IBM Security QRadar Incident Forensics
Version 7.3.0

Guide d'utilisation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 45.

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.

Présentation de l'utilisation d'IBM Security QRadar Incident Forensics

Le présent guide contient des informations sur les procédures d'investigation à effectuer à l'aide d'IBM® Security QRadar Incident Forensics en cas d'incident lié à la sécurité.

Utilisateurs concernés

Les examinateurs extraient des informations du trafic réseau et des documents dans le référentiel Forensics. Ces informations sont utilisées lors des investigations menées en cas d'incidents liés à la sécurité.

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 des données de paquet réseau capturé (PCAP) et inclut une fonction permettant de reconstruire ces données à leur forme initiale. Cette fonction de reconstruction peut reconstruire les données et les fichiers, dont les messages électroniques, les fichiers et les images joints, les appels téléphoniques voix sur IP (VoIP) et les sites Web. Les manuels et les autres documents qui accompagnent le programme contiennent des informations supplémentaires concernant les caractéristiques et les fonctions du programme et leur configuration. L'utilisation de ce programme peut impliquer différentes lois et réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, 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, aux réglementations et aux règles en vigueur et fait en sorte de 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 utilisateurs dans QRadar Incident Forensics version 7.3.0

IBM Security QRadar Incident Forensics version 7.3.0 permet désormais aux utilisateurs effectuant une reprise de sélectionner des unités Packet Capture (PCAP).

Sélection des unités PCAP disponible pour la reprise de QRadar Incident Forensics

Pour limiter l'affichage du trafic entrant aux unités PCAP de votre déploiement lors d'une reprise de QRadar Incident Forensics, sélectionnez une **unité Capture personnalisée**.

 En savoir plus sur la sélection des unités PCAP...

Chapitre 2. Investigations liées à la sécurité

IBM Security QRadar Incident Forensics vous permet de détecter les signes de menaces éventuelles, de détecter la cause première de ces menaces et d'empêcher qu'elles ne se reproduisent. Grâce aux outils Forensics, vous pouvez rapidement concentrer votre analyse sur l'auteur de la menace, le mode opératoire utilisé et les données qui ont été compromises.

En tant qu'examinateur Forensics, vous pouvez retracer les actions étape par étape des cybercriminels et reconstruire les données de réseau brutes liées à un incident de sécurité.

Lorsque votre organisation est informée de l'existence d'une menace, d'un risque de sécurité potentiel ou d'une violation des règles de conformité, vous devez définir des objectifs afin d'évaluer la portée de ces incidents, identifier les entités impliquées et comprendre les motivations.

Vous pouvez utiliser les outils d'IBM Security QRadar Incident Forensics dans des scénarios spécifiques pour les différents types d'investigations, tels que la sécurité des réseaux, l'analyse d'initiés, la fraude et le détournement et la collecte de preuves.

1. Récupérez et reconstruisez les sessions réseau vers et à partir d'une adresse IP.
2. A partir des incidents qui sont créés, vous pouvez interroger des catégories d'attributs pour recueillir des preuves.

   Lorsque vous créez une reprise, un incident est créé.
3. Utilisez des filtres de recherche pour extraire uniquement les informations qui vous intéressent.
4. En fonction du type d'analyse, choisissez l'outil forensics qui fournit la preuve dont vous avez besoin.

Contenu suspect

Vous pouvez utiliser la fonction de recherche pour rechercher un élément contextuel ou un identificateur que vous connaissez au sujet de l'attaquant ou de l'incident. Si vous utilisez le mot clé dans la recherche, un contenu suspect est renvoyé. Une partie du contenu suspect peut être pertinente pour l'investigation.

Outil de permutation de données

La permutation des données est obtenue en faisant apparaître le contenu renvoyé à l'issue d'une recherche sous forme de lien dynamique. Par exemple, si vous effectuez une recherche sur `"Tom"`, les résultats peuvent inclure les courriers électroniques rédigés par Tom, ses discussions en ligne, ainsi que d'autres informations contextuelles. Lorsque vous cliquez sur un courrier électronique pour l'afficher, chaque actif ou entité, par exemple des pièces jointes ou des ID d'ordinateur que Tom a utilisés, apparaissent sous forme de liens. Un examinateur peut utiliser ces liens pour accélérer ses investigations.

Outil d'impression numérique

Utilisez l'outil d'impression numérique pour consulter les données et mapper les relations entre des entités, telles que des adresses IP, des noms et des adresses

MAC, en fonction de la fréquence. Vous pouvez sélectionner un ou plusieurs résultats pour afficher la fréquence et le sens de la relation.

Outil Surveyor

Utilisez l'outil Surveyor pour afficher un calendrier linéaire des activités de manière à pouvoir retracer une attaque. Surveyor reconstruit la session et trie les documents par ordre chronologique.

Filtrage de contenu

Utilisez le filtrage de contenu pour examiner un sous-ensemble de catégories de contenu, tel que WebMail ou Pornography, afin d'éliminer ce qui n'est pas pertinent lorsque vous effectuez une recherche.

Investigations liées à la sécurité du réseau

Vous pouvez utiliser QRadar Incident Forensics pour détecter les activités malveillantes qui ciblent des actifs critiques et mener les investigations associées. Vous pouvez utiliser les outils Forensics intégrés pour vous aider à remédier à une violation de la sécurité du réseau et l'empêcher de se reproduire.

Utilisez les outils d'investigation de QRadar Incident Forensics pour vous aider à déterminer de quelle façon l'événement s'est produit, à minimiser son impact et à mettre tout en oeuvre pour empêcher toute nouvelle violation.

Patient zéro : Identification de la source d'une attaque

Dans ce scénario, une organisation est informée d'un cas de violation suspectée. Elle cherche à retrouver le point d'entrée d'une attaque pour en identifier la source. L'organisation doit placer en quarantaine les entités compromises afin d'empêcher la propagation de l'attaque à d'autres parties.

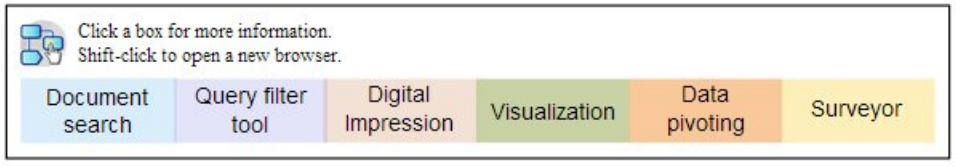
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Déterminer le type d'attaque.
- Identifier le point d'entrée de la menace.
- Obtenir des informations détaillées sur le contenu malveillant.
- Comprendre comment le contenu malveillant a été diffusé au-delà de son point d'entrée.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les attributs symptomatiques qui sont associés au contenu malveillant.

2. Utilisez les catégories de contenu pour exclure le contenu qui n'est pas pertinent pour les investigations.
3. Examinez le contenu suspect marqué par le produit.
4. Utilisez les outils d'impression numérique et de visualisation pour explorer les relations étendues du contenu malveillant, de l'auteur ou de la cible.
5. Utilisez l'outil de permutation de données et suivez les liens de données pour identifier le patient zéro.
6. Utilisez l'outil Surveyor pour afficher un calendrier linéaire des activités de manière à pouvoir retracer une attaque.

Systèmes compromis

Dans ce scénario, une organisation est informée que l'un ou plusieurs de ses systèmes ont été compromis par des techniques d'attaque informatique avancées, telles qu'une attaque de type "Watering Hole", un filoutage, une attaque en force brute ou une injection SQL.

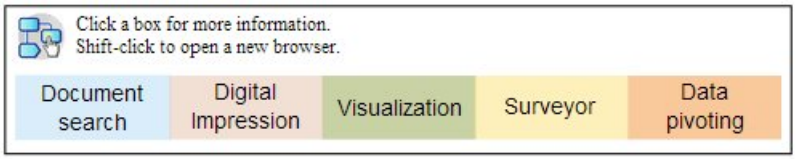
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Déterminer l'étendue de la compromission au sein de l'organisation.
- Comprendre le type de risque opérationnel de la compromission sur chaque système.
- Identifier les actions périphériques réalisées lors de l'attaque initiale pour contourner les activités de nettoyage et la détection.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher le contenu malveillant ou un document compromis.
2. Examinez le contenu suspect marqué par le produit.
3. Utilisez les outils d'impression numérique et de visualisation pour explorer les relations entre des entités qui résultent des systèmes compromis.
4. Utilisez l'outil Surveyor pour afficher un calendrier linéaire des activités de manière à pouvoir retracer une attaque.
5. Découvrez les incohérences ou les interactions suspectes entre des catégories de données en utilisant un format de recherche libre, l'outil de permutation de données et le contenu suspect.

Divulgation de données des entités non autorisées

Dans ce scénario, une organisation est informée que des données sensibles ont été divulguées à des entités non autorisées au sein de l'organisation ou à des parties externes.

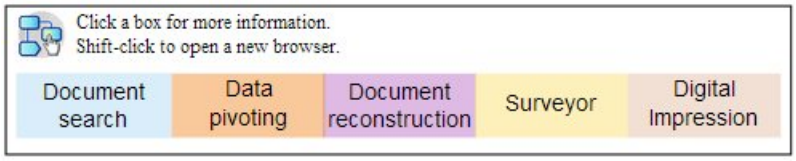
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Déterminer la nature et la quantité des données divulguées.
- Comprendre les techniques qui ont été employées.
- Démasquer les auteurs.
- Identifier la source de la fuite.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les identificateurs des données qui ont été divulguées.
2. Examinez le contenu suspect marqué par le produit.
3. Passez en revue la portée globale des données qui ont été ou qui sont divulguées en examinant la reconstruction des données.
4. Utilisez les outils d'impression numérique et de visualisation pour explorer toutes les relations entre des entités impliquées.
5. Utilisez l'outil Surveyor pour afficher un calendrier linéaire des activités de manière à pouvoir retracer une attaque.
6. Utilisez un format de recherche libre pour découvrir ce qui a motivé la divulgation des données.
7. Utilisez l'outil de permutation de données pour retrouver des liens avec d'autres données ayant éventuellement été divulguées.

Investigations liées à l'analyse d'initiés

QRadar Incident Forensics vous permet de détecter des collusions, ainsi que des actes de sabotage et de détournement de droits d'accès. Identifiez l'auteur et les complices de ces méfaits, les systèmes compromis et les pertes de données de document subies.

Utilisation des accès de façon détournée

Dans ce scénario, une organisation est informée que l'un ou plusieurs de ses employés utilisent leurs données d'identification de façon détournée ou en tant que proxy pour accéder à des données ou des systèmes sensibles et mener des activités illégales.

Objectifs

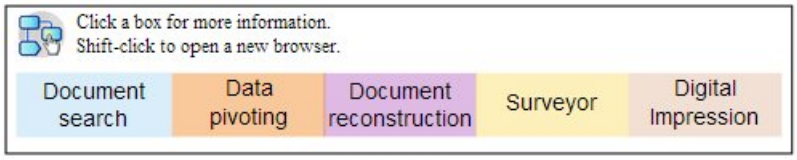
Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Déterminer l'identité de l'utilisateur.
- Déterminer la personne ou le système qui utilise cette identité pour mener des activités illégales.
- Comprendre l'objectif sur lequel repose l'utilisation détournée de l'accès.

- Déterminer si l'entité dispose d'autres identités susceptibles d'être utilisées de façon détournée.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les identités qui accèdent à des systèmes ou des données sensibles.
2. Identifiez les tentatives d'accès qui sont suspectes en examinant le contenu suspect, en effectuant des recherches au format libre, en permutant les données et en filtrant le contenu.
3. Visualisez la reconstruction des données associées au contenu qui fait l'objet d'un accès.
4. Retracez les modes d'accès et évaluez leur fréquence à l'aide de l'outil Surveyor.
5. Utilisez l'outil d'impression numérique pour découvrir les alias utilisés par une seule entité.

Collusion

Dans ce scénario, une organisation est informée qu'une ou plusieurs parties prenantes agissent ensemble ou avec la complicité de parties externes pour mener des activités qui lui portent préjudice.

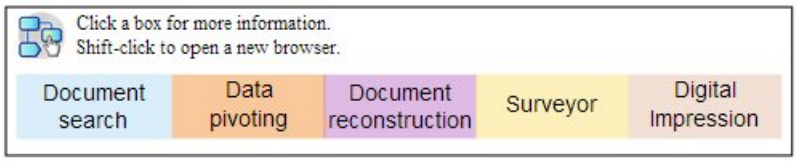
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Déterminer les entités qui sont de connivence.
- Comprendre la nature et les schémas des interactions entre les collaborateurs.
- Découvrir le contenu sur lequel repose le complot.
- Déceler la durée du complot pour comprendre la portée du risque.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les identificateurs des entités impliquées.
2. Examinez le contenu suspect marqué par le produit.
3. Utilisez l'outil d'impression numérique, de visualisation et le filtrage de contenu pour identifier les relations qui peuvent être suspectes.

