CONTINUOUS MONITORING

Une nouvelle approche de la protection proactive de votre périmètre global

QUALYS®
CONTINUOUS SECURITY

TABLE DES MATIÈRES

Dans un monde idéal, votre entreprise devrait pouvoir disposer d'une vue permanente de votre périmètre réseau global. Il s'agit d'un besoin vital pour contrer les auteurs de menaces susceptibles de lancer des attaques sophistiquées à tout moment depuis n'importe quel point du globe. Vos contrôles de sécurité réseau doivent être en mesure d'identifier et de repousser toute attaque, de prévenir les interruptions d'activité et aussi de protéger la confidentialité, l'intégrité et la disponibilité des données et des applications critiques, le tout automatiquement. Atteindre cet idéal est le Graal de la sécurité et la supervision continue est un processus crucial pour y parvenir.

Le présent guide décrit la nécessité de la supervision continue et propose un modèle pour créer une pratique de sécurité continue. Cette supervision permanente fournira à votre entreprise la vue la plus complète de son périmètre global. Elle vous permettra aussi d'identifier et de lutter de manière proactive contre les menaces qui peuvent être induites par des vulnérabilités logicielles ou des configurations système peu fiables.

LA NÉCESSITÉ DE LA SUPERVISION CONTINUE

Des processus métier souples tels que l'informatique dans le Cloud et la virtualisation ont transformé la nature jadis statique du périmètre du réseau de l'entreprise. Ce périmètre est aujourd'hui distribué, complexe et très dynamique tandis que des équipes opérationnelles indépendantes administrent et modifient les configurations des firewalls, routeurs, commutateurs, équilibreurs de charge, serveurs, applications et autres systèmes. L'analyse périmétrique et la réponse aux failles de sécurité involontaires liées à ces changements sont souvent lancées suite à un événement. Elles ne sont exécutées que de manière programmée, généralement une fois par semaine ou par mois. Ce qui laisse aux cybercriminels toute latitude pour exploiter les nouvelles vulnérabilités introduites et infiltrer les réseaux entre deux scans. Par ailleurs, de nouvelles vulnérabilités logicielles sont découvertes chaque jour sur des équipements et des applications, ce qui représente une source supplémentaire de menaces susceptibles d'exploiter des configurations qui évoluent sans cesse.

C'est ainsi qu'une étude de l'université du Michigan intitulée « How Vulnerable are Unprotected Machines on the Internet? » (« À quel point les machines non protégées sont-elles vulnérables sur Internet ? ») montre que les serveurs ayant des ports ouverts et autres vulnérabilités sont analysés sous 23 minutes environ après connexion à Internet et que des sondes destinées à localiser les vulnérabilités sont envoyées dès la 56ème minute. Le temps moyen avant le premier exploit est inférieur à 19 heures. Pour prévenir les exploits rapidement et de manière proactive, les entreprises ont besoin d'une nouvelle stratégie de défense opérationnelle : la supervision continue avec Continuous Monitoring
La supervision continue est un terme qui dit bien ce qu'il veut dire, à savoir que le processus de surveillance ne doit jamais s'interrompre afin que les actifs stratégiques hautement prioritaires fassent l'objet de l'attention immédiate du service d'intervention de l'équipe opérationnelle pour contrer les exploits de sécurité. Une analyse régulière à l'aide de Qualys Vulnerability Management, le service Web primé de gestion des vulnérabilités, est fondamentale. Mais une nouvelle approche automatisée peut relever d'un cran le niveau de vigilance de votre entreprise : Qualys Continuous Monitoring (CM), la solution de supervision continue de Qualys.

QUELLE FRÉQUENCE D'ANALYSE ?

Qualys vous recommande d'analyser l'ensemble de votre réseau au moins une fois par jour.

Les données d'inventaire, de configuration et de vulnérabilités des actifs collectées par Qualys Vulnerability Management sont le carburant du service Qualys Continuous Monitoring. Sans données fraîches, la supervision n'est pas « continue » et votre réseau est en danger.

Les actifs stratégiques à forte valeur doivent être analysés plusieurs fois par jour ou, mieux encore, en permanence grâce à la fonction d'« analyse continue » de Qualys Vulnerability Management.

