WHITEPAPER

Q1 Labs®
Total Security Intelligence | An IBM Company

ÉTAPES CONCRÈTES

Pour la protection des données de votre organisation

Rôle stratégique de la veille sécuritaire et de la protection des informations dans le développement de vos activités

UNE TÂCHE HERCULÉENNE POUR LES PDG, DIRECTEURS INFORMATIQUES, DIRECTEURS TECHNIQUES ET DIRECTEURS DE LA SÉCURITÉ DES INFORMATIONS - mettre en place des programmes qui couvrent les personnes, les technologies et les processus, afin de minimiser le « risque ». Le terme « risque » aura une signification différente selon les responsabilités d'un individu et le secteur dans lequel il travaille. Du point de vue de la sécurité des informations, l'une des principales préoccupations des fonctions de haute direction, des cadres informatiques et des professionnels de la sécurité est de réduire le risque d'accès non autorisé aux informations. La protection de vos actifs contre le cyberespionnage industriel exige une stratégie descendante.

Synthèse générale

La plupart des professionnels de la sécurité conviennent que la maturité du programme de sécurité des informations d'une organisation est directement proportionnelle à sa capacité de protéger les informations. Ce livre blanc présente cinq étapes concrètes pour la protection des données d'une organisation, ainsi que des conseils pour l'implémentation d'un programme complet et bien conçu de sécurité des informations. Ces étapes reposent sur la somme des connaissances acquises auprès des nombreux clients internationaux de Q1 Labs, notamment concernant les méthodes de référence.

Principales causes des intrusions

Il existe bien sûr de nombreuses statistiques et rapports établis par des sociétés d'analyse sectorielle qui couvrent les causes des accès non autorisés aux informations des entreprises. Quant aux données ici reprises, elles sont tirées de situations réelles et des expériences de clients Q1 Labs ayant implémenté QRadar pour la veille sécuritaire.

Principales causes des intrusions dans les réseaux des entreprises:

1.) L'organisation n'a pas investi dans une technologie de sécurité des informations (ce qui inclut notamment les commutateurs, les pare-feu, les systèmes de protection contre les intrusions, les réseaux privés virtuels, les systèmes de contrôle de la vulnérabilité et les systèmes de gestion des identités et de l'accès).

2.) L'organisation n'a pas mis en place un processus de veille sécuritaire suffisant pour son réseau.

3.) L'organisation n'exploite pas correctement la technologie de sécurité des informations dont elle dispose. Par exemple, les dispositifs réseau et de sécurité sont mal configurés.

4.) L'organisation n'a pas corrigé les principales vulnérabilités de son infrastructure.

5.) L'organisation ne peut pas efficacement minimiser les risques à cause d'un cloisonnement organisationnel et / ou technologique.

Il est vrai que la prise en charge de ces différents problèmes exige du temps. Certaines organisations mettent des années à les maîtriser dans leur intégralité. La bonne nouvelle est que même une amélioration mineure de la sécurité engendre une importante amélioration de la capacité à protéger les informations.

Cinq étapes concrètes de veille sécuritaire pour la protection de votre organisation contre les intrusions

Parvenir à un système mature de sécurité opérationnelle prend du temps et exige un suivi et une évolution constants. Cela étant dit, voici cinq renforcements de la sécurité à envisager pour améliorer de façon significative la capacité d'une organisation à se protéger contre les intrusions.

ÉTAPE 1 : Déployer la technologie adéquate

L'énumération de toutes les technologies de sécurité des informations à envisager par une organisation dépasse le cadre de notre propos. Néanmoins, quelques principes fondamentaux ne peuvent être ignorés. Les organisations doivent privilégier le déploiement de technologies qui répondent aux besoins suivants.

- **Contrôle du flux des informations au travers du réseau.**

Cela est possible par la simple implémentation de quelques pare-feu, ou peut exiger l'utilisation de passerelles plus avancées telles que les systèmes de protection contre les intrusions (IPS, Intrusion Protection System) ou des commutateurs (avec couche applicative adaptée). Le plus

souvent, le déploiement de ces technologies s'effectuera au travers de différentes couches.

- **Contrôle de l'accès aux informations.**

Un tel contrôle est généralement mis en place au travers d'un système centralisé d'authentification. Pour certaines organisations toutefois, des fonctionnalités de gestion plus avancées peuvent être nécessaires.

- **Mesures de bon sens pour la protection des environnements de production, notamment les antivirus, la prévention de la perte de données, la prévention des intrusions sur serveurs et le suivi de l'intégrité des fichiers.**

Beaucoup d'organisations sont depuis longtemps dotées de ce type de protections. Celles-ci doivent néanmoins être régulièrement réévaluées afin de vérifier qu'elles répondent toujours aux besoins de l'entreprise.

