Adaptation de la prévention des intrusions à vos ressources réseau

Les rubriques suivantes décrivent comment utiliser les règles recommandées par Cisco :

À propos des règles recommandées par Cisco

Vous pouvez utiliser les recommandations de règles de prévention des intrusions pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources. Cela vous permet d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

Le système formule un ensemble individuel de recommandations pour chaque politique de prévention des intrusions. Il recommande généralement des modifications d'état de règles pour les règles de texte standard et les règles d'objet partagé. Cependant, il peut également recommander des modifications pour les règles de préprocesseur et de décodeur.

Lorsque vous générez des recommandations d'état de règles, vous pouvez utiliser les paramètres par défaut ou configurer des paramètres avancés. Les paramètres avancés vous permettent de :

- Redéfinir les hôtes de votre réseau que le système surveille pour détecter les vulnérabilités
- Influencer les règles recommandées par le système en fonction du surdébit des règles
- Préciser s'il faut générer des recommandations pour désactiver les règles

Vous pouvez également choisir d'utiliser les recommandations immédiatement ou de les examiner (ainsi que les règles concernées) avant de les accepter.

Choisir d'utiliser les états de règles recommandés ajoute une couche de recommandations Cisco en lecture seule à votre politique de prévention des intrusions, choisir de ne pas utiliser les états de règles recommandés supprime la couche.

Le système ne modifie pas les états de règles que vous définissez manuellement :

- La définition manuelle des états de règles spécifiées *avant* de générer des recommandations empêche le système de modifier les états de ces règles à l'avenir.
- La définition manuelle des états de règles spécifiées *après* la génération de recommandations remplace les états recommandés de ces règles.

Astuces Le rapport sur les politiques de prévention des intrusions peut inclure une liste de règles avec des états de règles différents de l'état recommandé.

Lorsque vous affichez la page des règles filtrées par les recommandations, ou après avoir accédé à la page Rules (Règles) directement à partir du panneau de navigation ou de la page Policy Information (Renseignements sur les politiques), vous pouvez définir manuellement l'état des règles, trier les règles et effectuer toute autre action disponible dans la page Rules, telle que que la suppression de règles, la définition de seuils de règles, etc.

Remarque Talos Intelligence Group détermine l'état approprié de chaque règle des politiques fournies par le système. Si vous utilisez une politique fournie par le système comme politique de base et que vous permettez au système de définir vos règles selon l'état de règle recommandé par Cisco, les règles de votre politique de prévention des intrusions correspondent aux paramètres recommandés par Cisco pour vos ressources réseau.

Règles recommandées et multilocalisation de détention

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, si vous activez cette fonctionnalité dans une politique d'intrusion dans un domaine ancêtre, le système génère des recommandations en utilisant les données de tous les domaines enfants descendants. Cela peut activer des règles d'intrusion adaptées aux actifs qui peuvent ne pas exister dans tous les domaines enfants, ce qui peut affecter les performances.

Paramètres par défaut pour les recommandations de Cisco

Lorsque vous générez des recommandations Cisco, le système recherche dans votre politique de base des règles qui protègent contre les vulnérabilités associées à vos actifs de réseau et identifie l'état actuel des règles de votre politique de base. Le système recommande ensuite des états de règles et, si vous le souhaitez, définit les règles sur les états recommandés.

Le système effectue l'analyse de base suivante pour générer des recommandations :

Tableau 1 : Recommandations sur l'état des règles en fonction des vulnérabilités

La règle protège-t-elle les ressources découvertes?	État de la règle de la politique de base	État de la règle de recommandation
Oui	Désactivé	Générer des événements
	Générer des événements	Générer des événements
	Abandonner et générer des événements	Abandonner et générer des événements

La règle protège-t-elle les ressources découvertes?	État de la règle de la politique de base	État de la règle de recommandation
Non	N'importe lequel	Désactivé

Notez les éléments suivants dans le tableau :

- Si une règle est désactivée dans la politique de base ou définie sur Générer des événements, l'état recommandé est toujours Générer des événements.

