QUALYS™

Sodexho Alliance

SUPERVISER LA SÉCURITÉ RÉSEAUX D'UNE INFRASTRUCTURE IT MONDIALE ET DÉCENTRALISÉE

Leader mondial de la « Restauration et Services », le Groupe Sodexho compte plus de **313 000 collaborateurs** et est présent dans **76 pays** à travers le monde.

Le Projet :

- Les réseaux internes et externes
- Les serveurs système
- 512 adresses IP
- 119 domaines
- 6 appliances

*« QualysGuard allie fonctionnalités techniques, facilité d'utilisation et rentabilité. En moins d'un an, le nombre de vulnérabilités a baissé de **40%**. »*

Joe Ford
RSSI
Groupe Sodexho Alliance

Sodexho ALLIANCE
www.sodexho.com

« *Lors de mon arrivée chez Sodexho en 2002, il n'y avait pas de politique de sécurité globale. Toute l'infrastructure du groupe était hétérogène. Chaque région ou business unit, avaient son propre mode de fonctionnement et de gestion.*
Un vrai challenge pour un RSSI ! Avec QualysGuard, j'ai pu instaurer une méthodologie rigoureuse de gestion des vulnérabilités sans remettre en cause l'indépendance de nos filiales » déclare Joe Ford, RSSI du Groupe Sodexho Alliance.

Disposer d'une solution facile à implémenter mondialement

Depuis sa création, Sodexho a fait le choix de concéder à ses sites régionaux et ses business unit une grande autonomie.

Début 2003, il s'est produit un changement au sein du Groupe. Devant le nombre croissant des menaces, la Direction Générale n'a plus considéré la sécurité comme un poste de coût mais comme un investissement à rationaliser, ayant une importance et un impact sur l'ensemble de l'activité de l'entreprise. Sodexho a donc souhaité mettre en place une politique de sécurité globale déclinable dans le monde entier.

« *Nous avions plusieurs objectifs* » se rappelle Joe Ford. « *Définir le niveau global de sécurité de l'entreprise, mettre en place une politique de sécurité proactive mais aussi, conserver notre organisation décentralisée. Il nous fallait donc une solution facile à implémenter, à utiliser et à gérer. QualysGuard s'est imposée rapidement comme la solution idéale, alliant fonctionnalités techniques, facilité d'utilisation et rentabilité.* »

Préserver l'autonomie des filiales tout en instaurant une politique de sécurité cohérente

Partant d'un constat simple, « *Ce que nous ne connaissons pas peut s'avérer dangereux* », le premier challenge de Joe Ford a été de créer une cartographie précise du réseau externe en recensant l'ensemble des dispositifs disposant d'une adresse IP.

« *QualysGuard permet l'identification dynamique de tous les éléments du périmètre réseau et détecte, pour chacun de ces éléments, des informations sur la nature du système d'exploitation, le matériel, les adresses IP et ports courants ouverts. Dés le départ nous avons donc recensé tous les éléments de notre réseau automatiquement en disposant de l'information par filiale, par région ou par type de dispositifs.* »

La seconde étape a consisté à instaurer, dans chaque filiale, un suivi régulier des vulnérabilités. En août 2003, la direction du Groupe a donc annoncé la mise en place d'un programme obligatoire et gratuit de scans pour le début de l'année fiscale suivante. Avec un objectif clairement défini : permettre aux filiales de s'auto évaluer et de prendre les dispositions nécessaires pour renforcer la sécurité de leur réseau

« *Le modèle on demand est la solution idéale pour gérer les vulnérabilités et appliquer les correctifs dans une organisation décentralisée. Il élimine la surcharge de travail ainsi que les coûts de déploiement et de maintenance des solutions logicielles traditionnelles. Il permet également aux filiales de s'autogérer et de rester maître des actions à mener. Quant à moi, je peux superviser l'ensemble du réseau et vérifier l'application des patchs et des mesures décidées ensemble lors de nos comités de pilotage* » ajoute Joe Ford.

Sodexho Alliance : superviser la sécurité réseaux d'une Infrastructure IT mondiale et décentralisée

La mise en place de la solution s'est déroulée très simplement. Des sessions de formation de 30 minutes via Webex ont été assurées par le siège et un guide des meilleures pratiques de gestion de la sécurité réseaux a été envoyé aux directions informatiques afin de compléter leurs connaissances.

