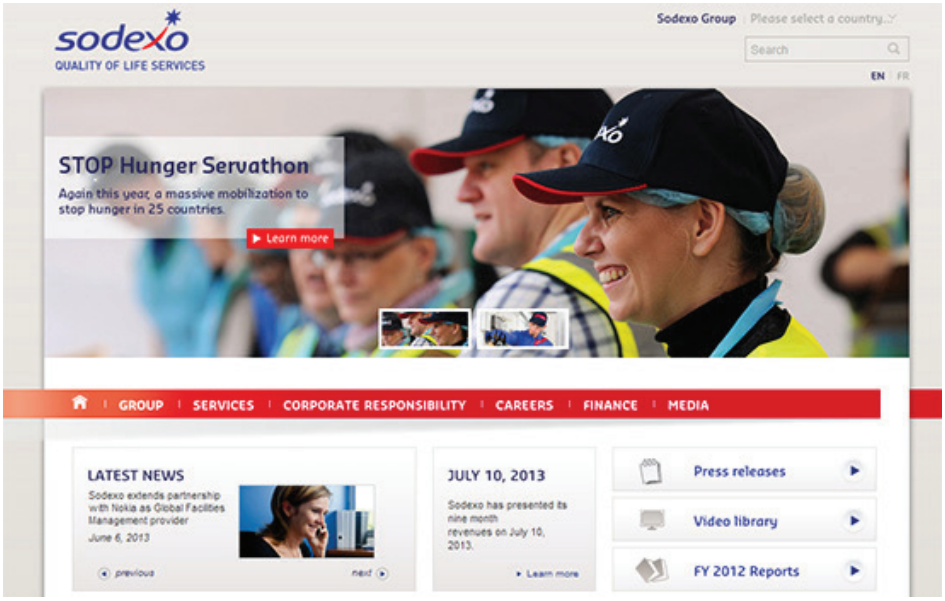
Gestion des risques de sécurité : automatiser la gestion des vulnérabilités pour sécuriser une entreprise d'envergure mondiale et de premier ordre

Grâce à la solution QualysGuard Vulnerability Management, Sodexo a une meilleure visibilité des vulnérabilités présentes sur son réseau de filiales mondiales qui couvre environ 13 000 adresses IP.



Entreprise d'envergure mondiale et de premier plan spécialisée dans la fourniture de services de qualité de vie, Sodexo offre un ensemble totalement intégré de services innovants pour plus de 100 métiers, depuis le développement de l'entreprise jusqu'à la motivation des employés en passant par la formation, la santé et la gestion des ressources. Avec plus de 420 000 employés travaillant sur plus de 34 000 sites répartis dans 80 pays et 20ème plus important employeur au monde, Sodexo est chaque jour au service de 75 millions de personnes.

Pour fournir son ensemble de services hétérogènes avec la qualité qu'exigent ses clients, Sodexo gère un large ensemble de ressources informatiques distribuées sur ses différentes entités, filiales et représentations. Ces ressources comprennent désormais de nouvelles solutions basées sur des infrastructures Cloud privées, publiques et hybrides. Alors que la tendance à la numérisation des services se poursuit et que Sodexo fournit

www.sodexo.com

INDUSTRIE : Consulting / Services

METIER : solutions de services sur site pour le développement de l'entreprise, la formation, la santé, la gestion des ressources et la motivation des employés.

PERIMETRE : HQ in France, worldwide

TAILLE : 420 000 employés dans 80 pays

DÉFI OPÉRATIONNEL : Sodexo avait besoin d'améliorer la visibilité des vulnérabilités de sécurité sur son infrastructure globale à la fois vaste et hétérogène et qui s'étend sur environ 13 000 adresses IP.

SOLUTION: Sodexo a déployé QualysGuard Vulnerability Management (VM) comme plate-forme stratégique pour garantir la visibilité des risques de sécurité opérationnelle.

