IBM Security QRadar Incident Forensics
Version 7.2.6

Guide d'administration

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 21.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.6 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Introduction à l'administration d'IBM Security QRadar Incident Forensics

Informations sur l'administration d'IBM® Security QRadar Incident Forensics.

Audience visée

Les administrateurs créent, gèrent et exécute une fonction Forensics de sorte que les utilisateurs, appelés examinateurs, puissent se concentrer sur l'examen des incidents de sécurité, ou cas, et l'exploration des données.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez àIBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à plus de documentation technique dans la bibliothèque produit QRadar, voir Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à

s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

Important

IBM Security QRadar Incident Forensics est conçu pour aider les sociétés à améliorer leur environnement et leurs données de sécurité. Plus spécifiquement, IBM Security QRadar Incident Forensics est conçu pour aider les sociétés à examiner et à mieux comprendre ce qui s'est produit dans les incidents de sécurité réseau. L'outil permet aux sociétés d'indexer et de rechercher les données des paquets réseau capturés (PCAP) et inclut une fonction qui permet de reconstruire ces données à leur format initial. Cette fonction de reconstruction permet de reconstruire des données et des fichiers, dont des messages électroniques, des fichiers et des images joints, des appels téléphoniques voix sur IP (VoIP) et des sites Web. Des informations complémentaires sur les caractéristiques et les fonctions du programme et la façon dont elles peuvent être configurés figurent dans les manuels et les autres documents accompagnant le programme. L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar Incident Forensics ne peut être utilisé qu'à des fins légales, dans le respect de la loi. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le propriétaire de la licence atteste qu'il a obtenu ou va obtenir les accords, autorisations ou licences nécessaire à l'activation légale d'IBM Security QRadar Incident Forensics.

Chapitre 1. Nouveautés pour les administrateurs dans QRadar Incident Forensics version 7.2.6

IBM Security QRadar Incident Forensics version 7.2.6 introduit de nouveaux inspecteurs qui identifient d'autres protocoles, domaines Web et types de fichier. Les administrateurs peuvent également auditer les utilisateurs et l'utilisation du système.

QRadar Incident Forensics peut traiter davantage de protocoles, de domaines Web et de types de fichier

Davantage d'inspecteurs, capables d'identifier plusieurs protocoles, domaines Web et types de fichier dans les fichiers PCAP et les documents envoyés par téléchargement, sont désormais pris en charge.

SPDY Protocole réseau ouvert utilisé pour le transport de contenu Web qui a été développé pour réduire le temps nécessaire au chargement des pages Web et pour améliorer la sécurité.

Samba (SMB)
Protocole pour le partage de fichiers, d'imprimantes, de ports série et de communications, comme les canaux de communication et les emplacements de courrier entre ordinateurs. La version 1 est prise en charge.

Web app classification (WAC)
QRadar Incident Forensics inspecte une URL et peut identifier le type d'application Web et de fonctionnement. Il utilise ensuite ces informations pour classifier le trafic en classes, en fonction de chaque application Web et fonctionnement.

Détection d'application QFlow
La détection d'application QFlow est utilisée lorsqu'aucun autre inspecteur ne peut détecter une application, une session ou un protocole. Elle inspecte les 64 premiers octets d'un paquet à la recherche d'une signature et essaie d'identifier l'application à partir de la signature et du port.

 En savoir plus...

Journaux d'audit pour le suivi et l'enregistrement de l'activité des utilisateurs et des applications

Les journaux d'audit fournissent une visibilité de ce que font les analystes de sécurité, y compris les mesures qu'ils prennent, les données auxquelles ils accèdent et les informations qu'ils consultent. Les preuves documentaires enregistrent la séquence des activités qui ont lieu au cours d'une enquête.

Les activités suivantes génèrent des événements dans les journaux d'audit :

- Créer un cas
- Supprimer un cas
- Supprimer une collecte
- Requêtes de tous les utilisateurs
- Vue Document

- Exporter un document

 En savoir plus...

Chapitre 2. Flux d'administration et accès utilisateur aux fonctions de Forensics

Une fois IBM Security QRadar Incident Forensics installé et configuré, un administrateur peut dépanner, gérer et surveiller le système et ses opérations. Il peut aussi gérer l'accès des utilisateurs aux cas.

Vous devez disposer des privilèges d'administration pour afficher les outils d'administration de QRadar Incident Forensics.

