Optimisation de l'intelligence sécuritaire

Utilisation des fonctions d'analyse Big Data pour améliorer la sécurité d'entreprise

Points clés

- Intégration des fonctions d'intelligence sécuritaire et d'analyses Big Data
- Diminution des risques, détection des fraudes et surveillance en temps réel de la cyber-sécurité.
- Utilisation d'un grand volume et d'une grande variété de données pour améliorer la sécurité d'entreprise
- Action sur les données en mouvement pour éviter les éventuelles attaques
- Lutte contre les menaces de plus en plus sophistiquées (menaces avancées persistantes, hacktivisme, cyber-attaques, dangers physiques et menaces internes).

Le Big Data a été l'événement majeur de ces dernières années. Les entreprises, après s'être consacrées à l'exploration et à l'expérimentation, commencent désormais à s'intéresser à l'utilisation des technologies Big Data pour résoudre les problèmes qu'elles rencontrent. Grâce à l'intégration de fonctions d'analyse Big Data aux solutions existantes de gestion de la sécurité de l'information, les entreprises peuvent préserver leur sécurité, anticiper de nouvelles attaques et agir avant qu'il ne soit trop tard.

Cinq utilisations des données Big Data à forte valeur ajoutée

IBM a mené des études, examiné les recherches d'analystes du secteur, et échangé ses points de vue avec plus de 300 clients et prospects. Dans ce contexte, l'entreprise a mis en œuvre des centaines de solutions Big Data. Cela a permis d'identifier les cinq utilisations à forte valeur ajoutée qui peuvent constituer les premières étapes de mise en œuvre d'un projet Big Data :

1. **Exploration Big Data :** recherche, visualisation et compréhension du Big Data pour l'optimisation des prises de décisions
2. **Vue optimisée à 360° du client :** amélioration de la compréhension du client, grâce à l'incorporation de sources d'informations internes et externes
3. **Extension des fonctions de sécurité/d'intelligence :** Diminution des risques, détection des fraudes et surveillance en temps réel de la cyber-sécurité
4. **Analyse des opérations :** Analyse d'un grand nombre de données machine, afin d'optimiser les résultats de l'entreprise et l'efficacité opérationnelle
5. **Accroissement des capacités d'entreposage de données :** intégration des capacités des entrepôts de données traditionnels et Big Data, afin d'acquérir de nouvelles perspectives tout en optimisant l'infrastructure d'entreposage existante

Elles ne doivent pas obligatoirement être séquentielles ou classées par ordre de priorité. Peu importe comment débutent les utilisateurs, l'important est qu'ils réussissent leurs premier pas. La solution consiste à identifier les cas d'utilisation les plus importants pour l'entreprise, compte tenu des défis qu'elle doit relever.

Ce livre blanc traite spécifiquement du perfectionnement de l'intelligence sécuritaire en entreprise.

Le besoin accru de sécurité

Les problèmes de sécurité n'ont jamais été aussi présents chez les chefs d'entreprise, des consommateurs et des gouvernements. La prolifération des données numériques a une incidence sur tous les aspects de notre vie, et change radicalement notre façon de penser sur la sécurité, tant dans le monde virtuel que dans le monde physique.

Par exemple, au cours du plus grand vol de banque de l'histoire, des pirates ont dérobé 45 millions de dollars sans même entrer dans une banque, utiliser le chantage ou la force physique. Les armes utilisées étaient un réseau Web complexe et un grand savoir-faire sur la Toile. Il a fallu l'intervention d'officiers de police de 17 pays pour parvenir à l'arrestation de sept personnes.

Une récente étude a révélé que les réseaux sociaux figuraient parmi les mécanismes les plus souvent utilisés pour l'accès aux Ministères de la Défense de gouvernements puissants. Pendant son discours sur l'état de l'Union de 2013, le Président Obama a d'ailleurs cité la cyber-sécurité comme faisant partie des priorités absolues pour les Etats-Unis.

Sur 40 % de sites Web, des règles de réinitialisation de mots de passe trop faibles permettent aux pirates de pénétrer sur le site en utilisant des programmes simples et automatisés, exécutés via des combinaisons de cinq lettres/chiffres[4].

