IPS 5.x et version ultérieure : Ajustement de la signature avec le filtre d'actions d'événements à l'aide de l'interface CLI et d'IDM

Contenu

Introduction

Ce document décrit comment accorder la signature avec le filtre d'action d'événement dans le Système de protection contre les intrusions Cisco (IPS) avec l'interface de ligne de commande (CLI) et le gestionnaire de périphériques d'ID (IDM).

Conditions préalables

Conditions requises

Ce document suppose que le Cisco IPS est installé et fonctionne correctement.

Composants utilisés

Les informations dans ce document sont basées sur le périphérique de la gamme Cisco 4200 IDS/IPS qui exécute la version de logiciel 5.0 et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Filtres d'action d'événement

Compréhension des filtres d'action d'événement

Des filtres d'action d'événement sont traités pendant qu'un liste dans un certain ordre et vous pouvez déplacer des filtres en haut ou en bas dans la liste.

Les filtres ont permis le capteur d'exécuter certaines actions en réponse à l'événement sans exiger du capteur d'exécuter toutes les actions ou de retirer l'événement entier. Les filtres fonctionnent à côté de la suppression des actions d'un événement. Un filtre qui enlève toutes les actions d'un événement efficacement consomme l'événement.

Note: Quand vous filtrez des signatures de champ, Cisco recommande que vous ne filtriez pas les adresses de destination. S'il y a de plusieurs adresses de destination, seulement la dernière adresse est utilisée pour apparier le filtre.

Vous pouvez configurer des filtres d'action d'événement pour enlever des actions spécifiques d'un événement ou pour jeter un événement entier et pour empêcher une transformation plus ultérieure par le capteur. Vous pouvez utiliser les variables d'action d'événement que vous avez définies aux adresses de groupe pour vos filtres. Pour la procédure sur la façon dont configurer des variables d'action d'événement, voyez ajouter, éditer, et supprimer la section de variables d'action d'événement.

Note: Vous devez préfacer la variable avec un symbole dollar ($) afin d'indiquer que vous utilisez une variable plutôt qu'une chaîne. Autrement, vous recevez la `mauvaises source et erreur de destination`.

Configuration de filtres d'action d'événement utilisant le CLI

Terminez-vous ces étapes afin de configurer des filtres d'action d'événement :

1. Ouvrez une session au CLI avec un compte qui a des privilèges d'administrateur.
2. Écrivez le sous-mode de règles d'action d'événement :
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. Créez le nom du filtre :
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   Employez **name1, name2**, et ainsi de suite afin de nommer vos filtres d'action d'événement. Utilisez le **commencer | extrémité | inactif | avant | après que** mots clé afin de spécifier où vous voulez insérer le filtre.
4. Spécifiez les valeurs pour ce filtre :Spécifiez la plage d'ID de signature :
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   Le par défaut est de 900 à 65535.Spécifiez la plage d'ID de subsignature :
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

Le par défaut est de 0 à 255.Spécifiez la plage d'adresses d'attaquant :
```
sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
```

Le par défaut est 0.0.0.0 à 255.255.255.255.Spécifiez la plage d'adresses de victime :
```
sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
```

Le par défaut est 0.0.0.0 à 255.255.255.255.Spécifiez la plage de port de victime :
```
sensor(config-eve-fil)#victim-port-range 0-434
```

Le par défaut est de 0 à 65535.Spécifiez la pertinence de SYSTÈME D'EXPLOITATION :
```
sensor(config-eve-fil)#os-relevance relevant
```

Le par défaut est de 0 à 100.Spécifiez la plage d'évaluation du risque.
```
sensor(config-eve-fil)#risk-rating-range 85-100
```

Le par défaut est de 0 à 100.Spécifiez les actions de retirer :
```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

Si vous filtrez une action de refuser, placez le pourcentage de refusent des actions que vous voulez :
```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

