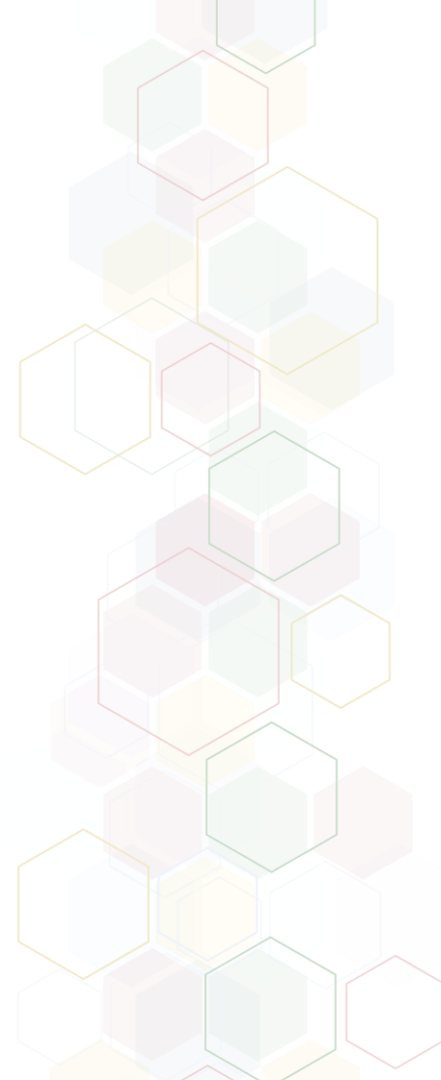


ManageEngine 

Vulnerability Manager Plus

Présentation du produit



Solution de gestion des menaces et des vulnérabilités axée sur l'établissement de priorités et offrant des correctifs intégrés pour les entreprises

- Il s'agit d'une solution multi-OS qui offre une visibilité complète, une évaluation, une remédiation et un reporting des vulnérabilités, des mauvaises configurations et des autres failles de sécurité sur le réseau de l'entreprise à partir d'une console centralisée.



4 étapes pour une gestion efficace de la vulnérabilité



Compatible avec Windows, Linux et Mac



Windows



Linux



Mac*

*Seule la gestion des correctifs est prise en charge pour macOS.

Fonctions principales

- ❖ Évaluation complète de la vulnérabilité
- ❖ Gestion de la configuration de la sécurité
- ❖ Gestion automatisée des correctifs
- ❖ Respect des critères CIS
- ❖ Rapports détaillés

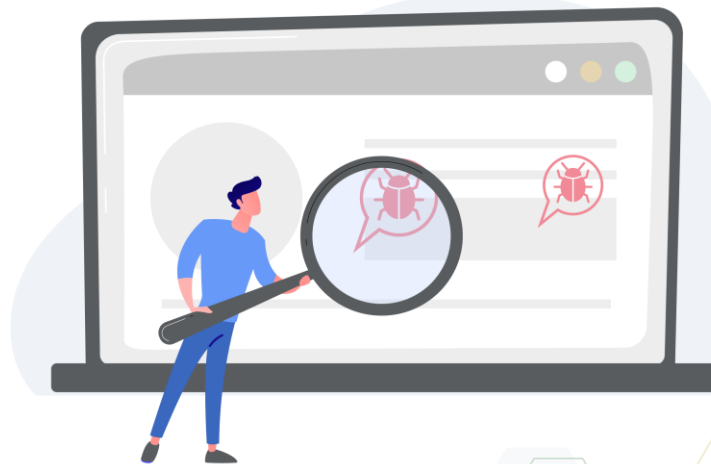


Évaluation et détection complètes des vulnérabilités

Identifiez et évaluez les risques réels liés à une multitude de vulnérabilités réparties dans vos systèmes d'exploitation, vos périphériques réseau et vos applications tierces.

Caractéristiques:

- ❖ Identifier les vulnérabilités et leur contexte, comme les scores CVSS et de gravité, afin de déterminer la priorité, l'urgence, l'impact et la disponibilité des correctifs.
- ❖ Savoir si un code d'exploitation a été divulgué publiquement pour une vulnérabilité.
- ❖ Garder un œil sur la durée de présence d'une vulnérabilité dans votre réseau.
- ❖ Utiliser un onglet dédié aux vulnérabilités divulguées publiquement et aux vulnérabilités de type "zero-day", et utiliser des solutions de contournement pour les atténuer avant que les correctifs n'arrivent.



