QualysGuard Vulnerability Management, gestion des risques de sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 29/7/2010 0:00:00

Les entreprises disposent maintenant dâ□□une solution clÃ© en main pour hiÃ©rarchiser et remÃ©dier plus efficacement Ã leurs problÃ¨mes de sÃ©curitÃ© critiques. Qualys, Inc., annonce lâ□□intÃ©gration au sein de **QualysGuard Vulnerability Management** (VM) dâ□□informations sur les exploits en temps rÃ©el.

Ces derniÃ¨res sont corrÃ©lÃ©es aux vulnÃ©rabilitÃ©s identifiÃ©es et fournissent des rÃ©fÃ©rences pertinentes et actualisÃ©es sur les exploits et les ressources de sÃ©curitÃ© associÃ©es. GrÃ¢ce Ã cette nouvelle fonctionnalitÃ©, les entreprises qui effectuent des analyses de vulnÃ©rabilitÃ© peuvent facilement consulter les tout derniers exploits grÃ¢ce aux bases intÃ©grÃ©es de fournisseurs tiers tels que Core Security et Immunity ainsi que les informations associÃ©es sur ces exploits fournies par Metasploit et The Exploit-DataBase. Les entreprises peuvent dÃ©sormais dÃ©finir des prioritÃ©s de remÃ©diation en fonction du niveau de risque Ã©valuÃ© pour les exploits corrÃ©lÃ©s.

Auparavant, les analyses de vulnÃ©rabilitÃ©s permettaient dâ□□obtenir une liste de failles et de leurs expositions (CVE) ; les exploits pour chaque CVE devaient ensuite Ãªtre recherchÃ©s manuellement, mobilisant le personnel chargÃ© de la sÃ©curitÃ© ou les consultants. Maintenant, les scans QualysGuard VM gÃ©nÃ¨rent automatiquement une liste dâ□□exploits disponibles pour chaque CVE en sâ□□appuyant sur les bases de donnÃ©es dâ□□exploits verifiÃ©s les plus complÃ¨tes de Core Security, Immunity, The Exploit-DataBase ou Metasploit. Ainsi, les entreprises peuvent Ã©valuer rapidement et facilement le niveau de risque de chaque vulnÃ©rabilitÃ© et hiÃ©rarchiser leur plan de remÃ©diation en consÃ©quence. Les informations sur les exploits peuvent aussi Ãªtre intÃ©grÃ©es aux rapports dâ□□analyse pour fournir une vue plus complÃ¨te des risques de sÃ©curitÃ©. En outre, les entreprises qui utilisent ces outils de test d'intrusion peuvent gÃ©nÃ©rer des rapports leur permettant dâ□□identifier et lancer les exploits sur des cibles prÃ©cises.

Â« *GrÃ¢ce Ã la collaboration entre Qualys et des fournisseurs de tests d'intrusion de premier ordre, la corrÃ©lation manuelle des vulnÃ©rabilitÃ©s avec les exploits est supprimÃ©e,* Â» dÃ©clare **Wolfgang Kandek**, directeur technique de Qualys. Â« *Les professionnels chargÃ©s de la sÃ©curitÃ© et les consultants voient plus clairement lâ□□exploitabilitÃ© des actifs informatiques et peuvent consacrer davantage de temps Ã remÃ©dier les problÃ¨mes et Ã planifier de maniÃ¨re proactive leur stratÃ©gie de sÃ©curitÃ©.* Â»

La nouvelle fonctionnalitÃ© de corrÃ©lation dâ□□exploitabilitÃ© comprend :

â□¢ Des bases mise Ã jour en temps rÃ©el 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 sÃ©lectionner la source des donnÃ©es dâ□□exploits de

leur choix.

â¢ Une colonne Â« Exploitability Â» dans la base de connaissances QualysGuard indiquant si des exploits ou informations dâexploitabilitÃ© sont disponibles pour une vulnÃ©rabilitÃ© auprÃ¨s de fournisseurs tiers et/ou de sources publiques.

â¢ Les dÃ©tails des exploits pour une vulnÃ©rabilitÃ© sÃ©lectionnÃ©e, notamment la rÃ©fÃ©rence CVE, une description de lâexploit fourni par la source et un lien vers lâexploit quand disponible.

â¢ La possibilitÃ© dâinclure ces donnÃ©es dans des rapports dâanalyse de vulnÃ©rabilitÃ©s.

Â« *Depuis des annÃ©es, Core Security est au cÅur de lâintÃ©gration des solutions dâanalyse et de test de la sÃ©curitÃ©. Les entreprises sâappuient sur cette intÃ©gration entre QualysGuard et IMPACT Pro pour amÃ©liorer leurs processus de gestion des vulnÃ©rabilitÃ©s,* Â» dÃ©clare **Fred Pinkett**, vice-prÃ©sident chargÃ© des produits chez Core Security. Â« *Ce nouveau niveau dâinformations fournira des donnÃ©es plus prÃ©cieuses et utiles aux entreprises qui utilisent QualysGuard et ces derniÃ¨res pourront donc dÃ©finir des prioritÃ©s de remÃ©diation et optimiser leur programme de sÃ©curitÃ©.* Â»

Â« *En raison de menaces toujours plus nombreuses et de lâadoption par les entreprises de nouvelles architectures informatiques, il est plus que jamais important de planifier de maniÃ¨re proactive des mesures de sÃ©curitÃ© pour protÃ©ger les donnÃ©es sensibles de lâentreprise,* Â» dÃ©clare **Justine Aitel**, CEO dâImmunity. Â« *En intÃ©grant les informations sur les exploits fournies par Immunity CANVAS avec les donnÃ©es de vulnÃ©rabilitÃ©s de QualysGuard VM, nous offrons Ã notre clientÃ¨le commune une solution unique pour maÃ®triser leur exposition aux risques. GrÃ¢ce Ã cette stratÃ©gie, les entreprises pourront hiÃ©rarchiser efficacement leurs efforts de remÃ©diation et ainsi amÃ©liorer la coordination entre les Ã©quipes opÃ©rationnelles et celles chargÃ©es de la sÃ©curitÃ©.* Â»

DisponibilitÃ©

La nouvelle fonctionnalitÃ© dâexploitabilitÃ© est disponible dÃ¨s aujourdâhui avec **QualysGuard VM**.