XDR分析用NVMのトラブルシューティングと有効化

内容

はじめに

このドキュメントでは、Cisco eXtended Detection and Response(XDR)/Network Visibility Module(NVM)のCisco XDR Analyticsをトラブルシューティングする方法について説明します。

前提条件

XDR統合を備えたアクティブなXDR分析ポータル

要件

単一のXDR統合でのXDR Analyticsアカウントの実行

使用するコンポーネント

- XDR分析
- XDR
- NVMセンサー
- セキュアクライアント（バージョン5.0+）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

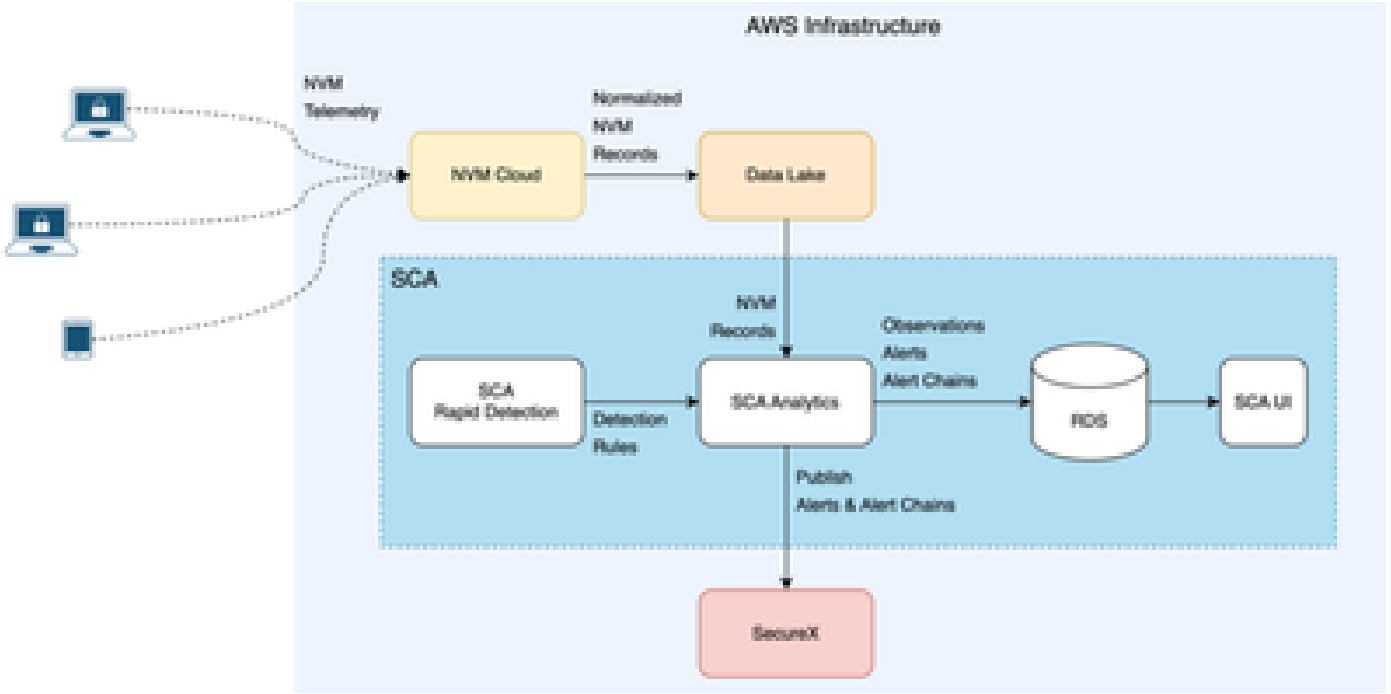
XDR分析NVMフロー

XDR分析がNVMテレメトリを消費
テレメトリは、Cisco Secure ClientのNVMコンポーネントによって生成されます。

NVMは、ユーザの動作、ネットワーク通信、プロセスを含むネットワークの可視性を強化し、インシデント調査の時間を短縮してエンドポイントの可視性のギャップを埋めます

