Détection de données sensibles

Les rubriques suivantes expliquent la détection des données sensibles et comment la configurer :

Principes de base de la détection des données sensibles

Des données sensibles telles que les numéros de sécurité sociale, les numéros de cartes de crédit, les numéros de permis de conduire, etc. peuvent être divulguées sur Internet, intentionnellement ou accidentellement. Le système fournit un préprocesseur de données sensibles qui peut détecter et générer des événements sur des données sensibles dans du texte ASCII, ce qui peut être particulièrement utile pour détecter les fuites accidentelles de données.

Les options globales de préprocesseur des données sensibles contrôlent le fonctionnement du préprocesseur. Vous pouvez modifier les options globales qui spécifient les éléments suivants :

- si le préprocesseur remplace tous les numéros de carte de crédit ou de sécurité sociale sauf les quatre derniers dans les paquets de déclenchement
- quels hôtes de destination de votre réseau surveiller à propos des données sensibles
- combien d'occurrences au total de tous les types de données dans une seule session entraînent un événement

Les types de données individuels identifient les données sensibles que vous pouvez détecter et pour lesquels générer des événements dans le trafic réseau de votre destination. Vous pouvez modifier les paramètres par défaut des options de type de données qui spécifient les éléments suivants :

- un seuil qui doit être atteint pour qu'un type de données détecté génère un seul événement par session

- les ports de destination à surveiller pour chaque type de données
- les protocoles d'application à surveiller pour chaque type de données

Vous pouvez créer et modifier des types de données personnalisés pour détecter les schémas de données que vous spécifiez. Par exemple, un hôpital peut créer un type de données pour protéger le numéro des malades ou une université peut créer un type de données pour détecter les numéros d'étudiants qui ont un schéma de numérotation unique.

Le système détecte les données sensibles par session TCP en faisant correspondre les types de données individuels au trafic. Vous pouvez modifier les paramètres par défaut pour chaque type de données et pour les options globales qui s'appliquent à tous les types de données dans votre politique de prévention des intrusions. Le système Firepower fournit des types de données prédéfinis et couramment utilisés. Vous pouvez également créer des types de données personnalisés.

Une règle de préprocesseur de données sensibles est associée à chaque type de données. Vous activez la détection des données sensibles et la génération d'événements pour chaque type de données en activant la règle de préprocesseur correspondante pour le type de données. Un lien sur la page de configuration vous amène à une vue filtrée des règles de données sensibles sur la page des règles, où vous pouvez activer et désactiver des règles et configurer d'autres attributs de règles.

Lorsque vous enregistrez des modifications à votre politique de prévention des intrusions, vous avez la possibilité d'activer automatiquement le préprocesseur des données sensibles si la règle associée à un type de données est activée et que la détection des données sensibles est désactivée.

Astuces Le préprocesseur des données sensibles peut détecter ces données dans les fichiers Microsoft Word non chiffrés qui sont téléversés et téléchargés par FTP ou HTTP; cela est possible grâce à la façon dont les fichiers Word regroupent le texte ASCII et les commandes de mise en forme séparément.

Le système ne détecte pas les données sensibles chiffrées ou masquées, ou les données sensibles dans un format compressé ou codé comme une pièce jointe de courriel codée en Base64. Par exemple, le système détecterait le nom distinctif (555)123-4567, mais pas une version brouillée où chaque numéro est séparé par des espaces, comme dans (5 5 5) 1 2 3 - 4 5 6 7, ou en intervenant HTML , tel que (555)-123-4567. Cependant, le système détecterait, par exemple, le numéro codé HTML (555)-123-4567, où aucun code d'intervention n'interrompt le modèle de numérotation.

Options globales de détection des données sensibles

Les options relatives aux données sensibles globales sont propres à la politique et s'appliquent à tous les types de données.

Mask (Masque)

Remplace par des X tous les numéros de cartes de crédit et de sécurité sociale, sauf les quatre derniers chiffres, dans le paquet de déclenchement. Les numéros masqués apparaissent dans la vue des paquets d'incidents d'intrusion dans l'interface Web et dans les paquets téléchargés.