Le par défaut est 100.Spécifiez l'état du filtre à désactivé ou à activer.
```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

Le par défaut est activé.Spécifiez l'arrêt sur le paramètre de correspondance.
```
sensor(config-eve-fil)#stop-on-match {true | false}
```

Vrai dit le capteur de cesser le traitement des filtres si cet élément s'assortit. **Faux** dit le capteur de continuer à traiter des filtres même si cet élément s'assortit.Ajoutez tous les commentaires que vous voulez employer afin d'expliquer ce filtre :
```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. Vérifiez les configurations pour le filtre :
```
sensor(config-eve-fil)#show settings
 NAME: name1

   ----------------------------------------------

      signature-id-range: 1000-10005 default: 900-65535

      subsignature-id-range: 1-5 default: 0-255

      attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255

      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255

      attacker-port-range: 0-65535 <defaulted>

      victim-port-range: 1-343 default: 0-65535

      risk-rating-range: 85-100 default: 0-100

      actions-to-remove: reset-tcp-connection default:

      deny-attacker-percentage: 90 default: 100
```

```
      filter-item-status: Enabled default: Enabled

      stop-on-match: True default: False

      user-comment: NEW FILTER default:

      os-relevance: relevant default: relevant|not-relevant|unknown

   ------------------------------------------------

senor(config-eve-fil)#
```

6. Afin d'éditer un filtre existant :

```
sensor(config-eve)#filters edit name1
```

7. Éditez les paramètres et voyez les étapes 4a par le pour en savoir plus 4l.
8. Afin de déplacer un filtre en haut ou en bas dans la liste de filtre :

```
sensor(config-eve-fil)#exit
sensor(config-eve)#filters move name5 before name1
```

9. Vérifiez que vous avez déplacé les filtres :

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

 ------------------------------------------------

   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)

   ------------------------------------------------

   ACTIVE list-contents

   ------------------------------------------------

      NAME: name5

      ------------------------------------------------

         signature-id-range: 900-65535 <defaulted>

         subsignature-id-range: 0-255 <defaulted>

         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         attacker-port-range: 0-65535 <defaulted>

         victim-port-range: 0-65535 <defaulted>

         risk-rating-range: 0-100 <defaulted>

         actions-to-remove: <defaulted>

         filter-item-status: Enabled <defaulted>

         stop-on-match: False <defaulted>

         user-comment: <defaulted>

      ------------------------------------------------
```

```
   ------------------------------------------------
   NAME: name1
   ------------------------------------------------
      signature-id-range: 900-65535 <defaulted>
      subsignature-id-range: 0-255 <defaulted>
      attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 0-65535 <defaulted>
      risk-rating-range: 0-100 <defaulted>
      actions-to-remove: <defaulted>
      filter-item-status: Enabled <defaulted>
      stop-on-match: False <defaulted>
      user-comment: <defaulted>
   ------------------------------------------------
   ------------------------------------------------
   NAME: name2
   ------------------------------------------------
      signature-id-range: 900-65535 <defaulted>
      subsignature-id-range: 0-255 <defaulted>
      attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 0-65535 <defaulted>
      risk-rating-range: 0-100 <defaulted>
      actions-to-remove: <defaulted>
      filter-item-status: Enabled <defaulted>
      stop-on-match: False <defaulted>
      user-comment: <defaulted>
   ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
```

```
    INACTIVE list-contents

    ----------------------------------------------

  ------------------------------------------------

  sensor(config-eve)#
```

10. Afin de déplacer un filtre à la liste inactive :

```
sensor(config-eve)#filters move name1 inactive
```

11. Vérifiez que le filtre s'est déplacé à la liste inactive :

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

    ----------------------------------------------

    INACTIVE list-contents

    ----------------------------------------------

        ----------------------------------------------

        NAME: name1

        ----------------------------------------------

            signature-id-range: 900-65535 <defaulted>

            subsignature-id-range: 0-255 <defaulted>

            attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

            attacker-port-range: 0-65535 <defaulted>

            victim-port-range: 0-65535 <defaulted>

            risk-rating-range: 0-100 <defaulted>

            actions-to-remove: <defaulted>

            filter-item-status: Enabled <defaulted>

            stop-on-match: False <defaulted>

            user-comment: <defaulted>

        ----------------------------------------------

        ----------------------------------------------

sensor(config-eve)#
```