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

NVMデータフロー – XDR分析

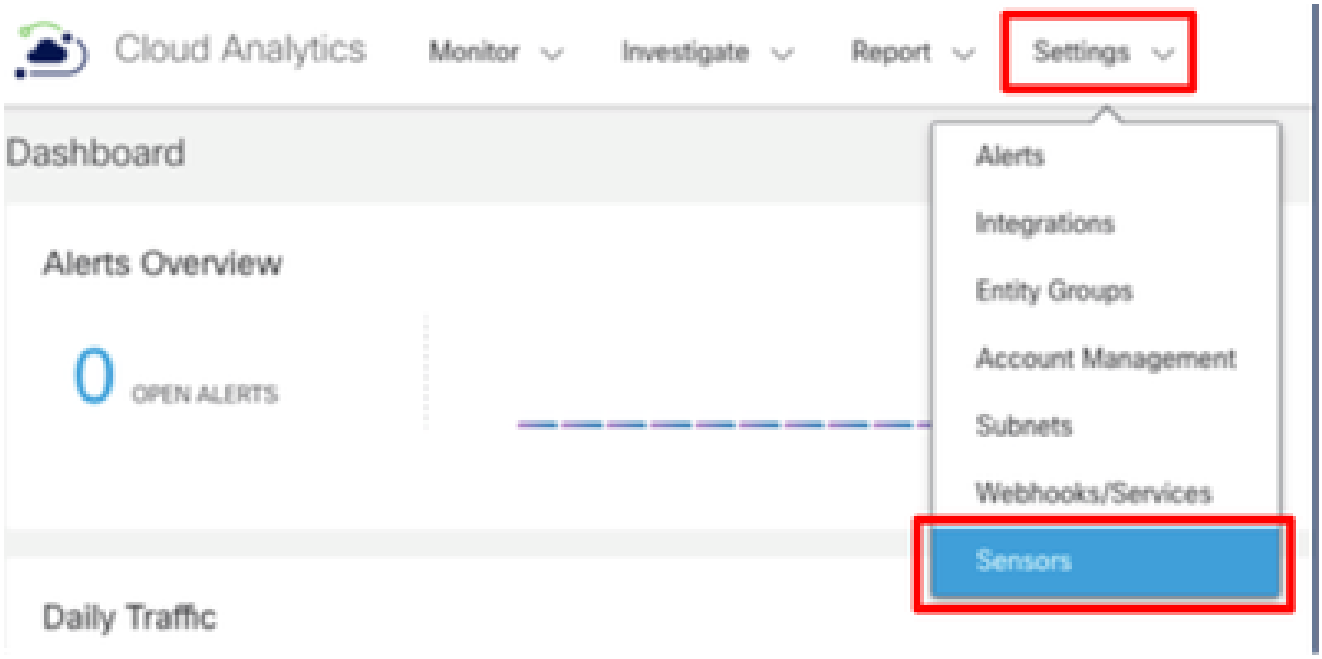


- 常に最新のSecure Clientバージョンを使用することをお勧めします。このワークフローでは、Secure Clientバージョン5.0以降を使用する必要があります。https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- 最新のSecure Clientバージョンおよび導入Proの更新を維持file: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloudがテレメトリボリュームを処理し、取り込みに使用できるようにします。Data Lakeがテレメトリを取り込み、標準化して効率的なストレージを実現します。
- XDR AnalyticsはNVMレコードを定期的（10分）に処理し、検出を生成 – 観察とアラート
- 迅速な検出により、設定を使用して簡単な観察とアラートをすばやく追加

