Octobre 2016

Combattre les menaces avec des renseignements de sécurité et des contrôles des terminaux

Hiérarchiser les vulnérabilités et faciliter leur résolution avec IBM QRadar et IBM BigFix

IBM

Sommaire

Introduction

Depuis les logiciels malveillants personnalisés jusqu'aux exploits Zero day, les menaces évoluées contre la sécurité prolifèrent dans le monde entier avec des attaques d'une sophistication sans précédent. Aujourd'hui, les cybercriminels privilégient le repérage de leurs victimes au moyen d'attaques par e-mail ou par les sites web, mais aussi en exploitant les vulnérabilités des terminaux eux-mêmes. Vastes, coordonnées et opérationnellement sophistiquées, ces attaques sont aujourd'hui menées à grande échelle sur Internet en court-circuitant les mécanismes de sécurité traditionnels. Et la variété des logiciels malveillants ne cesse d'augmenter.

Comment les entreprises peuvent-elles garder une longueur d'avance face à ces menaces évoluées ? Il est essentiel de maintenir un haut niveau de sécurité de base en faisant respecter de manière constante les politiques de sécurité et en appliquant les correctifs aux terminaux et aux serveurs. Pour autant, lorsque l'analyse des réseaux indique d'innombrables vulnérabilités pour chaque adresse IP, la lenteur du processus d'atténuation et de correction de ces points faibles peut conduire à de dangereuses failles de sécurité. Aujourd'hui, le personnel informatique doit prendre des décisions difficiles en fonction des risques pour savoir sur quel domaine focaliser ses actions, mais souvent sans une vision complète de l'environnement de sécurité. La situation est encore plus critique lorsque le nombre de vulnérabilités à l'échelle de l'entreprise augmente alors quelle ne dispose que de ressources et de compétences limitées pour y répondre. Outre la capacité à détecter de manière efficace les vulnérabilités, une entreprise doit également prendre en considération leur contexte élargi et corréler ces vulnérabilités avec les niveaux de risque pour focaliser leur résolution sur les domaines porteurs des risques les plus importants.

Ce livre blanc explique comment combattre les menaces évoluées contre la sécurité en adoptant une approche intégrée, intelligente et automatisée de la sécurité des terminaux et des périphériques. Il montre également comment élargir le contexte et les capacités de la solution IBM® QRadar Security Intelligence Platform avec les fonctions de contrôle et de sécurité intelligente d'IBM BigFix pour identifier, hiérarchiser et limiter les risques pesant sur la sécurité. Ce livre blanc examine aussi l'intérêt stratégique d'une utilisation conjointe de ces solutions pour lutter contre les modes d'attaque les plus récents.

IBM QRadar Security Intelligence Platform

QRadar Security Intelligence Platform est la pierre angulaire pour aider les entreprises à lutter efficacement contre des attaques de plus en plus sophistiquées afin de préserver leurs environnements réseau, protéger leurs actifs de propriété intellectuelle et éviter les perturbations de leurs activités. Loin de se contenter de surveiller les journaux et les flux réseau, la solution collecte des données et des activités issues de très nombreuses sources et procède à des corrélations en temps réel avec des règles et des systèmes de veille sur les menaces pour identifier rapidement les attaques pouvant exiger une action immédiate.

Fondé sur la plateforme QRadar Security Intelligence, IBM QRadar Risk Manager permet de gérer de manière proactive les configurations des périphériques et de les corréler avec la topologie réseau pour analyser et identifier les risques de sécurité et les vulnérabilités ouvrant la voie à des attaques.

Également fondé sur la plateforme QRadar Security Intelligence Platform, IBM QRadar Vulnerability Manager constitue une approche efficace pour détecter les vulnérabilités des périphériques connectés au réseau. Le logiciel permet également de collecter et de consolider les résultats d'analyse issus de différents scanners de vulnérabilités. En s'appuyant sur la plateforme QRadar Security Intelligence et les données produites par QRadar Risk Manager, QRadar Vulnerability Manager peut jouer le rôle de point de contrôle centralisé pour la génération de rapports et la hiérarchisation des vulnérabilités pour l'ensemble d'une entreprise.

