对XDR分析进行NVM故障排除并启用NVM

目录

简介

- 先决条件
  - 要求
  - 使用的组件
- XDR分析NVM流量
  - NVM数据流 — XDR分析
  - NVM传感器状态
  - NVM组织ID
  - NVM数据湖调配状态
  - 调试
- 观察与提示
  - NVM警报
  - NVM警报设置
  - NVM观察
  - NVM检测警告
- 结论

简介

本文档介绍如何对思科扩展检测和响应(XDR)/网络可视性模块(NVM)的Cisco XDR分析进行故障排除

先决条件

具有XDR集成的活动XDR分析门户

要求

通过单个XDR集成运行XDR分析帐户

使用的组件

- XDR分析
- XDR
- NVM传感器
- 安全客户端（版本5.0+）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

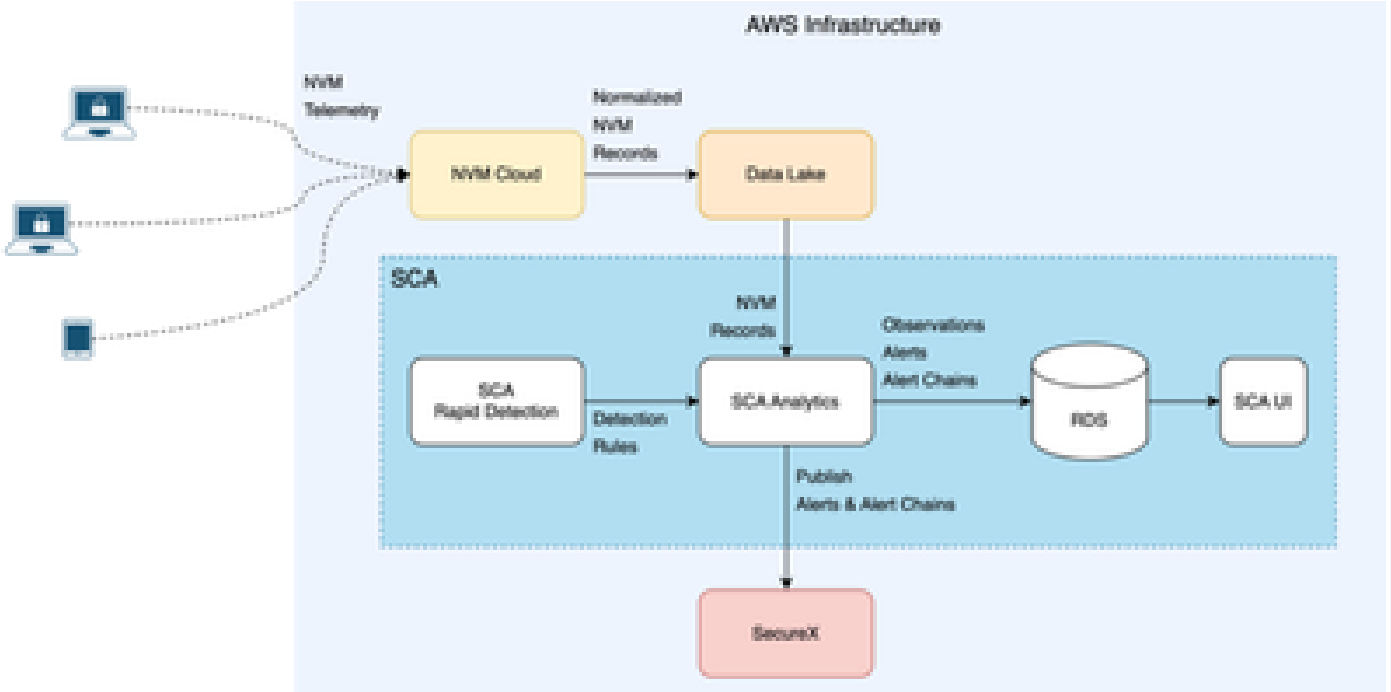
XDR分析NVM流量

XDR分析现在使用NVM遥测
