Surveillance du périphérique

Le système comprend des tableaux de bord et Event Viewer (la Visionneuse d'événements) que vous pouvez utiliser pour surveiller le périphérique et le trafic qui passe par le périphérique.

Activez la journalisation pour obtenir des statistiques de trafic.

Vous pouvez surveiller un large éventail de statistiques de trafic à l'aide des tableaux de bord de surveillance et de la visionneuse d'événements. Cependant, vous devez activer la journalisation pour indiquer au système quelles statistiques collecter. La journalisation génère différents types d'événements offrant une visibilité sur les connexions qui transitent par le système.

Les rubriques suivantes expliquent plus en détail les événements et les informations qu'ils fournissent, en se concentrant particulièrement sur la journalisation des connexions.

Types d'événements

Le système peut générer les types d'événements suivants. Vous devez générer ces événements pour voir les statistiques associées dans les tableaux de bord de surveillance.

Événements de connexion

Vous pouvez générer des événements pour les connexions car les utilisateurs génèrent du trafic qui traverse le système. Activez la journalisation de la connexion sur les règles d'accès pour générer ces événements. Vous pouvez également activer la journalisation sur les politiques de Security Intelligence et les règles de déchiffrement SSL pour générer des événements de connexion.

Les événements de connexion comprennent une grande variété d'informations sur une connexion, notamment les adresses IP et les ports source et de destination, les URL et les applications utilisées, ainsi que le nombre d'octets ou de paquets transmis. Les renseignements comprennent également l'action entreprise (par exemple, autoriser ou bloquer la connexion) et les politiques appliquées à la connexion.

Incidents d'intrusion

Le système examine les paquets qui traversent votre réseau pour détecter toute activité malveillante qui pourrait nuire à la disponibilité, à l'intégrité et à la confidentialité d'un hôte et de ses données. Lorsque

le système détecte une intrusion possible, il génère un incident d'intrusion, qui enregistre la date, l'heure, le type d'exploitation et des informations contextuelles sur la source de l'attaque et sa cible. Des incidents d'intrusion sont générés pour toute règle de prévention des intrusions définie pour bloquer ou alerter, quelle que soit la configuration de journalisation de la règle de contrôle d'accès à l'origine de l'invocation.

Événements liés aux fichiers

Les événements de fichier représentent les fichiers que le système a détectés, et éventuellement bloqués, dans le trafic réseau en fonction de vos politiques de fichiers. Vous devez activer la journalisation des fichiers sur la règle d'accès qui applique la politique de fichiers pour générer ces événements.

Lorsque le système génère un événement de fichier, le système consigne également la fin de la connexion associée, quelle que soit la configuration de journalisation de la règle de contrôle d'accès qui appelle.

Événements de programmes malveillants

Le système peut détecter les programmes malveillants dans le trafic réseau dans le cadre de la configuration globale de votre contrôle d'accès. AMP for Firepower peut générer un événement de logiciel malveillant, contenant le statut de l'événement résultant et des données contextuelles indiquant comment, où et quand le logiciel malveillant a été détecté. Cisco AMP pour les réseaux Vous devez activer la journalisation des fichiers sur la règle d'accès qui applique la politique de fichiers pour générer ces événements.

La disposition d'un fichier peut changer, par exemple, de « nettoyer » à malveillant ou d'un fichier malveillant à « nettoyer ». Si AMP for Firepower interroge le nuage AMP au sujet d'un fichier et que le nuage détermine que le statut a changé dans la semaine suivant la requête, le système génère des événements rétrospectifs de logiciel malveillant. Cisco AMP pour les réseaux Cisco AMP Cloud

Événements liés aux renseignements sur la sécurité

Les événements Security Intelligence sont un type d'événement de connexion généré par la politique Security Intelligence pour chaque connexion bloquée ou surveillée par la politique. Tous les événements Security Intelligence comportent un champ Catégorie de Security Intelligence renseigné.

À chacun de ces événements correspond un événement de connexion « régulière ». Comme la politique de renseignements sur la sécurité est évaluée avant de nombreuses autres politiques de sécurité, y compris le contrôle d'accès, lorsqu'une connexion est bloquée par les renseignements sur la sécurité, l'événement qui en résulte ne contient pas les renseignements que le système aurait pu recueillir lors d'une évaluation ultérieure, par exemple, l'identité de l'utilisateur.

Journalisation des connexions configurable

Vous devez enregistrer les connexions en fonction des besoins de sécurité et de conformité de votre entreprise. Si votre objectif est de limiter le nombre d'événements que vous générez et d'améliorer les rendements, activez la journalisation uniquement pour les connexions essentielles à votre analyse. Toutefois, si vous souhaitez obtenir une vue d'ensemble de votre trafic réseau à des fins de profilage, vous pouvez activer la journalisation pour des connexions supplémentaires.

Lors de la configuration de la journalisation des connexions, gardez à l'esprit que le système peut journaliser une connexion pour plusieurs raisons et que la désactivation de la journalisation à un endroit ne garantit pas que les connexions correspondantes ne seront pas journalisées.

Vous pouvez configurer la journalisation des connexions aux emplacements suivants.

- Règles de contrôle d'accès et action par défaut : la journalisation à la fin d'une connexion fournit la plupart des informations sur la connexion. Vous pouvez aussi journaliser le début de la connexion, mais ces événements comportent des informations incomplètes. La journalisation des connexions est désactivée

par défaut; vous devez donc l'activer pour chaque règle (et l'action par défaut) qui cible le trafic que vous souhaitez suivre.

- Security Intelligence policy (Politique Security Intelligence) : vous pouvez activer la journalisation afin de générer des événements de connexion Security Intelligence pour chaque connexion bloquée. Lorsque le système journalise un événement de connexion à la suite du filtrage Security Intelligence, il journalise aussi un événement Security Intelligence correspondant, qui est un type particulier d'événement de connexion que vous pouvez afficher et analyser séparément.
- Règles de déchiffrement SSL et action par défaut : vous pouvez configurer la journalisation à la fin d'une connexion. Dans le cas des connexions bloquées, le système met immédiatement fin à la session et génère un événement. Pour les connexions surveillées et les connexions que vous transmettez aux règles de contrôle d'accès, le système génère un événement à la fin de la session.

Journalisation automatique des connexions

Le système enregistre automatiquement les événements de fin de connexion suivants, indépendamment de toute autre configuration de journalisation.

- Le système consigne automatiquement les connexions associées aux incidents d'intrusion, sauf si la connexion est gérée par l'action par défaut de la politique de contrôle d'accès. Vous devez activer la journalisation sur l'action par défaut pour obtenir les événements d'intrusion pour le trafic correspondant.
- Le système consigne automatiquement les connexions associées aux événements liés aux fichiers et aux programmes malveillants. Il s'agit uniquement des événements de connexion : vous pouvez éventuellement désactiver la génération d'événements liés aux fichiers et aux programmes malveillants.