Cliquez ici pour savoir comment configurer l'« analyse continue » :
https://community.qualys.com/docs/DOC-3852

CM ET VULNERABILITY MANAGEMENT

La solution Qualys Continuous Monitoring fournit un aperçu complet et permanent des failles de sécurité potentielles. Ainsi, les entreprises peuvent immédiatement identifier et contrer de manière proactive les vulnérabilités potentielles avant que ces dernières ne se transforment en failles. Construite sur l'offre Qualys Cloud Platform, Qualys Continuous Monitoring utilise sa capacité d'analyse élastique pour s'adapter aux réseaux de toute taille et importance de manière dynamique. L'avantage premier est de pouvoir alerter immédiatement le service d'intervention de l'équipe opérationnelle dès qu'un changement non autorisé est détecté.

Il existe un étroit rapport symbiotique entre Qualys Continuous Monitoring et Qualys Vulnerability Management. Les vulnérabilités peuvent prendre la forme de menaces logicielles telles que des vers, des virus et autres. Elles peuvent aussi provenir de problèmes liés à la configuration de votre environnement informatique. La fusion des deux scénarios est une combinaison toxique de menaces qui exige une supervision et une remédiation continues. L'idée même de supervision continue repose sur la disponibilité de données ponctuelles et précises concernant votre environnement informatique, y compris sur les changements apportés aux systèmes et aux configurations qui facilitent de nouvelles vulnérabilités. Ces données sont automatiquement recueillies et analysées lors des scans. La supervision continue intervient immédiatement après communication de ces informations au service d'intervention pour appréciation et action.

Transformation de l'ancien modèle. Qualys CM transforme l'ancien processus reposant sur l'analyse et le reporting en analysant les résultats du scan d'après vos critères. De plus, ce service alerte automatiquement le service d'intervention concerné en lui fournissant des informations spécifiques et personnalisées pour chaque actif dont il est responsable. Auparavant, un gros rapport souvent nébuleux devait circuler entre les mains de toute une bureaucratie de responsables, de superviseurs et de techniciens. Résultat : la remédiation était souvent largement à la traîne derrière des menaces qui apparaissaient presque spontanément.

Qualys CM envoie rapidement des salves d'informations essentielles de type Twitter aux personnes directement concernées qui prendront alors des mesures ciblées immédiatement. Grâce à ce service Web, le service d'intervention a toujours une longueur d'avance sur les menaces à l'encontre des actifs les plus importants. Qualys CM vous permet de contrôler de manière granulaire les intervalles et les cibles qui font l'objet d'une notification, un point qui sera abordé en détails plus loin dans ce guide.

Des scans fréquents garantissent une supervision continue performante. C'est la fréquence d'analyse des vulnérabilités qui fait l'efficacité des alertes de Qualys CM. Aussi, si vous ne lancez un

scan qu'une fois par trimestre voire une fois par mois, « superviser en continu » les données issues de ces analyses ne présente qu'un intérêt limité car les vulnérabilités évoluent de minute en minute sur une surface d'attaque à la fois gigantesque et fluide. En raison de l'évolution permanente des menaces, Qualys vous invite à analyser votre réseau au moins une fois par jour et plus souvent encore pour les actifs critiques et prioritaires (voir la barre latérale en page 3). De cette manière, les données d'analyse des vulnérabilités seront vraiment actualisées et permettront à Qualys CM d'être un composant utile, et essentiel, à la protection de votre réseau contre les exploits.

CONTRÔLES DE SÉCURITÉ CRITIQUES ET RECOMMANDATIONS POUR CM

Il n'y a pas que Qualys qui préconise des scans fréquents et une supervision continue. En effet, depuis des années, l'institut américain des normes et technologies (National Institute of Standards and Technology - NIST) conseille aux agences fédérales de recourir à la supervision continue comme processus majeur pour gérer les risques. La publication spéciale 800-137 du NIST intitulée *Information Security Continuous Monitoring (ISCM)* for Federal Information Systems and Organizations (Supervision continue de la sécurité de l'information pour les systèmes d'information fédéraux et les entreprises) indique des procédures associées pour se conformer à la Loi fédérale sur la gestion de la sécurité des informations (FISMA). L'instauration de fréquences de supervision et d'évaluation figure parmi les « fonctions critiques » (p. 25) tandis que l'augmentation des fréquences est recommandée pour les systèmes critiques (pp. 25-27). Ces recommandations ont été difficiles à mettre en œuvre jusqu'à ce que Qualys CM soit disponible.