遥测由Cisco安全客户端中的NVM组件生成。

NVM提供增强的网络可视性，包括用户行为、网络通信和流程，从而缩短事件调查时间并填补终端可视性的空白

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

NVM数据流 — XDR分析



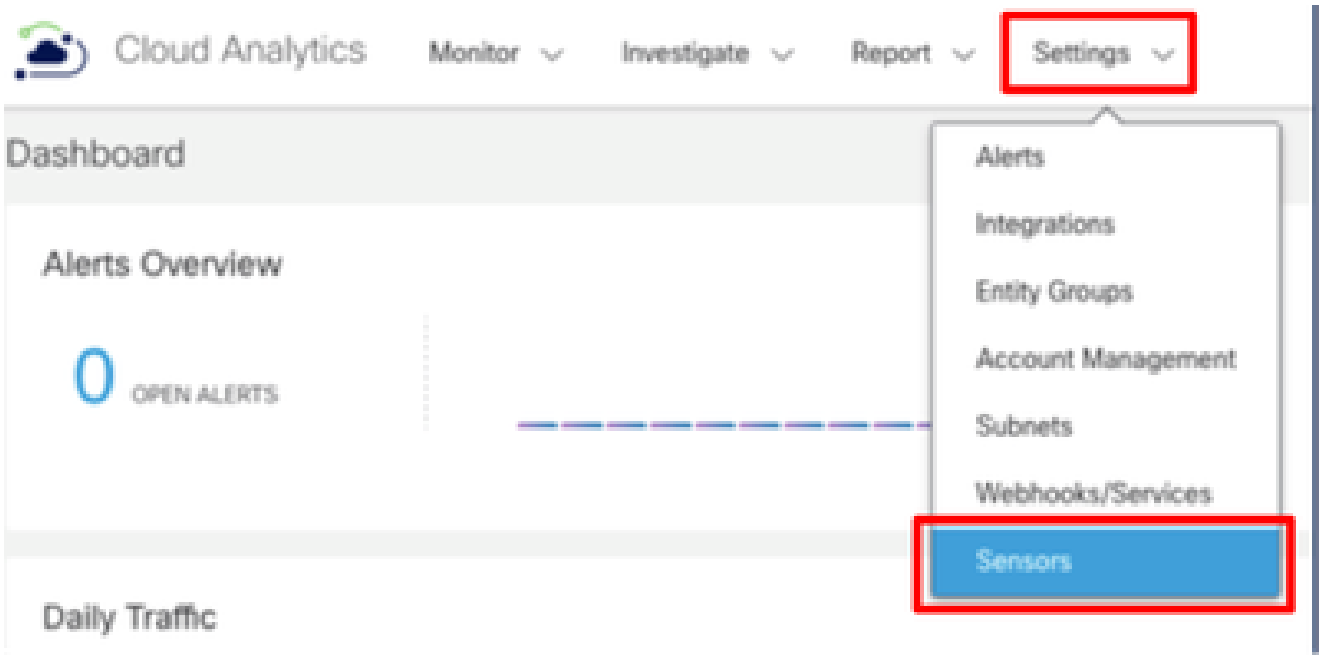
- 我们始终建议始终使用最新的Secure Client版本，此工作流程要求您使用Secure Client 5.0版或更高版本：https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- 维护最新安全客户端版本和部署Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM云可处理遥测卷，并使其可供接收数据湖接收遥测并对其进行规范化，以实现高效存储
- XDR分析定期处理NVM记录（10分钟）以生成检测 — 观察和警报
- 快速检测有助于使用配置快速添加简单的观察和警报

