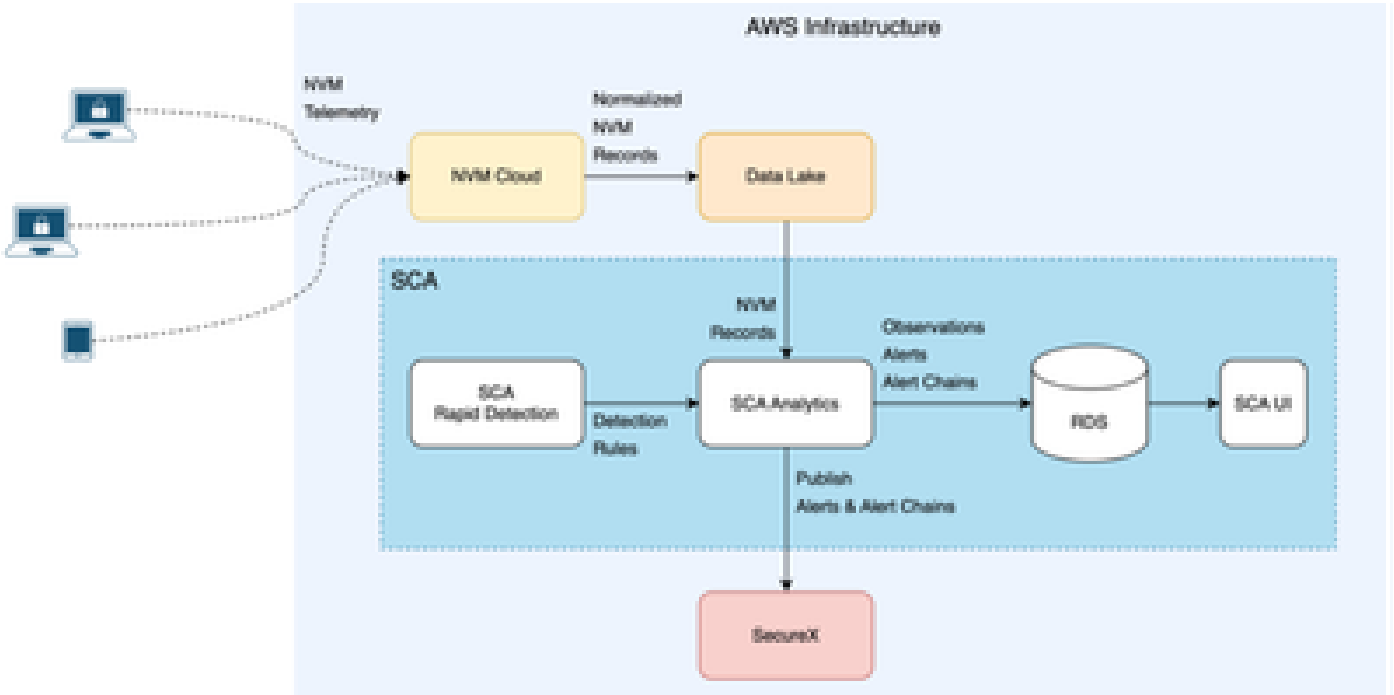
XDR Analytics NVM flows

XDR Analytics now consumes NVM telemetry
The telemetry is generated by the NVM component in Cisco Secure Client.

NVM provide enhanced network visibility, including user behaviors, network communications, and processes, thereby reducing incident investigation time and filling gaps in endpoint visibility

