Accordez l'IPS pour la prévention de faux positif utilisant le filtre d'action d'événement

Contenu

Introduction

Ce document fournit l'étape nécessaire afin d'accorder le Système de prévention d'intrusion (IPS) pour la prévention de faux positif utilisant le gestionnaire de périphériques IPS (IDM) ou le Manager Express IPS (IME). Le faux positif accordant sur l'IPS est réalisé par une caractéristique appelée le filtre d'Event Action (EAF).

Avant de commencer

Conditions requises

Les lecteurs de ce document devraient avoir la connaissance du Cisco IPS.

Composants utilisés

Les informations dans ce document ne sont pas basées sur le matériel et les versions de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Compréhension d'EAFs

EAFs sont configurés principalement pour l'accord de faux positif. L'EAF fournit la capacité de faire ne pas prendre une signature particulière a désiré des actions pour un sous-ensemble du

trafic.

EAFs sont utile dans les situations où on l'exige pour remplir de plusieurs conditions, comme :

- La signature X n'agit pas y pour un sous-réseau désiré du trafic.
- La signature X agit y pour tout autre trafic.

EAFs sont utile en faisant face au déclenchement bénin d'une signature.

Configuration

Exemple : Événement de faux positif : Déclencheurs de la signature 1300 pour le trafic provenant et aux hôtes de confiance connus.

Remarque: C'est juste un exemple pour la démonstration seulement. Si vous êtes incertain, qu'un événement particulier dû au déclencheur de signature soit bénin ou pas, entrez en contact avec le support technique de Cisco pour l'analyse approfondie.

Remarque: Référez-vous aux signatures de Système de protection contre les intrusions Cisco pour des informations supplémentaires sur des signatures IPS.

Procédez comme suit :

1. Vérifiez les actions par défaut pour la signature (1300, dans cet exemple) pour laquelle l'EAF doit être configuré.Les actions par défaut de la signature 1300 incluent l'**alerte de produit** et **refusent l'en ligne de connexion**.
2. Identifiez les hôtes pour lesquels cette signature ne devrait pas se déclencher. Par exemple, vous ne voulez pas que la signature se déclenche pour le trafic provenant un sous-réseau de confiance, tel que 10.1.1.1-10.1.1.254.
3. Créez un EAF pour les critères décrits dans l'étape 2 :D'IDM/IME, allez à la **configuration >** aux **stratégies >** aux **stratégies IPS**. Cliquez sur l'onglet de **filtres d'action d'événement**. Sous cet onglet, cliquez sur Add.Cette fenêtre est affichée :Configurez les divers champs tels que l'**ID de nom**, de **signature**, l'**IP d'attaquant**, etc.Cliquez sur l'icône à la droite des **actions de soustraire le** champ afin d'ouvrir la zone de dialogue d'actions d'éditer.Dans cette fenêtre, vous pouvez spécifier les actions de signature que vous ne voulez pas que l'IPS exécute.**Remarque:** Afin de sélectionner correctement des actions de signature que vous voulez soustraire, vous devez comprendre les actions par défaut de signatures comme décrit dans l'étape 1.Dans cet exemple, nous avons choisi l'**alerte de produit** et **refusons l'en ligne de connexion**.L'IPS ne prendra pas ces mesures si les 1300 déclencheurs de signature pour le trafic provenant 10.1.1.1-10.1.1.254.Pour tout autre trafic, l'action par défaut de signature de l'**alerte de produit** et **refusent l'en ligne de connexion** s'appliquera toujours.Après que vous choisissiez l'alerte de produit et refusiez l'en ligne de paquet, vous verrez ces actions remplir au bas de l'écran EAF :Cliquez sur OK, et puis **appliquez** afin de sauvegarder les modifications.

Pour la configuration du filtre d'action d'événement utilisant le CLI, référez-vous à la section d'interface de ligne de commande IPS à la page de guides de configuration. Du guide de configuration compétent, cliquez sur **en configurant des règles d'action d'événement**, et recherchez « configurer des filtres d'action d'événement ».

Informations connexes

- Support et documentation techniques - Cisco Systems