D'autres recommandations formulées par les contrôles de sécurité critiques (CSC), autrefois appelés les « 20 contrôles de sécurité du SANS Institute », proposent en une approche de la cybersécurité hiérarchisée et basée sur les risques. Elles sont le fruit d'un processus consensuel auquel a participé un large panel de professionnels de la cybersécurité travaillant pour les autorités et le marché et qui ont été interrogés sur ce qui donne des résultats dans la pratique et ce par quoi ils commencent. Désormais gérés par le Conseil sur la cybersécurité, dont Qualys est membre fondateur et participant actif pour le développement des contrôles de sécurité critiques, les CSC sont devenus une référence. En effet, ces contrôles accompagnent les directeurs de la sécurité de l'information (DSSI) et les directeurs du système d'information (DSI) dans le déploiement des processus les plus efficaces et des outils nécessaires pour sécuriser l'ensemble de leur informatique selon la nature des risques.

For example, the CSCs advise that any unauthorized machine connected to the Internet be identified within 24 hours, and patching vulnerabilities in critical operating systems and applications should occur within 48 hours.

Les CSC recommandent notamment l'identification sous 24 heures de toute machine non autorisée qui serait connectée à Internet et que soient également déployés sous 48 heures des correctifs pour les vulnérabilités affectant les systèmes d'exploitation et les applications critiques.

RECOMMANDATIONS FORMULÉES PAR LES CONTRÔLES DE SÉCURITÉ CRITIQUES :

Scans – Lancement de scans automatiques une fois par semaine ou plus souvent encore afin de détecter les vulnérabilités.

Alertes – L'efficacité de ces dernières doit être mesurée en quelques minutes seulement.

Découverte – Identification des serveurs non autorisés sous 24 heures.

Correctifs – Déploiement de ces derniers sur les systèmes critiques dans les 48 heures.

Source : Contrôles de sécurité critiques gérés par le Conseil sur la Cybersécurité

Le CSC 4 concerne l'évaluation et la remédiation continues des vulnérabilités. Ce contrôle invite à lancer des scans automatiques des vulnérabilités une fois par semaine ou plus souvent. Il recommande aux entreprises de mesurer l'efficacité des alertes déclenchées « en quelques minutes » sachant que le facteur temps est crucial pour la supervision continue.

Positionnement de Qualys Continuous Monitoring par rapport à cette exigence

- Qualys Vulnerability Management est programmée pour détecter périodiquement les vulnérabilités sur l'ensemble des systèmes connectés au réseau.
- Qualys propose également des scans à la demande pour des contrôles ad-hoc ou pour rechercher des vulnérabilités spécifiques telles que « les ports interdits », comme recommandé par le contrôle CSC 4.
- La solution offre aussi une fonction d'analyse continue des systèmes et des sous-réseaux critiques.
- Qualys rapporte les vulnérabilités détectées dans des vues centrées sur les patchs et au moyen d'informations « de substitution » afin de rendre l'analyse et la remédiation plus performantes.
- Les rapports intègrent les normes CVE et CVSS pour garantir une analyse souple des résultats.
- Le suivi de la remédiation via un système de tickets interne assure visibilité et contrôle tout en garantissant la sécurité des systèmes et des réseaux critiques.
- Qualys CM envoie une notification immédiate à propos des vulnérabilités détectées et propose des voies de remédiation au service d'intervention.

Pour plus d'informations sur les contrôles CSC : http://www.CouncilOnCybersecurity.org/critical-controls.

COMMENT UTILISER EFFICACEMENT QUALYS CM

Qualys Continuous Monitoring est un service SaaS vendu séparément et qui s'utilise avec Qualys Vulnerability Management. Qualys CM offre de puissantes options de configuration pour répondre aux besoins spécifiques des grandes entreprises. La stratégie de configuration s'articule autour de trois axes pour une utilisation efficace de Qualys CM : Où, Quoi et Qui.

