Risoluzione dei problemi e abilitazione di NVM per XDR Analytics

Sommario

Introduzione

Questo documento descrive come risolvere i problemi di Cisco XDR Analytics per Cisco eXtended Detection and Response (XDR) / Network Visibility Module (NVM)

Prerequisiti

Portale Active XDR Analytics con integrazione XDR

Requisiti

Esecuzione dell'account XDR Analytics con l'integrazione XDR singola

Componenti usati

- XDR Analytics
- XDR
- Sensore NVM
- Secure Client (versione 5.0+)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

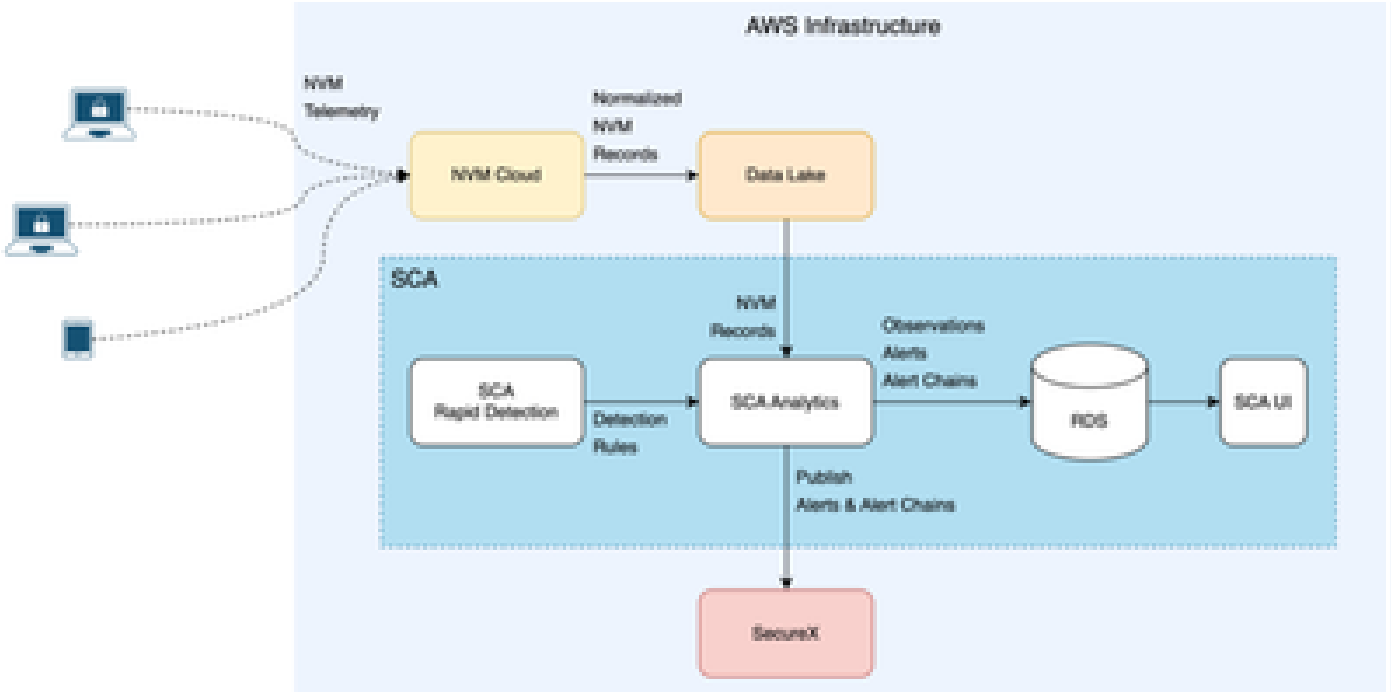
Flussi NVM di XDR Analytics

XDR Analytics utilizza ora la telemetria NVM
La telemetria viene generata dal componente NVM in Cisco Secure Client.

