IBM Security QRadar Incident Forensics
Version 7.3.0

Guide d'administration

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 33.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.0 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.

Utilisateurs concernés

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 à IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à d'autres documents techniques dans la bibliothèque produit QRadar, voir la note technique Accessing IBM Security Documentation (en anglais) (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir la note technique Support and Download (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Instructions relatives aux bonnes pratiques de sécurité

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 de sécurité et leurs données. Plus spécifiquement, IBM Security QRadar Incident Forensics est conçu pour aider les sociétés à enquêter et à mieux comprendre ce qui s'est passé lors des 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 que dans un but réglementaire et de façon légale. 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 reconnaît qu'il obtient ou a obtenu les consentements, les autorisations ou les licences nécessaires à l'activation de son utilisation légale d'IBM Security QRadar Incident Forensics.

Chapitre 1. Nouveautés pour les administrateurs dans QRadar Incident Forensics version 7.3.0

IBM QRadar Network Insights version 7.3.0 introduit une option supplémentaire pour le format QFlow.

Option TLV disponible pour QRadar Network Insights

Utilisez les collecteurs QFlow pour exporter des données vers le processeur QFlow au format TLV (tab-length-value). Dans le cas de nouvelles installations IBM Security QRadar ou de mises à niveau QRadar dont le déploiement ne contient pas de dispositif QRadar Network Insights, choisissez le format `TLV` dans le menu **Format QFlow**.

 En savoir plus sur le format TLV...

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 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 (version 1)
  - Lanman 2.1
  - NT 0.12
- 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 **Add New Case**.
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 **Add New Case**.

     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 **Add files**, sélectionnez les fichier et cliquez sur **Start upload**.
   - 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**.

Remarque : Les clients FTP doivent prendre en charge TLS version 1.2 (fichier `vsftpd.conf`). La liste suivante décrit les versions de client FTP minimales prises en charge :

- WinSCP 5.7
- FileZilla 3.9.0.6

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 **Schedule Actions**.
2. Cliquez sur **Add New Action**.
3. Depuis la liste **Select Action**, choisissez une action et indiquez les paramètres.
   - Pour créer un nouvel index pour les cas en cours, sélectionnez **Optimize 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 **Age Out Documents**.

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

Chapitre 7. Gestion du contenu suspect

En tant qu'administrateur, vous pouvez marquer un contenu suspect en utilisant la fonction Gestion du contenu suspect.

Règles Yara

Pour marquer un contenu suspect dans des fichiers figurant dans le trafic réseau de QRadar Incident Forensics, vous pouvez importer et utiliser des règles Yara existantes afin de spécifier les règles personnalisées exécutées sur les fichiers.

Chaque règle Yara commence par la règle de mot clé, suivie d'un identificateur de règle. Les règles Yara comportent deux sections :

1. Définition des chaînes : dans la section de définition des chaînes, spécifiez les chaînes qui font partie de la règle. Chaque chaîne utilise un identificateur qui comprend un signe dollar ($) suivi d'une séquence de caractères alphanumériques séparés par des traits de soulignement.
2. Condition : dans la section de la condition, définissez la logique de la règle. Cette section doit comporter une expression booléenne, qui définit les conditions dans lesquelles un fichier correspond à la règle.

L'exemple ci-dessous présente une règle Yara simple :

```
rule simple_forensics : qradar
{
    meta:
        description = "Cette règle cherche une chaîne str1 avec un décalage de 25 octets
                       dans le fichier."
    strings:
        $str1 = "pattern of interest"

    condition:
        $a at 25
}
```

L'exemple ci-dessous présente une règle Yara plus complexe :

```
rule ibm_forensics : qradar
{
    meta:
        description = "Cette règle marque un contenu comportant une séquence de
                       caractères hexadécimaux et la chaîne str1 3 fois au moins."

    strings:
        $hex1 = {4D 2B 68 00 ?? 14 99 F9 B? 00 30 C1 8D}
        $str1 = "IBM Security!"


    condition:
        $hex1 and (#str1 > 3)
}
```

Lorsque la règle Yara est transférée, le fichier journal du serveur utilise des règles spécifiées lorsqu'un fichier est détecté lors d'une récupération ou d'un transfert PCAP. Si un contenu correspondant est détecté, la zone **Contenu suspect** est ajoutée sous l'onglet **Attributs** d'un document. La zone **Contenu suspect** contient le nom de la règle Yara et les balises identifiées par la règle.

Restriction : La mise en oeuvre des modules Yara n'est pas disponible actuellement.