IBM BigFix pour la sécurité des terminaux

La protection la plus efficace contre les attaques de terminaux consiste à identifier les vulnérabilités des logiciels ou des configurations et de sécuriser les terminaux avant qu'un exploit ne puisse infliger des dommages à l'ensemble du réseau. À cet effet, la solution de sécurité et de gestion des terminaux BigFix permet de surveiller en permanence la configuration, les logiciels installés, les systèmes d'exploitation des terminaux ou la conformité des correctifs logiciels et de produire des rapports de conformité pour l'ensemble des appareils, et ce, qu'il s'agisse de règles standards ou personnalisées. BigFix permet également de résoudre rapidement les problèmes de conformité à l'aide de messages IBM Fixlet pour modifier l'état de la configuration d'un terminal, appliquer les correctifs appropriés, éliminer les logiciels malveillants ou stopper les processus suspects. Ce cycle permanent surveillance-rapport-résolution permet d'éliminer efficacement les fenêtres offrant des possibilités d'attaques.

Selon une étude réalisée en 2015 portant sur les détournements de données, près de la moitié des nouvelles vulnérabilités détectées ont été exploitées au cours des quatre premières semaines de leur signalement, car les pirates savent que la plupart des entreprises ne peuvent pas les corriger efficacement.[1] Une correction efficace reste donc la meilleure approche pour limiter le risque d'exploitation de vulnérabilités inédites par un logiciel malveillant. BigFix apporte un processus de correction automatisé, simplifié et efficace pour l'ensemble des terminaux, connectés ou non au réseau, et ce, pour différents systèmes d'exploitation et applications. La mise en œuvre des correctifs avec BigFix permet de réduire significativement les temps du cycle de correction et de réduire considérablement les coûts d'exploitation.

Pour les vulnérabilités temporairement dépourvues de correctifs (Zero-day), BigFix apporte une fonction de mise en quarantaine à distance pour isoler du réseau les terminaux, ce qui permet de les protéger des attaques et d'éviter d'en infecter d'autres jusqu'à ce qu'un correctif ou une autre solution soit disponible.

Résoudre les lacunes de la gestion des vulnérabilités

Pour se protéger des menaces contre la sécurité, les entreprises ont besoin d'une approche complète pour identifier et limiter les risques les plus prioritaires dans un environnement informatique en évolution constante. Cette approche doit comporter les actions suivantes :

- Connaître l'état instantané des différents terminaux.
- Identifier les vulnérabilités de chaque terminal.

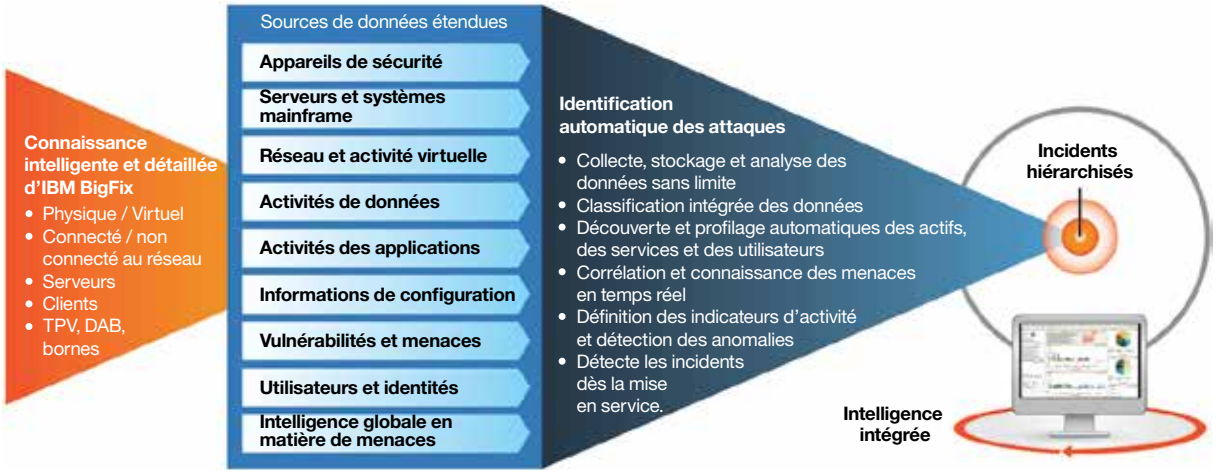
- Hiérarchiser les vulnérabilités.
- Mettre rapidement en œuvre des actions pour résoudre ou limiter les vulnérabilités les plus prioritaires des terminaux ou mettre en quarantaine les appareils.
- Confirmer que l'action corrective a permis d'obtenir un état plus sécurisé du terminal.

