Secure Access Activity Search affiche des noms de règles INCONNUS

Table des matières

Problème

Au cours d'une migration Umbrella vers SSE, les événements de recherche d'activité d'accès sécurisé affichent le nom de la règle comme INCONNU au lieu d'afficher les règles de stratégie nommées. Ce comportement a été observé pour différents types de trafic, y compris le trafic autorisé tel que les requêtes vers chatgpt.com. La question était de savoir si ces entrées de nom de règle INCONNU indiquaient un problème de configuration de stratégie ou de migration nécessitant une correction.

Environnement

- Accès sécurisé Cisco (SSE)
- Organisation en cours de migration de Umbrella vers SSE
- Rapports de recherche d'activité d'accès sécurisé
- Trafic classé comme domaines nouvellement vus

Résolution

Le comportement Nom de règle INCONNU est attendu et normal pour les événements traités par la logique système d'accès sécurisé plutôt que par les règles créées/nommées par le client. Cela se produit généralement pour le trafic classé comme domaines nouvellement vus, où le domaine a été récemment vu au moment de la requête et est signalé comme tel dans les rapports d'activité de recherche d'activité ou de sécurité.

Interprétation des événements de recherche d'activité avec des noms de règles INCONNUS

Lorsque vous rencontrez des événements dont le nom de la règle est INCONNU, vérifiez ces champs d'événement pour déterminer la raison de l'application et confirmer l'application correcte de la stratégie :

- Action - Indique si le trafic a été autorisé ou bloqué
- Motif de blocage d'événement / Motif de blocage - Fournit des détails spécifiques sur l'application
- Catégories - Affiche la catégorisation du contenu (comme les domaines récemment vus)
- Domaine de destination/IP - Cible de la demande
- Identité utilisateur/source - Source du trafic
- Horodatage : moment où l'événement s'est produit

Si le champ Categories affiche Newly Seen Domains, alors UNKNOWN dans le champ rule-name est le comportement attendu et n'indique pas un échec de la migration ou une corruption de politique.

Étapes de validation d'un comportement inattendu

Si le trafic était censé correspondre à une règle nommée spécifique mais affiche UNKNOWN, collectez ces informations pour la validation du chemin de stratégie :

- 2-3 exemples d'horodatages d'événements
- Domaine/IP de destination pour chaque événement
- Identité utilisateur/source pour chaque événement

Ces informations peuvent être utilisées pour comparer le chemin de stratégie attendu au comportement réel de l'événement et déterminer si une étude plus approfondie est nécessaire.

Motif

Le nom de la règle UNKNOWN apparaît lorsque la logique système Secure Access traite le trafic plutôt que d'appliquer une règle de stratégie créée/nommée par le client. Il s'agit d'un comportement documenté pour certaines catégories de trafic, en particulier les domaines nouvellement vus, où les mécanismes intégrés de catégorisation et de gestion ont priorité sur les règles nommées lors de l'évaluation initiale du domaine.

Autres informations utiles

- Activer la sécurité des nouveaux domaines
- Assistance technique de Cisco et téléchargements

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.