Problèmes connus de Cisco XDR

Table des matières

Introduction

Problèmes identifiés

- Incidents
- Enquêtes
- Centre de contrôle
- Intégrations Cisco
- Cisco Identity Intelligence
- Intégrations de tiers
- Actifs
- Automatisation XDR
- Appareils/Capteurs
- Client sécurisé
- XDR Forensics
- XDR-Analytics
- Orbital

Problèmes résolus

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 identifiés

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

Cisco Identity Intelligence

1. Un petit nombre de clients disposent de modules Cisco Identity Intelligence en double

État : problème identifié et résolution en attente

Détails : Certains clients ont accidentellement provisionné un deuxième module lorsque Cisco Identity Intelligence a été intégré au produit XDR. Les clients affectés afficheront désormais des sources CII en double dans Asset Insights et des cibles d'automatisation CII en double.

Solution : S/O

Étapes suivantes : Ingénierie recherchant les causes/solutions

Résolution : le correctif pour la création de doublons sera publié dans la version 2.57. Un correctif pour les doublons existants est en cours d'étude.

Intégrations de tiers

1. Valeur de fournisseur de cloud manquante pour les flux OCI dans l'Observateur d'événements XDR-A

État : problème identifié et résolution en attente

Détails : la colonne du fournisseur de cloud dans l'Observateur d'événements XDR-A est actuellement vide pour les flux ingérés à partir d'OCI.

Solution : les utilisateurs peuvent toujours filtrer ces flux en tapant manuellement « OCI » dans le filtre de table.

Étapes suivantes : Cisco travaille à la mise en oeuvre d'un correctif pour ce problème.

Résolution : février 2026

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 vous référer à l'article.

XDR Forensics

1.- Exécution d'actions d'analyse XDR lorsque l'élément de l'incident XDR n'a pas été résolu mais que le module Analyse est installé

État : en cours d'investigation

Détails :L'analyse XDR dépend des ressources à résoudre dans un incident XDR avant que les actions d'analyse ne puissent être exécutées sur une ressource à partir de l'onglet Preuves d'un incident. Si Cisco XDR ne parvient pas à résoudre une ressource dans un incident XDR, cela empêche l'acquisition de preuves d'analyse XDR d'être disponible à partir de l'incident.

Solution : pivotez de la console XDR de Cisco vers XDR Forensics pour effectuer l'action d'analyse.Dans le menu de navigation gauche de Cisco XDR, cliquez sur Investigate > Forensics

Dans XDR Forensics, cliquez sur Assets dans le menu de navigation de gauche, sélectionnez l'actif approprié et obtenez les preuves et/ou l'action souhaitée.Sélectionnez le cas approprié dans le menu déroulant afin qu'il soit automatiquement associé à l'incident XDR.

Étapes suivantes : à déterminer

Résolution : à déterminer

CDETS de suivi:ID de bogue Cisco CSCwr69610

2.- Les opérations d'analyse XDR peuvent être bloquées par Cisco Secure Endpoint ou par l'action de réponse d'isolation des terminaux d'une autre solution de sécurité des terminaux.

État : en cours d'investigation

Détails : XDR Forensics peut être bloqué par Cisco Secure Endpoint, EDR ou l'application d'isolation d'un autre outil de sécurité de point d'extrémité.Assurez-vous que les exclusions et listes d'autorisation appropriées pour l'analyse XDR sont configurées sur l'outil de sécurité des terminaux.

Solution de contournement:

(Exemple basé sur la fonctionnalité d'isolation de Cisco Secure Endpoint, mais s'applique généralement à d'autres logiciels de sécurité de terminal)

Obtenir les adresses IP

· Effectuer une recherche/recherche de l'URL de votre locataire XDR Forensics (peut être obtenu en basculant dans XDR Forensics et en copiant l'URL à partir du navigateur (supprimez le https, et tout depuis la première barre oblique jusqu'à la fin)

· Notez toutes les adresses IP.

Ajouter une liste Isolation IP Allow

· Dans le produit de sécurité des terminaux, par exemple - Cisco Secure Endpoint, accédez à Outbreak Control > IP Block & Allow Lists

· Sélectionnez l'onglet des listes Isolation IP Allow. Si vous en avez déjà un, vous pouvez le mettre à jour. Sinon, utilisez le bouton « Create IP List » pour en ajouter un nouveau

· Donnez-lui un nom et une description, puis ajoutez les adresses IP de l'étape précédente

· Enregistrer la liste

Ajouter la liste verte à la stratégie

· Accédez à Cisco Secure Endpoint's Management > Policies

· Choisissez la stratégie que vous souhaitez mettre à jour et cliquez pour la modifier

· Accédez à Advanced Settings > Endpoint Isolation

· (Si nécessaire) Cochez la case Autoriser l'isolation des points de terminaison

· Dans les listes Isolation IP Allow Lists, sélectionnez la ou les listes à inclure

•Cliquez sur Save (enregistrer)

Étapes suivantes : à déterminer

Résolution : à déterminer

CDETS de suivi : ID de bogue Cisco CSCwr69614

3. - La modification des autorisations de rôle par défaut dans l'analyse XDR peut entraîner des erreurs non intuitives dans l'intégration de l'incident XDR et de l'analyse XDR pour les utilisateurs.

État : En cours d'investigation

Détails : Dans XDR version 2.5.6 (publiée le 17-12-2025), les administrateurs globaux de

XDR Forensics peuvent désormais modifier les autorisations de rôle utilisateur dans XDR Forensics pour un contrôle plus précis. Cependant, la modification des autorisations liées à l'acquisition de base, aux fonctions de l'interpréteur de commandes distant InterACT et au cas entraînera des erreurs d'autorisation dans l'intégration entre XDR Incident et XDR Forensics. Par exemple, un utilisateur dont le rôle a été modifié pour supprimer l'autorisation d'interpréteur de commandes distant verra toujours l'option d'action d'interpréteur de commandes distant dans l'interface utilisateur XDR, mais ne pourra pas établir la session d'interpréteur de commandes distant. Bien que documentée dans les notes de version de XDR Forensics, cette erreur due à la restriction des autorisations peut ne pas être intuitive pour un utilisateur sur la console XDR.

Solution :les administrateurs globaux d'analyse XDR doivent valider les autorisations modifiées avec la fonctionnalité de rôle d'utilisateur prévue avant de procéder à l'implémentation.

Étapes suivantes : à déterminer

Résolution : à déterminer

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. Il y a également eu des mises à jour de l'expiration des périphériques IP qui sont considérés comme étant associés à un nouveau nom d'hôte pour accélérer l'expiration.

Étapes suivantes : S/O

Résolution : À venir / À déterminer

Suivi des CDET : ID de bogue Cisco CSCwo67299

Orbital

1. Limite de déploiement pour les clients Secure Endpoint essentiels

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 : à déterminer

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: Les clients XDR de n'importe quel niveau qui possèdent également Secure Endpoint essentials peuvent être empêchés d'installer Orbital, car le connecteur Secure Endpoint désactive activement Orbital. Pour résoudre ce conflit, contactez le TAC.

Solution : S/O

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 reportez-vous aux 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'incident 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, reportez-vous aux 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.