4. Utilisez l'outil Surveyor pour suivre les activités des entités impliquées et obtenir le contenu des interactions.
5. Découvrez les motivations des entités complices en examinant les documents reconstruits.
6. Utilisez un format de recherche libre et l'outil de permutation de données pour rechercher le début des activités de complicité.

Sabotage

Dans ce scénario, une organisation est informée qu'une ou plusieurs parties prenantes tentent d'interrompre des opérations. La partie prenante peut être utilisée en tant que proxy.

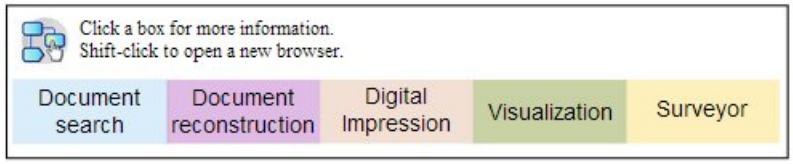
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Identifier le saboteur.
- Comprendre les techniques employées par le saboteur.
- Evaluer l'impact et la portée de l'interruption.
- Cerner les vulnérabilités qui ont été exploitées par le saboteur.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les symptômes du sabotage.
2. Examinez le contenu suspect marqué par le produit.
3. Utilisez la navigation visuelle, l'outil d'impression numérique et le filtrage de contenu pour explorer les symptômes et détecter les identificateurs du saboteur.
4. Utilisez l'outil Surveyor pour tracer les activités du saboteur.
5. Utilisez la reconstruction des données pour découvrir les rôles et les motivations du saboteur.
6. Utilisez la reconstruction des données pour examiner le contenu utilisé par le saboteur.
7. Utilisez un format de recherche libre, l'outil Surveyor et le contenu suspect pour révéler les procédures et les systèmes compromis qui ont permis le sabotage.

Investigations liées aux fraudes et aux détournements

Utilisez QRadar Incident Forensics pour localiser les transactions non autorisées, les affectations de ressources non approuvées, les écarts de protocole et les soustractions aux contrôles juridiques.

Transactions non autorisées

Dans ce scénario, une organisation est informée que des transactions non autorisées ont un impact financier négatif sur ses activités.

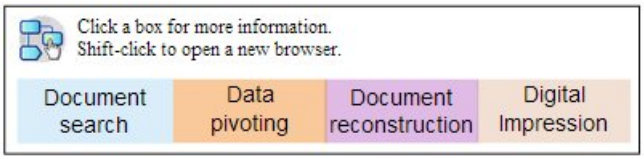
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Localiser les transactions non autorisées.
- Identifier les entités impliquées et responsables des transactions non autorisées.
- Comprendre la fréquence et les tendances des transactions non autorisées.
- Evaluer la portée du risque lié aux transactions non autorisées.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher des transactions incohérentes ou suspectes.
2. Utilisez un format de recherche libre et l'outil de permutation de données pour rechercher les répétitions de ces transactions.
3. Utilisez l'outil de permutation de données et l'outil d'impression numérique pour découvrir les entités qui sont associées aux transactions suspectes.
4. Découvrez le contenu des transactions afin d'en révéler la valeur quantitative en examinant les documents reconstruits.

Affectation de ressources non approuvée

Dans ce scénario, une organisation suspecte l'existence d'une affectation de ressources non approuvée susceptible d'avoir un impact financier négatif sur ses activités.

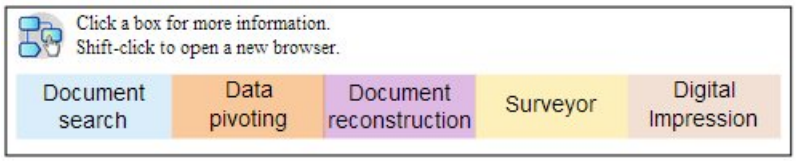
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Localiser la mauvaise affectation des ressources.
- Identifier les entités qui sont impliquées et responsables de la mauvaise affectation des ressources.
- Comprendre les motivations qui ont conduit à la mauvaise affectation des ressources.
- Evaluer la taille et la portée des ressources mal affectées.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les communications qui sont associées à des ressources affectées.
2. Utilisez un format de recherche libre, les outils de permutation de données et d'impression numérique pour rechercher les identificateurs des entités qui sont responsables de l'affectation de ressources non approuvée.
3. Traitez le contenu des interactions impliquées pour évaluer les motivations en examinant les documents reconstruits et en utilisant l'outil de visualisation.
4. Utilisez l'outil Surveyor pour retracer les activités d'affectation et déterminer la quantité de ressources mal affectées.

Ecarts de protocole et soustractions aux contrôles juridiques

Dans ce scénario, une organisation est informée que des processus métier, des protocoles informatiques et des contrôles juridiques ont été contournés, ce qui peut avoir un impact financier négatif.

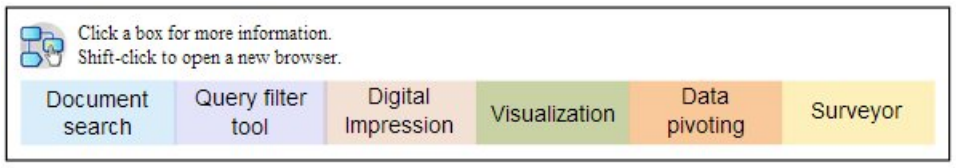
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Evaluer les protocoles ou les contrôles juridiques qui ont été contournés.
- Cerner les entités qui ont eu ce comportement.
- Comprendre les motivations de ces entités.
- Evaluer l'ampleur de cet écart de conduite.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les processus métier qui sont régis par des protocoles ou des contrôles.
2. Utilisez un format de recherche libre, l'outil de permutation de données et la reconstruction des données pour établir des références croisées avec la documentation qui décrit les protocoles et les contrôles juridiques.
3. Utilisez le filtrage de contenu et un format de recherche libre pour découvrir les entités spécifiques où les protocoles/contrôles ont été contournés.
4. Utilisez les outils d'impression numérique, de visualisation, de permutation de données et le filtrage de contenu pour rechercher les identificateurs d'entité associés.
5. Utilisez l'outil Surveyor pour retracer les activités des entités afin d'explorer les motivations possibles.

Investigations liées à la collecte de preuves

Utilisez QRadar Incident Forensics pour évaluer le risque de vulnérabilité au sein de l'organisation, établir un niveau de confiance pour l'identification des menaces ou des auteurs des menaces et affiner les pratiques en matière de sécurité.

Niveau de fiabilité de l'identification des menaces

Dans ce scénario, une organisation est informée de l'existence d'une menace, d'une attaque ou d'une vulnérabilité. Pour justifier les efforts de résolution qui pourraient empêcher le fonctionnement normal de l'organisation, celle-ci souhaite définir un intervalle de confiance pour tout risque associé.

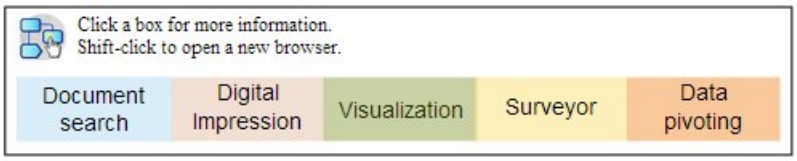
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Valider la susceptibilité au risque de sécurité.
- Déterminer s'il existe des preuves qui viennent étayer le risque de sécurité.
- Evaluer l'étendue et les répercussions financières du risque de sécurité.
- Comprendre la nature du risque de sécurité.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre, le contenu suspect et l'outil de permutation de données pour rechercher la menace, l'attaque ou la vulnérabilité en utilisant comme point de départ les entités potentiellement ciblées.
2. Utilisez un format de recherche libre et l'outil de permutation de données pour compiler les occurrences.
3. Utilisez un format de recherche libre pour établir des références croisées entre les documents susceptibles de faire référence à l'impact.
4. Utilisez les outils d'impression numérique et de visualisation pour identifier les entités concernées.
5. Utilisez l'outil Surveyor pour analyser les activités qui sont associées à la menace ou à l'auteur de la menace.

Procédure visant à affiner les pratiques de sécurité

La détection de comportements nouveaux et présentant des risques incite une organisation à évaluer l'efficacité des pratiques de sécurité existantes. Dans ce scénario, une organisation cherche à évaluer efficacité de ses règles de sécurité face aux risques encourus.

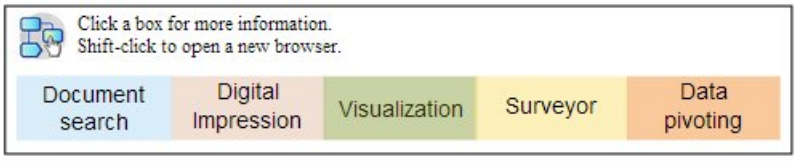
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Reconnaître les comportements nouveaux ou présentant des risques.
- Evaluer l'efficacité des règles de sécurité existantes.
- Comprendre les failles de sécurité qui apparaissent en raison d'opérations dynamiques.
- Evaluer l'efficacité des pratiques de sécurité proposées.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les comportements nouveaux ou présentant des risques, par exemple, pour les utilisateurs mobiles et les services basés sur le cloud, en utilisant les connaissances sur un domaine et une organisation.
2. Examinez le contenu suspect et utilisez l'outil Surveyor pour établir des références croisées entre ces comportements et des règles ou des pratiques de sécurité existantes.
3. Utilisez un format de recherche libre, l'outil Surveyor, la reconstruction du contenu et la visualisation pour analyser la fréquence et les faux résultats positifs des alertes liées aux règles de sécurité.
4. Utilisez un format de recherche libre, l'outil Surveyor, les outils de permutation de données et de visualisation pour découvrir les faux résultats négatifs qui ne sont pas détectés par les règles ou les pratiques de sécurité existantes.

Evaluation des risques

Dans ce scénario, une organisation est invitée à réaliser une évaluation des risques par un bulletin de sécurité décrivant des vulnérabilités, des attaques ou un comportement malveillant. L'évaluation des risques détermine si l'organisation est susceptible d'être ou est déjà comprise.

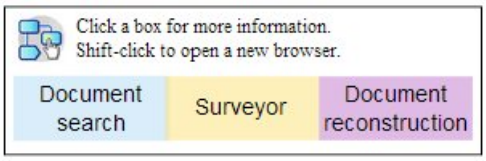
Objectifs

Pour résoudre le problème, l'organisation s'est fixé les objectifs suivants :

- Evaluer l'existence de vulnérabilités identifiées dans l'organisation.
- Détecter la présence malveillante de parties externes.
- Découvrir la preuve d'une compromission.
- Déterminer si l'organisation est victime d'une attaque.
- Déterminer l'identité de l'utilisateur.

Investigation

Utilisez les outils présents sur l'onglet **Forensics** pour vous aider dans vos investigations.



1. Utilisez un format de recherche libre pour rechercher les caractéristiques des vulnérabilités, des attaques ou de tout autre comportement malveillant spécifiés dans le bulletin de sécurité.
2. Utilisez un format de recherche libre pour effectuer une recherche par références croisées ou d'autres données pour obtenir des indicateurs.
3. Utilisez l'outil Surveyor pour faire des recherches sur les interactions qui ont pu exploiter les vulnérabilités ayant été identifiées.
4. Examinez le contenu suspect marqué par le produit.
5. Examinez le contenu sur lequel repose les interactions présentant un risque potentiel en utilisant la reconstruction des données.
6. Utilisez l'outil Surveyor pour retracer les activités des entités présentant un risque potentiel.

Chapitre 3. Initiation aux enquêtes d'expert

Pour commencer à utiliser les enquêtes d'expert IBM Security QRadar Incident Forensics, utilisez le menu **Quick Start** pour explorer et filtrer les données qui se trouvent dans le référentiel médico-légal. Ce tableau de bord contient des requêtes de synthèse prédéfinies que vous pouvez utiliser pour lancer une recherche ou obtenir des relations pour une entité.

Pour commencer, suivez ces directives :

1. Lancez une reprise ou une recherche médico-légale d'une infraction sur l'onglet **Infractions**.
   - Si vous cliquez avec le bouton droit sur une infraction ou une adresse IP et exécutez une reprise médico-légale, la criminalistique récupère les données de capture brutes pour les plages de temps spécifiées à partir du périphérique de capture, extrait et reconstruit les documents, puis ajoute les résultats au référentiel médico-légal.
   - Si vous cliquez avec le bouton droit sur une infraction ou une adresse IP et exécutez une recherche médico-légale, le référentiel médico-légal est filtré et exploré pour cette adresse IP. Les résultats sont ensuite affichés dans la grille principale de l'onglet **Forensics**. Vous pouvez affiner votre recherche en élaborant des requêtes.