Conseils pour la journalisation des connexions

Gardez les conseils suivants à l'esprit lors de l'examen de la configuration de votre journalisation et de l'évaluation des statistiques connexes :

- Lorsque vous autorisez le trafic avec une règle de contrôle d'accès, vous pouvez utiliser une politique de prévention des intrusions ou de fichiers associée pour inspecter davantage le trafic et bloquer les intrusions, les fichiers interdits et les programmes malveillants avant que le trafic n'atteigne sa destination finale. Notez, cependant, que l'inspection par défaut des fichiers et des intrusions est désactivée pour les charges utiles chiffrées. Si les politiques de prévention des intrusions ou de fichiers trouvent une raison de bloquer une connexion, le système consigne immédiatement un événement de fin de connexion, quels que soient vos paramètres de journal de connexion. La journalisation des connexions autorisées fournit la plupart des informations statistiques sur le trafic dans votre réseau.
- Une connexion de confiance est une connexion gérée par une règle de contrôle d'accès Trust (confiance) ou l'action par défaut dans une politique de contrôle d'accès. Cependant, les connexions de confiance ne sont pas inspectées pour détecter les données de découverte, les intrusions ou les fichiers interdits et les programmes malveillants. Par conséquent, les événements de connexion pour les connexions de confiance contiennent des informations limitées.
- Pour les règles de contrôle d'accès et les actions par défaut de la politique de contrôle d'accès qui bloquent le trafic, le système consigne les événements de début de connexion. Le trafic correspondant est refusé sans autre inspection.

- La journalisation des connexions TCP bloquées lors d'une attaque par déni de service (DoS) peut affecter le rendement du système et submerger la base de données avec plusieurs événements similaires. Avant d'activer la consignation pour une règle Block (Bloquer), évaluez si la règle surveille le trafic sur une interface exposée à Internet ou une autre interface vulnérable aux attaques DoS.
- Si vous sélectionnez l'option **Bypass Access Control policy for decrypted traffic** (Politique de contournement du contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) lorsque vous configurez les profils de connexion VPN d'accès à distance, ou si vous activez la commande **sysopt connection permit-vpn**, tout le trafic de VPN de site à site ou d'accès à distance contourne l'inspection et la politique de contrôle d'accès. Ainsi, vous n'obtiendrez aucun événement de connexion pour ce trafic, et le trafic ne sera reflété dans aucun tableau de bord statistique.

Envoi d'événements à un serveur Syslog externe

Outre l'affichage des événements par le biais de FDM, qui a une capacité limitée de stockage des événements, vous pouvez configurer de manière sélective les règles et les politiques pour envoyer des événements à un serveur syslog externe. Vous pouvez ensuite utiliser les fonctionnalités et le stockage supplémentaire de la plateforme de serveur syslog sélectionnée pour afficher et analyser les données d'événement.

Pour envoyer des événements à un serveur syslog externe, modifiez chaque règle, action par défaut ou politique qui active la journalisation des connexions et sélectionnez un objet serveur syslog dans les paramètres de journalisation. Pour envoyer des incidents d'intrusion à un serveur syslog, configurez le serveur dans les paramètres de la politique de prévention des intrusions. Pour envoyer des événements de fichier ou de programme malveillant à un serveur syslog, configurez le serveur dans **Device (Appareil)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation**.

Pour en savoir plus, consultez l'aide de chaque type de règle et de politique, ainsi que Configuration des serveurs Syslog.

Évaluation des événements à l'aide des services en nuage Cisco, tels que Cisco Threat Response

En plus d'utiliser Event Viewer (Visionneuse d'événements) et vos propres serveurs syslog, vous pouvez envoyer des événements de connexion ainsi que des événements d'intrusion prioritaires, de fichiers et de programmes malveillants à un serveur Cisco en nuage. Les services en nuage de Cisco, tels que Cisco Threat Response, peuvent extraire les événements de ce serveur en nuage et vous pouvez ensuite utiliser ces services pour évaluer ces événements.

Ces services en nuage sont distincts de Cisco Firepower Threat Defense et FDM. Si vous choisissez d'utiliser un service qui vous oblige à envoyer ces événements dans le nuage Cisco, vous devez activer la connexion sur la page **Device (appareil)** > **System Settings (Paramètres système** > **Cloud Services (Services en nuage)**. Consultez Envoi d'événements à Cisco Cloud.

Vous pouvez vous connecter à Cisco Threat Response dans la région des États-Unis https://visibility.amp.cisco.com/, https://visibility.eu.amp.cisco.com dans la région de l'UE. Vous pouvez regarder des vidéos sur l'utilisation et les avantages de l'application sur YouTube à http://cs.co/CTRvideos. Pour en savoir plus sur l'utilisation de Cisco Threat Response avec Cisco Firepower Threat Defense, consultez le *guide d'intégration de Cisco Secure Firewall Threat Defense et de SecureX threat response*, à https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Tableaux de bord du trafic et du système

Le système comprend plusieurs tableaux de bord que vous pouvez utiliser pour analyser le trafic passant par le périphérique et les résultats de votre politique de sécurité. Utilisez ces renseignements pour évaluer l'efficacité globale de votre configuration et pour identifier et résoudre les problèmes de réseau.

Les tableaux de bord des unités d'un groupe de haute disponibilité affichent les statistiques pour ce périphérique uniquement. Les statistiques ne sont pas synchronisées entre les unités.

Remarque Les données utilisées dans les tableaux de bord liés au trafic sont collectées à partir des règles de contrôle d'accès qui permettent la connexion ou de la journalisation des fichiers, et d'autres politiques de sécurité qui permettent la journalisation. Les tableaux de bord ne reflètent pas le trafic qui correspond aux règles pour lesquelles aucune journalisation n'est activée. Assurez-vous de configurer vos règles avec les informations qui vous intéressent. En outre, les renseignements sur les utilisateurs sont disponibles uniquement si vous configurez des règles d'identité pour recueillir l'identité des utilisateurs. Enfin, les informations sur les intrusions, les fichiers, les programmes malveillants et les catégories d'URL ne sont disponibles que si vous avez une licence pour ces fonctionnalités et si vous configurez les règles qui utilisent les fonctionnalités.

Procédure

Étape 1 Cliquez sur **Monitoring** (Superviser) dans le menu principal pour ouvrir la page Dashboards (Tableaux de bord).

Vous pouvez sélectionner des plages de temps prédéfinies, comme la dernière heure ou la dernière semaine, ou définir une plage de temps personnalisée avec des heures de début et de fin spécifiques, pour contrôler les données affichées dans les graphiques et les tableaux du tableau de bord.

