IBM Software
Livre blanc pour décideurs éclairés

Janvier 2013

Guide des décideurs informatiques sur les approches de sécurité intelligente

De la gestion des journaux et du SIEM à une sécurité intelligente

Sommaire

2 Introduction

2 Définir les objectifs de la sécurité intelligente

4 Identifier le problème

5 Aller au-delà de la gestion des journaux, des événements et des informations de sécurité (SIEM)

7 Déterminer la valeur économique de la sécurité intelligente

9 Protéger les bénéfices

11 Mettre en place une sécurité intelligente

11 Conclusion

12 Pour plus d'informations

Introduction

La sécurité intelligente s'appuie sur les mêmes concepts que ceux qui ont fait le succès de la Business Intelligence (BI) en tant que technologie d'entreprise. Elle constitue une avancée essentielle pour les organisations qui reconnaissent l'importance de la sécurité des informations pour leur activité. Cet enjeu est véritablement stratégique dans le monde actuel, où les entreprises instrumentées, interconnectées et intelligentes collectent, traitent, utilisent et stockent un volume d'informations inédit.

Trop souvent, la réponse aux nouvelles menaces sur la sécurité des informations s'apparente à une « rustine » avec une technologie ad hoc, de nouvelles stratégies ou de nouvelles règles réactives. Dans une large mesure, ceci s'explique par le fait qu'un programme de sécurité unifiée – fondé sur des analyses automatiques d'informations unifiées dans toute l'infrastructure informatique – est coûteux, complexe, difficile à mettre en œuvre et inefficace. De fait, la plupart des organisations sont incapables de détecter les menaces et de gérer les risques de manière optimale.

Ce livre blanc montre comment la sécurité intelligente corrige ces lacunes et permet aux organisations – grandes entreprises, PME ou organismes publics – de sécuriser leurs informations à moindre coût. En particulier, il montre la réponse apportée par la sécurité intelligente à des points critiques dans cinq domaines :

- Consolidation des silos de données
- Détection des menaces
- Découverte des fraudes
- Évaluation et gestion des risques
- Conformité à la réglementation

Définir les objectifs de la sécurité intelligente

Les organisations les plus performantes affichent d'excellents résultats, car elles savent exploiter leurs informations. Grâce à l'utilisation automatisée de la technologie de BI, elles exécutent des analyses qui valorisent au maximum leur masse gigantesque de données.

En appliquant cette même approche et en mettant en place un programme de sécurité intelligente, elles peuvent sécuriser leurs informations. Tout comme la BI aide les entreprises à prendre des décisions qui optimisent les opportunités et minimisent les risques, la sécurité intelligente permet d'être plus performant dans la détection des menaces, l'identification des risques liés à la sécurité et à la non-conformité, ainsi que la définition des priorités pour la résolution des problèmes.

Le cas de la BI est particulièrement parlant. Elle permet aux organisations de prendre des décisions stratégiques en automatisant l'analyse des données bien au-delà des capacités de l'analyse manuelle. Avec la mise en place de solutions informatiques d'analyse métier dans leurs environnements uniques, les organisations prospères valorisent pleinement leurs téraoctets (To) et pétaoctets (Po) de données, qu'il s'agisse de chiffres de ventes, de données démographiques sur les clients, de coûts d'expédition ou de matières premières.

Le cas de la sécurité intelligente est aussi frappant, sinon plus. Les entreprises et les organismes publics disposent de volumes massifs de données qui peuvent contribuer à détecter les menaces et les vulnérabilités, s'ils ont les moyens et la volonté de les collecter, de les agréger et, surtout, de les analyser. Ces données ne proviennent pas seulement de solutions de sécurité ponctuelles, mais également de sources telles que les configurations de périphériques réseau, de serveurs, du trafic réseau, des applications, des utilisateurs et de leurs activités.

La sécurité intelligente limite le risque, facilite la mise en conformité, assure un réel retour sur investissement (ROI) et optimise les investissements dans les technologies de sécurité existantes. Ses objectifs sont les suivants :

- analyser un grand volume d'informations pour obtenir un petit nombre d'actions à prendre grâce à un processus décisionnel efficace appliqué à des milliards de données ;
- mettre en œuvre la collecte et l'analyse de données par l'automatisation et en apportant une simplicité d'utilisation ;
- proposer des applications performantes qui extraient toute la valeur des données pour appréhender et contrôler le risque, détecter les problèmes et hiérarchiser la résolution ;
- valider que l'organisation a mis en place les bonnes règles ;
- s'assurer que les contrôles mis en place par l'organisation favorisent effectivement la mise en œuvre de ces règles.