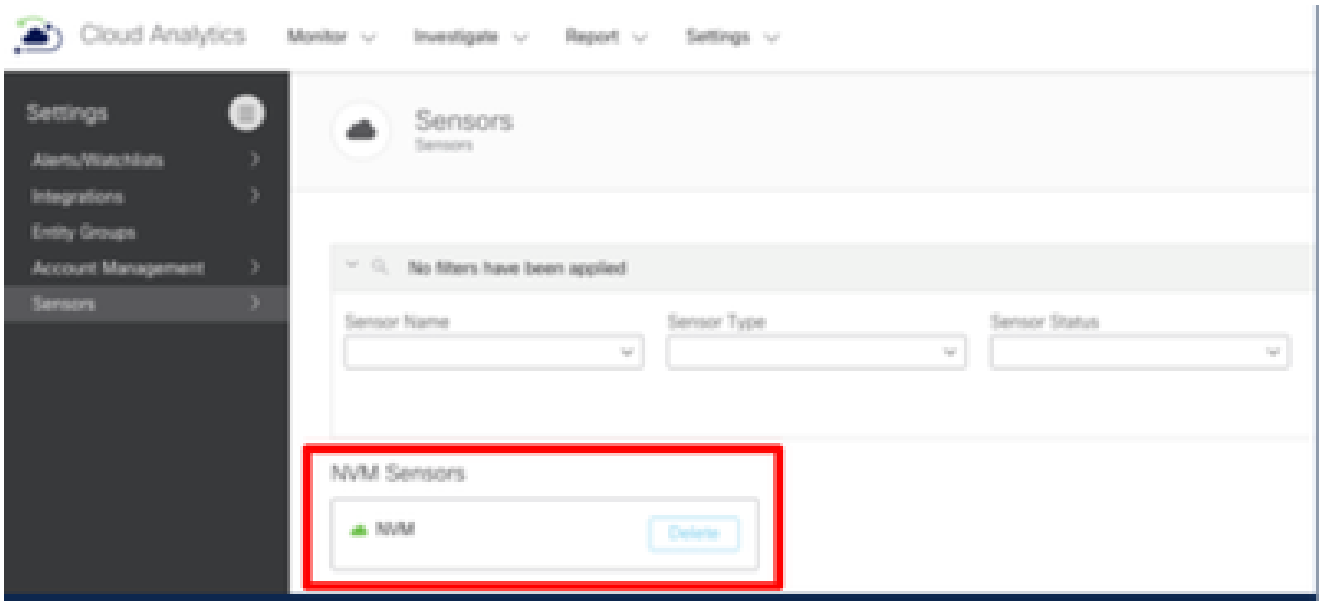
- XDR Analyticsは、アラートを攻撃チェーン（以前のアラートチェーン）に相関させます。
- ユーザはXDRにアラートと攻撃チェーンを公開できます。

