IBM Security

IBM

IBM QRadar

Détectez les menaces récentes grâce à la plateforme d'analyse de la sécurité la plus sophistiquée du marché

Livre blanc IBM Security

Partir à la conquête de l'inconnu

Les professionnels de la sécurité vivent dans un monde d'incertitude constante. Leurs entreprises sont frappées de toutes parts, chaque jour, à chaque minute, par des menaces et des attaques. Lorsque des agresseurs persévérants réussissent à s'introduire dans les systèmes, ils se déplacent lentement et calmement. Ils recherchent les données critiques tout en brouillant les pistes. En fait, une récente étude a montré que le délai moyen d'identification d'une attaque était de 256 jours tandis que le temps moyen pour la circonscrire était de 82 jours.[1] Par conséquent, la vie dans un SOC (Security Operations Center) est stressante ; de nombreuses équipes ignorent ce qu'elles ignorent.

L'époque où les équipes de sécurité pouvaient simplement verrouiller le périmètre, interdire de nombreuses formes d'accès à Internet et lutter contre la dernière attaque est révolue. Aujourd'hui, les entreprises exigent une connectivité quasi permanente afin de maintenir l'activité tout en arrêtant simultanément les menaces avancées, en identifiant les fraudes et les malveillances internes, et en assurant une conformité continue. Les nouvelles exigences visent à analyser le maximum d'informations afin de détecter les activités menaçantes qui rôdent sous la surface – et à réagir plus rapidement. Les analystes du SOC doivent développer une très forte capacité à détecter les écarts par rapport aux activités normales, et les solutions qu'ils choisissent doivent pouvoir évoluer, en pénétrant dans chaque recoin de l'entreprise avec une plateforme unique et cohérente.

[1] « 2015 Cost of a Data Breach Study: Global Analysis, » *Ponemon Institute Research Report*, Mai 2015.

Détecter les menaces et agir

Pour rester en tête, les entreprises doivent pouvoir « détecter » les chaînes d'activités malveillantes de la même manière qu'une personne qui sent le danger lorsqu'elle voit, entend, sent ou ressent une situation inquiétante. Elles ont besoin d'une plateforme de sécurité capable :

- De se déployer rapidement sur un réseau entier, y compris les ressources Cloud.
- De détecter des différences minimes dans l'environnement, par exemple des intrus qui rôdent ou des membres malveillants de l'entreprise.
- De découvrir les attaques sans avoir à dépendre de spécialistes très compétents.
- De collecter, normaliser et corréler des milliards d'événements, hiérarchisés en fonction des types de problèmes.
- D'identifier les vulnérabilités importantes et les risques afin d'éviter toute violation.

Le côté positif de la situation est que les analystes de SOC actuels ne sont plus seuls. A l'instar des agresseurs, ils mettent en commun leurs connaissances et expertises. L'émergence de ces nouvelles infrastructures de partage d'applications et de renseignements sur les menaces permet de limiter l'efficacité des nouveaux logiciels malveillants et kits d'exploitation de vulnérabilités (exploit kits), ainsi que l'impact des vulnérabilités zero-day ou one-day. Toutefois, de nombreux analystes de SOC sont encore limités par des systèmes de gestion des logs vieillissants ou des solutions basiques de gestion des événements et des informations de sécurité (SIEM) qui génèrent des alertes excessives en raison de la présence d'une seule instance de comportement suspicieux.

Eliminer les menaces grâce à l'analyse

Les violations de sécurité les plus graves ne commencent pas avec un big bang. En effet, les cybercriminels lancent des attaques « faibles et lentes » qui peuvent persister pendant des mois. Ne serait-il pas fantastique que vous puissiez identifier des changements subtils et associés dans l'environnement, puis alerter les équipes de sécurité lorsque des choses étranges surviennent ?

QRadar peut « détecter » les chaînes d'événements malveillants, en identifiant des signaux clairs dans le bruit.

