QUALYS™

Sodexho Alliance

SUPERVISING NETWORK SECURITY ACROSS A GLOBAL & DECENTRALISED IT INFRASTRUCTURE

With more than **313,000 employees** in **76 countries** worldwide, Sodexho is the global market leader in food and management services.

IT Scope

- Internal & external networks
- Server systems only
- 512 IP addresses
- 119 domains
- 6 appliances

"QualysGuard combines technical functionality, ease of use and a good ROI. In less than one year, Sodexho has decreased its vulnerabilities by **40%**. *"*

Joe Ford,
Global Security Chief Officer,
Sodexho Alliance

Sodexho ALLIANCE
www.sodexho.com

«When I arrived at Sodexho in 2002, there was no global security policy. The group infrastructure was heterogeneous and each area or business unit had its own way of managing operations. However, Sodexho wanted to adopt a cohesive security policy worldwide. That's very challenging for an information security officer ! With QualysQuard, I estalished a clear process for securing our networks and maintaining the independence of our subsidiaries» says Joe Ford, Global Security Chief Officer of Sodexho Alliance.

A Solution Easily Deployed Around the World

From its inception Sodexho chose to give its regions and business unit autonomy. But at the beginning of 2003, it made a significant change in Group policy. With the growing number of threats, general management stopped viewing security as a cost item and began to regard it as an investment with a significant bearing on all operating activities.

«We had several goals» Joe Ford recalls. *«They included definition of a global security policy and implementation of a proactive security programme while still preserving our decentralised organisation. After the evaluation it became obvious that we needed a solution that combine technical features, was easy to implement and use and also offered low cost of ownership.»*

Self-Management for Subsidiaries with a Cohesive Policy Across the Group

Starting from a simple observation, *«What we don't know can hurt us»*, Joe Ford's first challenge was to create a precise map of the external network to find out exactly what devices were connected to it.

«The scans allow dynamic identification of all elements within the network perimeter and detects, for each, information on the nature of the operating system, the IP addresses and the open common ports. Today, we are able to automatically list all the elements of our network, ending up with access to information for each subsidiary, region and type of device.»

The second phase of the project set out to establish regular monitoring of vulnerabilities in every subsidiary. In August 2003, group managers implemented a compulsory programme of free scans. The goal was clearly set out defined: to enable subsidiaries to self-assess and improve their network security.

«QualysGuard Enterprise is the best security approach for managing vulnerabilities and patches within a decentralised organisation. The on demand model eliminates the costs of deployment and maintenance and allows subsidiaries to be self-sufficient in their management. Now, I can easily check the application of patches and security measures for the entire network via the dynamic reports.» adds Ford.

Sodexho Alliance: supervising network security across a global & decentralised IT infrastructure

Implementation of the solution has been very simple. To support the IT managers, half-hour training sessions via Webex were set up by the head office. Managers also received a guide of the internal best practices to supplement their knowledge.

Within a year 40% decline in network vulnerabilities

Based on the information delivered by the reports, Sodexho introduced a rigorous vulnerability management methodology with precise security policies and clear priorities.

Customised reporting allows Sodexho to track compliance with the company's security rules and ensure the network always contains the latest patches.

«*With the first scan reports, we have established what measures we need to take with each subsidiary and so prioritise our actions. Sodexho's top priorityes was naturally to concentrate on level 4 and 5 vulnerabilities. But it was also to understand our network in order to launch a genuine risk management policy in which devices are sorted according to their importance to the way the business operates. We worked closely together to define realistic goals for remediation. It was essential to work closely with our operational teams and put some drive into the project.*»

Technical reports offer security managers details on the criticality of each vulnerability discovered, the consequences of an exploit, the corrective action required, and links to the official patches. Higher level reports provide Sodexho's general managers with a global view of the state of security at the company and allow them to track security progress over time.

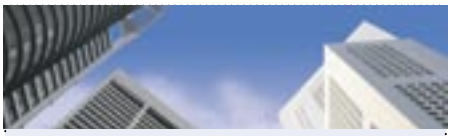
Sodexho set up its account with 74 users, 6 Business Units and 7 Managers and works with each organisational unit to give them control and responsibility over their own resources.

> *"The on demand model is the best security approach for managing vulnerabilities and patches within a decentralized organization. It allows branches to be self-sufficient. Now, I can easily check the application of security measures via dynamic reports."*
>
> ***Joe Ford.***

Today, the group's subsidiaries are all more aware of the vulnerability management programme and the best scores are published on the Group intranet. In less than a year, Sodexho has decreased its vulnerabilities by 40%.

«*We are very happy with the support from the Qualys team. They worked with us in modifying the user interface, which was not too user-friendly at first, and make it easier to obtain the support of all our subsidiaries.*» concludes Ford.

«*Our successful with experience on our external networks convinced us we should also implement the solution internally. The reports act as a very powerful management tool, and not simply just a pile of security data. I am sure our operations teams will be able to easily prioritise their actions and cope with managing both internal and external threats.*"



QUALYSGUARD® ENTERPRISE

CONTEXT

- Network topology, system configurations and security level unknown
- No vulnerability management solution
- No ability to centralise the supervision

NEEDS

- Establish a consistent policy throughout the group
- Centralise network security supervision
- Implement a proactive subsidiary autonomy

2 KEY FACTORS FOR SUCCESS

- **Self-management for subsidiaries**
  - Preservation of the decentralised organisation
  - A solution on demand: easy to implement, to use and to manage
  - Operational teams
  - Involvement of the IT Managers and the operational teams
- **Definition of a clear methodology**
  - Prioritisation of tasks and devices
  - Definition of realistic goals for remediation

07/2004 - Printed in France