為XDR分析排除故障並啟用NVM

目錄

簡介

本檔案介紹如何對思科延伸偵測和回應(XDR)/網路能見度模組(NVM)的Cisco XDR分析進行疑難排解

必要條件

具有XDR整合的活動XDR分析門戶

需求

運行具有單個XDR整合的XDR Analytics帳戶

採用元件

- XDR分析
- XDR
- NVM感測器
- 安全使用者端（5.0+版）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

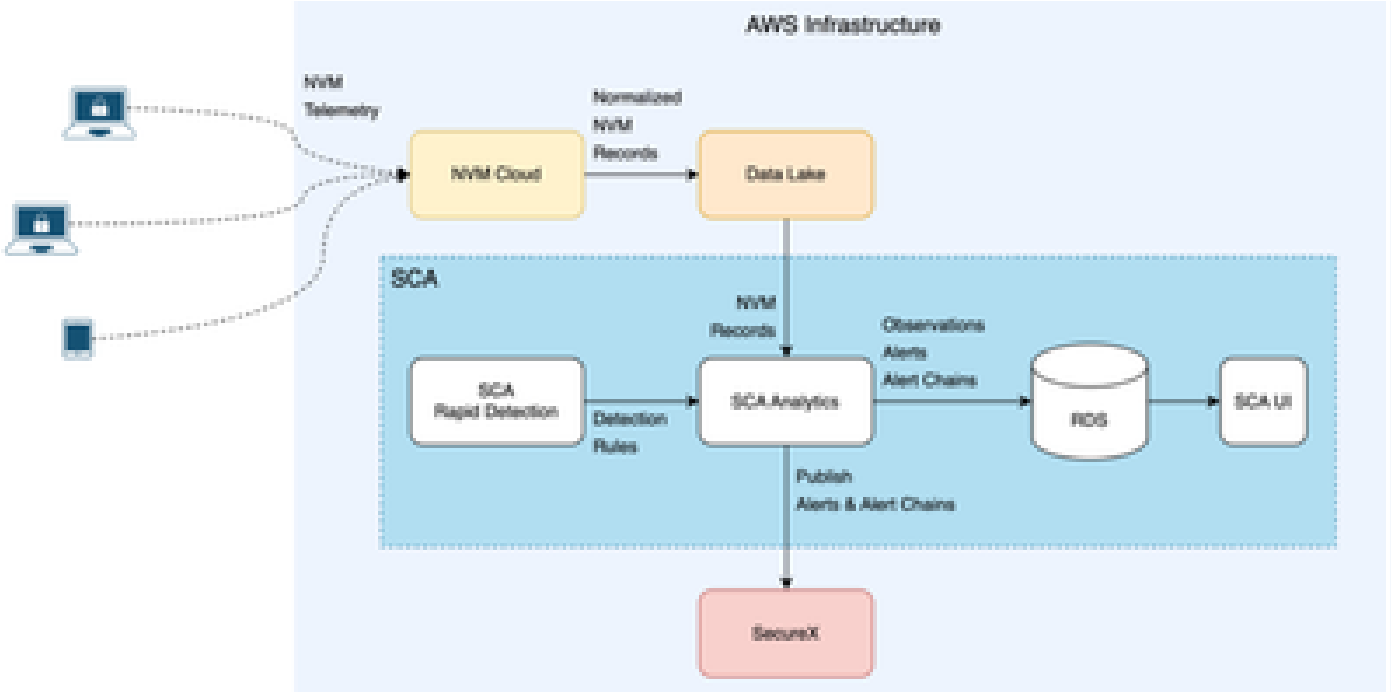
XDR分析NVM流

XDR分析現在使用NVM遙測
遙測由Cisco安全客戶端中的NVM元件生成。

NVM提供增強的網路可視性，包括使用者行為、網路通訊和流程，從而縮短事件調查時間，並填補終端可視性的空白