Réseaux

Spécifie l'hôte ou les hôtes de destination à surveiller pour les données sensibles. Vous pouvez spécifier une seule adresse IP, un bloc d'adresses ou une liste d'adresses séparées par des virgules. Le système interprète un champ vide comme `n'importe quelle`, c'est-à-dire n'importe quelle adresse IP de destination.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Seuil global

Spécifie le nombre total d'occurrences de tous les types de données au cours d'une seule session que le préprocesseur doit détecter dans n'importe quelle combinaison avant de générer un événement de seuil global. Vous pouvez spécifier de 1 à 65 535.

Cisco recommande de définir la valeur de cette option comme étant supérieure à la valeur de seuil la plus élevée pour tout type de données individuel que vous activez dans votre politique.

Notez les points suivants concernant les seuils globaux :

- Vous devez activer la règle de préprocesseur 139:1 pour détecter et générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés sur les occurrences de type de données combinées.
- Le préprocesseur génère jusqu'à un événement de seuil global par session.
- Les événements de seuil globaux sont indépendants des événements de type de données individuels; c'est-à-dire que le préprocesseur génère un événement lorsque le seuil global est atteint, que le seuil d'événement pour tout type de données individuel ait ou non été atteint, et inversement.

Options des types de données sensibles individuelles

Au minimum, chaque type de données personnalisé doit préciser un seuil d'événement et au moins un port ou protocole d'application à surveiller.

Chaque type de données fourni par le système utilise un mot-clé `sd_pattern` autrement inaccessible pour définir un schéma de données intégré à détecter dans le trafic. Vous pouvez également créer des types de données personnalisés pour lesquels vous utilisez des expressions régulières simples pour spécifier vos propres schémas de données.

Les types de données sensibles s'affichent dans toutes les politiques de prévention des intrusions où la détection des données sensibles est activée. Les types de données fournis par le système s'affichent en lecture seule. Pour les types de données personnalisés, les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Tableau 1 : Options des types de données individuels

Option	Description
Type de données	Spécifie le nom unique du type de données.
Seuil	Spécifie le nombre d'occurrences du type de données lorsque le système génère un événement. Vous pouvez spécifier de 1 à 255. Notez que le préprocesseur génère un événement pour un type de données détecté par session. Notez également que les événements de seuil globaux sont indépendants des événements de type de données individuels; c'est-à-dire que le préprocesseur génère un événement lorsque le seuil d'événement de type de données est atteint, que le seuil d'événement global ait ou non été atteint, et inversement.
Ports de destination	Spécifie les ports de destination à surveiller pour le type de données. Vous pouvez spécifier un port unique, une liste de ports séparés par des virgules ou `n'importe` quel port de destination.
Protocoles d'application	Spécifie jusqu'à huit protocoles d'application à surveiller pour le type de données. Vous devez activer les détecteurs d'applications pour identifier les protocoles d'application à surveiller. Notez que, pour les périphériques de la version classique, cette fonctionnalité nécessite une licence de contrôle.
Schéma	Spécifie le modèle à détecter. Ce champ est uniquement présent pour les types de données personnalisés.

Sujets connexes

Activation et désactivation des détecteurs

Types de données sensibles fournis par le système

Chaque politique de prévention des intrusions comprend des types de données fournies par le système pour détecter les schémas de données couramment utilisés, comme les numéros de carte de crédit, les adresses de courriel, les noms distinctifs américains et les numéros de sécurité sociale américains avec ou sans tirets.

Chaque type de données fourni par le système est associé à une seule règle de préprocesseur de données sensibles qui a un ID de générateur (GID) de 138. Vous devez activer la règle de données sensibles associée dans la politique de prévention des intrusions dans générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour chaque type de données que vous souhaitez utiliser dans votre politique.

Le tableau suivant décrit chaque type de données et répertorie la règle de préprocesseur correspondante.