Les tableaux de bord liés au trafic comprennent les types d'affichage suivants :

- Top 5 bar graphs (5 principaux graphiques à barres) : ils sont affichés dans le tableau de bord **Network Overview** (Aperçu du réseau) et dans les tableaux de bord récapitulatifs par élément que vous voyez si vous cliquez sur un élément dans un tableau de bord. Vous pouvez faire basculer les informations entre le nombre de **Transactions** ou **Data Usage** (l'utilisation des données) (total des octets envoyés et reçus). Vous pouvez également faire basculer l'affichage pour afficher toutes les transactions, les transactions autorisées ou les transactions refusées. Cliquez sur le lien **View More** (Afficher plus) pour voir le tableau associé au graphique.
- Tables (Tableaux) : les tableaux affichent les éléments d'un type particulier (par exemple, applications ou URL categories (catégories d'URL Web)) avec le nombre total de transactions de cet élément, les transactions autorisées, les transactions bloquées, l'utilisation des données et les octets envoyés et reçus. Vous pouvez faire basculer les nombres entre **les valeurs** brutes et **les pourcentages**, et afficher les 10, 100 ou 1 000 principales entrées. Si l'élément est un lien, cliquez dessus pour afficher un tableau de bord récapitulatif avec des informations plus détaillées.

Étape 2 Cliquez sur les liens **Dashboard** (Tableau de bord) dans la table des matières pour afficher les tableaux de bord pour les données suivantes :

- **Network Overview**(Aperçu du réseau) : affiche des renseignements récapitulatifs sur le trafic dans le réseau, y compris les règles d'accès (politiques) correspondantes, les utilisateurs lançant le trafic, les applications utilisées dans les connexions, les menaces de prévention des intrusions (signatures) correspondantes, les web categories (catégories d'URL Web)) pour les URL consultées et les destinations les plus fréquentes pour les connexions.
- **Users (Utilisateurs)** : affiche les principaux utilisateurs de votre réseau. Vous devez configurer les politiques d'identité pour voir les informations des utilisateurs. S'il n'y a pas d'identité d'utilisateur, l'adresse IP source est incluse. Vous pourriez voir les entités spéciales suivantes :
  - **Failed Authentication** (Échec de l'authentification) : l'utilisateur a été invité à s'authentifier, mais n'a pas réussi à saisir une paire nom d'utilisateur/mot de passe valide dans le nombre maximal de tentatives autorisées. L'échec de l'authentification n'empêche pas l'utilisateur d'accéder au réseau, mais vous pouvez écrire une règle d'accès pour limiter l'accès au réseau pour ces utilisateurs.
  - **Guest** (Invité) : les utilisateurs invités sont similaires aux utilisateurs en Failed Authentication (Échec de l'authentification), sauf que votre règle d'identité est configurée pour identifier ces utilisateurs comme Guest (Invité). Les utilisateurs invités ont été invités à s'authentifier et n'ont pas réussi à le faire dans les limites du nombre maximal de tentatives.
  - **No Authentication Required** (Aucune authentification requise) : l'utilisateur n'a pas été invité à s'authentifier, car ses connexions correspondaient à des règles d'identité ne spécifiant aucune authentification.
  - **Unknown** (Inconnu) : aucun mappage d'utilisateur n'existe pour l'adresse IP et aucun échec d'authentification n'a encore été enregistré. En règle générale, cela signifie qu'aucun trafic HTTP n'a encore été vu à partir de cette adresse.
- **Applications** : affiche les principales applications, telles que HTTP, utilisées dans le réseau. Les informations sont disponibles uniquement pour les connexions qui sont inspectées. Les connexions sont inspectées si elles correspondent à une règle « autorisée » ou à une règle de blocage qui utilise des critères autres que la zone, l'adresse et le port. Ainsi, les informations d'application ne sont pas disponibles si la connexion est de confiance ou bloquée avant d'atteindre une règle nécessitant une inspection.
- **Web Applications** (Applications Web) : affiche les principales applications Web, comme Google, utilisées dans le réseau. Les conditions de collecte des informations sur les applications Web sont les mêmes que celles du tableau de bord des applications.
- **URL Categories (Catégories d'URL)** : affiche les principales catégories de sites Web, tels que jeux d'argent ou établissements d'enseignement, qui sont utilisées dans le réseau en fonction de la catégorisation des sites Web visités. Vous devez avoir au moins une règle de contrôle d'accès qui utilise la catégorie d'URL comme critère de correspondance de trafic pour obtenir ces informations. Les renseignements seront disponibles pour le trafic qui correspond à la règle ou pour le trafic qui doit être inspecté pour déterminer s'il correspond à la règle. Vous ne verrez pas les informations de catégorie (ou de réputation) pour les connexions qui correspondent à des règles antérieures à la première règle de contrôle d'accès de catégorie Web.
- **Access and SI Rules** (Règles d'accès et de Security Intelligence : affiche les principales règles d'accès et les équivalents de règles de Security Intelligence en correspondance avec le trafic réseau.
- **Zones** : affiche les principales paires de zones de sécurité pour le trafic entrant et sortant du périphérique.
- **Destinations** : affiche les principales destinations du trafic réseau.

- **Attackers** (Agresseurs) : affiche les principaux attaquants, qui sont la source des connexions qui déclenchent les incidents d'intrusion. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.
- **Targets** (Cibles) : affiche les cibles principales des incidents d'intrusion, qui sont les victimes d'une attaque. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.
- **Threats** (Menaces) : affiche les principales règles d'intrusion qui ont été déclenchées. Vous devez configurer des politiques d'intrusion sur les règles d'accès pour afficher ces informations.
- **File Logs** (Journaux de fichiers) : affiche les principaux types de fichiers vus dans le trafic réseau. Vous devez configurer des politiques de fichiers sur les règles d'accès pour afficher ces informations.
- **Malware** (Programmes malveillants) : affiche les principales combinaisons d'actions et de dispositions des programmes malveillants. Vous pouvez faire un zoom avant pour afficher les renseignements sur les types de fichiers associés. Vous devez configurer des politiques de fichiers sur les règles d'accès pour afficher ces informations.
  - Les actions possibles sont : Malware Cloud Lookup (Recherche dans le nuage de programmes malveillants), Block (Blocage), Archive Block (Encrypted) (Blocage d'archive – chiffré), Detect (Détection), Custom Detection (Détection personnalisée), Cloud Lookup Timeout (Expiration de la requête de recherche dans le nuage), Malware Block (Blocage de programmes malveillants), Archive Block (Depth Exceeded) (Blocage d'archive – profondeur dépassée), Custom Detection Block (Blocage de détection personnalisée), TID Block (Blocage TID), Archive Block (Failed to Inspect) (Blocage d'archive – échec de l'inspection).
  - Les dispositions possibles sont : Malware (Programme malveillant), Unknown (Inconnu), Clean (Propre), Custom Detection (Détection personnalisée), Unavailable (Non disponible).
- **SSL Decryption** (Déchiffrement SSL) : affiche la répartition du trafic chiffré et en texte brut via le périphérique, ainsi que la répartition de la façon dont le trafic chiffré a été déchiffré selon les règles de déchiffrement SSL.
- **System (Système)** : affiche une vue globale du système, y compris un affichage des interfaces et de leur état (passez le curseur sur une interface pour voir ses adresses IP), le débit moyen global du système (en tranches de 5 minutes jusqu'à une heure, puis en tranches d'une heure pour des périodes plus longues), ainsi que des renseignements récapitulatifs sur les événements du système, l'utilisation du processeur, l'utilisation de la mémoire et l'utilisation du disque. Vous pouvez restreindre le graphique de débit pour afficher une interface précise plutôt que toutes les interfaces.