- **Visibilité de la situation en matière de sécurité.**

La technologie fondamentale requise ici est une solution centralisée de gestion des journaux et / ou de gestion des informations et incidents de sécurité (SIEM, Security Information and Event Management) qui intègre d'origine des fonctionnalités de détection des anomalies et de capture de contenus.

- **Cryptage des informations chaque fois que nécessaire.**

Les organisations peuvent faire appel à un réseau privé virtuel pour répondre à ce besoin.

- **Détection des failles de l'infrastructure de sécurité.**

Pour ce faire, un ou plusieurs systèmes de contrôle de la vulnérabilité seront généralement nécessaires, le cas échéant complétés d'autres outils.

- **Besoins avancés de sécurité, notamment la prévention de la perte de données.**

Pour répondre à ces besoins, il convient de déployer des technologies avancées permettant un processus de veille sécuritaire complet, avant, pendant et après un incident.

En dernière analyse, ce sont les besoins dictés par l'activité qui détermineront les technologies déployées et la mesure dans laquelle celles-ci sont exploitées. Un enseignement majeur tiré de l'expérience des clients Q1 Labs est que très souvent, l'exploitation de la conformité crée un budget permettant d'investir dans des technologies de sécurité qui se révéleront payantes au final, pour autant qu'une réflexion suffisante soit menée pour la sélection des technologies adéquates et leur implémentation.

ÉTAPE 2 : Exploiter les informations à votre avantage

Après avoir collaboré avec plus de 1 600 clients, Q1 Labs sait que plus le volume des données réseau analysées par une organisation est important, meilleure est la capacité de cette dernière à minimiser et quantifier le risque pesant sur ses informations. Le prérequis fondamental pour ce faire est bien évidemment de déployer une solution capable d'efficacement donner un sens à l'ensemble des données collectées. Les besoins des organisations pour la collecte et l'analyse des informations sont variables.

Au minimum, une gestion élémentaire des journaux peut être nécessaire afin de gérer le risque pour les informations d'une seule application, comme l'exigent certaines réglementations. Au maximum, une solution complète de veille sécuritaire qui examine sans exception les événements de tous les systèmes du réseau sera requise.

Lors de la sélection d'un système de gestion des journaux, d'un système de gestion des informations et incidents de sécurité et / ou d'une solution complète de veille sécuritaire, certaines considérations importantes s'imposent.

- **Simplicité de l'acquisition, du déploiement et de la maintenance de la technologie.**

Cela peut paraître évident mais il est tout à fait surprenant de constater combien d'organisations retiennent des solutions qui exigent une armada de personnel et de services professionnels. Cherchez-vous à lancer un véritable projet scientifique?

- **Normalisation et classification des informations par la solution.**

Cet aspect est fréquemment négligé lors de l'évaluation d'un système de gestion des informations et incidents de sécurité. Il s'agit peut-être du plus important. Les données des événements réseau sont réellement complexes. Pourquoi voudriez-vous d'une solution incapable d'offrir une classification commune pour l'ensemble des données collectées ?

- **Sécurité de la collecte, du stockage et de l'archivage des journaux.**

Ces fonctionnalités devraient être considérées comme obligatoires pour toute solution de veille sécuritaire.

- **Réduction de milliards d'événements à l'évaluation de quelques incidents de sécurité, dont la détection est réellement utile et sur lesquels vous pouvez agir.**

Dies kann schwierig sein, da angeblich jede Lösung eine detaillierte Einschätzung des Sicherheitsstatus bietet. Viele

Korrelierungsmaschinen scheitern jedoch, da sie sich nur die Daten in einem einzigen Silo ansehen – sie korrelieren nicht zwischen den Datensilos (Anwendungen, Nutzeridentität, Assets, Inhalt etc.), oder sie gehen nicht tief genug oder sind nicht umfassend genug was die benötigten Daten betrifft, um Vorfälle richtig zu erkennen.

- **Simplicité de la personnalisation de la solution afin de répondre aux besoins opérationnels uniques de l'organisation, notamment pour l'analyse des données de sources uniques ou personnalisées?**

Les organisations qui évaluent des solutions de veille sécuritaire doivent veiller à répondre à leurs besoins de collecte des données à court et long terme.

- **Extensibilité de la solution.**

Les besoins en termes d'extensibilité sont variés. Ils vont de l'augmentation du nombre d'événements pour un centre de données à la prise en charge d'un environnement distribué. Il importe de disposer d'une solution extensible, qui évolue sans pour autant introduire une complexité inutile.