- XDR分析将警报关联到攻击链（以前称为警报链）

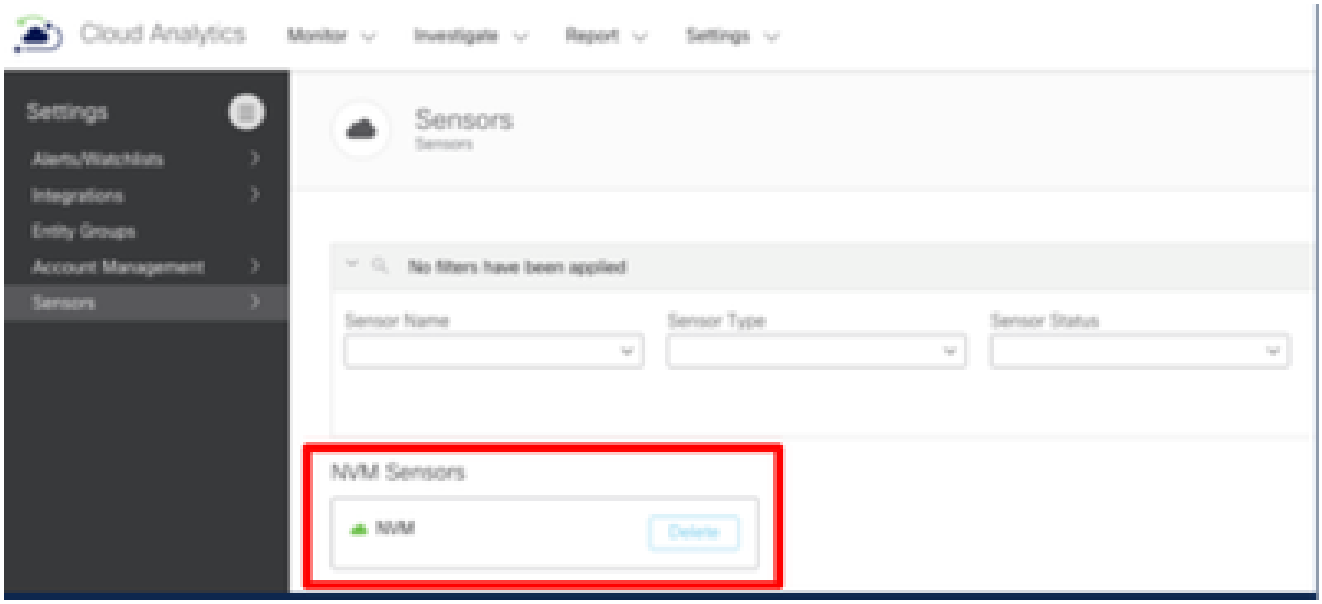
- 用户可以向XDR发布警报和攻击链。

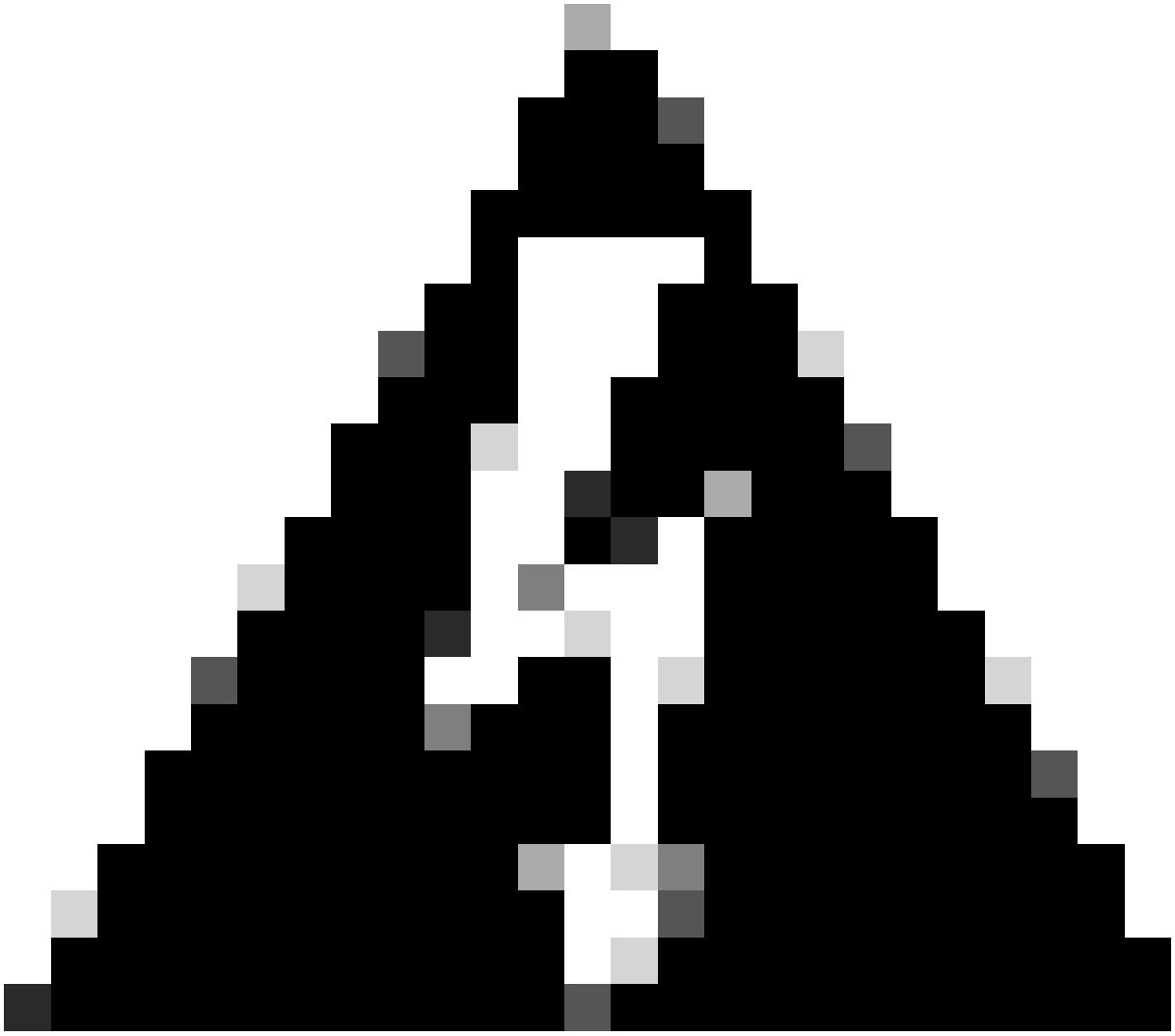
NVM传感器状态

- 确保创建NVM传感器： — 从XDR分析控制面板导航到设置>传感器



- 然后确认NVM传感器在传感器列表中可用





警告：XDR分析门户最多必须有一个与其关联的XDR租户/组织。

NVM组织ID

- 确认NVM客户端在API终端中显示相同的组织ID: https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/



NVM数据湖调配状态

- API终端可确保数据湖正常入网，可以使用此API终端确认关联：https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datalake/

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

- 通过门户获得访问权限的所有用户都可以访问这些终端（门户管理员、TAC、工程）

调试

- 调试响应代码：

响应代码	所需操作
已成功调配DataLake	通过事件查看器验证NVM流
无法调配数据湖，未检测到XDR组织	使用XDR一键集成来连接XDR和XDR分析
无法调配数据记录，检测到多个XDR组织	联系TAC寻求帮助