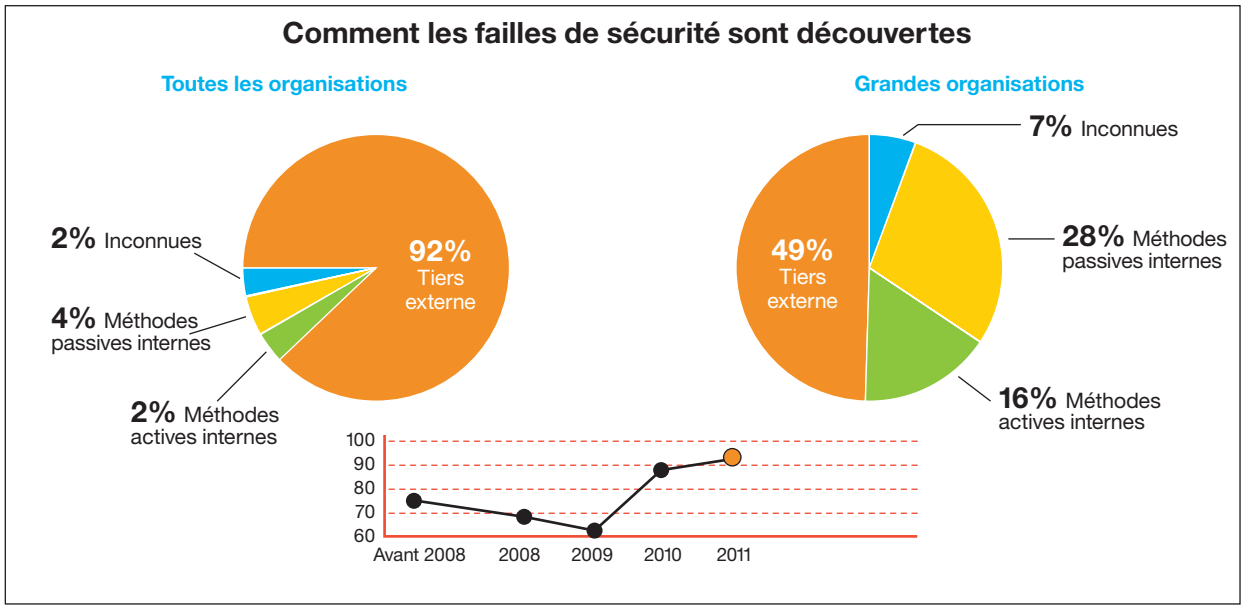
Les organisations ont encore beaucoup de chemin à parcourir pour comprendre leur environnement de sécurité informatique. Selon un rapport récent d'ESG, 59 % des organisations de plus de 1000 employés sont sûres ou relativement sûres d'avoir été la cible d'une attaque persistante avancée (APT)[1]. Pour ESG, la plupart des responsables sécurité des informations sont dans une position de perdant. D'un côté, ils sont confrontés à un environnement menaçant et doivent sécuriser de nouvelles initiatives informatiques, comme le cloud, la mobilité et les réseaux sociaux. De l'autre, ils ont des outils en silos, des équipes en sous-effectif et des processus manuels pour assurer leur sécurité[2].

De plus, un rapport Verizon Data Breach Investigations a révélé que plus de la moitié des atteintes à la sécurité des données passent inaperçues pendant des mois. Selon cette étude, ces dernières années, les tiers découvrent ces atteintes beaucoup plus fréquemment que les organisations qui en sont victimes. En fait, le nombre de failles mises au jour par des tiers atteint des sommets inédits, avec plus de 90 % de toutes les organisations averties par des tierces parties.[3]

Identifier le problème

Le modèle de sécurité d'il y a 10 ou 12 ans ne répond plus aux défis du moment, à l'heure où les « hooligans d'Internet » ont cédé la place aux activités de criminels organisés. Ce modèle est obsolète et ne permet pas de faire face aux menaces et aux environnements informatiques actuels. La sécurité périmétrique a évolué vers une forme hautement distribuée, car d'une part les employés, les partenaires et les clients travaillent désormais à distance sur Internet, et d'autre part les criminels exploitent de nouveaux vecteurs d'attaque et cherchent à tromper la confiance des utilisateurs. Les réglementations publiques et sectorielles vont vers des pénalités plus importantes et des conditions d'application plus strictes.