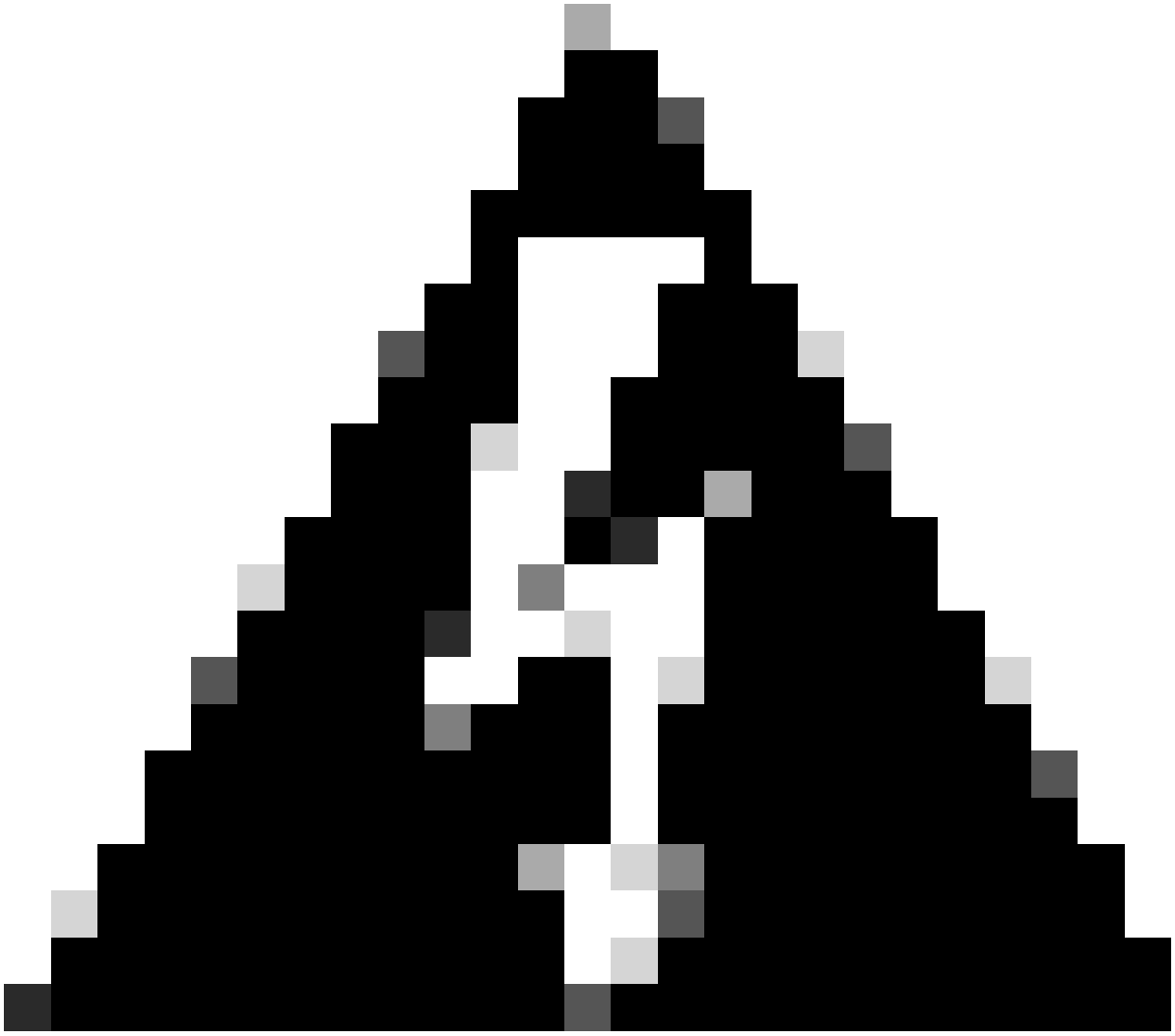
NVMセンサーステータス

- NVMセンサーが作成されたことを確認します。- XDR Analyticsダッシュボードから、設定>センサーに移動します。



- 次に、NVMセンサーがセンサーリストで使用可能であることを確認します





警告: XDR分析ポータルには、最大1つのXDRテナント/組織が関連付けられている必要があります。

NVM組織ID

- NVMクライアントのAPIエンドポイントに表示される組織IDが同じであることを確認します（図1の矢印Aを参照）。
  https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/

NVM Data Lakeプロビジョニングステータス

- データレイクが適切にオンボーディングされていることを確認するためのAPIエンドポイントでは、次のAPIエンドポイントを使用して関連付けを確認できます。https://XDR

Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/

- ポータルを通じてアクセス権が付与されたすべてのユーザは、これらのエンドポイント（ポータル管理者、TAC、エンジニアリング）にアクセスできます。

デバッグ

- デバッグ応答コード：

応答コード	アクションが必要
DataLakeが正常にプロビジョニングされました	イベントビューアによるNVMフローの検証
データレイクをプロビジョニングできません。XDR組織が検出されませんでした	XDRとXDR Analyticsを接続するには、XDRワンクリック統合を使用します
データレイクをプロビジョニングできません。複数のXDR組織が検出されました	TACに問い合せる