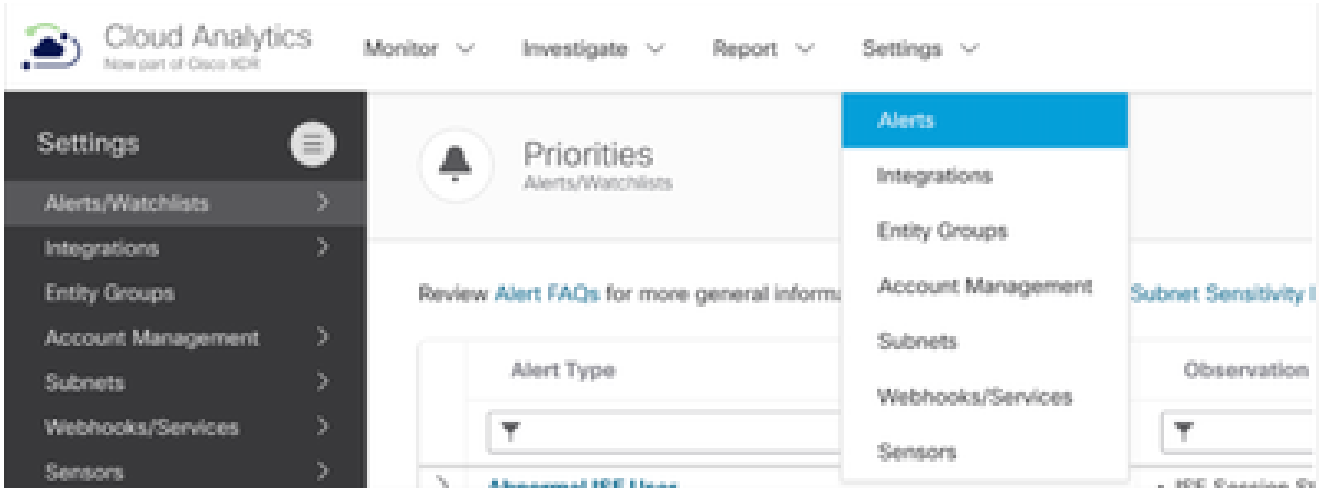
- 如果上述任何步骤失败，请从安全客户端界面运行安全客户端诊断和报告工具(DART)以诊断问题（始终请求以管理员身份运行DART）
  收集安全客户端的DART捆绑包