   Lorsque QRadar Incident Forensics reçoit une demande de recherche, il traite les données de capture de paquets et les remet dans le format qui a été envoyé au destinataire désigné. Les documents Microsoft Word, par exemple, sont récupérés sous forme de fichiers Word. Les appels téléphoniques Voix sur IP sont récupérés sous forme de fichiers audio. Les fichiers récupérés sont ensuite indexés à l'aide de contenus de métadonnées et de fichiers pour les rendre consultables.
2. Dans l'onglet **Forensics**, cliquez sur **Quick Start**.

   Après avoir exécuté une reprise ou une recherche, au lieu de faire des recherches de forme libre et de construire vos propres requêtes, vous pouvez démarrer rapidement votre enquête en utilisant les requêtes prédéfinies dans le menu **Quick Start** dans l'onglet **Forensics**. Par exemple, vous pouvez regarder la catégorie **Suspect Content** et exécutez l'une des requêtes telles que **entity alert**. *Suspect content* est basé sur un ensemble défini de règles basées sur le contenu qui signale une activité suspecte. Une *entity alert* indique une éventuelle entité malveillante impliquée dans la violation d'une politique de sécurité..

   Les capacités de catégorisation et de filtrage de contenu contribuent à réduire le volume des données renvoyées
3. Dans la **Grille**, sélectionnez les documents à examiner.

   QRadar Incident Forensics renvoie les résultats de recherche des priorités. De même que l'optimisation des moteurs de recherche privilégie les sites dans une recherche sur Internet, les occurrences les plus fréquentes apparaissent en haut de la liste.

   Vous pouvez commencer à faire pivoter les données en cliquant sur les liens et en recherchant les métadonnées associées au document. Les capacités de pivot de données offrent différents points de vue de la recherche et des résumés de données.

4. Pour étudier les relations entre toutes les actions et l'incident de sécurité, dans la vue du document, sélectionnez un lien et cliquez avec le bouton droit de la souris sur **Get relations for**.

   Après avoir enquêté sur les attributs, filtrez les informations que vous réunissez en connectant les entités.

5. Cliquez sur **Digital Impressions** pour suivre la trace de l'identité et obtenir un ensemble compilé des associations.

   Une impression numérique est un index des métadonnées qui peuvent aider à identifier les agresseurs présumés ou les voyous en suivant la piste des utilisateurs malveillants. Dans la construction de ces relations, QRadar Incident Forensics utilise des données provenant de sources de réseau telles que les adresses IP, les adresses MAC et les ports et les protocoles TCP. Il peut trouver des informations telles que des ID de chat, et il peut lire des informations telles que l'identification de l'auteur à partir d'applications de traitement texte ou de tableur. Une impression numérique peut aider à découvrir les associations en liant l'identité de l'entité à des informations d'identification pour les autres utilisateurs ou entités.

Recherches et signets QRadar Incident Forensics

Les examinateurs utilisent IBM Security QRadar Incident Forensics pour extraire des données pertinentes à partir du trafic réseau et de documents.

Recherche et ajout de signets pour des enregistrements

Pour permettre des activités intuitives relevant du domaine criminalistique, QRadar Incident Forensics extrait des données de paquet et importe d'autres contenus. Cette technologie fournit des fonctions d'exploration de données basée sur la recherche, de reconstruction de session et d'intelligence criminalistique dans le but de mener des investigations sur les incidents liés à la sécurité.

Les examinateurs commencent leurs investigations en menant des actions à granularité grossière, puis affinent leurs constatations afin d'obtenir un ensemble de résultats pertinents définitifs. Une approche simplifiée de haut niveau consiste à commencer par rechercher un grand nombre d'enregistrements et à leur ajouter un signet. Il convient ensuite de se concentrer sur les enregistrements auxquels un signet a été ajouté afin d'identifier un ensemble d'enregistrements. L'étape suivante consiste à déterminer les éléments qui sont pertinents et à personnaliser des requêtes de manière à inclure et/ou exclure des éléments. Ces éléments serviront ensuite à démontrer une hypothèse.

A mesure que vous développez de nouvelles pistes, vous pouvez les suivre en utilisant d'autres méthodes. Vous pouvez utiliser les outils de visualisation et d'analyse pour évaluer manuellement et automatiquement la pertinence des résultats. Vous pouvez également différencier les requêtes afin de considérer un même problème sous différents angles.

Traitement des résultats auxquels un signet a été ajouté

Lorsque les résultats que vous obtenez sont significatifs pour votre investigation, vous pouvez leur ajouter un signet afin de les examiner de manière plus approfondie et les déterminer définitivement. Ajoutez plus de signets que vous pensez en avoir besoin. Si vous avez un doute, ajoutez un signet. Vous souhaitez éliminer les éléments non pertinents et vous concentrer sur ce que vous estimez pertinent.

Une fois que vous avez ajouté un signet à un ensemble de résultats que vous considérez comme pertinents, vous pouvez affiner l'examen.

1. Examinez chaque document auquel un signet a été ajouté au moyen des outils de visualisation et d'analyse.
2. Associez des notes de cas aux documents et prenez une décision définitive concernant la pertinence de chacun d'eux par rapport au cas.
3. Si un enregistrement n'est pas pertinent, retirez le signet.

   Au cours du processus d'investigation, vous avez identifié les éléments pertinents dans le référentiel et vous disposez à présent d'un ensemble d'enregistrements pertinents marqués par un signet.
4. Imprimez, exportez et traitez les enregistrements pertinents.

Recherche et examen des documents

Les examinateurs recherchent des documents pertinents pour une piste ou une hypothèse concernant la survenue d'un incident de sécurité.

Recherches

Au lieu de passer au crible manuellement des masses de documents, qui, pour la plupart, n'ont pas de rapport avec le cas présent, les examinateurs utilisent le référentiel Forensics afin d'extraire des documents répondant aux caractéristiques intéressantes. Par exemple, un document qui appartient à une période ou à un sujet d'intérêt spécifique ou un document envoyé ou reçu d'un attaquant suspecté.

Les recherches peuvent être spécifiques. Par exemple, la recherche de la chaîne de caractères exacte "Mission Alpha" est une recherche spécifique. Les recherches peuvent aussi être d'ordre général. Par exemple, la recherche portant sur la chaîne "find all social security numbers wherever they exist in the repository" est plus générale.

Les recherches peuvent être simples et basées uniquement sur un critère. Les résultats des recherches complexes doivent satisfaire à plusieurs conditions. Par exemple, une opération visant à rechercher tous les courriers électroniques entre deux attaquants suspectés et à exclure les courriers électroniques contenant des pièces jointes constitue une recherche complexe. La finalité d'une recherche est de réduire avec rapidité et précision le nombre d'enregistrements afin d'obtenir un jeu de documents gérable. La réduction du nombre de documents à traiter par l'examinateur augmente la probabilité de la pertinence de ces documents pour le cas.

Reprise Forensics

Pour extraire les données de capture de paquet brutes des périphériques de capture de paquet, exécutez un travail de reprise Forensics sur un(e) ou plusieurs ports ou adresses IP.

Reprise sur une adresse IP ou un port

Exécutez une reprise Forensics pour extraire les données de capture brutes du périphérique de capture. Vous pouvez exécuter une reprise sur plusieurs adresses IP ou ports. Si vous n'entrez pas d'adresse IP ou de port, le trafic TCP et UDP dans son ensemble est récupéré. Si vous en entrez plusieurs, séparez-les d'une virgule.

Exécutez une reprise Forensics en cliquant avec le bouton droit de la souris dans QRadar, ou en sélectionnant l'icône d'**exécution de la reprise**  dans l'onglet Forensics.

Restriction : En règle générale, vous pouvez entrer environ 7 adresses IPv4 et 7 ports ou un maximum de 255 caractères à la fois. Les zones **Adresse IP** et **Port** sont combinées avec d'autres expressions pour créer une chaîne de filtre. La chaîne de filtre ne peut pas dépasser plus de 255 caractères

Réexécution de reprise

Dans l'onglet Forensics, utilisez l'option de réexécution de la reprise sur la grille de résultats pour exécuter une reprise précédemment créée. Si, par exemple, les résultats renvoient des données incomplètes, vous réexécutez une reprise Forensics afin d'inclure des adresses IP différentes ou vous changez la période spécifiée dans l'exécution du travail de reprise précédent.

Pour réexécuter le travail de reprise Forensics précédent, cliquez sur l'option permettant de **réexécuter cette reprise Forensics**. Lorsque vous réexécutez un travail de reprise, la page Reprise Forensics comporte les valeurs de l'exécution précédente. Vous pouvez exécuter une reprise identique ou bien changer les valeurs générées automatiquement.

Vous pouvez réexécuter une reprise uniquement quand le travail est terminé, possède le statut Terminé Annulé ou Echec.

Cas Forensics

Les cas sont des conteneurs logiques destinés à la collection des documents importés et des fichiers de capture de paquet.

Les cas sont créés par les administrateurs ou les examinateurs disposant de droits suffisants pour créer des cas. Les administrateurs créent des cas et les affectent à des examinateurs. Les examinateurs peuvent créer un nouveau cas lorsqu'ils extraient les données de capture de paquet à partir d'une adresse IP dans IBM Security QRadar.

Tâches associées:

«Téléchargement de fichiers et documents PCAP à partir de systèmes externes dans des cas Forensics», à la page 19
Vous pouvez télécharger des données externes dans des cas spécifiques.

Collections

Utilisez des collections pour regrouper des données associées provenant d'une source spécifique, comme un fichier de données de capture de paquet (PCAP), un fichier PDF ou un flux réseau.

Les collections sont utilisées pour identifier et gérer des groupes de données associées. Vous pouvez supprimer rapidement les données regroupées dans la collection une fois l'investigation terminée.

Les collections sont créées par les administrateurs ou les examinateurs. Les administrateurs créent des collections pour charger manuellement les données dans IBM Security QRadar Incident Forensics. Les administrateurs ajoutent également

les collections à des cas. Les examinateurs peuvent créer une collection lorsqu'ils commencent à extraire les données de capture de paquet à partir d'une adresse IP dans IBM Security QRadar.

Concernant les collections et les noms de collection, tenez compte des règles suivantes :

- Les noms de collection doivent être uniques.
- Les cas comportent une ou plusieurs collections.
- Les collections peuvent être ajoutées à plusieurs cas.
- Les résultats de la recherche renvoient des données en double lorsqu'un examinateur possède deux cas avec la même collection.
- Si un nom de collection n'est pas unique lors du transfert d'un nouveau fichier PCAP, la collection initiale est supprimée avant le transfert du nouveau fichier PCAP.

Téléchargement de fichiers et documents PCAP à partir de systèmes externes dans des cas Forensics

Vous pouvez télécharger des données externes dans des cas spécifiques.

Avant de commencer

Un administrateur doit activer les droits d'accès FTP sécurisés pour l'utilisateur qui souhaite télécharger des fichiers externes.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar Incident Forensics peut importer des données à partir de n'importe quel répertoire accessible figurant sur le réseau. Les formats pouvant être utilisés pour ces données sont nombreux. Il s'agit notamment mais pas exclusivement des formats suivants :

- Fichiers de format PCAP à partir de sources externes
- Documents, tels que des fichiers texte, des fichiers PDF, des feuilles de calcul et des présentations
- Fichiers image
- Flux de données en continu à partir d'applications
- Flux de données en continu à partir de sources PCAP externes

Vous pouvez télécharger plusieurs fichiers dans un cas.

Restriction : Le nom de cas doit être unique. Vous ne pouvez pas créer un cas portant le même nom qu'un cas existant.

Procédure

1. Dans le client FTP, procédez comme suit :
   a. Vérifiez que le protocole TLS (Transport Layer Security) est sélectionné.
   b. Ajoutez l'adresse IP à l'hôte QRadar Incident Forensics.
   c. Créez un ID connexion qui utilise le nom d'utilisateur et le mot de passe QRadar Incident Forensics qui ont été créés.
2. Connectez-vous au serveur QRadar Incident Forensics et créez un nouveau répertoire.

3. Pour utiliser un accès 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.
4. Pour utiliser un accès FTP et stocker d'autres types de fichier que PCAP, sous le répertoire que vous avez créé pour le cas, créez un répertoire nommé `import` et faites glisser les fichiers vers ce répertoire.
5. Pour redémarrer le serveur FTP, entrez la commande suivante :

   ```
   etc/init.d/vsftpd restart
   ```
6. Pour redémarrer le serveur qui déplace les fichiers de la zone de téléchargement vers le répertoire QRadar Incident Forensics, entrez la commande suivante :

Résultats

Votre cas apparaît désormais dans l'un des outils affichés sur l'onglet **Forensics**.