La plupart des solutions de gestion des vulnérabilités se focalisent sur l'identification et la hiérarchisation des vulnérabilités, mais sans l'intelligence et les capacités nécessaires pour résoudre efficacement les vulnérabilités en fonction de leurs priorités. D'où l'intérêt de l'offre d'IBM qui permet aux entreprises de résoudre ces lacunes dans la gestion des vulnérabilités en conjuguant les capacités de BigFix et celles de la plateforme QRadar Security Intelligence Platform. En effet, grâce à cette solution intégrée, il est possible d'identifier et de hiérarchiser les vulnérabilités des systèmes d'exploitation ou des applications exploitées par les attaquants, puis de les résoudre pour éviter ou minimiser l'impact sur l'entreprise.

Établir une gestion du risque en boucle fermée intégrant un contrôle intelligent des périphériques et des terminaux

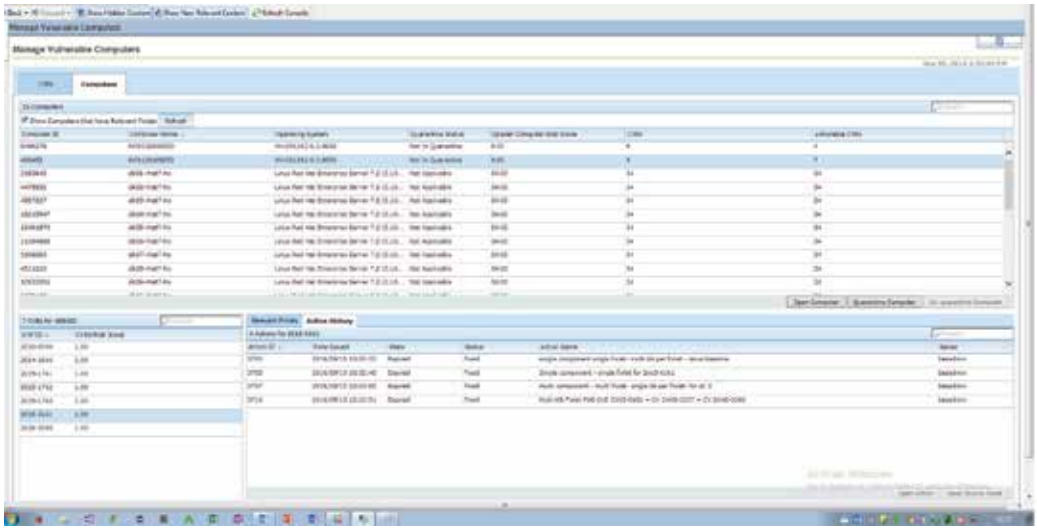
Face à l'évolution vers des menaces évoluées de plus en plus furtives, dynamiques et nuisibles, il n'a jamais été aussi essentiel de disposer de ressources intégrées, intelligentes et automatisées. Une solution intégrée associant QRadar Security Intelligence Platform et BixFix apporte aux équipes chargées des opérations et de la sécurité informatiques les moyens nécessaires pour protéger ensemble les actifs face à des attaques de plus en plus sophistiquées.

BigFix apporte à la plateforme QRadar Security Intelligence des informations détaillées en quasi temps réel sur l'état des terminaux, notamment grâce aux rapports sur les correctifs appliqués et les changements récents de configuration, ce qui permet d'améliorer la fiabilité de l'analyse des risques du système. Pour être plus précis, l'agent BigFix installé sur un terminal connecté ou non au réseau de l'entreprise, évalue en permanence la conformité aux règles de configuration et d'application des correctifs logiciels. Il peut ainsi adresser l'état le plus récent à QRadar, qui, à son tour, corrèle cet état avec d'autres événements relatifs à la sécurité ou les activités réseau pour repérer les incidents suspects.