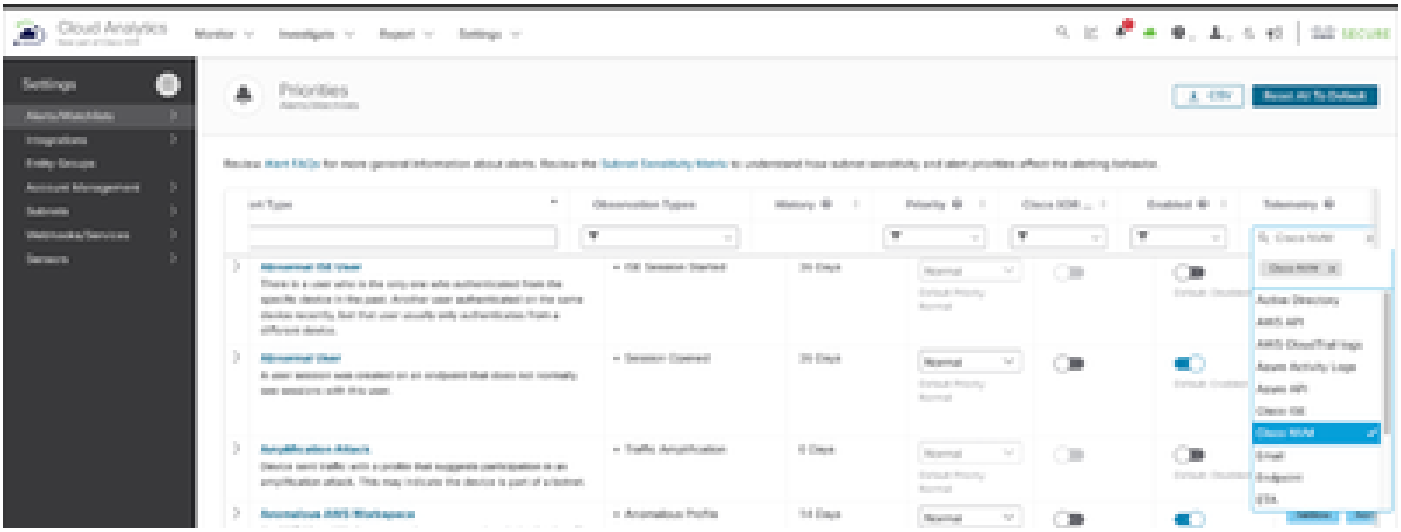
观察与提示

NVM警报

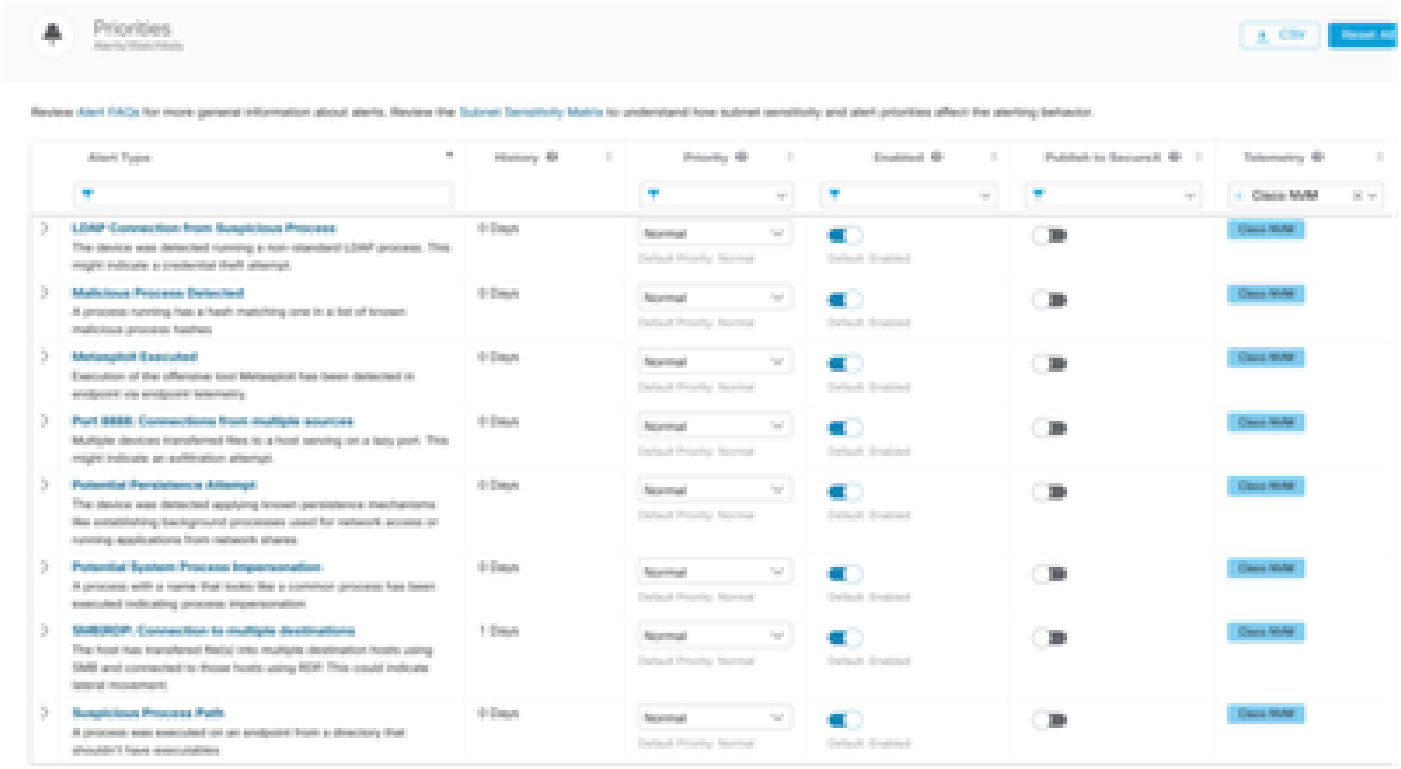
- 登录XDR分析门户
- 设置(Settings)>警报(Alerts)遥测(Telemetry)>思科NVM