POURQUOI QUALYSGUARD :

- Souplesse : le modèle économique SaaS est souple et évite les dépenses d'investissement.
- Qualité : la solution Qualys fournit des évaluations à la fois précises et ponctuelles des vulnérabilités de sécurité. Ces évaluations sont accompagnées de plans de remédiation concrets.
- Exhaustivité : la solution Qualys offre un reporting consolidé au niveau du Groupe, de chaque entité et de chaque pays afin de fournir une vue complète.

davantage d'outils basés Web à ses employés et à ses clients, le profil des risques informatiques ne cesse d'évoluer. L'entreprise doit donc conserver en permanence une longueur d'avance sur les menaces.

Pour réduire les risques informatiques que posent les vulnérabilités connues et inconnues et déployer un nouvelle gouvernance de la sécurité informatique au niveau global, l'équipe Sodexo chargée des services technologiques globaux (Global Technology Services) a déployé comme standard une solution de gestion des vulnérabilités.

Cycle de vie complet de l'audit réseau et de la gestion des vulnérabilités

Après avoir évalué différentes options, Sodexo a sélectionné QualysGuard Vulnerability Management (VM) basée sur QualysGuard Cloud Platform comme solution stratégique pour automatiser le cycle de vie de l'audit réseau et la gestion des vulnérabilités au niveau mondial. La solution QualysGuard offre une gamme complète de fonctionnalités, notamment la découverte et la cartographie du réseau, la classification des actifs par priorité, le reporting de l'évaluation des vulnérabilités ainsi que le suivi de la remédiation en fonction du risque pour l'activité de l'entreprise.

John Bruylant, CTO chez Sodexo au niveau du Groupe, déclare : « QualysGuard s'est avérée supérieure aux autres solutions auxquelles nous nous intéressions. En effet, le modèle économique de logiciels fournis sous la forme de services (SaaS) évite de réaliser des investissements lourds dans une infrastructure dédiée. En outre, la qualité, l'exhaustivité et la granularité du reporting nous permettent de comprendre les risques informatiques pour notre activité. Non seulement QualysGuard VM détecte et classe les vulnérabilités, mais formule aussi des recommandations précises sur la manière de les corriger. Il s'agit là d'un avantage critique pour les équipes d'entités plus petites disposant de peu de ressources en sécurité informatique. Désormais, ces équipes peuvent savoir rapidement ce qu'elles doivent faire et où trouver les informations supplémentaires si nécessaire. »

« Non seulement QualysGuard VM détecte et classe les vulnérabilités, mais elle formule aussi des recommandations précises sur la manière de les corriger. Il s'agit là d'un avantage critique pour les équipes d'entités plus petites et aux ressources de sécurité informatique limitées. »

John Bruylant,
CTO au niveau Groupe, Sodexo

Capitaliser sur le succès initial

Si QualysGuard VM a été sélectionnée par Sodexo comme solution de référence mondiale pour la gestion des vulnérabilités, c'est suite à l'intégration réussie de cette solution au sein du Groupe Services Avantages et Récompenses (BRS), anciennement Solutions de motivation (SVC). En 2004, l'entité BRS avait déployé QualysGuard VM pour renforcer la sécurité de ses 30 filiales à travers le monde.

Auparavant, BRS s'efforçait de gérer les audits techniques sur site via son infrastructure en évolution rapide. Même si ces audits fournissaient une vue claire et détaillée du niveau de sécurité et du profil de risque pour chaque filiale, le tout avec des recommandations d'amélioration, il n'était cependant pas possible de les lancer plus d'une fois tous les deux ans.

L'entité BRS a donc choisi QualysGuard VM pour compléter ses audits sur site afin de disposer d'une gestion des vulnérabilités permanente et d'une vue sans cesse actualisée du profil de risque pour ses filiales. La solution Qualys a été retenue pour sa simplicité de déploiement et d'administration, sa capacité à répondre aux besoins des filiales de toute taille ainsi que pour son efficacité pour identifier les vulnérabilités émergentes.