Importation des règles Yara

Vous pouvez importer vos règles Yara existantes dans IBM Security QRadar Incident Forensics et les utiliser pour rechercher et marquer un contenu malveillant. Un fichier importé peut comporter plusieurs règles Yara.

Procédure

1. Sous l'onglet **Admin**, sélectionnez **Gestion du contenu suspect**.
2. Cliquez sur **Sélectionner un fichier**.
3. Dans la fenêtre Téléchargement de fichier, cherchez le fichier à importer et cliquez sur **Ouvrir**.

   Important : Les noms de règles Yara doivent être uniques.

Résultats

Lorsque la règle Yara a été importée correctement, un message s'affiche.

Que faire ensuite

Les règles Yara qui viennent d'être importées ne sont pas appliquées rétroactivement. Après l'importation des règles Yara, vous devez effectuer un déploiement complet pour appliquer les modifications.

Suppression des règle Yara

Vous pouvez supprimer toute les règles Yara existantes dans IBM Security QRadar Incident Forensics. Pour désactiver les règles Yara, transférez un fichier contenant une règle vide.

Avant de commencer

Procédure

1. Pour créer un fichier contenant une règle vide, suivez cette procédure :
   a. Copiez la règle ci-dessous dans un éditeur de texte de votre choix :

   ```
   rule empty
   {
    condition:
              false
   }
   ```

   b. Sauvegardez comme fichier texte.
2. Sous l'onglet **Admin**, sélectionnez **Gestion du contenu suspect**.
3. Cliquez sur **Sélectionner un fichier**.
4. Dans la fenêtre Téléchargement de fichier, cherchez le fichier que vous avez créé lors de l'étape 1 et cliquez sur **Ouvrir**.
5. Cliquez sur **Sauvegarder**.

Résultats

La règle unique renvoie toujours un résultat **`false`**, qui permet de transmettre le validateur. Elle supprime toutes les règles existantes et est insérée dans la base de

données. Elle ne marque jamais de contenu comme suspect.

Chapitre 8. 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
- Affecter 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.

Chapitre 9. Examen des menaces avec QRadar Network Insights

Utilisez IBM QRadar Network Insights pour analyser vos données réseau en temps réel et observer le comportement des menaces sur votre réseau.

QRadar Network Insights est une solution d'analyse des menaces réseau qui détecte rapidement et facilement les menaces d'initiés, l'exfiltration des données et l'activité de logiciel malveillant. Les indicateurs de menace principaux sont regroupés et font l'objet d'un suivi avec une visibilité complète du trafic réseau.

Examens en temps réel des menaces avec QRadar Network Insights

IBM QRadar Network Insights permet d'analyser en temps réel les données réseau et fournit un niveau avancé de détection des menaces et d'analyse.

Les menaces de cybersécurité avancées sont de plus en plus difficiles à détecter et à prévenir. L'activité malveillante se fait souvent passer pour une utilisation normale, ce qui permet aux menaces de se déplacer et de communiquer via les réseaux pour mener à bien leurs objectifs. Ainsi, les mutations de logiciel malveillant qui évitent la détection basée sur les signatures et les techniques d'ingénierie sociale, comme le hameçonnage, permettent d'ouvrir la porte à ces attaques.

Capacité de recherche

La capacité de recherche de QRadar Network Insights recherche et extrait des indicateurs importants des données de paquet, par exemple, les informations de flux, les métadonnées, le contenu extrait et le contenu suspect. Vous pouvez utiliser le contenu extrait pour une analyse rétrospective sur le long terme.

Intégration à IBM Security QRadar Incident Forensics

QRadar Network Insights enregistre les activités des applications, capture les artefacts et identifie les actifs, les applications et les utilisateurs qui participent aux communications réseau. QRadar Network Insights est étroitement lié à IBM Security QRadar Incident Forensics pour les examens post incident et les activités de traque des menaces. QRadar Incident Forensics et IBM QRadar Network Packet Capture capturent, reconstruisent et rejouent la totalité des conversations, mais QRadar Network Insights permet de détecter les incidents et vous informe lorsque des éléments suspects apparaissent lors d'une conversation.

Le contenu suspect peut provenir de sources variées, comme un logiciel malveillant, des ports non standard, des expressions régulières ou des règles Yara.