- 遥测>思科NVM





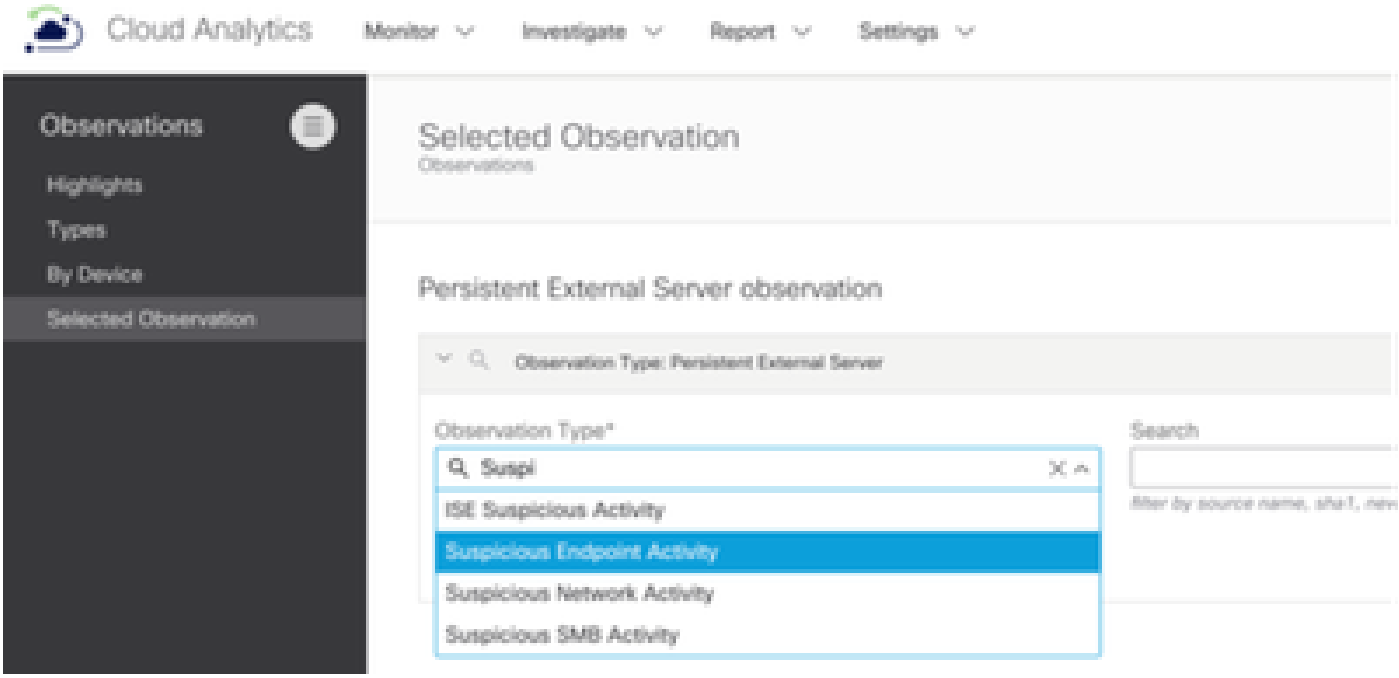
NVM警报设置



NVM观察

— 可疑终端活动
- XDR分析门户

— 监控>观察
— 选定观察
— 过滤可疑终端活动



NVM检测警告

- NVM仅捕获具有关联网络连接的流程和流数据
— 默认情况下，NVM配置为仅在流结束时报告流数据

结论

这些步骤可帮助您浏览XDR分析，以使用NVM信息启用观察和警报，并对工作流程进行故障排除。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。