Où : où s'applique Qualys CM ? Votre entreprise doit hiérarchiser ses actifs par priorité lorsque Qualys CM signale à votre équipe qu'un incident nécessite une remédiation. A priori, vous devez déjà utiliser la hiérarchisation des actifs à l'aide de Qualys Vulnerability Management pour attribuer des valeurs pondérées et personnalisées qui indiquent la valeur métier des actifs critiques. Ces informations peuvent être exploitées par Qualys CM et gérées à l'aide de profils de supervision. Un profil peut être appliqué à un serveur unique ou à un groupe de serveurs au moyen de tags d'actifs ou de la saisie manuelle de plages d'adresses IP. Les profils garantissent le traitement des actifs hautement prioritaires par le service d'intervention.

Quoi : que recherche Qualys CM sur votre réseau ? Le service d'intervention de votre équipe opérationnelle s'appuie sur la capacité de Qualys CM à détecter avec précision les problèmes présentant un intérêt particulier pour la sécurité de votre réseau. Ils s'appuient sur des ensembles de règles facilement configurables pour les classes de vulnérabilités courantes, y compris pour des besoins spécifiques. Un ensemble de règles peut être créé ex nihilo ou reprendre des critères existants sélectionnés par des tags d'actifs. Il s'agit généralement des éléments suivants :

- **Serveur** – Qualys CM détecte le moment précis où les systèmes apparaissent, disparaissent ou exécutent des systèmes d'exploitation inattendus. Le destinataire d'une alerte peut rapidement examiner en profondeur toutes les données associées qui ont été collectées par Qualys Vulnerability Management. Il s'agit notamment du résumé du nom, de l'adresse IP, du nom du serveur DNS, du nom NetBIOS, du système d'exploitation, des ports ouverts, des logiciels installés, des vulnérabilités affectant le serveur et de l'historique des notifications d'alerte fournissant du contexte pour savoir si le serveur a été régulièrement touché par des vulnérabilités.
- **Changements apportés à l'OS sur les serveurs existants** – Qualys CM signale les changements apportés aux systèmes d'exploitation sur les serveurs existants.
- **Vulnérabilité** – Lorsque la vulnérabilité reste ouverte, Qualys CM l'identifie comme « active » et demande sa remédiation. Les vulnérabilités nouvelles, rouvertes et fermées sont également marquées.
- **Certificat SSL** – Qualys CM identifie les certificats qui ont expiré, qui arrivent à expiration, pirates ou inconnus, tous pouvant potentiellement entraîner l'interruption de services et d'applications de votre réseau.

- **Port ou service** – Ports récemment ouverts, modifications apportées aux ports, nouveaux services sur les ports et fermeture de ports sont des vecteurs courants d'attaques et d'exploits. Qualys CM consigne tous ces événements et vous alerte en conséquence.
- **Logiciels** – L'installation d'un logiciel nouveau ou non autorisé, le passage à une version ultérieure ou antérieure de logiciels existants ainsi que les suppressions de programmes peuvent aussi affaiblir la surface d'attaque du périmètre et sont gérés par Qualys CM.