En réponse, le secteur de la sécurité a proposé des produits nouveaux et plus performants contre chaque menace. Tous ces outils valorisent la sécurité globale de l'entreprise, mais ce sont par nature des îlots de technologie. Comme ils ne s'inscrivent pas dans un programme de sécurité à l'échelle de l'entreprise, ils ont tendance à fragmenter l'effort global.



Source : Verizon Risk Team, « 2012 Data Breach Investigations Report », Verizon Communications, Inc., 2012

Souvent, les organisations ne savent pas qu'elles ont été attaquées et le découvrent par un tiers qui les en informe. Lorsque des failles sont identifiées en interne, elles le sont soit par des méthodes actives conçues tout spécialement pour la détection, soit par des méthodes passives dans lesquelles un incident n'est pas reconnu comme faille par un processus non orienté sécurité.

Souvent, les organisations doivent gérer des données incomplètes lorsqu'un outil de sécurité ne reconnaît pas une menace ou un risque car il n'est pas corrélé à d'autres sources de données. Ceci dit, même lorsque des données sont collectées auprès de plusieurs sources, les analystes sont bloqués par le volume qui complique considérablement la génération d'informations exploitables.

La sécurité intelligente répond à ces problèmes sur l'ensemble du cycle de la sécurité, en centralisant les données de plusieurs silos, en les normalisant et en effectuant des analyses automatiquement. Ainsi, les organisations peuvent hiérarchiser le risque et déployer à moindre coût des ressources de détection, de prévention, de réponse et de résolution.

Aller au-delà de la gestion des journaux et du SIEM

Le concept de sécurité intelligente est partiellement présent dans les outils SIEM qui corrèlent et analysent les données agrégées et normalisées des journaux. Les outils de gestion des journaux centralisent et automatisent le processus d'interrogation, mais ils n'ont ni la souplesse ni les fonctionnalités de corrélation et d'analyse du SIEM et, à plus forte raison, de la sécurité intelligente.

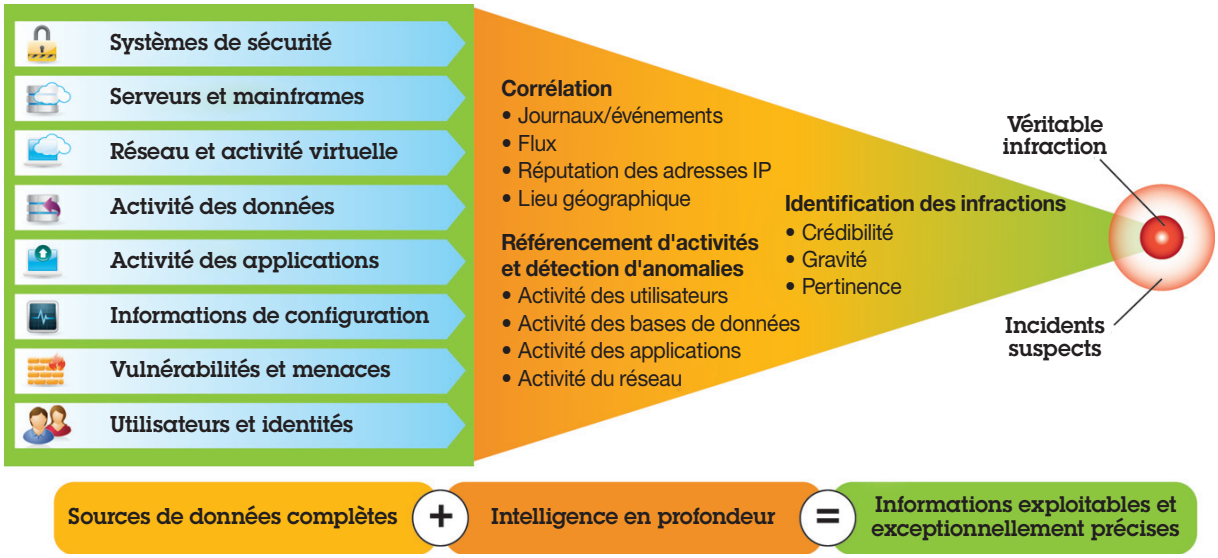
Mais le SIEM doit être considéré comme une étape plutôt que comme un aboutissement, l'objectif final étant la sécurité intelligente complète. Le SIEM est un outil très puissant en termes de gestion des événements et joue un rôle prépondérant dans la détection des menaces. Cependant, pour être complète, la sécurité intelligente doit englober et analyser un panel d'informations beaucoup plus large. Elle requiert un suivi permanent de toutes les sources de données pertinentes dans l'infrastructure informatique, ainsi qu'une évaluation des informations dans des contextes qui débordent largement du cadre des fonctionnalités de type SIEM.

