Renseignements de sécurité

La politique de renseignements de sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Les rubriques suivantes expliquent comment mettre en œuvre Security Intelligence.

À propos des renseignements sur la sécurité

La politique de renseignements de sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Le système supprime ce trafic indésirable avant de l'évaluer avec la stratégie de contrôle d'accès, réduisant ainsi la quantité de ressources système utilisées.

Vous pouvez bloquer le trafic en fonction des éléments suivants :

- Flux Cisco Talos Intelligence Group (Talos) : Talos fournit un accès à des flux de renseignements de sécurité régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Le système télécharge régulièrement des mises à jour de flux; ainsi, les nouvelles informations sur les menaces sont disponibles sans que vous ayez à redéployer la configuration.

Remarque Les flux Talos sont mis à jour par défaut toutes les heures. Vous pouvez modifier la fréquence de mise à jour et même mettre à jour les flux à la demande à partir de la page **Device (Périphérique)** > **Updates (Mises à jour)**.

- Network and URL Objects (Objets de réseau et d'URL) : si vous connaissez des adresses IP ou des URL spécifiques que vous souhaitez bloquer, vous pouvez créer des objets pour celles-ci et les ajouter à la liste des adresses bloquées ou à la liste des autorisations. Notez que vous ne pouvez pas utiliser d'objets réseau avec des spécifications de FQDN (nom de domaine complet) ou de plage.

Vous créez des listes distinctes pour les adresses IP (réseaux) et les URL.

Remarque Si une demande HTTP/HTTPS s'adresse à une URL qui utilise une adresse IP au lieu d'un nom d'hôte, le système recherche la réputation de l'adresse IP dans les listes d'adresses réseau. Vous n'avez pas besoin de dupliquer les adresses IP dans les listes de réseaux et d'URL.

Création d'exceptions aux listes de blocage

Pour chaque liste de blocage, vous pouvez créer une liste d'exceptions associée, aussi appelée liste « Do Not Block (Ne pas bloquer) ». Le seul objet de la liste d'exceptions est d'exempter les adresses IP ou les URL qui apparaissent dans la liste de blocage. Autrement dit, si vous trouvez une adresse ou une URL que vous devez utiliser et dont vous savez qu'elle est sûre, mais qu'elle figure dans un flux configuré dans la liste de blocage, vous pouvez exempter ce réseau/cette URL sans retirer complètement la catégorie de la liste de blocage.

Le trafic exempté est ensuite évalué par la stratégie de contrôle d'accès. La décision finale sur l'autorisation ou l'abandon des connexions dépend de la règle de contrôle d'accès à laquelle les connexions correspondent. La règle d'accès détermine également si une inspection de prévention des intrusions ou de programmes malveillants est appliquée à la connexion.

Catégories de flux de renseignements sur la sécurité

Le tableau suivant décrit les catégories disponibles dans les flux Cisco Talos Intelligence Group (Talos). Ces catégories sont disponibles à la fois pour le blocage de réseau et d'URL.

Ces catégories peuvent changer au fil du temps, de sorte qu'un flux nouvellement téléchargé peut comporter des changements de catégorie. Lors de la configuration des renseignements sur la sécurité, vous pouvez cliquer sur l'icône d'information à côté d'un nom de catégorie pour afficher une description.

Tableau 1 : Catégories de flux Cisco Talos Intelligence Group (Talos)

Catégorie de renseignements sur la sécurité	Description
Agresseurs	Analyseurs et hôtes actifs connus pour les activités malveillantes sortantes
fraude_bancaire	Sites qui se livrent à des activités frauduleuses liées aux services bancaires électroniques
bogon	Réseaux de bogons et adresses IP non attribuées
Robots logiciels	Sites qui hébergent des pipettes de programmes malveillants binaires
CNC	Sites qui hébergent des serveurs de commande et de contrôle pour les réseaux de zombies
Cryptominage	Hôtes fournissant un accès à distance aux ensembles et aux portefeuilles dans le but d'exploiter des crypto-devises

Catégorie de renseignements sur la sécurité	Description
Dga	Algorithmes de programmes malveillants utilisés pour générer un grand nombre de noms de domaine agissant comme points de rendez-vous avec leurs serveurs de commande et de contrôle
Kit d'exploit	Trousses de logiciels conçues pour identifier les vulnérabilités des logiciels des clients.
Risque_élevé	Les domaines et les noms d'hôte qui correspondent aux algorithmes de sécurité prédictive OpenDNS du graphique de sécurité
Ioc	Hôtes qui ont été observés en train de s'engager dans les indicateurs de compromission (IOC)
partage_de_liens	Sites Web qui partagent des fichiers protégés par des droits d'auteur sans autorisation
Malveillant	Sites ayant un comportement malveillant qui ne correspondent pas nécessairement à une autre catégorie de menace, plus précise,
Maliciels	Sites qui hébergent des fichiers binaires ou des kits d'exploit de programmes malveillants
Nouvellement_vu	Les domaines qui ont été récemment enregistrés ou qui ne sont pas encore vus par télémétrie. **Attention** Actuellement, cette catégorie ne comporte aucun flux actif et est réservée pour une utilisation future.
Mandataires_ouverts	Des mandataires ouverts qui permettent la navigation anonyme sur le Web
Relais_ouvert	Ouvrir les relais de messagerie connus pour être utilisés pour les pourriels
Hameçonnage	Les sites qui hébergent des pages d'hameçonnage
Intervention	Adresses IP et URL qui participent activement à des activités malveillantes ou suspectes
Pourriels	Hôtes de messagerie connus pour envoyer des pourriels
Logiciel espion	Sites connus pour contenir, diffuser ou soutenir des activités de logiciels espions et publicitaires
Suspect	Fichiers qui semblent suspects et dont les caractéristiques ressemblent à celles d'un logiciel malveillant connu
nœud_exit_de_tor	Hôtes connus pour offrir des services de nœud de sortie pour le réseau d'anonymisation Tor

Exigences de licence pour les renseignements sur la sécurité

Vous devez activer la licence **Menace** pour utiliser Security Intelligence. Consultez Activation ou désactivation des licences facultatives.