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

NVM data flows – XDR Analytics



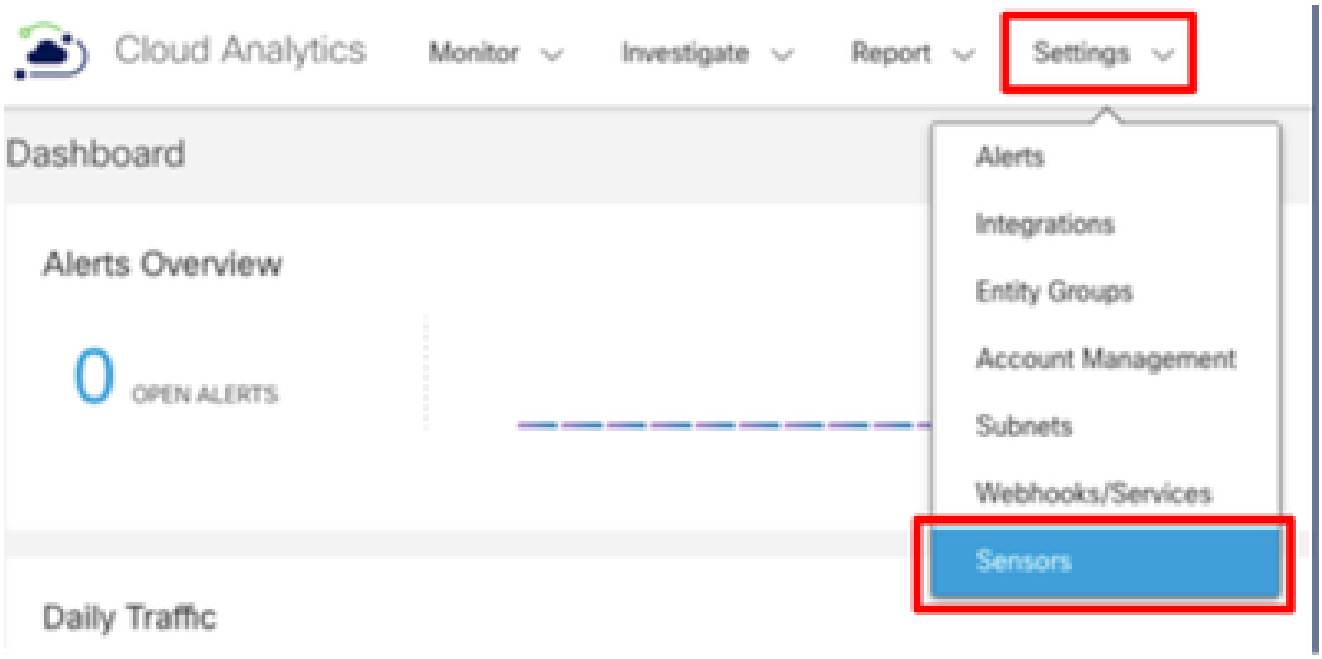
- We always recommend staying up to date with your Secure Client versions, this workflow requires you to use Secure Client version 5.0 or later : https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Maintain an update to date Secure Client version and Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud handles the telemetry volume and makes it available for ingest Data Lake ingests the telemetry and normalize it for efficient storage
- XDR Analytics processes NVM records at regular intervals (10 minutes) to generate detections - Observations & Alerts
- Rapid Detections help quickly add simple observations & alerts using configurations

- XDR Analytics correlates alerts into Attack Chains (formerly Alert Chains)

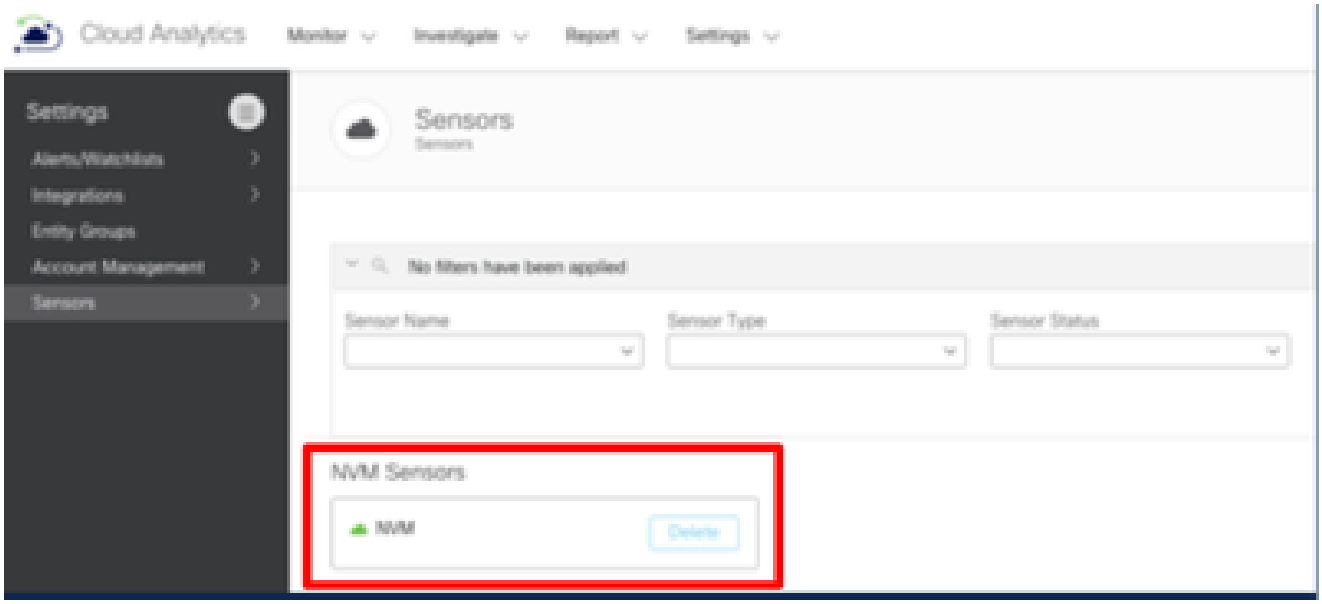
- User can publish Alert & Attack Chains to XDR