  Remarque
  Les informations affichées dans le tableau de bord System (Système) se trouvent au niveau général du système. Si vous vous connectez à l'interface de ligne de commande du périphérique, vous pouvez utiliser diverses commandes pour afficher des informations plus détaillées. Par exemple, les commandes **show cpu** et **show memory** comprennent des paramètres pour afficher d'autres détails, alors que ces tableaux de bord affichent les données des commandes **show cpu system** et **show memory system**.

Étape 3 Vous pouvez également cliquer sur ces liens dans la table des matières :

- **Events (Événements)** : pour afficher les événements à mesure qu'ils se produisent. Vous devez activer la journalisation des connexions dans les règles d'accès individuelles pour voir les événements de connexion liés à ces règles. Activez également la journalisation dans la politique Security Intelligence et les règles de déchiffrement SSL pour voir les événements Security Intelligence et obtenir des données

d'événements de connexion supplémentaires. Ces événements peuvent vous aider à résoudre les problèmes de connexion de vos utilisateurs.

- **Sessions** : pour afficher et gérer les sessions utilisateur FDM. Pour en savoir plus, consultez Gérer les sessions des utilisateurs FDM.

Surveillance de statistiques supplémentaires à l'aide de l'interface de ligne de commande

Les tableaux de bord FDM fournissent une grande variété de statistiques liées au trafic passant par le périphérique et à l'utilisation générale du système. Cependant, vous pouvez obtenir des informations supplémentaires sur les domaines non couverts par les tableaux de bord en utilisant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique (voir Connexion avec l'interface de ligne de commande (CLI)).

L'interface de ligne de commande comprend une variété de commandes **show** pour fournir ces statistiques. Vous pouvez également utiliser l'interface de ligne de commande pour le dépannage général, y compris des commandes telles que **ping** et **traceroute**. La plupart des commandes **show** ont des commandes associées **clear** pour réinitialiser les statistiques à 0. (Vous ne pouvez pas effacer les statistiques à partir de la console d'interface de ligne de commande.)

Vous pouvez trouver la documentation pour les commandes dans Référence de commande Cisco Firepower Threat Defense, http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Par exemple, vous pourriez trouver les commandes suivantes généralement utiles.

- **show nat** affiche le nombre d'occurrences pour vos règles de NAT.
- **show xlate** affiche les traductions NAT actuellement actives.
- **show conn** fournit des renseignements sur les connexions actuelles passant par le périphérique.
- **show dhcpd** fournit des renseignements sur les serveurs DHCP que vous configurez sur les interfaces.
- **show interface** fournit des statistiques d'utilisation pour chaque interface.

Affichage des événements

Vous pouvez afficher les événements générés par vos politiques de sécurité qui permettent la journalisation. Des événements sont également générés pour les politiques de prévention des intrusions et de fichiers qui sont déclenchées.

Le tableau du visualiseur d'événements affiche les événements générés en temps réel. À mesure que de nouveaux événements sont générés, les événements plus anciens sont sortis de la table.

Avant de commencer

La génération d'événements de types particuliers dépend des éléments suivants en plus des connexions qui correspondent à la politique associée :

- Événements de connexion : une règle d'accès doit activer la journalisation des connexions. Vous pouvez aussi activer la journalisation des connexions dans la politique de renseignements sur la sécurité et dans les règles de déchiffrement SSL.
- Événements d'intrusion : une règle d'accès doit appliquer une politique de prévention des intrusions.
- Événements liés aux fichiers et aux programmes malveillants : une règle d'accès doit appliquer une politique de fichiers et activer la journalisation des fichiers.
- Événements liés aux renseignements sur la sécurité : vous devez activer et configurer la politique de renseignements sur la sécurité et activer la journalisation.

Procédure

Étape 1 Cliquez sur **Monitoring** (Surveillance) dans le menu principal.

Étape 2 Sélectionnez **Events** (Événements) dans la table des matières.

La visionneuse d'événements organise les événements sur des onglets en fonction des types d'événement. Pour en savoir plus, consultez Types d'événements, à la page 1.

Étape 3 Cliquez sur l'onglet qui affiche le type d'événement que vous souhaitez afficher.

Vous pouvez effectuer les opérations suivantes avec la liste d'événements :

- Cliquez sur **Pause** pour arrêter l'ajout de nouveaux événements afin de pouvoir rechercher et analyser un événement plus facilement. Cliquez sur **Resume** (Reprendre) pour permettre l'affichage des nouveaux événements.
- Sélectionnez une fréquence d'actualisation différente (5, 10, 20 ou 60 secondes) pour contrôler la vitesse d'affichage des nouveaux événements.
- Créez un affichage personnalisé qui inclut les colonnes que vous souhaitez. Pour créer un affichage personnalisé, cliquez sur le bouton + dans la barre d'onglets ou cliquez sur **Add/Remove Columns** (Ajouter/Supprimer des colonnes). Vous ne pouvez pas modifier les onglets prédéfinis ; ainsi, l'ajout ou la suppression de colonnes crée un nouvel affichage. Pour en savoir plus, consultez Configuration des vues personnalisées, à la page 10.
- Pour modifier la largeur d'une colonne, cliquez sur le séparateur d'en-tête de colonne et faites-le glisser jusqu'à la largeur souhaitée.
- Passez le curseur sur un événement et cliquez sur **View Details** (Afficher les détails) pour afficher les informations complètes sur un événement. Pour obtenir une description des différents champs d'un événement, consultez Description des champs d'événement, à la page 12.

Étape 4 Si nécessaire, appliquez un filtre au tableau pour vous aider à localiser les événements souhaités en fonction de divers attributs d'événement.

Pour créer un nouveau filtre, saisissez manuellement le filtre en sélectionnant des éléments atomiques dans la liste déroulante et en entrant la valeur du filtre, ou créez un filtre en cliquant sur une cellule du tableau des événements qui contient une valeur sur laquelle vous souhaitez filtrer. Vous pouvez cliquer sur plusieurs cellules dans la même colonne pour créer une condition OU parmi les valeurs, ou cliquer sur des cellules dans différentes colonnes pour créer une condition ET parmi les colonnes. Si vous créez le filtre en cliquant sur

les cellules, vous pouvez également modifier le filtre obtenu pour l'affiner. Pour plus d'informations sur la création de règles de filtrage, consultez Événements de filtrage, à la page 11.

