

Dépannage de l'intégration cloud de Cisco XDR et Secure Malware Analytics

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Dépannage](#)

[Licence](#)

[Mosaïques de module](#)

[Rôle Administrateur](#)

[Délai](#)

[Recréer le module](#)

Introduction

Ce document décrit comment dépanner le module cloud Secure Malware Analytics avec Cisco XDR.

Contribution de Javi Martinez, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cloud Secure Malware Analytics
- Cisco XDR

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Console cloud Secure Malware Analytics (compte d'utilisateur avec droits d'administrateur)
- Console Cisco XDR (compte d'utilisateur avec droits d'administrateur)

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Secure Malware Analytics Cloud est une plate-forme avancée et automatisée d'analyse des programmes malveillants et d'analyse des menaces de programmes malveillants dans laquelle les fichiers suspects ou les destinations Web peuvent être déclenchés sans impact sur l'environnement utilisateur.

Dans le cadre de l'intégration avec Cisco XDR, Secure Malware Analytics est un module de référence qui permet de basculer vers le portail Secure Malware Analytics pour collecter des informations supplémentaires sur les hachages de fichiers, les adresses IP, les domaines et les URL dans la banque de connaissances Secure Malware Analytics Cloud (SMA Cloud).

Reportez-vous au dernier Guide d'intégration du cloud Secure Malware Analytics,

- [Nuage NAM](#).
- [Cloud UE](#).

Dépannage

Licence

- Vérifiez que vous disposez d'une licence SMA appropriée pour accéder à la console Secure Malware Analytics Cloud

Mosaïques de module

- Vérifiez que vous avez sélectionné les vignettes appropriées pour le module cloud Secure Malware Analytics
Accédez au portail Cisco XDR > Tableau de bord > Bouton Personnaliser > Sélectionnez le module SMA Cloud > Ajouter les vignettes appropriées

Rôle Administrateur

- Vérifiez que vous disposez d'un compte Secure Malware Analytics avec le rôle Administrateur dans le portail Secure Malware Analytics
Accédez au portail Cisco XDR > Administration > Votre compte
- Vérifiez que vous disposez d'un compte SecureX avec des droits d'administrateur dans le portail SecureX
Accédez au portail Malware Analytics > Mon compte Malware Analytics

Remarque : si vous ne disposez pas du rôle Admin dans la console Secure Malware Analytics et la console Cisco XDR, votre administrateur peut modifier le rôle du compte directement à partir du

portail en question

Délai

- Vérifiez que l'horodatage est correctement défini sur le portail Cisco XDR.
Accédez à Cisco XDR portal > Dashboard > Timeframe option > Sélectionnez la période appropriée dans en fonction de l'activité SMA

Recréer le module

- Supprimez l'ancien module SMA et créez-en un nouveau.
Accédez à Secure Malware Analytics Cloud Console > Mon compte Malware Analytics > Clé API > Copier la clé API
Accédez au portail Cisco XDR > Modules d'intégration > Sélectionnez le module SMA Cloud > Ajouter la clé API et l'URL (Sélectionnez le cloud SMA) > Créer le tableau de bord

Remarque : seuls les utilisateurs disposant du rôle Administrateur de l'organisation ou Utilisateurs peuvent obtenir la clé API qui active le module d'intégration Secure Malware Analytics dans Cisco XDR.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.