L'ère numérique a également eu des conséquences sur la protection des biens physiques (propriétés, bâtiments et personnes). Les autorités de police doivent pouvoir répondre aux menaces grâce à l'utilisation d'informations actualisées décrivant certains comportements prédéfinis (tels que l'intrusion de personnes, de véhicules ou d'objets dans des zones sécurisées). Elles doivent être capables d'identifier des incidents et de les relier à d'autres, d'effectuer des analyses de données de réseaux sociaux, de vidéo surveillance, d'enregistrements géospatiaux, de données de capteurs (ou d'autres sources de données) afin d'identifier proactivement tout incident et d'en assurer le suivi, pour renforcer la sécurité de notre quotidien.

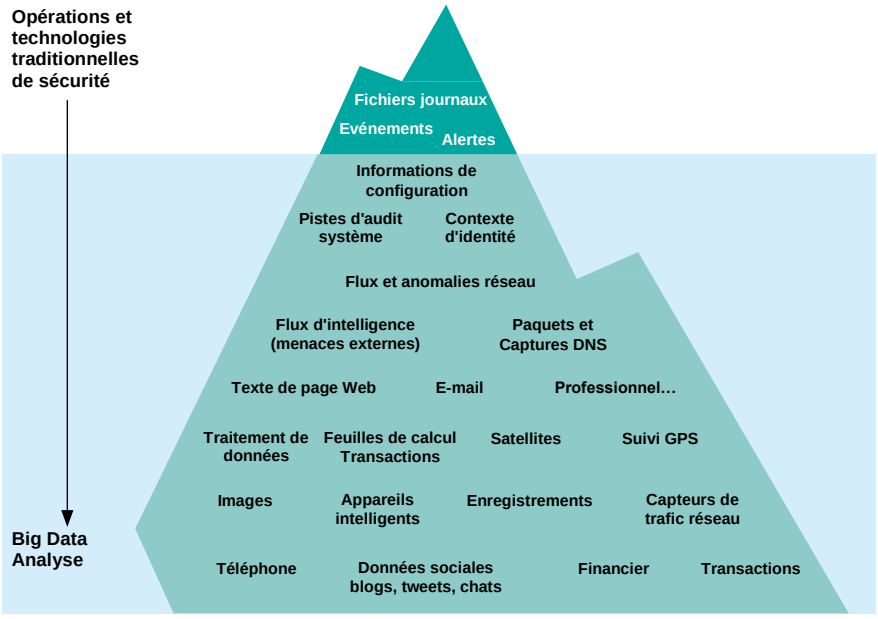
Les exemples sont nombreux. Les entreprises doivent étendre leur périmètre de mesures de sécurité pour inclure des mesures telles que le cryptage, la surveillance, le masquage de données, ainsi que des fonctions complémentaires d'intelligence sécuritaire, telles que les analyses Big Data. L'intelligence sécuritaire avec fonctions d'analyse Big Data permet de perfectionner l'application des mesures de sécurité et de confidentialité au sein de l'entreprise.

Ce que signifie le Big Data pour la sécurité

Nous nous trouvons à un moment unique dans notre histoire : nous pouvons maintenant analyser le monde qui nous entoure pour réagir aux incidents de sécurité, et pour assurer notre protection et prendre des mesures en temps réel.

Le phénomène du Big Data présente des opportunités uniques pour les entreprises, en leur permettant de capitaliser sur les données en provenance de sources multiples, dans le but d'optimiser leurs systèmes de sécurité (voir la Figure 1). Parmi ces sources, citons les données structurées traditionnelles ou les nouvelles sources non structurées (fichiers journaux, données d'instrumentation, données réseau, flux de surveillance vidéo, informations géospatiales, données de réseaux sociaux, etc.).

Des données plus volumineuses, dans des formats toujours plus variés, accélèrent les rythmes des entreprises. La difficulté consiste à en tirer parti avant que les pirates ne passent à l'action ou n'identifient les vulnérabilités.