Exemple de flux de travaux d'administration

Le diagramme ci-après illustre un exemple de flux de travaux pour l'administration de QRadar Incident Forensics.

1. Utilisez la fonction de gestion de serveur pour filtrer les catégories Web et le trafic que vous ne voulez pas surveiller.
2. Utilisez la fonction Droits utilisateur de Forensics pour affecter des cas aux examinateurs.
3. Utilisez la fonction Gestion des cas pour créer et supprimer des cas et importer du contenu externe sur le système.
4. Utilisez la fonction Actions planifiées pour planifier la maintenance, par exemple la suppression d'anciens documents, le paramétrage de la base de données et la reconfiguration du serveur QRadar Incident Forensics.

Rôles utilisateur

Pour ajouter des comptes utilisateur, vous devez d'abord créer des profils de sécurité pour répondre aux besoins d'accès spécifiques de vos utilisateurs. Pour plus d'informations sur la configuration des profils de sécurité, consultez le manuel *IBM Security QRadar SIEM Administration Guide*.

Dans l'outil Rôles utilisateur, sous l'onglet **Admin** de QRadar, vous pouvez affecter les rôles utilisateur suivants :

Admin
: Les utilisateurs peuvent visualiser et accéder à tous les cas qui sont affectés aux utilisateurs et à tous les incidents et ils disposent automatiquement d'un accès complet à QRadar Incident Forensics.

Forensics
: Les utilisateurs peut afficher et accéder à l'onglet **Forensics**, mais ils ne peuvent pas créer de cas.

Create cases in Incident Forensics
: Les utilisateurs peuvent créer automatiquement des cas Forensics.

Chapitre 3. Gestion des serveurs

Les administrateurs peuvent dépanner, gérer et surveiller le système IBM Security QRadar Incident Forensics et ses opérations.

Pour surveiller ou modifier les paramètres de serveur ou pour afficher les utilisateurs qui sont connectés au système, lancez l'outil Gestion de serveur :

1. Connectez-vous à QRadar en tant qu'administrateur.
2. Cliquez sur l'onglet **Admin**.
3. Depuis la section **Forensics** du volet principal, cliquez sur **Gestion de serveur**.

Paramètres de configuration du serveur

Utilisez les paramètres du serveur dans l'outil de gestion de serveur IBM Security QRadar Incident Forensics pour configurer les paramètres système qui affectent tous les hôtes gérés. Après avoir modifié un paramètre, vous devez déployer vos modifications en utilisant le menu **Déployer les changements** dans l'onglet **Admin**.

Effacement de l'historique de recherche à la déconnexion
L'historique de recherche est effacé lorsque les utilisateurs se déconnectent. La recherche effacée concerne la liste de l'historique de requêtes dans l'assistant de requête et le dernier utilisateur mentionné dans la zone **Search Criteria Input** de la page Search and Results.

Nombre de noeuds à visualiser par défaut
Nombre maximal de noeuds que l'outil de visualisation peut afficher. Vous pouvez configurer le nombre de noeuds à afficher lorsque les noeuds ont été affichés une première fois. Le paramétrage du nombre de noeuds affichés concerne uniquement cette instance de l'outil de visualisation.

Filtres de l'inspecteur de protocole et de domaine

Vous pouvez exclure certains types de trafic des examens en désactivant les inspecteurs de protocole ou de domaine dans l'outil Gestion de serveur. Utilisez l'option **Inspector Filter**.

Les inspecteurs de protocole et de domaine traitent les données de trafic réseau versées et tentent d'identifier et d'indexer les données de façon significative. L'identification et l'indexation de ces données permet aux examinateurs d'avoir un plus grand contrôle pour la recherche des informations.

Dès lors que les données de trafic réseau sont versées et que les protocoles sont identifiés, les données sont encore inspectées par l'inspecteur de protocole approprié. Les données de trafic réseau qui sont identifiées par l'inspecteur de protocole HTTP sont de nouveau inspectées et indexées par les inspecteurs de domaine.

Inspecteur de protocole
Les inspecteurs de protocole peuvent identifier des protocoles tels que HTTP, POP3, FTP et telnet. Vous pouvez exclure des inspecteurs de protocole. Lorsque des inspecteurs sont exclus, toutes les données de trafic

réseau qui sont associées à l'inspecteur sont encore versées mais le trafic est identifié et indexé uniquement à un niveau générique.

