L'analyse de sécurité pour les déploiements multicloud

Solution IBM Security QRadar SIEM

Sommaire

01

La révolution multicloud est en plein essor

La sécurité intelligente, indispensable pour l'entreprise moderne

L'adoption du multicloud hybride est en pleine expansion, et s'accompagne de la migration d'une quantité croissante de données, d'applications et de charges de travail vers le cloud. Avec le développement du télétravail et des interactions qui se font désormais de plus en plus en ligne et non en face à face, l'utilisation du cloud devrait atteindre de nouveaux sommets.[1]

Gartner estime que le secteur des services du cloud public connaîtra une croissance exponentielle en 2022. Le segment du marché du cloud qui devrait avoir la croissance la plus rapide sera l'infrastructure en tant que service (IaaS), qui, selon les prévisions de Gartner, atteindra 76,6 milliards USD en 2022.[2]

La sécurité doit être placée au cœur de ces initiatives cloud. Les violations de sécurité sur le cloud peuvent coûter plus de 50 000 USD aux entreprises en moins d'une heure.[3] Les entreprises utilisant l'IaaS doivent sécuriser proactivement leurs systèmes d'exploitation, gérer des configurations réseau et bien entendu protéger les données s'exécutant sur ces systèmes.

Pour garantir la sécurité des informations métier, les analystes de sécurité doivent disposer d'une visibilité totale de tout leur écosystème IT : réseaux, applications et activités s'exécutant sur site et dans le cloud. Ils doivent pouvoir détecter les menaces en temps réel, identifier l'utilisation de services cloud non autorisés, et avoir une visibilité suffisante pour savoir si leurs comptes et leurs ressources cloud sont correctement configurés de manière à préserver la sécurité.

> 1 milliard d'enregistrements perdus

Une configuration incorrecte des environnements cloud a provoqué la perte de plus d'un milliard d'enregistrements en 2019.[3]

> 50 000 USD de pertes en moins d'une heure

Les violations de sécurité sur le cloud peuvent coûter plus de 50 000 USD aux entreprises en moins d'une heure.[3]

02

Libérez la puissance des solutions IBM Security QRadar

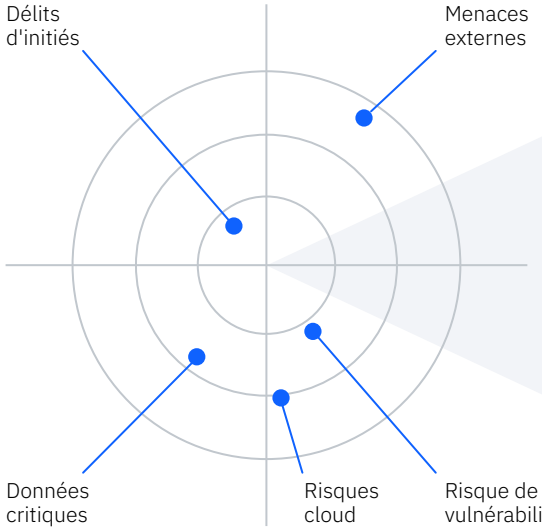
Dotez-vous d'une visibilité complète des services cloud

La solution SIEM (information sur la sécurité et gestion des événements) IBM Security QRadar propose des intégrations en profondeur à de nombreux services cloud, dont Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365, IBM Cloud, etc.

La solution QRadar, qui collecte et normalise des informations de sécurité dans des environnements cloud et sur site, utilise une analytique avancée pour trier automatiquement des millions d'événements. La solution permet d'identifier les menaces les plus critiques et émet des alertes hiérarchisées et claires sur les incidents potentiels afin de protéger les environnements hybrides sur site et multicloud.

La solution fournit en outre aux analystes de sécurité une interface unifiée dans laquelle ils peuvent visualiser les menaces les plus graves, passer en revue l'enchaînement chronologique des événements et obtenir instantanément des informations sur les attaques potentielles. Des fonctionnalités robustes prêtes à l'emploi garantissent le déploiement rapide et l'évolutivité dans quasiment tous les environnements pris en charge.

Informez-vous sur la solution QRadar pour sécuriser votre environnement cloud →



Détection et hiérarchisation automatiques des menaces

La solution IBM Security QRadar SIEM collecte, analyse et crée des données provenant de nombreuses sources afin de détecter et hiérarchiser les menaces les plus graves qui nécessitent d'être étudiées.