- Analyse d'un **grand nombre** de données non traditionnelles et non structurées
- Augmentation significative du **volume** de données stockées, à des fins d'utilisation judiciaire et d'analyse d'historique
- Visualisation et interrogation de données (nouvelles méthodes)
- Analyse des données en continu, maintien de la **vitesse** des données

Figure 1 : La présence d'attaques de plus en plus sophistiquées a créé un besoin d'analyses Big Data

Les solutions d'intelligence sécuritaire qui font largement appel aux analyses Big Data pourront aider les entreprises à survivre dans un paysage de menaces complexes. En matière de sécurité, les experts recommandent d'adopter un état d'esprit innovant et une approche nouvelle.

"Certaines entreprises seront une cible, quoi qu'elles fassent, mais beaucoup d'entre elles le deviennent à cause de ce qu'elles font. Si votre entreprise constitue une cible de choix, essayez de comprendre ce que les personnes malveillantes risquent de tenter contre vous et jusqu'où s'étend leur motivation".

Verizon 2013 Data Breach Investigations Report[5]

"Recherchez des solutions de gestion de la sécurité de l'information et des solutions d'analyse réseau et de visibilité (NAV) afin d'utiliser le Big Data pour optimiser vos prises de décisions dans le domaine de la sécurité".

John Kindervag, Forrester Research[6]

"Des référentiels de données de sécurité permettent de protéger l'intelligence sécuritaire et de détecter les capacités des analyses et des dispositifs de mise en œuvre".

Gartner Realize That Big Security Data Is Not Big Security Nor Big Intelligence, Joseph Feiman, 19 avril 2013

Détection des menaces de sécurité

Les pirates et les criminels, très organisés, réussissent à contourner les défenses sécuritaires traditionnelles. Les types d'attaques sont trop nombreux pour pouvoir être expliqués ici ; mais ils peuvent être classés en six catégories principales, mentionnées ci-après :

1. **APT (Advanced Persistent Threats - Menaces avancées persistantes)** Les pirates ont la capacité et l'intention de cibler une entité spécifique de façon persistante et efficace. Ils ont accès à un vaste éventail de techniques, et restent silencieux. Leur approche est lente, coordonnée et adaptable, plutôt qu'aveugle et automatisée.
2. **Cybermilitantisme (ou Hacktivisme) :** Piratage pour des raisons politiques ou sociales.
3. **Cyber-attaques :** attaques visant à endommager ou à détruire un réseau informatique.
4. **Menaces internes :** utilisateurs malveillants dotés de connaissances approfondies de la structure informatique de la victime (comptes d'utilisateurs, mots de passe, conception, notamment).
5. **Fraude :** entités malveillantes tentant de comprendre et de contourner des processus commerciaux, afin d'en retirer des gains financiers.
6. **Attaques physiques :** bombes, incendies, armes à feu ou actes de terrorisme dans un lieu physique (stade, rue, domicile ou édifice gouvernemental, par exemple).

Lorsque les entreprises tentent de contrecarrer ce genre d'attaques, elles doivent tout d'abord établir une base, un modèle de comportement normal d'applications, de bases de données, d'utilisateurs et d'actifs, pour que toute anomalie indiquant une éventuelle attaque puisse être détectée.

Méthode de création d'une plateforme d'intelligence sécuritaire dotée de fonctions d'analyse Big Data

Pour créer une plateforme de sécurité dans l'univers informatique actuel, quatre exigences doivent être respectées.

1. Surveillance des comportements réseau afin de détecter les cyber-menaces (connues ou non)

La première exigence consiste à protéger les réseaux contre les attaques. Une protection appropriée nécessite une identification avancée des menaces, telles que les botnets. Un botnet est un réseau d'ordinateurs infectés contrôlés par un botmaster. Ce réseau infecte les entreprises par l'intermédiaire de sites Web malveillants, de fichiers exécutables et de clés USB ou de fichiers PDF. Les botnets peuvent compter quelques centaines d'hôtes ou plusieurs millions, et peuvent générer un trafic important sur le réseau. Mais ce trafic malveillant est souvent sous-estimé et mal compris, car le volume de transmissions TCP/IP est extrêmement élevé et contient de grandes quantités de trafic DNS (Domain Name System).