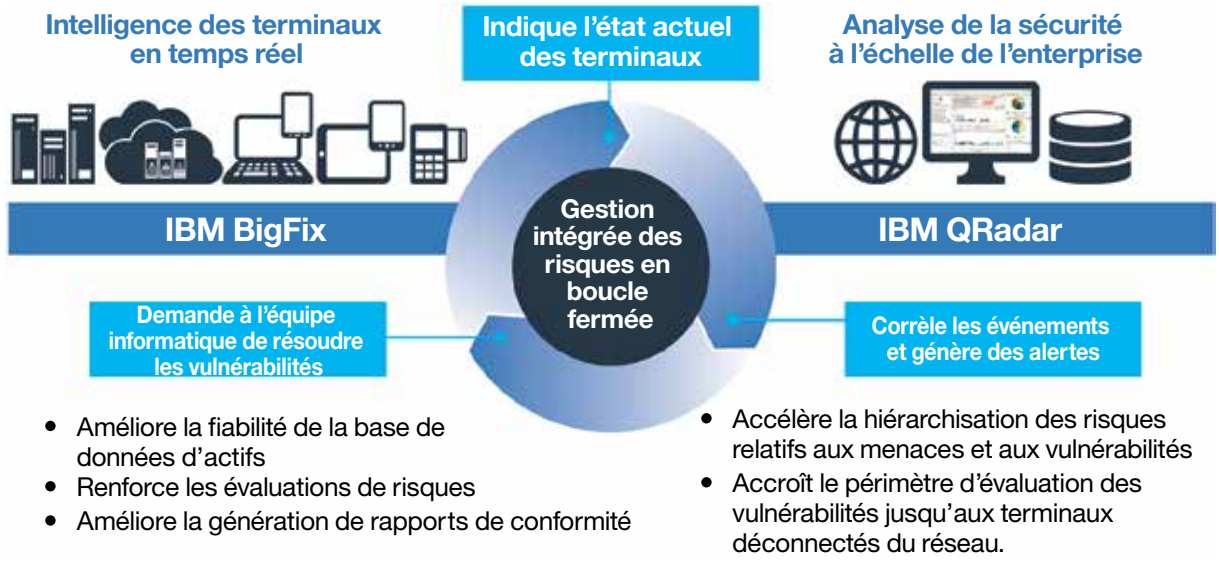
IBM BigFix adresse les états les plus récents des terminaux à IBM QRadar, qui les corrèle avec les événements de sécurité pour repérer et hiérarchiser les incidents suspects.

QRadar Vulnerability Manager permet d'analyser les vulnérabilités, ou de les collecter auprès de BigFix et d'autres scanners de terminaux. Chaque actif se voit ensuite affecter un score de risque en fonction de la corrélation avec le contexte élargi obtenu à l'aide de QRadar Risk Manager, qui englobe la topologie du réseau et les activités de communication. Les vulnérabilités et les scores de risques relatifs à l'actif sont ensuite adressés à BigFix. Pour chaque vulnérabilité détectée par QRadar, BigFix peut identifier les actions de résolution appropriées (correctif logiciel ou mise en quarantaine) que l'équipe informatique doit mettre en œuvre. En outre, l'équipe informatique peut hiérarchiser les actions de résolution en conjuguant le score de risque de l'actif, le nombre de vulnérabilités pour chaque terminal ou les résolutions possibles, ce qui permet d'apporter très en amont une solution aux vulnérabilités les plus critiques.



IBM BigFix peut résoudre efficacement les vulnérabilités identifiées par QRadar Vulnerability Manager et génère différents indicateurs pour aider les clients à hiérarchiser leurs actions de résolution.

Une fois l'action de résolution mise en œuvre, l'état du terminal est renvoyé à QRadar, qui le corrèle de nouveau avec les événements de sécurité ou les activités réseau, ce qui permet d'actualiser les incidents déjà signalés. En associant les capacités de contrôle et de sécurité intelligente des terminaux qu'apporte BigFix avec l'approche intelligente de la sécurité à l'échelle de l'entreprise de QRadar, une entreprise peut établir un programme permanent de gestion en boucle fermée du risque pour lutter avec efficacité contre les menaces pesant sur la sécurité.



Ensemble, IBM BigFix et IBM QRadar constituent un système de gestion du risque en boucle fermée doté d'une gestion intelligente et en temps réel des terminaux et d'outils d'analyse de la sécurité à l'échelle de l'entreprise.