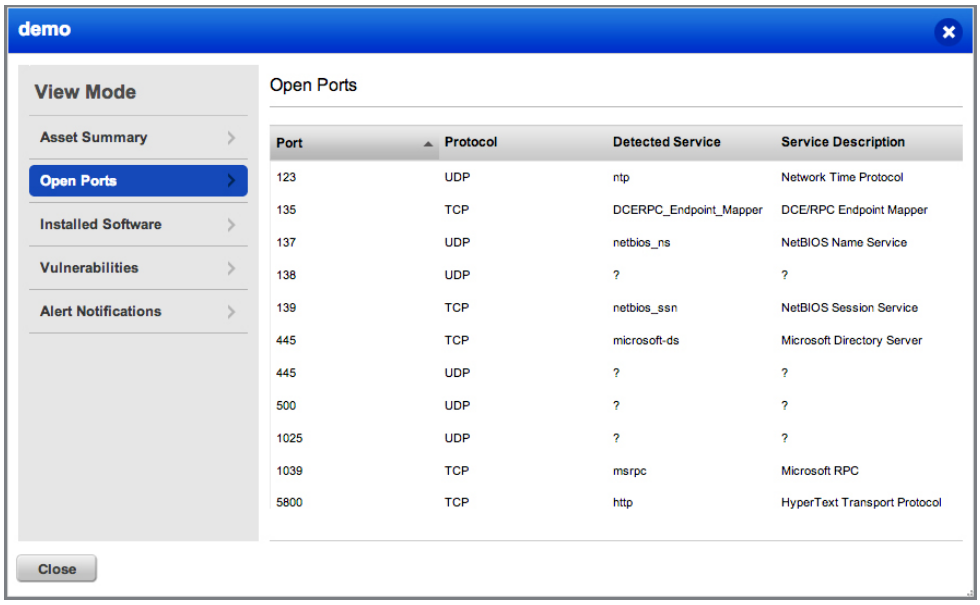

Figure 1 : Qualys Continuous Monitoring signale tous les ports ouverts, les protocoles et les services associés sur chaque serveur.

BOMBE À RETARDEMENT

Le flux continu de nouvelles vulnérabilités et les changements constants au sein de votre environnement informatique font que la mèche sera toujours courte et qu'elle ne laissera que peu de temps pour réparer les actifs hautement prioritaires.

Pour les serveurs connectés à Internet avec des ports ouverts et des services actifs :

Temps moyen avant le 1er scan	Temps moyen avant la 1ère analyse des vulnérabilités	Temps moyen avant le 1er exploit
23 minutes	**56** minutes	**19** heures

Source: "How Vulnerable are Unprotected Machines on the Internet?" (« À quel point les machines non protégées sont-elles vulnérables sur Internet ? ») (Étude réalisée par l'Université du Michigan, 2014)

« À une époque où les compromis se succèdent en permanence, les **entreprises doivent passer** d'une stratégie de « réponse à un incident », qui considère les incidents comme occasionnels et non répétitifs, **à une approche basée sur une réponse continue** à des attaques incessantes, la capacité des pirates à pénétrer les systèmes et l'information ne pouvant jamais être complètement bloquée tandis que les systèmes doivent être considérés comme compromis en permanence et donc **continuellement surveillés** »

déclare **Neil MacDonald,** déclare Neil MacDonald, vice-président et analyste distingué chez Gartner.