Valeur des flux

Les flux fournissent de la visibilité à QRadar sur l'activité réseau, car ils permettent de détecter les actifs lorsque des unités se connectent à un réseau. QRadar Network Insights vous permet de corréler les données de flux avec les données d'événement et donc de détecter les menaces qui ne peuvent pas être identifiées par les journaux seuls. IBM Security QRadar QFlow Collector fournit les flux

réseau et reconnaît également les applications Layer 7. Vous pouvez aussi capturer le début des sessions. QRadar Network Insights révèle les menaces précédemment masquées et les comportements malveillants.

Concepts associés:

«Niveaux d'inspection de flux de QRadar Network Insights», à la page 28
Pour améliorer les performances, vous devez choisir le débit de flux approprié requis en configurant le paramètre **Niveau d'inspection de flux**.

Déploiements QRadar Network Insights

IBM QRadar Network Insights est un hôte géré que vous associez à la console QRadar.

Dans le cas d'un déploiement QRadar Network Insights, vous devez sélectionner l'option de dispositif `6200` lors de l'installation. Pour plus d'informations sur l'installation du dispositif QRadar Network Insights, voir *IBM Security QRadar Incident Forensics - Guide d'installation*.

Dans le cas d'un déploiement QRadar Network Insights, vous devez allouer une licence à l'option de dispositif `6200`. QRadar Network Insights requiert une licence distincte pour le dispositif `6200`, mais la licence QRadar Network Insights n'est pas nécessaire sur la console QRadar.

Relation entre le dispositif QRadar Network Insights et IBM Security QRadar Incident Forensics

Vous pouvez déployer QRadar Network Insights séparément du déploiement IBM Security QRadar Incident Forensics Processor. QRadar Network Insights ne requiert d'une connexion à la console QRadar et ne nécessite pas de connexion au dispositif QRadar Incident Forensics.

Application QRadar Network Insights

Le dispositif QRadar Network Insights 1920 est fourni avec deux cartes réseau de troisième génération. Les cartes réseau sont connectées directement au réseau pour faciliter l'inspection des paquets en temps réel.

La capacité d'acheminement de flux configurable permet d'équilibrer la charge entre plusieurs dispositifs. La configuration matérielle facilite le traitement en mémoire et permet d'effectuer une analyse en temps réel des données réseau.

Tableau 2. Spécifications des cartes réseau

Dispositif 1920	Description
`Serveur`	X3650 M5
`UC`	2 x E5-2680 v4 14C 2,4 GHz 35 Mo 2400 MHz 120 W
`Mémoire RAM`	8 x 16 Go
`Unité de disque dur`	2 unités SSD de 200 Go
`ServeRAID`	M1215
`Cartes d'E-S`	Intel X520 2P 10 GbE + 2 x 10G SR 2 x NT40E3 4P 40G + 2 x 10G SR + 2 x 10G LR
`P/S`	2 x 900 W

Configuration requise pour QRadar Network Insights

Après avoir installé IBM QRadar Network Insights et l'avoir associé à la console QRadar Console en tant qu'hôte géré, vous devez configurer votre dispositif avant de commencer à l'utiliser pour examiner les menaces sur votre réseau. Le dispositif QRadar Network Insights lit les paquets bruts d'un tap réseau ou d'un port SPAN, puis génère des paquets IPFIX. Les paquets IPFIX sont envoyés au processus QFlow sur la console QRadar Console.

Configuration du format de QFlow Collector

En tant que gestionnaire d'un cluster d'hôtes gérés, vous pouvez choisir le format que vos collecteurs QFlow Collector utiliseront pour exporter des données vers QFlow Processor : TLV ou Contenu.

Avant de commencer

Assurez-vous que les conditions requises ci-dessous sont remplies :

__ • Installez une console QRadar Console avec QRadar Network Insights associé en tant qu'hôte géré.

__ • Effectuez un déploiement complet après avoir associé IBM QRadar Network Insights en tant qu'hôte géré.

Procédure

1. Connectez-vous à QRadar : `https://`*`adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe est celui du compte de l'utilisateur root.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau de navigation, cliquez sur **Paramètres système**.
4. Cliquez sur le menu **Paramètres QFlow** et choisissez le format QFlow.

Tableau 3. Options du format QFlow

Format QFlow	Description
`TLV`	Paramètre de format QFlow par défaut. Choisissez **TLV** (tab-length-value) pour les nouvelles installations ou pour les mises à niveau qui ne contiennent pas de dispositif QRadar Network Insights dans leur déploiement.
`Contenu`	Choisissez **Contenu** pour les mises à niveau qui contiennent un dispositif QRadar Network Insights dans leur déploiement. Cela signifie que le déploiement peut continuer à fonctionner tel qu'il est.