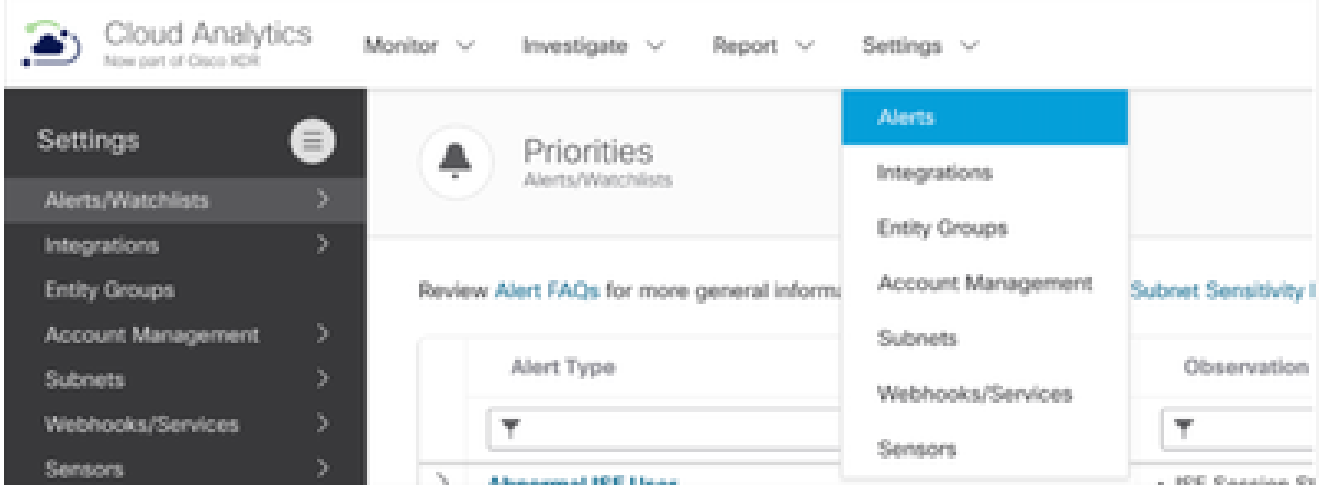
- これらの手順のいずれかが失敗した場合、セキュアクライアントインターフェイスからセキュアクライアント診断およびレポートツール(DART)を実行して問題を診断します（常に管理者としてDARTの実行を要求します）
セキュアクライアントのDARTバンドルの収集

