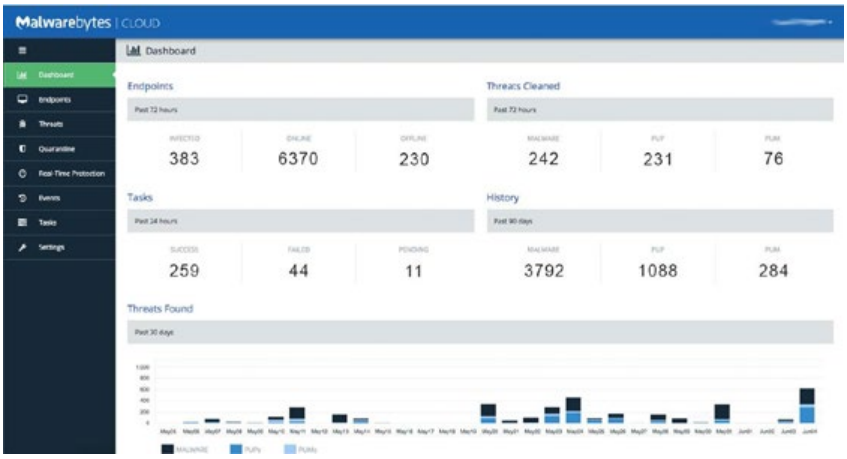
FICHE TECHNIQUE

Malwarebytes Incident Response

Détection des menaces et remédiation centralisées

Les cybercriminels adoptent des approches de plus en plus sophistiquées pour cibler leurs victimes et obtenir les informations nécessaires à l'exécution de leurs attaques. Malgré les milliards dépensés par les entreprises, les établissements d'enseignement et les organismes publics pour améliorer leurs solutions de sécurité, les menaces sont toujours capables de pénétrer les défenses des réseaux et terminaux. Les processus de réponse à ces incidents[1] sont longs et fastidieux, 6 à 8 heures étant généralement nécessaires rien que pour réparer ou réimager un seul terminal. D'après une étude du Ponemon Institute, l'identification d'une attaque malveillante ou criminelle prend environ 229 jours et sa suppression 82 jours[2]. Les entreprises doivent fournir les meilleures sources de télémétrie et les meilleures méthodes de remédiation à leurs services de sécurité.

Malwarebytes Incident Response est un outil de détection des menaces et de remédiation qui s'appuie sur une plateforme de gestion hautement évolutive hébergée dans le cloud. Il analyse le réseau de terminaux à la recherche de menaces avancées telles que les malwares, les PUP et les adwares, et les élimine complètement. Malwarebytes Incident Response optimise votre capacité de détection des menaces ainsi que le délai nécessaire pour répondre à une attaque tout en vous offrant les avantages d'une solution évolutive, flexible et automatisée.



Console cloud Malwarebytes – Tableau de bord

Références

[1]De manière générale, la réponse aux incidents (incident response) fait référence aux outils, processus et ressources mis en oeuvre par les organisations pour faire face à une cyberattaque identifiée et réduire les risques associés à celle-ci.

[2]Source : Ponemon Institute, étude de 2016 sur le coût d'une violation de données, juin 2016.

CARACTÉRISTIQUES TECHNIQUES

INCIDENT RESPONSE

Moteur Incident Response
Trois modes d'analyse (à la demande, planifiée, automatique) rapides et extrêmement efficaces.

Plusieurs modes d'analyse
Les modes d'analyse rapide, de recherche de menaces et personnalisée ne dérangent pas les utilisateurs finaux.

Moteur Linking Engine
Technologie indépendante des signatures qui identifie et élimine complètement les artefacts associés à la charge utile de la menace primaire.

Plateforme cloud Malwarebytes
La console dans le cloud permet un contrôle facile et centralisé de la gestion des règles de sécurité, des déploiements et de l'identification des menaces.

Gestion des actifs
Fournit des informations pertinentes sur les systèmes des terminaux, dont : objets de mémoire, logiciels installés, programmes lancés au démarrage, etc

Forensic Timeliner
Collecte les événements des journaux Windows et les présente sous la forme d'une unique frise chronologique.