12. Quittez le sous-mode de règles d'action d'événement :

```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```

13. Appuyez sur **entrent** afin d'appliquer vos modifications ou entrer **aucun** afin de les jeter.

Configuration de filtres d'action d'événement utilisant IDM

Terminez-vous ces étapes afin d'ajouter, éditer, supprimer, activer, désactiver, et déplacer des

filtres d'action d'événement :

1. Ouvrez une session à IDM avec un compte qui a des privilèges d'administrateur ou d'opérateur.
2. Choisissez la **configuration > les stratégies > les règles d'action d'événement > le rules0 > les filtres d'action d'événement** si la version de logiciel est 6.x. Pour la version de logiciel 5.x, choisissez les **filtres d'action de règles > d'événement d'action de configuration > d'événement.**L'onglet de filtres d'action d'événement apparaît comme affiché.
3. Cliquez sur Add afin d'ajouter un filtre d'action d'événement.La boîte de dialogue de filtre d'action d'événement d'ajouter apparaît.
4. Dans la zone d'identification, écrivez un nom comme **name1** pour le filtre d'action d'événement.Un nom par défaut est fourni, mais vous pouvez le changer à un nom plus signicatif.
5. Dans le domaine actif, cliquez sur la case d'option d'**oui** afin d'ajouter ce filtre à la liste de sorte qu'elle la prenne effet sur des événements de filtrage.
6. Dans le domaine activé, cliquez sur la case d'option d'**oui** afin d'activer le filtre.**Note**: Vous devez également cocher la case de **filtres d'action d'événement d'utilisation** sur l'onglet de filtres d'action d'événement ou aucun des filtres d'action d'événement ne devient activé indépendamment de si vous cochez la case d'**oui** dans la boîte de dialogue de filtre d'action d'événement d'ajouter.
7. Dans le domaine d'ID de signature, écrivez les id de signature de toutes les signatures auxquelles ce filtre devrait être appliqué.Vous pouvez utiliser une liste, par exemple, 1000, 1005, ou une plage, par exemple, **1000-1005** ou une des variables de SIG si vous les définissiez sur la préface de tableau de variables d'événement la variable avec $.
8. Dans le domaine d'ID de SubSignature, écrivez les id de subsignature des subsignatures auxquels ce filtre devrait être appliqué. Par exemple, **1-5**.
9. Dans la zone adresse d'attaquant, écrivez l'adresse IP de l'hôte de source.Vous pouvez utiliser une des variables si vous les définissiez sur la préface de tableau de variables d'événement la variable avec $. Vous pouvez également écrire une plage d'adresses, par exemple, **10.89.10.10-10.89.10.23**. Le par défaut est 0.0.0.0-255.255.255.255.
10. Dans le domaine de port d'attaquant, introduisez le numéro de port utilisé par l'attaquant afin d'envoyer le paquet offensant.
11. Dans la zone adresse de victime, écrivez l'adresse IP de l'hôte réceptif.Vous pouvez utiliser une des variables si vous les définissiez sur la préface de tableau de variables d'événement la variable avec $. Vous pouvez également écrire une plage d'adresses, par exemple, **192.56.10.1-192.56.10.255**. Le par défaut est 0.0.0.0-255.255.255.255.
12. Dans le domaine de port de victime, introduisez le numéro de port utilisé par l'hôte victime afin de recevoir le paquet offensant. Par exemple, **0-434**.
13. Dans le domaine d'évaluation du risque, écrivez une plage rr pour ce filtre. Par exemple, **85-100**.Si le rr pour un événement fait partie de la marge que vous spécifiez, l'événement est traité contre les critères de ce filtre.
14. Des actions de soustraire la liste déroulante, choisissez les actions que vous voulez que ce filtre enlève de l'événement. Par exemple, choisissez la **connexion TCP de remise**.**Conseil** : Maintenez la **touche Ctrl** afin de choisir plus d'une action d'événement dans la liste.
15. Dans la liste déroulante de pertinence de SYSTÈME D'EXPLOITATION, choisissez si vous voulez savoir si l'alerte est appropriée au SYSTÈME D'EXPLOITATION qui a été identifié pour la victime. Par exemple, choisissez **approprié**.

16. Dans le domaine de pourcentage de refuser, écrivez le pourcentage des paquets afin de refuser pour refusent des caractéristiques d'attaquant. Par exemple, **90**.Le par défaut est de 100 pour cent.
17. Dans l'arrêt sur le match field, choisissez une de ces cases d'option :**Oui** — Si vous voulez l'action d'événement filtre le composant pour cesser de traiter après que les actions de ce filtre particulier soient enlevéesAucun filtre qui restent n'est traité ; donc, aucune action supplémentaire ne peut être enlevée de l'événement.**NO-** si vous voulez continuer à traiter les filtres supplémentaires