Pour protéger les réseaux et identifier les botnets, les entreprises doivent surveiller toutes les activités d'un réseau TCP/IP, afin de détecter l'activité anormale constituant potentiellement une menace. Pour cela, elles peuvent utiliser des algorithmes analytiques pour rechercher des indicateurs de menaces cachés.

Les fonctions d'analyse Big Data sont essentielles, car elles permettent de détecter, d'identifier et de surveiller une machine en analysant en temps réel une grande quantité de données. Les solutions utilisées surveillent la totalité du trafic (requêtes DNS, listes noires/blanches et accès aux bases de données) afin de comprendre la menace. Cette analyse doit être intégrée à des mesures d'intelligence externes, afin de développer un profil de menace exhaustif.

2. Détection des fuites de données

Pour comprendre si elle est en présence d'une fuite de données, une entreprise doit tout d'abord surveiller les informations auxquelles les employés ou les machines ont accès. Ensuite, elle doit déterminer si les employés ont accès à des informations sensibles (même s'ils possèdent les autorisations correspondantes) et avoir connaissance de tout changement soudain de mode d'accès. Normalement, un représentant de service d'assistance clientèle a accès aux dossiers des clients, mais si la moyenne quotidienne du nombre de dossiers traités passe brutalement de 25 à 500, il est légitime de s'inquiéter. L'entreprise doit alors déterminer s'il existe un risque de fuite d'informations confidentielles.

Bien comprendre l'accès aux données et l'historique des modifications permet d'obtenir une sécurité efficace, et est par ailleurs exigé en vertu de différentes directives industrielles et gouvernementales (PCI DSS, HIPAA et SOX, notamment).

Les fonctions d'analyse Big Data permettront d'améliorer la surveillance, grâce à l'utilisation de nouvelles sources de données (données Internet, satellite, audio/vidéo, par exemple), qui élargiront le champ des corrélations et rapprochements possibles.

3. Intégration des analyses judiciaires et de l'intelligence criminelle

La troisième exigence consiste à effectuer le suivi de criminels en temps réel, afin d'anticiper et d'éviter l'activité criminelle. Cela implique de surveiller différentes sources d'informations (libres ou non), afin de préciser les points suivants :

- Qui parle à qui, de quoi et comment ?
- Quelle est l'opinion communément répandue au sujet d'une personne, d'une entreprise ou d'un gouvernement spécifique?
- Quels sont les activités, sites, centres d'intérêt, plans des personnes et des groupes (et plus particulièrement des personnes figurant sur une liste noire) ?
- Est-on en présence d'autres contenus suspects ?

Exemples de données ayant besoin d'une analyse : modèles d'activité de base de données, enregistrements de données d'appels, trafic Web et capteurs physiques. Pour identifier et prévenir l'activité criminelle, il est nécessaire de disposer de fonctions avancées d'analyse de données de réseaux sociaux, d'informations géospatiales, de données de type texte, image, vidéo et voix.

4. Soutien des autorités de police

Les fonctions d'analyse des extractions en temps réel de données relatives à la géolocalisation de personnes recherchées sont possibles grâce à l'utilisation de détecteurs (GPS sur téléphone mobile, par exemple), ce qui permet d'aider les autorités de police à prévoir et à éviter de façon proactive les activités criminelles. Les fonctions intelligentes de surveillance incluent des fonctions puissantes d'analyse prédictive sur différents flux simultanés de données de surveillance (structurées et non structurées), qui peuvent provenir de sources automatisées ou non, ou encore de caméras de sécurité, et qui permettent d'alerter les services de police en cas de problème potentiel de sécurité. Cette approche, associée à des fonctions de reconnaissance en temps réel, peut aider la police dans ses enquêtes intra ou transfrontalières.

Quatre capacités de base doivent être associées pour que ces trois exigences soient respectées : une plateforme d'intelligence sécuritaire, une plateforme d'analyse des données en continu et une infrastructure d'analyse Hadoop. Ce point est illustré par la Figure 2.