Une fois que vous avez créé le filtre, effectuez l'une des opérations suivantes :

- Pour appliquer le filtre et mettre à jour le tableau afin d'afficher uniquement les événements qui correspondent au filtre, cliquez sur le bouton **Filter** (Filtrer).
- Pour effacer un filtre entier que vous avez appliqué et faire revenir le tableau à un état non filtré, cliquez sur **Reset Filters** (Réinitialiser les filtres) dans la zone **Filter** (Filtrer).
- Pour effacer l'un des éléments atomiques d'un filtre, passez le curseur sur l'élément et cliquez sur le **X** pour l'élément. Ensuite, cliquez sur le bouton **Filter** (Filtrer).

Configuration des vues personnalisées

Vous pouvez créer vos propres vues personnalisées afin de pouvoir voir facilement les colonnes que vous souhaitez lors de l'affichage des événements. Vous pouvez également modifier ou supprimer des vues personnalisées, bien que vous ne puissiez pas modifier ou supprimer les vues prédéfinies.

Procédure

Étape 1 Sélectionnez **Monitoring (Surveillance** > **Events (Événements)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un affichage basé sur un affichage personnalisé (ou prédéfini), cliquez sur l'onglet de l'affichage, puis cliquez sur le bouton **+** à gauche des onglets.
- Pour modifier un affichage personnalisé existant, cliquez sur l'onglet correspondant à l'affichage.

Remarque
Pour supprimer un affichage personnalisé, cliquez simplement sur le bouton **X** dans l'onglet de l'affichage. Cette suppression est irréversible.

Étape 3 Cliquez sur le lien **Add/Remove Columns** (Ajouter/Supprimer des colonnes) au-dessus du tableau des événements à droite, puis sélectionnez ou désélectionnez les colonnes jusqu'à ce que la liste sélectionnée ne comporte que les colonnes à inclure dans la vue.

Cliquez et faites glisser les colonnes entre les listes disponibles (mais non utilisées) et sélectionnées. Vous pouvez également cliquer et faire glisser les colonnes dans la liste sélectionnée pour modifier l'ordre de gauche à droite des colonnes dans le tableau. Pour une description des colonnes, consultez Description des champs d'événement, à la page 12.

Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer vos modifications de colonnes.

Remarque
Si vous modifiez la sélection de colonnes lors de l'affichage d'un affichage prédéfini, un nouvel affichage est créé.

Étape 4 Si nécessaire, modifiez la largeur des colonnes en cliquant sur les séparateurs de colonne et en les faisant glisser.

Événements de filtrage

Vous pouvez créer des filtres complexes pour limiter le tableau des événements aux événements qui vous intéressent actuellement. Vous pouvez utiliser les techniques suivantes, seules ou en combinaison, pour créer un filtre :

En cliquant sur les colonnes

La façon la plus simple de créer un filtre est de cliquer sur les cellules du tableau des événements qui contiennent les valeurs sur lesquelles vous souhaitez filtrer. Cliquer sur une cellule met à jour le champ **Filter** (Filtre) avec une règle correctement formulée pour cette combinaison de valeurs et de champ. Cependant, l'utilisation de cette technique nécessite que la liste d'événements existante contienne les valeurs souhaitées.

Vous ne pouvez pas filtrer sur toutes les colonnes. Si vous pouvez filtrer sur le contenu d'une cellule, elle est soulignée lorsque vous passez le curseur dessus.

Sélection d'éléments atomiques

Vous pouvez également créer un filtre en cliquant dans le champ **Filter** (Filtre) et en sélectionnant l'élément atomique souhaité dans la liste déroulante, puis en saisissant la valeur de correspondance. Ces éléments comprennent des champs d'événement qui ne sont pas affichés sous forme de colonnes dans le tableau des événements. Ils comprennent également des opérateurs pour définir la relation entre la valeur que vous saisissez et les événements à afficher. Alors que le fait de cliquer sur les colonnes entraîne toujours un filtre « = (=) », lorsque vous sélectionnez un élément, vous pouvez également sélectionner « supérieur à (>) » ou « inférieur à (<) » pour les champs numériques.

Quelle que soit la façon dont vous ajoutez un élément au champ **Filter** (Filtre), vous pouvez effectuer une saisie dans ce champ pour ajuster l'opérateur ou la valeur. Cliquez sur **Filter** (Filtre) pour appliquer le filtre au tableau.

Opérateurs pour les filtres d'événement

Vous pouvez utiliser les opérateurs suivants dans un filtre d'événement :

=	Est égal à. L'événement correspond à la valeur spécifiée. Vous ne pouvez pas utiliser de caractères génériques.
!=	N'est pas égal à. L'événement ne correspond pas à la valeur spécifiée. Vous devez saisir le ! (point d'exclamation) pour créer une expression non égale.
>	Supérieur à. L'événement contient une valeur supérieure à la valeur spécifiée. Cet opérateur est disponible pour les valeurs numériques uniquement, telles que le port et l'adresse IP.
<	Inférieur à. L'événement contient une valeur inférieure à la valeur spécifiée. Cet opérateur est disponible pour les valeurs numériques uniquement.

Règles pour les filtres d'événements complexes

Lors de la création d'un filtre complexe qui contient plusieurs éléments atomiques, gardez les règles suivantes à l'esprit :

- Les éléments du même type ont une relation OU entre toutes les valeurs de ce type. Par exemple, l'inclusion de l'initiateur IP=10.100.10.10 et de l'initiateur IP=10.100.10.11 correspond aux événements qui ont l'une de ces adresses comme source de trafic.
- Les éléments de différents types ont une relation ET. Par exemple, l'inclusion de l'initiateur IP=10.100.10.10 et du port de destination/type ICMP=80 correspond aux événements qui ont cette adresse source et ce port de destination uniquement. Les événements de 10.100.10.10 vers un autre port de destination ne sont pas affichés.
- Les éléments numériques, y compris les adresses IPv4 et IPv6, peuvent préciser des plages. Par exemple, vous pourriez spécifier Destination Port=50-80 pour enregistrer tout le trafic pour les ports de cette plage. Utilisez un tiret pour séparer les numéros de début et de fin. Les plages ne sont pas autorisées pour tous les champs numériques. Par exemple, vous ne pouvez pas spécifier une plage d'adresses IP dans l'élément Source.
- Vous ne pouvez pas utiliser de caractères génériques ou d'expressions régulières.

