

Qualys enrichit QualysGuard Vulnerability Management en intégrant les bases d'*exploits* fournies par Core Security, Immunity, Metasploit et The Exploit-DataBase

Les entreprises disposent maintenant d'une solution clé en main pour hiérarchiser et remédier plus efficacement à leurs problèmes de sécurité critiques

Black Hat, Las Vegas, NV – le 27 juillet 2010 Qualys®, Inc., le principal fournisseur de solutions à la demande pour la gestion des risques de sécurité informatique et de la conformité, annonce l'intégration au sein de QualysGuard Vulnerability Management (VM) d'informations sur les *exploits* en temps réel. Ces dernières sont corrélées aux vulnérabilités identifiées et fournissent des références pertinentes et actualisées sur les *exploits* et les ressources de sécurité associées. Grâce à cette nouvelle fonctionnalité, les entreprises qui effectuent des analyses de vulnérabilité peuvent facilement consulter les tout derniers *exploits* grâce aux bases intégrées de fournisseurs tiers tels que Core Security et Immunity ainsi que les informations associées sur ces *exploits* fournies par Metasploit et The Exploit-DataBase. Les entreprises peuvent désormais définir des priorités de remédiation en fonction du niveau de risque évalué pour les *exploits* corrélés.

Auparavant, les analyses de vulnérabilités permettaient d'obtenir une liste de failles et de leurs expositions (CVE) ; les *exploits* pour chaque CVE devaient ensuite être recherchés manuellement, mobilisant le personnel chargé de la sécurité ou les consultants. Maintenant, les scans QualysGuard VM génèrent automatiquement une liste d'*exploits* disponibles pour chaque CVE en s'appuyant sur les bases de données d'*exploits* vérifiés les plus complètes de Core Security, Immunity, The Exploit-DataBase ou Metasploit. Ainsi, les entreprises peuvent évaluer rapidement et facilement le niveau de risque de chaque vulnérabilité et hiérarchiser leur plan de remédiation en conséquence. Les informations sur les *exploits* peuvent aussi être intégrées aux rapports d'analyse pour fournir une vue plus complète des risques de sécurité. En outre, les entreprises qui utilisent ces outils de test d'intrusion peuvent générer des rapports leur permettant d'identifier et lancer les *exploits* sur des cibles précises.

« Grâce à la collaboration entre Qualys et des fournisseurs de tests d'intrusion de premier ordre, la corrélation manuelle des vulnérabilités avec les exploits est supprimée, » déclare Wolfgang Kandek, directeur technique de Qualys. *« Les professionnels chargés de la sécurité et les consultants voient plus clairement l'exploitabilité des actifs informatiques et peuvent consacrer davantage de temps à remédier les problèmes et à planifier de manière proactive leur stratégie de sécurité. »*

La nouvelle fonctionnalité de corrélation d'exploitabilité comprend :

- Des bases mise à jour en temps réel sur les *exploits* fournis par Core Security, Immunity (et leurs partenaires Agora, Dsquare, Enable Security et White Phosphorous), Metasploit et The Exploit-DataBase. Les entreprises peuvent sélectionner la source des données d'*exploits* de leur choix.
- Une colonne « Exploitability » dans la base de connaissances QualysGuard indiquant si des *exploits* ou informations d'exploitabilité sont disponibles pour une vulnérabilité auprès de fournisseurs tiers et/ou de sources publiques.
- Les détails des *exploits* pour une vulnérabilité sélectionnée, notamment la référence CVE, une description de l'*exploit* fourni par la source et un lien vers l'*exploit* quand disponible.
- La possibilité d'inclure ces données dans des rapports d'analyse de vulnérabilités.

« Depuis des années, Core Security est au cœur de l'intégration des solutions d'analyse et de test de la sécurité. Les entreprises s'appuient sur cette intégration entre QualysGuard et IMPACT Pro pour améliorer leurs processus de gestion des vulnérabilités, » déclare Fred Pinkett, vice-président chargé

des produits chez Core Security. « Ce nouveau niveau d'informations fournira des données plus précieuses et utiles aux entreprises qui utilisent QualysGuard et ces dernières pourront donc définir des priorités de remédiation et optimiser leur programme de sécurité. »

« En raison de menaces toujours plus nombreuses et de l'adoption par les entreprises de nouvelles architectures informatiques, il est plus que jamais important de planifier de manière proactive des mesures de sécurité pour protéger les données sensibles de l'entreprise, » déclare Justine Aitel, CEO d'Immunity. « En intégrant les informations sur les exploits fournies par Immunity CANVAS avec les données de vulnérabilités de QualysGuard VM, nous offrons à notre clientèle commune une solution unique pour maîtriser leur exposition aux risques. Grâce à cette stratégie, les entreprises pourront hiérarchiser efficacement leurs efforts de remédiation et ainsi améliorer la coordination entre les équipes opérationnelles et celles chargées de la sécurité. »

Disponibilité

La nouvelle fonctionnalité d'exploitabilité est disponible dès aujourd'hui avec QualysGuard VM. Pour obtenir plus d'informations sur cette fonctionnalité et visionner une présentation en direct, rendez-vous sur le site de la communauté Qualys : <http://community.qualys.com/community/qualysguard/vm>.

A propos de Qualys

Qualys® Inc est le principal fournisseur de solutions « à la demande » pour la gestion des vulnérabilités et de la conformité sous la forme de services (SaaS). Déployables en quelques heures seulement, partout dans le monde, les solutions SaaS de Qualys fournissent aux entreprises une vue immédiate et permanente de l'état de leur sécurité et de leur conformité.

Actuellement utilisé par plus de 4000 entreprises dans 85 pays, dont 42 des 100 premières sociétés mondiales du classement établi par Fortune, le service QualysGuard® réalise plus de 500 millions d'audits IP par an. Qualys a opéré le plus important déploiement de ressources de gestion des vulnérabilités au monde au sein d'une société figurant parmi les 50 premières entreprises mondiales du classement Fortune.

Qualys a signé des accords stratégiques avec des fournisseurs de services d'infogérance (« managed services ») de premier ordre et des cabinets de conseil tels que BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, SecureWorks, Symantec, Tata Communications et TELUS.

Plus d'information sur www.qualys.com