Les cas d'utilisations réussies de systèmes de gestion des journaux et de systèmes de gestion des informations et incidents de sécurité sont innombrables. Les organisations qui utilisent leurs données et informations à leur avantage via une solution efficace de gestion de la sécurité se trouvent en bien meilleure posture afin de minimiser le risque d'intrusion pour leur réseau.

ÉTAPE 3 : Veiller en permanence à la configuration adéquate des dispositifs afin d'anticiper les menaces

Une configuration toujours adéquate des dispositifs, voilà qui semble formidable. Dans la réalité, cependant, la tâche peut relever du défi. Les principes fondamentaux à respecter sont ici très simples : assurez-vous du verrouillage de tous les ports du réseau, excepté aux points nécessaires compte tenu des besoins spécifiques de l'activité. Pour ce faire, vous devez être en mesure d'évaluer l'efficacité des configurations déployées sur le réseau. Des solutions automatisées d'audit des configurations existent pour vous y aider. Dans ce domaine, la performance de certaines fonctionnalités ne doit pas être négligée lors de l'évaluation des outils:

- Automatisation de la collecte des configurations
- Préservation de la cohérence des configurations pour différents types de dispositifs, et le cas échéant pour différents fournisseurs
- Interprétation du flux du trafic sur le réseau en fonction des configurations et simplicité d'analyse et de compréhension
- Image précise de la configuration réseau, même lorsque des dispositifs sont mal configurés ou que des données manquent
- Automatisation rapide du suivi et de la notification des changements de configuration risqués

L'objectif essentiel pour cette étape est de rechercher des outils qui contribuent à réduire les obstacles à l'analyse efficace de configurations complexes et offrent des fonctionnalités d'automatisation exceptionnelles capables de rapidement déceler les modifications risquées de configuration et de les notifier.

ÉTAPE 4 : Veiller à corriger les principales vulnérabilités

Les systèmes de contrôle de la vulnérabilité sont devenus un outil important pour les administrateurs de systèmes de sécurité afin de s'assurer que les dispositifs du réseau ne sont pas exposés suite à des vulnérabilités parfaitement connues. Historiquement, ces outils ont pu poser quelques problèmes, généralement parce qu'ils signalent les vulnérabilités sans les accompagner du contexte propre au dispositif concerné. Cela peut donner lieu à de nombreuses fausses alertes et à une surcharge d'informations. Il ne fait aucun doute que les systèmes exposés à des vulnérabilités bien connues constituent les cibles privilégiées des attaques malveillantes. Les organisations qui souhaitent s'assurer de la correction des principales vulnérabilités doivent chercher à élargir leurs possibilités, grâce à des solutions qui offrent les fonctionnalités suivantes:

- Normalisation efficace des vulnérabilités selon un cadre commun
- Évaluation du risque de vulnérabilités en conjonction avec la configuration spécifique du réseau. Il importe de pouvoir classifier les systèmes, précisément en fonction de leur vulnérabilité propre.
- Analyse des vulnérabilités sous différents angles, y compris grâce aux résultats de différents systèmes de contrôle des vulnérabilités, de l'analyse passive des vulnérabilités et de l'analyse du comportement des utilisateurs.

- Automatisation de la détection des modifications de configuration du réseau qui introduisent de nouvelles vulnérabilités potentielles.

Il importe ici, non pas d'examiner les vulnérabilités de manière isolée, mais bien d'adopter une approche plus globale des risques via une analyse beaucoup plus pertinente du réseau et de la sécurité.

ÉTAPE 5 : Implémenter un référentiel de veille sécuritaire intégré fondé sur la gestion du risque

Grâce à son expérience de longue date, Q1 Labs comprend les difficultés rencontrées par de nombreuses entreprises afin de parvenir à la visibilité requise sur la sécurité de leurs informations, suite à un cloisonnement organisationnel et / ou technologique. La règle pour la plupart des solutions de gestion de la sécurité est que plus celles-ci reçoivent d'informations, plus l'organisation est à même de détecter et de minimiser les risques. Vaincre le cloisonnement exige fréquemment des modifications d'ordre organisationnel et / ou opérationnel. Mais en dernière analyse, lorsque la main droite apprend enfin ce que fait la main gauche, l'amélioration obtenue peut être considérable et des économies peuvent de plus être réalisées grâce à la consolidation des données. Les organisations qui souhaitent introduire un référentiel intégré de veille sécuritaire doivent rechercher une solution qui offre les fonctionnalités suivantes :