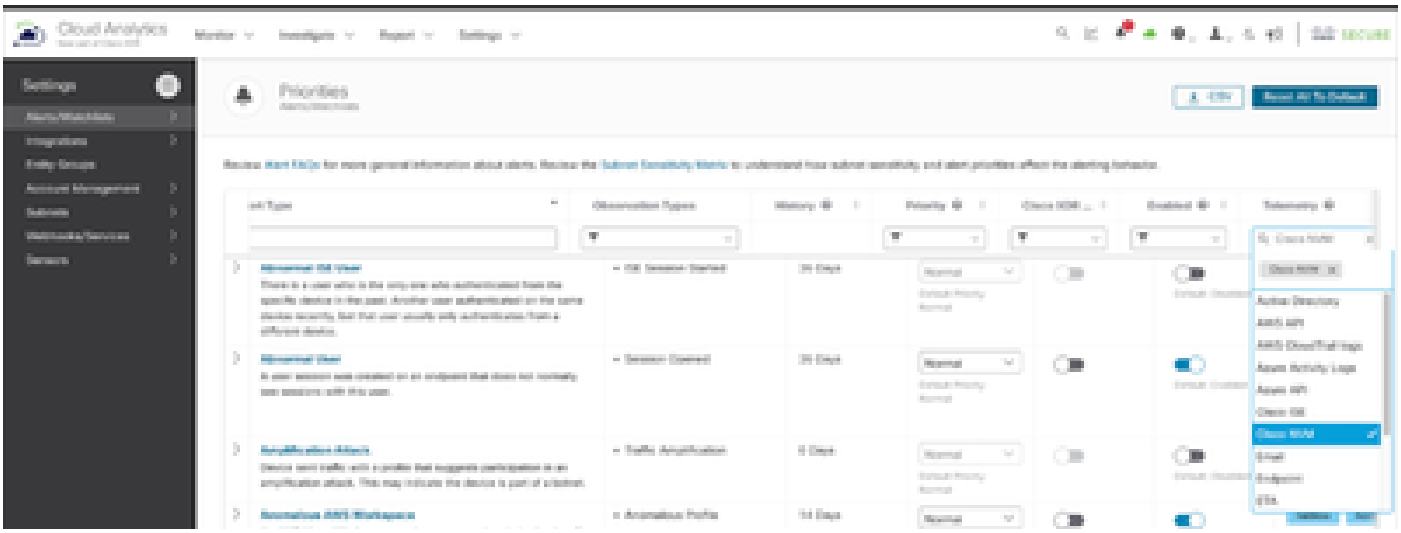
観察とアラート

NVMアラート

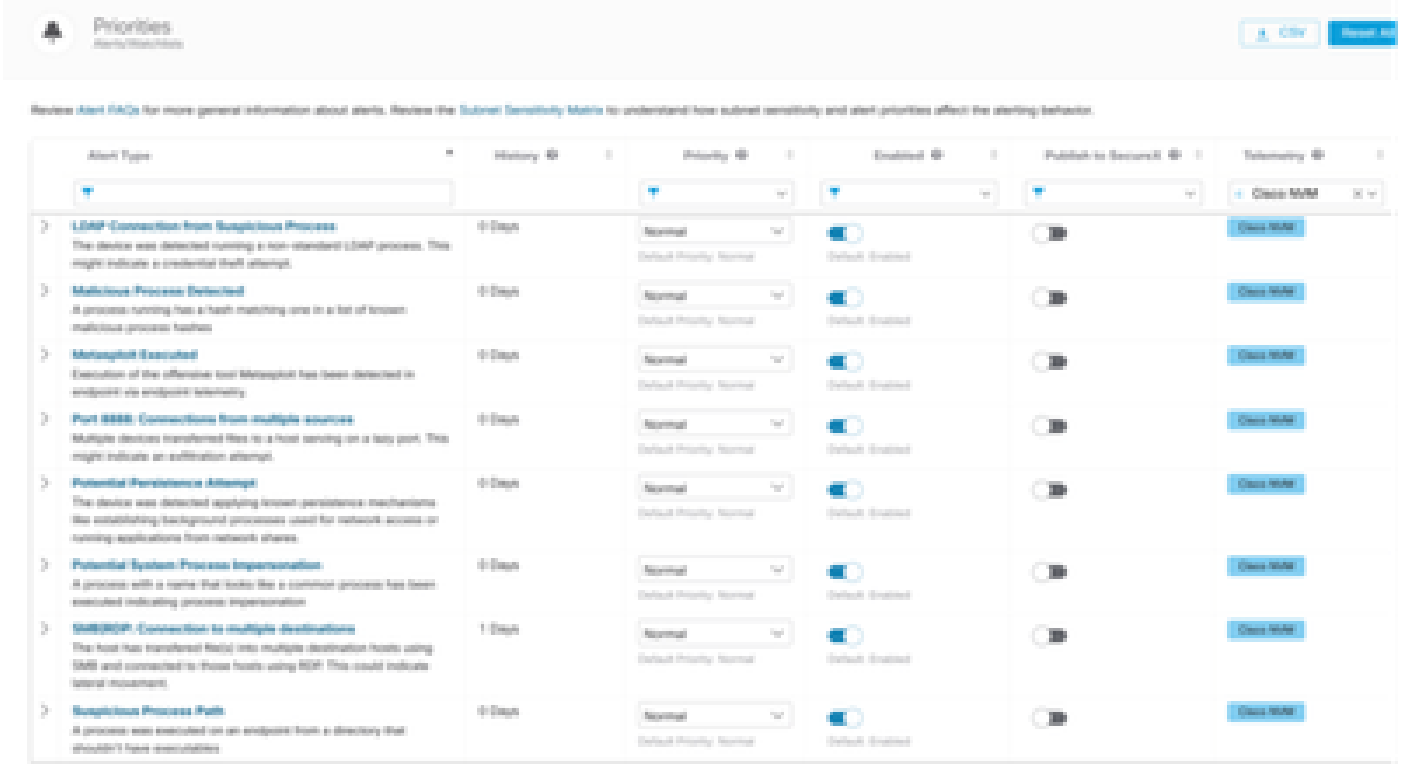
- XDR Analyticsポータルにログインします。
- 設定>アラートテレメトリ> Cisco NVM