  Par exemple, si la politique de base est Aucune règle active, dans laquelle toutes les règles sont désactivées, il n'y aura aucune recommandation d'abandon et de génération d'événements.

- Les recommandations de suppression et de génération d'événements ne sont formulées que pour les règles déjà définies comme Abandon et génération d'événements dans la politique de base.

  Si vous souhaitez qu'une règle soit définie comme Supprimer et Générer des événements et que la règle a été désactivée ou définie comme Générer des événements dans la politique de base, vous devez réinitialiser manuellement l'état de la règle.

Lorsque vous générez des recommandations sans modifier les paramètres avancés pour les règles recommandées par Cisco, le système recommande des modifications d'état des règles pour tous les hôtes de l'ensemble de votre réseau découvert.

Par défaut, le système génère des recommandations uniquement pour les règles avec un surdébit faible ou moyen, et génère des recommandations pour désactiver les règles.

Le système ne recommande pas d'état de règle pour une règle de prévention des intrusions qui repose sur une vulnérabilité que vous désactivez à l'aide de la fonction de qualification de l'impact.

Le système vous recommande toujours d'activer une règle locale associée à une vulnérabilité tierce mappée à un hôte.

Le système ne fait pas de recommandations d'état pour les règles locales non mappées.

Sujets connexes

Mappages des produits tiers

Paramètres avancés pour les recommandations de Cisco

Inclure toutes les différences entre les recommandations et les états des règles dans les rapports de stratégie

Par défaut, un rapport de politique de prévention des intrusions répertorie les règles activées de la politique, c'est-à-dire les règles définies pour générer des événements ou pour supprimer et générer des événements. L'activation de l'option **Inclure toutes les différences** répertorie également les règles dont les états recommandés diffèrent de leurs états enregistrés. Pour en savoir plus sur les rapports sur les politiques, consultez À propos du déploiement de la configuration.

Réseaux à examiner

Spécifie les réseaux surveillés ou les hôtes individuels à examiner pour les recommandations. Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux.

Les listes d'adresses à l'intérieur des hôtes que vous spécifiez sont reliées par une opération OU, à l'exception des négations, qui sont reliées par une opération ET après que toutes les opérations OU ont été calculées.

Si vous souhaitez adapter dynamiquement le traitement actif des règles pour des paquets spécifiques en fonction des informations sur l'hôte, vous pouvez également activer Mises à niveau des profils adaptatifs.

Seuil de recommandation (par surdébit de règle)

Empêche le système de recommander ou d'activer automatiquement des règles de prévention des intrusions avec un surdébit plus élevé que le seuil que vous choisissez.

Le surdébit est basé sur l'impact potentiel de la règle sur les performances du système et sur la probabilité que la règle génère de faux positifs. L'autorisation de règles avec un surdébit plus élevé entraîne généralement plus de recommandations, mais peut affecter les performances du système. Vous pouvez afficher l'évaluation de surdébit d'une règle dans la vue détaillée de la règle sur la page des règles de prévention des intrusions.

Notez que le système ne prend pas en compte le surdébit des règles dans les recommandations pour désactiver les règles. En outre, les règles locales sont considérées comme sans surdébit, sauf si elles sont mappées à une vulnérabilité tierce.

La génération de recommandations pour les règles avec le taux de surdébit à un paramètre particulier ne vous empêche pas de générer des recommandations avec un surdébit différent, puis de générer à nouveau des recommandations pour le paramètre de surdébit d'origine. Vous obtenez les mêmes recommandations d'état de règles pour chaque paramètre de surdébit chaque fois que vous générez des recommandations pour le même ensemble de règles, quel que soit le nombre de fois que vous générez des recommandations ou le nombre de paramètres de surdébit différents avec lesquels vous générez. Par exemple, vous pouvez générer des recommandations avec un surdébit défini à moyen, puis à élevé, puis à nouveau à moyen; Si les hôtes et les applications de votre réseau n'ont pas changé, les deux ensembles de recommandations avec un surdébit défini à moyen sont les mêmes pour cet ensemble de règles.

Accepter les recommandations pour désactiver les règles

Spécifie si le système désactive les règles de prévention des intrusions en fonction des recommandations de Cisco.

