



OFFRIR UN SLA SÉCURITÉ ROBUSTE ET INDUSTRIALISÉ.

Offrir une garantie de sécurité à ses clients est un exercice périlleux. Surtout si l'on ne maîtrise pas les plate-formes que l'on accepte de garantir car elles sont gérées par le client ! C'était pourtant l'ambition de l'hébergeur Agarik : assurer à ses clients grands comptes un niveau de sécurité correspondant à l'Etat de l'Art du moment. Et accepter la responsabilité d'un piratage éventuel si ce dernier devait exploiter une vulnérabilité connue.

“Malgré son coût, la prévention est vitale en matière de sécurité. Je considère qu'il s'agit d'une faute de la part d'un DSI de ne pas faire auditer sa sécurité.”



Laurent Seror, Directeur
Opérationnel
Agarik

“Qualys est notre juge de paix : si nous sommes piratés via une vulnérabilité qu'il avait identifié, nous sommes responsables. Mais cela n'est encore jamais arrivé sur des clients protégés par QualysGuard”
Laurent Seror, Directeur opérationnel d'Agarik.

Fournir un tel SLA (Service Level Agreement) n'a que peu de sens si l'on décide seul de ses conditions d'application. Il est en effet guère crédible d'être juge et partie au moment de déterminer les responsabilités afin de dédommager un client.

“Nous avons donc recherché un tiers de confiance qui permette de donner une vision indépendante de l'état de sécurité de la plate-forme”, se souvient Laurent Seror, Directeur opérationnel d'Agarik.

Pour cela l'hébergeur se tourne d'abord vers des outils d'audit de vulnérabilité logiciels exploités en interne. “Mais cela ne réglait pas le problème : nous étions toujours à l'origine des mesures et il n'y avait donc aucune indépendance”, poursuit-il.

Agarik testera alors - sans succès - une offre en ligne concurrente avant de porter son choix sur Qualys. “Nous avons bien entendu apprécié la qualité des analyses, mais c'est tout de même le minimum que l'on attend d'un service de ce type. Nous y avons surtout trouvé un outil parfaitement industrialisable, ce qui est un critère essentiel pour nous”, explique Laurent Seror.

Equipes réduites et industrialisation poussée

Essentiel car depuis 1997 Agarik mise fortement sur l'industrialisation de ses processus: l'hébergeur a développé un outil de workflow propriétaire capable d'assurer la supervision et d'automatiser la gestion de son Système d'Information à travers des interfaces web. La solution d'audit des vulnérabilités choisie doit donc pouvoir s'y intégrer et devenir un indicateur comme les autres.

“Notre workflow est un développement entièrement propriétaire, mais construit autour de standards”, explique Laurent Seror. La plate-forme est en effet bâtie sur une base Oracle (pour l'enregistrement des alertes en temps réel) et MySQL (pour la gestion de l'inventaire), animée par un moteur écrit en C++, lui-même étendu par des plugins Java. Son interface utilise Ajax et PHP, ainsi qu'un peu de Perl pour assurer la connectivité avec un serveur SMTP. Enfin, l'ensemble communique via XML et des messages SOAP qui se chargent de normaliser les différentes sources d'informations (les “sondes”) chargées d'ausculter le réseau et les serveurs.

Et c'est précisément là que QualysGuard a tiré son épingle du jeu : “Son grand atout est de pouvoir s'intégrer à notre plate-forme via sa librairie MSAPI (Managed Service API, fournie par l'éditeur). Grâce à cela, le service d'audit des vulnérabilités devient une source XML que nous surveillons parmi d'autres”, se félicite Laurent Seror.

L'intégration n'aura demandé qu'une dizaine de jours à un développeur en interne : les deux applications étaient déjà “orientées service” et leur connexion s'en est trouvée grandement facilitée par l'ouverture intrinsèque de XML. Il aura suffi à Qualys de fournir une DTD (définition de document XML) permettant d'interpréter automatiquement les rapports d'analyse des vulnérabilités, et à Agarik de l'intégrer à un “parser” XML de son crû.

