# Leader Européen des Solutions CRM pour le Secteur Pharmaceutique

*« Auparavant, la gestion des vulnérabilités était laborieuse, aléatoire et beaucoup trop consommatrice de temps. Cette charge ne pouvant être prise en compte dans l'environnement actuel, CEGEDIM devait pouvoir s'appuyer sur une solution rapide, simple et pragmatique. Avec les rapports fournis par QualysGuard, l'équipe ne consacre plus que 10% de son temps à identifier les failles dignes d'attention. Un retour sur investissement indiscutable ! »*

Frédéric Callard, Responsable Réseaux & Télécoms
**CEGEDIM**

Cegedim a pour principal objectif d'apporter aux laboratoires pharmaceutiques les bases de données et les outils informatiques les plus performants afin d'optimiser leur communication avec les professionnels de santé.

Les savoirs faire requis sur ce coeur de métier ont conduit rapidement le Groupe à maîtriser les technologies et les services de pointe relatifs aux bases de données, aux applications de gestion, à l'informatique, à Internet et aux réseaux.

« *Notre activité et surtout notre secteur d'intervention font de la sécurité des systèmes d'information un élément crucial de notre offre. Nous accédons et hébergeons des données confidentielles sur l'activité de nos clients. Un incident majeur de sécurité entraînerait une perte de revenus considérables pour notre société, et plus grave, une perte de notre capital confiance que le Groupe a mis des années à bâtir et qui serait difficilement rattrapable. Dans ce contexte, nous ne pouvons pas nous permettre de voir nos réseaux attaqués par négligence. Et, malgré un réseau concentré et des équipes sécurité attentives, Cegedim a fait de la prévention et de la gestion des risques informatiques une priorité* » déclare le Responsable du projet.

**Garantir le niveau de sécurité et assurer la continuité de l'activité**

Cegedim dispose d'un réseau informatique centralisé. Bien que présent dans 80 pays à travers le monde, l'infrastructure informatique a depuis le départ été concentrée en un lieu unique où sont présents les 600 serveurs de l'entreprise. Si cette organisation limite les risques d'attaques et facilite la gestion de l'infrastructure dans son ensemble, elle n'exclut pas pour autant les risques d'impact sur l'activité du Groupe.

«*C'est probablement la centralisation de nos systèmes informatiques qui nous a fait prendre conscience de la nécessité de mener une politique de sécurité proactive de gestion des risques. Avant l'utilisation de QualysGuard, nous récoltions les informations sur les alertes de manière aléatoire, via les bulletins publiés par les différents éditeurs, sans méthodologie établie ni personne responsable des mises à jour.* » Souligne le responsable du projet. *« Dans ces conditions, difficile de vérifier l'application des patchs, des actions correctives et quasiment impossible de définir des standards pour l'ensemble des serveurs !*»

En 2002, le Groupe prend conscience de la nécessité de mettre en place une politique de gestion des risques continue et rigoureuse. Avec la complexification des attaques, notamment l'apparition de plus en plus fréquente des attaques applicatives, ainsi que la généralisation d'Internet dans le secteur de la santé, Cegedim ne veut pas prendre le risque de compromettre sa réputation et son activité. De plus, les solutions de Cegedim se doivent d'allier performance et conformité avec le Code de la Santé Publique ainsi que les réglementations Informatiques et Liberté en vigueur dans tous les pays concernés, ce qui entraîne différentes contraintes en terme de sécurité informatique, à respecter.

«*L'utilisation systématique du port 80, par exemple, était devenue problématique. Ce port, qui doit être obligatoirement ouvert pour accéder à Internet, était celui de toutes les vulnérabilités. En interne, les ressources nécessaires à la surveillance de nos différentes applications aux nouvelles formes d'attaques étant considérables et ne pouvant pas fonctionner en mode fermé, la mise en place d'une méthodologie rigoureuse de gestion des risques devenait une urgence !*» Se rappelle le responsable du projet.

**Connaître le réseau et détecter les vulnérabilités**

Cependant chez Cegedim, urgence ne signifie pas précipitation. L'équipe sécurité du groupe a évalué pendant huit mois plusieurs solutions, dont Intranode, Nessus, Foundstone ou encore E eye, avant de retenir QualysGuard pour gérer la sécurité de ses 160 serveurs publics.

*«Nous avons mis en place une plateforme de tests afin de choisir la solution la mieux adaptée à nos contraintes et à nos exigences. Nous avons retenu Qualys pour 3 raisons: ses performances techniques, son orientation métier et son TCO. La solution propose une interface où toutes les fonctionnalités sont facilement accessibles et le modèle on demand répondait à nos contraintes : une solution utilisable par tous, ne nécessitant aucune ressource pour assurer le déploiement et la maintenance de la solution»* complète le responsable du projet.

La première étape a été de mener un inventaire afin de recenser tous les dispositifs visibles sur le réseau externe. Ensuite, Cegedim a mené des audits de vulnérabilités afin de définir son niveau réel de sécurité.