Inspecteurs de domaine
Les inspecteurs de domaine inspectent des sites web spécifiques. Vous pouvez exclure des inspecteurs de domaine. Lorsque vous excluez des inspecteurs de domaine, toutes les données de trafic réseau HTTP qui sont associées à l'inspecteur sont encore versées mais le trafic est identifié et indexé uniquement à un niveau HTTP. Pour que les inspecteurs de domaine soient actifs, l'inspecteur de protocole HTTP doit aussi être actif.

Par défaut, tous les filtres sont activés et vous pouvez voir le trafic provenant de tous les protocoles. La seule exception est le trafic SIP (Session Initiation Protocol). Ce protocole d'établissement d'appel, qui fonctionne au niveau de la couche d'application, est désactivé par défaut.

A faire : Lorsque vous modifiez la configuration des filtres d'inspecteur, la nouvelle configuration est appliquée à chaque nouveau cas créé. Les inspecteurs qui sont activés ont une influence sur les documents qui sont créés pour un cas et les enquêteurs perdent la capacité de rechercher certains inspecteurs. Les utilisateurs ne savent quels sont les inspecteurs qui sont appliqués à un cas.

Tout protocole qui n'est pas traité par un inspecteur est catégorisé comme inconnu.

Filtre de catégories Web

Vous pouvez choisir les types de pages Web et serveurs Web qui sont reconnus à l'aide de filtres de catégories Web.

Par exemple, vous pouvez exclure certains types de trafics réseau HTTP des enquêtes. Lorsque des données de trafic réseau HTTP sont versées, elles sont classées et les documents qui en résultent sont regroupés.

Les administrateurs peuvent filtrer les données de trafic réseau HTTP pour empêcher que les données soient versées.

Pour exclure, ou filtrer, le trafic pour une catégorie ou un groupe, désactivez ce groupe ou cette catégorie dans l'outil Gestion de serveur.

La catégorisation, le regroupement et le filtrage Web affectent les données de trafic réseau HTTP lorsqu'elles sont versées et n'ont aucun effet sur les données qui se trouvent déjà sur le système.

Lorsqu'un filtre de groupe est défini de manière à exclure les données, les données de trafic réseau HTTP qui sont associées aux catégories de ce groupe sont filtrées afin d'être exclues lors de l'utilisation, quelle que soit la catégorie associée.

Exemple : qu'advient-il lorsque vous utilisez un filtre de catégorie Web pour exclure le trafic ?

Vous décidez d'exclure le trafic qui contient des données provenant de sites d'actualités ou de magazines.

1. Sous l'onglet **Admin** de QRadar, cliquez sur **Gestion de serveur**.
2. Cliquez sur **Web Category Filter** et sur **Off** en regard du filtre **News / Magazines**.
3. Cliquez sur le filtre **Webmail / Unified Messaging**, puis sur **On**.

A présent, lorsqu'un utilisateur examine le trafic versé dans l'onglet **Forensics**, il voit que le trafic qui contient à la fois des données **News / Magazines** et **Webmail / Unified Messaging** n'est pas versé même si le filtre **Webmail / Unified Messaging** est activé.

Protocoles et types de document pris en charge

IBM Security QRadar Incident Forensics capture le contenu des paquets de flux réseau puis indexe et traite le contenu et les métadonnées.

La liste ci-dessous décrit les protocoles pris en charge que QRadar Incident Forensics peut traiter :

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB
- SMTP
- SPDY
- TLS (SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

La liste ci-dessous décrit les domaines pris en charge (sites web) et les langues prises en charge que QRadar Incident Forensics peut traiter :

- AOL (Accessible, Basic, Standard) (EN)
- Charter (EN)
- Facebook (Mobile, Desktop) (AR,CN,DE,EN,ES,FR,RU)
- Gmail (Classic, Standard) (AR,CN,DE,EN,ES,FR,RU)
- Hotmail (AR,CN,DE,EN,ES,FR,RU)
- LinkedIn (DE,EN,ES,FR,RU)
- MailCom (CN,EN,ES,FR,RU)
- MailRu (RU)
- Maktoob (AR,EN)
- Myspace (EN)

- QQMail (EN,CN)
- Twitter (EN)
- YAHOO Mail (Standard, Classic) (EN)
- YAHOO Note (EN)
- YouTube (AR,CN,DE,EN,ES,FR,RU)
- Comcast (Zimbra) (EN)