IBM QRadar Security Intelligence Platform est la seule solution de sécurité basée sur IBM Sense Analytics capable :

- De développer des profils d'utilisateurs et d'actifs pour des activités légitimes de référence.
- De détecter des comportements anormaux chez les individus (y compris les employés de l'entreprise, les partenaires, les clients et les invités) ainsi que dans les réseaux, les applications et les données.
- De relier les activités suspicieuses actuelles et historiques, ce qui renforce la précision des incidents identifiés.
- De récupérer et de ré-éxécuter une activité sur le réseau et d'enquêter sur le contenu du paquet dans sa forme d'origine.
- De trouver et de prioriser les faiblesses avant qu'elles ne soient exploitées.

Les produits qui font des analyses ponctuelles ne sont pas fiables ; ils ne peuvent pas associer une nouvelle activité du réseau aux utilisateurs « à risque », par exemple ceux qu'on connaît pour s'être déjà rendus sur des sites Internet ayant mauvaise réputation. Sense Analytics permet d'éliminer les menaces en corrélant le comportement des utilisateurs avec les événements dans les logs, les flux réseau, les renseignements sur les menaces, les vulnérabilités et le contexte métier. Il permet aux entreprises de se concentrer sur les menaces les plus dangereuses et les plus immédiates qui les concernent en identifiant des signaux clairs dans le « bruit » – et les guide dans les efforts de remédiation afin de minimiser tout dommage potentiel.

Comment fonctionne Sense Analytics ?

Sans données, l'analyse est inutile, et sans un grand nombre de données, elle est tout simplement faible. Une partie de ces données viennent du fonctionnement de votre réseau, certaines sont stockées dans des applications, d'autres sont dérivées d'analyses précédentes, et d'autres proviennent en flux d'une source externe. QRadar collecte les données de sécurité brutes à partir de tout appareil, application ou utilisateur au sein du réseau – qu'il se trouve sur le site de l'entreprise ou qu'il soit hébergé dans un environnement Cloud.

Sense Analytics peut :

- **Analyser les données de sécurité**
- **Comprendre le contexte**
- **Faire le profil des utilisations**

Une fois que les données sont collectées, les appliances QRadar effectuent des analyses en temps réel à la recherche de signaux immédiats de danger, puis mêle les résultats à d'autres renseignements stockés relatifs aux réseaux, aux utilisateurs ou aux métadonnées de fichier concernés. QRadar permet aux équipes de sécurité de comprendre les liens entre les activités en cours et les faits qui se sont déroulés dans le passé. Un élément clé pour détecter le changement est d'avoir les bons paramètres pour l'activité de référence.

Analyser les données de sécurité pour détecter les menaces

Basé sur Sense Analytics, QRadar utilise l'analyse avancée basée sur l'état pour transformer les données de sécurité en cours en informations pertinentes. Les équipes de sécurité peuvent définir différentes conditions pour détecter plus facilement les activités à risque, y compris :

Avec QRadar, une entreprise énergétique internationale peut analyser deux milliards d'événements par jour – corrélant des données en temps réel – pour identifier les 20 à 25 infractions potentielles qui présentent le risque le plus élevé.

- Des changements dans les comportements pour repérer les écarts par rapport aux activités normales.
- Des anomalies qui peuvent révéler un nouveau trafic réseau ou un trafic qui cesse brutalement.
- Des violations de seuil pour trouver les occurrences d'une activité qui dépassent un niveau défini.

Un changement dans le comportement habituel des utilisateurs ou un changement des identités est souvent l'un des premiers signes d'une violation du réseau et, éventuellement, que les données d'identification d'une personne ont été mises en danger. Sense Analytics compare non seulement l'activité en temps réel à des modèles historiques mais détecte également une nouvelle utilisation des applications, de nouvelles visites de sites Internet et de nouvelles activités de transfert de fichiers. Il peut également exclure les faux positifs en extrayant les données des systèmes d'identité organisationnels, permettant aux analystes du SOC de voir un récent reporting ou un changement de fonctions d'une personne donnée.