Conclusion

Pour assurer une gestion plus efficace des vulnérabilités, les entreprises ont besoin d'une approche intégrée englobant une connaissance intelligente des terminaux et les informations relatives au contexte du réseau. Parallèlement, les équipes informatiques ont besoin de déterminer les plannings de correction des vulnérabilités au moyen d'un système de gestion des terminaux, en distinguant les correctifs nécessaires de ceux qui ne le sont pas, et s'assurer ainsi que les actions de résolution sont efficacement hiérarchisées. En outre, le personnel informatique doit rapidement mettre en œuvre des actions pour une sécurité plus intelligente et procéder aux mises à jour nécessaires sur tous les terminaux de l'entreprise.

D'où l'intérêt des solutions QRadar et BigFix qui peuvent travailler de concert pour permettre aux entreprises de garder une longueur d'avance sur les menaces les plus évoluées. Cette approche intelligente, automatisée et intégrée a un intérêt stratégique car elle permet une gestion consolidée et une utilisation efficace des ressources de sécurité. Il est possible de rationaliser les délais de réponse aux incidents, notamment le temps entre l'apparition de la vulnérabilité et sa détection, en conjuguant les détails de l'état des terminaux, disponibles en quasi temps réel avec BigFix, et la sécurité intelligente des solutions QRadar qui permettent de réaliser la synthèse de millions d'événements de sécurité, présentée sous la forme d'une liste exploitable et hiérarchisée de points faibles. Les entreprises peuvent ainsi adopter une approche proactive pour renforcer leurs ressources informatiques face aux menaces les plus persistantes, avec, à la clé, une réduction significative des risques.

La sécurité nationale exige une gestion en temps réel de la conformité des terminaux et des périphériques

Les agences fédérales américaines sont confrontées à d'innombrables menaces contre la sécurité, ce qui a suscité la mise en place d'obligations légales conduisant au déploiement de solutions capables de surveiller, gérer et limiter en permanence les vulnérabilités. D'où l'intérêt exceptionnel de l'intégration des solutions QRadar et BigFix pour les agences fédérales américaines.

À cet effet, une solution de cybersécurité d'entreprise peut aider les organismes gouvernementaux à lutter contre les menaces et éliminer les vulnérabilités. À titre d'exemple, plus de 50 organismes fédéraux américains ont standardisé la mise en œuvre de BigFix pour gérer et sécuriser plus de 3 millions de postes de travail, de serveurs (physiques et virtuels) et d'autres terminaux englobant un très grand nombre de stations. Ces solutions assurent la sécurité et la conformité en temps réel et en continu des terminaux et des périphériques en s'appuyant sur une bibliothèque contenant plusieurs milliers de vérifications.

Pour plus d'informations

Pour en savoir plus sur les solutions IBM QRadar Security Intelligence Platform, IBM BigFix ou les autres solutions IBM Security, contactez votre représentant IBM ou votre partenaire commercial IBM, ou consultez le site à l'adresse suivante : **ibm.com**/security/fr-fr/

À propos des solutions IBM Security

IBM Security propose l'une des gammes les plus évoluées et les mieux intégrées de produits et de services de sécurité pour l'entreprise. Issues de l'équipe IBM X-Force, division de recherche et de développement d'IBM connue dans le monde entier, les solutions de sécurité intelligente permettent de protéger de manière globale le personnel, les infrastructures, les données et les applications des entreprises, en proposant notamment des offres de gestion des identités et des accès, de sécurité des bases de données, de développement d'applications, de gestion du risque, de gestion des périphériques et des terminaux, et de sécurité des réseaux. Ces offres permettent aux entreprises de gérer plus efficacement les risques et de mettre en œuvre des solutions de sécurité intégrées pour les mobiles, le Cloud, les médias sociaux et d'autres architectures d'entreprise. IBM dispose de l'une des plus vastes entités au monde pour la recherche, le développement et la mise en œuvre de solutions de sécurité pour l'entreprise, surveille 15 milliards événements de sécurité par jour dans plus de 130 pays et détient plus de 3 000 brevets relatifs à la sécurité.

En outre, IBM Global Financing vous propose différentes options de financement pour vous aider à acquérir la technologie nécessaire pour développer votre activité. Nous assurons la gestion complète du cycle de vie des produits et des services informatiques, depuis l'achat jusqu'à la cession. Pour en savoir plus, visitez le site : **ibm.com**/financing/fr

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

[1] « 2015 Data Breach Investigations Report », *Verizon*, avril 2015. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Veuillez recycler

WGW03051-FRFR-02