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

NVM資料流 — XDR分析



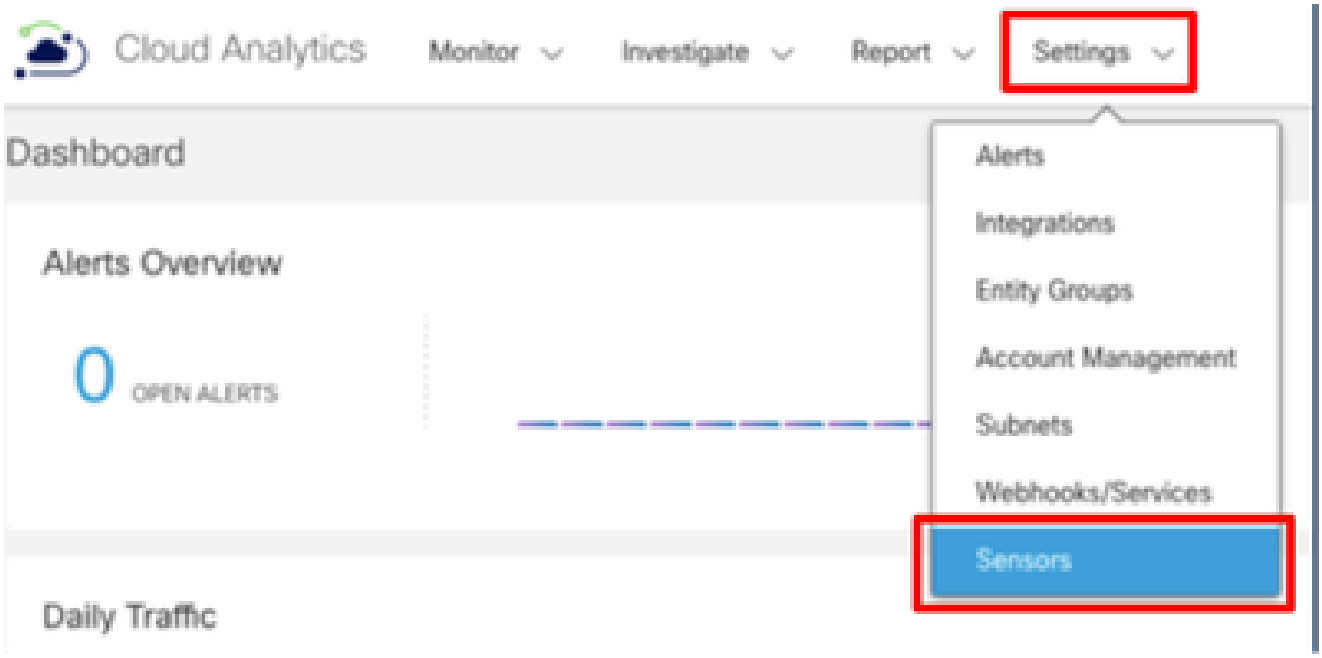
- 我們始終建議保持您的Secure Client版本的最新狀態，此工作流程要求您使用Secure Client 5.0版或更高版本
  ：https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- 維護最新的Secure Client版本和部署
  Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud處理遙測卷，並使其可用於接收資料湖接收遙測並對其進行規範化，以實現高效儲存
- XDR分析定期處理NVM記錄（10分鐘）以生成檢測 — 觀察和警報
- 快速檢測有助於使用配置快速新增簡單的觀察和警報