Comprendre le contexte en analysant des événements, des flux, des paquets

Une source de contexte performante mais souvent négligée peut être dérivée de données de flux de réseau natives – les données qui identifient les adresses IP, les ports, les protocoles, et même les applications ou le contenu « payload » traversant le réseau – tout cela capturé via des inspections immédiates et en profondeur des paquets ou la récupération post-incident des paquets entiers. Cela permet aux équipes de sécurité de :

- Faire le profil du trafic réseau « normal » et d'obtenir des alertes quand les conditions changent.
- Trouver de nouveaux hôtes ou des hôtes à risque communiquant avec des IP malveillantes.
- Détecter de nouvelles menaces de sécurité sans utiliser les signatures.
- Répéter les actions pas à pas d'un intrus détecté ou d'un utilisateur malveillant.
- Obtenir de la visibilité dans la couche d'application et de détecter du contenu suspicieux ou une utilisation inappropriée.

Sense Analytics utilise les données réseau pour fournir un contexte à chaque événement, incident ou infraction corrélée Il peut détecter si un serveur web arrête de répondre aux communications, identifier un changement significatif dans le niveau d'activités des services communément utilisés, et générer des alertes lorsque de nouveaux services ou protocoles apparaissent sur le réseau. Cette analyse révèle aussi les types d'application et identifie les non-concordances de port et de protocole – ce qui peut accélérer les investigations.

Faire le profil des utilisations pour stocker les renseignements et gérer le risque

Une solution de sécurité conçue pour rechercher rapidement dans les données, en temps réel, va passer à côté d'un grand nombre d'incidents, qui exige des connaissances antérieures des applications clés, des personnes qui les utilisent, de leur niveau de performance type, de leurs hôtes associés et des périodes d'activité intense ou faible. Connaître ces paramètres est crucial pour exploiter les renseignements.

La capacité à stocker des connaissances en faisant le profil des actifs et des individus est une caractéristique fondamentale de Sense Analytics. QRadar identifie automatiquement les actifs et crée des profils d'actifs, en utilisant les données de flux de réseau et les analyses de vulnérabilités. Les profils définissent ce qu'est un actif, identifient comment il communique avec les autres actifs, liste les applications autorisées et avertit de la présence des vulnérabilités connues. QRadar utilise ensuite tout ce contexte pour réduire le bruit et fournir des incidents de façon ultra-précise.

Développer des connaissances sur ce que font les utilisateurs du réseau est tout aussi important pour la détection d'attaque et de violation. QRadar peut tracer les adresses IP et MAC, les ID d'e-mails et les pseudos de « Chat », par exemple. Il peut exploiter d'autres programmes de gestion des accès et des identités d'IBM ou de tiers afin de fournir un contexte utile pour les investigations d'incidents. Il peut utiliser toutes ces associations pour qualifier le périmètre de son analyse, et inclure ou exclure les individus ou archétypes associés à l'activité suspecte – en cours ou observée récemment.

Explorer les cas d'utilisation qui démontrent la puissance de Sense Analytics

Dans de nombreux environnements, la complaisance et les défaillances au niveau des pratiques de sécurité signifient que les actifs critiques ne sont pas nécessairement aussi sécurisés qu'ils le pourraient ou qu'ils devraient l'être. Les entreprises doivent limiter l'impact d'une violation inévitable. Elles ont besoin de solutions qui couvrent l'environnement complet sans « angles morts ».

Dès qu'il est installé, QRadar commence à créer une veille sécuritaire exploitable qui peut renforcer les défenses d'une entreprise. Les cas d'utilisation pour lesquels la solution offre une efficacité rapide sont les suivants :

- Détection de menaces avancées
- Protection des données critiques
- Surveillance des menaces internes
- Gestion des risques et des vulnérabilités
- Détection du trafic non autorisé
- Investigation d'expert

Cas d'utilisation :

Détection de menaces avancées

Grâce à l'analyse en temps réel, les équipes de sécurité peuvent détecter si un hôte se rend sur un domaine potentiellement malveillant, mais une alerte n'est pas forcément nécessaire pour une simple visite. Toutefois, si ce même hôte commence à faire preuve d'un comportement suspicieux de type beaconing – détecté par une analyse de l'historique sur du long terme – et qu'il se met en outre à transférer anormalement des volumes de données élevés s'écartant des comportements de référence, la combinaison des trois conditions permet à QRadar de générer une alerte élevée unique.