Requêtes de référentiel Forensics

Les examinateurs spécifient les caractéristiques des documents qui les intéressent pour l'extraction de la base de données Forensics. Pour un examen, plusieurs requêtes sont utilisées pour rechercher un ensemble de documents.

Plusieurs requêtes et l'inspection manuelle d'un petit ensemble de documents offrent plus de résultats qu'en passant au crible le référentiel entier. Les idées de requêtes suivantes et de requêtes affinées surviennent souvent lors de l'inspection d'un document non pertinent.

Une quantité accrue et une spécificité des termes des requêtes entraînent une plus grande pertinence des ensembles de résultats. Votre objectif est de définir autant que vous en savez des résultats souhaités et d'être très spécifique lorsque cela est possible. Vous pouvez entrer un nombre indéfini de termes de requête dans les critères de recherche. Vous séparez les termes avec un espace ou avec un opérateur booléen. Les termes séparés uniquement avec un espace impliquent un opérateur logique booléen OR. L'opérateur OR signifie que les résultats des termes sont tout aussi souhaitables les uns que les autres. Les résultats correspondant à la plupart des termes de la recherche sont placés en haut de la liste pour indiquer l'importance de la correspondance aux termes de la requête.

Un critère de recherche unique est également appelé terme de requête. Les recherches impliquent généralement plusieurs termes de requête. L'ensemble de termes de requête pour une recherche unique est également appelé chaîne de requête. L'expertise de la formulation des requêtes exige de la pratique, mais cela n'est pas difficile. Cela n'implique réellement que quelques termes de requête et l'apprentissage de la création et de la négation des termes dans des combinaisons qui vous permettent d'obtenir les résultats escomptés. Dans la mesure où les chaînes de requête sont enregistrées dans QRadar Incident Forensics, vous pouvez affiner en continu vos recherches lorsque vous en savez plus sur les données afin d'obtenir, à terme, exactement ce que vous voulez.

Tâches associées:

«Visualisation des relations et des associations», à la page 32
La fenêtre Visualize vous permet de voir les relations entre les attributs au sein de documents restaurés. Par exemple, vous pouvez examiner les adresses e-mail qui ont communiqué avec une adresse e-mail spécifique.

Termes de requête à structure libre

Les examinateurs cherchent des correspondances exactes de chaînes de caractères en entrant directement les termes de requête souhaités dans la zone de critères de recherche sur l'onglet **Forensics**. Vous pouvez utiliser des requêtes comportant un seul mot ou plusieurs mots.

Le tableau ci-dessous décrit le type de requêtes de recherche pouvant être utilisées.

Tableau 1. Types de requêtes à structure libre

Type de requête de recherche	**Description**	**Exemple**
Requête comportant un seul mot	Recherche un terme dans les documents.	chiots
Requête unique avec des caractères génériques	Recherche une correspondant pou un ou plusieurs caractères au milieu ou à la fin d'un terme de requête. **Restriction :** Les caractères génériques ne peuvent pas être utilisés comme premier caractère d'une recherche.	te?t test* te*t
Requête comportant plusieurs mots	Spécifie que les résultats de la recherche sont renvoyés dans l'ordre de pertinence des termes de requête. Les documents contenant les deux termes de requête sont répertoriés en premier, suivis des documents contenant un seul des termes de requête. Ces documents sont classés par ordre décroissant de nombre d'occurrences du terme de requête.	chiots gratuits
Requête comportant plusieurs mots avec des guillemets doubles	Correspond à la chaîne exacte. Les documents contenant les deux mots, mais pas dans cet ordre et dans cette proximité, ne sont pas renvoyés dans les résultats. Effectivement, les guillemets doubles convertissent des deux mots en une chaîne simple ou un terme de requête. Pour le moteur de recherche, ils ne sont plus considérés comme deux mots distincts.	"chiots gratuits"
Requête comportant plusieurs mots et utilisant l'opérateur AND	Spécifie que les deux termes de requête doivent être présents dans le document pour aboutir à une correspondance. Les termes de la requête peuvent apparaître dans un ordre quelconque et il n'est pas nécessaire qu'ils se trouvent en étroite proximité.	chiots AND gratuits

Balises de métadonnées

Les entités courantes sont marquées pour permettre aux examinateurs d'extraire rapidement les ensembles de résultats exacts des documents pertinents.

De nombreux champs de métadonnées peuvent être utilisés dans l'index d'Incident Forensics en fonction du type de session, de document ou de protocole.

Lorsque vous spécifiez un nom de balise de métadonnées, il doit être exact et exister dans le référentiel Forensics.

Le tableau ci-dessous répertorie les types de recherche de balise de métadonnées.

Tableau 2. Recherche de balise de métadonnées

Type de recherche de balise de métadonnées	Format	Exemple
Standard	`MetadataTag:<valeur>`	`ApplicationProtocol:http`
Caractère générique	`MetadataTag:*`	`CreditCardNumber:*`
Plage	`MetadataTag:[<valeur de début> TO <valeur de fin>`	`Duration:[30 TO 56]`

Concepts associés:

«Annotations d'un document», à la page 25
Les examinateurs ajoutent un signet et des notes à des documents pour suivre des idées et la justification des documents concernant leur cas.

Combinaisons booléennes

Plusieurs termes de requête peuvent être reliés les uns aux autres à l'aide d'opérateurs booléens simples dans le but de créer des chaînes de requête hautement ciblées. Ces dernières renvoient des résultats correspondant exactement à ce que recherche un examinateur.

Les opérateurs booléens standard sont AND (ET), OR (OU), NOT (DIFFERENT DE) et (). L'opérateur AND spécifie que les deux termes de requête doivent correspondre dans le document. L'opérateur OR spécifie que l'un ou l'autre terme de requête doit être détecté dans un document. L'opérateur NOT correspond à la négation ou à la suppression des résultats correspondant aux termes de requête à éliminer. L'opérateur () regroupe des termes et des valeurs de requête afin d'appliquer des fonctions à un ensemble, d'appliquer différentes valeurs à une fonction ou de clarifier la syntaxe.

Les opérateurs booléens doivent être en majuscules.

Le tableau ci-dessous répertorie les opérateurs booléens et des exemples de chaîne de requête.

Tableau 3. Opérateurs booléens pour les chaînes de requête

Opérateur booléen	Exemple de chaîne de requête	Explication de l'exemple
AND	`TcpPort:80 AND Protocol:http`	Deux termes de requête sont utilisés pour détecter tout le trafic Web standard. Si les tests Web ont lieu sur le port 8080, cela ne correspond pas car les deux termes de requête ne sont pas vrais.
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	Trois termes de requête sont utilisés pour limiter les résultats aux résultats provenant des collections de documents Yahoo, CNN et MSN dans le référentiel Forensics.

Tableau 3. Opérateurs booléens pour les chaînes de requête (suite)

Opérateur booléen	Exemple de chaîne de requête	Explication de l'exemple
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	Recherche le trafic utilisant des ports non standard. Le premier terme de requête recherche le trafic HTTP standard et le second terme de requête élimine tout le trafic qui utilise les ports HTTP acceptés.

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		Ces requêtes utilisent efficacement les parenthèses pour atteindre des objectifs complexes. Sans les parenthèses, ces requêtes sont plus longues et plus complexes à formuler et à déboguer.

Outil de générateur de requête

Utilisez l'outil de générateur de requête pour créer des recherches ou gérer des recherches sauvegardées.

L'outil de générateur de requête guide les examinateurs, par le biais d'une interface graphique, dans la procédure de création de recherches puissantes utilisant des listes catégorisées de termes de requêtes avec des exemples.

Tableau 4. Paramètres de l'outil de générateur de requête

Paramètre	Description
Select Category	Filtre la liste des balises de métadonnées disponibles dans la liste **Select Field**.
Select Field	Balises de métadonnées utilisées pour marquer les informations dans le référentiel Forensics.
Query Example	Exécute la requête qui se trouve dans la zone **Query Input** et indique le nombre de résultats.
New	Remplace une requête existante par la nouvelle requête lorsque vous cliquez sur **Insert Query**.
AND	Combine une nouvelle requête avec la requête existante lorsque vous cliquez sur **Insert Query**. Les documents doivent correspondre aux deux termes de requête.
OR	Combine la nouvelle requête avec la requête existante lorsque vous cliquez sur **Insert Query**. Les documents doivent correspondre à l'un ou l'autre des termes.

Les examinateurs peut sauvegarder et organiser les recherches dans des dossiers sur le système de fichiers, ce qui permet un partage entre examinateurs. Les examinateurs utilisent des descriptions ou des noms pour les requêtes enregistrées à des fins de référence, de gestion et de compréhension.

La fonction **Use Query** sur l'onglet **Query** est utilisée pour envoyer une requête enregistrée dans la zone **Search Criteria Input** pour exécution.

Les examinateurs utilisent la liste de requêtes précédente pour rechercher les requêtes exécutées précédemment et les réexécuter en sélectionnant simplement la requête qu'ils souhaitent exécuter et en cliquant sur **Insert Query**.

Outil de filtre de requête

L'outil de filtre de requête utilise les données actives pour fournir des indices visuels afin de créer des filtres persistants.

Le filtre de requête est un filtre d'arrière-plan persistant qui permet de réduire la taille de l'ensemble de documents actifs sur lequel porte la chaîne de requête. Un filtre vous permet de réduire la taille de l'ensemble de documents disponibles sans surcharger la chaîne de requête avec des termes de requête statique. Vous étendez ainsi votre contrôle sur la chaîne de requête.

Le filtre de requête constitue un excellent point de départ pour une investigation car il procure des listes de types de filtre basées sur les cas, la mise à jour dynamique et un résumé des résultats en temps réel. Les listes de types de filtre sont renseignées à l'aide de toutes les valeurs trouvées dans les cas dont vous disposez. Vous pouvez afficher rapidement les données qui sont contenues dans les cas dont vous disposez. La sélection ou la désélection des éléments de liste de types de filtre met à jour automatiquement le résumé des résultats. L'utilisation du filtre vous permet d'obtenir rapidement un ensemble de documents de taille réduite.

Il n'est pas recommandé d'activer le filtre de requête par défaut pour les requêtes que vous souhaitez réutiliser. Pour ce type de requête, créez un nouveau filtre de requête. Si vous avez modifié le filtre de requête par défaut, réinitialisez-le lorsque vous avez fini de l'utiliser afin d'éviter que des documents soient exclus par erreur de vos prochaines requêtes de recherche.

Résultats des filtres actifs

Les examinateurs affichent les résultats des filtres actifs dans la section de résumé des résultats de l'outil de filtre de requête.

Si le filtre est modifié, le résumé est mis à jour afin d'afficher le nombre total de documents et le nombre de documents disponibles. Le nombre total de documents est le nombre de documents disponibles pour l'examinateur avant application du filtre. Le nombre de documents disponibles est le nombre de documents disponibles après application du filtre. Les examinateurs utilisent ces nombres pour estimer l'efficacité de leur filtre et l'ajuster de façon appropriée lorsqu'ils le créent.

Filtres de recherche pour l'outil de filtre de requête

Les examinateurs filtrent les données des cas qui leurs sont affectés. Les données sont séparées en groupes par type de filtre, par exemple, Adresse IP ou Adresse MAC.

Grâce à l'action logique alternative, l'examinateur peut inclure ou exclure les éléments sélectionnés dans la liste.

Chaque groupe de filtres de recherche possède une action logique alternative, qui permet de définir que les éléments sélectionnés dans la liste sont inclus ou exclus. Lorsqu'il est défini que les éléments de la liste sont inclus avec un opérateur logique AND, cela signifie que chaque document disponible contient tous les

éléments sélectionnés. En cas d'exclusion, un opérateur logique OR est utilisé, ce qui signifie que chaque document disponible contient l'un des éléments sélectionnés.

Les examinateurs peuvent utiliser le groupe **UserQuery** pour formuler leurs propres chaînes de requête à ajouter au filtre.

Limitation du nombre de documents renvoyés dans une recherche

Vous pouvez ajouter des filtres à vos demandes IBM Security QRadar Incident Forensics pour limiter le nombre ou le type de documents que vous voyez dans la page de résultats de recherche.

Procédure

1. Dans l'onglet **Forensics**, cliquez sur l'icône **Query Filters**.

   Les données sont séparées en groupes par type de filtre.
2. Dans la fenêtre Search Filters, pour chaque type de filtre, choisissez d'inclure les documents dans les résultats de recherche en cliquant sur **Include** ou **Exclude**.
3. Pour trouver un élément dans un groupe de filtres, procédez comme suit :
   a. Dans la colonne **Filter Type**, développez un groupe de filtres.
   b. Dans la fenêtre Search, sélectionnez les critères et cliquez sur **Find**.