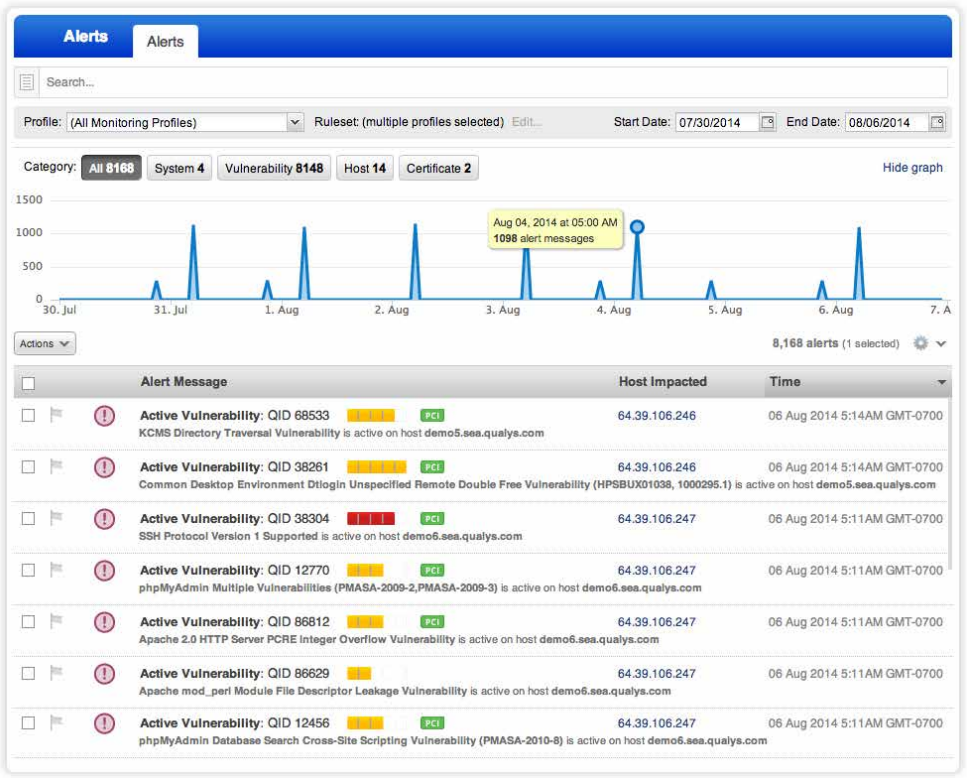

Figure 2 : Grâce aux alertes envoyées par Qualys Continuous Monitoring, le service d'intervention peut immédiatement analyser les détails tels que les nouveaux ports ouverts, les ports fermés ou les modifications sur les ports.

Qui : qui est averti par CM et à quelle fréquence ? Un moteur de politiques intégré à Qualys CM veille à ce que les notifications soient bien envoyées au service d'intervention spécifique chargé de remédier les actifs prioritaires affectés.

En plus de spécifier qui doit recevoir des alertes spécifiques, Qualys CM propose huit intervalles standard pour notifier les événements. Les deux premiers, « toutes les 5 minutes » et « toutes les 20 minutes » sont réservés aux événements les plus critiques et doivent être utilisés pour une véritable « supervision continue ». Par exemple, si un membre du service d'intervention est désigné pour recevoir des alertes toutes les cinq minutes, cette personne recevra toutes les alertes libellées comme prioritaires qui ont été déclenchées au cours des cinq dernières minutes. Regrouper la transmission d'alertes dans des intervalles de 5 ou 20 minutes permet de réduire le spam par email ou radiomessagerie tout en garantissant une notification ponctuelle.

Des intervalles plus longs, par exemple toutes les 12 heures, une fois par jour ou une fois par semaine sont appropriés pour les événements à faible priorité et peuvent être utilisés pour les personnes chargées de traiter ces tâches.

Des alertes peuvent également être envoyées aux personnes qui ne sont pas autorisées à utiliser des services Qualys. Ainsi, un analyste du centre de sécurité peut ne pas être directement impliqué dans la remédiation, mais être informé des vulnérabilités urgentes susceptibles d'affecter le réseau.

Intégration de la gestion SIEM aux systèmes d'entreprise. Une nouvelle API extensible intègre les alertes Qualys CM aux systèmes d'entreprise de réponse aux incidents grâce à des intégrations à des plates-formes phares de gestion des informations et des événements de sécurité (SIEM), parmi lesquelles Splunk et HP ArcSight. Qualys CM utilise le format CEF (Common Event Format) pour envoyer des événements à toutes les principales solutions de gestion SIEM et de réponse aux incidents, y compris des alertes email qui sont directement envoyées dans la boîte de réception du service d'intervention.

EXEMPLES DE RÉSULTATS OBTENUS GRÂCE À QUALYS CM

Les alertes envoyées par Qualys CM au service d'intervention indiquent les changements opérés sur la surface d'attaque d'une entreprise et qui sont susceptibles de créer un compromis de sécurité des actifs. Quelques exemples d'événements importants typiques :

- **Découverte d'une nouvelle vulnérabilité** – Des alertes sont envoyées selon le niveau de gravité de la vulnérabilité et le serveur affecté. Vous pouvez également spécifier des alertes pour des vulnérabilités particulières. Par exemple, même si des correctifs ont été publiés pour le tristement célèbre bogue Heartbleed, cette vulnérabilité continue d'apparaître en raison du déploiement de serveurs infectés par de mauvaises images utilisées pour la configuration. Spécifier une règle qui recherche « QID 42220 » permettra d'identifier immédiatement la présence de cette vulnérabilité et Qualys CM informera le service d'intervention en conséquence.
- **Nouveau serveur** – L'apparition d'un nouveau serveur sur votre réseau est un événement important. Vous pouvez par exemple spécifier une règle autorisant les serveurs de la DMZ à exécuter uniquement Linux et à n'avoir que les ports 80 et 443 ouverts ainsi que le port 22 pour l'administration à distance. Qualys CM détectera immédiatement les serveurs qui dérogent à cette règle et informera le service d'intervention en conséquence.
- **Nouveau port ouvert** – Un serveur peut avoir été solidement configuré, mais si un port est délibérément ou accidentellement ouvert, cet événement exposera la machine à des attaques. Qualys CM détecte cet événement et alerte le service d'intervention en conséquence. Les règles spécifiées via Qualys CM peuvent surveiller des critères granulaires associés aux ports, notamment les serveurs qui n'exécutent pas Windows avec le port 80 ouvert.

