

Gestion des vulnérabilités moderne

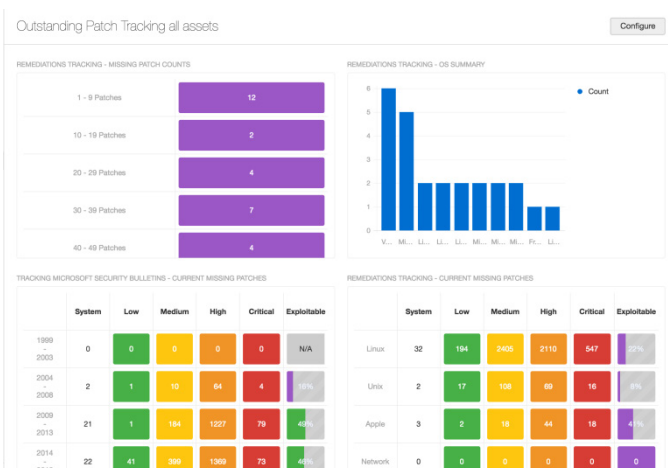
Le paysage informatique d'aujourd'hui évolue, et pour cette raison, la gestion des vulnérabilités doit également évoluer. Les environnements informatiques d'aujourd'hui sont caractérisés par des actifs à la fois traditionnels et dynamiques. Pour remplacer ou compléter les serveurs physiques, les organisations adoptent des actifs virtuels ou basé sur le cloud, qui peuvent être déployés aussi rapidement que nécessaire. Ces actifs, de même que les appareils mobiles aujourd'hui omniprésents, entrent et sortent sur les réseaux en un instant. Les scans trimestriels, mensuels ou hebdomadaires traditionnels ne sont plus suffisants pour assurer la visibilité requise.

Les organisations ont besoin de solutions modernes qui offrent plusieurs façons d'identifier les vulnérabilités des actifs dynamiques d'aujourd'hui, qui peuvent proposer des recommandations claires sur la manière de hiérarchiser et d'adresser les vulnérabilités, et qui sont suffisamment souples pour répondre aux besoins variés des différentes organisations.

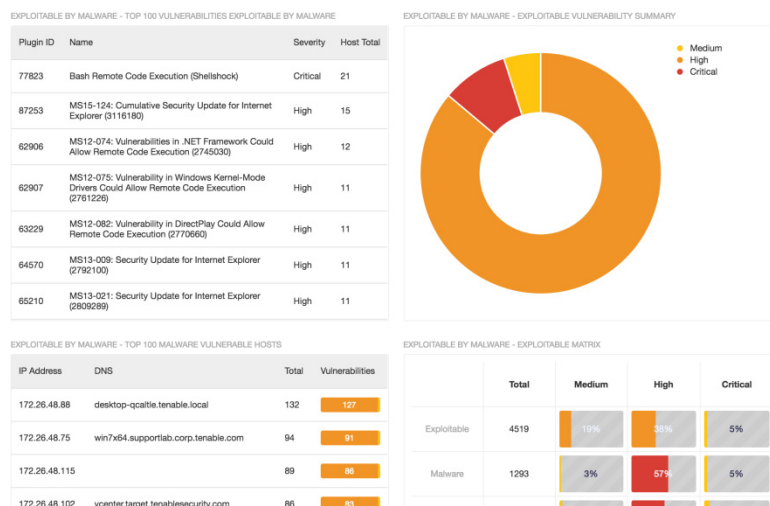
L'application de gestion des vulnérabilités Tenable.io™ propose une approche nouvelle et moderne afin de résoudre les plus grands défis actuels en termes de gestion des vulnérabilités. En utilisant un algorithme avancé d'identification des actifs, la gestion des vulnérabilités Tenable.io offre les informations les plus précises à propos des actifs dynamiques et des vulnérabilités, dans des environnements en constante évolution. Son interface simplifiée, ses modèles et guides intuitifs ainsi que son intégration harmonieuse aident les équipes sécurité à optimiser leur efficacité. Lorsque la visibilité et les informations sont primordiales, la gestion des vulnérabilités Tenable.io vous aide à vous concentrer sur la mesure appropriée, à chaque fois.

Principaux avantages

- **Un modèle flexible d'octroi de licences pour les actifs améliore le retour sur investissement** : la gestion des vulnérabilités Tenable.io offre un modèle d'octroi de licences inédit, basé sur les actifs, et qui ne requiert qu'une seule licence par actif, même si cet actif a plusieurs adresses IP
- **Des options d'audit plus complètes qui éliminent les zones d'ombre** : la gestion des vulnérabilités Tenable.io comprend des capteurs Nessus, un mélange de scanners actifs, d'agents et de capteurs d'audit passif pour optimiser la couverture du scan et réduire les zones d'ombre de vulnérabilité
- **Le suivi des vulnérabilités basé sur les actifs améliore la précision** : la gestion des vulnérabilités Tenable.io permet de suivre les actifs et leurs vulnérabilités avec une plus grande précision que toutes les solutions précédentes
- **Les intégrations prédéfinies tirent parti des solutions complémentaires** : la gestion des vulnérabilités Tenable.io est fournie avec des intégrations prédéfinies avec de nombreuses solutions complémentaires, de sorte que vous pouvez rapidement et facilement améliorer vos pratiques en matière de vulnérabilités et protéger votre entreprise



La gestion des vulnérabilités Tenable.io vous permet, à tout moment, d'identifier l'état des vulnérabilités dans votre environnement.