La liste ci-dessous décrit les formats de document pris en charge que QRadar Incident Forensics peut traiter :

- HyperText Markup Language
- XML et formats dérivés
- Formats de document Microsoft Office
- Format OpenDocument
- Format de Document Portable
- Format Electronic Publication Format
- Format de texte riche (RTF)
- Formats de compression et de conditionnement
- Formats texte
- Formats audio
- Formats d'image
- Formats vidéo
- Fichiers et archives de classe Java™
- Format mbox

Détection d'application QFlow

La détection d'application QFlow est utilisée lorsqu'aucun autre inspecteur ne peut détecter une application, une session ou un protocole. Elle inspecte les 64 premiers octets d'un paquet à la recherche d'une signature et essaie d'identifier l'application à partir de la signature et du port. Les exemples d'applications, de sessions ou de protocoles que l'application QFlow peut être en mesure d'identifier incluent, sans toutefois s'y limiter, les éléments ci-après.

- BitTorrent
- Blubster
- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- PeerEnabler
- Piolet
- UpdateDaemon
- VNC

Chapitre 4. Gestion des cas

En tant qu'administrateur, vous pouvez gérer des cas et des collectes à l'aide de la fonction Gestion des cas. Vous pouvez créer des cas pour les collectes de documents ou les fichiers de capture de paquet (pcap) et aussi importer des fichiers externes sur le système IBM Security QRadar Incident Forensics.

Optimisation de la gestion des cas

Pour affiner la gestion des cas, vous pouvez utiliser l'option **Flush**. Pour les données *pcap de diffusion*, qui constituent une série de fichiers pcap liés de manière logique pour former un fichier pcap volumineux, vous pouvez forcer les données en mémoire tampon à écrire sur le disque. L'option **Flush** force les hôtes QRadar Incident Forensics à écrire des flux non terminés sur disque, ce qui simplifie ultérieurement la recherche dans ces flux.

Graphiques de distribution

Si vous prévoyez de supprimer un cas, vous pouvez utiliser les graphiques de manière visuelle pour passer rapidement en revue le contenu du cas. Vous pouvez vérifier le type de fichier, les protocoles et les domaines dans le cas.

Téléchargement de fichiers pcap vers des hôtes gérés

Vous pouvez télécharger manuellement les données pcap à partir de sources externes. Vous pouvez spécifier sur quel hôte géré QRadar Incident Forensics vous souhaitez télécharger les données pour traitement. Par exemple, si vous avez trois hôtes gérés et trois fichiers pcap, vous pouvez télécharger chacun vers un hôte géré différent. Pour les fichiers pcap plus volumineux, utilisez FTP.

Création des cas

Les cas sont des conteneurs logiques pour votre collecte de fichiers document et PCAP importés. Vous pouvez utiliser un seul cas pour tous les fichiers pcap ou créer plusieurs cas. Les cas peuvent être restreints à des utilisateurs spécifiques.

Procédure

1. Sous l'onglet **Admin**, sélectionnez **Gestion de cas**.
2. Cliquez sur l'option **Ajouter Nouveau**.
3. Dans la zone **Nom de cas**, entrez un nom unique.

   Restriction : Les noms de cas ne peuvent pas contenir d'espaces.
4. Cliquez sur **Sauvegarder**.

Résultats

Un nouveau répertoire basé sur le nom du cas est créé : `/case_input/<case_name>`. Ce répertoire est utilisé pour importer vos fichiers PCAP.

Envoi par téléchargement de fichiers aux cas

En tant qu'administrateur, vous pouvez télécharger des fichiers et des documents externes de capture de paquets (pcap), tels que des tableurs, des fichiers texte et des fichiers image, vers la fonction de gestion des cas IBM Security QRadar Incident Forensics.

Les types de fichiers suivants sont pris en charge :

- HyperText Markup Language
- XML et formats dérivés
- Formats de document Microsoft Office
- Format OpenDocument
- Format de Document Portable
- Format Electronic Publication Format
- Format de texte riche (RTF)
- Formats de compression et de conditionnement
- Formats texte
- Formats audio
- Formats d'image
- Formats vidéo
- Fichiers et archives de classe Java
- Format mbox

Cette fonction restreint le nombre de fichiers que vous pouvez ajouter à un cas ainsi que la taille de fichier maximum.