Tableau 2 : Types de données sensibles fournis par le système

Type de données	Description	GID de la préproces
Numéros de cartes de crédit	fait correspondre les numéros de cartes de crédit à quinze et seize chiffres VISA®, MasterCard®, Discovery® et American Express®, avec ou sans leurs tirets ou espaces habituels; utilise également l'algorithme de Luhan pour vérifier les chiffres de vérification des cartes de crédit.	138:2
Adresses de courriel	Fait correspondre les adresses de courriel.	138:5
Numéros de téléphone des États-Unis	Correspond aux noms distinctifs des États-Unis selon le modèle `(\d {3}) ?\d {3}-\d {4}.`	138:6
Numéros de sécurité sociale américains sans tirets	Correspondance des numéros de sécurité sociale américains à 9 chiffres qui ont des numéros de région à 3 chiffres valides, des numéros de groupe à 2 chiffres valides et qui n'ont pas de tirets.	138:4
Numéros de sécurité sociale américains avec des tirets	Correspondance des numéros de sécurité sociale américains à 9 chiffres qui ont des numéros de région à 3 chiffres valides, des numéros de groupe à 2 chiffres valides et des tirets.	138:3

Pour réduire les faux positifs des numéros à 9 chiffres autres que les numéros de sécurité sociale, le préprocesseur utilise un algorithme pour valider le numéro de zone à 3 chiffres et le numéro de groupe à 2 chiffres qui précèdent les numéros de série à 4 chiffres de chaque numéro de sécurité sociale. Le préprocesseur valide les numéros de groupe de sécurité sociale jusqu'en novembre 2009.

Exigences de licence pour la détection des données sensibles

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection ou comme indiqué dans une procédure.

Exigences et conditions préalables à la détection des données sensibles

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Configuration de la détection de données sensibles

Étant donné que la détection des données sensibles peut avoir une incidence importante sur les performances de votre système, Cisco vous recommande de respecter les directives suivantes :

- Choisissez la politique par défaut No Rules Active (aucune règle active) comme politique de base en matière de prévention des intrusions.
- Vérifiez que les paramètres suivants sont activés dans la politique d'analyse de réseau correspondante :
  - **Configuration FTP et Telnet** sous **les préprocesseurs de la couche d'application**
  - **IP de défragmentation** et **configuration des flux TCP** sous **Préprocesseurs de la couche transport/réseau**.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Avant de commencer

Pour les périphériques classiques, cette procédure nécessite la licence Protection ou Contrôle.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** ( ) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Vous avez les choix suivants :

- Modifiez les paramètres globaux comme décrit dans Options globales de détection des données sensibles, à la page 2.
- Choisissez un type de données dans la section **Targets** (cibles) et modifiez la configuration du type de données comme décrit dans Options des types de données sensibles individuelles, à la page 3.
- Si vous souhaitez inspecter des données sensibles personnalisées, créez un type de données personnalisé; voir Types de données sensibles personnalisées, à la page 9.

Étape 7 Ajouter ou supprimer des protocoles d'application à surveiller pour un type de données; voir Protocoles d'applications surveillés et données sensibles, à la page 7.

Remarque Pour détecter des données sensibles dans le trafic FTP :

- Assurez-vous que la politique de fichiers est activée pour la politique de contrôle d'accès.
- Vous devez ajouter le protocole d'application `données FTP`.

Étape 8 Pour afficher les règles de préprocesseur des données sensibles, cliquez éventuellement sur **Configure Rules for Sensitive Data Detection** (Configurer des règles pour la détection des données sensibles).

Vous pouvez activer ou désactiver n'importe quelle règle répertoriée. Vous pouvez également configurer des règles de données sensibles pour toute autre action disponible sur la page Rules (Règles), telle que la suppression des règles, la prévention des attaques basée sur le débit, etc. Consultez Règles de prévention des intrusions pour plus d'informations.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

Si vous activez les règles de prétraitement des données sensibles dans votre politique sans activer la détection de ce, vous êtes invité à activer la détection des données sensibles lorsque vous enregistrez les modifications apportées à votre politique.