QRadar peut également détecter un changement soudain du trafic réseau, comme l'apparition d'une nouvelle application sur un hôte ou la fin d'un service type, en le détectant comme une situation anormale. Les anomalies ne sont pas facilement repérées par les équipes de sécurité car elles font des recherches dans les logs systèmes – contrairement aux signatures de logiciels malveillants ou d'autres attaques définies contre des vulnérabilités connues. Par définition, une anomalie est une bizarrerie, et peut être uniquement découverte par un outil de sécurité qui contrôle les actions de tous les utilisateurs et toutes les entités et en fait le profil.

Cas d'utilisation :

Protection des données critiques

Du jour au lendemain, une nouvelle application commence à s'exécuter sur un hôte réseau. Cette activité peut faire suite à une nouvelle exigence métier ou à l'installation d'une application de discussion en ligne. Mais si cet hôte a accès aux données critiques, et qu'une vulnérabilité réseau connue lui est associée, QRadar peut créer une alerte de haut niveau de priorité pour inciter les équipes de sécurité à enquêter sur l'incident.

QRadar détecte rapidement si le trafic d'événements dépasse un niveau d'activité spécifique et génère une alerte. Le seuil ou la limite peut être basé sur n'importe quelle donnée collectée dans QRadar, par exemple les configurations des appareils réseau, les serveurs, la télémétrie du trafic réseau, les applications et les utilisateurs finaux et leurs activités. Et comme un changement de comportement ou une anomalie, QRadar peut enrichir l'alerte avec le contexte des identités utilisateur, des ports et des protocoles en cours d'utilisation, des réputations IP et des activités de menace rapportées afin de fournir aux équipes de sécurité une perspective approfondie de l'incident.

Cas d'utilisation :

Surveillance des menaces internes

Le représentant d'un service client se met soudain à télécharger le double de la quantité normale de données depuis un système d'information client, ce qui peut être dû à une nouvelle activité d'analyse des ventes. Mais si QRadar sait que le représentant s'est récemment rendu sur un site web potentiellement suspect, et qu'il voit maintenant que de faibles quantités de données sont envoyées vers un site d'un concurrent, le personnel de sécurité peut être informé avant qu'un gros volume d'informations ne fuit.

Sa capacité à faire le profil des entités et des individus permet à QRadar de se démarquer des autres produits de sécurité. L'association d'un ensemble de données exhaustif, du contexte métier et de renseignements sur les menaces – couplée à la capacité de détecter les écarts par rapport au comportement normal ainsi que de détecter les comportements autorisés et non autorisés – constitue une fonctionnalité de détection des incidents extrêmement performante.

Cas d'utilisation :

Gestion des risques et des vulnérabilités

Dès qu'une nouvelle entité fait son apparition sur le réseau, QRadar détecte automatiquement son existence grâce à un profilage passif des logs et des données de flux. Grâce à son analyseur de vulnérabilités parfaitement intégré, QRadar peut déclencher l'analyse de cette nouvelle entité afin de découvrir si elle présente des vulnérabilités urgentes ou à risque élevé exposées à des sources de menace potentielles.

Par exemple, si un nouveau serveur est ajouté au réseau, QRadar peut détecter s'il lui manque des correctifs critiques ou s'il a des données d'identification administratives par défaut. QRadar peut alors demander à l'équipe concernée de résoudre le problème et/ou de programmer un correctif, puis faire remonter le problème si cette tâche n'a pas été réalisée dans les temps.

De plus, les divulgations de nouvelles vulnérabilités sont automatiquement corrélées aux données existantes sans nécessité de nouvelle analyse, ce qui améliore la rapidité et la précision de la détection. Les économies opérationnelles résultantes permettent également aux analystes de sécurité de consacrer plus de temps aux tactiques proactives, comme les activités d'analyse du risque et de correction des vulnérabilités.