Description des champs d'événement

Les événements peuvent contenir les informations suivantes. Vous pouvez voir ces informations lorsque vous affichez les détails de l'événement. Vous pouvez également ajouter des colonnes au tableau du Visualiseur d'événements pour afficher les informations qui vous intéressent le plus.

Voici une liste complète des champs disponibles. Tous les champs ne s'appliquent pas à tous les types d'événement. Notez que les informations disponibles pour un événement de connexion peuvent varier selon le comment, le pourquoi et le moment où le système a enregistré la connexion.

Action

Pour les événements de connexion ou de renseignements de sécurité, l'action associée à la règle de contrôle d'accès ou à l'action par défaut ayant journalisé la connexion :

Autoriser

Connexions explicitement autorisées

Confiance

Connexions de confiance. Les connexions TCP détectées par une règle de confiance dès le premier paquet ne génèrent qu'un événement de fin de connexion. Le système génère l'événement une heure après le dernier paquet de session.

Bloquer

Connexions bloquées. L'action **Block (Bloquer)** peut être associée aux critères d'accès Allow (Autoriser) dans les conditions suivantes :

- Connexions pour lesquelles un exploit a été bloqué par une politique de prévention des intrusions.
- Connexions pour lesquelles un fichier a été bloqué par une politique de fichiers.
- Connexions bloquées par les renseignements de sécurité.

- Connexions bloquées par une politique SSL.

Action par défaut

Indique que la connexion a été traitée par l'action par défaut.

Pour les événements de fichier ou de programme malveillant, l'action de règle de fichier associée à l'action de règle pour la règle à laquelle le fichier correspond et toutes les options d'action de règle de fichier associées.

Connexion autorisée

Si le système a autorisé le flux du trafic pour l'événement.

Application

L'application détectée dans la connexion.

Pertinence commerciale de l'application

La pertinence commerciale associée au trafic d'application détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type d'application détectée dans la connexion est pertinent sur le plan commercial; ce champ affiche la valeur la plus basse (le type de moins pertinent) de ceux-ci.

Catégories d'applications, balise d'application

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

Risque lié à l'application

Le risque associé au trafic d'application détecté lors de la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type d'application détecté lors de la connexion est associé à un risque. ce champ affiche le plus élevé d'entre eux.

Type de bloc

Le type de blocage spécifié dans la règle de contrôle d'accès correspondant au flux de trafic dans l'événement : blocage ou bloc interactif.

Application client, version du client

L'application client et la version de ce client détectées dans la connexion.

Pertinence commerciale pour le client

La pertinence commerciale associée au trafic client détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type de client détecté dans la connexion est associé à une pertinence commerciale ; ce champ affiche la valeur la plus basse (le type de moins pertinent) de ceux-ci.

Catégorie du client, balise du client

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

Risque lié au client

Le risque associé au trafic client détecté lors de la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type de client détecté lors de la connexion est associé à un risque ; ce champ affiche le plus élevé d'entre eux.

Connexion

L'ID unique pour le flux de trafic, généré en interne.

Indicateur de type de bloc de connexion

Le type de blocage spécifié dans la règle de contrôle d'accès correspondant au flux de trafic dans l'événement : blocage ou bloc interactif.

Octets de connexion

Le nombre total d'octets pour la connexion.

Temps de connexion

Le temps pour le début de la connexion.

Horodatage de la connexion

L'heure à laquelle la connexion a été détectée.

Connexion refusée

Si le système a refusé le flux de trafic pour l'événement.

Pays et continent de destination

Le pays et le continent de l'hôte de réception.

IP de la destination

L'adresse IP utilisée par l'hôte de réception dans un incident d'intrusion, de fichier ou de programme malveillant.

Port de destination / code ICMP ; port de destination ; code de destination

Le port ou le code ICMP utilisé par le répondeur de session.

Balise de groupe de sécurité de destination, nom de la balise de groupe de sécurité de destination

Le numéro et le nom de la balise de groupe de sécurité TrustSec associés à la destination, le cas échéant.

Direction

La direction de la transmission d'un fichier.

Disposition

Disposition du fichier :

Maliciels

Indique que le Cisco AMP Cloud a classé le fichier comme programme malveillant ou que l'indice de menace du fichier a dépassé le seuil de programme malveillant défini dans la politique de fichiers. L'analyse locale des programmes malveillants peut aussi marquer des fichiers comme programmes malveillants.

Sain

Indique que le Cisco AMP Cloud a classé le fichier comme propre, ou qu'un utilisateur a ajouté le fichier à la liste des fichiers propres.

Inconnu

Indique que le système a interrogé le Cisco AMP Cloud, mais qu'aucune disposition n'a été attribuée au fichier ; en d'autres termes, le Cisco AMP Cloud n'a pas classé le fichier.

Détection personnalisée

Le fichier a été ajouté à la liste des détections personnalisées.

Non disponible

Indique que le système n'a pas pu interroger le Cisco AMP Cloud. Vous pouvez voir un faible pourcentage d'événements avec cette disposition; c'est un comportement attendu.

S. O.

Indique qu'une règle de détection de fichiers ou de blocage de fichiers a traité le fichier et que le système n'a pas interrogé le Cisco AMP Cloud.

Interface de sortie, Zone de sécurité de sortie

L'interface et la zone par lesquelles la connexion est sortie du périphérique.

Routeur virtuel de sortie

Le nom du routeur virtuel, le cas échéant, auquel l'interface de destination appartient.

Événement, Type d'événement

Le type d'événement.

Secondes de l'événement, Microsecondes de l'événement

L'instant, en secondes ou en microsecondes, où l'événement a été détecté.

Catégorie de fichier

Les catégories générales de type de fichier, par exemple : documents Office, Archive, Multimédia, Fichiers exécutables, Fichiers PDF, Codé, Graphique ou fichiers système.

Horodatage de l'événement du fichier

La date et l'heure de création du fichier (ou du fichier de programme malveillant).

Nom de fichier

Nom du fichier.

Action découlant d'une règle sur un fichier

L'action associée à la règle de fichiers qui a détecté le fichier, et toutes les options d'action associées à une règle de fichier.

SHA-256 du fichier

Valeur de hachage SHA-256 du fichier.

Taille du fichier (Ko)

La taille du fichier, en kilo-octets. La taille du fichier peut être vide si le système a bloqué le fichier avant sa réception complète.

Type de fichier (File Type)

Le type de fichier, par exemple HTML ou MSEXE.

Politique sur les fichiers et les programmes malveillants

La politique de fichiers associée à la génération de l'événement.

Indicateur de type de bloc de journal de fichier

Le type de blocage indiqué dans la règle de fichiers correspondant au flux de trafic dans l'événement : block (blocage) ou interactive block (blocage interactif).

Règle de politique de pare-feu, Règle de pare-feu

La règle de contrôle d'accès ou l'action par défaut qui a géré la connexion.