La tecnologia NVM migliora la visibilità della rete, in particolare per quanto riguarda i comportamenti degli utenti, le comunicazioni di rete e i processi, riducendo i tempi di analisi degli incidenti e colmando le lacune nella visibilità degli endpoint

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

Flussi di dati NVM - XDR Analytics

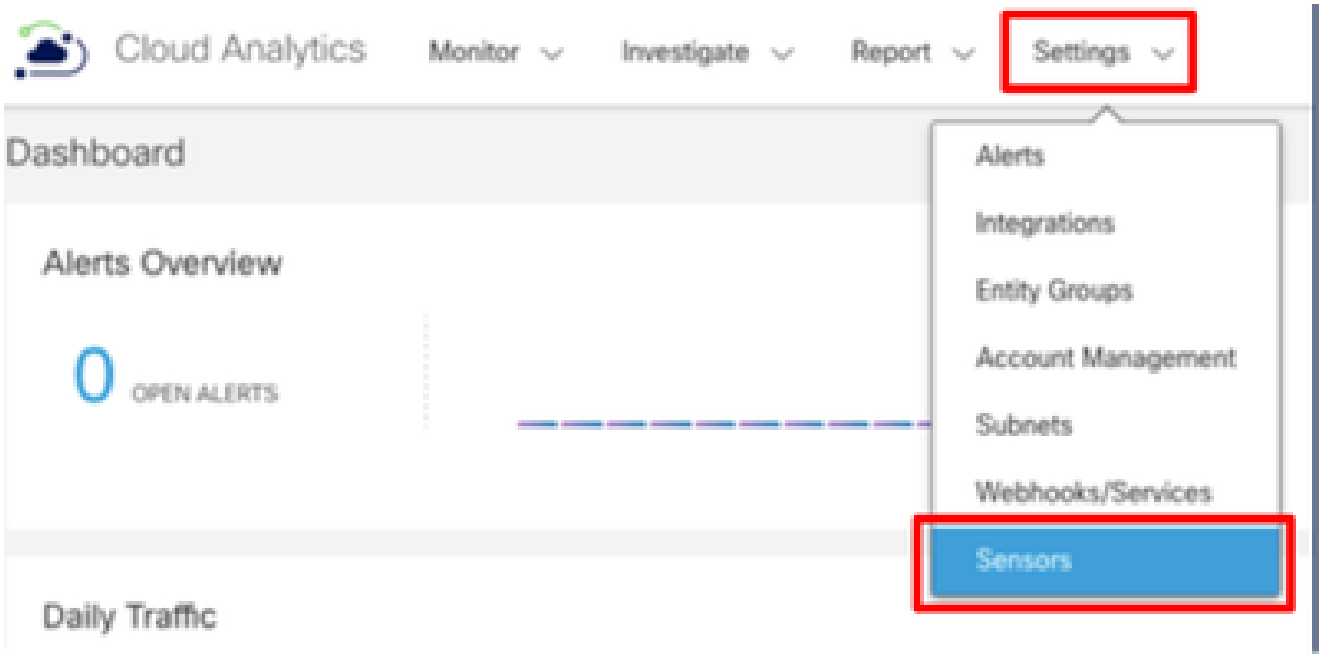


- È sempre consigliabile essere sempre aggiornati sulle versioni di Secure Client. Questo flusso di lavoro richiede l'utilizzo di Secure Client versione 5.0 o successiva: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Mantenere aggiornato Secure Client versione e Deployment Profile: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud gestisce il volume di telemetria e lo rende disponibile per l'acquisizione. Data Lake acquisisce la telemetria e la normalizza per uno storage efficiente