03

Intégrez la solution QRadar à Amazon Web Services (AWS)

Etendez la visibilité dans AWS pour renforcer votre stratégie de sécurité

Environ 76 % des entreprises utilisent AWS dans des proportions variables.[1] Alors que cette transition de l'informatique traditionnelle sur site vers le cloud se poursuit, les équipes de sécurité ont besoin d'une visibilité de leur infrastructure, de leurs applications et de leurs données sur le cloud, tout comme dans un environnement sur site.

Identifiez les risques d'exposition des données
Certaines des plus importantes violations des dernières années n'ont pas été le fait d'agresseurs malveillants. Elles résultent en fait d'erreurs de configuration volontaires des compartiments Amazon Simple Storage Service (Amazon S3) qui ont entraîné une exposition publique de données sensibles.

La solution QRadar permet aux équipes de sécurité d'analyser proactivement leurs environnements AWS, soit sur une base ad hoc, soit dans le cadre d'un programme d'analyse régulier afin de rechercher activement ces configurations erronées et d'alerter les analystes lorsqu'elles sont détectées. Une fois en possession de ces alertes, les équipes de sécurité peuvent commencer le processus de réponse pour pallier les lacunes et protéger leurs données.

Détectez les menaces contre les données et les charges de travail cloud
Face à la migration des données sensibles et des ressources métier critiques vers le cloud, AWS est devenu une cible de choix pour les agresseurs. Si les comptes AWS sont compromis, soit directement par un hameçonnage ciblé, soit lors d'une mutation latérale, les données et les charges de travail AWS risquent de tomber sous le contrôle d'un agresseur. Pour éviter les dommages, il est vital de pouvoir envoyer des avertissements unifiés et précoces concernant les menaces. QRadar rassemble les données de sécurité AWS, y compris AWS CloudTrail, AWS CloudWatch et AWS Virtual Private Cloud (VPC) Flow Logs au sein d'une solution d'analytique de sécurité centralisée. Cette solution permet aux équipes des opérations de sécurité d'effectuer le suivi des menaces externes et des délits d'initiés à partir d'une seule et même interface.

La solution QRadar peut collecter les événements de vos produits de sécurité à l'aide d'un fichier plug-in appelé un **DSM (Device Support Module)**.

Grâce à des protocoles pris en charge et aux modules DSM (Device Support Modules), la solution QRadar s'intègre aux composants AWS suivants pour mettre en œuvre une analyse de sécurité avancée :

AWS CloudTrail. L'intégration QRadar offre une bonne visibilité de l'activité des utilisateurs en enregistrant les actions effectuées sur votre compte. Elle prend en charge les événements d'audit collectés à partir des compartiments Amazon S3, et d'un groupe de journaux dans AWS CloudWatch Logs.

AWS Security Hub. Cette intégration a recours à un système intégré d'analytique et de mécanismes de défense en temps réel qui permet aux équipes de sécurité d'avoir une visibilité étendue des alertes de sécurité à haute priorité. Elle permet aussi d'effectuer des contrôles de conformité automatiques via le tableau de bord d'un centre des opérations de sécurité (SOC). En s'intégrant à AWS Security Hub Amazon Findings Format (AFF), la solution QRadar optimise l'agrégation des événements dans plusieurs dispositifs et instances de sécurité d'AWS, ainsi que dans les solutions de sécurité AWS Partner Network (APN), et permet ainsi une analyse de sécurité approfondie.

Amazon GuardDuty. Cette intégration permet aux utilisateurs d'analyser des flux continus de métadonnées générés par l'activité sur leur compte et sur le réseau détectée dans les événements d'AWS CloudTrail, dans Amazon VPC Flow Logs, et dans les journaux du serveur de noms de domaine (DNS).

Amazon VPC Flow Logs. Cette intégration permet aux clients de collecter, stocker et analyser les journaux de flux du réseau. Elle permet de surveiller et de résoudre les problèmes de connectivité et de sécurité afin de s'assurer du bon fonctionnement des règles d'accès au réseau.

Amazon AWS Content Extension. Cette extension de contenu permet une analyse syntaxique des nouveaux événements. Elle vient s'ajouter à la solution AWS intégrée à QRadar et accélérer l'analyse syntaxique des données d'événement critiques. Les données, par exemple, l'identificateur d'instance, le nom de fichier, le nom de rôle, le nom du stockage, et ainsi de suite, sont instantanément accessibles aux utilisateurs qui peuvent surveiller les modifications et générer des rapports sur la sécurité relative de leurs environnements cloud.

