Malwarebytes Incident Response

Le programme de remédiation le plus complet et le plus fiable

AVANTAGES CLÉS

- Remédiation des menaces automatisée, précise et complète
- Communication entre les cloisonnements opérationnels
- Réduction du temps de présence des malwares
- Compensation des pénuries de personnel et de compétences
- Réduction des coûts et simplification de la gestion des réponses aux incidents

RÉCOMPENSES

Entreprise la plus prometteuse des États-Unis

Produit de l'année

Innovation de sécurité de l'année

Votre centre de réaction aux attaques informatiques (CIRT, cyber incident response team) doit faire face à des incidents de sécurité de plus en plus fréquents et toujours plus variés avec les coûts et la complexité que cela implique en termes de remédiation.

En effet, plus de 60 % des attaques nécessitent au moins neuf heures de travail de la part des organisations victimes avant d'être éliminées.[1] Plus que jamais, il est temps que celles-ci abandonnent leur démarche réactive au profit de processus de réponse aux incidents automatisés qui exploitent au mieux des ressources limitées contre les attaques ininterrompues des menaces avancées.

Malwarebytes Incident Response est votre solution pour une suppression complète et précise des menaces, garantissant un processus de réponse aux incidents plus efficient et efficace. Notre approche automatisée vous permet de renforcer votre modèle de sécurité et d'assurer la communication entre les cloisonnements opérationnels.

Caractéristiques clés

Remédiation automatisée

Grâce à notre technologie de remédiation automatisée, vos équipes de cybersécurité n'ont plus besoin de mettre manuellement en œuvre des solutions ad hoc pour éliminer les malwares et restaurer les machines après une infection. Elles y gagnent des ressources et un temps précieux. Les tâches automatisées par notre programme sont effectuées plus rapidement et plus précisément. Résultat : les malwares restent moins longtemps sur vos machines.

Remédiation complète

La plupart des solutions offrent des capacités de remédiation partielles qui n'éliminent que les composants actifs des malwares. Le moteur de liaison Malwarebytes Linking Engine met en œuvre une approche propriétaire qui détecte et élimine aussi les artefacts dynamiques et autres artefacts associés aux malwares. Notre moteur applique des techniques de séquencement associé afin de garantir l'élimination permanente des mécanismes de persistance des malwares. Notre méthodologie de remédiation avancée assure aux organisations l'identification rapide des malwares et leur suppression complète.

La meilleure télémétrie

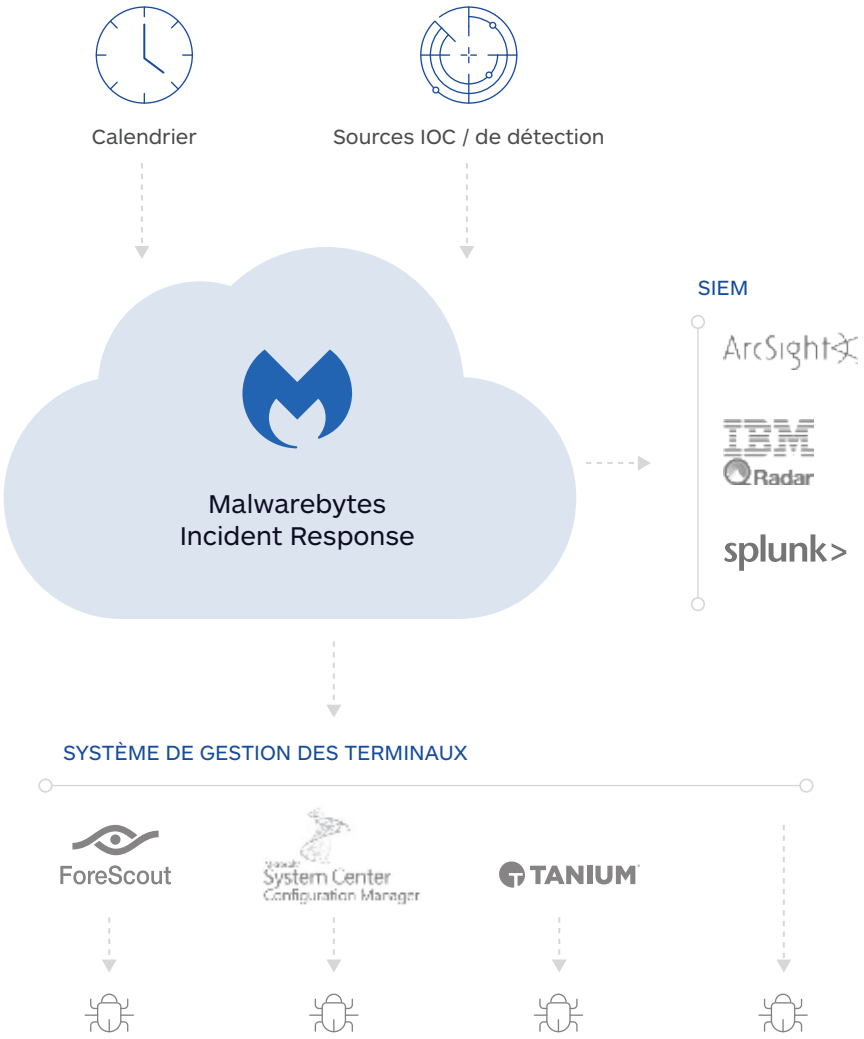
Nos équipes de cyber-veille sont expertes en matière de remédiation et sont au fait des « pires scénarii », c'est-à-dire les attaques qui parviennent à s'exécuter sur les terminaux d'entreprises. Nos systèmes d'analyse de données massives et les recherches de nos experts nous permettent de réparer plus de 3 millions de terminaux chaque jour. Nous exploitons ces ressources télémétriques précieuses sur les malwares zero day afin d'optimiser la réactivité de nos technologies face aux nouvelles menaces et de mieux anticiper les malwares de demain.

Traque proactive

Des menaces sont certainement déjà présentes dans votre environnement. Une fois un terminal infecté, les attaquants en profitent souvent pour propager l'infection latéralement aux autres terminaux. Malwarebytes permet à vos équipes de cybersécurité de planifier l'exécution des analyses pour procéder à une traque proactive des indicateurs de compromis (IOC) les plus récents. Notre solution vous encourage à toujours envisager le pire et à renforcer significativement votre stratégie de sécurité en conséquence.

Déploiement flexible et intégration simple

Le déploiement de Malwarebytes est flexible et s'adapte à vos besoins : vous avez le choix entre un agent permanent installé sur les terminaux et géré depuis le cloud ou un agent temporaire déployé aux terminaux (Breach Remediation). De plus, l'agent temporaire simplifie l'intégration à vos systèmes SIEM et de gestion des terminaux existants. Notre solution implémente des actions immédiates dès que votre SIEM détecte des IOC sur le réseau. Par exemple, Malwarebytes peut engager un processus de réaction à un incident sur la base des alertes émises par vos solutions Splunk ou ForeScout.



Ressources en ligne

Pour en savoir plus à propos de Malwarebytes Incident Response, rendez-vous sur :
malwarebytes.com/business/incidentresponse/
Actualités : blog.malwarebytes.com/
Demander un essai : malwarebytes.com/business/licensing

Références

[1] *Understanding the Depth of the Global Ransomware Problem*, Osterman Research

Santa Clara, Californie | malwarebytes.com | corporate-sales@malwarebytes.com | 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. Fondée en 2008 et basée en Californie, la société possède des bureaux en Europe et en Asie et emploie une équipe internationale de chercheurs spécialisés dans les menaces et d'experts de la sécurité.