Cas d'utilisation :

Détection du trafic non autorisé

La plupart des entreprises prenant à présent en charge des terminaux BYOD (bring-your-own-device), les équipes de sécurité voient de plus en plus de trafics réseau associés à des applications de réseaux sociaux. Les utilisateurs consultent souvent leurs systèmes de messagerie d'entreprise et restent connectés avec leurs contacts via Facebook, LinkedIn, Twitter et autres services – avec un appareil unique. QRadar collecte et analyse ces données, et note quand, par exemple, les sessions de discussion en ligne commencent à se connecter via le port 80, le port normalement réservé au trafic HTTP. D'autres connexions avec des serveurs de réseaux de zombies connus vérifient rapidement l'injection de logiciels malveillants et invitent l'équipe de sécurité à agir.

QRadar collecte et analyse les données depuis des appareils mobiles et BYOD depuis la couche réseau et les systèmes de gestion des terminaux. Il peut détecter des menaces potentiels – par exemple un appareil débridé, des applications suspectes installées sur un appareil ou des communications Internet potentiellement malveillantes – puis déclencher la mise en quarantaine de l'appareil et/ou la remontée à l'équipe de sécurité concernée afin qu'elle agisse.

Cas d'utilisation :

Enquête d'expert et investigation sur les menaces

Durant une enquête sur une infraction, un analyste de sécurité découvre qu'un ou plusieurs employés ont été victimes d'une arnaque par hameçonnage et que l'agresseur s'est fixé quelque part et qu'il s'est étendu à un serveur hôte interne. Le modèle correspond à un modèle identifié par X-Force et est connu pour injecter un logiciel RAT (remote-access Trojan), qui est difficile à détecter.

En quelques clics de souris, QRadar récupère tous les paquets réseau associés à l'incident et reconstruit les mouvements pas à pas, indiquant à l'analyste de sécurité exactement où et quand le logiciel RAT a été installé. Le workflow expert permet à l'analyste de créer rapidement et facilement un profil détaillé du logiciel malveillant et d'associer les voies d'infection via une analyse du lien afin d'identifier le « patient zéro » et toute autre partie infectée. En conséquence, l'équipe de sécurité peut facilement réparer le dommage et minimiser les récurrences.

IBM offre des renseignements exploitables sur une infraction active et une défense plus forte

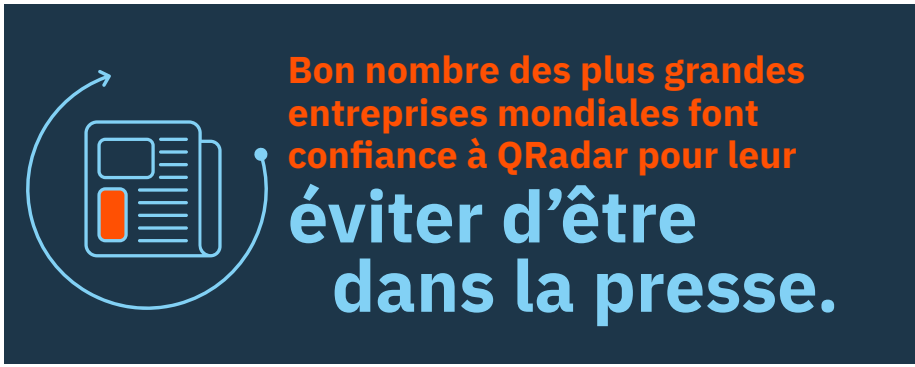
La sécurité des informations est une priorité de la direction, mais de nombreuses entreprises dépendent de dizaines de produits pour des éclairages ponctuels. Le personnel très compétent utilise des moteurs de recherche pour éplucher des montagnes de données, mais de plus en plus souvent, les agresseurs évitent la détection en commutant les IP, les protocoles, les ports et les applications pour s'accrocher, s'étendre et réunir les données importantes en cas de violation réussie.

IBM QRadar est différent. Il se déploie rapidement indépendamment de l'ampleur du réseau et commence à donner des résultats en quelques heures. Ses capacités de type cognitif et ses renseignements stockés peuvent associer les attaques liées émanant de la même source ou correspondant aux mêmes données cibles. QRadar délivre ces renseignements exploitables afin de répondre aux besoins en cours et futurs – de la détection des menaces avancées à la surveillance des menaces internes en passant par la détection de fraudes, à la gestion des risques et des vulnérabilités, aux enquêtes d'expert et au reporting de conformité.