- XDR分析將警報關聯到攻擊鏈（以前稱為警報鏈）

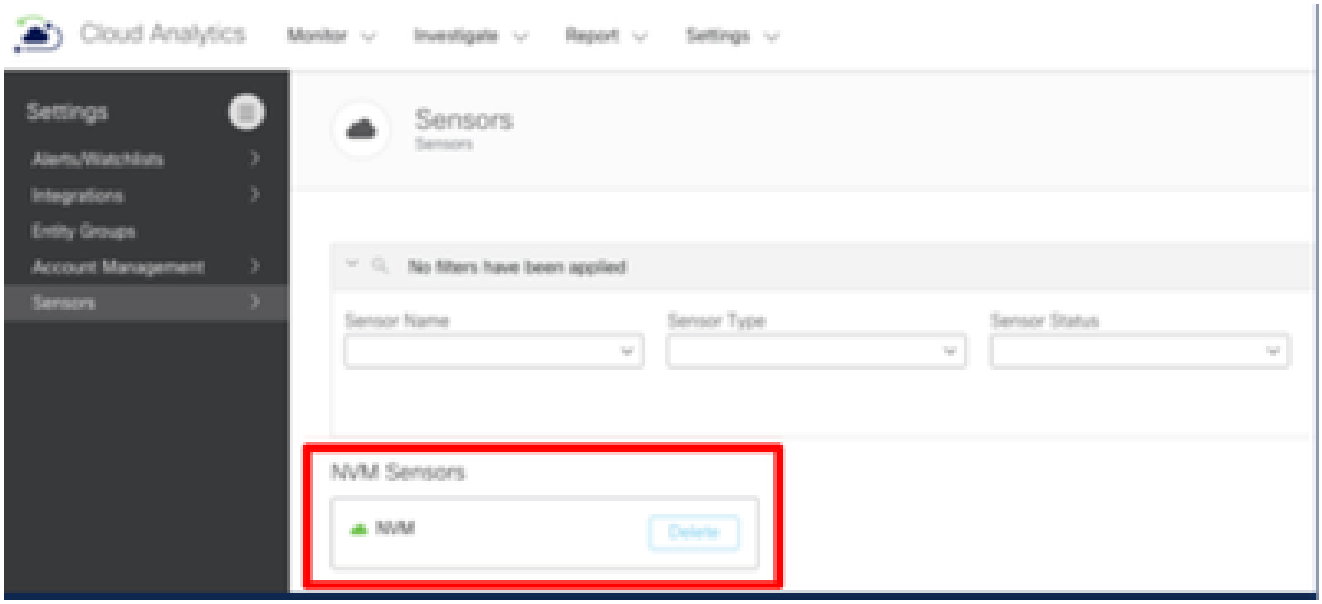
- 使用者可以向XDR發佈警報和攻擊鏈。

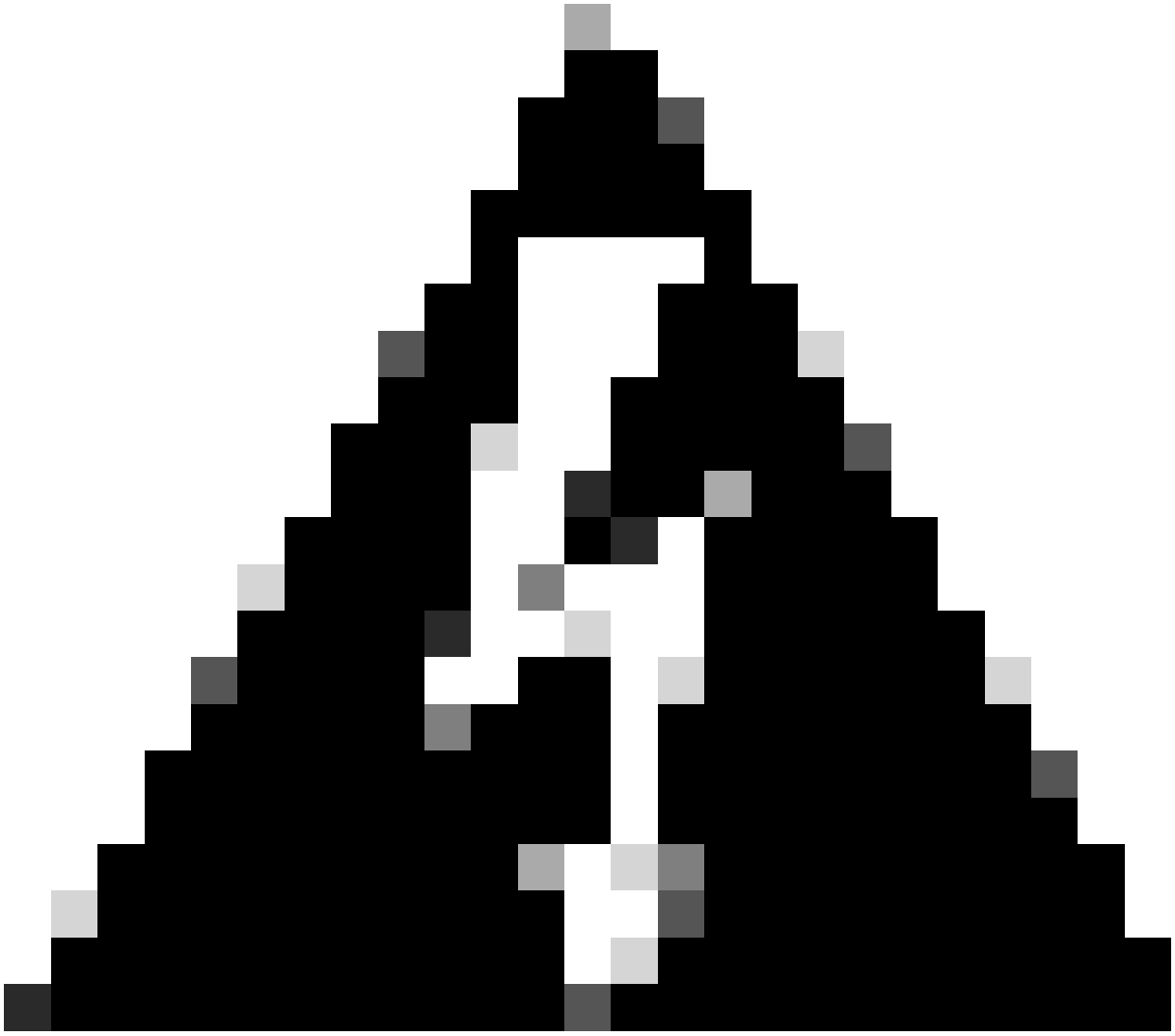
NVM感測器狀態

- 確保NVM感測器已建立： — 從XDR分析控制面板導航至「設定」>「感測器」



- 然後確認NVM感測器在感測器清單中可用





警告：XDR分析門戶最多必須有一個與其關聯的XDR租戶/組織。

NVM組織ID

- 確認NVM客戶端具有在API終結點中顯示的相同組織ID: https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/org/

NVM資料湖調配狀態

- API終結點為確保資料湖正確入網，可以使用此API終結點確認關聯：https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/

```
Pretty print
"Datalake provisioned successfully"
```

- 通過門戶獲得訪問許可權的所有使用者都可以訪問這些終端（門戶管理員、TAC、工程）

調試

- 調試響應代碼：

響應代碼	需採取的行動
已成功設定DataLake	通過事件檢視器驗證NVM流
無法設定資料湖，未檢測到XDR組織	使用XDR一鍵整合來連線XDR和XDR分析
無法設定資料記錄，檢測到多個XDR組織	聯絡TAC以取得協助