Un déploiement mondial pour une sécurité complète

La sécurité informatique n'est pas seulement une affaire d'outils. En effet, les structures et politiques de l'entreprise qui intègrent une culture de la sécurité sont tout aussi importantes. Sodexo a déployé une équipe de services de sécurité opérationnelle (SOS) au sein du département Global Technology Services (GTS) pour renforcer la sécurité des systèmes d'information au sein de l'entreprise.

« Notre mission consiste à déployer une gouvernance et une excellence opérationnelle de l'informatique sans nuire à la souplesse ni à l'efficacité des différentes entités, » explique M. Bruylant. « Nous avons déployé des appliances QualysGuard au sein de nos filiales et édicté le reporting des vulnérabilités automatisé au rang de standard pour le Groupe afin de réduire le nombre de vulnérabilités internes. »

QualysGuard est fournie sous la forme d'un service informatique interne aux différentes entités dans le cadre du programme de gestion des vulnérabilités de Sodexo. Les responsables VM de chaque entité produisent des rapports consolidés qui mesurent les performances du programme pour la partie de l'infrastructure qui leur incombe.

Développer la standardisation à partir de QualysGuard

Aujourd'hui, Sodexo utilise QualysGuard VM quotidiennement à l'échelle mondiale pour analyser les vulnérabilités au sein de ses systèmes d'information. La fréquence d'analyse dépend notamment de la criticité des actifs, mais aussi d'événements spécifiques tels que les fusions et acquisitions et les incidents de sécurité majeurs. En outre, le département en charge de réaliser les audits internes s'appuie sur la plate-forme QualysGuard pour procéder à des évaluations périodiques.

QualysGuard VM classe les vulnérabilités en fonction des risques qu'elles représentent pour l'activité, ce qui est en partie déterminé par les propres règles de Sodexo en matière d'évaluation des risques. Ainsi, l'entreprise peut se concentrer sur les vulnérabiltiés les plus critiques et adopter les meilleures pratiques de l'industrie en matière de remédiation.

« Les vulnérabilités de niveau 4 ou 5, c'est-à-dire celles qui sont urgentes ou critiques, doivent être résolues en priorité absolue en fonction de la politique de patch du pays concerné,» commente John Bruylant. « Grâce aux améliorations permanentes qu'apporte Qualys, QualysGuard VM est un outil de plus en plus fin et efficace. Dorénavant, cette solution peut

établir une corrélation entre les vulnérabilités découvertes sur des serveurs spécifiques et identifier le risque réel que présente une vulnérabilité spécifique. Par exemple, la solution rétrogradera une vulnérabilité classée à l'origine comme critique si ce dernier doit exploiter une vulnérabilité qui n'existe pas sur ce serveur particulier. »

La solution Qualys continue d'être déployée chez Sodexo à mesure que ses besoins évoluent. Initialement confinée à des points d'accès externes, l'analyse des vulnérabilités traite désormais aussi les systèmes et équipements présents sur les réseaux internes.

Étendre la sécurité au Cloud et aux paiements

Cherchant à faire face aux nouvelles contraintes métier dans un souci de rentabilité et à proposer de nouveaux services aux clients, Sodexo adopte massivement des solutions dans le Cloud agiles. Pour assurer la sécurité, l'entreprise prévoit d'intégrer QualysGuard au cycle de vie du développement de nouvelles applications dans le Cloud. De même, lorsque cela s'impose, Sodexo s'appuie sur les fonctionnalités de QualysGuard pour garantir la conformité des services de paiement au standard PCI-DSS.

« Grâce à la vision et à l'évolution permanente de notre partenaire stratégique Qualys, nous avons la garantie que la plate-forme QualysGuard continuera de nous fournir des analyses et des prévisions sur les risques à mesure que notre infrastructure se développera et évoluera, » conclut John Bruylant.

« Avec la solution Qualys, nous pouvons comprendre clairement les risques de sécurité opérationnelle au niveau du Groupe, de chaque région et de chaque pays. Cette solution nous permet également de prendre des décisions plus éclairées en matière de remédiation des vulnérabilités. »