Les principales raisons qui incitent les leaders de la sécurité à choisir QRadar sont :

- Un tableau de bord de sécurité simple à utiliser qui met en lumière les menaces les plus importantes et qui prend en charge une investigation rapide et efficace et un workflow de résolution.
- Une évolutivité quasi-illimitée, soutenue par les renseignements sur les menaces de X-Force et la puissance collaborative d'IBM X-Force Exchange.
- L'IBM Security App Exchange, avec des applications (applis) IBM ou développées par des partenaires qui étendent les capacités de QRadar sans complexité supplémentaire.
- La plateforme unique intégrée avec visibilité globale, donnant des éclairages sur l'activité du réseau, des applications et des utilisateurs.

Mettre en lumière les menaces les plus importantes



Une fois la menace, l'attaque ou la violation détectée, il est temps de passer à l'action. QRadar offre aux équipes de sécurité une interface utilisateur web qui a le même aspect sur l'ensemble de la plateforme. Passer d'une tâche à l'autre – surveiller l'activité des logs, observer l'activité du réseau, examiner les infractions étroitement liées, exécuter des analyses des risques et des vulnérabilités ou encore effectuer une analyse d'expert – est aussi simple que de cliquer sur un onglet pour afficher un tableau de bord rempli d'informations. Chaque tableau de bord contient de nombreuses informations de veille sécuritaire, organisées en affichages extrêmement visuels de l'activité récente et facilement examinée en quelques clics.

Passez quelques minutes à regarder les projections ou à examiner en détails une infraction rapportée. Les équipes de sécurité peuvent rapidement comprendre la nature du problème mis en lumière ; les vulnérabilités exploitées ; l'injection d'un réseau de zombies, d'un RAT ou d'autres programmes malveillants ; et l'étendue des données perdues. Il est à présent temps d'agir avant qu'un réel dommage ne survienne.

Bénéficiez du pouvoir d'agir – à grande échelle

Grâce à la plus grande plateforme QRadar, les équipes de sécurité peuvent clairement comprendre ce qui s'est passé et les conséquences si elles n'agissent pas rapidement. Les capacités clés comme la surveillance des menaces, la gestion des risques et des vulnérabilités et le reporting de la conformité sont typiquement à un clic et peuvent se passer les données pertinentes entre elles. En outre, QRadar inclut l'intégration avec les renseignements sur les menaces émanant de X-Force pour des mises à jour horaires sur les techniques d'attaques globales et les souches de logiciels malveillants.

En cas de violation, la technologie experte intégrée QRadar met à disposition des analystes du SOC des paquets de données pour une infraction associée, détaillant extrêmement clairement les actions pas-à-pas des agresseurs. Déjouer certaines menaces nécessite simplement de bloquer les communications avec une adresse IP externe, mais pour d'autres, il est nécessaire de mobiliser les équipes de réponse d'urgence pour isoler et reconfigurer les hôtes, désactiver les logiciels malveillants et corriger les vulnérabilités. Mais que se passe-t-il si votre équipe ne sait pas exactement ce qu'il faut faire ? Il faut alors demander de l'aide, collaborer avec ses pairs, trouver une solution voire embaucher une équipe de services professionnelle.

L'infrastructure ouverte QRadar – et l'IBM Security App Exchange – facilitent les intégrations étroites avec des solutions IBM et tierces. Par exemple, l'une des applis du site passe les données d'infraction QRadar à la plateforme Incident Response Platform de Resilient Systems pour action immédiate. Une autre appli offre une capacité de partage des données similaire avec la solution de gestion des terminaux Carbon Black Enterprise Response.

Etendre les capacités avec l'IBM Security App Exchange

L' IBM Security App Exchange étend la flexibilité de QRadar de manière exponentielle. Ce site de collaboration de premier plan permet aux clients, développeurs et partenaires commerciaux de partager des applis, des extensions d'applis de sécurité et des améliorations apportées aux produits IBM Security.