5. Cliquez sur **Sauvegarder**.
6. Dans la barre de menus de l'onglet **Admin**, cliquez sur **Déployer la configuration entière** et confirmez les modifications.
7. Actualisez le navigateur Web pour afficher l'onglet **Forensics**.

Configuration de DTLS sur un hôte géré QRadar Network Insights

Pour empêcher l'écoute clandestine et la contrefaçon, vous devez configurer DTLS (Datagram Transport Layer Security) sur un hôte géré QRadar Network Insights. Vous devez d'abord configurer une source de flux.

Procédure

1. Ajoutez QRadar Network Insights en tant qu'hôte géré.
   a. Cliquez sur l'onglet **Admin**.
   b. Dans le panneau de navigation, cliquez sur **Gestion du système et de la licence** sous la section **Configuration système**.
   c. Sélectionnez l'hôte géré QRadar Network Insights. Le type de dispositif est `6200`.
   d. Cliquez sur l'icône **Actions de déploiement** et sélectionnez **Ajouter l'hôte**.
   e. Lorsque vous y êtes invité, indiquez l'adresse IP et le mot de passe root de l'hôte géré QRadar Network Insights, puis cliquez sur **Ajouter**.
2. Pour configurer une source de flux, procédez comme suit :
   a. Ouvrez une session dans QRadar en tant qu'administrateur.
   b. Cliquez sur l'onglet **Admin**.
   c. Dans le panneau de navigation, cliquez sur **Sources de flux** sous la section **Flux**.
   d. Cliquez sur l'icône **Ajouter**.
   e. Indiquez un **Nom de la source de flux** descriptif.
   f. Sélectionnez un **Collecteur de flux cible** ou acceptez la valeur fournie.
   g. Sélectionnez **Netflow v.1/v.5/v.7/v.9/IPFIX** comme **Type de la source de flux**.
   h. Entrez une valeur pour **Port de surveillance** ou acceptez la valeur fournie.
   i. Sélectionnez `DTLS` dans la liste **Protocole de liaison**.
   j. Cliquez sur **Sauvegarder**.
   k. Dans la barre de menus de l'onglet **Admin**, cliquez sur **Déployer la configuration entière** et confirmez les modifications.
   l. Actualisez le navigateur Web.
3. Pour configurer la communication DTLS, procédez comme suit :

   Remarque : Si vous modifiez la source de flux ou le collecteur de flux QRadar de n'importe quel hôte géré QRadar Network Insights du déploiement, vous devez à nouveau exécuter le script de configuration de DTLS.
   a. Cliquez sur l'icône **Actions de déploiement** et sélectionnez **Modifier une connexion d'hôte**.
   b. Dans la page Modifier une connexion QRadar Network Insights, sélectionnez la source de flux et le collecteur de flux QRadar.
   c. Cliquez sur **Sauvegarder**.
   d. Fermez la page Gestion du système et de la licence.
   e. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.
   f. Utilisez **SSH** pour vous connecter en tant qu'utilisateur root à la console QRadar Console.
   g. Exécutez la commande suivante pour configurer le certificat DTLS :
   ```
   python /opt/qradar/bin/qflow_dtls_cert_setup.py
   ```
   h. Ouvrez une session dans QRadar en tant qu'administrateur.
   i. Dans l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.

Niveaux d'inspection de flux de QRadar Network Insights

Pour améliorer les performances, vous devez choisir le débit de flux approprié requis en configurant le paramètre **Niveau d'inspection de flux**.

Le débit de flux est lié aux niveaux de visibilité via le contenu disponible, comme la source, la destination, le protocole et les types de fichier spécifiques.

Les niveaux d'inspection de flux sont cumulés, de telle sorte que chaque niveau prend les propriétés du niveau précédent.

Flux

Il s'agit du niveau d'inspection le plus faible. Les flux sont détectés par un 5-uplet et les octets et paquets allant dans chaque direction sont comptés. Ce type d'information est similaire à ce que vous obtenez à partir d'un routeur ou d'un commutateur réseau qui n'effectue pas d'inspection en profondeur des paquets. Ce niveau prend en charge la bande passante la plus élevée, mais génère la quantité la moins élevée d'informations liées aux flux.

Les attributs générés par QRadar Network Insights le niveau d'inspection de flux sont : valeurs 5-uplet, ID flux, nombres de paquets et d'octets, et heures de début et de fin des flux.

