Risoluzione dei problemi di integrazione cloud Cisco XDR e Secure Malware Analytics

Sommario

Introduzione

Questo documento descrive come risolvere i problemi relativi al modulo Secure Malware Analytics Cloud con Cisco XDR.

Contributo di Javi Martinez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Malware Analytics Cloud
- Cisco XDR

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Console cloud di analisi malware sicuro (account utente con diritti di amministratore)
- Console Cisco XDR (account utente con diritti di amministratore)

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.

Premesse

Cisco Secure Malware Analytics Cloud è una piattaforma avanzata e automatizzata di analisi malware e malware threat intelligence in cui file sospetti o destinazioni web possono essere detonati senza impatto sull'ambiente utente.

Nell'integrazione con Cisco XDR, Secure Malware Analytics è un modulo di riferimento che consente di eseguire il pivot nel portale Secure Malware Analytics per raccogliere informazioni aggiuntive su hash di file, IP, domini e URL nell'archivio delle conoscenze di Secure Malware Analytics Cloud (SMA Cloud).

Fare riferimento alla più recente guida all'integrazione di Secure Malware Analytics Cloud,

- NAM Cloud.
- EU Cloud.

Risoluzione dei problemi

Licenza

- Verificare di disporre di una licenza SMA corretta per poter accedere alla console Secure Malware Analytics Cloud

Tessere del modulo

- Verificare di aver selezionato i ***riquadri*** corretti per il modulo cloud Secure Malware Analytics
  Accedere al portale Cisco XDR > Dashboard > Pulsante Personalizza > Selezionare il modulo SMA Cloud > Aggiungere le tessere appropriate

ruolo Amministratore

- Verificare di disporre di un account Analisi malware protetto con ruolo di amministratore nel portale Analisi malware protetto
  Accedere al portale Cisco XDR > Amministrazione > Il proprio account

- Verificare di disporre di un account SecureX con diritti di amministratore nel portale SecureX
  Passare a Portale Analisi malware > Account Analisi malware

Nota: se non si dispone del ruolo di amministratore nella console di analisi malware sicuro e nella console Cisco XDR, l'amministratore può modificare il ruolo dell'account direttamente dal portale in questione

Tempi

- Verificare che l'opzione Timestamp (Data e ora) sia impostata correttamente sul portale Cisco XDR.
  Accedere al portale Cisco XDR > Dashboard > Opzione intervallo di tempo > Selezionare l'intervallo di tempo appropriato in base all'attività SMA

Ricrea modulo

- Eliminare il vecchio modulo SMA e crearne uno nuovo.
  Passare a Console cloud di analisi malware protetto > Account di analisi malware > Chiave API > Copia la chiave API
  Accedere a Cisco XDR Portal > Integration modules > Select the SMA Cloud module > Add the API key and URL (Select the SMA Cloud) > Create the Dashboard (Scegli il portale Cisco XDR > Moduli di integrazione > Seleziona il modulo SMA Cloud > Aggiungi la chiave API e l'URL (Seleziona il

cloud SMA) > Crea dashboard)

Nota: solo gli utenti con il ruolo Org Admin o Users possono ottenere la chiave API che abilita il modulo di integrazione Secure Malware Analytics in Cisco XDR.

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).