Procédure

1. Sous l'onglet **Admin**, dans la section **Forensics**, cliquez sur **Gestion de cas**.
2. Sélectionnez un cas.
   - Pour ajouter des fichiers externes à un cas existant, sélectionnez ce cas dans la liste des **cas**.
   - Pour ajouter des fichiers à un nouveau cas, cliquez sur l'option **Ajouter Nouveau**.

     Restriction : Les noms de cas ne peuvent pas contenir d'espaces.
3. Dans la liste d'**envoi par téléchargement vers l'hôte**, sélectionnez l'hôte géré dont vous souhaitez traiter les fichiers.
4. Pour ajouter des fichiers pcap ou d'autres types de documents, choisissez l'une des méthodes suivantes :
   - Cliquez sur **Ajouter pcaps**, sélectionnez les fichiers, puis cliquez sur **Démarrer l'envoi par téléchargement**.
   - Faites glisser les fichiers vers la boîte de téléchargement.

   Une fois l'envoi par téléchargement terminé, les fichiers apparaissent dans la liste **Collectes**.

Chapitre 5. Affectation de cas aux utilisateurs

En tant qu'administrateur, vous pouvez accorder aux utilisateurs l'accès aux données Forensics, affecter des cas aux utilisateurs et configurer les droits d'accès des utilisateurs, par exemple l'accès FTP. Les utilisateurs ne peuvent pas afficher des données tant qu'aucun cas ne leur a été affecté et ils peuvent uniquement afficher les données des cas auxquels ils sont affectés.

Soyez prudent lorsque vous affectez des cas aux utilisateurs non administrateurs qui ont un accès restreint aux réseaux. Ils peuvent voir des documents qui proviennent des adresses IP auxquelles ils n'ont pas normalement accès. Par exemple, si vous affectez à un utilisateur non administrateur un cas qui contient des informations sur les ressources financières ou humaines, il peut voir les données quand il examine le cas.

Pourquoi et quand exécuter cette tâche

Les administrateurs peuvent effectuer les tâches suivantes :

- Affecter plusieurs utilisateurs à un cas.
- Supprimer un cas d'un utilisateur.
- Visualiser et accéder à tous les cas qui sont affectés à un utilisateur.

Les utilisateurs peuvent uniquement afficher les cas qui leur sont explicitement affectés.

Procédure

1. Cliquez sur l'onglet **Admin**, puis sur **Droits utilisateur Forensics**.
2. Dans la liste **Utilisateurs**, sélectionnez un utilisateur.
3. Dans la liste de cas **Disponible**, sélectionnez un ou plusieurs cas et cliquez sur la flèche (>) pour déplacer ces cas vers la liste **Affectés**.

   Conseil : Par défaut, un utilisateur doté de privilèges d'administration est affecté à tous les cas. Les flèches gauche (<) et droite (>) ne sont pas affichées.

Importation manuelle de fichiers dans un cas Forensics

A la différence de l'outil de gestion des cas, il n'y a pas restrictions concernant la taille de fichier ou le nombre de fichiers lorsque vous procédez à l'importation manuelle de fichiers. Vous pouvez créer manuellement un cas et y copier des fichiers ou copier manuellement des fichiers dans un cas existant.

Par exemple, vous pouvez utiliser la commande **scp** pour copier de manière sécurisée des fichiers d'un autre hôte dans le répertoire `/opt/ibm/forensics/case_input/case_input/` sur l'hôte IBM Security QRadar Incident Forensics.

Avant de commencer

Effectuez une copie de sauvegarde des fichiers importés. Une fois le fichier importé et traité, le fichier d'origine est supprimé.

Procédure

1. A l'aide de SSH, connectez-vous à QRadar Incident Forensics en tant que superutilisateur.
2. Pour créer un nouveau cas, accédez au répertoire `/opt/ibm/forensics/case_input` et entrez la commande suivante :

   `mkdir /opt/ibm/forensics/case_input/<case_name>`
3. Pour copier des fichiers dans un cas, utilisez une commande **scp** ou un autre programme de transfert de fichier pour copier les fichiers dans le répertoire correspondant au type de fichier.

   Le tableau ci-dessous répertorie la structure de répertoire pour les fichiers importés.

Tableau 1. Structure de répertoire des fichiers de cas.