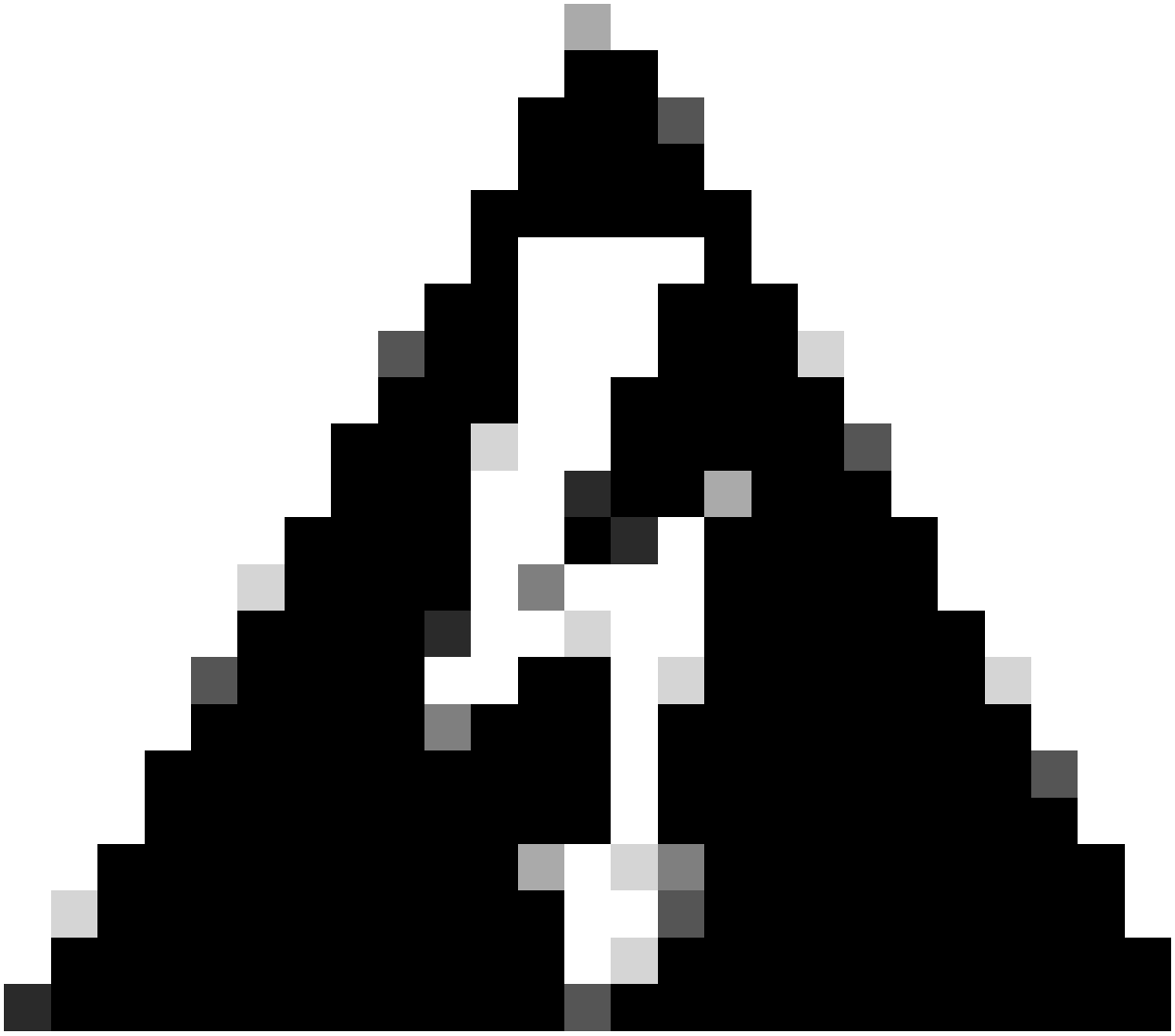
NVM Sensor Status

- Ensuring the NVM Sensor is created:- From the XDR Analytics Dashboard, navigate to settings > Sensors



- Then Confirm that the NVM sensor is available in the sensor list





Warning: XDR Analytics Portal must have at most a single XDR Tenant/Organization associated with it.