18. Dans le domaine de commentaires, entrez dans tous les commentaires que vous voulez enregistrer avec ce filtre, tel que le but de ce filtre ou pourquoi vous avez configuré ce filtre d'une manière particulière. Par exemple, **NOUVEAU FILTRE**.**Conseil** : Cliquez sur l'**annulation** afin d'annuler vos modifications et fermer la boîte de dialogue de filtre d'action d'événement d'ajouter.
19. Cliquez sur **OK**.Le nouveau filtre d'action d'événement apparaît maintenant dans la liste sur l'onglet de filtres d'action d'événement comme affiché.
20. Cochez l'**action d'événement d'utilisation ignore la** case comme affichée.**Note**: Vous devez cocher l'**action d'événement d'utilisation ignore la** case sur l'action d'événement ignore l'onglet ou rien l'action d'événement ignore devenu activée indépendamment de la valeur que vous placez dans la boîte de dialogue de filtre d'action d'événement d'ajouter.
21. Choisissez un filtre existant d'action d'événement dans la liste afin de l'éditer, et puis cliquez sur Edit.La boîte de dialogue de filtre d'action d'événement d'éditer apparaît.
22. Changez toutes les valeurs dans les domaines que vous devez modifier.Voir les étapes 4 à 18 pour les informations sur la façon dont se terminer les champs.**Conseil** : Cliquez sur l'**annulation** afin d'annuler vos modifications et fermer la boîte de dialogue de filtre d'action d'événement d'éditer.
23. Cliquez sur **OK**.Le filtre édité d'action d'événement apparaît maintenant dans la liste sur l'onglet de filtres d'action d'événement.
24. Cochez l'**action d'événement d'utilisation ignore la** case.**Note**: Vous devez cocher l'**action d'événement d'utilisation ignore la** case sur l'action d'événement ignore l'onglet ou rien l'action d'événement ignore est activée indépendamment de la valeur que vous placez dans la boîte de dialogue de filtre d'action d'événement d'éditer.
25. Choisissez un filtre d'action d'événement dans la liste afin de la supprimer, et puis cliquez sur Delete.Le filtre d'action d'événement n'apparaît plus dans la liste sur l'onglet de filtres d'action d'événement.
26. Filtrez en haut ou en bas dans la liste afin de déplacer une action d'événement, choisissez-la, et puis cliquez sur **se relèvent** ou **abaissent**.**Conseil** : Clic **remis à l'état initial** afin d'enlever vos modifications.
27. Cliquez sur Apply afin d'appliquer vos modifications et sauvegarder la configuration révisée.

Configuration de variable d'événement

Terminez-vous ces étapes afin d'ajouter, éditer, et supprimer des variables d'événement :

1. Procédure de connexion. Par exemple, utilisez un compte avec des privilèges d'administrateur ou d'opérateur.
2. Choisissez la **configuration > les stratégies > les règles d'action d'événement > le rules0 > les variables d'événement** si la version de logiciel est 6.x. Pour la version de logiciel 5.x,

choisissez les **règles d'action de configuration > d'événement > les variables d'événement**.L'onglet de variables d'événement apparaît.
3. Cliquez sur Add afin de créer une variable.La boîte de dialogue variable d'ajouter apparaît.
4. Dans la zone d'identification, écrivez un nom pour cette variable.**Note**: Le nom valide peut seulement contenir des nombres ou des lettres. Vous pouvez également utiliser un trait d'union (-) ou un trait de soulignement (_).
5. Dans le domaine de valeur, écrivez les valeurs pour cette variable.Spécifiez la pleines adresse IP ou plages ou ensemble de plages. Exemple :10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Note**: Vous pouvez utiliser des virgules comme délimiteurs. Assurez-vous qu'il n'y a aucun espace de remorquage après la virgule. Autrement, vous recevez une `validation avez manqué` message d'erreur.**Conseil** : Cliquez sur l'**annulation** afin d'annuler vos modifications et fermer la boîte de dialogue de variable d'événement d'ajouter.
6. Cliquez sur **OK**.La nouvelle variable apparaît dans la liste sur l'onglet de variables d'événement.
7. Choisissez la variable existante dans la liste afin de l'éditer, et puis cliquez sur Edit.La boîte de dialogue de variable d'événement d'éditer apparaît.
8. Dans le domaine de valeur, écrivez vos modifications à la valeur.
9. Cliquez sur **OK**.La variable d'événement éditée apparaît maintenant dans la liste sur l'onglet de variables d'événement.**Conseil** : Choisissez la **remise** afin d'enlever vos modifications.
10. Cliquez sur Apply afin d'appliquer vos modifications et sauvegarder la configuration révisée.

Informations connexes

- Page de support de Système de protection contre les intrusions Cisco
- Support et documentation techniques - Cisco Systems