L'un des avantages de la sécurité intelligente par rapport au SIEM réside dans sa capacité à contextualiser les données issues de sources très différentes. Ceci réduit le nombre de faux positifs, indique aux utilisateurs non seulement les ressources indûment exploitées, mais aussi les mesures prises en conséquence, et permet d'accélérer la détection et la réponse aux incidents.

La sécurité intelligente doit inclure une diversité de données beaucoup plus large, en tenant compte du contexte dans lequel les systèmes fonctionnent. Ce contexte inclut, entre autres, les journaux des périphériques du réseau et de sécurité, les vulnérabilités, les données de configuration, la télémétrie du trafic réseau, les événements et activités des d'applications, les identités des utilisateurs, les ressources, la géolocalisation et les contenus des applications.

Tout ceci produit un volume considérable de données. La sécurité intelligente génère une valeur importante en s'appuyant sur ces données pour définir un contexte très spécifique autour de chaque enjeu potentiel, et exécute des analyses de pointe pour détecter précisément un éventail croissant de menaces.

Par exemple, l'exploitation potentielle d'un serveur web signalée par un système de détection des intrusions peut être confirmée par une activité sortante inhabituelle détectée par des fonctionnalités NBAD (détection d'anomalies dans le comportement du réseau).



IBM QRadar Security Intelligence Platform offre une sécurité intelligente complète.

Autre exemple, vous avez un rapport indiquant qu'un serveur présente une vulnérabilité potentielle qui vient tout juste d'être découverte. Mais si ces vulnérabilités se comptent par centaines dans votre organisation, comment évaluer la menace qui concerne ce serveur en particulier ? La sécurité intelligente peut analyser toutes les données disponibles et vous signaler :

- la présence ou l'absence de la vulnérabilité ;
- la valeur que l'organisation accorde à la ressource ou aux données ;
- la probabilité d'une exploitation basée sur les modèles de menace par chemin d'attaque ;
- les informations de configuration qui peuvent indiquer, par exemple, que le serveur n'est pas accessible suite à une modification d'un paramètre par défaut ;
- la présence d'outils de protection, comme un système de prévention des intrusions.

Soit vous envisagez une menace interne. Les 260 000 câbles diplomatiques sur des questions miliaires, diffusés par WikiLeaks en 2010, ont été obtenus par un militaire américain qui disposait d'une habilitation et qui, selon l'acte d'accusation, a « intentionnellement outrepassé ses droits d'accès ». D'après les journaux, il a profité d'une faille dans les stratégies visant à prévenir les téléchargements non autorisés[4]. Mais l'analyse des données corrélées, en appliquant les contextes de plusieurs sources, aurait pu empêcher la fuite avant qu'elle ne cause des dommages.

Déterminer la valeur économique de la sécurité intelligente

L'un des arguments les plus convaincants en faveur de la sécurité intelligente, c'est son efficacité opérationnelle qui se traduit par une meilleure utilisation du personnel, du temps et de l'infrastructure. Elle peut combiner plusieurs technologies de réseau et de sécurité dans un système intégré, au lieu d'exploiter des produits indépendamment.

La sécurité intelligente est d'autant plus essentielle que la responsabilité opérationnelle de la sécurité est de plus en plus confiée aux équipes en charge des opérations réseau. Il est sensé de dupliquer cette consolidation des responsabilités opérationnelles avec la consolidation au niveau de la couche d'intelligence. Imaginez que vous lancez plusieurs tâches sur une plate-forme au sein de l'organisation, que vous développez des compétences pour plusieurs fonctions, puis que vous déployez les droits d'accès en fonction des rôles.

