Événements de sécurité basés sur le webhook are not Received at the On-prem HTTP Connector for SIEM Integration

Table des matières

Problème

Les événements de sécurité basés sur Webhook ne sont pas reçus au niveau du connecteur HTTP local pour l'intégration SIEM.

Environnement

- Produit : Cisco Secure Access (SSE)
- Technologie : Assistance pour les solutions - Création de rapports et consignation d'accès sécurisé
- Type d'intégration : intégration tierce basée sur Webhook
- Connecteur cible : connecteur HTTP sur site
- État du tableau de bord : chargement des intégrations tierces réussi dans Admin > Intégrations tierces

Résolution

Pour résoudre les problèmes de remise de webhook avec les intégrations tierces de Cisco Secure Access, configurez les règles de pare-feu pour autoriser le trafic HTTPS entrant à partir de ces plages IP source Cisco SSE.

Configuration de pare-feu requise

Autorisez le trafic HTTPS entrant de ces plages d'adresses IP source Cisco SSE vers votre connecteur local :

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

Ces plages d'adresses IP représentent les adresses IP partagées utilisées par Cisco SSE dans

les régions de l'Union européenne et des États-Unis pour la livraison du webhook.

Étapes de vérification

Étape 1 : vérifiez l'état de l'intégration tierce dans le tableau de bord SSE.

Accédez à Admin > Third Party Integrations dans votre tableau de bord SSE et vérifiez que les intégrations se chargent correctement pour votre organisation.

Étape 2 : Configurez les règles de pare-feu.

Mettez à jour votre pare-feu réseau et les pare-feu intermédiaires pour autoriser les connexions HTTPS entrantes des plages IP SSE fournies vers votre serveur de connecteurs sur site.

Étape 3 : Surveillez la livraison des événements webhook.

Après avoir implémenté les modifications du pare-feu, surveillez votre connecteur HTTP local pour vérifier que les événements webhook sont reçus de Cisco SSE.

Dépannage supplémentaire

Si les événements webhook ne sont toujours pas reçus après la configuration des règles de pare-feu :

- Vérifiez que le connecteur local est correctement configuré et qu'il écoute sur le port attendu.
- Vérifiez la connectivité réseau entre les adresses IP source SSE et le point d'extrémité de votre connecteur.
- Vérifiez la configuration de l'intégration webhook dans le tableau de bord SSE.
- Envisagez de planifier une session de dépannage en direct pour examiner la livraison du webhook en temps réel.

Motif

L'échec de la remise du webhook se produit lorsque les pare-feu réseau bloquent les connexions HTTPS entrantes entre les adresses IP source Cisco SSE et le connecteur HTTP local. Cisco SSE utilise des plages d'adresses IP spécifiques, allant de l'infrastructure partagée dans les régions de l'UE et des États-Unis à la fourniture d'événements webhook. Ces plages doivent être explicitement autorisées via des configurations de pare-feu pour la fourniture d'événements réussie.

Autres informations utiles

- 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.