# Problèmes connus de Cisco XDR

## Table des matières



## Introduction

Cet article présente les problèmes techniques connus de Cisco XDR.

Les problèmes techniques peuvent être reconnus par Cisco, en cours d'examen, en attente de résolution ou considérés comme fonctionnant comme prévu.

## Problèmes connus :

### Incidents

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

### Enquêtes

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

### Centre de contrôle

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

### Intégrations Cisco

1. Cisco XDR - Cisco Secure Firewall - Intégration complète

Détails : Pour assurer une intégration transparente entre Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) et Security Analytics and Logging (SAL), un mappage manuel est nécessaire. Ce processus implique de contacter le TAC Cisco pour effectuer les configurations et mappages nécessaires.

Solution : contactez le TAC pour vous aider à relier les comptes concernés et à assurer une intégration adéquate des systèmes.

Résolution attendue : À DÉTERMINER

## Intégrations de tiers

1.- Les clients Microsoft disposant de licences de type G ne peuvent pas utiliser les intégrations Microsoft XDR.

État : Fonctionnement tel que conçu

Détails : les droits de type G de Microsoft sont fournis en accès dans des environnements contrôlés pour les entités gouvernementales uniquement.

Étapes suivantes : Cisco collabore avec Microsoft pour comprendre les exigences d'intégration à l'environnement Microsoft GCC dans lequel les droits de type G Microsoft sont fournis. S'il est viable, Cisco XDR a l'intention de s'intégrer aux licences Microsoft de type G pour Microsoft Defender for Endpoint, O365 et EntraID.

Résolution attendue : Résolue, intégration disponible ici.

## Actifs

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

## Automatisation XDR

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

## Appareils/Capteurs

Aucun problème connu pour cette fonctionnalité XDR pour le moment.

## Client sécurisé

Afin de consulter les questions pour Secure Client, veuillez suivre l'article.

## XDR-Analytics

1. - Plusieurs adresses IP et/ou plusieurs noms d'hôtes peuvent être associés à un nom de périphérique unique dans XDR-A