Par ailleurs, la sécurité intelligente valorise d'autres aspects de l'informatique, comme la résolution de problèmes liés aux systèmes, les pannes de réseau, la prise en charge des utilisateurs et l'analyse des autorisations.

La sécurité intelligente permet aux organisations d'utiliser des outils intégrés dans un cadre commun et d'exploiter des données unifiées pour résoudre toutes sortes de problèmes liés à la sécurité. Pour illustrer ce propos, considérons cinq situations parmi les plus fréquentes, où la sécurité intelligente offre une réelle valeur ajoutée.

Consolidation des silos de données

Sans une technologie automatisée, les analyses de BI sont difficiles à exécuter. Les données qui permettraient aux utilisateurs de comprendre les retours, les chaînes d'approvisionnement, etc. sont disponibles, mais cloisonnées dans différentes applications et bases de données. C'est à l'analyste de compiler les données de toutes ces sources dans des feuilles de calcul ou des bases de données pour effectuer des analyses manuelles. L'analyse de sécurité pose des problèmes similaires. La sécurité intelligente, quant à elle, offre des avantages similaires en termes d'efficacité. Du point de vue de la sécurité, les données peuvent résider dans trois types de silos :

- Données présentes dans des périphériques de sécurité, des applications et des bases de données disparates.
- Données collectées dans des produits spécifiques, des applications, etc., créant ainsi un autre silo ; ces données sont stockées dans une autre base de données, mais il n'y a ni communication ni coordination entre les bases de données de configuration.
- Silos organisationnels de données, propres à chaque division, groupe d'opérations, service ou groupe.

Dans les deux premiers cas, la sécurité intelligente fusionne les silos en intégrant les flux de données des différents produits dans un cadre commun permettant d'effectuer des analyses automatisées sur diverses technologies d'informatique et de sécurité. En termes de sécurité, ceci offre toutes les fonctionnalités de détection et d'évaluation des risques que la télémétrie consolidée de la sécurité intelligente peut apporter. Pour un directeur des systèmes d'information, réduire le nombre de silos permet de rationaliser les solutions de sécurité qui, sinon, devraient être gérées individuellement. Le troisième cas de figure requiert une coopération importante entre des groupes généralement séparés, imposant un réalignement des processus et des responsabilités, et parfois une pression de la part de la direction.

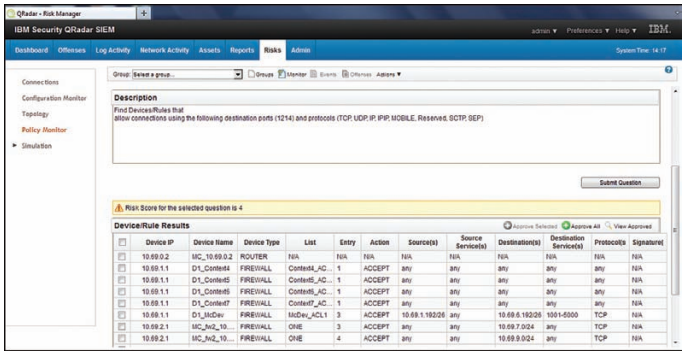
La croissance exponentielle du volume de toutes ces données disparates ne fait que compliquer le problème. Chacun de ces silos peut générer des volumes massifs de données dans différents formats, pour différentes finalités. Parfois, ils peuvent créer différentes stratégies ou exigences de conformité. Seule une sécurité intelligente automatisée est en mesure de gérer les pétaoctets de données de sécurité et de les analyser dans tous les silos opérationnels et organisationnels.

Détection des menaces

En quelques années, alors que les entreprises s'ouvraient au commerce électronique et aux utilisateurs distants, la sécurité a évolué d'un modèle périmétrique centralisant toutes les stratégies dans le pare-feu, vers une forme beaucoup plus distribuée. Elle se concentre désormais sur les serveurs, les applications et les informations qui sortent de l'organisation.

De plus, nous constatons régulièrement les effets de plus en plus dévastateurs des attaques très ciblées, qui visent notamment des entreprises très en vue. En général, les intrusions ciblées sont multiphases, multifacettes, difficiles à détecter et très compliquées à éradiquer. Les menaces persistantes avancées se caractérisent par la ténacité des pirates et les ressources qu'ils ont à leur disposition.