      Lorsque vous recherchez un enregistrement dans le groupe de filtres **Webcategory**, toutes les zones de catégorie correspondantes sont affichées. Par exemple, lorsque vous recherchez **Webcategory equal chat**, **Chat**, et des catégories apparentées, telles que **Instant Messaging**, **Webmail/Unified Messaging**, **Search Engines/Web catalogs/Portals**, et **Cloud** sont affichés.

Annotations d'un document

Les examinateurs ajoutent un signet et des notes à des documents pour suivre des idées et la justification des documents concernant leur cas.

Les documents peuvent être marqués par un signet dans l'écran des résultats principaux et dans l'outil Surveyor dans le tableau chronologique qui affiche la séquence d'échange des documents lors d'une interaction. Les requêtes et les investigations pouvant être complexes, les examinateurs ajoutent un signet pour tous les enregistrements, y compris pour les documents avec peu d'intérêt. L'utilisation de signets élimine le besoin de récréer les requêtes complexes et les lignes d'investigation. Il est possible de créer des annotations après avoir ajouté un signé pour un enregistrement.

Lors d'une investigation, vous souhaitez parfois suivre deux chemins ou plus. Utilisez la fonction de navigateur pour dupliquer l'onglet en cours. Cela vous évite d'avoir à vous rappeler que vous devez revenir en arrière pour suivre les autres chemins ou à mémoriser le chemin pour accéder au point de branchement. Vous pouvez le faire autant de fois que nécessaire. Suivez les différents chemins dans un autre onglet et ajoutez un signet sur les documents pertinents. Vous pouvez ajouter une note désignant le chemin qui vous a conduit à chaque document auquel un signet a été ajouté.

L'utilisation de notes vous permet d'enregistrer des informations lors de vos investigations. Seul un administrateur est en mesure de supprimer des notes. Les notes sont marquées avec l'ID utilisateur de l'examinateur et l'horodatage

correspondant au moment où elles ont été entrées. Les notes sont émises avec le document reconstruit et ses attributs lors de l'exportation des documents.

Concepts associés:

«Balises de métadonnées», à la page 21
Les entités courantes sont marquées pour permettre aux examinateurs d'extraire rapidement les ensembles de résultats exacts des documents pertinents.

Chapitre 4. Outils d'investigation

Les examinateurs utilisent les outils Surveyor, d'impression numérique, d'exportation et de visualisation pour gérer les données de différentes manières.

La page des résultats de la recherche est la page par défaut sur l'onglet **Forensics**. Les résultats de la recherche sont disponibles sous l'onglet **Grid**. Les examinateurs utilisent les résultats de la recherche dans le tableau pour rechercher rapidement des documents et y accéder. Sous l'onglet **Grid**, utiliser les outils Surveyor, d'impression numérique, d'exportation et de visualisation pour approfondir les investigations.

Indicateur de ligne

L'indicateur de ligne fournit un identificateur unique pour chaque document renvoyé dans un ensemble de résultats; Utilisez l'indicateur de ligne pour envoyer un document et tous les documents associés nécessaires à l'outil de visualisation Reconstructed View.

Tri des lignes

Vous pouvez trier les lignes affichées dans le tableau. Etant donné que le nombre total de résultats peut être supérieur au nombre de résultats affichés sur la grille, l'intégralité de l'ensemble de résultats ne peut pas être triée.

Indicateur de documents affichés

L'indicateur de documents affichés est un cercle de petite taille qui passe du rouge au vert pour indiquer si un examinateur a visualisé un document.

Sélection des documents

Les examinateurs utilisent la sélection des documents affichés pour sélectionner le nombre de documents qui s'affichent dans le tableau de résultats. Vous pouvez utiliser SELECT ALL pour envoyer les documents à une fonction suivante et vous pouvez envoyer de nombreux documents pour traitement ou visualisation. Lorsque vous sélectionnez des documents à l'aide du sélectionneur de documents affichés, vous sélectionnez tous les documents et non pas uniquement les documents présents dans la grille.

Visualisation du réseau et des documents

Les examinateurs utilisent l'outil de visualisation pour détecter les modèles de détection, comprendre l'endroit où il y a le plus de congestion du trafic réseau et des documents au cours d'une période spécifiée et afficher le contenu suspect. Par exemple, les examinateurs peuvent visualiser les modèles de trafic réseau, comme les accès aux serveurs en dehors des heures de bureau.

L'outil VGrid est divisé en tranches horaires. Le contenu suspect (trafic réseau ou documents) est signalé par un rectangle rouge dans le tableau. Un rectangle vert signale un contenu normal. Une tranche horaire associée à une couleur vive indique un surplus de trafic. Plus la couleur est saturée, plus le trafic est important. La vivacité de la couleur d'une tranche horaire est relative aux données

actuelles affichées dans l'outil VGrid. Par exemple, une tranche horaire dont la couleur est vive fonce à mesure que d'autres tranches horaires sont reçoivent plus de données.

Les examinateurs peuvent afficher les types de trafic réseau et le nombre de documents pour chaque tranche horaire contenant du contenu.

Inspection du trafic réseau et des documents dans une tranche horaire

Les examinateurs souhaitent peut-être inspecter des documents individuels, des sites Web visités ou des courriers électroniques dans une tranche horaire spécifique.

Procédure

1. Sous l'onglet **Forensics**, sélectionnez l'onglet **VGrid**.
2. Pour inspecter le contenu d'une tranche horaire, utilisez l'une des options suivantes :
   - Pour afficher les types de trafic réseau et le nombre de documents, passez la souris sur la tranche horaire.
   - Pour rechercher le contenu de la tranche horaire, sélectionnez une ou plusieurs tranches horaires. Cliquez avec le bouton droit et sélectionnez select **Search selected time blocks**.
   - Pour afficher la séquence d'événements, sélectionnez la tranche horaire, puis sélectionnez **Surveyor**.
   - Pour visualiser le contenu, sélectionnez une tranche horaire, puis sélectionnez **Visualize**.

Outil Surveyor

Utilisez l'outil Surveyor pour visualiser une séquence d'événements dans un incident de sécurité lorsqu'ils se produisent.

Les examinateurs utilisent cet outil pour savoir ce que les attaquants suspectés ont affiché et effectué. L'outil Surveyor décrit la séquence chronologique des activités dans un incident de sécurité dans un visualiseur vidéo. Comme l'outil Surveyor est lié à l'heure, la sélection d'un document unique dans l'écran des résultats n'affiche que peu de résultats. Si trop peu de documents ont été sélectionnés, étendez la fenêtre de temps autour des documents sélectionnés sur l'onglet **Attributes**. Développez la période en cliquant sur le lien **Show Context**.

Utilisez l'onglet des **attributs** pour afficher les informations métadonnées de certificat. Vous cliquez avec le bouton droit de la souris sur une adresse IP pour filtrer en fonction des événements, des flux et des actifs, ou bien sur une adresse MAC pour filtrer en fonction des événements et des actifs.

Vous pouvez filtrer leurs requêtes par heure, protocole et adresse IP.

Vous utilisez l'onglet de **liste** pour découvrir une liste chronologique des documents envoyés et reçus.

Les numéros d'ID de document en vert indiquent qu'un document a été revu par un examinateur, tandis que les documents portant des numéros d'ID rouge n'ont pas été revus.

Vue des documents reconstruits

L'onglet **View** affiche une vue reconstruite du document sélectionné dans la partie gauche de l'écran, sans la vue List.

Cette combinaison puissante de séquencement à gauche et la reconstruction dans la partie droite peuvent permettre de découvrir ce que les attaquants suspectés ont affiché et effectué sur le réseau. Outre les documents visibles qui sont passés sur le réseau, l'outil Surveyor affiche également les échanges en coulisses entre ordinateurs et les échanges de certificats qui ont eu lieu.

Tâches associées:

Chapitre 5, «Examen du trafic réseau pour rechercher une adresse IP», à la page 41
Pour bénéficier de la visibilité du contenu pertinent dans les conversations qui ont eu lieu lors d'un incident de sécurité, vous pouvez restaurer et reconstruire le trafic réseau associé à une adresse IP. Vous pouvez également rechercher des cas existants qui sont liés à une adresse IP.

Contenu d'un document extrait

L'onglet **Text** affiche le contenu extrait du document. Le contenu du document n'est pas mis en forme.

Ce texte provient de l'indexeur de moteur de recherche.

Exportation de documents dans QRadar Incident Forensics

Dans IBM Security QRadar Incident Forensics, tous les documents exportés, sauf les documents pcap exportés, incluent le document reconstruit, le texte brut du document, les attributs et les notes qui sont joints au document.

Lorsque les documents pcap sont exportés, aucune reconstruction ne s'effectue. Par exemple, lorsque vous exportez une page Web, tout ce que le navigateur a téléchargé lors de la connexion principale est téléchargé. Habituellement, la plupart du contenu du texte est téléchargé lors de la connexion principale. Cependant, la plupart des navigateurs modernes utilisent plusieurs connexions pour télécharger d'autres éléments, tels que des feuilles de styles et des images qui ne font pas partie de l'exportation. Lorsque vous exportez, le contenu pcap n'est pas reconstruit en premier lieu.

Un autre exemple inclut des protocoles complexes, tels que FTP et VOIP, où il existe une connexion de contrôle et de commande principale et une connexion de données distincte. Si vous exportez les fichiers pcap pour un appel VoIP ou un téléchargement FTP, les données ne sont pas reconstruites et vous pourriez obtenir des résultats que vous n'attendiez pas.

Exportation de documents au format pcap

Vous pouvez exporter des documents en tant que fichiers pcap depuis plusieurs dispositifs IBM Security QRadar Incident Forensics et IBM Security QRadar Packet Capture.

Restriction : Le contenu exporté au format pcap n'est pas reconstruit.

Procédure

1. Pour exporter des données depuis une sélection de documents, dans la grille de reprise de l'onglet **Forensics**, sélectionnez les cases en regard de ces documents puis cliquez sur **Export**.

Vous pouvez sélectionner jusqu'à 25 documents à exporter au format pcap.

2. Depuis la liste **Select Export Type**, cliquez sur **PCAP**.
3. Une fois que tous les documents d'un hôte QRadar Incident Forensics sont exportés, cliquez sur **Download**.
4. Si l'exportation d'un document échoue, essayez de le réexporter en cliquant sur le message **FAIL**.

Résultats

Si vous exportez un fichier pcap unique, le fichier pcap est téléchargé. Si vous exportez plus d'un fichier pcap, ces fichiers sont compressés au format .zip. Le fichier compressé est téléchargé.

Chaque document conserve l'adresse IP de l'hôte QRadar Incident Forensics et l'adresse IP du périphérique QRadar Packet Capture d'origine du document. Si vous retirez un hôte QRadar Incident Forensics ou bien déplacez un périphérique QRadar Packet Capture, vous ne serez peut-être pas en mesure de procéder à l'exportation.

Outil d'impression numérique

Une *impression numérique* est un ensemble compilé d'associations et de relations qui identifient les trajets d'identité. L'outil d'impression numérique reconstruit les relations réseau afin de vous permettre d'identifier une entité qui attaque et de déterminer son mode de communication et les autres entités avec lesquelles elle communique.

Utilisez l'outil d'impression numérique pour répondre rapidement aux questions importantes suivantes :

- Que sait-on de cet attaquant suspecté, de cet ordinateur ou de cette adresse IP ?
- A qui cet attaquant suspecté a-t-il parlé ?
- Qui appartient à son réseau de contacts ?
- L'attaquant suspecté essaie-t-il de déguiser son identité ?

Identificateurs en ligne

Les identificateur en ligne, par exemple, les adresses électroniques, les adresses Skype, les adresses MAC, les ID de conversation instantanée, les ID médias sociaux ou les ID Twitter, permettent d'identifier les entités ou les personnes. Les entités ou les personnes connues détectés dans le trafic réseau et les documents sont marqués automatiquement.

IBM Security QRadar Incident Forensics établit une corrélation entre les identificateurs marqués qui ont agi en interaction les uns avec les autres pour produire une impression numérique.

Les relations de collection dans les rapports d'impression numérique représentent une présence électronique collectée en continu, associée à un attaquant ou à une entité liée à un réseau, ou à un terme de métadonnées de l'impression numérique. Les examinateurs peuvent cliquer sur un identificateur d'impression numérique marqué associé à un document. Le rapport de l'impression numérique qui en résulte est présenté sous forme de tableau, organisé par type d'identificateur.