- テレメトリ> Cisco NVM


Cloud Analytics
Monitor
Investigate
Report
Settings
Settings
Alerts/Watchlists
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
Priorities
Alerts/Watchlists
Alerts
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
Alert Type
Observation

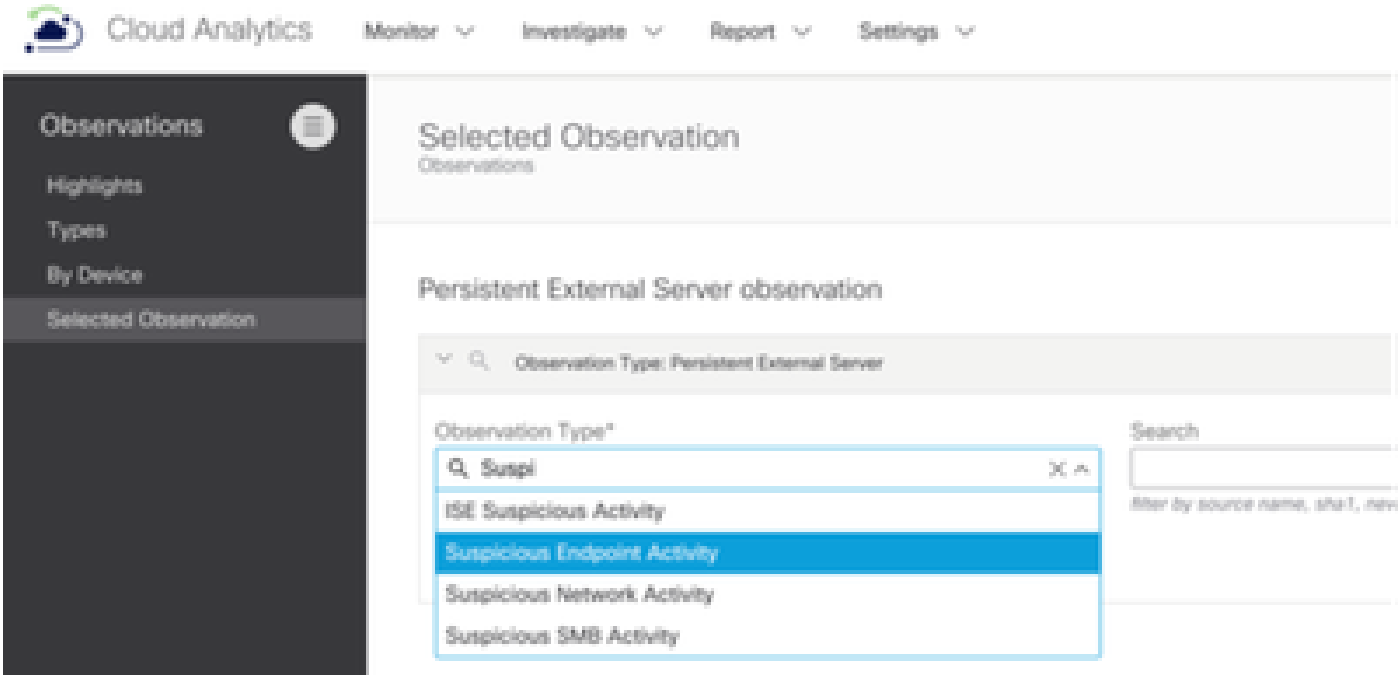


NVMアラート設定



NVMの観察

– 不審なエンドポイントのアクティビティ
- XDR分析ポータル
- [モニタ] > [観測]
– 選択された観察
– 疑わしいエンドポイントアクティビティのフィルタリング



NVMの検出に関する注意事項

- NVMは、関連するネットワーク接続があるプロセスとフローデータのみをキャプチャします。
- NVMは、デフォルトではフローの最後でのみフローデータを報告するように設定されています

結論

これらの手順は、XDR分析をナビゲートして、NVM情報を使用した観察とアラートを有効にし、ワークフローをトラブルシューティングするのに役立ちます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。