Il est primordial d'intégrer de l'intelligence dans les diverses technologies de sécurité qui ont été développées en réponse aux nouvelles menaces. Comme nous l'avons déjà vu dans la partie sur le contexte de la sécurité, une activité qui semble anodine dans une partie de l'infrastructure peut se révéler être une menace lorsque ces données sont corrélées à d'autres sources. Par exemple, un utilisateur malveillant peut désactiver la journalisation, mais il ne peut pas interrompre l'activité du réseau. Parfois, les applications propriétaires ne créent pas de



L'écran de hiérarchisation des risques montre une évaluation des risques demandée par un utilisateur.

fichiers journaux et certaines parties du réseau ne sont pas protégées par un pare-feu. Mais la sécurité intelligente reste capable d'identifier les applications et les services exécutés entre cet hôte et le réseau, et dans ce cas reconnaître une menace potentielle.

Découverte des fraudes

La sécurité intelligente est absolument essentielle pour détecter efficacement les fraudes. Outre la télémétrie du réseau et les données provenant de l'infrastructure de commutation/routage et de la couche de mise en œuvre des systèmes de sécurité, la clé consiste à comprendre les utilisateurs et les données des applications.

Pour détecter des fraudes, il faut surveiller tout ce qui transite sur le réseau : activité et événements du réseau, activité du serveur et des applications, activité de chaque utilisateur.

La sécurité intelligente permet aux organisations de relier l'utilisateur à une ressource particulière. En associant l'activité du réseau, du serveur DNS (Domain Name Server) des applications aux informations d'annuaire, par exemple, la sécurité intelligente peut identifier un utilisateur par son adresse IP et sa session VPN (réseau privé virtuel).

Évaluation et gestion des risques

La sécurité intelligente constitue la pierre angulaire de la gestion des risques, grâce à l'analyse des impacts et la modélisation des menaces. C'est toute la différence entre réagir aux attaques sur le réseau et protéger l'une des ressources les plus importantes.

L'analyse des impacts se fonde sur la valeur qu'une organisation accorde à une ressource particulière et sur les conséquences négatives si la sécurité de celle-ci est compromise. La sécurité intelligente apporte une solution en identifiant les ressources stratégiques par une recherche et une classification des données et des ressources. De plus, elle répond à plusieurs questions. Quel est le niveau d'exposition de la ressource aux menaces ? A-t-elle accès directement à Internet ? Présente-t-elle des vulnérabilités connues que des pirates peuvent exploiter ?

La modélisation des menaces tient compte de tous ces facteurs et d'autres encore. Elle identifie non seulement les vulnérabilités sur le système cible, mais également les chemins d'attaque possibles qui exploitent les failles entre la cible et Internet : règles de pare-feu mal définies, listes de contrôle d'accès aux routeurs mal configurées, etc.

Conformité à la réglementation

La conformité est un principe fondamental de la sécurité intelligente. Cette dernière répond à de nombreuses exigences de conformité, notamment à tous les aspects de la surveillance. Par exemple, elle ne répond pas à toutes les exigences du standard PCI (Payment Card Industry), mais toutes les exigences du standard PCI liées à la surveillance sont prises en charge d'une manière que le SIEM et la gestion des journaux ne permettent pas. La sécurité intelligente fournit des données grâce auxquelles il est possible de remplir et de prouver les exigences en matière d'audit pour toutes les réglementations.

En surveillant toute l'infrastructure informatique – événements, modifications de configuration, activité du réseau, activité des applications et des utilisateurs –, la sécurité intelligente consolide les fonctionnalités de conformité dans une même suite de produits, au lieu de multiplier les produits qui apportent chacun leur pierre à l'édifice.

Protéger les bénéfices

La sécurité intelligente, comme la BI, permet aux organisations de prendre de meilleures décisions. Les organisations traitent davantage d'informations avec une efficacité accrue dans toute l'infrastructure informatique. Avec la technologie de BI, les organisations gagnent en performance : au lieu de payer des analystes à traiter une partie des données disponibles pendant des heures, la BI automatise l'analyse sur l'ensemble des données et fournit des informations sur les rôles propres à la tâche concernée.

