Brinks anticipe les audits sécurité du Groupe avec Qualys

La filiale française parvient à tenir les délais imposés par les standards du groupe Brinks en anticipant les audits.

Avec 70 000 personnes dans plus de cent pays, les camions de transport de fonds de la Brinks ont une image bien connue. Mais au delà des fonds, la société est aussi un spécialiste de la sécurité des biens précieux au sens large (bijoux, métaux précieux), des coffres forts, du traitement des chèques et même de la sécurité aérienne.

Basé aux Etats-Unis, le siège du groupe impose des règles de sécurité strictes à ses filiales. Et justement, la filiale française était confrontée à un défi de taille : bien qu'étant la plus importante d'Europe elle était fort naturellement tenue aux mêmes exigences de sécurité que les autres, qui ont moins de serveurs et un périmètre moins important à surveiller. "Nous étions comparés aux autres filiales en valeur absolue sur le nombre d'anomalies, et le temps de résolution exigé est le même pour tout le monde car il ne tient compte que de la criticité de la vulnérabilité. Ainsi des filiales qui ont peu de serveurs ont en principe moins de vulnérabilités et plus de temps pour les corriger. Donc, nos infrastructures étaient scannées par les Etats-Unis régulièrement et nous nous faisions régulièrement épinglés", se souvient Vincent Lauriat, DSI de la Brinks. Le standard du Groupe engage en effet contractuellement les filiales sur les délais de résolution. Le choix est alors fait de s'équiper d'une solution de gestion de vulnérabilités et de conformité propre à la filiale française afin d'anticiper les audits du siège et disposer ainsi de plus de temps pour leur correction.

BRINKS

www.brinks.fr

NDUSTRIE : Banques / Sécurité

METIER : Transport de fond et gestion du backoffice fiduciaire

PERIMETRE : National

TAILLE : 6000 employés

DÉFI OPÉRATIONNEL : Se préparer aux audits menés par la Sécurité Groupe depuis les Etats-Unis afin de disposer d'une marge de manoeuvre plus importante pour corriger les vulnérabilités et respecter les engagements pris par le DSI et la DG France auprès du Groupe.

SOLUTION:
QualysGuard VM & PC

POURQUOI QUALYSGUARD :

- Outil indépendant des équipes, en mode SaaS
- Solution utilisée par la Sécurité Groupe
- Solution reconnue par l'auditeur français
- Lien entre les références Qualys et CVE pour les vulnérabilités
- Déploiement instantané
- Simplicité de prise en main

Un regard extérieur sur les vulnérabilités

"Nous avions déjà des outils d'analyse des vulnérabilités Open Source, mais peu de processus industrialisés et formalisés. Et en plus ils étaient utilisés par la même équipe qui exploite la production informatique, elle était donc juges et partie. Nous recherchions ainsi une solution SaaS du marché, afin d'avoir une vue de notre posture sécurité depuis l'extérieur par un tiers !", explique Vincent Lauriat.

"Avec une informatique très centralisée pour une centaine de sites, nous étions auparavant plutôt en mode réactif, alors qu'avec l'asset management de QualysGuard nous pouvons être proactifs pour découvrir et corriger nos postes informatiques"

Vincent Lauriat,
DSI de la Brinks

Au moment du choix, l'offre de Qualys s'est imposée pour des raisons très pragmatiques. "C'était un choix de facto car il s'agit déjà de la solution utilisée par les Etats-Unis pour nous évaluer. Il nous semblait donc logique de choisir la même solution pour être sur le même barème. Et puis notre auditeur SOX externe nous a rassuré en nous disant qu'il reconnaissait les rapports Qualys comme faisant foi", poursuit le DSI. La conduite du changement et l'appropriation de la solution ont été facilitées : en effet plusieurs nouvelles recrues à la SSI connaissent déjà le produit.

Après un rapide test d'une version d'évaluation gratuite, Brinks commande un lot d'adresses IP externes et ses équipes se mettent immédiatement au travail car l'horloge tourne ! L'objectif est de rattraper l'écart avec les exigences du Groupe avant le prochain audit. "La prise en main a été très rapide, et nous étions immédiatement opérationnels. Je le dis d'autant plus volontiers que je n'ai jamais lu une documentation Qualys", reconnaît Stéphane Guyodo, Responsable Innovation IT et Sécurité.

Parallèlement au démarrage des analyses automatiques, l'équipe rencontre les métiers pour leur présenter un plan d'actions et les sensibiliser : "On a bien fait comprendre aux équipes de la DSI et aux métiers que nous étions soumis par le Groupe, de manière contractuelle, à corriger toutes les vulnérabilités de niveau 3, 4 et 5. Cet engagement a été signé par le PDG et moi-même. Et qu'il faudra donc s'y tenir fermement !", se souvient Vincent Lauriat.

Mais le DSI a une autre bonne raison d'être exigeant sur ce point particulier : il souhaite éviter à tout prix de devoir entrer dans le processus de remédiation imposé par le Groupe. "Lorsque le siège aux Etats-Unis nous remonte une vulnérabilité on entre alors dans un processus très lourd. Et surtout si l'on ne peut pas la corriger dans les délais imposés, il faut alors aller se justifier dans un progiciel de conformité interne dédié à SOX, qui ne concerne pas que l'informatique mais tous les processus touchés par la loi SOX (comptabilité, paie…). Nous souhaitons être exemplaires et conformes aux exigences du Groupe !"

Désormais, il n'existe plus de vulnérabilités externes critiques (niveaux 5,4, 3) et l'attention se tourne désormais vers les failles de niveau 1 et 2. Sur l'interne, les équipes analysent désormais en priorité les serveurs et intègrent chaque nouveau poste de travail mastérisé au plan d'analyse automatique (et une copie du master est régulièrement re-scannée afin d'identifier d'éventuelles vulnérabilités présentes qui viendraient d'être ajoutées à la base des signatures QualysGuard).

Des procédures de remédiation internes

Toutes les vulnérabilités découvertes font l'objet d'une procédure de remédiation propre à la filiale. "Nous utilisons l'outil de gestion des tickets intégré à la solution QualysGuard. Nous apprécions

d'ailleurs le fait de pouvoir générer un rapport au format PDF pour chaque ticket, que l'on dirige ensuite vers le bon contact pour correction, sans avoir besoin de donner un accès à la plate-forme en ligne", précise Stéphane Guyodo. Ces tickets sont ensuite suivis dans un outil spécifique destiné aux interventions de prestataires chargé de les appliquer. Autre point appréciable : jusqu'à présent personne n'a remis en question la pertinence des tickets. "Les vulnérabilités découvertes sont toujours acceptées et non discutées !", apprécie Stéphane Guyodo.

Maintenant que les choses sont sous contrôle, l'équipe de Vincent Lauriat a d'autres projets pour la solution QualysGuard. "Nous envisageons d'étendre son usage vers la conformité SOX, en pouvant prouver un certain niveau de configuration pour certaines machines, voire tout simplement leur existence. Et c'est là que l'historisation des analyses va s'avérer très utile. Et puis on pourra aussi mettre un tag sur chaque actif afin de déterminer lesquelles sont soumises à SOX. Cela nous permettra d'être beaucoup plus fins dans la remédiation : par exemple si l'on doit corriger un équipement qui nécessite un redémarrage, mais que ce n'est pas le bon moment, on pourra être plus souples si on sait qu'il ne s'agit pas d'une machine du périmètre SOX", conclue Stéphane Guyodo.