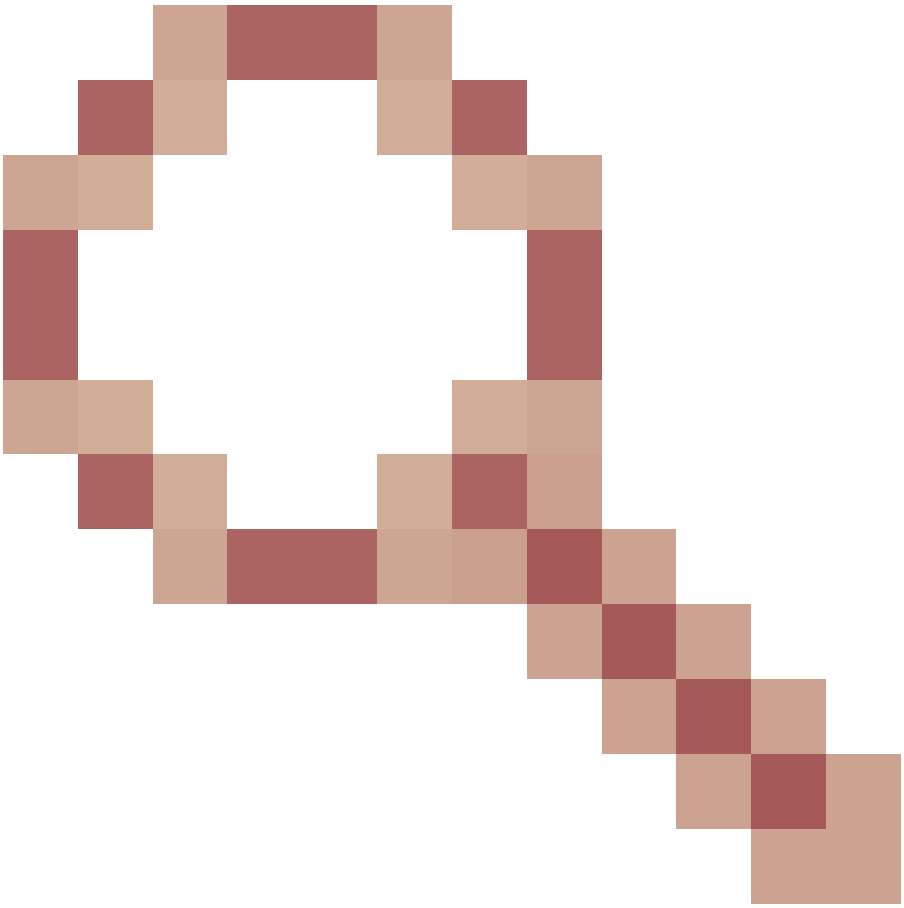
État : Non résolu/Différé

Détails: Plusieurs adresses IP actives peuvent être associées à un seul périphérique dans le portail SNA/XDR-A. Cela peut inclure les périphériques NVM et non-NVM. Certains périphériques ont également plusieurs noms d'hôte. Selon l'implémentation actuelle, l'enregistrement des périphériques peut avoir pour résultat qu'un périphérique a plus d'une adresse IP (emplacement). Certaines de ces adresses IP peuvent provenir du réseau domestique de l'utilisateur et entrer en collision avec les adresses IP du réseau de l'entreprise.

Solution : il n'y a pas de solution de contournement pour ce problème pour le moment, et le problème existe toujours dans l'architecture actuelle. Il est à espérer que ce problème pourra être mieux résolu à l'avenir, une fois que la nouvelle architecture sera mise en oeuvre, ce qui permettra de normaliser les activités réseau des deux sources ONA et NVM vers OCSF et de les regrouper.

Étapes suivantes : S/O

Résolution : À venir / À déterminer



CDET de suivi : CSCwo67299

## Problèmes résolus

1.- Cisco XDR - Lien d'intégration Cisco Secure Endpoint ne fonctionnant pas sur le portail Cisco XDR

État : Problème identifié et résolution en attente

Détails: Dans les onglets Admin > Integrations, le lien Secure Endpoint « Enable » est rompu. Une fois que nous avons cliqué sur le bouton d'activation, il est redirigé vers la page Threat Response et passe en boucle à la page du sélecteur d'organisation XDR au lieu d'accéder à la console Secure Endpoint.

Solution de contournement: L'intégration peut être effectuée à partir du portail Cisco Secure Endpoint

Étapes suivantes : Cisco s'efforce de mettre en oeuvre le correctif pour ce problème

Résolution attendue : ce problème a été résolu.

2.- Les règles d'automatisation des incidents XDR cessent de fonctionner de manière inattendue

État : problème identifié et résolution en attente

Détails : les règles d'automatisation des incidents optimisées par les workflows et les déclencheurs cessent de façon inattendue. Cela n'est pas indiqué dans l'interface utilisateur XDR, sauf lors de la vérification des mesures pour le temps d'exécution des workflows. Ce faisant, les clients verront des workflows réduits ou zéro s'exécuter, selon la durée pendant laquelle le problème a été en cours.

Étapes suivantes : Cisco a identifié ce problème comme étant un problème au sein du serveur principal XDR et s'efforce de le résoudre. Cisco prévoit également de mettre en oeuvre des fonctionnalités de surveillance et de suivi d'état supplémentaires pour éviter que ce problème ne se reproduise à l'avenir.

Solution : désactivez et réactivez la règle pour démarrer un redémarrage du déclenchement et du traitement de la règle de workflow.

Résolution attendue : Résolue.

3. - Cisco XDR-Analytics - Échec de l'installation ONA dans les environnements virtuels avec une erreur indiquant « échec de la vérification de la somme de contrôle »

État : problème identifié et résolution en attente

Détails: Lors du déploiement d'un capteur ONA dans un environnement virtuel, l'ISO ne parvient pas à terminer le processus d'installation et rencontre des erreurs.

Solution de contournement: Installez Ubuntu Server 24.04 indépendamment avec l'ISO Ubuntu et suivez les étapes d'installation avancées pour exécuter ONA en tant que service. Utilisez la compatibilité U2 7.0

Étapes suivantes : S/O

Résolution : Ce problème a été résolu dans la dernière version du capteur ONA

4.-La vignette MTTR sur le Control Center affiche des nombres inexacts d’incidents qui ont été

résolus à l’aide de l’un des nouveaux états tels que « Fermé : Faux positif", "Fermé : « Menace confirmée » ou autre.

État : Problème identifié et résolution en attente

Détails: De nouveaux états d'incidents ont été introduits le 15 janvier et la vignette ne prend pas ces états en considération. Les nouveaux états de résolution sont interprétés comme des travaux en cours. Par conséquent, même si cet incident a été clos à l'aide de l'un des nouveaux états, il est comptabilisé comme des travaux en cours.

Solution : Aucune

Étapes suivantes : Aucune

Résolution attendue : Résolue

Si vous devez contacter l'assistance Cisco, suivez les instructions fournies dans ce lien.

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.