L'intérêt de l'informatique, c'est sa capacité à automatiser le traitement, qu'il s'agisse d'achats, de logistique, de planification des ressources de l'entreprise, etc. Celui de la sécurité intelligente, c'est sa capacité à automatiser la sécurité, notamment à comprendre le risque, à surveiller les menaces et les vulnérabilités de l'infrastructure, et à hiérarchiser la résolution.

En centralisant les outils de sécurité et les données de l'infrastructure informatique, la sécurité intelligente permet de consolider la gestion et d'utiliser plus efficacement les ressources dédiées à la sécurité. Les organisations peuvent renforcer leur sécurité sans augmenter les coûts opérationnels et humains, ni acheter, gérer et intégrer plusieurs produits.

La sécurité intelligente offre des avantages considérables en termes de coût et d'efficacité. Elle peut :

- Réduire les coûts liés au déploiement et aux opérations ; au lieu d'embaucher du personnel, les organisations utilisent les équipes en place pour adapter la sécurité à l'activité de l'entreprise.
- Rendre l'achat de produits plus simple et moins cher ; les organisations achètent une seule plate-forme et pas plusieurs produits.
- Faciliter le déploiement grâce à une plate-forme unifiée au lieu de plusieurs produits qui doivent ensuite être intégrés pour offrir des capacités de sécurité intelligente tout juste acceptables.
- Proposer à un large panel d'organisations, des fonctionnalités de sécurité que seules les entreprises les plus en pointe pouvaient auparavant s'offrir.
- Automatiser la collecte, la normalisation et l'analyse de volumes massifs de données de sécurité provenant des silos techniques et organisationnels ; cette fonctionnalité applique un contexte enrichi à chaque analyse.
- Renforcer la détection des menaces par la contextualisation, pour identifier les attaques susceptibles d'échapper à une technologie de sécurité particulière.
- Améliorer la réponse aux incidents par une détection rapide et précise.
- Offrir un retour sur investissement sur le personnel ; les organisations peuvent mettre en place de nouveaux services de sécurité, comme une surveillance mondiale des menaces, sans étoffer leurs équipes.
- Permettre aux entreprises de mettre en place des programmes de sécurité extrêmement robustes, qui traitent des milliards de documents par jour et proposent des actions prioritaires toutes les 24 heures.

Mettre en place une sécurité intelligente

IBM QRadar Security Intelligence Platform fournit une suite hautement intégrée de solutions conçues pour aider les organisations à mettre en place une sécurité intelligente complète sur un système d'exploitation unifié et gérée grâce à une console unique.

Grâce à des outils SIEM robustes, cette plate-forme offre des fonctionnalités remarquables de sécurité intelligente, avec une palette d'applications de sécurité et de surveillance du réseau très performantes dans une solution unifiée. Ceci permet aux organisations de déployer des ressources de gestion de la sécurité et du réseau en fonction de l'analyse d'un lot complet de sources de données.

Cette plate-forme s'appuie sur le système d'exploitation IBM QRadar Security Intelligence Operating System, qui permet à IBM d'offrir un éventail de services communs d'intégration, de normalisation, d'entreposage, d'archivage et d'analyse des données. Grâce à cette structure unifiée, les fonctionnalités de workflow, de rapport, d'alerte et de tableau de bord sont homogènes. Elles prennent en charge les stratégies et processus dans toute l'organisation, identifient les menaces et évaluent les risques rapidement, tout en répondant aux besoins du personnel – audit, exploitation, encadrement et direction – en informations de sécurité et en réponse aux incidents.

Outre ses puissantes fonctionnalités SIEM et de gestion des journaux, la technologie IBM Security QRadar QFlow assure une surveillance étroite du réseau grâce à des fonctionnalités sophistiquées de détection d'anomalies. Ces fonctionnalités ajoutent un contexte enrichi aux analyses qui, sans cela, ne s'appuieraient que sur des données journalisées. La fonction de surveillance du réseau de QRadar QFlow collecte des informations dynamiques sur toutes les conversations au niveau de la couche applicative.

De plus, QRadar Security Intelligence Platform étend ses fonctionnalités de sécurité intelligente aux environnements de réseau virtuel grâce à sa technologie IBM Security QRadar VFlow, assurant ainsi un haut niveau de détection des menaces et de gestion des risques pour la consolidation des data centers et les initiatives de cloud public et privé.