Obtention des informations de relation

Un rapport d'impression numérique affiche les interactions entre un *identificateur de centrage* et tous les autres identificateurs. Un *identificateur de centrage* est l'identificateur en ligne qui est la source d'intérêt dans un incident de sécurité.

L'identificateur de niveau supérieur dans de nombreuses catégories correspond généralement à l'identité de l'identificateur de centrage dans ce type ou cette catégorie d'identificateur. Par exemple, si l'identificateur est une adresse MAC, l'adresse électronique qui a le plus d'interactions est plus probablement l'attaquant suspecté qui est propriétaire de l'ordinateur. Toutefois, si les adresses IP sont attribuées de manière dynamique, vous devez également examiner les adresses IP affectées sur un intervalle de temps.

Les corrélations entre les autres catégories et l'identificateur de centrage sont généralement moins fortes. Avant de décider d'agir en fonction de l'impression numérique, validez les données à l'aide de sources indépendantes. Utilisez l'outil d'impression numérique pour étendre le rayon d'une investigation à davantage d'attaquants et d'entités suspectés.

Etude des relations pour le suivi des trajets d'identité

L'impression numérique reconstruit les relations réseau afin de vous permettre d'identifier une entité qui attaque et les autres entités avec lesquelles elle communique.

L'outil d'impression numérique affiche la distribution de fréquences des événements corrélés. Il affiche les relations entre des entités et calcule le nombre d'occurrences d'une relation. Plus le nombre est élevé, plus la relation est forte. Par exemple, si vous visualisez les relations entre une adresse électronique et d'autres entités, vous pouvez voir qui communique avec qui. Vous pouvez visualiser les adresses IP qui sont associées à l'adresse électronique, les adresses IP visitées par le suspect, ainsi que les autres noms qui sont associés à l'adresse électronique.

Dans les déploiements répartis, vous pouvez choisir de voir les relations pour un noeud de votre organisation.

Procédure

1. Sélectionnez un résultat dans la liste de documents de la grille et cliquez sur l'onglet destiné à l'**impression numérique**.
2. Dans la liste, sélectionnez un élément que vous souhaitez explorer.

   Par défaut, le rapport de l'impression numérique qui en résulte est présenté sous forme de tableau, organisé par type d'identificateur. Tous les identificateurs qui ont interagi avec l'identificateur de centrage sont affichés. Les identificateurs de centrage sont organisés par type d'identificateur et sont triés par fréquence d'interaction.
3. Si vous voyez un identificateur d'intérêt, sélectionnez-le.

   Les identificateurs sont des hyperliens et vous pouvez les utiliser comme identificateur de centrage d'un autre rapport. Un autre onglet est créé et le nouvel identificateur de centrage est affiché. Vous pouvez voir avec qui un agresseur suspecté interagit et les interactions. Vous pouvez développer le rayon d'une investigation pour voir d'autres agresseurs et entités suspectés avec lesquelles ils interagissent.
4. Pour examiner un autre hôte, sélectionnez l'adresse IP dans la liste **Select Remote Host**.

Dans les installations réparties, vous pouvez choisir l'hôte QRadar Incident Forensics, puis afficher l'impression numérique. La vue par défaut est l'hôte principal, mais vous pouvez sélectionner un hôte secondaire qui est associé avec l'hôte QRadar Incident Forensics.

5. Pour voir une visualisation des associations et relations des interactions de l'identificateur de centrage avec d'autres identificateurs, cliquez sur l'onglet **Visualize Data**.

Outil Visualize

Vous pouvez explorer visuellement les associations et les relations au sein de plusieurs attributs et catégories de données.

La fenêtre Visualize vous permet de voir une carte des relations de métadonnées d'un ou deux documents, ou encore d'une vaste sélection de documents. Lorsque de nombreux documents sont sélectionnés, l'examinateur obtient une vue exhaustive des relations de métadonnées et de la fréquence relative. Les examinateurs peuvent alors suivre ces pistes pour approfondir leur examen d'un incident de sécurité.

La visualisation des documents sélectionnés peut être reconstruite facilement avec une autre relation en modifiant une relation ou les deux.

La visualisation affiche chaque relation contenue dans les documents sélectionnés, ainsi que des indices concernant la fréquence de la relation. Chaque noeud représente une portion distincte de métadonnées liées, provenant des documents sélectionnés. La taille représente la fréquence relative par rapport aux autres noeuds. Des liens montrent les connections entre les différentes portions de métadonnées et représentent la fréquence par un élément de taille. Les examinateurs peuvent utiliser les noeuds pour identifier les voies possibles à examiner de façon approfondie.

Visualisation des relations et des associations

La fenêtre Visualize vous permet de voir les relations entre les attributs au sein de documents restaurés. Par exemple, vous pouvez examiner les adresses e-mail qui ont communiqué avec une adresse e-mail spécifique.

Procédure

1. Dans la grille de reprise, cliquez sur les cases à cocher correspondant aux documents que vous voulez examiner et cliquez sur **Visualize**.
2. Sélectionnez la disposition, le nombre de documents à afficher, et les relations entre les attributs que vous souhaitez voir, puis cliquez sur Refresh.
3. Utilisez les commandes de zoom pour voir plus ou moins de détails de l'image.
4. Pour effectuer une nouvelle recherche ou modifier le filtre actif, cliquez avec le bouton droit sur un noeud.

   Dans ce menu contextuel, vous pouvez afficher cette portion de métadonnées afin d'effectuer une nouvelle recherche. Vous pouvez également modifier le filtre actif pour inclure ou exclure les métadonnées.

   Restriction : Vous pouvez afficher jusqu'à 9999 documents en même temps dans une fenêtre Visualize.

Analyse des artefacts pour rechercher un contenu suspect ou malveillant

En tant qu'analyste de la sécurité, vous pouvez rechercher des menaces qui ont échappé à la détection en analysant des artefacts reconstruits, tels que des fichiers et des images. Pour comprendre les liens entre les collaborateurs et les artefacts, vous pouvez également étudier les liens vers et à partir de ces fichiers et images.

Exemple - Utilisation de l'analyse d'artefact pour trouver la source d'une attaque (patient zéro)

John est un analyste de la sécurité chez Replay Industries. Plusieurs systèmes sont infectés en dépit de toutes les mesures de sécurité en place. Après qu'il a identifié et mis ces systèmes en quarantaine, John a besoin de savoir comment ces systèmes ont été infectés et si d'autres actifs sont également compromis.

Récupération des paquets à partir d'une adresse IP

A partir des adresses IP et de la période approximative concernées, John est en mesure d'utiliser QRadar Incident Forensics pour récupérer les données des paquets appropriés.

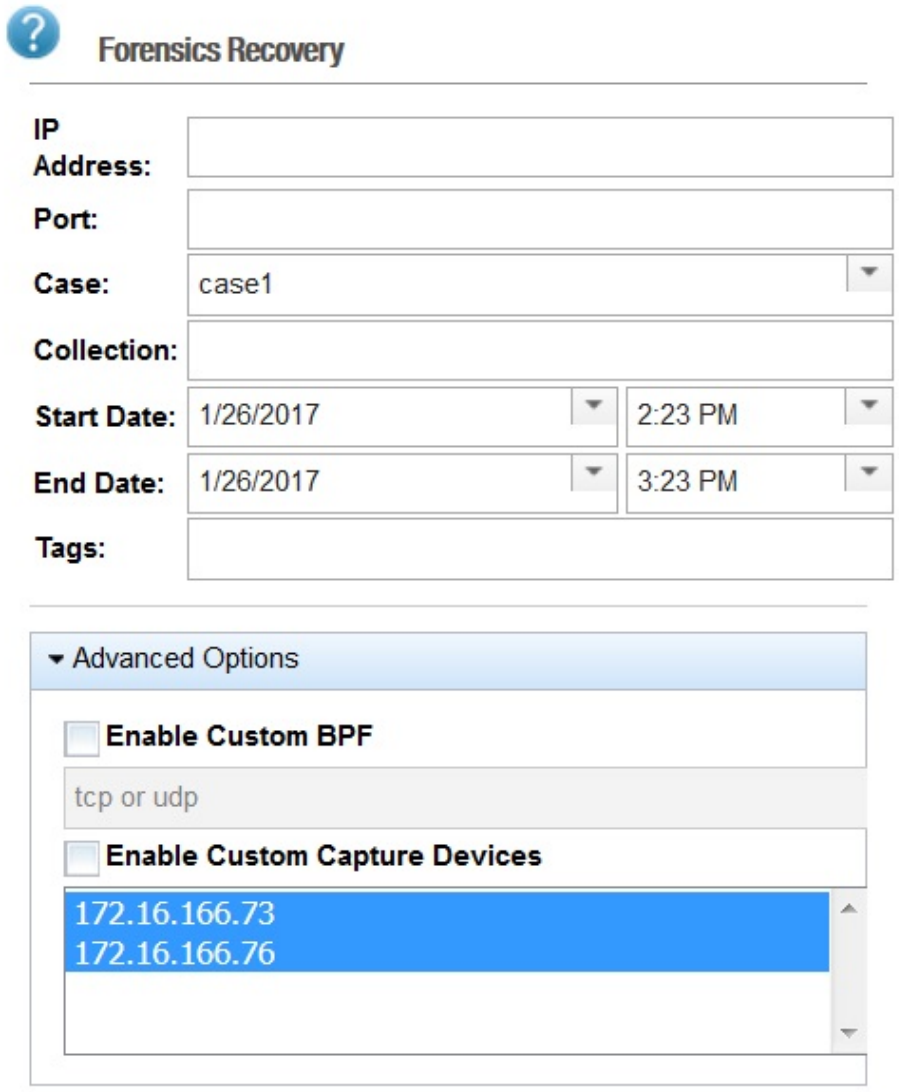


Figure 1. Récupération à partir d'une adresse IP

Analyse des fichiers

A la recherche de contenu exécutable, John commence par utiliser les fonctionnalités d'analyse des fichiers incluses dans QRadar Incident Forensics. Il peut maintenant consulter la liste de tous les fichiers, combien de fois ils ont été envoyés, s'ils contenaient des fichiers ou des scripts intégrés et leurs scores d'entropie. John détecte rapidement un fichier image que QRadar Incident Forensics a signalé comme à la fois un contenu suspect et comme contenant un script intégré.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

Figure 2. Attributs d'analyse des fichiers

L'*indice d'entropie de fichier* , qui mesure le caractère aléatoire des données et est utilisé pour trouver des logiciels malveillants chiffrés, et la répartition d'entropie montrent aussi clairement qu'une partie du fichier n'est pas ce qu'elle devrait être. Une analyse plus poussée révèle que ce fichier contient une nouvelle forme de code malveillant qui a échappé aux mesures de sécurité existantes et est responsable des systèmes infectés.

Dans le schéma ci-dessous, l'entropie est utilisée comme un indicateur de la variabilité de bits par octet. Étant donné que chaque caractère dans une unité de données est constitué de 1 octet, la valeur d'entropie indique la variation des caractères et la compressibilité de l'unité de données. Les variations dans les valeurs d'entropie du fichier pourraient indiquer que le contenu suspect est caché dans les fichiers. Par exemple, les valeurs d'entropie élevées peuvent révéler que les données sont stockées chiffrées et compressées, et les valeurs inférieures peuvent indiquer que, lors de l'exécution, le contenu est déchiffré et stocké dans différentes sections.