Premier paquet

La date et l'heure auxquelles le premier paquet de la session a été vu.

Référent HTTP

Référent HTTP, qui représente le référent d'une URL demandée pour le trafic HTTP détecté dans la connexion (comme un site Web qui a fourni un lien vers une autre URL ou a importé un lien vers une autre URL).

Réponse HTTP

Code d'état HTTP envoyé en réponse à une requête HTTP d'un client sur une connexion.

Classification IDS

La classification à laquelle appartient la règle qui a généré l'événement.

Interface d'entrée, Zone de sécurité d'entrée

L'interface et la zone par lesquelles la connexion est entrée dans le périphérique.

Routeur virtuel d'entrée

Le nom du routeur virtuel, le cas échéant, auquel l'interface source appartient.

Octets de l'initiateur, Paquets de l'initiateur

Le nombre total d'octets ou de paquets transmis par l'initiateur de la session.

Pays et continent de l'initiateur

Le pays et le continent de l'hôte qui a lancé la session. Disponible uniquement si l'adresse IP de l'initiateur est routable.

IP de l'initiateur

L'adresse IP de l'hôte (et le nom d'hôte, si la résolution DNS est activée) qui a lancé la session dans un événement de connexion ou de renseignements de sécurité.

Résultat en ligne

Si le système a abandonné ou aurait abandonné le paquet qui a déclenché un incident d'intrusion s'il travaillait en mode en ligne. La règle déclenchée n'est pas réglée sur Drop and Generate Events (Abandonner et générer des événements).

Politique de prévention des intrusions

La politique de prévention des intrusions à laquelle la règle de prévention des intrusions, de préprocesseur ou de décodeur qui a généré l'événement a été activée.

Indicateur de type de bloc IPS

L'action de la règle de prévention des intrusions correspondant au flux de trafic dans l'événement.

Dernier paquet

La date et l'heure auxquelles le dernier paquet de la session a été vu.

Étiquette MPLS

L'étiquette de commutation multiprotocole par étiquette (MPLS) associée au paquet qui a déclenché l'incident d'intrusion.

Indicateur de type de bloc de programme malveillant

Le type de blocage indiqué dans la règle de fichiers correspondant au flux de trafic dans l'événement : block (blocage) ou interactive block (blocage interactif).

Message

Pour les événements d'intrusion, le texte explicatif de l'événement. Pour les événements de programme malveillant ou de fichier, toutes les informations supplémentaires associées à l'événement de programme malveillant.

IP de destination de la NAT

Pour les paquets soumis à la traduction d'adresses réseau (NAT), l'adresse IP de destination traduite.

Port de destination de la NAT

Pour les paquets soumis à la traduction d'adresses réseau (NAT), le port de destination traduit.

IP source de la NAT

Pour les paquets soumis à la traduction d'adresses réseau (NAT), l'adresse IP source traduite.

Port source de la NAT

Pour les paquets soumis à la traduction d'adresses réseau (NAT), le port source traduit.

Domaine NetBIOS

Le domaine NetBIOS utilisé dans la session

Pays et continent du client d'origine

Le pays et le continent de l'hôte client d'origine qui a lancé la session. Disponible uniquement si l'adresse IP du client d'origine est routable.

IP du client d'origine

L'adresse IP d'origine du client qui a lancé une connexion HTTP. Cette adresse est dérivée des champs d'en-tête X-Forwarded-For (XFF) ou True-Client-IP HTTP ou de leur équivalent.

Politique, Révision de la politique

La stratégie de contrôle d'accès et sa révision, qui comprend la règle d'accès (pare-feu) associée à l'événement.

Priorité

La priorité de l'événement déterminée par Cisco Talos Intelligence Group (Talos) : élevée, moyenne ou basse.

Protocole

Le protocole de transport utilisé dans la connexion.

Motif

La ou les raisons pour lesquelles la connexion a été enregistrée, dans les situations expliquées dans le tableau suivant. Ce champ est autrement vide.

Motif	Description
Blocage DNS	Le système a refusé la connexion sans inspection, en fonction du nom de domaine et des données de Security Intelligence. Une raison de blocage DNS est jumelée à une action de blocage, Domaine introuvable ou Gouffre, selon l'action de règle DNS.
Moniteur DNS	Le système aurait refusé la connexion en fonction du nom de domaine et des données Security Intelligence, mais vous avez configuré le système pour surveiller, plutôt que refuser, la connexion.
Flux d'éléphants	La connexion est suffisamment importante pour être considérée comme étant un flux d'éléphants, c'est-à-dire un flux qui peut être suffisamment volumineux pour affecter les performances globales du système. Par défaut, les elephant flows (flux d'éléphants) sont ceux dont la taille est supérieure à 1 Go/10 secondes. Vous pouvez régler les seuils d'octets et de temps pour l'identification des flux d'éléphants dans la CLI du périphérique à l'aide de la commande **system support elephant-flow-detection**.
Blocage de fichiers	La connexion contient un fichier ou un programme malveillant dont le système a empêché la transmission. Un motif de blocage de fichier est toujours associé à une action de blocage de fichier.
Détection personnalisée de fichier	La connexion contient un fichier de la liste de détection personnalisée dont le système a empêché la transmission.
Moniteur de fichiers	Le système a détecté un type de fichier particulier dans la connexion.
Autoriser la reprise du fichier	La transmission de fichiers a été bloquée à l'origine par une règle de blocage des fichiers ou de blocage de fichiers malveillants. Après le déploiement d'une nouvelle politique de contrôle d'accès autorisant le fichier, la session HTTP a repris automatiquement.
Blocage de reprise des fichiers	La transmission de fichiers était à l'origine autorisée par une règle de fichier Detect Files ou Malware Cloud Lookup. Après le déploiement d'une nouvelle politique de contrôle d'accès bloquant le fichier, la session HTTP s'est arrêtée automatiquement.
Blocage de prévention des intrusions	Le système a bloqué ou aurait bloqué un exploit (violation de politique de prévention des intrusions) détecté dans la connexion. Une cause de blocage de prévention des intrusions est jumelée à une action de blocage pour les exploits bloqués et d'autorisation pour les exploits qui auraient été bloqués.
Moniteur de prévention des intrusions	Le système a détecté, mais n'a pas bloqué, un exploit détecté dans la connexion. Cela se produit lorsque l'état de la règle de prévention des intrusions déclenchée est défini sur Generate Events (générer des événements).
Blocage d'adresse IP	Le système a refusé la connexion sans inspection, en fonction de l'adresse IP et des données de Security Intelligence. Un motif de blocage d'IP est toujours associé à une action de blocage.

Motif	Description
Blocage SSL	Le système a bloqué une connexion chiffrée en fonction de la configuration d'inspection SSL. Un motif de blocage SSL est toujours associé à une action de blocage.
Blocage d'URL	Le système a refusé la connexion sans inspection, en fonction de l'URL et des données de Security Intelligence. Un motif de blocage d'URL est toujours associé à une action de blocage.