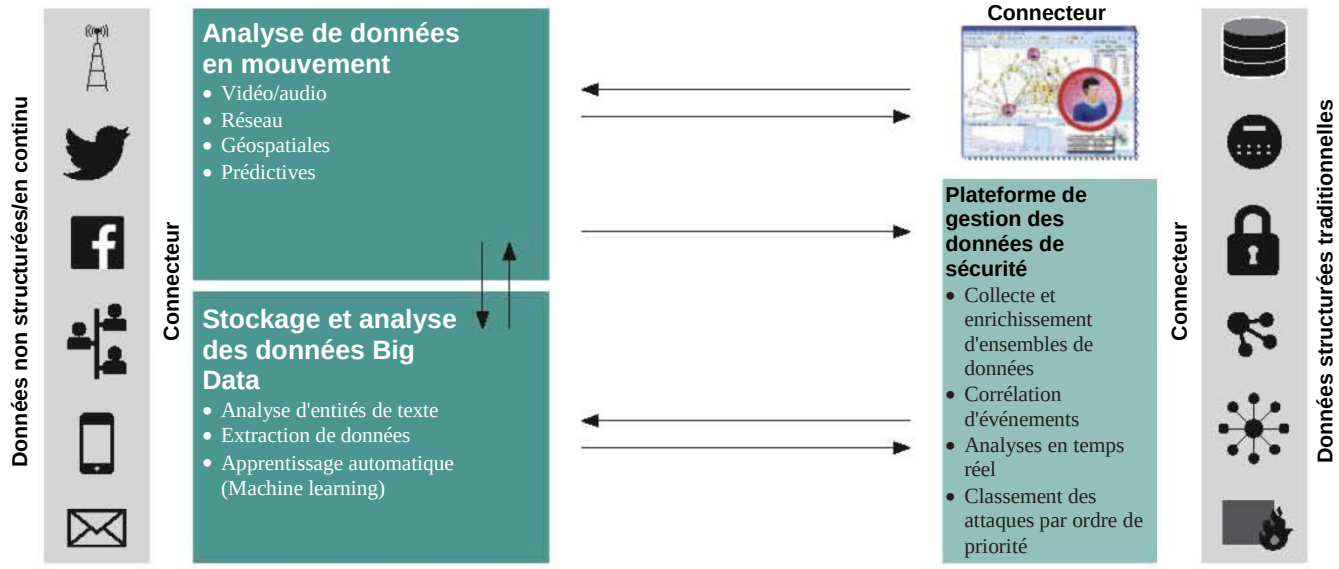


Figure 2 : Intelligence sécuritaire et Big Data

Programme IBM Quick Start pour les technologies Big Data

Téléchargement gratuit, mise en route rapide. Pour aider les clients dans leur mise en route de projet Big Data, IBM a lancé le programme Quick Start, qui permet aux utilisateurs d'accéder rapidement aux principales technologies Big Data du marché. Téléchargeable gratuitement, cette plateforme leader sur le marché permet aux utilisateurs d'essayer la technologie Big Data au sein de leur environnement unique. Elle ne contient pas de limites de volume de données ou de date.

- IBM InfoSphere BigInsights Quick Start Edition – www.ibm.com/software/data/infosphere/biginsights/quick-start/
- IBM InfoSphere Streams Quick Start Edition – www.ibm.com/software/data/infosphere/streams/ quick-start/

Avantages de l'intégration des fonctions d'intelligence sécuritaire aux analyses Big Data

Lorsque des fonctions d'analyse Big Data sont ajoutées à une solution d'intelligence sécuritaire, les avantages sont de taille. Tout d'abord, cela aide les utilisateurs à mieux comprendre les menaces potentielles avant qu'elles ne se produisent, ce qui leur permet d'agir en temps réel. Ensuite, cela permet de détecter les fraudes, d'identifier les comportements de base en faisant ressortir les anomalies dès qu'elles se produisent. Enfin, cela permet de surveiller en permanence l'état de sécurité de l'entreprise. Ces fonctions permettent aux utilisateurs d'agir pour éviter les activités criminelles.

En résumé, les fonctions d'intelligence sécuritaire associées aux fonctions d'analyse Big Data permettent de tirer profit des énormes volumes de données qui circulent dans les entreprises pour anticiper et prévoir les menaces et pour agir via des analyses prédictives. Cela permet d'analyser les flux de données en mouvement au fil de l'eau et d'effectuer des analyses sophistiquées sur les données collectées.