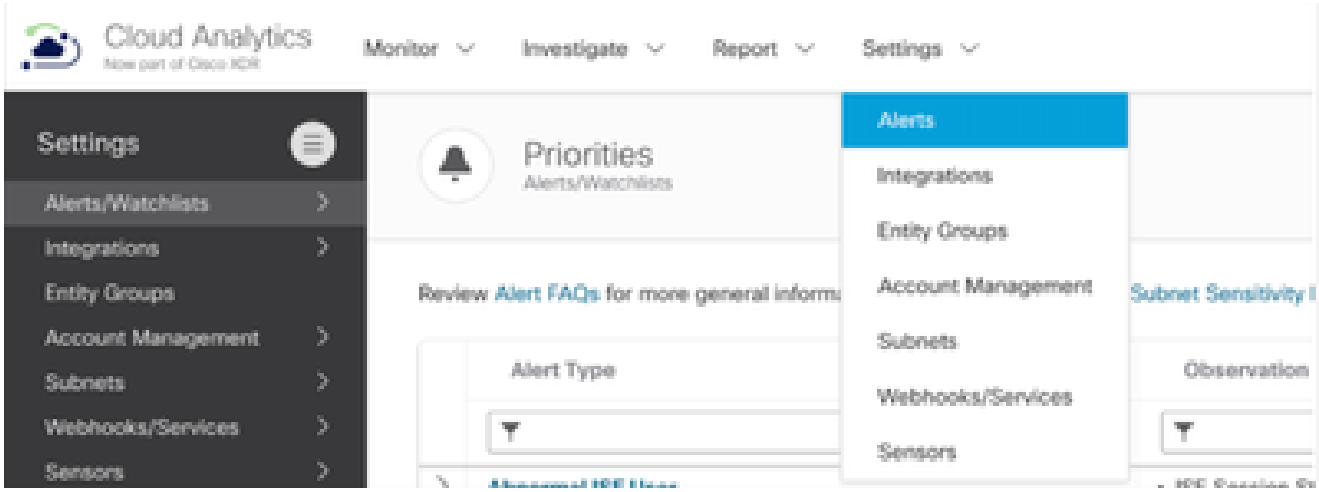
- 如果其中任何步驟失敗，請從「安全客戶端」介面運行安全客戶端診斷和報告工具(DART)以診斷問題（始終請求以管理員身份運行DART）
  收集安全客戶端的DART捆綁包