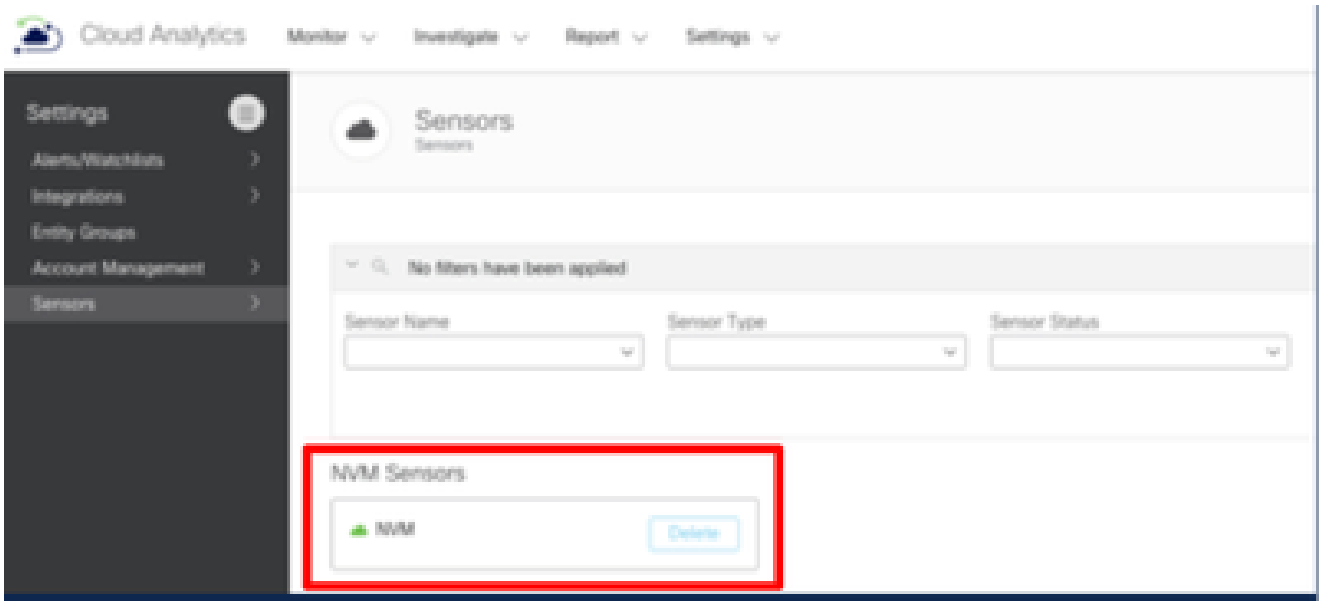
- XDR Analytics elabora i record NVM a intervalli regolari (10 minuti) per generare rilevamenti - Osservazioni e avvisi
- Il rilevamento rapido consente di aggiungere rapidamente semplici osservazioni e avvisi utilizzando le configurazioni
- XDR Analytics mette in correlazione gli avvisi nelle catene di attacchi (in precedenza, catene di avvisi)
- L'utente può pubblicare le catene di avvisi e attacchi su XDR.

