Q1 Labs®
Total Security Intelligence

Plateforme de veille sécuritaire QRadar

Quelle que soit l'envergure d'une entreprise, la veille sécuritaire s'impose de plus en plus comme incontournable. La masse des réglementations à respecter ne cesse de croître et la protection des données est un défi permanent. À cela s'ajoute une croissance exponentielle du volume de données généré par des utilisateurs et des dispositifs toujours plus nombreux. À défaut d'une approche novatrice permettant de conserver la maîtrise de cette masse d'informations, une entreprise peut développer certaines vulnérabilités. C'est pourquoi une solution de veille sécuritaire n'est pas simplement un plus ; c'est une nécessité incontournable.

Une maîtrise et une visibilité optimales face aux défis sécuritaires actuels

Q1 Labs est un fournisseur international de produits de veille sécuritaire de nouvelle génération, économiques et à forte valeur ajoutée. Le produit phare de la société, la QRadar Security Intelligence Platform, intègre des fonctions auparavant séparées, par exemple la gestion des informations et incidents de sécurité (GIIS), la gestion du risque, la gestion des journaux et l'analyse réseau. Cette solution complète de veille sécuritaire est tout simplement la plus intelligente, la plus intégrée et la plus automatisée disponible sur le marché. QRadar vous offre une visibilité cruciale sur les opérations effectuées via vos réseaux, centres de données et applications, pour une meilleure protection de vos actifs informatiques et un meilleur respect des réglementations.

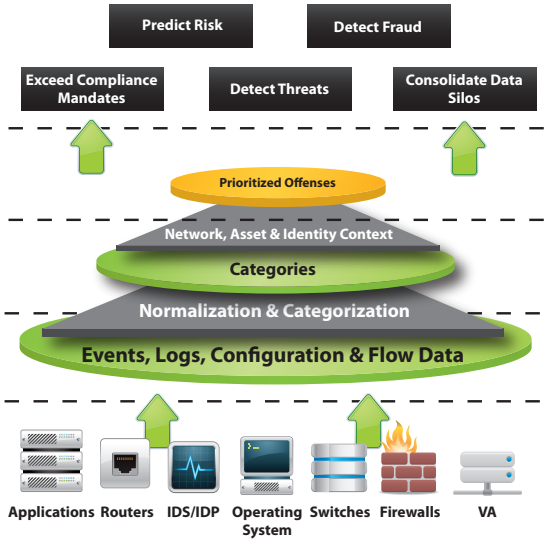
Plus de 1 600 entreprises ont choisi QRadar, la solution de veille sécuritaire la plus intelligente, la plus intégrée et la plus automatisée disponible sur le marché.

Détection d'un plus grand nombre de menaces

Les menaces et les attaques liées à Internet se font de plus en plus sophistiquées. Les données d'une organisation renferment des renseignements qui permettent de détecter des problèmes graves. Il peut par exemple s'agir d'employés subtilisant des informations exclusives et confidentielles, d'espionnage industriel ou encore d'un réseau d'ordinateurs zombies tentant de pénétrer dans un système pour subtiliser les informations de cartes de crédit. QRadar vous aide à identifier les attaques à prendre au sérieux contre vos données d'entreprise et à détecter les anomalies dans le comportement de vos utilisateurs ou dans l'utilisation de vos applications et réseau(x).

Regroupement des réserves de données

De nombreuses entreprises génèrent des millions voire des milliards d'enregistrements et d'incidents chaque jour, et les données des incidents et journaux générés par leurs dispositifs réseau recèlent une foule d'informations. Malheureusement, ces dernières résident fréquemment dans des réserves de données, souvent ignorées et toujours sous-exploitées. QRadar fait converger les fonctionnalités de visualisation précédemment séparées de l'activité réseau, des paramètres de sécurité et des opérations effectuées offertes par votre infrastructure informatique, au sein d'une plateforme de veille sécuritaire intelligente



Mise en oeuvre de la Total Security Intelligence

et extensible. Vous êtes ainsi en mesure de rapidement réagir en cas de problème, et d'extraire les informations réseau et de sécurité pertinentes jusqu'au niveau des applications et utilisateurs, pour une résolution plus efficace face à des menaces réseau et à des infractions aux règles.