Gestion de la configuration de la sécurité

Suivez les dérives de la configuration et déployez des configurations sécurisées pour éliminer les ailles de sécurité.

Caractéristiques :

- ❖ Identifier les mauvaises configurations dans les systèmes d'exploitation, les applications et les navigateurs, et les remettre en conformité.
- ❖ Auditer les pare-feu, les antivirus et l'état de BitLocker.
- ❖ Empêcher les tentatives de force brute en appliquant des politiques de mots de passe complexes, de verrouillage de compte et de connexion sécurisée.
- ❖ Gérer et modifier les configurations de sécurité en partageant les autorisations, en modifiant les contrôles des comptes d'utilisateurs et en désactivant les protocoles existants afin de réduire la surface d'attaque sans interrompre les activités de l'entreprise.



Gestion automatisée des correctifs

Téléchargez, testez et déployez en toute transparence des correctifs pour plusieurs systèmes d'exploitation et plus de 850 applications tierces.

Caractéristiques:

- ❖ Corrélation automatique entre les informations sur les vulnérabilités et la gestion des correctifs.
- ❖ Automatisation des correctifs pour Windows, macOS, Linux et plus de 850 applications tierces.
- ❖ Personnalisation des politiques de déploiement pour un déploiement sans problème.
- ❖ Test et approbation des correctifs avant leur déploiement dans l'environnement du produit et déclinaison des correctifs à des groupes spécifiques en fonction des besoins de l'utilisateur.



Respect des critères CIS

Exploitez les politiques disponibles pour vous conformer aux normes CIS.

Caractéristiques:

- ❖ Aide à l'audit et au maintien de la conformité avec les critères CIS.
- ❖ Automatisation des audits des actifs par rapport à plusieurs critères CIS à la fois.
- ❖ Obtention d'une remédiation détaillée pour chaque violation.



Renforcement des serveurs web

Détectez et corrigez les SSL périmés, l'accès inapproprié au répertoire racine du site web et d'autres failles du serveur web.

Caractéristiques :

- ❖ Surveillance continue de vos serveurs web pour détecter les configurations par défaut et non sécurisées.
- ❖ Analyse des configurations erronées des serveurs web en fonction du contexte et recommandations en matière de sécurité.
- ❖ Vérification de la configuration des certificats SSL et de l'activation du protocole HTTPS pour sécuriser la communication entre les clients et les serveurs.
- ❖ Vérification de la restriction des droits d'accès au répertoire racine du serveur afin d'empêcher tout accès non autorisé.



Audit des logiciels à haut risque et des ports actifs

Gérez les logiciels à haut risque et vérifiez l'activité des ports dans votre réseau dans le cadre de la gestion des vulnérabilités.

Caractéristiques:

- ❖ Vigilance à l'égard des logiciels hérités qui sont en fin de vie ou sur le point de l'être.
- ❖ Obtention d'informations en temps réel sur les logiciels peer-to-peer et les outils de partage à distance jugés dangereux, et élimination de ces derniers d'un simple clic.
- ❖ Visibilité permanente sur les ports actifs et détection des cas où un port a été activé par des exécutable malveillants.



Rapports détaillés

Les entreprises peuvent prendre des décisions éclairées en s'appuyant sur un tableau de bord dynamique et riche en graphiques et sur un ensemble intuitif de rapports prédéfinis.

Types de rapports :

- ❖ Rapports exécutifs
- ❖ Plus de 10 rapports prédéfinis
- ❖ Rapports de planification
- ❖ Rapports de requête personnalisés



Quels sont les avantages de Vulnerability Manager Plus pour votre organisation ?

- Identification précoce des menaces exploitables de manière imminente et ne nécessitant que peu ou pas d'intervention de la part de l'utilisateur.
- Réduction des efforts consacrés à la gestion des vulnérabilités grâce à une console centrale et à des tableaux de bord détaillés.
- Élimination de la nécessité d'investir dans des outils de gestion des correctifs distincts.
- Prévention d'amendes importantes grâce au respect de la conformité et des réglementations en matière de cybersécurité.



Pour en savoir plus, visitez le site :

<https://www.pgsoftware.fr/uems/vulnerability-manager-plus>

Essayez-le gratuitement !

<https://www.pgsoftware.fr/uems/vulnerability-manager-plus/telecharger>