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

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de détection des données sensibles 138:2, 138:3, 138:4, 138:5, 138:6, 138:>999999 ou 139:1. Pour plus de renseignements, consultez États des règles d'intrusion, Options globales de détection des données sensibles, à la page 2, Types de données sensibles fournis par le système, à la page 4, et Types de données sensibles personnalisées, à la page 9.
- Déployer les changements de configuration.

Sujets connexes

Cas particulier : détection des données sensibles dans le trafic FTP, à la page 8

Protocoles d'applications surveillés et données sensibles

Vous pouvez spécifier jusqu'à huit protocoles d'application à surveiller pour chaque type de données. Au moins un détecteur doit être activé pour chaque protocole d'application sélectionné. Par défaut, tous les détecteurs fournis par le système sont activés. Si aucun détecteur n'est activé pour un protocole d'application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application.

Vous devez spécifier au moins un protocole d'application ou un port à surveiller pour chaque type de données. Cependant, sauf dans le cas où vous souhaitez détecter des données sensibles dans le trafic FTP, Cisco vous

recommande, pour la couverture la plus complète, de spécifier les ports correspondants lorsque vous spécifiez les protocoles d'application. Par exemple, si vous spécifiez HTTP, vous pouvez également configurer le port HTTP 80 bien connu. Si un nouvel hôte de votre réseau met en œuvre HTTP, le système surveille le port 80 pendant l'intervalle pendant lequel il détecte le nouveau protocole d'application HTTP.

Dans le cas où vous souhaitez détecter des données sensibles dans le trafic FTP, vous devez préciser le protocole d'application `des données FTP` ; il n'y a aucun avantage à préciser un numéro de port.

Sujets connexes

Activation et désactivation des détecteurs
Cas particulier : détection des données sensibles dans le trafic FTP, à la page 8

Cas particulier : détection des données sensibles dans le trafic FTP

Vous déterminez généralement le trafic à surveiller pour les données sensibles en spécifiant les ports à surveiller ou les protocoles d'application dans les déploiements.

Toutefois, le fait de spécifier des ports ou des protocoles d'application n'est pas suffisant pour détecter des données sensibles dans le trafic FTP. Les données sensibles du trafic FTP se trouvent dans le trafic du protocole d'application FTP, qui se produit par intermittence et utilise un numéro de port transitoire, ce qui le rend difficile à détecter. Pour détecter des données sensibles dans le trafic FTP, vous **devez** inclure les éléments suivants dans votre configuration :

- Précisez le protocole d'application `des données FTP` pour activer la détection des données sensibles dans le trafic FTP.

  Dans le cas particulier de la détection de données sensibles dans le trafic FTP, la spécification du protocole d'application de `données FTP` ne déclenche pas la détection, mais le traitement rapide du processeur FTP/Telnet pour détecter les données sensibles dans le trafic FTP.

- Vérifiez que le détecteur de données FTP, qui est activé par défaut, est activé.
- Assurez-vous que votre configuration comprend au moins un port pour surveiller les données sensibles.
- Assurez-vous que la politique de fichiers est activée pour la politique de contrôle d'accès.

Notez qu'il n'est pas nécessaire de préciser un port FTP, sauf dans le cas peu probable où vous souhaitiez détecter uniquement des données sensibles dans le trafic FTP. La plupart des configurations de données sensibles incluront d'autres ports comme les ports HTTP ou les ports de messagerie. Dans le cas où vous souhaitez spécifier un seul port FTP et aucun autre port à surveiller, Cisco vous recommande de spécifier le port de commande FTP `23`.

Sujets connexes

Le décodeur Telnet/FTP
Activation et désactivation des détecteurs
Configuration de la détection de données sensibles, à la page 6

Types de données sensibles personnalisées

Chaque type de données personnalisé que vous créez crée également une règle de préprocesseur de données sensibles unique qui a un ID de générateur (GID) de 138 et un ID de Snort (SID) de 1000000 ou plus, c'est-à-dire un SID pour une règle locale.