Grâce à l'IBM Security App Exchange, les entreprises peuvent :

- Bénéficier d'applis qui étendent les capacités des solutions IBM Security.
- Partager les meilleures pratiques et apprendre des autres.
- Trouver des solutions et des cas d'utilisation qui renforcent la valeur stratégique des opérations de sécurité.

L'ensemble du code est revu par IBM par rapport aux critères définis avant qu'il n'apparaisse sur le site. Et les équipes de sécurité peuvent télécharger et installer les solutions indépendamment – en dehors des cycles de publication des éditions officielles des produits. Elles peuvent ainsi appliquer de nouveaux cas d'utilisation de sécurité sans avoir à ajouter une complexité inutile des solutions.

Les utilisateurs QRadar peuvent notamment télécharger du contenu sur les différents secteurs, menaces, appareils et fournisseurs depuis l'IBM Security App Exchange. En outre, ils peuvent accéder à des rapports personnalisés, des tableaux de bord, des analyses spécialisées et des informations sur les menaces.

Déployez une plateforme unique avec une visibilité globale

Les environnements de sécurité actuels sont hyper complexes – souvent, les données de sécurité sont distribuées entre plusieurs solutions de différents fournisseurs, toutes avec des interfaces et des formats de stockage des données différents. Pour détecter efficacement les menaces existantes et émergentes, les équipes de sécurité ont besoin d'une vue consolidée de ces données, combinée à des capacités d'analyse de détection des menaces et de réponse complètes. QRadar utilise une seule base de données fédérée pour toutes les données de sécurité qui sont spécifiquement conçues pour une collecte évolutive depuis des systèmes sur site et dans le Cloud, le stockage, le reporting et des performances de recherche d'investigation très rapides. En outre, QRadar est optimisé pour une analyse des incidents en temps réel ou de l'historique, détectant les incidents quelques secondes après leur apparition – et non des heures, des jours ou des semaines après.

QRadar offre également un ensemble hautement intégré de cas d'utilisation liés à la sécurité, avec des cas supplémentaires disponibles via l'IBM Security App Exchange. Les équipes de sécurité peuvent utiliser une console unique, basée sur un tableau de bord pour toutes les fonctions, y compris la surveillance de la sécurité en temps réel ; la gestion proactive des risques et des vulnérabilités ; et la détection, l'analyse et la résolution des incidents. Ce hub unique pour les opérations et les réponses de sécurité mêle les renseignements des produits IBM et tiers – soutenu par une interface utilisateur et un workflow cohérents – afin d'améliorer l'efficacité de votre équipe d'opérations de sécurité.

Pour plus d'informations

Pour en savoir plus sur IBM QRadar Security Intelligence Platform basée sur Sense Analytics, veuillez contacter votre représentant ou partenaire commercial IBM, ou rendez-vous sur le site : **ibm.com**/security

A propos d'IBM Security

IBM Security possède un des portefeuilles d'offres les plus avancés et les plus intégrés en termes de produits et de services de sécurité destinés aux entreprises. Soutenu par l'entité de recherche et développement de renommée mondiale X-Force, le portefeuille d'offres IBM Security fournit une veille sécuritaire qui aide les organisations à protéger de manière globale leur personnel, leurs infrastructures, leurs données et leurs applications. Il offre pour cela des solutions de gestion des identités et des accès, de sécurisation des bases de données et des développements d'applications, des solutions de gestion des risques, de gestion des terminaux, de sécurité réseau, etc. Ces solutions permettent aux organisations de gérer efficacement les risques et de mettre en place une sécurité intégrée pour les appareils mobiles, le cloud, les médias sociaux et d'autres architectures d'entreprise. Dans le domaine de la sécurité, IBM dirige l'une des plus importantes organisations de recherche, de développement et de mise en œuvre au monde, surveille chaque jour 15 milliards d'événements dans plus de 130 pays et détient plus de 3000 brevets.

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

L'adresse de la page d'accueil IBM est :
ibm.com

WGW03211-FRFR-00