NVM Org ID

- Confirm that the NVM clients have the same org ID show in the API endpoint : https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/

NVM Data Lake Provisioning Status

- The API endpoints to ensure the data lake is onboarded properly, the association can confirmed using this API endpoint :*https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/*

- All users granted access through the portal can hit these endpoints (portal admins, TAC, Engineering)

Debugging

- Debugging response codes:

Response Code	Action Required
DataLake provisioned successfully	Validate NVM flows via Event Viewer
Unable to provision data lake, no XDR organization detected	Use the XDR one-click integration to connect XDR and XDR Analytics
Unable to provision datalake, Multiple XDR organizations detected	Contact TAC for Assistance

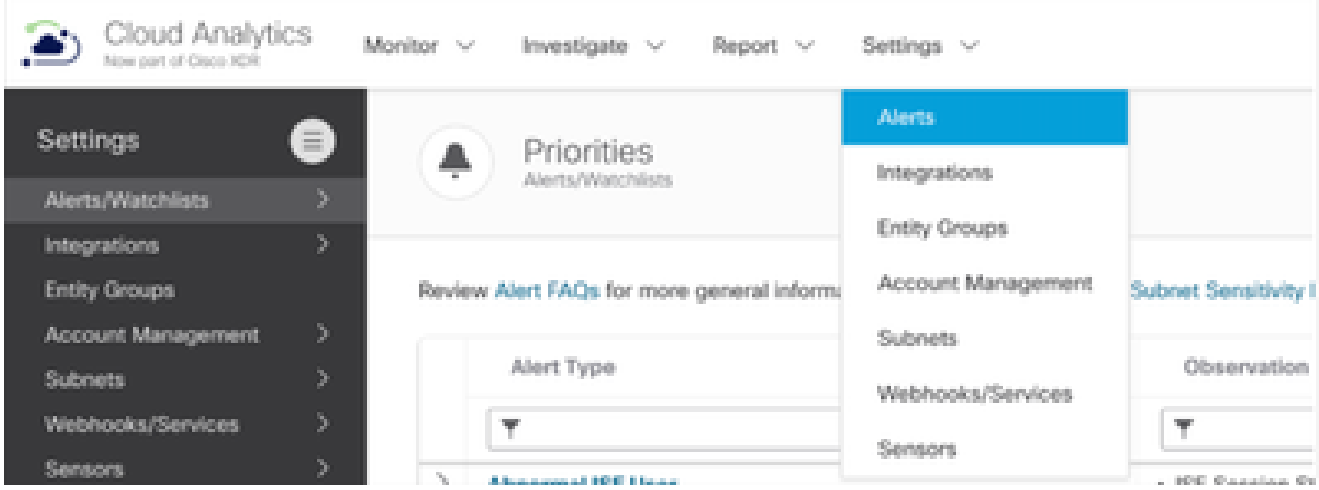
- If any of these steps fail, run the Secure Client Diagnostics And Reporting Tool (DART) from the Secure Client interface to diagnose the problem (Always request DART be run as administrator) [Collect DART Bundle for Secure Client]