Répertoire	Description
`/opt/ibm/forensics/case_input/<case_name>`	Répertoire utilisé pour importer une série ou un flux connecté de fichiers pcap.
`/opt/ibm/forensics/case_input/<case_name>/singles`	Répertoire utilisé pour importer des fichiers pcap individuels.
`/opt/ibm/forensics/case_input/case_input/<case_name>/import`	Répertoire utilisé pour importer un seul fichier ou un type de fichier autre que pcap, par exemple, des documents Microsoft Word, des PDF Adobe Acrobat, des fichiers texte et des images.

Important : Si un trait d'union est utilisé dans un nom de fichier, il est remplacé par un tiret bas lors de l'importation du fichier

Résultats

Après une importation réussie, le nom de votre fichier apparaît automatiquement dans la fenêtre Collectes du cas que vous avez créé.

Autorisation des utilisateurs à envoyer par FTP des fichiers pcap et des documents provenant de systèmes externes pour des cas forensics

Pour l'envoi par téléchargement de données à inclure dans des cas spécifiques, les administrateurs peuvent accorder des droits FTP sécurisés aux utilisateurs et gérer le cas auquel les données sont associées. Les utilisateurs peuvent choisir les processus hôtes IBM Security QRadar Incident Forensics qui sont requis par FTP.

Pour modifier un mot de passe une fois l'accès FTP activé, vous devez désactiver l'accès FTP et sauvegarder l'utilisateur, puis réactiver l'accès, et entrer le nouveau mot de passe.

Avant de commencer

Assurez-vous que vous créez ou affectez des rôles pour les enquêteurs médico-légaux dans l'outil Rôles d'utilisateur sur l'onglet **Admin**.

Par défaut, le fichier `/etc/vsftpd/vsftpd.conf` est configuré de sorte que cinq ports sont ouverts : 55100-55104. Vous pouvez modifier la plage de ports en éditant le fichier `/etc/vsftpd/vsftpd.conf` et en remplaçant les valeurs des paramètres `pasv_min_port` et `pasv_max_port` par la plage de ports que vous souhaitez. Vous devez déployer vos modifications de configuration en cliquant sur **Déployer les changements** dans l'onglet **Admin**.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar Incident Forensics peut importer des données depuis n'importe quel répertoire accessible situé sur le réseau. Les données peuvent avoir plusieurs formats, notamment les suivants :

- Fichiers au format PCAP standard depuis des sources externes
- Documents tels que des fichiers texte, des fichiers PDF, des feuilles de calcul et des présentations
- Fichiers image
- Données de diffusion en flux depuis des applications
- Données de diffusion en flux depuis des sources PCAP externes

Les utilisateurs peuvent envoyer par téléchargement plusieurs fichiers vers un cas et un administrateur peut autoriser plusieurs utilisateurs à accéder à ce cas.

Restriction : Le nom de cas doit être unique. Un seul utilisateur est associé à un cas ; par conséquent, deux utilisateurs ne peuvent pas créer de cas ayant le même nom.

Procédure

1. Sous **Admin**, cliquez sur **Droits utilisateur Forensics**.
2. Dans la liste **Utilisateurs**, sélectionnez un utilisateur.
3. Dans le volet **Editer l'utilisateur**, sélectionnez la case à cocher **Enable FTP access**.
4. Entez et confirmez le mot de passe FTP de l'utilisateur.
5. Pour sauvegarder les modifications apportées aux droits, cliquez sur **Sauvegarder l'utilisateur**.
6. Dans le client FTP, procédez comme suit :
   a. Assurez-vous que le protocole TLS (Transport Layer Security) est sélectionné.
   b. Ajoutez l'adresse IP de l'hôte QRadar Incident Forensics.
   c. Créez une connexion qui utilise le nom d'utilisateur et le mot de passe QRadar Incident Forensics qui ont été créés.
7. Connectez-vous au serveur QRadar Incident Forensics et créez un nouveau répertoire.
8. Pour envoyer par FTP et stocker des fichiers pcap, sous le répertoire que vous avez créé pour le cas, créez un répertoire nommé `singles` et faites glisser les fichiers pcap vers ce répertoire.
9. Pour envoyer par FTP et stocker d'autres fichiers autres que des fichiers pcap, sous le répertoire que vous avez créé pour le cas, créez un répertoire nommé `import` et faites glisser les fichiers dans ce répertoire.
10. Pour redémarrer le serveur FTP, entrez la commande suivante :

    ```
    etc/init.d/vsftpd restart
    ```

11. Pour redémarrer le serveur qui déplace les fichiers de la zone de téléchargement vers le répertoire QRadar Incident Forensics, entrez la commande suivante :

    ```
    /etc/init.d/ftpmonitor restart
    ```

Résultats

Un administrateur voit les données qui sont envoyées par téléchargement dans la gestion des cas. Un utilisateur peut voir ses cas dans l'un des outils de l'onglet **Forensics**.