Application IBM Security QRadar Cloud Visibility. Cette application inclut des tableaux de bord AWS spécifiques et diverses améliorations, notamment :

- Gestion simplifiée de la source de journal
- Gestion des identités et des accès (IAM) pour les comptes, les utilisateurs et les rôles IAM
- Remplissage automatique de la hiérarchie du réseau QRadar
- Visualisation Amazon VPC Flow Log
- Intégration à AWS Security Hub et Amazon Detective

Pourquoi utiliser la solution QRadar pour surveiller les environnements AWS ?

- Elle offre une visibilité centralisée des risques et des menaces dans les déploiements cloud.
- Elle permet aux analystes de sécurité de rechercher proactivement les configurations erronées nécessitant une intervention.
- Elle élimine les silos pour mieux comprendre l'enchaînement de bout en bout des événements relatifs à un incident.
- Elle utilise l'apprentissage automatique pour identifier les utilisateurs à haut risque et détecter les délits d'initiés.

En savoir plus sur IBM Security QRadar Amazon AWS Content Extension →

04

Intégrez la solution QRadar à Microsoft Azure

Améliorez la visibilité et traitez les événements de plusieurs millions d'appareils

L'adoption de Microsoft Azure a connu une croissance régulière, et 61 % des entreprises déclarent utiliser ce service. Face à la migration de quantités de plus en plus importantes de données et de charges de travail vers Azure, les pratiques de sécurité doivent s'adapter pour protéger les ressources dans ce nouvel environnement. La solution QRadar propose des fonctionnalités robustes et prêtes à l'emploi qui permettent d'inclure les données de sécurité Azure dans un programme d'analyse de sécurité à l'échelle de toute l'entreprise.

Grâce à des protocoles pris en charge et aux modules DSM, la solution QRadar s'intègre aux composants Azure suivants pour mettre en œuvre une analyse de sécurité avancée :

Azure Activity Logs. Ce service Azure de collecte d'événements natifs ingère d'énormes volumes de données et d'événements de télémétrie. Ces informations peuvent facilement être envoyées à la solution QRadar et permet aux équipes de sécurité d'avoir une vision plus approfondie des risques et menaces potentiels dans les environnements Azure.

Azure Active Directory. L'intégration de la solution QRadar à Azure Active Directory permet aux équipes de sécurité de surveiller la gestion des identités et des accès, ainsi que les événements de sécurité provenant de ressources externes, telles que Microsoft Office 365 et Microsoft Azure.

API Microsoft Graph Security. Grâce au protocole de QRadar pour l'API Microsoft Graph Security, les entreprises peuvent ingérer les alertes de l'API Microsoft Graph Security, et les analystes de sécurité peuvent étudier rapidement les infractions.

Application QRadar Cloud Visibility. La solution QRadar peut détecter les problèmes potentiels dans les environnements Azure et traiter les cas d'utilisation de sécurité. Une fois les infractions créées, l'application QRadar Cloud Visibility permet aux utilisateurs de les gérer dans le tableau de bord Azure Offense Overview.

Le tableau de bord Azure Offense Overview affiche les données des infractions actives dans les graphiques suivants :

- Tous les utilisateurs par magnitude
- Tous les utilisateurs par règles associées
- Infractions les plus graves
- Tous les utilisateurs par nombre d'infractions
- Indicateur de niveau de magnitude

IBM Security QRadar Content Extension for Azure. L'extension de contenu QRadar Azure ajoute des règles, des rapports et des recherches sauvegardées qui complètent les fonctionnalités QRadar d'analyse syntaxique des événements pour les déploiements Azure.

Cette extension de contenu concerne tout particulièrement la gestion de la sécurité des réseaux, la modification des règles de sécurité et la gestion du réseau virtuel.

Pourquoi utiliser la solution QRadar pour protéger et surveiller les environnements Azure ?

- QRadar détecte les tendances révélatrices de comportements anormaux dans toute l'infrastructure informatique grâce à des règles de sécurité.
- Il surveille et diagnostique le trafic réseau via les groupes de sécurité de réseau Azure.
- Il gère plus efficacement les réseaux virtuels.
- Collectez les journaux des événements et les données de sécurité du flux réseau dans les passerelles de réseau locaux.
- Surveillez la performance et l'utilisation des applications Web s'exécutant dans Azure.

En savoir plus sur QRadar Content Extension for Azure →

05

Intégrez la solution QRadar à Google Cloud Platform

Détectez rapidement les anomalies et les menaces en temps réel

Google Cloud Platform est l'une des principales solutions cloud, avec une base d'utilisateurs en pleine expansion (35 %).[1] La solution propose une suite de services cloud qui utilisent l'infrastructure Google. La solution IBM Security QRadar permet une intégration avancée à Google Cloud Platform. Elle offre une visibilité centralisée en collectant, recherchant et analysant des centaines de données provenant de charges de travail résidant dans tous les environnements. Vos équipes de sécurité pourront mieux détecter les menaces et y réagir plus efficacement quel que soit le lieu où elles se produisent.