Heures de réception

La date et l'heure auxquelles l'événement a été généré.

Hôte référencé

Si le protocole de connexion est HTTP ou HTTPS, ce champ affiche le nom d'hôte utilisé par le protocole respectif.

Octets du répondeur, Paquets du répondeur

Le nombre total d'octets ou de paquets transmis par le répondeur de session.

Pays et continent du répondeur

Le pays et le continent de l'hôte qui a répondu à la session. Disponible uniquement si l'adresse IP du répondeur est routable.

IP du répondeur

L'adresse IP de l'hôte (et le nom d'hôte, si la résolution DNS est activée) du répondeur de session dans une connexion ou un événement de renseignements de sécurité.

SI Category ID (Catégorie de renseignements de sécurité)

Le nom de l'objet qui contient l'élément bloqué, tel qu'un nom d'objet de réseau ou d'URL, ou le nom d'une catégorie de flux.

Signature :

L'ID de signature pour un événement lié à un fichier ou à un programme malveillant.

Pays et continent de la source

Le pays et le continent de l'hôte d'envoi. Disponible uniquement si l'adresse IP source est routable.

IP de la source

L'adresse IP utilisée par l'hôte expéditeur dans un événement d'intrusion, de fichier ou de programme malveillant.

Port source/type ICMP ; Port source ; Type de port source

Le port ou le type ICMP utilisé par l'initiateur de la session.

Balise du groupe de sécurité source, Nom de la balise du groupe de sécurité source

Le numéro de balise du groupe de sécurité TrustSec et le nom associé à la source, le cas échéant.

Action réelle du SSL

L'action réelle que le système a appliquée à la connexion. Cette action peut différer de l'action attendue. Par exemple, une connexion peut correspondre à une règle qui applique le déchiffrement, mais qui n'a pas pu être déchiffrée pour une raison quelconque.

Action	Description
Bloquer/Bloquer avec réinitialisation	Représente les connexions chiffrées bloquées.
Déchiffrer (Resigner)	Représente une connexion sortante déchiffrée à l'aide d'un certificat de serveur re-signé.
Déchiffrer (remplacer la clé)	Représente une connexion sortante déchiffrée à l'aide d'un certificat de serveur autosigné avec une clé publique remplacée.
Déchiffrer (clé connue)	Représente une connexion entrante déchiffrée à l'aide d'une clé privée connue.
Action par défaut	Indique que la connexion a été gérée par l'action par défaut.
Ne pas déchiffrer	Représente une connexion que le système n'a pas déchiffrée.

Empreinte digitale du certificat SSL

Valeur de hachage SHA utilisée pour authentifier le certificat.

Statut du certificat SSL

Cela s'applique uniquement si vous avez configuré une condition de règle SSL État du certificat. Si le trafic chiffré correspond à une règle SSL, ce champ affiche une ou plusieurs des valeurs d'état de certificat de serveur suivantes :

- Autosigné
- Valide
- Signature non valide
- Émetteur non valide
- Expiré
- Inconnu
- Non valide pour le moment
- Retiré

Si le trafic non déchiffrable correspond à une règle SSL, ce champ affiche Not Checked (Non contrôlé).

Suite de chiffrement SSL

La suite de chiffrement utilisée dans la connexion.

Action attendue de SSL

L'action spécifiée dans la règle SSL à laquelle la connexion correspond.

Indicateurs de flux SSL

Les dix premiers indicateurs de niveau de débogage pour une connexion chiffrée.

Messages de flux SSL

Les messages SSL/TLS échangés entre le client et le serveur lors de l'établissement de liaison SSL, tels que HELLO_REQUEST et CLIENT_HELLO. Consultez http://tools.ietf.org/html/rfc5246 pour obtenir plus d'informations sur les messages échangés dans les connexions TLS.

Protocole SSL

Le nom de la politique de déchiffrement SSL appliquée à la connexion.

Règle SSL

Le nom de la règle de déchiffrement SSL appliquée à la connexion.

ID de la session SSL

L'ID de session hexadécimal négocié entre le client et le serveur lors de l'établissement de liaison.

Identifiant du billet SSL

Valeur de hachage hexadécimale des informations du ticket de session envoyées lors de l'établissement de la liaison SSL.

Catégorie d'URL SSL

La catégorie d'URL du serveur Web de destination telle qu'elle est déterminée lors du traitement du déchiffrement SSL.

Version SSL

La version SSL/TLS utilisée dans la connexion.

Indicateurs TCP

Les indicateurs TCP détectés dans la connexion.

Total des paquets

Le nombre total de paquets transmis lors de la connexion, qui comprend **Initiator Packets** (Paquets de l'initiateur) et **Responder Packets** (Paquets du répondeur).

URL, catégorie d'URL, réputation d'URL, score de réputation d'URL

L'URL demandée par l'hôte surveillé au cours de la session ainsi que sa catégorie, sa réputation et son score de réputation associés, le cas échéant.

Pour le filtrage des demandes de recherche DNS, la catégorie et la réputation concernent le FQDN affiché dans le champ DNS Query (Requête DNS). Le champ URL sera vide, car la recherche de catégorie/réputation est effectuée pour une demande DNS plutôt que pour une demande Web.

Si le système identifie ou bloque une application SSL, l'URL demandée est dans le trafic chiffré, de sorte que le système identifie le trafic selon un certificat SSL. Pour les applications SSL, ce champ indique donc le nom usuel contenu dans le certificat.

Utilisateur

L'utilisateur associé à l'adresse IP de l'initiateur.

VLAN

L'ID de VLAN le plus à l'intérieur associé au paquet qui a déclenché l'incident.

Pertinence commerciale des applications Web

La pertinence commerciale associée au trafic d'application Web détecté dans la connexion : très élevée, élevée, moyenne, faible ou très faible. Chaque type d'application Web détectée dans la connexion a une pertinence commerciale associée ; ce champ affiche la plus faible (la moins pertinente) d'entre elles.

Catégories d'applications Web, étiquette d'application Web

Critères qui caractérisent l'application pour vous aider à comprendre la fonction de l'application.

Risque lié aux applications Web

Le risque associé au trafic d'application Web détecté dans la connexion : très élevé, élevé, moyen, faible ou très faible. Chaque type d'application détecté lors de la connexion est associé à un risque; ce champ affiche le plus élevé d'entre eux.

Application Web

L'application Web, qui représente le contenu ou l'URL demandée pour le trafic HTTP détecté dans la connexion.

Si l'application Web ne correspond pas à l'URL de l'événement, le trafic est probablement référencé, comme le trafic publicitaire. Si le système détecte du trafic référencé, il stocke l'application de référence (si disponible) et répertorie cette application comme application Web.

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.