Le module d'évaluation des risques IBM Security QRadar Risk Manager fournit un audit détaillé des configurations, avec un contexte de gestion des risques que les outils de SIEM sont incapables de fournir. Ce module évalue le risque et modélise les menaces potentielles visant les ressources stratégiques, en déterminant les chemins d'attaque possibles selon la valeur des données qu'elles contiennent.

QRadar Security Intelligence Operating System fournit une plate-forme permettant aux utilisateurs d'ajouter d'autres modules de sécurité qui répondent aux nouveaux enjeux de la sécurisation intelligente et de l'évaluation intelligente des risques pour l'infrastructure de l'entreprise. Ceci évite de gérer de nouvelles couches d'intégration de données, différents systèmes de stockage, de nouveaux moteurs d'analyse et plusieurs infrastructures de création de rapports pour prendre en compte les nouvelles applications de sécurité et sources de données potentielles.

Conclusion

Les organisations visionnaires ont pris conscience de la valeur de la BI. Leur réussite s'explique par leur capacité d'analyser et d'exploiter les informations essentielles extraites de volumes massifs de données. De même, la sécurité intelligente est essentielle, car la sécurité des informations fait partie intégrante du monde des affaires du XXIe siècle. Grâce à l'exécution de moteurs d'analyse puissants et automatisés sur des données centralisées issues de sources couvrant l'ensemble de l'infrastructure informatique, la mise en œuvre d'une sécurité de haut niveau à moindre coût est non seulement possible, mais indispensable.

Pour plus d'informations

Pour en savoir plus sur les offres IBM de sécurité intelligente, contactez votre représentant ou votre partenaire commercial IBM, ou visitez le site **ibm.com**/security.

De plus, IBM Global Financing (IGF) peut vous aider à acquérir les logiciels dont votre entreprise a besoin de façon plus rentable et stratégique. Nous nous associerons à des clients susceptibles de prétendre à un crédit pour personnaliser une solution de financement adaptée à votre entreprise et à vos objectifs de développement, mettrons en place une gestion efficace de la trésorerie et améliorerons votre coût total de possession. Financez vos investissements informatiques indispensables et propulsez votre entreprise vers l'avenir grâce à IGF. Pour en savoir plus, consultez le site : **ibm.com**/financing/fr/

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

La page d'accueil d'IBM est accessible à l'adresse suivante : **ibm.com**/fr.

[1] Jon Oltsik, « Research Report: U.S. Advanced Persistent Threat Analysis », Enterprise Strategy Group, 1er novembre 2011. http://www.esg-global.com/research-reports/research-report-us-advanced-persistent-threat-analysis/?keywords=advanced%20persistent

[2] Jon Oltsik, « Enterprise Information Security in Transition: An Opportunity for IBM », Enterprise Strategy Group, 15 octobre 2012. http://www.esg-global.com/briefs/enterprise-information-security-in-transition-an-opportunity-for-ibm/

[3] Verizon RISK Team, « 2012 Data Breach Investigations Report », *Verizon*, 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[4] Thomas Shanker, « Loophole May Have Aided Theft of Classified Data », *The New York Times*, 8 juillet 2010. http://www.nytimes.com/2010/07/09/world/09breach.html

Ces informations concernent les produits, programmes et services commercialisés par IBM France et n'impliquent aucunement l'intention d'IBM de les commercialiser dans d'autres pays.

Les références aux produits, programmes et services d'IBM n'impliquent pas que seuls ces produits, programmes et services peuvent être utilisés. Tout produit, programme ou service équivalent peut être utilisé.

Cette publication a uniquement un rôle informatif.
Ces informations peuvent faire l'objet de modifications sans préavis.
Contactez votre agence commerciale ou votre revendeur IBM pour obtenir les toutes dernières informations sur les produits et les services IBM.

Cette publication contient des adresses Internet autres que celles d'IBM. IBM ne peut pas être tenu responsable des informations publiées sur ces sites.

IBM ne donne aucun avis juridique, comptable ou d'audit et ne garantit pas que ses produits ou services soient conformes aux lois applicables. Il incombe aux clients de s'assurer que la législation et la réglementation applicables en matière de titres sont respectées, notamment au niveau national.

Les photographies présentées dans ce document peuvent représenter des maquettes.

Veuillez recycler

WGW03018-FRFR-00