Déchiffrage du trafic SSL et TLS dans QRadar Incident Forensics

Pour localiser des menaces masquées, IBM Security QRadar Incident Forensics peut déchiffrer le trafic SSL. Si vous fournissez la clé privée et l'adresse IP du serveur ou la clé de session d'un navigateur et d'autres informations de session, l'inspecteur de protocole peut déchiffrer le trafic SSL.

Si la clé de session est générée depuis des sites externes ou générée par un autre navigateur, l'inspecteur de protocole ne peut pas déchiffrer le trafic SSL depuis une session de navigateur.

Restriction : Le mécanisme d'échange de clé `Diffie Hellman` n'est pas pris en charge lorsque du trafic chiffré est déchiffré via une clé privée. Lorsque vous utilisez une clé privée, d'autres méthodes d'échange de clé, par exemple RSA, sont prises en charge.

La restriction `Diffie Hellman` ne s'applique pas lorsque le trafic est déchiffré à l'aide d'informations détectées dans un journal de clés.

Pourquoi et quand exécuter cette tâche

Le déchiffrement est pris en charge pour les protocoles suivants :

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Les fichiers journaux de clé sont générés par les navigateurs Chrome, Firefox et Opera avec la variable d'environnement SSLKEYLOGFILE. Les formats de clé suivants sont pris en charge pour la clé de session SSLKEYLOGFILE :

- RSA
- DH

Procédure

1. A l'aide de SSH, connectez-vous à l'hôte principal QRadar Incident Forensics en tant que superutilisateur.
2. Cherchez l'emplacement des clés dans le fichier `/opt/qradar/forensics.conf`.

    ```
    <sslkeys
    keydir="/opt/ibm/forensics/decapper/keys"
    keylogs="/opt/ibm/forensics/decapper/keylogs"/>
    ```

3. Copiez les clés dans le répertoire qui est spécifié dans le fichier `/opt/qradar/forensics.conf`.

- Pour les clés privés, copiez la clé dans le répertoire `/opt/ibm/forensics/decapper/keys`.

  Exemple :

  ```
  <keys>
   <key file=" /opt/ibm/forensics/decapper/keys/key_name">
      <address> 1.2.3.4</address>
      <range> 1.2.3.0-1.2.3.255</range>
    </key></keys>
  ```

- Pour les fichiers journaux générés par le navigateur, copiez les fichiers dans le répertoire `/opt/ibm/forensics/decapper/keylogs/default`.

Si vous modifiez les sous-répertoires dans les répertoires `/opt/ibm/forensics/decapper/keys` ou `/opt/ibm/forensics/decapper/keylogs`, vous devez redémarrer le service decap.

Pour redémarrer ce service, entrez la commande suivante : `service decapper restart`

Chapitre 6. Actions planifiées dans QRadar Incident Forensics

Vous pouvez planifier la maintenance, par exemple la suppression d'anciens documents, le paramétrage de la base de données et la reconfiguration du serveur IBM Security QRadar Incident Forensics.

S'il y a un grand nombre de documents, les actions planifiées, comme la suppression des documents anciens, peut prendre un certain temps. Si vous souhaitez supprimer l'intégralité d'un cas, utilisez l'outil de gestion de cas.

Suppression de documents.

Les administrateurs peuvent supprimer les documents obsolètes en fonction de l'horodatage réseau des documents.

Vous pouvez supprimer des documents, ce qui inclut les fichiers pcap et d'autres types de fichier, à partir d'un cas ou du serveur. La suppression d'anciens documents permet de conserver la vitesse de la recherche de documents.