Vous devez activer la règle de données sensibles associée pour activer la détection, générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour chaque type de données personnalisé que vous souhaitez utiliser dans votre politique.

Pour vous aider à activer les règles relatives aux données sensibles, un lien sur la page de configuration vous amène à une vue filtrée de la page des règles de la politique de prévention des intrusions qui affiche toutes les règles personnalisées et fournies par le système relatives aux données sensibles. Vous pouvez également afficher des règles personnalisées sur les données sensibles ainsi que des règles locales personnalisées en sélectionnant la catégorie de filtrage local dans la page des règles de politique de prévention des intrusions. Notez que les règles personnalisées relatives aux données sensibles ne sont pas répertoriées dans la page de l'éditeur de règles de prévention des intrusions (**Objects (objets)** > **Intrusion Rules (règles d'intrusion)**).

Une fois que vous avez créé un type de données personnalisé, vous pouvez l'activer dans n'importe quelle politique de prévention des intrusions dans le système ou, pour les déploiements multidomaine, dans le domaine actuel. Pour activer un type de données personnalisé, vous devez activer la règle de données sensibles associée dans toute politique que vous souhaitez utiliser pour détecter ce type de données personnalisé.

Schémas de données dans des types de données sensibles personnalisées

Vous définissez le modèle de données pour un type de données personnalisé à l'aide d'un ensemble simple d'expressions régulières comprenant les éléments suivants :

- trois métacaractères
- les caractères d'échappée qui vous permettent d'utiliser les métacaractères comme caractères littéraux
- six classes de caractères

Les métacaractères sont des caractères littéraux qui ont une signification particulière dans les expressions régulières.

Tableau 3 : Métacaractères de schémas de données sensibles

Métacaractère	Description	Exemple
`?`	Correspond à zéro ou une occurrence du caractère ou de la séquence d'échappement précédente; c'est-à-dire que le caractère ou la séquence d'échappement qui le précède est facultatif.	`colou?r` correspond à `color` ou `colour`
`{n}`	Correspondre au caractère ou à la séquence d'échappement précédent n fois.	Par exemple, `\d{2}` correspond à `55`, `12`, et ainsi de suite; `\l{3}` correspond à `AbC`, `www`, et ainsi de suite; `\w{3}` correspond à `a1B`, 25C, et ainsi de suite `x{5}` correspond à `xxxxx`

Métacaractère	Description	Exemple
\	Vous permet d'utiliser des métacaractères comme caractères réels et est également utilisé pour spécifier une classe de caractères prédéfinie.	`\?` correspond à un point d'interrogation,`\\` à une barre oblique inverse,`\d` à des caractères numériques, etc.

Vous devez utiliser une barre oblique inverse pour éviter certains caractères pour que le préprocesseur des données sensibles les interprète correctement comme des caractères littéraux.

Tableau 4 : Caractères de modèle de données sensibles échappés

Utilisez ce caractère d'échappement ...	Pour représenter ce caractère littéral...
\?	?
\{	{
\}	}
\\	\

Lors de la définition d'un modèle personnalisé de données sensibles, vous pouvez utiliser des classes de caractères.

Tableau 5 : Classes de caractères de schéma de données sensibles

Classes de caractères	Description	Définition de la classe de caractères
\d	Correspond à n'importe quel caractère numérique ASCII de 0 à 9	0 à 9
\D	Correspond à tout octet qui n'est pas un caractère ASCII numérique	et non entre 0 et 9
\l (« ell » minuscule)	Correspond à n'importe quelle lettre ASCII	a-zA-Z
\L	Correspond à tout octet qui n'est pas une lettre ASCII	et non de a-zA-Z
\w	Correspond à n'importe quel caractère alphanumérique ASCII Notez que, contrairement aux expressions régulières PCRE, celles-ci n'incluent pas de trait de soulignement (_).	[a-zA-Z0-9_]
\W	Correspond à tout octet qui n'est pas un caractère alphanumérique ASCII	pas a-zA-Z0-9

Le préprocesseur traite les caractères saisis directement, plutôt que dans le cadre d'une expression régulière, comme des caractères littéraux. Par exemple, le modèle de données 1234 correspond à `1234`.