En moins d'un an, baisse de plus de 40% du nombre de vulnérabilités

Avec QualysGuard, Sodexho a instauré une méthodologie rigoureuse de gestion des vulnérabilités en fixant des règles précises de sécurité et en hiérarchisant les dispositifs à surveiller.

« En se basant sur les rapports des premiers scans, nous avons pu définir avec chaque filiale les mesures à prendre et hiérarchiser nos actions. La priorité a bien sûr été de nous focaliser sur les vulnérabilités de niveaux 4 et 5 mais aussi de comprendre notre réseau afin de lancer une véritable politique de Risk Management où les dispositifs sont classés en fonction de leur importance et leur niveau de criticité sur notre activité. »

Les rapports techniques offrent aux responsables sécurité une synthèse IP par IP et détaillent, pour chaque vulnérabilité décelée, le niveau de criticité, ses conséquences si elle est exploitée, les actions de correction à mener et le lien vers les patchs officiels.
Les rapports destinés aux directions générales offrent une vision globale et l'indice de sécurité permet de suivre l'évolution du niveau de sécurité et de hiérarchiser les menaces en fonction de leur impact sur l'activité de l'entreprise.

« Les ingénieurs de Qualys ont rapidement collaboré avec nos équipes afin de modifier l'interface utilisateur, qui n'était pas si conviviale au départ, tout simplement pour faciliter l'adhésion de toutes nos filiales. Le modèle on demand et la culture de l'entreprise leur permettent de véritablement répondre aux préoccupations et besoins des utilisateurs de manière quasi instantanée. »

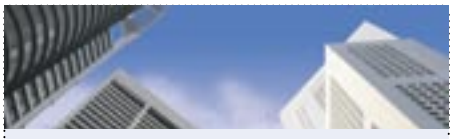
Aujourd'hui, les filiales du Groupe sont sensibilisées au programme de gestion des vulnérabilités et paient pour leur utilisation de Qualys. Plus de 500 adresses IP sont surveillées régulièrement et les meilleurs scores sont publiés sur le site Intranet du Groupe.

L'implication des différents directeurs informatiques permet d'améliorer constamment le processus mis en place et les résultats parlent d'eux même : une baisse de plus de 40% du nombre des vulnérabilités a été constatée en moins d'un an.

> *« Le modèle on demand élimine la surcharge de travail et les coûts des solutions logicielles traditionnelles tout en permettant aux filiales de s'autogérer. Quant à moi, je peux superviser l'ensemble du réseau et vérifier l'application des patchs et mesures décidées en comité. »*
>
> ***Joe Ford.***

Fort de cette expérience, fin 2004, le Groupe Sodexho a décidé d'utiliser QualysGuard pour surveiller ses réseaux internes, désormais tout aussi critiques que les réseaux externes.

« Comme les rapports sont véritablement un outil de gestion très utile, pas uniquement une pile de données, je suis certain que nos équipes pourront aisément hiérarchiser leurs actions et manager les menaces sur l'ensemble de nos réseaux, sans être surchargées. Et le plus important, c'est que nos équipes opérationnelles partagent cet avis ! »



QUALYSGUARD® ENTERPRISE

CONTEXTE

- Topologie réseau, configurations système et niveau de sécurité inconnus
- Pas de gestion de vulnérabilités
- Pas de supervision centralisée

BESOINS

- Superviser les réseaux de manière centralisée
- Etablir un processus de gestion de vulnérabilités proactif et continu
- Préserver l'autonomie des filiales avec des outils faciles à installer et à utiliser

2 FACTEURS CLÉ DE SUCCÈS

- **Autogestion des filiales**
  - Respect de l'infrastructure décentralisée avec une solution on demand : pas d'installation, pas de maintenance et facilité d'utilisation
  - Collaboration avec les équipes opérationnelles sur la mise en œuvre de la solution
- **Une méthodologie rigoureuse et précise**
  - Formations de 30 mn via Webex et création d'un guide sur les best practices internes pour soutenir les managers IT
  - Hiérarchisation des composants réseaux et des actions à mener
  - Définition d'un plan d'actions réaliste