Flush case

Pour affiner la gestion des cas, vous pouvez utiliser l'option **Flush Case**. Pour les données *pcap de diffusion*, qui constituent une série de fichiers pcap liés de manière logique pour former un fichier pcap volumineux, vous pouvez forcer les données en mémoire tampon à écrire sur le disque. L'option **Flush Case** force les hôtes QRadar Incident Forensics à écrire des flux non terminés sur disque, ce qui ensuite simplifie la recherche dans ces flux ultérieurement.

Optimisation de la base de données

Les administrateurs peuvent optimiser la base de données afin de réorganiser l'index du moteur de recherche en segments et de supprimer les documents effacés.

L'action planifiée d'**optimisation de base de données** est similaire à une commande **`defrag`**.

Lorsque vous optimisez la base de données, un index est créé. Une fois l'index généré, le nouvel index remplace l'ancien. Etant donné que deux index existent jusqu'au remplacement de l'ancien index, la commande d'optimisation d'index nécessite le double d'espace disque.

Avant d'optimiser votre base de données, vous devez vous assurer que la taille de l'index ne dépasse pas 50% de l'espace disponible sur votre disque dur.

Planification d'actions pour les hôtes QRadar Incident Forensics

Vous pouvez planifier des tâches de maintenance sur les hôtes IBM Security QRadar Incident Forensics.

Vous pouvez planifier les tâches suivantes :

- Créer un nouvel index pour les cas actuellement disponibles.

- Retirer (*rendre obsolète*) les documents que vous ne voulez plus conserver au terme d'un délai spécifié.
- Forcer l'écriture de données sur le disque.

Procédure

1. Sous l'onglet **Admin**, dans la section **Forensics**, cliquez sur **Planification d'actions**.
2. Cliquez sur **Ajouter une action**.
3. Depuis la liste **Sélectionner une action**, choisissez une action et indiquez les paramètres.
   - Pour créer un nouvel index pour les cas en cours, sélectionnez **Optimiser index**.

     Le nouvel index a besoin d'environ deux fois l'espace d'un index existant. Vérifiez que vous disposez d'un espace suffisant.
   - Pour supprimer des documents dont l'horodatage réseau est antérieur à un âge spécifique, sélectionnez **Rendre obsolètes les documents**.

     Les index sont également supprimés lors de la suppression de documents.
   - Pour écrire des flux indéterminés sur disque, sélectionnez **Vider le cas**.
4. Cliquez sur **Sauvegarder**.
5. Pour exécuter, éditer ou supprimer l'action, sélectionnez celle-ci dans la liste **Actions** et cliquez sur **run**, **edit** ou **delete**.

Chapitre 7. Audit de l'utilisateur et de l'utilisation du système dans QRadar Incident Forensics

Les journaux d'audit sont des enregistrements chronologiques qui identifient les comptes utilisateur associés à l'accès aux données. Ces journaux peuvent détecter tout accès inhabituel ou non autorisé et identifier des problèmes, par exemple des travaux qui ont échoué.

Les activités suivantes génèrent des événements dans les journaux d'audit :

- Créer un cas
- Supprimer un cas
- Supprimer une collecte
- Requêtes de tous les utilisateurs
- Vue Document
- Exporter un document

Restriction : La journalisation des événements de création de collecte n'est pas prise en charge.

Procédure

1. Utilisez SSH pour vous connecter à QRadar Console ou à QRadar Incident Forensics Standalone en tant qu'administrateur.
2. Accédez au répertoire `/var/log/audit`.
3. Ouvrez le fichier `audit.log` dans un éditeur, par exemple vi, afin de passer en revue le contenu, ou utilisez la commande **`grep`** pour rechercher une entrée spécifique.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Licence de Propriété Intellectuelle
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées de International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services sont des marques d'IBM ou peuvent appartenir à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à www.ibm.com/legal/copytrade.shtml.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Remarques sur les règles de confidentialité

Les produits IBM Software, notamment les logiciels sous forme de services (“Offres logicielles”), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations d'utilisation en vue d'améliorer l'expérience de l'utilisateur final, d'ajuster les interactions avec l'utilisateur final ou à d'autres fins. Dans de nombreux cas, aucune information identifiant la personne n'est collectée par les offres logicielles. Certaines de nos Offres logicielles vous permettent de collecter des informations identifiant la personne. Si cette Offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées ci-dessous.

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur

l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies, notamment de cookies, à ces fins, reportez-vous aux Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et à la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr, ainsi qu'à la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).