Un traitement automatisé

Concrètement des analyses sont lancées automatiquement chaque nuit. “Le rapport est alors récupéré au format XML et traité par notre parser. Les résultats peuvent ensuite être injectés dans notre moteur de règles. En fonction de la criticité des événements, et du seuil de déclenchement choisi par chaque client, le moteur remonte les alertes. Elles apparaissent alors dans la console unique qui nous sert à piloter la totalité de notre infrastructure, au côté des autres indicateurs”, détaille Laurent Seror.

La gestion de la sécurité devient ainsi un service comme un autre. “Au même titre que l'état des serveurs Apache ou de la connectivité, la sécurité doit être au vert. Et je suis au vert lorsque QualysGuard n'a pas découvert de vulnérabilité exploitable”, résume le directeur opérationnel.

Lorsque ce n'est pas le cas, en revanche, la plate-forme d'Agarik facilite également le suivi des incidents. L'hébergeur contacte le client et applique des mesures de contournement. Celles-ci peuvent être fournies avec le rapport de Qualys, spécifiées par le client ou encore venir de la propre base de connaissances d'Agarik. “Tout cela est suivi et documenté, et chaque intervention met à jour le ticket d'incident jusqu'à sa résolution”, se félicite Laurent Seror.

Le client, lui, en prendra connaissance en temps réel dans sa propre console d'administration ou durant le comité de pilotage mensuel avec les équipes d'Agarik.

Un service évolutif ouvert aux clients

Chaque client dispose d'une version à périmètre réduit de la console d'Agarik, limitée à ses propres systèmes. Il peut ainsi suivre en temps réel l'évolution des analyses de vulnérabilités programmées ou en commander de nouvelles à volonté. “Si ces dernières remontent des vulnérabilités qui n'avaient pas encore été identifiées, nous en sommes prévenus en même temps que le client. Le processus de résolution est alors exactement le même : une alerte apparaît sur la console principale et un technicien doit l'acquiescer”, précise Laurent Seror.

Pour l'heure la corrélation des événements est réalisée par un technicien. Mais Agarik prévoit d'étendre sa plate-forme afin de faire du diagnostic et de la résolution automatique, grâce à un véritable moteur de corrélation. “L'objectif est de traiter automatiquement 80% des problèmes que nous rencontrons quotidiennement”, ambitionne Laurent Seror.

L'autre grande évolution de la plate-forme concerne enfin ITIL. “C'est un chantier en cours depuis notre rachat par Bull. Nous travaillons actuellement à intégrer notre workflow dans une démarche ITIL. Ce ne devrait pas être une difficulté majeure car l'essentiel est déjà là. C'est surtout une question de sémantique”, reconnaît Laurent Seror. En effet, en prenant en charge via QualysGuard les incidents de sécurité, en les traitant avec les autres événements de production et en les intégrant dans un système de gestion de tickets, la plate-forme en place fait déjà presque de l'ITIL sans le savoir.

LE METIER

Agarik est un hébergeur à forte valeur ajoutée. Son rôle est de décharger la DSI de la tâche d'exploitation des plates-formes tout en conservant ses méthodes de travail (processus et reporting propres à l'entreprise).

LE PERIMETRE

Quarante personnes, dont environ 10% affectées à la R&D, pour un chiffre d'affaire prévisionnel de 7 millions d'euros en 2007. Agarik gère pour ses clients des plates-formes Windows, Solaris, Linux (LAMP) et FreeBSD, ainsi que tout types de serveurs applicatifs.

LE PROBLEME

Offrir un SLA sur la sécurité alors que l'hébergeur n'a pas le contrôle des serveurs et des applications mises en ligne par ses clients. Il lui faut trouver un “juge de paix” capable d'arbitrer le SLA.

LE DEFI OPERATIONNEL

La solution choisie doit être industrialisable. Elle doit s'intégrer parfaitement à un workflow propriétaire basé sur les services web (SOAP et XML). Pour cela, elle doit être conçue comme une application orientée service (SOA).

LA SOLUTION

QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode “Software as a Service” (SaaS). Utilisation des rapports au format XML et intégration à l'aide de la bibliothèque MSAPI (Managed Services API) de Qualys. Ajout de deux boîtiers d'audit sur le réseau interne.

POURQUOI QUALYS ?

- Flexibilité (ouverture du service via une API)
- Accompagnement technique de bonne qualité.
- Forte expertise en sécurité.
- Culture technique proche de celle d'Agarik.

SITE WEB

www.agarik.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