- Réduction des silos technologiques par l'intégration et l'analyse d'un large spectre d'informations, notamment les données des réseaux, des réseaux virtuels, des actifs, et des applications, ainsi que les données relatives à la sécurité, aux vulnérabilités et à la configuration.
- Réduction des silos opérationnels et fonctions de sécurité répondant le mieux aux besoins d'un large spectre d'utilisateurs, notamment les opérateurs, les analystes, les auditeurs et les cadres.
- Classification des risques d'incident sur base de l'impact global sur les activités
- Détection et notification automatisées des nouveaux risques introduits sur le réseau
- Référentiel intégré de veille sécuritaire pour l'évaluation des risques afférents à l'ensemble des informations pertinentes

L'essentiel dans cette étape est de comprendre que l'objectif premier de la veille sécuritaire est de disposer du contexte et de corréler ces informations avec celles de l'ensemble du processus de veille sécuritaire. Une solution de veille sécuritaire doit permettre à l'organisation de répondre aux questions suivantes:

- Quels sont les risques qui menacent l'organisation et comment ceux-ci peuvent-ils être réduits ou prévenus?
- Que se passe-t-il à un moment donné et comment détecter les menaces sur base des renseignements disponibles et grâce à la visibilité sur la situation?
- Comment déterminer ce qu'il s'est passé après un incident et comment comprendre l'impact ou les coûts à l'aide des analyses afin de déterminer comment un incident s'est propagé ou ce qui a été volé ?

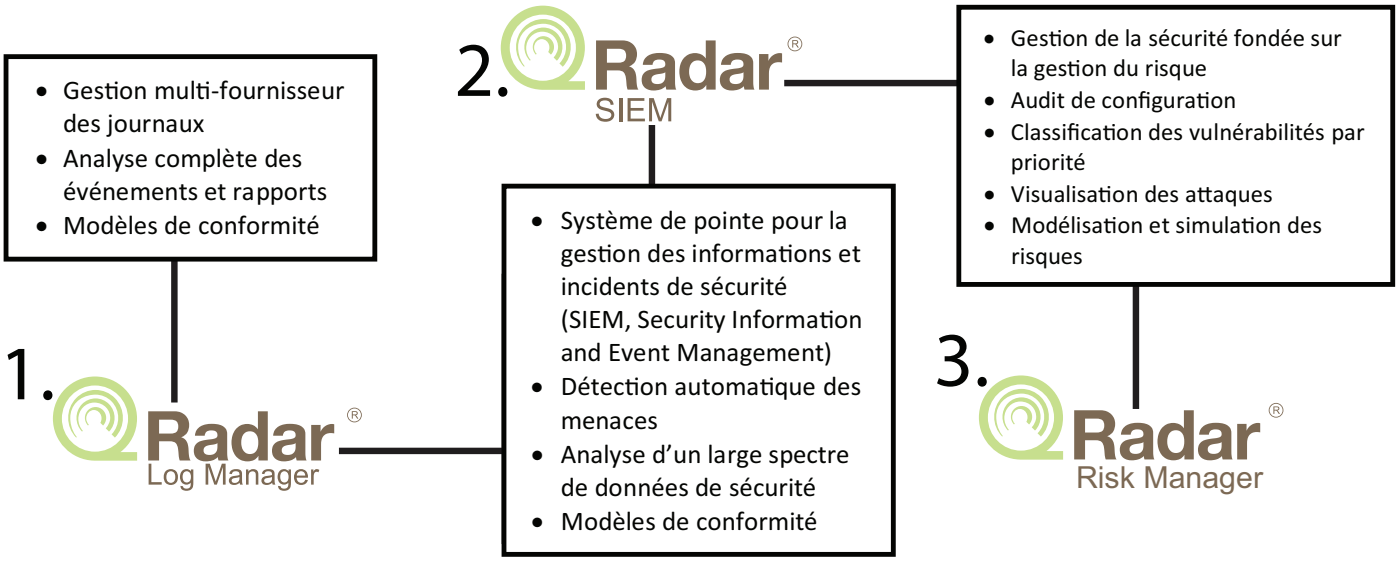
ÉTAPES SUIVANTES

Les cinq étapes ci-dessus reprennent de nombreuses considérations sur la manière de construire un programme plus mature pour la gestion de la sécurité des informations. Un élément important consiste à travailler avec un partenaire capable de fournir une solution de veille sécuritaire qui répond aux besoins de l'organisation où qu'elle se trouve dans son évolution vers une approche complète fondée sur la gestion du risque.