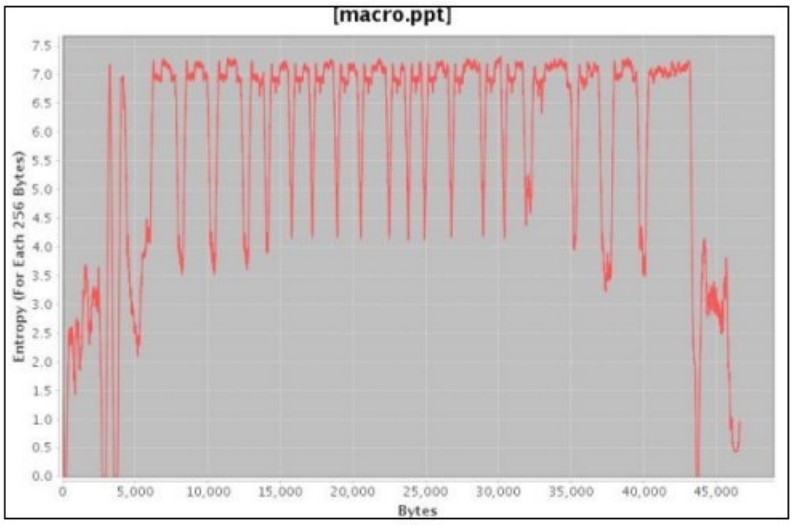


Figure 3. Exemple de graphique d'entropie de fichier qui montre des scripts intégrés

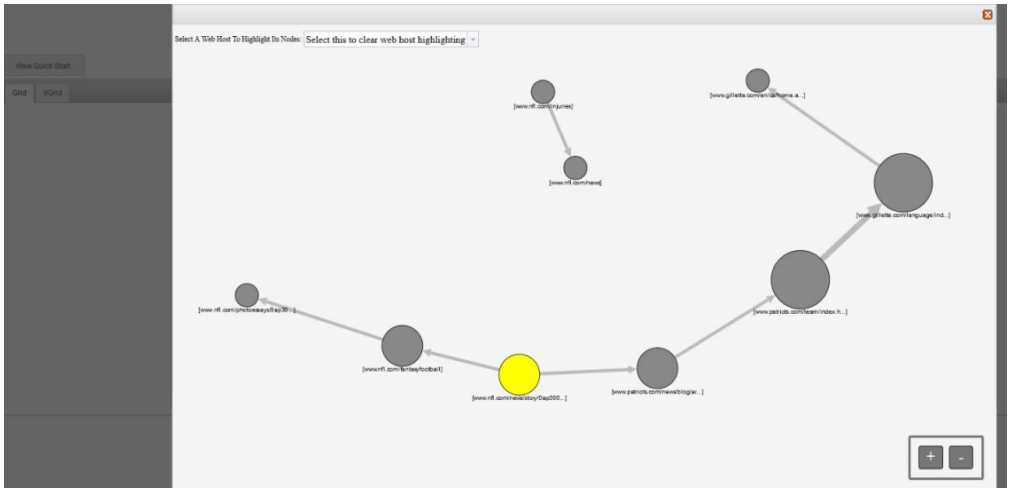
John doit maintenant comprendre d'où provient ce fichier et qui d'autre peut l'avoir. John utilise QRadar Incident Forensics pour trouver rapidement le serveur Web qui a fourni le fichier image infecté. La page Web en question est connue pour diffuser les dernières informations sur l'équipe NFL très populaire et elle est compromise. Même si le site Web contenait de nombreuses images, seule l'image trouvée par John à l'aide de l'analyse de fichier contenait le logiciel malveillant.

Analyse des liens pour visualiser la communication du site Web

Pour déterminer quels autres systèmes pourraient être touchés, John utilise l'analyse des liens afin de visualiser rapidement tous les sites qui ont été consultés. Malgré le trafic très important sur les sites Web des entreprises avec lesquelles Replay a travaillé, un petit sous-ensemble d'accès ressort clairement sur l'hôte du site Web infecté. John analyse ces liens pour voir quels autres serveurs sur son réseau ont été utilisés pour accéder à cet hôte Web.

Dans son enquête, John utilise les noeuds dans le graphique, qui représentent les pages Web et les flèches entre les noeuds qui représentent les relations ou les transactions entre les pages Web afin d'évaluer rapidement les modèles de trafic et

de voir comment les documents ont été consultés. Plus le noeud est grand, plus le nombre de liens est élevé dans le chemin du document. Plus la flèche de lien est grande, plus fréquemment le lien a été utilisé.



Étant un site d'informations NFL populaire, il n'est pas surprenant de constater qu'un certain nombre d'autres serveurs ont été en contact avec cet hébergeur et qu'ils ont pu être potentiellement affectés.

Analyse d'image

Pour réduire la liste des serveurs qui ont téléchargé le fichier image malveillant, John passe à l'analyse d'image et peut rapidement voir tous les fichiers image qui ont été envoyés ou reçus.

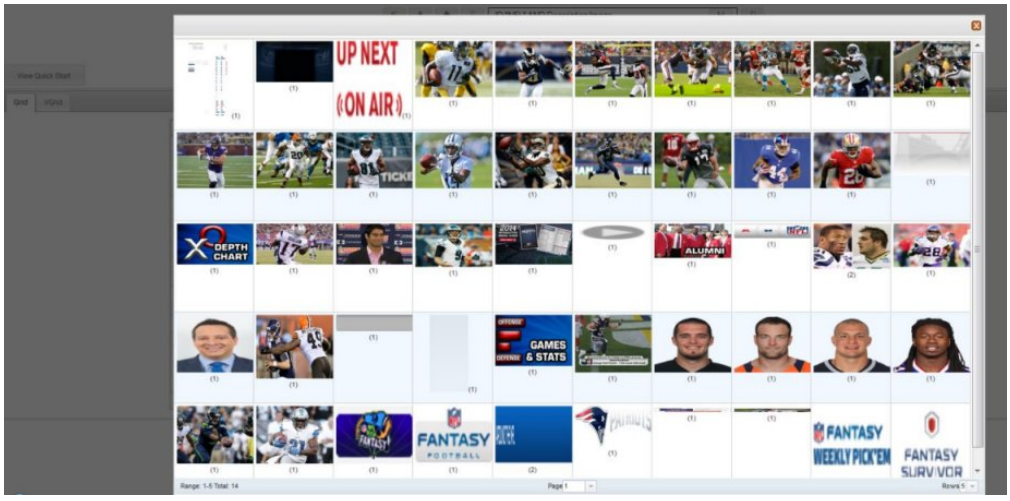


Figure 4. Exemple d'analyse d'image et de distribution d'image

John confirme rapidement que l'ensemble de ses serveurs infectés et 2 serveurs qu'il ignorait ont tous eu accès au fichier image compromis.

John détermine également que plusieurs des autres serveurs qui ont accédé au même site n'ont pas téléchargé le fichier infecté. John dispose maintenant des informations dont il a besoin pour mettre en quarantaine ces 2 serveurs supplémentaires et créer un nouvel hachage du fichier infecté que Replay

Industries peut télécharger et partager avec d'autres sur IBM X-Force Exchange.

Analyse de fichiers pour rechercher le contenu intégré et des activités malveillantes

Pour rechercher des menaces cachées dans des fichiers, vous pouvez consulter les valeurs d'entropie de fichiers, télécharger des fichiers et des scripts intégrés pour une analyse plus approfondie et afficher le document et ses attributs..

Parce que les intrus peuvent masquer le contenu de fichiers binaires dans des fichiers conteneurs, vous pouvez utiliser l'analyse de fichiers dans IBM Security QRadar Incident Forensics pour examiner si les fichiers contiennent des scripts intégrés ou tout autre contenu binaire.

L'*entropie de fichier* mesure le caractère aléatoire des données dans un fichier et est utilisée pour déterminer si un fichier contient des données masquées ou des scripts suspects. L'échelle du caractère aléatoire est comprise entre 0, non aléatoire, et 8, totalement aléatoire, par exemple un fichier chiffré. Plus une unité peut être compressée, plus la valeur d'entropie est faible ; moins une unité peut être compressée, plus la valeur d'entropie est élevée.

Dans le schéma ci-dessous, l'entropie est utilisée comme un indicateur de la variabilité de bits par octet. Étant donné que chaque caractère dans une unité de données est constitué de 1 octet, la valeur d'entropie indique la variation des caractères et la compressibilité de l'unité de données. Les variations dans les valeurs d'entropie du fichier pourraient indiquer que le contenu suspect est caché dans les fichiers. Par exemple, les valeurs d'entropie élevées peuvent révéler que les données sont stockées chiffrées et compressées, et les valeurs inférieures peuvent indiquer que, lors de l'exécution, le contenu est déchiffré et stocké dans différentes sections.

Procédure

1. Sous l'onglet **Forensics**, sélectionnez un ou plusieurs fichiers récupérés dans la vue **Grille**.
2. Dans le menu des outils d'investigation dans le haut de la grille, cliquez sur **Analyse de fichier**.

   Dans les résultats, chaque ligne de la grille contient des données d'analyse d'un document, par exemple, le nom du fichier, la description, si le contenu suspect est détecté et les valeurs d'entropie.
3. Pour trier les fichiers selon un attribut spécifique, comme l'entropie, cliquez sur le titre de la colonne associée.
4. Dans la liste des fichiers, cliquez avec le bouton droit de la souris sur un fichier pour un complément d'enquête
   - Pour examiner le document et ses attributs, cliquez sur **Afficher le document**.
   - Pour examiner un graphique d'entropie et vérifier si un fichier ou un script intégré peut contenir des logiciels malveillants, cliquez sur **Afficher l'entropie**.

     Vous pouvez utiliser des valeurs d'entropie pour savoir si le fichier peut contenir du code malveillant. Par exemple, les fichiers texte ASCII sont généralement très compressibles et ont de faibles valeurs d'entropie. Les données chiffrées ne sont normalement pas compressibles et ont généralement une valeur d'entropie élevée. Les logiciels malveillants sont souvent compressés et cachés dans des fichiers et des images.

- Pour télécharger des fichiers intégrés, cliquez sur **Extraire les fichiers imbriqués** et sélectionnez les fichiers à télécharger.

  Cette option est disponible uniquement pour les documents avec des fichiers ou des scripts intégrés. Les fichiers sont téléchargés à l'emplacement de téléchargement de votre navigateur Web. Veillez à ne pas ouvrir des scripts potentiellement nocifs dans un environnement non protégé.

Analyse d'images pour rechercher des menaces cachées ou une activité suspecte

Les images visualisées sont triées selon la taille et la pertinence avec un nombre de fréquences entre parenthèses. Cette analyse peut vous être utile quand un salarié utilise les ressources de l'entreprise pour regarder des images inappropriées, restreintes ou interdites. Par exemple, ces images peuvent liées à des avions, certains bâtiments ou des lieux qui sont des cibles pour les failles de sécurité.

Avec l'analyse d'image, vous pouvez afficher les images les plus pertinentes à partir d'un ou plusieurs documents dans un ou plusieurs fichiers de capture de paquets en un seul affichage, au lieu d'être obligé d'ouvrir chaque document et de visionner les images.

Procédure

1. Dans l'onglet **Forensics**, dans la vue **Grille**, sélectionnez un ou plusieurs documents qui contiennent l'image dans la description.
2. Dans le menu des outils d'investigation dans le haut de la grille, cliquez sur **Analyse d'image**.

   Dans les résultats, les versions en miniature de toutes les images qui sont contenues dans les documents sont affichées par ordre de pertinence. Le nombre entre parenthèses à côté de l'image indique le nombre d'instances de l'image dans le document. Si vous placez le curseur sur une image miniature, l'image s'agrandit.
3. Cliquez avec le bouton droit sur une image pour plus d'informations
   - Pour examiner l'image et ses attributs, cliquez sur **Afficher le document**.
   - Pour examiner un graphique d'entropie et vérifier si l'image peut contenir des logiciels malveillants, cliquez sur **Afficher l'entropie**.

     Vous pouvez utiliser des valeurs d'entropie pour savoir si le fichier peut contenir du code malveillant. Par exemple, les fichiers images bitmap et les fichiers texte ASCII sont généralement très compressibles et ont de faibles valeurs d'entropie. Les données chiffrées ne sont normalement pas compressibles et ont généralement une valeur d'entropie élevée. Les logiciels malveillants sont souvent compressés et cachés dans des fichiers et des images.

Analyse des liens pour rechercher les connexions et les relations

Dans l'analyse des liens, les liens montrent le point commun entre les sites Web qui ont été consultés. Pendant les enquêtes d'incident de sécurité, vous pouvez rapidement voir où il existe un chevauchement et comment les gens communiquent.

Par exemple, si vous pensez qu'un groupe d'agresseurs opère de concert mais que vous ne savez pas comment, vous pouvez examiner un ensemble de documents à

partir d'un certain nombre d'utilisateurs et utiliser l'analyse de liens pour afficher les pages Web communes. Vous pouvez ensuite enquêter sur des sites Web spécifiques.

Procédure

1. Sous l'onglet **Forensics**, sélectionnez une ou plusieurs pages Web dans la vue **Grille**.
2. Dans le menu des outils d'investigation dans le haut de la grille, cliquez sur **Analyse de lien**.

   S'il existe une relation entre des sites Web, un graphique Cytoscape montre les pages Web sous forme de cercles (nœuds) et les liens vers et depuis ces pages Web sous forme de flèches. Plus le noeud est grand, plus le nombre de liens est élevé dans le chemin du document. Plus la flèche de lien est grande, plus fréquemment le lien a été utilisé. Les noeuds sélectionnés sont en jaune.
3. Pour étudier la communication à partir d'un hôte Web spécifique, dans la liste**Select Web Host**, sélectionnez l'hôte Web.

   Les nœuds qui représentent les pages Web de l'hébergeur choisi sont mis en évidence sous forme de cercles gris foncé.
4. Pour agrandir ou réduire la taille des cercles (nœuds) et des flèches, utilisez les commandes d'agrandissement (+) ou de réduction (-).