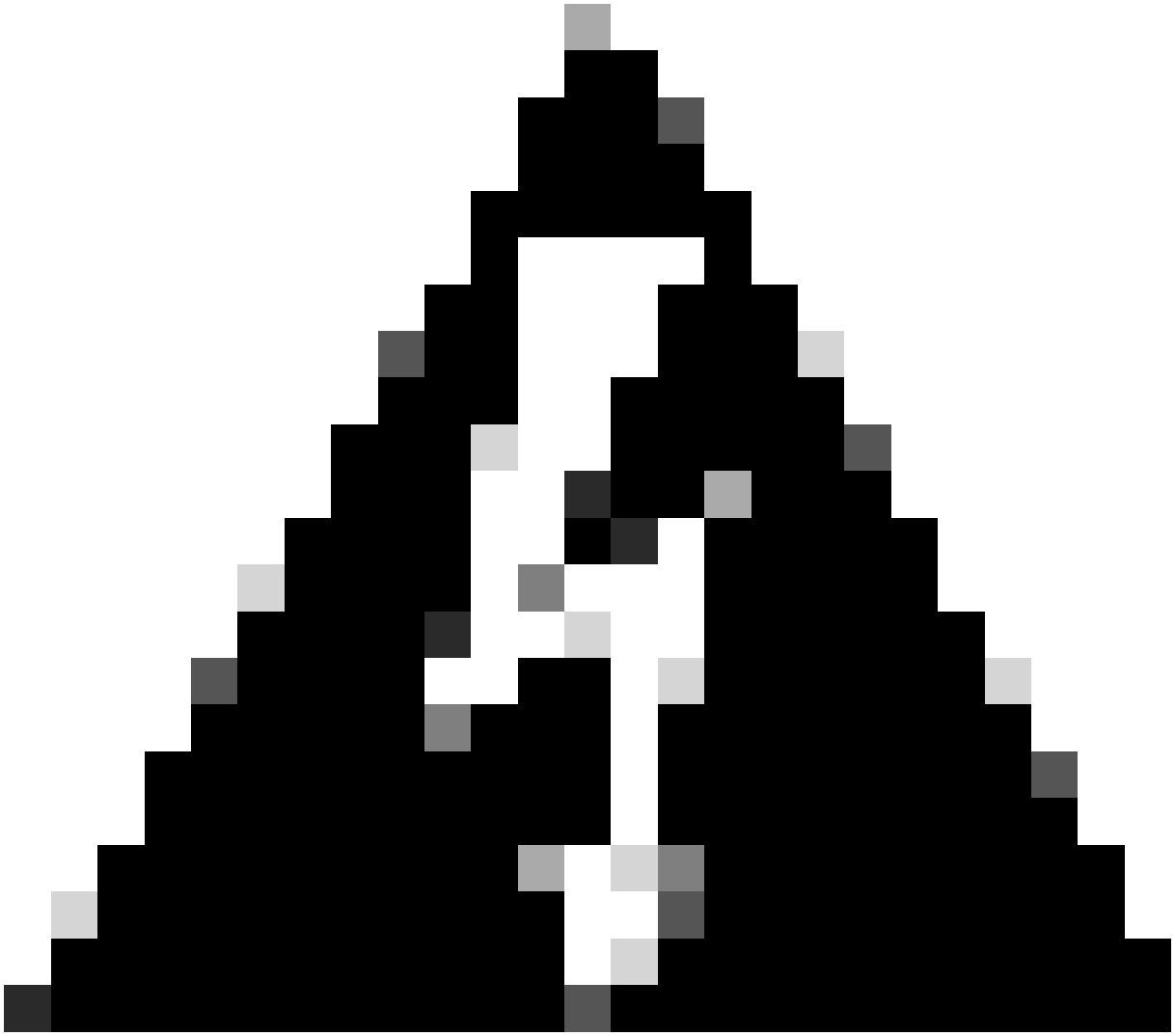
Stato del sensore NVM

- Verifica della creazione del sensore NVM:- Dal dashboard di XDR Analytics, passare a impostazioni > Sensori



- Confermare quindi che il sensore NVM sia disponibile nell'elenco dei sensori





Avviso: Al portale di analisi XDR deve essere associato un solo tenant/organizzazione XDR.

ID organizzazione NVM

- Confermare che i client NVM presentino lo stesso ID organizzazione nell'endpoint API: https://XDR Analytics_PORTAL_URL/api/v3/integations/securex/orgs/

Stato provisioning NVM Data Lake

- Gli endpoint API per garantire il corretto caricamento del Data Lake. L'associazione può essere confermata utilizzando questo endpoint API:https://XDR Analytics_Portal_URL/api/v3/integations/securex/orgs/onboard_datalake/

- Tutti gli utenti a cui è concesso l'accesso tramite il portale possono accedere a questi endpoint (amministratori del portale, TAC, progettazione)

Debug

- Codici di risposta di debug:

Codice di risposta	Azione richiesta
Provisioning di Data Lake completato	Convalida dei flussi NVM tramite il Visualizzatore eventi
Impossibile effettuare il provisioning del data lake. Nessuna organizzazione XDR rilevata	Utilizzare l'integrazione XDR con un solo clic per collegare XDR e XDR Analytics
Impossibile effettuare il provisioning del datalake. Rilevate più organizzazioni XDR	Contatta TAC per assistenza