De nombreux clients IBM saisissent ces opportunités et ont pu obtenir des résultats mesurables. Par exemple, aux Etats-Unis, un service public peut désormais analyser en temps réel 1,6 Go/seconde de données vidéo. Un autre client (organisme de défense nationale) a pu identifier 43 hôtes infectés parmi des centaines de noms de domaines possibles. Ce client a détecté le transfert de plus de 350 documents portant le mot clé Confidentiel sur le réseau, et plus de 900 accès à Facebook au cours d'une plage de 45 minutes.

Un service public des Etats-Unis traite 1,6 Go de données en continu par seconde

Le partenaire commercial d'IBM TerraEchos, Inc., fournisseur de systèmes de surveillance et de détection leader sur le marché, propose aux entreprises des solutions de sécurité avancées pour infrastructures sensibles et sites de grande superficie. L'un des clients de TerraEchos est un laboratoire scientifique d'ingénierie appliquée chargé de soutenir la mission du Ministère de l'Energie des Etats-Unis dans le cadre de ses travaux sur l'énergie nucléaire, les sciences et la Défense Nationale.

Ce laboratoire s'est tourné vers TerraEchos pour la mise en œuvre d'un système avancé de sécurité et de surveillance basé sur le système TerraEchos Adelos® S4 (un serveur IBM System x3650) et sur le logiciel IBM InfoSphere® Streams. Cette solution contient une technologie audio avancée faisant appel à la fibre optique, sous licence de l'US Navy.

Le logiciel InfoSphere Streams, véritable plateforme d'analyse sous-jacente, permet à la solution Adelos S4 d'effectuer en temps réel l'analyse et la classification des données audio. Il permet de collecter des données issues de différents types de capteurs, et d'incorporer des flux de données associées (structurées ou non) à un système intégré de détection des menaces, de classification, de corrélation, de prévision et de communication, via le recours à une architecture orientée service.

Cette solution permet de collecter et de transmettre en temps réel des données audio sans interruption issues des locaux du laboratoire, ce qui permet aux membres de l'équipe de sécurité de disposer d'informations sans précédent sur chaque événement. Ce système permet au personnel du laboratoire et au personnel de sécurité de savoir (d'entendre) ce qui se passe, même lorsque la perturbation a lieu à des kilomètres. Cela leur permet d'identifier de manière fiable une menace de sécurité potentielle et de la classer, puis de prendre toute mesure appropriée. Les intrusions sont classées dans les catégories Biologique, Mécanique ou Environnementale, et représentées au sein d'un domaine spatial, ce qui permet de faire la différence entre un intrus humain, animal ou mécanique.

“Le gouvernement des Etats-Unis travaille en collaboration avec IBM Research depuis 2003 sur une approche radicalement nouvelle en matière d'analyses de données, qui permet d'effectuer des analyses complexes, rapides et évolutives des flux de données en circulation. Ce projet a connu un succès tel que le gouvernement américain va déployer d'autres installations afin de permettre aux autres entités gouvernementales de se donner les moyens de réussir leurs projets”.

Gouvernement des Etats-Unis

Portefeuille IBM de solutions analytiques Big Data

IBM est le seul fournisseur capable d'offrir des solutions d'intelligence sécuritaire avec fonctions d'analyse Big Data, comme l'illustre la Figure 2.

IBM QRadar® Security Intelligence Platform permet de consolider des données d'événements et réseau provenant de milliers d'appareils, de nœuds finaux et d'applications répartis au sein d'un réseau. Cette plateforme permet de réaliser des activités de normalisation et de corrélation sur des données brutes, afin de faire la distinction entre les menaces réelles et les faux positifs. Ce logiciel peut également intégrer (en option) l'application IBM Security X-Force® Threat Intelligence, qui offre une liste d'adresses IP potentiellement malveillantes (hôtes maliciels, spams et autres menaces). Et grâce à la plateforme QRadar Security Intelligence Platform, vous pouvez effectuer la corrélation entre les vulnérabilités d'un système et des événements et données réseau, ce qui permet d'affecter des priorités aux incidents de sécurité.