Détection des fraudes internes

Certaines des plus importantes menaces peuvent provenir de l'intérieur même des entreprises. Ces dernières ne disposent toutefois fréquemment pas des renseignements nécessaires pour établir précisément le lien entre les coupables et les malversations constatées. Grâce au suivi des utilisateurs et des applications, les organisations peuvent établir quel est le comportement habituel des utilisateurs afin de faciliter l'identification des comportements anormaux ou risqués ainsi que des vulnérabilités.

Prévision des risques en fonction de votre activité

Les équipes informatiques et de sécurité sont en permanence confrontées au défi de la gestion du risque et de la prévention des attaques, compte tenu de vulnérabilités toujours plus diverses. QRadar est aussi une solution préventive. Elle permet non seulement d'évaluer les risques en présence pendant et après une attaque, mais également de répondre à de nombreuses questions avant tout incident, ce qui peut énormément améliorer l'efficacité opérationnelle et réduire les risques de sécurité réseau.

Conformité élargie

Les entreprises doivent aujourd'hui se conformer à un nombre croissant de réglementations et de normes, comme par exemple la loi américaine Sarbanes-Oxley, le guide méthodologique britannique GPG13, les dispositions des autorités de réglementation financières, la réglementation Garante en Italie, les réglementations pour la protection et la sécurité des données comme les lois américaines HIPAA, FISMA, GLBA, les normes spécifiques aux cartes de paiement, les normes en matière d'alimentation électrique, etc. Le volume énorme des données et incidents générés par une organisation constitue une mine d'informations très précieuses à des fins d'audit. C'est pourquoi QRadar met en corrélation les informations collectées et intègre toutes les données de surveillance, pour offrir des données plus précises aux opérateurs, des analyses de granularité adéquate aux responsables de la gestion des incidents et des rapports plus complets aux auditeurs.

Intelligente, intégrée et automatisée

La QRadar Security Intelligence Platform offre une architecture unifiée de collecte, de stockage, d'analyse et de consultation des données liées à la journalisation, aux menaces, aux vulnérabilités et au risque. QRadar est non seulement une solution intelligente, intégrée et automatisée, mais également modulaire. Elle présente ainsi le grand avantage de pouvoir être utilisée en toute transparence par divers départements, utilisateurs et fonctions (opérateurs, analystes, auditeurs, etc.), qui peuvent travailler à partir de différents modules QRadar.

Everything CHANNEL 5 STAR PARTNER PROGRAM WINNER 2010

Gartner

Q1 Labs se classe parmi les leaders de la GIIS selon le Gartner SIEM Magic Quadrant Report 2011.

Plateforme de veille sécuritaire QRadar

Intelligente

QRadar détecte un plus grand nombre de menaces que d'autres solutions, et offre une meilleure visibilité. Comment ? En permettant le suivi d'un volume de données plus important et en s'appuyant sur des techniques d'analyse plus intelligentes.

Intégrée

Conçu spécifiquement et d'emblée pour intégrer en une seule solution la gestion des journaux, la GIIS et la gestion du risque, QRadar vous permet de couvrir un volume énorme de données de journalisation, sans compromettre l'exploitation des renseignements issus de la GIIS.

- Une plateforme unique regroupant toutes les fonctions de recherche, de définition de règles et de création de rapports.
- Une interface utilisateur intuitive tout aussi unique, qui rassemble les tâches de gestion des journaux, de modélisation du risque, d'affectation de priorités aux vulnérabilités, de détection des incidents et d'analyse d'impact.

Automatisée

QRadar est simple à déployer et à gérer, grâce à des fonctionnalités automatisées de sécurité et de détection des dispositifs réseau, ainsi qu'à des outils de conformité et de définition de règles. Par l'automatisation des tâches fastidieuses de détection et de paramétrage des dispositifs, QRadar fait disparaître la complexité rebutante qui afflige les plateformes de veille sécuritaire traditionnelles.

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

DSQROVFE0911