*«Auparavant, la gestion des vulnérabilités était laborieuse, aléatoire et beaucoup trop consommatrice de temps. Cette charge ne pouvant être prise en compte dans l'environnement actuel, CEGEDIM devait pouvoir s'appuyer sur une solution rapide, simple et pragmatique. Avec les rapports fournis par QualysGuard, l'équipe ne consacre plus que 10% de son temps à identifier les failles dignes d'attention. Un retour sur investissement indiscutable !»*

Pour toute détection d'une faille, QualysGuard définit son degré de sévérité en combinant différents paramètres : la typologie de la faille mais aussi le dispositif concerné et son niveau de criticité. Cela permet aux équipes de se focaliser sur les menaces en fonction de leur impact sur l'activité de l'entreprise. De plus, un lien vers les correctifs officiels est proposé ce qui permet à l'équipe Sécurité de réagir immédiatement aux vulnérabilités à haut risque : elle alerte le service concerné et gère, avec ses ingénieurs, les actions de correction qui s'imposent.

«Nous avons d'abord connu une phase de « mise en route », où la priorité a été la mise en conformité du niveau de sécurité sur l'ensemble des réseaux externes. Les équipes opérationnelles disposaient, par exemple, d'un mois pour corriger les vulnérabilités de niveau 4 et 5. Aujourd'hui, une gestion beaucoup plus dynamique et proactive a pu s'instaurer.»

**Automatiser la gestion des vulnérabilités grâce à des rapports dynamiques**

Basé sur les rapports fournis par QualysGuard, Cegedim a mis en place un comité de contrôle des vulnérabilités constitué des administrateurs des services concernés.

Deux journées d'information ont permis de sensibiliser les équipes système au projet et de les former sur la solution de Qualys. Désormais, chaque équipe de production dispose d'un compte afin de gérer de manière autonome les dispositifs qui la concernent. Chaque mois, chaque responsable édite un rapport afin de vérifier les actions réalisées et de définir les objectifs de chacun pour le mois à venir.

«Aujourd'hui, nous avons la certitude que les patchs sont mis à jour, que les règles de la politique de sécurité sont respectées et que la configuration des équipements est adaptée» déclare le responsable du projet.

Cegedim souhaite maintenant déployer QualysGuard sur ses réseaux internes. «Avant d'utiliser QualysGuard, compte tenu notre charge de travail que demande ce service, instaurer ce projet en interne nous semblait impossible. Mais notre expérience sur nos réseaux externes nous a convaincus de la faisabilité du projet. La charge de travail pour maintenir un niveau de sécurité en accord avec les attentes de nos clients internes comme externes est maintenant tout à fait acceptable et cette charge est devenue gérable par les équipes en place qui soutiennent d'ailleurs désormais l'extension de la politique de gestion des vulnérabilités à nos réseaux internes.»

## PRESENTATION DE CEGEDIM

Cegedim compte 7200 collaborateurs et a réalisé en 2006 un chiffre d'affaires de 541 millions d'euros. Dendrite inclus, le chiffre d'affaires 2006 en base annuelle cumulée s'établirait à 877 millions d'euros.
- 80 pays connectés
- 170 serveurs externes
- 10 domaines

## ACTIVITE

Leader en Europe sur son cœur de métier historique, CEGEDIM accompagne les plus grands laboratoires pharmaceutiques mondiaux dans leurs projets de CRM (Customer Relationship Management) et mesure l'efficacité de leurs actions marketing-vente. Avec ses outils de CRM, fortement valorisés par les bases de données stratégiques du Groupe, CEGEDIM apporte aux départements marketing et ventes un éclairage avisé sur leur marché et leurs cibles, afin d'optimiser leurs stratégies et leur retour sur investissement.

## PROBLEMATIQUE

**Le contexte**
- Pas de vue globale du niveau de sécurité du Groupe
- Gestion des vulnérabilités de manière aléatoire
- Augmentation croissante des risques

**Les besoins**
- Superviser de manière globale le niveau de sécurité
- Instaurer une méthodologie de gestion de vulnérabilités rigoureuse et continue
- Impliquer les services de production et déléguer les actions correctives aux équipes opérationnelles
- Disposer de rapports concis sur l'évolution du niveau de sécurité pour la Direction Générale

## LES FACTEURS CLES DE SUCCES

**L'implication des équipes opérationnelles**
- Formations pour sensibiliser les équipes et leur permettre de maîtriser la solution QualysGuard
- Création d'un compte pour chaque équipe de production afin de permettre une autonomie de management

**Une solution en adéquation avec les ressources du Groupe**
- Pas de maintenance et une mise à jour quotidienne et automatique de la base de vulnérabilités
- Hiérarchisation des menaces selon leur niveau de criticité
- Des informations précises sur les actions à mener

## SITE WEB

www.cegedim.com


QUALYS®
www.qualys.com

**USA – Qualys, Inc.**
1600 Bridge Parkway
Redwood Shores
CA 94065
Tél. : 1 (650) 801 6100
sales@qualys.com

**Royaume-Uni – Qualys, Ltd.**
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
Tél. : +44 (0) 1753 872101

**Allemagne – Qualys GmbH**
Aéroport de Munich
Terminalstrasse Mitte 18
85356 Munich
Tél. : +49 (0) 89 97007 146

**France – Qualys Technologies**
Maison de la Défense
7, Place de la Défense
92400 Courbevoie
Tél. : +33 (0) 1 41 97 35 70

ON DEMAND SECURITY