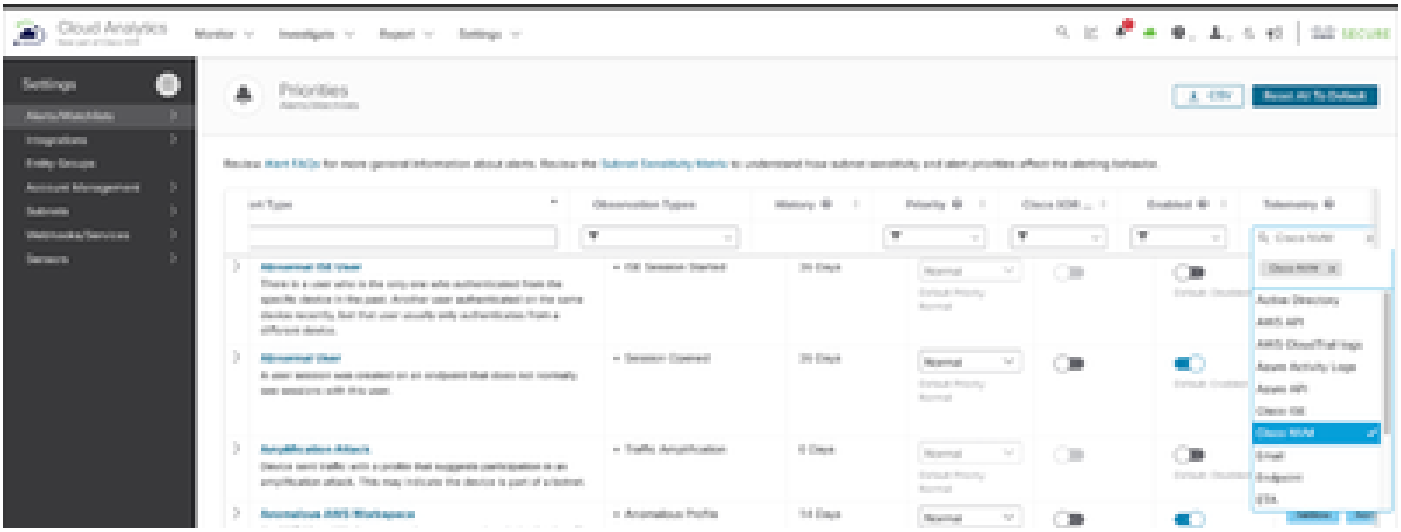
Observations & Alerts

NVM Alerts

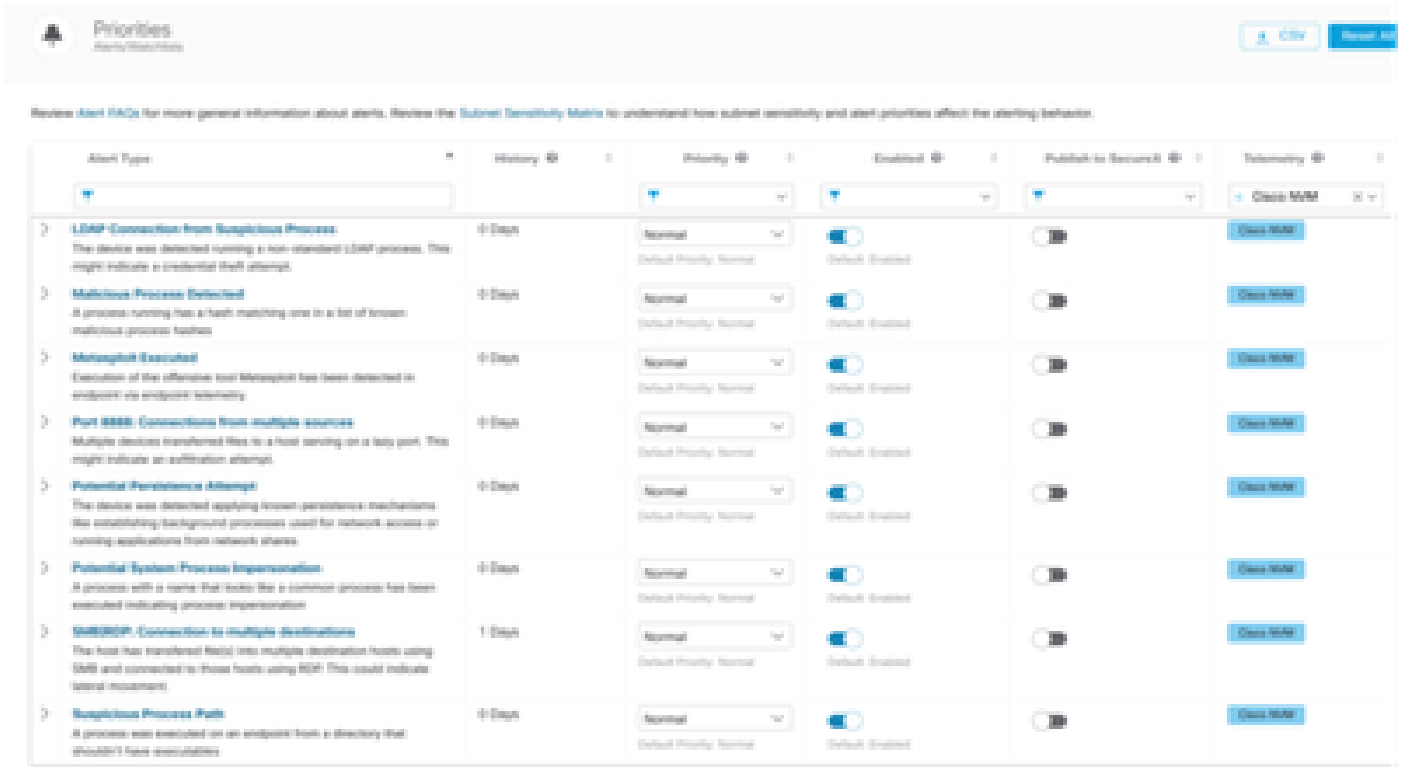
- Login to XDR Analytics portal
- Settings > AlertsTelemetry > Cisco NVM