POUR EN SAVOIR PLUS

Solution faisant partie de Qualys Cloud Platform, Qualys Continuous Monitoring est vendue sous la forme d'un abonnement annuel avec Qualys Vulnerability Management. Pour en savoir plus et tester une version d'évaluation gratuite pendant 7 jours, rendez-vous sur https://qualys.com/cm-trial

- **Nouveau logiciel installé** – Qualys CM peut envoyer une alerte si un nouveau logiciel vient d'être installé sur un serveur (mise à niveau montante ou descendante), ou si ce dernier exécute une version du logiciel désuète et/ou non corrigée. Cette fonctionnalité est activée en configurant Qualys Vulnerability Management pour que ce service lance une analyse authentifiée et déclare le scanner auprès du serveur comme un utilisateur autorisé de la machine.
- **Changements au niveau d'un certificat SSL** – Ces alertes sont généralement associées à de nombreux serveurs. Des certificats nouveaux, même s'ils sont valides et non expirés, peuvent figurer parmi les critères d'alerte granulaires. Cet événement est important parce qu'il détecte lorsqu'une personne peut avoir obtenu un certificat valide, mais pas celui qui devrait être utilisé pour un serveur spécifique. Par exemple, si votre entreprise achète uniquement des certificats Verisign, une règle le spécifiera et détectera automatiquement un certificat non valide acheté ailleurs, par exemple chez GoDaddy.

Il est possible de réutiliser aussi souvent que vous le souhaitez des ensembles de règles, notamment ceux régissant les résultats décrits ci-dessus, ce qui simplifie la gestion et l'utilisation de Qualys CM.

Enfin, la nouvelle fonctionnalité de recherche guidée (Guided Search Box) tout-en-un de Qualys CM permet de localiser et d'analyser rapidement des informations détaillées sur un événement.

La supervision continue n'est pas seulement un produit ou une solution. Il s'agit aussi d'une approche critique pour protéger en permanence le périmètre de votre réseau. Qualys Continuous Monitoring offre une vue complète et permanente de votre périmètre avec des alertes intégrées qui vous permettent d'agir rapidement contre les menaces potentielles lors de changements dans votre environnement réseau.

À PROPOS DE QUALYS

Qualys Inc. (NASDAQ : QLYS), est le principal fournisseur de solutions de sécurité et de conformité dans le Cloud avec plus de 6 700 clients dans plus de 100 pays, dont une majorité des sociétés présentes aux classements Fortune 100 et Forbes Global 100. Qualys Cloud Platform et sa suite de solutions intégrée aident les entreprises à simplifier leurs opérations de sécurité et à réduire le coût de la conformité. Cette plate-forme délivre un service à la demande de renseignement sur la sécurité. Elle automatise le spectre complet de l'audit, de la conformité et de la protection des systèmes d'information et des applications Web Fondée en 1999, Qualys a signé des accords stratégiques avec des fournisseurs de services d'infogérance (« managed services ») et des cabinets de conseil de premier ordre tels qu'Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon et Wipro Qualys est également l'un des fondateurs de la Cloud Security Alliance et du Conseil sur la cybersécurité. Pour plus d'informations, consultez **www.qualys.com.**

QUALYS®
CONTINUOUS SECURITY

Qualys, Inc. – Siège social
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T 1 (800) 745.4355

Qualys est une société d'envergure mondiale avec des représentations dans le monde entier.
Pour connaître le bureau le plus proche de chez vous, rendez-vous sur **http://www.qualys.com**