Plateforme de veille sécuritaire QRadar® de Q1 Labs

Q1 Labs propose une gamme de solutions de veille sécuritaire qui assistent les organisations de toutes tailles opérant dans de nombreux secteurs afin de répondre à un large spectre de besoins en matière de sécurité des informations. De plus, la plateforme de veille sécuritaire QRadar® offre une gamme de produits à l'épreuve de l'avenir qui permet aux organisations de développer leur approche de veille sécuritaire en parallèle avec leur programme spécifique de sécurité des informations. Le schéma ci-dessous donne un aperçu général de la plateforme de veille sécuritaire QRadar et des produits choisis par beaucoup de nos clients afin de répondre à leurs exigences croissantes en matière de sécurité :

CINQ ÉTAPES CONCRÈTES POUR LA PROTECTION DES DONNÉES DE VOTRE ORGANISATION



Mode de transition de nos clients de la gestion des journaux à la veille sécuritaire

Grâce aux solutions de veille sécuritaire de Q1 Labs, les organisations peuvent efficacement développer leur programme de sécurité des informations afin de répondre à de nombreux besoins évoqués plus haut en disposant de la solution la plus intelligente, la plus intégrée et la plus automatisée actuellement disponible.

1.) Gestion extensible des journaux à l'échelle de l'entreprise

- Centralisation de la collecte et du stockage sécurisé des événements et journaux pour l'ensemble d'une organisation et tous ses fournisseurs
- Respect aisé des réglementations
- Visibilité des données des journaux permettant d'agir et d'exploiter les analyses de sécurité
- Mise à niveau aisée grâce à un processus à l'épreuve de l'avenir pour la migration vers une solution complète de gestion des informations et incidents de sécurité

2.) Grande visibilité grâce au système de gestion des informations et incidents de sécurité (SIEM)

- Capacité d'améliorer l'efficacité des investissements d'infrastructure grâce à des analyses avancées et à des informations sur le comportement des utilisateurs et la sécurité
- Visibilité complète de la situation de l'organisation vis-à-vis de la sécurité des informations afin de détecter les menaces
- Réduction de milliards d'événements à une liste d'incidents de sécurité à examiner, avec indication du niveau de priorité
- Détection automatisée de menaces passant généralement inaperçues pour les solutions qui n'intègrent pas les silos opérationnels et technologiques

3.) Gestion complète de la sécurité fondée sur la gestion du risque

- Collecte automatisée des configurations du réseau et de l'infrastructure de sécurité
- Détection rapide des configurations risquées introduites
- Classification puissante des risques par priorité, qui exploite un large spectre d'indicateurs de risque, notamment l'activité réseau, la topologie réseau et les résultats du système de contrôle des vulnérabilités
- Modélisation et simulation avancées des menaces

Synthèse : considérations à prendre en compte pour l'établissement d'une stratégie à long terme

De nombreuses considérations couvrant les personnes, les processus et les technologies doivent être prises en compte par les organisations afin d'améliorer leur capacité à protéger leurs informations, qui constituent pour elles de précieuses ressources. Déjà penser à la ligne d'arrivée alors qu'elles viennent tout juste d'entrer dans la course peut paraître insurmontable pour les organisations de toutes tailles. Lors de la planification d'une stratégie à long terme, il importe de comprendre que chaque amélioration, si mineure soit-elle, apportée à un programme de sécurité, s'avérera largement payante pour autant qu'une réflexion suffisante soit accordée à la définition, la planification et l'implémentation de cette amélioration. L'expérience acquise par Q1 Labs auprès de ses clients révèle quelques étapes éprouvées qui permettent de réduire considérablement le risque d'accès non autorisé aux informations d'une entreprise :

- Déployer des technologies réseau et de sécurité suffisantes qui contrôlent correctement l'accès aux informations sensibles
- Implémenter une solution efficace de gestion des journaux et / ou de gestion des informations et incidents de sécurité (SIEM) capable d'exploiter un large spectre de données de sécurité afin de suivre, détecter et corriger les incidents de sécurité importants
- Adopter une approche proactive de la gestion de la sécurité basée sur la gestion du risque capable de minimiser les configurations risquées du réseau et les vulnérabilités du système

L'existence d'individus mal intentionnés prêts à tout pour voler des informations intéressantes aux organisations vulnérables est aujourd'hui bien réelle. Les entreprises qui exploitent des solutions de veille sécuritaire afin de développer leur programme de sécurité au travers des différentes méthodes décrites ci-dessus sont clairement moins vulnérables face à ces attaques malveillantes, que celles-ci soient d'origine interne ou externe à l'organisation.

Q1 Labs, an IBM Company
890 Winter Street, Suite 230
Waltham, MA 02451 USA
1.781.250.5800, info@Q1Labs.com

WPFSPABFL0312