L'acceptation des recommandations pour désactiver les règles restreint la couverture de vos règles. L'omission des recommandations pour désactiver les règles augmente votre couverture de règles.

Sujets connexes

Mises à jour des profils d'utilisateurs adaptatifs et règles recommandées par Cisco

Génération et application de recommandations Cisco

Le démarrage ou l'arrêt de l'utilisation des recommandations Cisco peuvent prendre plusieurs minutes, en fonction de la taille de votre réseau et de l'ensemble de règles de prévention des intrusions.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, si vous activez cette fonctionnalité dans une politique d'intrusion dans un domaine ancêtre, le système génère des recommandations en utilisant les données de tous les domaines enfants descendants. Cela peut activer des règles d'intrusion adaptées aux actifs qui peuvent ne pas exister dans tous les domaines enfants, ce qui peut affecter les performances.

Avant de commencer

- Les recommandations deCisco comportent les exigences suivantes :
  - Licence de défense contre les menaces— IPS
  - Licence traditionnelle—Protection
  - Rôles utilisateur à Admin ou Administrateur d'intrusion
- Configurez une politique de découverte de réseau avant de commencer les étapes. Configurez la politique de découverte de réseau pour définir des hôtes internes afin que les recommandations de Cisco soient appropriées. Consultez, Personnalisation de la découverte de réseau.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions Snort 2, cliquez sur Recommandations de **Cisco**.

Étape 2 (Facultatif) Configurer les paramètres avancés, voir Paramètres avancés pour les recommandations de Cisco, à la page 3.

Étape 3 Générer et appliquer les recommandations

- **Generate and Use Recommendations** : (Générer et utiliser les recommandations) Génère des recommandations et modifie l'état des règles en conséquence. Disponible uniquement si vous n'avez jamais généré de recommandations.
- **Generate Recommendations**(générer des recommandations) : Que vous utilisiez ou non des recommandations, génère de nouvelles recommandations, mais ne modifie pas l'état des règles en conséquence.
- **Update Recommendations** (Mettre à jour les recommandations) : Si vous utilisez des recommandations, génère des recommandations et modifie l'état des règles en conséquence. Sinon, génère de nouvelles recommandations sans modifier l'état des règles.
- **Use Recommendations**(utiliser les recommandations) : Modifie l'état des règles pour qu'elles correspondent à toutes les recommandations non mises en œuvre.
- **Do Not Use Recommendations** (Ne pas utiliser les recommandations) : Arrête l'utilisation des recommandations. Si vous avez modifié manuellement l'état d'une règle avant d'appliquer les recommandations, l'état de la règle revient à la valeur que vous lui avez donnée. Sinon, l'état de la règle revient à sa valeur par défaut.

Lorsque vous générez des recommandations, le système affiche un résumé des modifications recommandées. Pour afficher une liste des règles pour lesquelles le système recommande un changement d'état, cliquez sur **View** (afficher) à côté du nouvel état de règle proposé.

Étape 4 Évaluer et ajuster les recommandations que vous avez mises en œuvre.

Même si vous acceptez la plupart des recommandations de Cisco, vous pouvez remplacer les recommandations individuelles en définissant les états des règles manuellement. voir Définition des états des règles d'intrusion.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Détection de script

La détection de script empêche le blocage trop tardif des défaillances de prévention des intrusions à l'aide d'une inspection partielle. Lorsque des fichiers HTML sont transférés entre un client et un serveur, ces fichiers peuvent contenir des scripts malveillants, tels que JavaScript, pour lancer une attaque. Lorsque de tels scripts malveillants sont trouvés, l'inspection partielle permet à toute règle IPS de correspondre au script malveillant, et l'inspecteur efface ce segment de données grâce à l'inspection et à la détection. Le fichier malveillant n'atteint jamais sa destination. Cette fonctionnalité prend en charge le trafic HTTP/1 et HTTP/2.

Cette fonction est activée par défaut. Pour la désactiver, définissez **`http_inspect.script_detection=true`** sur false (faux).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.