L'exemple de modèle de données suivant, qui est utilisé dans la règle de données sensibles 138:4 fournie par le système, utilise la classe de caractères des chiffres d'échappée, les métacaractères du multiplicateur et du spécificateur d'option, le tiret littéral (-) et les parenthèses gauche et droite (). pour détecter les noms distinctifs américains :

```
(\d{3}) ?\d{3}-\d{4}
```

Faites preuve de prudence lorsque vous créez des schémas de données personnalisés. Examinez le modèle de données suivant pour détecter les noms distinctifs qui, bien qu'ils utilisent une syntaxe valide, pourraient provoquer de nombreux faux positifs :

```
(?\d{3})? ?\d{3}-?\d{4}
```

Étant donné que le deuxième exemple combine des parenthèses facultatives, des espaces et des tirets facultatifs, il détectera, entre autres, les noms distinctifs selon les schémas souhaitables suivants :

- `(555)123-4567`
- `555123-4567`
- `5551234567`

Cependant, le deuxième exemple de schéma détectera également, entre autres, les schémas potentiellement non valides suivants, produisant des faux positifs :

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

Considérez enfin, à des fins d'illustration seulement, un exemple extrême dans lequel vous créez un schéma de données qui détecte la lettre minuscule `a` en utilisant un seuil d'événement faible dans tout le trafic de destination sur le réseau d'une petite entreprise. Un tel modèle de données pourrait submerger votre système avec des millions d'événements en seulement quelques minutes.

Configuration des types de données sensibles personnalisées

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Vous ne pouvez pas supprimer un type de données si la règle sur les données sensibles pour ce type de données est activée dans une politique de prévention des intrusions.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** ( ) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Cliquez sur **Ajouter** ( ) à côté de **Types de données**.

Étape 7 Saisissez un nom pour le type de données.

Étape 8 Saisissez le modèle que vous souhaitez détecter avec ce type de données; voir Schémas de données dans des types de données sensibles personnalisées, à la page 9.

Étape 9 Cliquez sur **OK**.

Étape 10 Si vous le souhaitez, cliquez sur le nom du type de données et modifiez les options décrites dans Options des types de données sensibles individuelles, à la page 3.

Étape 11 Vous pouvez également supprimer un type de données personnalisé en cliquant sur **Supprimer** ( ), puis sur **OK** pour confirmer.

Remarque Si la règle sur les données sensibles pour ce type de données est activée dans une politique de prévention des intrusions, le système avertit que vous ne pouvez pas supprimer le type de données. Vous devez désactiver la règle de données sensibles dans les politiques concernées avant de tenter à nouveau la suppression. voir Définition des états des règles d'intrusion.

Étape 12 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, 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

- Activer la règle de prétraitement des données sensibles personnalisée associée dans chaque politique où vous souhaitez utiliser ce type de données; voir Définition des états des règles d'intrusion.
- Déployer les changements de configuration.

Sujets connexes

Modification des types de données sensibles personnalisées, à la page 12

Modification des types de données sensibles personnalisées

Vous pouvez modifier tous les champs des types de données sensibles personnalisés. Notez, cependant, que lorsque vous modifiez le champ de nom ou de modèle, ces paramètres changent dans toutes les politiques de prévention des intrusions sur le système. Vous pouvez définir des valeurs propres à la politique pour les autres options.

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** (Modifier) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Dans la section **Targets** (objectifs), cliquez sur le nom du type de données personnalisé.

Étape 7 Cliquez sur **Edit Data Type Name and Template** (Modifier le nom et le modèle du type de données).

Étape 8 Modifiez le nom et le modèle du type de données; voir Schémas de données dans des types de données sensibles personnalisées, à la page 9.

Étape 9 Cliquez sur **OK**.

Étape 10 Définir les options restantes sur des valeurs propres à la politique; voir Options des types de données sensibles individuelles, à la page 3.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, 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.

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.