Le logiciel IBM InfoSphere BigInsights™ s'appuie sur l'infrastructure Apache™ Hadoop® pour fournir des analyses et faciliter l'identification des menaces de sécurité. IBM n’utilise pas d’instructions fork et maintient la compatibilité de l'interface de programmation Hadoop. Des modules IBM Hadoop figurent dans InfoSphere Biglnsights, ainsi qu'une technologie IBM qui ne figure pas dans les solutions Hadoop libres.

Ce logiciel permet d'améliorer la précision d'analyse et de fournir des informations à la plateforme QRadar Security Intelligence Platform, constituant une source d'apprentissage en continu et en boucle fermée. Résultat : une solution intelligente et intégrée qui permet de collecter, de surveiller, d'analyser des données d'entreprise et de sécurité et de créer le reporting correspondant, de façon totalement innovante.

IBM InfoSphere Streams est une plateforme informatique avancée qui permet à des applications développées par les utilisateurs d'intégrer et d'analyser les données entrantes (en provenance de milliers de sources différentes) en temps réel, et d'en assurer la corrélation. Il permet de traiter des débits de données très élevés (pouvant atteindre des millions d'événements ou de messages par seconde). Le logiciel InfoSphere Streams a été conçu pour analyser les données en mouvement et pour offrir des temps de réponse de moins d'une milli-seconde (ce qui permet aux utilisateurs d'afficher des informations et des événements au fur et à mesure de leur déroulement, élément essentiel de l'intelligence sécuritaire). Ce logiciel permet d'améliorer la précision d'analyse et de fournir des informations à la plateforme QRadar Security Intelligence Platform, constituant une source d'apprentissage en continu et en boucle fermée.

InfoSphere Streams offre un environnement de développement simple. Les utilisateurs peuvent optimiser leurs applications existantes à l'aide de l'environnement de développement intégré Eclipse, doté de fonctionnalités Glisser-déposer et de visualisation. Le logiciel InfoSphere Streams offre une architecture évolutive, qui permet d'intégrer des sources de données structurées et non structurées, et d'utiliser en association d'autres technologies de sécurité.

IBM PureData™ for Analytics, intégrant la technologie IBM Netezza, est un dispositif intelligent d'une grande simplicité, permettant d'effectuer des analyses précises. Il simplifie et optimise les performances de services de données pour applications analytiques. Il permet d'exécuter des algorithmes très complexes en quelques minutes (au lieu de longues heures auparavant), offrant une vitesse de 10 à 100 fois supérieure à celle des systèmes traditionnels, sans compter qu'il affiche une accélération du retour sur investissement (charge de 5 To/heure) et une grande simplicité d'utilisation.

Toutes les offres ci-dessus sont intégrées au portefeuille IBM de produits de sécurité et de confidentialité des données (incluant **IBM InfoSphere Guardium® et IBM InfoSphere Optim™**[7]). InfoSphere Guardium Data Activity Monitor offre des contrôles en temps réel de la sécurité des données, des fonctions d'audit de base de données, des fonctions automatisées de reporting de conformité, des fonctions de contrôle d'accès aux données, des fonctions de gestion de la vulnérabilité de bases de données et de découverte automatique de données sensibles.

IBM InfoSphere Optim permet de bénéficier d'options de masquage statique et dynamique sur demande. Grâce à l'intelligence sécuritaire avec fonctions d'analyse Big Data, les entreprises peuvent appliquer intelligemment leurs politiques de sécurité et de confidentialité.

Avez-vous besoin d'une plateforme de sécurité équipée de fonctions d'analyses Big Data ?

Si vous répondez Oui aux questions suivantes, il est probable que vous ayez besoin d'une solution de sécurité incluant des fonctions d'analyse Big Data :

- Souhaitez-vous effectuer l'analyse et la corrélation de données plus vastes, pour éviter les cyber-attaques, les menaces physiques, les demandes d'indemnisation frauduleuses ou les prises de contrôle de comptes ?
- Avez-vous besoin d'enrichir votre solution de sécurité en incluant des données d'e-mail, de réseaux sociaux ou d'autres données non structurées, afin d'améliorer la détection des cyber-menaces et d'y apporter les solutions correspondantes ?
- Avez-vous besoin de mieux détecter et surveiller les activités criminelles et terroristes, en effectuant la corrélation d'un nombre accru de sources, pour y découvrir des associations ou des modèles ?
- Souhaitez-vous optimiser vos systèmes de sécurité et de surveillance à l'aide de données en temps réel provenant d'appareils ou capteurs vidéo, audio, thermiques ou autres ?