Flux enrichis

Chaque flux est identifié et inspecté par l'un des protocoles ou inspecteurs de domaine ; cette inspection peut générer de nombreuses sortes d'attributs.

La liste suivante décrit les attributs générés par QRadar Network Insights via le niveau d'inspection des flux enrichis :

- Valeurs des métadonnées HTTP, y compris la catégorisation des URL
- ID application ID et action
- Informations relatives au fichier (nom, taille, hachage)
- Noms d'utilisateur d'origine et du destinataire
- Valeurs de contenu suspect limité

Flux de contenu enrichis

Il s'agit du paramètre par défaut et du niveau d'inspection le plus élevé. Effectue les mêmes opérations que le niveau Flux enrichis, mais analyse et inspecte en plus le contenu des fichiers qu'il trouve. Cela permet de déterminer le type de contenu de manière plus précise et de générer davantage de valeurs de contenu suspectes lors de l'inspection du contenu des fichiers.

La liste suivante décrit les attributs générés par QRadar Network Insights via le niveau d'inspection des flux de contenu enrichis :

- Informations personnelles
- Données confidentielles
- Scripts imbriqués
- Redirections
- Contenu suspect basé sur le contenu configurable

Tableau 4. Remarques relatives aux performances

Paramètre de niveau d'inspection de flux	**Performances**
`Flux`	10 Gbps

Tableau 4. Remarques relatives aux performances (suite)

Paramètre de niveau d'inspection de flux	Performances
`Flux enrichis`	Environ 10 Gbps. Les performances varient en fonction du niveau d'inspection, de la recherche, des critères d'extraction et des données réseau.
`Flux de contenu enrichis (avancé)`	Environ 3,5 Gbps. Des performances de 10 Gbps peuvent être atteintes avec plusieurs dispositifs.

Concepts associés:

«Examens en temps réel des menaces avec QRadar Network Insights», à la page 25
IBM QRadar Network Insights permet d'analyser en temps réel les données réseau et fournit un niveau avancé de détection des menaces et d'analyse.

Configuration des paramètres QRadar Network Insights

Dans un souci d'amélioration des performances, configurez les niveaux de flux produits par les dispositifs QRadar Network Insights dans votre déploiement. Chaque niveau d'inspection fournit une visibilité plus approfondie et extrait plus de contenu.

Procédure

1. Ouvrez une session dans QRadar en tant qu'administrateur.
2. Cliquez sur l'onglet **Admin**.
3. Dans le panneau de navigation, cliquez sur **Paramètres système**.
4. Cliquez sur le menu **Paramètres Network Insights**.
5. Dans **Niveau d'inspection de flux**, sélectionnez le débit de flux requis. Reportez-vous au tableau suivant pour comprendre les niveaux d'inspection de flux :

Tableau 5. Niveaux d'inspection de flux

Niveau d'inspection de flux	Description
`Flux`	Niveau d'inspection le plus faible. Les flux sont détectés par un 5-uplet et les octets et paquets allant dans chaque direction sont comptés.
`Flux enrichis`	Chaque flux est identifié et inspecté par l'un des protocoles ou inspecteurs de domaine ; cette inspection peut générer de nombreuses sortes d'attributs.
`Flux de contenu enrichis`	Paramètre par défaut. Niveau d'inspection le plus élevé. Effectue les mêmes opérations que les Flux enrichis, mais analyse et inspecte en plus le contenu des fichiers qu'il trouve.

6. Cliquez sur **Sauvegarder**.
7. Dans la barre de menus de l'onglet **Admin**, cliquez sur **Déployer la configuration entière**.
8. Actualisez le navigateur Web.

Que faire ensuite

Déployez l'hôte géré QRadar Incident Forensics Processor.

Détection des menaces avec QRadar Network Insights

Si vous souhaitez avoir une visibilité en temps réel des menaces sur votre réseau, utilisez QRadar Network Insights pour détecter les indicateurs de cyberattaques et l'activité malveillante associée.

Téléchargement du contenu de QRadar Network Insights

Téléchargez le contenu (extension) de QRadar Network Insights depuis IBM Security App Exchange (http://exchange.xforce.ibmcloud.com/hub/extension/522bf1095f047b0b37225d8efc5d4877). Utilisez l'outil **Gestion des extensions** pour l'installer.

Pour plus d'informations sur l'utilisation de l'outil **Gestion des extensions**, voir *IBM Security QRadar Administration Guide*.

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
U.S.A.

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 :

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

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 tacites, 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.

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

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 et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

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.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées 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. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

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

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.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des 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 de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et 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 que 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).