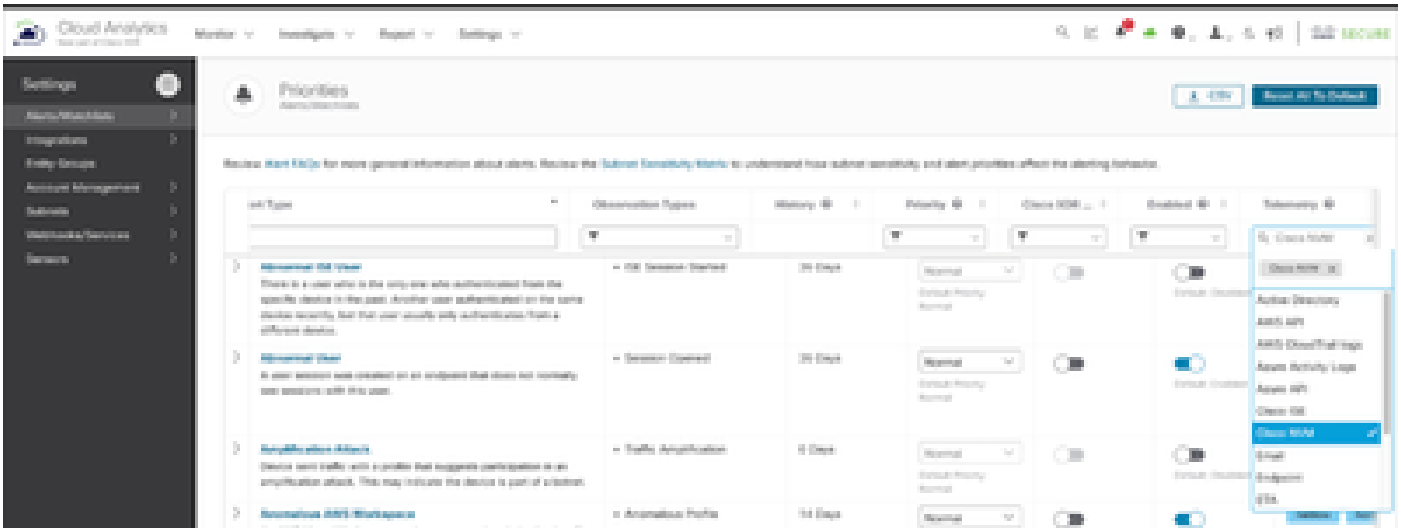
觀察與警報

NVM警報

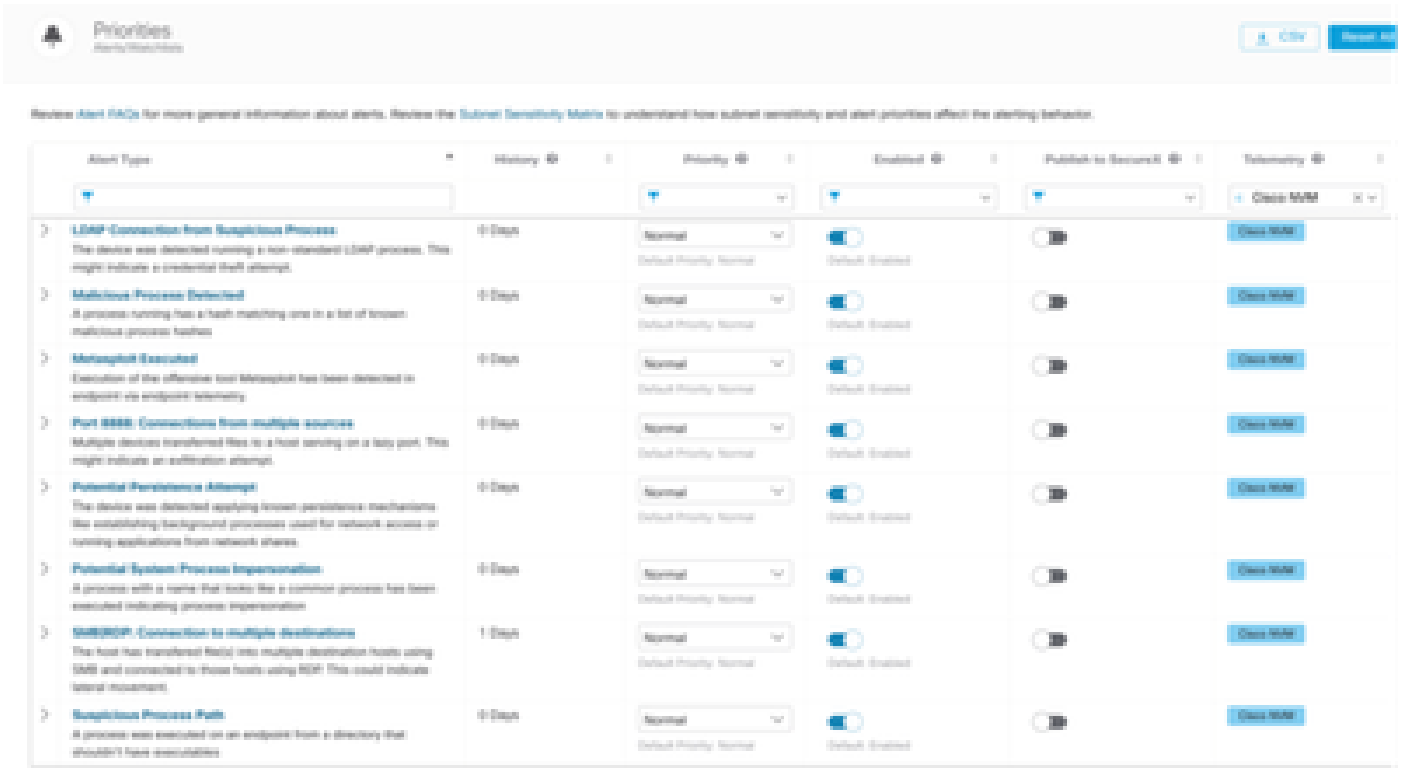
- 登入到XDR分析門戶
- 設定>警報遙測>思科NVM

- 遙測>思科NVM





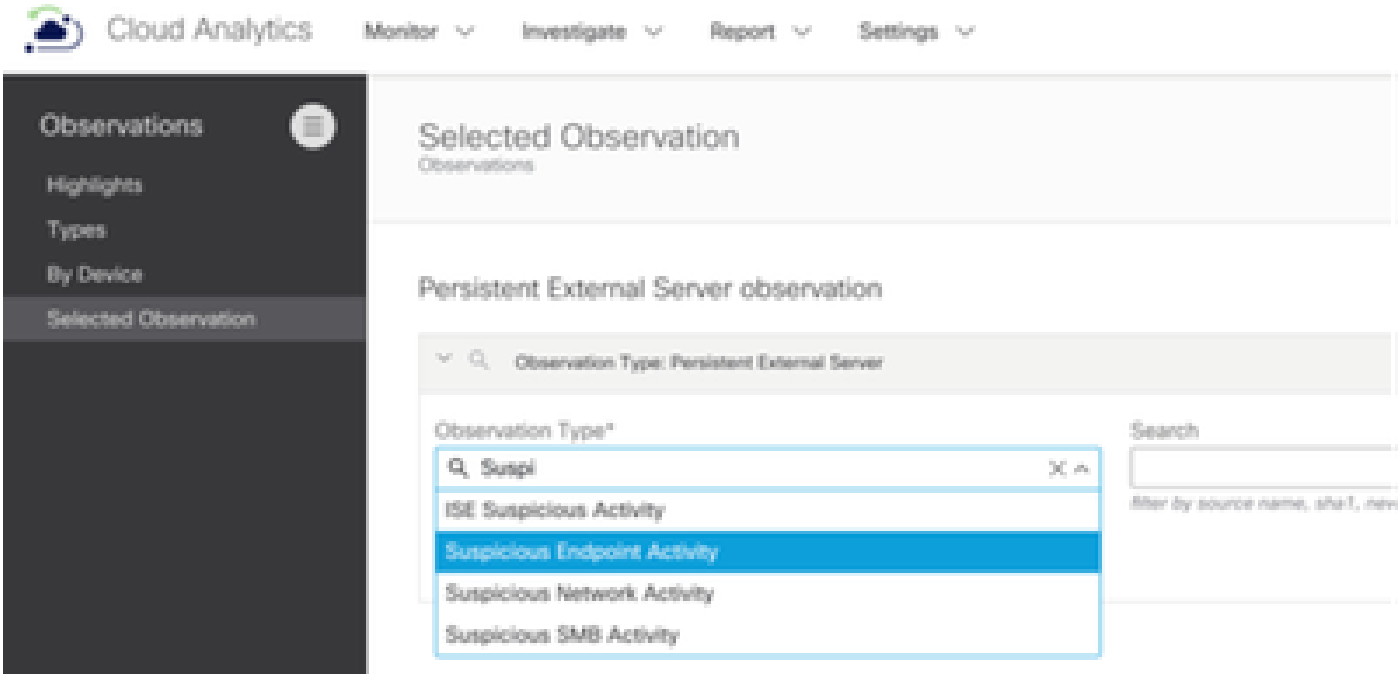
NVM警報設定



NVM觀察

— 可疑終端活動
- XDR分析門戶

— 監控>觀察
— 選定觀察
— 過濾可疑終端活動



NVM檢測警告

- NVM僅捕獲具有關聯網路連線的流程和流資料
— 預設情況下，NVM配置為僅在流結束時報告流資料

結論

這些步驟可幫助您導航XDR分析，以使用NVM資訊啟用觀察和警報，並排除工作流故障。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。