   Vous pouvez également faire rouler vers le haut ou vers le bas la molette de la souris pour augmenter ou diminuer la taille des nœuds et des flèches.
5. Pour déplacer un ou plusieurs noeuds, cliquez et déplacez les nœuds.

   Vous pouvez déplacer le graphique entier en cliquant n'importe où dans l'arrière-plan, puis en maintenant et en déplaçant le curseur.

Reprise depuis une page de document Attributes

Lorsque vous visualisez l'onglet **Attributes** d'un document, vous pouvez exécuter une reprise sur une adresse IP ou un port.

Procédure

1. Depuis la page Search dans l'onglet **Forensics**, effectuez une recherche.
2. Cliquez sur un des documents dans la liste des documents retournés pour l'ouvrir.
3. Cliquez sur l'onglet **Attributes**.
4. Cliquez sur une adresse IP ou un port.
5. Dans le menu, cliquez sur **Run Recovery for**.

Chapitre 5. Examen du trafic réseau pour rechercher une adresse IP

Pour bénéficier de la visibilité du contenu pertinent dans les conversations qui ont eu lieu lors d'un incident de sécurité, vous pouvez restaurer et reconstruire le trafic réseau associé à une adresse IP. Vous pouvez également rechercher des cas existants qui sont liés à une adresse IP.

Lors de la reconstruction du trafic réseau à partir d'une adresse IP, un incident est créé. Les examinateurs peuvent visualiser une séquence d'événements provenant de l'incident de sécurité ou afficher les documents de l'incident.

IBM Security QRadar Incident Forensics indexe l'ensemble des données réseau, des données de fichier, des métadonnées et des caractères textuels disponibles qui se trouvent dans chaque fichier récupéré.

Dans les déploiements répartis, plusieurs unités et hôtes QRadar Incident Forensics capturent et traitent les données. Vous pouvez afficher les résultats de reprise après incident agrégés ou les résultats par hôte et unité de capture.

Procédure

1. Pour créer un cas et obtenir des données à partir de périphériques de capture de paquet, dans QRadar, cliquez avec le bouton droit de la souris sur une adresse IP puis sélectionnez **Exécuter la reprise Forensics** ou cliquez sur l'icône de reprise Forensics  .
   a. Définissez les paramètres de reprise Forensics à l'aide des informations ci-après.

Tableau 5. Paramètres de reprise Forensics

Paramètre	Description
IP Adress (Adresse IP)	Utilisez une commande pour séparer plusieurs adresses IP. Si aucune adresse ou aucun port n'est indiqué, la valeur TCP ou UDP par défaut est utilisée.
Port	Utilisez des virgules pour séparer plusieurs ports.
Case (Cas)	Le nom de cas doit être unique.
Collection	Les données restaurées sont regroupées dans une collection et associées au cas. Le nom de la collection doit être unique. Si le nom de la collection existe dans le cas, la collection initiale est supprimée.
Tags (Balises)	Facultatif. Utilisées pour rapidement extraire des ensembles de résultats précis de documents pertinents. Utilisez une virgule pour séparer plusieurs balises. Utilisez des caractères alphanumériques uniquement, les caractères spéciaux ne sont pas autorisés.
Enable Custom BPF (Berkeley Packet Filter) (Activation du filtre BPF)	Disponible pour les administrateurs. Cette case à cocher active une zone d'entrée BPF pour la saisie d'une adresse IP et d'un port.

Tableau 5. Paramètres de reprise Forensics (suite)

Paramètre	Description
Enable Custom Capture Devices (Activation des unités Capture personnalisées)	Disponible pour les administrateurs. Cette case à cocher permet de générer la liste des unités PCAP de votre déploiement. Sélectionnez celles de votre choix pour limiter l'affichage du trafic entrant à ces unités.

b. Cliquez sur **OK**, puis sur l'onglet Forensics.

   Traitement des incidents : Si un message indiquant que vous ne disposez pas des droits appropriés pour récupérer des données s'affiche, assurez-vous que votre profil de sécurité est autorisé à accéder à l'adresse IP. Dans certains cas, si vous avez utilisé un caractère # dans la zone **Balises**, il est possible que ce message s'affiche.

c. Cliquez sur l'icône Incidents  pour afficher vous incidents. Développez ou réduisez le contenu lors de la navigation dans la hiérarchie.

d. Pour afficher les documents de l'incident, cliquez sur l'option permettant d'afficher les **résultats de la recherche**.

e. Pour visualiser une séquence d'événements pour l'incident, cliquez sur l'option permettant d'afficher la **page de résultats Surveyor**.

f. Pour retirer ou annuler un incident particulier, cliquez sur **Supprimer ou Annuler cet incident**.

g. Pour réexécuter le travail de reprise Forensics précédent, cliquez sur l'option permettant de **réexécuter cette reprise Forensics**. Si, par exemple, les résultats renvoient des données incomplètes, vous réexécutez une reprise Forensics afin d'inclure des adresses IP différentes ou vous changez la période spécifiée dans l'exécution du travail de reprise précédent.

2. Pour rechercher des cas existants, dans QRadar, cliquez avec le bouton droit de la souris sur une adresse IP et cliquez sur **Exécuter la recherche Forensics**.

   a. Dans l'onglet **Forensics**, cliquez sur l'icône Incidents.

   b. Pour étudier un agrégat des activités qui sont associées à un incident, mettez en évidence un cas en le survolant avec votre souris, puis cliquez sur l'icône de recherche.

   c. Pour examiner des activités par hôte QRadar Incident Forensics et unité de capture dans les déploiements répartis, développez l'entrée **Cas** puis l'entrée **Collection**.

   d. Pour afficher une liste chronologique des interactions dans un incident, mettez en évidence la collection en la survolant avec la souris, puis cliquez sur l'icône de l'outil Surveyor.

Concepts associés:

«Vue des documents reconstruits», à la page 29
L'onglet **View** affiche une vue reconstruite du document sélectionné dans la partie gauche de l'écran, sans la vue List.

Filtre BPF personnalisé

Pour afficher uniquement certains types de trafic lorsque vous exécutez une reprise Forensics, vous pouvez choisir de créer un filtre BPF (Berkeley Packet Filter) personnalisé.

Dans Forensics Recovery, la sélection de la case à cocher active une zone de saisie BPF où vous indiquez un filtre BPF qui filtrera le trafic réseau.

Utilisez la syntaxe BPF pour indiquer des filtres BPF. Une expression se compose d'une ou de plusieurs primitives. Les primitives sont des références à une ou plusieurs zones d'un en-tête de protocole de réseau. Par exemple, host, port, tcp port constituent des primitives. Vous pouvez générer des expressions de filtrage complexes en utilisant les opérateurs AND, OR et NOT.

Exemples de filtre :

```
host 10.0.0.1
port 80
tcp port 80 and host 10.0.0.1
host 10.0.0.1 or host 10.0.0.2 or port 80 or port 443
```

Pour créer un filtre BPF personnalisé, vous devez avoir accès au rôle utilisateur Admin. Tous les utilisateurs non-administrateur ont un accès en lecture seule à la zone de texte BPF. Les administrateurs peuvent entrer une expression BPF.

Restriction : La reprise Forensics s'appliquera à l'entrée BPF fournie. Si les résultats de votre reprise ne sont pas ceux attendus, vérifiez votre entrée de reprise et votre filtre BPF afin de vous assurer que les critères sont corrects.

Même si elle n'est pas utilisée par le filtre BPF personnalisé, la zone BPF comporte toujours le contenu des zones **IP Address** ou **Port**. Si aucune adresse IP ou aucun port n'est indiqué(e), le filtre BPF personnalisé utilise par défaut les valeurs TCP ou UDP.

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.

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).

Glossaire

Ce glossaire contient les termes du logiciel et des produits IBM Security QRadar Incident Forensics et leur définition.

Les références croisées suivantes sont utilisées dans ce glossaire :

- *Voir* renvoie d'un terme peu utilisé au terme généralement utilisé ou d'une abréviation à la forme développée.
- *Voir aussi* renvoie à un terme connexe ou contraire.

Pour tout autre terme et définition, veuillez vous référer au site Web de terminologie IBM (ouvre une nouvelle fenêtre).

A

anomalie
Ecart par rapport au comportement attendu du réseau.

attaquant
Utilisateur (logiciel ou personne) qui tente d'endommager un système informatique ou d'accéder à des informations non destinées à un accès public. Voir aussi attaque.

attaque
Tentative, par une personne non autorisée, de compromettre l'opération d'un logiciel ou d'un système en réseau. Voir aussi attaquant.

C

carte des relations de métadonnées
Carte qui affiche des métadonnées connexes à partir de documents de cas.

cas
Informations contenues dans une base de données relative à une investigation spécifique.

catégorie
Ensemble d'éléments regroupés selon une description ou une classification spécifique. Les catégories peuvent représenter différents niveaux d'informations dans une dimension.

chiffrement
En sécurité informatique, processus consistant à transformer les données en un format non intelligible afin que les données originales ne puissent pas être obtenues ou puissent l'être uniquement à l'aide d'un processus de déchiffrement.

collection
Ensemble de données portant un nom spécifique et associé à un cas. Par exemple, un ensemble ordonné de paquets réseau capturés.

conversation
Flux de données entre au moins deux points d'extrémité de réseau qui est reconstruit de manière scientifique. Par exemple, une conversation de réseau social.

D

désemballage
Processus qui consiste à décompiler les données de capture de paquet de manière à produire un rapports de résultats à partir de toutes les données importées.

dispositif de capture de paquet
Dispositif autonome qui intercepte et journalise des données relatives au trafic.

E

élément de navigation
Elément d'interface Web qui affiche la position de l'utilisateur dans un site. Il s'agit généralement d'une suite d'hyperliens disposés horizontalement en haut ou en bas de la page. Ces liens indiquent les pages qui ont été consultées et permettent à l'utilisateur de remonter jusqu'au point de départ de la navigation.

enregistrement de flux
Enregistrement de la conversation entre deux hôtes.

examinateur Forensics
Utilisateur qui extrait des données pertinentes à partir du trafic réseau et les documente dans le référentiel Forensics.

H

hypothèse
Explication proposée pour un incident en fonction des preuves disponibles ayant été collectées pour un cas. Une hypothèse doit pouvoir faire l'objet d'un test et d'une falsification.

I

identificateur de centrage
Elément de catégorie avec lequel tous les autres identificateurs ont interagi. Il s'agit de l'élément central d'une investigation.

identité
Collection d'attributs provenant d'une source de données et représentant une personne, une organisation, un lieu ou un élément.

impression numérique
Rapport comportant des identificateurs marqués qui sont reliés les uns aux autres pour un cas spécifique.

incident
Voir incident lié à la sécurité.

incident lié à la sécurité
Evénement au cours duquel les opérations de réseau normales sont violées, compromises ou attaquées.

informations de capture de paquet
Données relatives au trafic qui sont collectées par un périphérique de capture.

infraction
Message envoyé ou événement généré en réponse à une condition surveillée. Par exemple, une infraction indiquera si une règle a été violée ou si le réseau se trouve en état d'attaque.

inspecteur de domaine
Inspecteur spécialisé conçu pour déconstruire et extraire les données criminalistiques provenant de sites Web de domaines spécifiques, tels que Facebook ou Gmail.

inspecteur de protocole
Inspecteur spécialisé conçu pour extraire les données criminalistiques provenant de protocoles de réseau, tels que HTTP ou FTP.

M

métadonnées
Données qui décrivent les caractéristiques des données (données descriptives).

O

opérateur booléen
Fonction intégrée qui indique une opération logique AND, OR ou NOT lorsque des ensembles d'opérations sont évaluées. Les opérateurs booléens sont : &&, || et !.

outil Surveyor
Outil qui affiche la séquence chronologique des activités dans un incident de sécurité dans un visualiseur.

P

périphérique de capture
Voir dispositif de capture de paquet.

présence électronique collectée en continu
Identité en ligne d'un attaquant sous la forme d'une collection d'impressions numériques reliées.

R

relation d'impression numérique
Relation entre des identificateurs marqués pour un cas spécifique.

S

super-flux
Flux unique composé de plusieurs flux aux propriétés similaires permettant d'améliorer la capacité de traitement en réduisant les contraintes de stockage.

T

trace Impressions numériques qui connectent les individus impliqués dans un cas à d'autres individus qui ne sont pas impliqués dans ce cas.

trafic Lors de la communication de données,

quantité de données transmises par un point particulier d'un chemin.

trafic réseau importé
Trafic réseau capturé qui a été traité par le processus de désemballage de Forensics.

travail de reprise
Processus qui consiste à récupérer les données de capture faisant l'objet d'une requête et à les transmettre à l'unité de désemballage pour importation.

V

vulnérabilité
Risque lié à la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

Index