Avantages clés

Automatisation

Vous pouvez prédéployer Malwarebytes Incident Response sur vos terminaux pour bénéficier de ses capacités avancées de détection et de remédiation en un seul clic. Le programme s'intègre également à vos outils actuels SIEM, de gestion des terminaux et de détection des menaces afin d'automatiser la réponse en cas d'alerte incident. L'automatisation accélère les processus de réponse aux incidents des entreprises tout en réduisant le temps de présence des menaces.

Flexibilité

Malwarebytes Incident Response inclut un logiciel agent permanent unifié ainsi que des agents temporaires (Breach Remediation) pour offrir une plus grande flexibilité de déploiement en fonction de l'infrastructure informatique de votre entreprise. Malwarebytes s'intègre facilement à votre solution de sécurité actuelle, et est compatible avec votre système d'exploitation (Windows et Mac OS X) et votre infrastructure.

Évolutivité

Malwarebytes Incident Response est déployé depuis notre nouvelle plateforme cloud Malwarebytes de gestion des terminaux. La plateforme cloud Malwarebytes simplifie le déploiement et la prise en main de Malwarebytes Incident Response ainsi que des autres solutions Malwarebytes, que vous ayez un seul terminal ou des millions. Cette console centralisée sur le cloud vous évite d'avoir à faire l'acquisition d'une solution matérielle sur site qu'il faudra ensuite maintenir.

CONFIGURATION REQUISE

Composants inclus

Plateforme cloud Malwarebytes
Malwarebytes Incident Response (agents permanents Windows et Mac OS X)
Breach Remediation (agents temporaires Windows CLI, Mac GUI, Mac CLI)
Forensic Timeliner (Windows)
Assistance téléphonique et par e-mail

Configuration matérielle requise

MS Windows
Processeur : 1 GHz
RAM : 1 Go (clients) ; 2 Go (serveurs)
Espace disque : 100 Mo (programme + journaux)
Connexion Internet active

Mac
Tout dispositif Apple Mac prenant en charge Mac OS X (version 10.10 ou ultérieure)
Connexion Internet active

Systèmes d'exploitation pris en charge

Windows 10® (32 bits, 64 bits)
Windows 8.1® (32 bits, 64 bits)
Windows 8® (32 bits, 64 bits)
Windows 7® (32 bits, 64 bits)
Windows Vista® (32 bits, 64 bits)
Windows XP® SP3 (32 bits uniquement)
Windows Server 2016® (32 bits, 64 bits)
Windows Server 2012/2012R2® (32 bits, 64 bits)
Windows Small Business Server 2011
Windows Server 2008/2008R2® (32 bits, 64 bits)
Windows Server 2003® (32 bits uniquement)
Mac OS X (version 10.10 ou ultérieure)

Remarque : les systèmes d'exploitation Windows Server utilisant l'option d'installation Server Core ne sont pas pris en charge.

L'intégration au Centre de notifications Windows n'est pas prise en charge sur les systèmes d'exploitation Microsoft Windows Server.

www.g-sys.lu
+352 26 17 53 96

G-Sys : Partenaire du développement de votre activité

Fondée en 1997 par des passionnés de la programmation informatique, la Société G-Sys est éditeur de logiciels et intégrateur de services informatiques.
G-Sys est à l'origine éditeur d'un logiciel de gestion commerciale. Elle a étendu ses compétences et ses expertises métiers au fil des années en proposant aujourd'hui, une offre globale et unique.

Active et reconnue sur le marché des PME au Luxembourg et dans la Grande-Région (Belgique, France et Allemagne), G-Sys aborde l'ensemble des projets avec une vision à long terme, tant en terme d'investissement qu'en terme de stratégie. La clé d'un partenariat durable passe par cette approche saine et rassurante.

malwarebytes.com/business
1.800.520.2796

Malwarebytes est l'entreprise de cybersécurité nouvelle génération à qui des millions de personnes font confiance dans le monde entier. Malwarebytes protège de manière proactive les particuliers et les entreprises contre les menaces dangereuses telles que les malwares, les ransomwares et les exploits qui échappent à la vigilance des solutions antivirus traditionnelles. Le produit phare de l'entreprise combine des fonctionnalités avancées de détection heuristique des menaces avec des technologies indépendantes des signatures afin de détecter et d'arrêter les cyberattaques avant qu'elles ne causent des dégâts. Plus de 10 000 entreprises dans le monde entier font confiance à Malwarebytes et recommandent ses solutions.