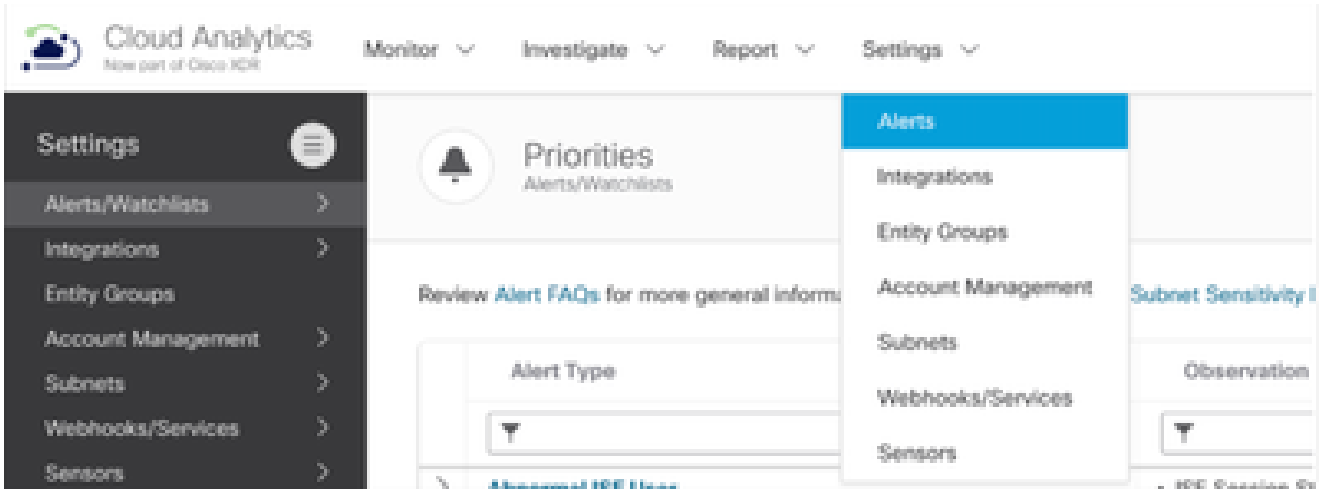
- Se una di queste operazioni ha esito negativo, eseguire lo strumento di diagnostica e segnalazione client sicuri (DART, Secure Client Diagnostics And Reporting Tool) dall'interfaccia client sicuri per diagnosticare il problema (richiedere sempre l'esecuzione di DART come amministratore)
  Raccogli bundle DART per Secure Client