Grâce à des protocoles pris en charge et aux modules DSM, la solution QRadar s'intègre aux composants Google Cloud Platform suivants pour mettre en œuvre une analyse de sécurité avancée :

Rapports d'activités Google G Suite. La solution QRadar offre la visibilité des événements d'activité des audits générés au sein de la plateforme Google G Suite, y compris la connexion, le compte utilisateur, Google Drive et Google Admin.

Votre équipe de sécurité pourra obtenir des informations sur les cas d'utilisation suivants :

- Compte désactivé en raison d'activité suspecte
- Informations utilisateur téléchargées sous la forme d'un fichier CSV (à cellules séparées par une virgule)
- Privilèges administrateur révoqués par l'utilisateur
- L'acteur a modifié la question secrète de récupération du compte ou sa réponse
- L'acteur a modifié les droits de partage utilisateur
- L'acteur a déplacé un élément du dossier source vers le dossier de destination
- L'utilisateur a été suspendu

Protocole Google Cloud Pub/Sub. Le protocole QRadar pour Google Cloud Pub/Sub permet aux utilisateurs de renforcer la visibilité de tous les éléments créant un collecteur de données dans Pub/Sub, et donne la possibilité aux équipes de sécurité d'agir plus rapidement.

06

Surveillez les solutions SaaS

Surveillez les données de vos applications SaaS avec les modules DSM de QRadar

Les entreprises utilisent déjà les applications de logiciels sous forme de services (SaaS) pour améliorer leur agilité, travailler plus rapidement et accompagner les projets générateurs de revenus. L'adoption du SaaS est en pleine croissance. Selon les prévisions de Gartner, cette solution cloud basée sur les services vaudra 143,7 milliards USD d'ici 2022.[2]

La solution QRadar aide les entreprises à se doter d'une bonne visibilité de l'utilisation des applications SaaS et permet aux équipes de sécurité de détecter et de bloquer plus efficacement les menaces. Les modules DSM préconfigurés permettent une intégration en toute transparence aux autres solutions de votre environnement. Les modules DSM sont testés et validés par l'équipe de sécurité IBM avant le déploiement.

La solution QRadar aide votre équipe à surveiller facilement les données de vos applications SaaS, y compris Salesforce.com, Office 365, les environnements Box, et ainsi de suite. Une fois ces données incorporées à votre programme d'analyse de sécurité, votre équipe disposera d'informations avancées sur les menaces potentielles et pourra détecter les incidents potentiels ciblant les données de ces solutions. Vos analystes de sécurité seront mieux armés pour déceler très tôt les initiés malveillants dans leur cycle d'attaque et les empêcher de compromettre les données sensibles stockées dans ces applications et ces services.

En savoir plus sur les modules DSM pris en charge par la solution QRadar →

La solution QRadar permet l'intégration via des modules DSM, en proposant une gamme variée d'offres SaaS et IaaS populaires.

Amazon CloudTrail
Amazon CloudWatch
Amazon VPC Flows

Microsoft Azure Event Hubs

Microsoft Office 365

Box.com

Netskope Active

Cloudera Navigator

CloudPassage Halo

Skyhigh Networks

OpenStack

Cisco Cloud Web Security

VMware

Salesforce

Okta

Google Cloud Platform

Plateforme Red Hat® Ansible®

07

Autonomisez votre équipe de sécurité en la dotant des outils adaptés

Explorez la famille des produits QRadar

Pour résumer, les solutions IBM Security QRadar vous fournissent des informations critiques indispensables à vos environnements cloud en pleine expansion. Cette famille de solutions vous permet de regrouper de nombreux silos de données au sein d'une seule et unique plateforme offrant une visibilité complète, l'analyse de la sécurité, et la détection des menaces. Elle vous aide à identifier les comportements anormaux afin de vous protéger des délits d'initiés et des menaces externes, d'identifier les vulnérabilités qui mettent involontairement en péril les données sensibles, et de détecter l'utilisation de services cloud non autorisés.

Ces fonctionnalités réunies vous fournissent une vue complète du système, du réseau et de l'activité utilisateur dans votre entreprise. Elles permettent d'obtenir des indications intelligentes pour lutter proactivement contre les risques et les menaces.