Avec plusieurs tableaux de bord et rapports prédéfinis, notamment ce tableau de bord « Exploitable par des malware », la gestion des vulnérabilités Tenable.io aide les équipes sécurité à prioriser efficacement la correction des vulnérabilités.

Capacités clés

Modèle flexible d'octroi de licences pour les actifs

La gestion des vulnérabilités Tenable.io offre un modèle d'octroi de licences inédit basé sur les actifs, qui ne requiert qu'une seule licence par actif, même si cet actif a plusieurs adresses IP. Le modèle flexible de la solution autorise également les scans lorsque le nombre de licences est temporairement dépassé, en récupérant automatiquement les licences des actifs rarement scannés ou sujet à des pics ponctuels.

Options d'audit complètes

La gestion des vulnérabilités Tenable.io tire parti des capteurs Nessus, un mélange de scanners actifs, d'agents et de capteurs d'audit passifs pour optimiser la couverture du scan et réduire les zones d'ombre de vulnérabilité. Ce mélange de capteurs de données permet d'inclure les actifs difficiles à scanner à votre programme de gestion des vulnérabilités, de sorte que les appareils transitoires analysés par les agents, ainsi que les systèmes sensibles tels que les appareils médicaux et les systèmes de contrôle industriels, peuvent être surveillés au moyen d'un audit passif du trafic.

Suivi précis des vulnérabilités basé sur les actifs

La gestion des vulnérabilités Tenable.io permet de suivre les actifs et leurs vulnérabilités avec une plus grande précision que toutes les solutions précédentes. Un algorithme avancé d'identification des actifs utilise un ensemble complet d'attributs (comme l'identifiant Tenable, le nom NetBIOS, l'adresse MAC et d'autres encore) pour assurer le suivi précis des changements d'actifs, quel que soit leur mode d'itinérance ou leur durée de vie.

Intégrations prédéfinies

La gestion des vulnérabilités Tenable.io est fournie avec des intégrations prédéfinies pour la gestion des correctifs populaires, la gestion des identifiants, la gestion des appareils mobiles et d'autres solutions complémentaires à la gestion des vulnérabilités, de sorte que vous pouvez rapidement et facilement améliorer vos pratiques en matière de vulnérabilités et protéger votre entreprise.

Interface utilisateur simplifiée

Grâce à son interface moderne et sa messagerie guidée dans l'application, la plateforme de gestion des vulnérabilités Tenable.io exécute des tâches courantes, comme les audits, dans la plus grande simplicité. Les modèles prédéfinis et les audits de configuration alignés sur les meilleures pratiques, comme CIS et DISA STIG, permettent de protéger votre organisation sans déployer autant d'efforts que d'habitude.

API documentée et SDK intégré

Automatisez facilement le partage des fonctions et des données de vulnérabilité de Tenable.io, ou développez la plateforme Tenable.io en optimisant un ensemble d'API et de SDK entièrement documenté. Le recours à ces outils est gratuit. Vous pouvez ainsi optimiser la valeur des données de vulnérabilité.

SLA avec garantie de disponibilité

Tenable offre la meilleure garantie de disponibilité du secteur de la gestion des vulnérabilités, grâce à un accord de niveau de service solide (SLA) pour Tenable.io. Des crédits de services sont offerts si le SLA n'est pas respecté, comme pour les fournisseurs clés du cloud, notamment Amazon Web Services.

Prestataire de scans approuvé certifié PCI

Tenable.io est une solution ASV (prestataire de scans approuvé certifié PCI) qui permet aux sites marchands et aux prestataires de services de démontrer que leurs systèmes Internet sont sécurisés conformément aux exigences et aux normes de sécurité des données PCI (PCI DSS) en matière de scans externes des vulnérabilités réseau.

Formation

Tenable propose des formations aux débutants et à ceux qui souhaitent disposer des connaissances et du savoir-faire requis pour maximiser leur utilisation de Tenable.io, ainsi que des formations spécialisées pour les utilisateurs plus avancés.

Les cours sont disponibles à la demande sur le [site Web de Tenable](#).



Pour en savoir plus : Merci de visiter [tenable.com](#)

Nous contacter : Envoyez-nous un e-mail à sales@tenable.com ou accédez à [tenable.com/contact](#)

Copyright © 2017, Tenable Network Security, Inc. Tous droits réservés. Tenable Network Security et Nessus sont des marques déposées de Tenable Network Security, Inc. Tenable et Tenable.io sont des marques de Tenable Network Security, Inc. Les marques de tous les autres produits ou services appartiennent à leurs titulaires respectifs. EN-APR122017-V6