Configurer les renseignements sur la sécurité

La politique de renseignements sur la sécurité vous donne l'occasion d'abandonner rapidement le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Les connexions autorisées sont toujours évaluées par les politiques de contrôle d'accès et sont susceptibles d'être interrompues. Vous devez activer les licences IPS license (licence IPS) et pour pouvoir utiliser Security Intelligence.

Procédure

Étape 1 Sélectionnez **Policies (Politiques)** > **Security Intelligence**.

Étape 2 Si la politique n'est pas activée, cliquez sur le bouton **Enable Security Intelligence** (Activer Security Intelligence).

Vous pouvez désactiver la politique à tout moment en cliquant sur le commutateur **Security Intelligence** pour le mettre sur **Off** (Désactivé). Votre configuration est conservée, de sorte que lorsque vous réactivez la politique, vous n'avez pas besoin de la reconfigurer.

Étape 3 Configurer Security Intelligence.

Il existe des listes de blocage distinctes pour les réseaux (adresses IP) et les URL.

a) Cliquez sur l'onglet **Network** (Réseau) ou **URL** pour afficher la liste que vous souhaitez configurer.

b) Dans la liste de blocage/abandon, cliquez sur **+** pour sélectionner les objets ou les flux dont vous souhaitez abandonner immédiatement les connexions.

Le sélecteur d'objet organise les objets et les flux sur des onglets distincts par type. Si l'objet que vous souhaitez n'existe pas encore, cliquez sur le lien **Create New Object** (Créer un nouvel objet) en bas de la liste et créez-le maintenant. Pour une description des flux Cisco Talos Intelligence Group (Talos), cliquez sur le bouton **i** à côté du flux. Consultez aussi Catégories de flux de renseignements sur la sécurité, à la page 2.

Remarque
Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau /0. Cela inclut les objets réseau any-ipv4 et any-ipv6. Ne sélectionnez pas ces objets pour le blocage réseau.

c) Dans la liste Do Not Block (Ne pas bloquer), cliquez sur **+** et sélectionnez les exceptions à la liste de blocage.

La seule raison de configurer cette liste est de faire des exceptions pour les adresses IP ou les URL qui se trouvent dans la liste de blocage. Les connexions exemptées sont ensuite évaluées par votre politique de contrôle d'accès et peuvent être abandonnées de toute façon.

d) Répétez le processus pour configurer l'autre liste de blocage.

Étape 4 (Facultatif) Cliquez sur le bouton **Edit Logging Settings** (Paramètres de journalisation) ( ) pour configurer la journalisation.

Si vous activez la journalisation, toutes les correspondances avec les entrées de liste bloquées sont enregistrées. Les correspondances avec les entrées d'exceptions ne sont pas journalisées, bien que vous obteniez des messages de journalisation si les connexions exemptées correspondent aux règles de contrôle d'accès avec la journalisation activée.

Configurez les paramètres suivants :

- **Connection Events Logging** (Journalisation des événements de connexion) : cliquez sur la bascule pour activer ou désactiver la journalisation.
- **Syslog** : si vous souhaitez envoyer une copie des événements à un serveur syslog externe, sélectionnez cette option et sélectionnez l'objet serveur qui définit le serveur syslog. Si l'objet requis n'existe pas déjà, cliquez sur **Add Syslog Server** (Ajouter un serveur syslog) et créez-le.

  Comme le stockage d'événements sur l'appareil est limité, l'envoi des événements à un serveur journal système externe peut fournir un stockage à plus long terme et améliorer votre analyse des événements.

Surveillance de l'intelligence de sécurité

Si vous activez la journalisation pour la politique Security Intelligence, le système génère des événements Security Intelligence pour chaque connexion qui correspond à un élément d'une liste de blocage. Les événements de connexion correspondent à ces connexions.

Les statistiques pour les connexions abandonnées s'affichent dans les différents tableaux de bord disponibles sur la page Surveillance.

Le tableau de bord **Monitoring (Surveillance)** > **Access And SI Rules (Règles d'accès et SI)** affiche les principales règles d'accès et les règles Security Intelligence équivalentes qui correspondent au trafic.

En outre, vous pouvez sélectionner **Monitoring (Surveillance)** > **Events (Événements**, puis l'affichage **Security Intelligence (Security Intelligence)**, pour voir les événements Security Intelligence, ainsi que les événements de connexion associés sous l'onglet **Connection (Connexion)**.

- Le champ SI Category ID (ID de catégorie SI) dans un événement indique l'objet mis en correspondance dans la liste de blocage, par exemple un objet ou un flux de réseau ou d'URL.
- Le champ Reason (Raison) d'un événement de connexion explique pourquoi l'action affichée dans l'événement a été appliquée. Par exemple, une action Block (Blocage) associée à des raisons telles que IP Block (Blocage IP) ou URL Block (Blocage d'URL) indique qu'une connexion a été abandonnée par Security Intelligence.

Exemples pour les renseignements sur la sécurité

Le chapitre de cas d'utilisation comprend un exemple de mise en œuvre des politiques de sécurité Security Intelligence. Veuillez consulter Comment bloquer les menaces.

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.