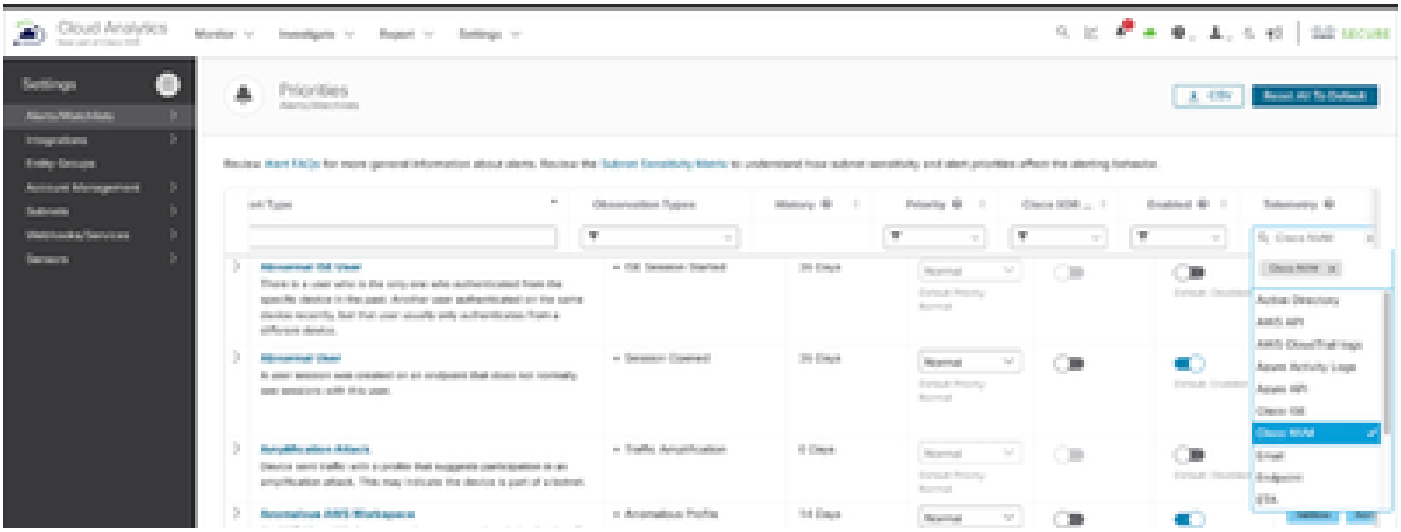
Osservazioni e avvisi

Allarmi NVM

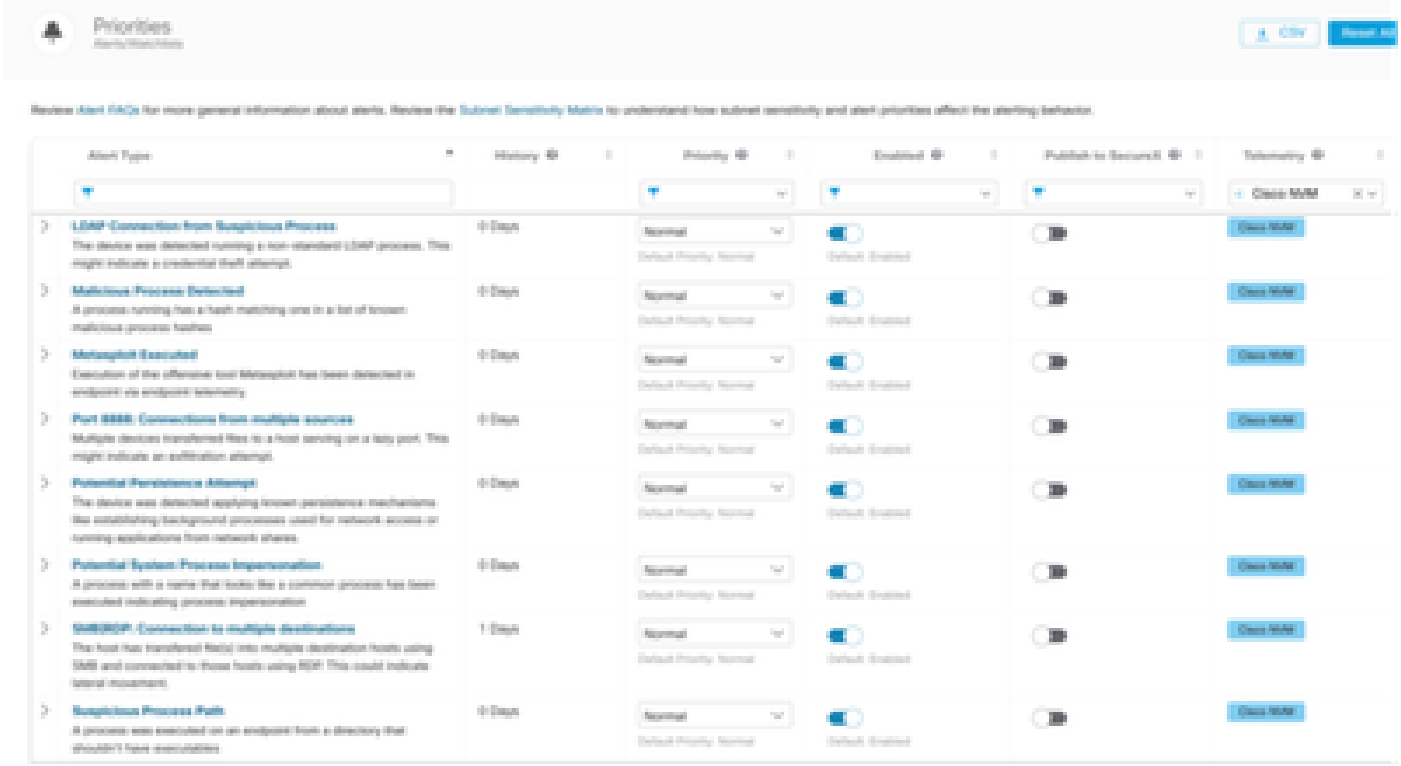
- Accedi al portale XDR Analytics
- Impostazioni > Telemetria avvisi > Cisco NVM

