Dépannage des utilisateurs Active Directory manquants dans le rapport de recherche d'activité dans Umbrella

Table des matières

Introduction

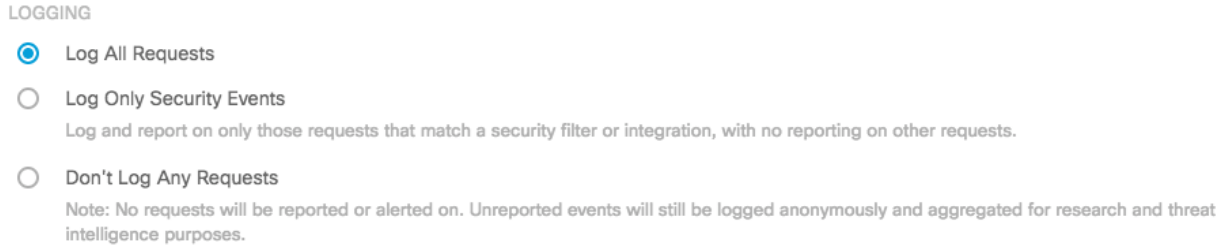
Ce document décrit le rapport de recherche d'activité dans Cisco Umbrella. Le rapport de recherche d'activité est un rapport presque en direct de toutes les requêtes DNS que vos utilisateurs font. Si vous avez configuré l'intégration Cisco Umbrella Active Directory (AD), vous pouvez vous attendre à ce que vos utilisateurs AD remplissent la colonne Identité dans votre recherche d'activité. Cependant, il existe des situations où les utilisateurs ne figurent pas dans la colonne Identité.

Résolution

Si vous pensez que vous devriez voir des utilisateurs AD directement dans la colonne Identité de la recherche d'activité, mais que vous ne les voyez pas, ou que vous en voyez quelques-uns, mais pas autant que vous le pensiez, voici quelques éléments à vérifier :

1. Sites et Active Directory
    - Vérifiez tous vos composants AD pour vous assurer qu'il n'y a pas d'erreurs ou de problèmes signalés. Si vous voyez des indicateurs d'état gris, orange ou rouge sur l'un des composants, obtenez ces informations et ouvrez un ticket d'assistance (umbrella-support@cisco.com).
        - Test de diagnostic d'un utilisateur affecté (un utilisateur qui n'apparaît pas dans la recherche d'activité)
        - Capture d'écran de la console de l'appliance virtuelle (VA), avec tous les messages d'erreur développés
        - Journaux d'audit du connecteur AD
2. Paramètres de journalisation
    - Dans les paramètres avancés de chaque stratégie, une section en bas concerne la quantité à consigner. Vous pouvez le définir sur :
        - Consigner toutes les demandes
        - Enregistrer uniquement les événements de sécurité

    - Ne pas consigner les demandes
- Si votre stratégie est actuellement définie sur « Enregistrer uniquement les événements de sécurité », cela peut expliquer pourquoi vous ne voyez pas autant de requêtes que vous le souhaitez, ou aucun résultat de la part de certains utilisateurs.



3. Priorité de stratégie correcte
    - Si une stratégie s'applique à une identité réseau qui est plus élevée dans la liste des stratégies que votre stratégie utilisateur AD, la stratégie Identité réseau va probablement s'appliquer. Cela signifie que dans la recherche d'activité, vous verrez le réseau comme étant l'identité signalée. Consultez également la documentation Cisco Umbrella sur les meilleures pratiques et la priorité des politiques.

Motif

Où la recherche d'activité obtient-elle l'« identité » ?

Lorsqu'une requête DNS arrive dans Umbrella, en supposant que votre intégration AD fonctionne comme prévu, ces informations sont transmises dans la requête :

- Adresse IP interne
- Hachage d'identité AD (utilisateur, hôte ou les deux)
- IP de sortie
- Domaine en cours de requête

Le hachage d'identité AD est ajouté à la requête par l'appliance virtuelle, à qui ces informations sont transmises, et l'adresse IP interne correspondante pour l'événement de connexion à partir du connecteur AD.

Cisco Umbrella utilise ensuite ces informations pour rechercher l'entreprise et déterminer la politique à appliquer. Si aucune stratégie n'est spécifiquement appliquée à vos utilisateurs AD, mais qu'une stratégie est appliquée à vos réseaux ou sites, Cisco Umbrella applique la stratégie en utilisant cette identité. Cela signifie que lorsque la requête, l'identité et la réponse sont signalées dans la recherche d'activité, l'identité qui a déclenché la stratégie qui est signalée. Les autres informations sont toujours balisées dans la demande, de sorte que vous pouvez toujours rechercher un utilisateur AD et obtenir l'activité qui signale un réseau en tant qu'identité. En outre, si vous exportez les données de la recherche d'activité dans un fichier CSV, toutes les informations d'identité associées à la requête s'affichent.

Additional Information

Si vous ne voyez toujours aucun utilisateur AD, veuillez contacter l'assistance (umbrella-

support@cisco.com), avec un résultat de test de diagnostic, et tous les journaux d'audit du connecteur AD qui sont pertinents.

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.