Examiner ou contester les faux positifs IPS avec Umbrella

Table des matières

Introduction

Ce document décrit comment examiner ou contester les faux positifs du service de prévention des intrusions (IPS) avec Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Le système de prévention des intrusions de Cisco Umbrella détecte (et bloque éventuellement) les paquets qui sont considérés comme associés à une menace connue, une vulnérabilité, mais aussi simplement lorsque le format du paquet est inhabituel.

Les administrateurs choisissent la liste de signatures IPS utilisée pour détecter les menaces en fonction des listes par défaut suivantes :

- Connectivité sur la sécurité
- Sécurité et connectivité équilibrées
- La sécurité sur la connectivité
- Détection maximale

Il est important de se rappeler que la liste de signatures choisie peut avoir un impact important sur le nombre de faux positifs IPS rencontrés. Les modes les plus sécurisés (tels que la détection maximale et la sécurité sur connectivité) sont censés créer des détections IPS indésirables car ils mettent l'accent sur la sécurité. Les modes les plus sécurisés ne sont recommandés que lorsque la sécurité totale est requise, et l'administrateur doit anticiper la nécessité de surveiller et d'examiner un grand nombre d'événements IPS.

Pour plus d'informations sur les différents modes, consultez la documentation IPS.

Examiner les détections IPS

Utilisez la recherche d'activité sur le tableau de bord Umbrella pour afficher les événements IPS. Pour chaque événement, il existe deux informations importantes :

- ID/Catégorie/Nom de signature IPS. Recherche possible sur https://snort.org
- Numéro CVE (le cas échéant). Recherche possible sur https://www.cve.org/

Toutes les détections IPS n'indiquent pas une attaque/exploitation connue. La plupart des signatures (en particulier en mode de détection maximale) indiquent simplement la présence d'un certain type de trafic ou une violation de protocole. Il est important d'examiner les sources d'informations mentionnées précédemment ainsi que d'autres détails sur l'événement (comme la source/destination) pour déterminer si l'événement nécessite une enquête plus approfondie de votre équipe de sécurité.

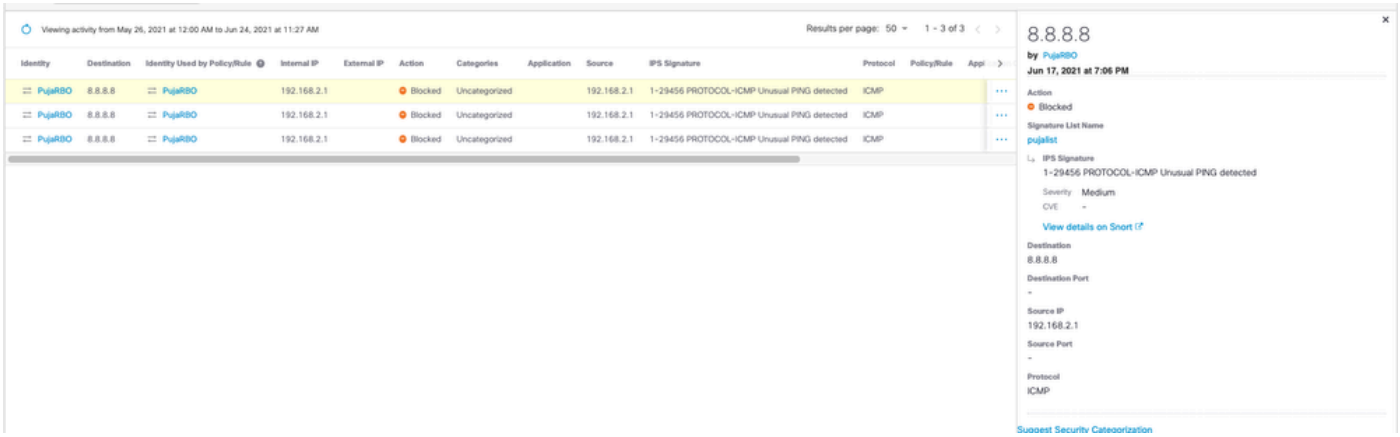
La catégorie de signature peut être utile pour fournir un contexte supplémentaire sur le type de détection IPS. Consultez les catégories disponibles sur snort.org.

Violations de protocole

Dans cet exemple, un événement IPS est lié à cette signature :
https://www.snort.org/rule_docs/1-29456

La description de la signature est la suivante :

"La règle recherche le trafic PING entrant dans le réseau qui ne respecte pas le format normal d'une requête PING."



4403885889428

Dans ce cas, la règle Snort ne détecte pas nécessairement une attaque particulière, mais détecte plutôt un paquet ICMP mal formé qui a été bloqué. D'après les informations disponibles sur snort.org et d'autres détails sur l'événement (comme la source/destination), l'administrateur peut décider que cet événement ne nécessite pas d'enquête supplémentaire

Compatibilité des applications

Certaines applications légitimes ne sont pas compatibles avec les signatures IPS, en particulier lorsque les modes les plus agressifs (détection maximale) sont configurés. Dans ces scénarios, l'application peut être bloquée pour les raisons décrites dans la section Violation du protocole. L'application peut utiliser un protocole de manière inattendue ou utiliser un protocole personnalisé sur un port qui est normalement réservé à un autre trafic.

Même si l'application est légitime, ces détections sont souvent valides et ne peuvent pas toujours être corrigées par Cisco.

Si une application légitime est bloquée par IPS, Umbrella recommande de contacter le fournisseur de l'application avec les détails de l'événement/de la signature. La compatibilité des applications tierces avec les signatures IPS doit être testée à l'adresse snort.org.

Il n'est actuellement pas possible d'exclure une application/destination individuelle de l'analyse IPS.

Désactivation des signatures IPS

Si une signature provoque des problèmes de compatibilité avec une application tierce, elle peut être désactivée (temporairement ou définitivement). Cela ne doit être fait que lorsque vous faites confiance à l'application et que vous avez déterminé que la valeur de l'application l'emporte sur les avantages de sécurité de la signature spécifique.

Suivez les étapes de la documentation Ajouter une liste de signatures personnalisée pour obtenir des informations sur la création d'une liste de signatures personnalisée. Vous pouvez utiliser vos paramètres actuels comme modèle, puis désactiver les règles souhaitées en les définissant sur Log Only ou Ignore.

Soutien

Événements historiques

Umbrella Support n'est pas en mesure de fournir des détails supplémentaires sur l'historique des événements IPS. Les événements IPS vous informent que le trafic ne correspond pas à la signature IPS. Les détails de la signature sont disponibles publiquement sur snort.org. Umbrella ne stocke pas de copie du trafic/des paquets bruts et n'est donc pas en mesure de fournir davantage de contexte ou de confirmation sur la nature d'un événement IPS.

Problèmes IPS / faux positifs

Si vous souhaitez contester un problème IPS actuel (tel qu'un faux positif), veuillez contacter l'assistance Umbrella.

Afin d'étudier ces problèmes, une capture de paquets est requise par Umbrella Support. Le contenu brut des paquets est nécessaire pour déterminer comment le trafic a déclenché la détection IPS. Vous devez être en mesure de répliquer le problème afin de générer la capture de paquets.

Avant de créer un ticket, utilisez un outil tel que Wireshark pour générer la capture de paquets lors de la réplication du problème. Des instructions sont disponibles dans notre base de connaissances.

L'assistance Umbrella peut également vous aider à générer la capture de paquets. Ils doivent planifier un moment où le problème avec l'utilisateur ou l'application concerné peut être recréé.

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.