- Telemetria > Cisco NVM



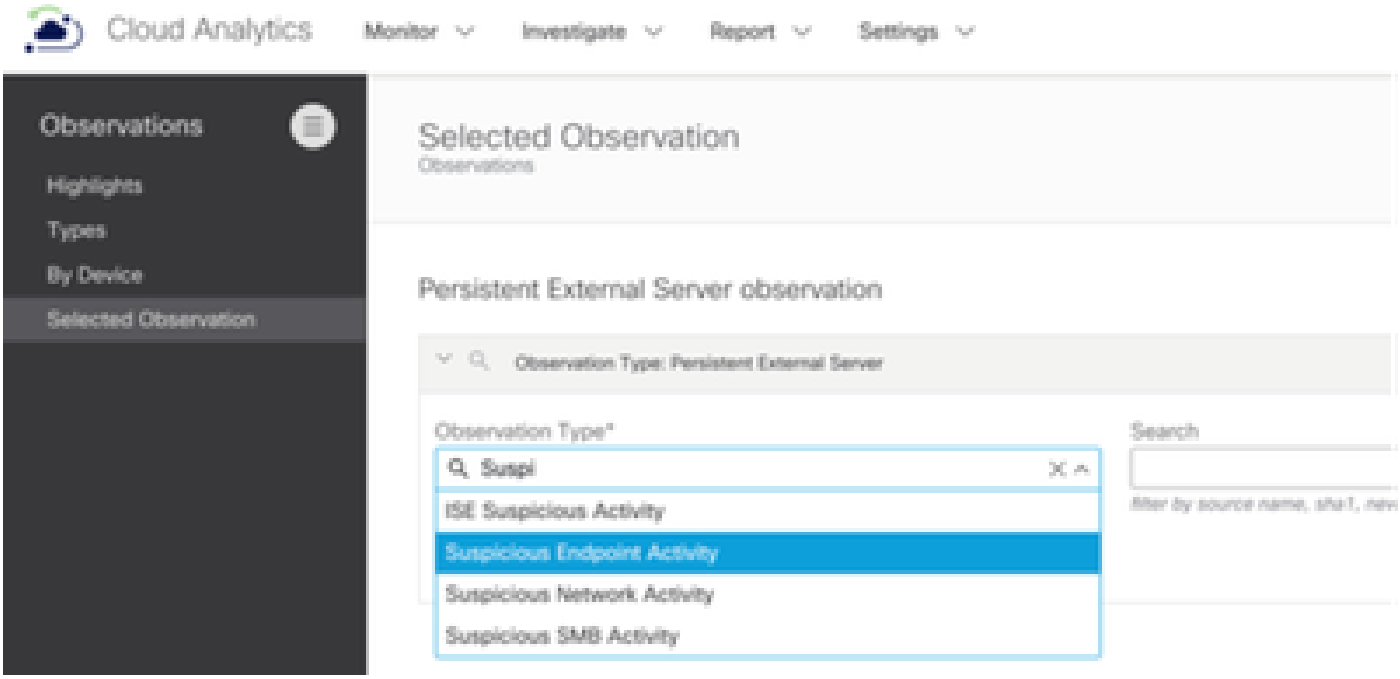


Impostazioni avviso NVM



Osservazioni sulla NVM

- Attività degli endpoint sospetti
- Portale XDR Analytics
- Monitoraggio > Osservazioni
- Osservazione selezionata
- Filtra attività endpoint sospette



Avvertenze di rilevamento NVM

- NVM acquisisce solo i processi e i dati di flusso che hanno una connessione di rete associata
- NVM è configurato per riportare i dati di flusso solo alla fine del flusso per impostazione predefinita

Conclusioni

Questi passaggi consentono di spostarsi all'interno di XDR Analytics per attivare Osservazioni e avvisi utilizzando le informazioni NVM e la risoluzione dei problemi del flusso di lavoro.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).