- Telemetry > Cisco NVM



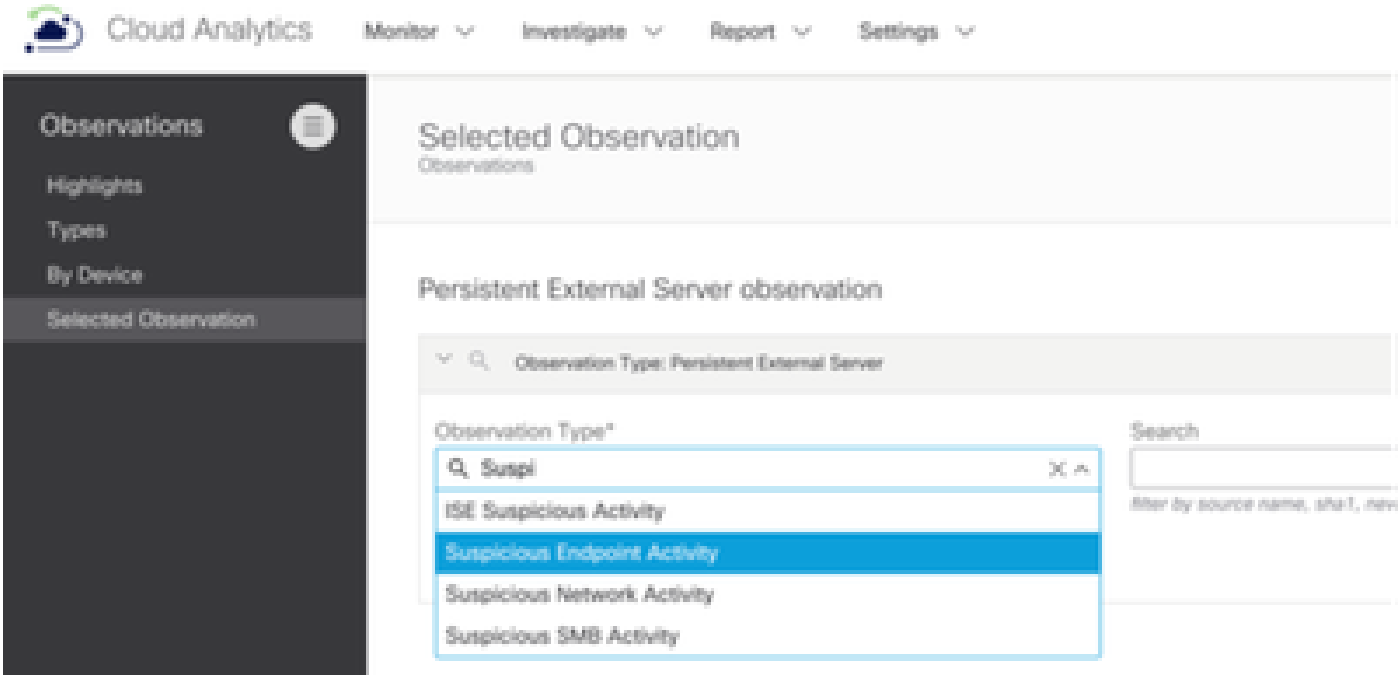


NVM Alert Settings



NVM Observations

– Suspicious Endpoint Activity
- XDR Analytics portal
- Monitor > Observations
- Selected Observation
- Filter Suspicious Endpoint Activity



NVM Detection Caveats

- NVM only captures processes & flow data that have an associated network connection
- NVM is configured to report flow data only at the end of flow by default

Conclusion

These steps help you navigating through XDR Analytics to enable Observations and Alerts using NVM information and troubleshooting the workflow.