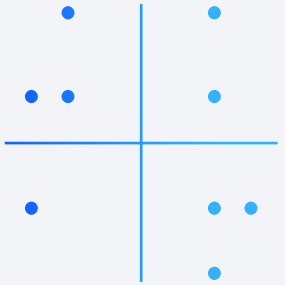
La solution QRadar centralise la collecte et l'analyse des flux de données et des informations sur les menaces dans différents environnements, dont AWS, Azure, IBM Cloud, les applications SaaS, les clouds privés et les infrastructures traditionnelles sur site. Vous pouvez choisir de déployer les matériels ou logiciels sur site, de déployer les machines virtuelles dans les environnements IaaS ou d'utiliser la solution QRadar comme un service cloud d'IBM.

Lors de votre transition vers le multicloud, vous avez l'assurance de pouvoir compter sur les mêmes fonctionnalités de sécurité, de surveillance et d'analyse dans toute l'entreprise.

En savoir plus →

IBM a été nommé parmi les leaders dans le dernier Gartner Magic Quadrant sur les systèmes SIEM (informations sur la sécurité et gestion des événements) **pour la 11ème fois consécutive.**

Lire le rapport →



08

Pourquoi les solutions IBM Security ?

IBM est l'une des plus grandes entreprises au monde de recherche, de développement et de distribution de solutions de sécurité.

IBM Security propose l'un des portefeuilles de produits et de services de sécurité d'entreprise parmi les plus sophistiqués et les plus intégrés du marché. Ce portefeuille, qui bénéficie de la collaboration d'IBM X-Force®, une équipe de renommée mondiale, fournit des renseignements de sécurité afin d'aider les entreprises à protéger globalement leurs infrastructures, leurs données et leurs applications. Il propose des solutions dans les domaines suivants : gestion des identités et des accès, sécurité des bases de données, gestion des applications, gestion des risques, gestion des points de terminaison, sécurité réseau, et bien d'autres encore. Ces solutions permettent aux entreprises de gérer efficacement le risque et de mettre en œuvre une sécurité intégrée pour les architectures mobile, cloud et de réseaux sociaux, ainsi que d'autres architectures métier d'entreprise.

IBM Global Financing propose en outre de nombreuses solutions de paiement pour vous aider à acquérir la technologie indispensable à la croissance de votre entreprise. IBM assure la gestion totale du cycle de vie des produits et services IT, de l'achat jusqu'à la mise au rebut. Pour plus d'informations, rendez-vous sur ibm.com/financing.

Pour plus d'informations
Pour en savoir plus sur la solution QRadar de renseignement de sécurité, contactez votre représentant IBM ou votre partenaire commercial IBM, ou visitez le site ibm.com/security/security-intelligence/qradar.

IBM surveille des **milliards** d'événements de sécurité par jour dans plus de **130 pays,** et a déposé plus de **3 000 brevets de sécurité.**

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Visitez la page d'accueil d'IBM à l'adresse suivante :
ibm.com

Le présent document contient des informations en vigueur à la date de la première publication et susceptibles d'être modifiées par IBM à tout moment. Toutes les offres mentionnées ne sont pas distribuées dans tous les pays où IBM exerce son activité.

Déclaration de bonnes pratiques de sécurité : la sécurité du système IT englobe la protection des systèmes et des informations grâce à la prévention, la détection et la réponse en cas d'accès internes et externes non autorisés. Un accès non autorisé peut entraîner la modification, la destruction, le détournement ou l'utilisation impropre des informations, ou une détérioration ou une utilisation impropre de vos systèmes, notamment en vue de les utiliser pour attaquer autrui. Aucun système ou produit IT ne doit être considéré comme entièrement sécurisé, et aucun produit, service ou dispositif de sécurité ne peut être entièrement efficace pour empêcher une utilisation ou un accès inappropriés. Les systèmes, produits et services d'IBM sont conçus pour fonctionner dans le cadre d'une stratégie de sécurité globale et conforme à la loi qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent nécessiter des performances maximales des autres systèmes, produits et services. IBM NE GARANTIT PAS QUE LES SYSTÈMES, PRODUITS OU SERVICES SONT PROTÉGÉS CONTRE LES AGISSEMENTS MALVEILLANTS OU ILLÉGAUX D'UN TIERS OU QU'ILS PROTÉGERONT VOTRE ENTREPRISE CONTRE DE TELS AGISSEMENTS.

1 10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera, *Forbes*, 2 mai 2020

2 Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, *Gartner*, 2 avril 2019

3 Cloud Threat Landscape Report 2020, *IBM Security X-Force®* Incident Response and Intelligence Services, mai 2020