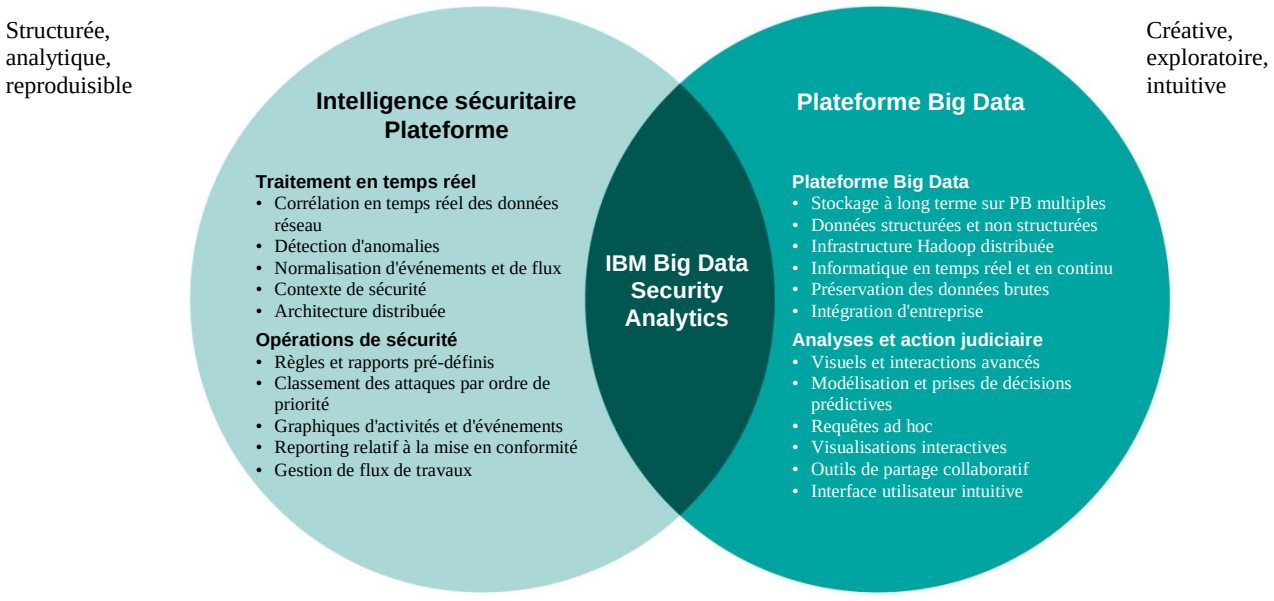


Figure 3 : Intégration des fonctions d'intelligence sécuritaire et d'analyses Big Data

Si vous souhaitez explorer de façon plus détaillée le cas d'utilisation d'intelligence sécuritaire, contactez votre représentant IBM local, ou visitez le site Web suivant : www.ibm.com/software/data/bigdata/use-cases.html

1 http://thehackernews.com/2013/05/the-biggest-bank- robbery-in-history.html
2 http://thehackernews.com/2013/05/us-department-of- defense-officials-are.html
3 www.bizjournals.com/washington/blog/fedbiz_ daily/2013/02/obama-confirms-cybersecurity-order-in. html?page=all
4 http://thehackernews.com/2013/08/short-password-reset-code-vulnerability.html
5 www.verizonenterprise.com/DBIR/2013/
6 "Control And Protect Sensitive Information In The Era Of Big Data", Forrester Research, Inc., 12 juillet 2012.
7 www.ibm.com/software/data/security-privacy/

IBM
17 Avenue de l'Europe
92275 Bois Colombes Cedex
France

Imprimé en France
Octobre 2013

IMS14435-FRFR-00