



# Vulnerability Scanning

Évitez les risques inutiles dans votre centre de données et patchez à temps

Les organisations prennent conscience des risques auxquels elles sont confrontées uniquement lorsque des failles de sécurité font la une des médias. **Savez-vous qu'aujourd'hui, le non-patching de logiciels est l'une des trois grandes portes d'entrée pour les hackers** ? En effet, la majorité des cyberattaques réussies trouvent leur origine dans une vulnérabilité connue qui n'a pas été corrigée. Ou, pire encore, dans une vulnérabilité que l'organisation ne connaissait pas du tout.

En 2022, un nombre record de 26 448 failles de sécurité logicielles ont été signalées dans le monde entier. Le nombre de vulnérabilités critiques a augmenté de 59 % par rapport à 2021 pour atteindre 4 135. Le recensement continu de toutes ces nouvelles vulnérabilités est une tâche considérable. Si l'on ajoute à cela les ressources limitées dont disposent les équipes informatiques, cette situation entraîne vite des **dysfonctionnements**. Mais ce qui est beaucoup plus grave, **c'est qu'il en résulte également une exposition inutile à des risques parfaitement évitables**.

Avec notre **scan des vulnérabilités**, la détection des failles est une tâche ni coûteuse ni chronophage. Notre solution aide votre équipe informatique à identifier et analyser une quantité gigantesque de vulnérabilités connues. Vos collaborateurs peuvent désormais se consacrer à d'autres tâches et, par exemple, corriger sans attendre toutes ces vulnérabilités. Ainsi, vous **passez** de la détection **à la résolution efficace de vos problèmes de sécurité**.

## Scan des vulnérabilités : la sécurité à prix fixe

Notre prix dépend du nombre d'appareils à scanner pour détecter les vulnérabilités. Notre offre de base couvre 500 appareils. Vous pouvez compléter ce kit de démarrage avec des packs supplémentaires de 250 appareils chacun. Notre tarif est fixe tant pour l'offre de base que pour les packs complémentaires. Vous connaissez ainsi toujours le budget à allouer au scan des vulnérabilités. Fini les mauvaises surprises.

### Notre approche : évitez les risques inutiles en 5 étapes.

- 1. Lancement et entretien préliminaire** : Un premier entretien nous aide à comprendre vos besoins et à déterminer le nombre précis d'appareils que nous devons scanner pour détecter les vulnérabilités. Vous sélectionnez l'offre qui vous convient le mieux à partir de cette analyse initiale.
- 2. Visite client et implémentation** : Nous venons installer et configurer notre solution de Vulnerability Scanning chez vous. Il s'agit d'un service sur mesure. Nous le faisons en concertation et en étroite collaboration avec vos propres responsables IT.
- 3. Collecte de données** : Collecte des données sur vos appareils, y compris des informations sur les vulnérabilités, les mauvaises configurations et d'autres problèmes de sécurité.
- 4. Analyse à distance** : Nous traitons et analysons les données dans notre centre d'analyse. Cette analyse identifie les problèmes de sécurité et attribue un score de risque à chaque problème.
- 5. Reporting** : Nous vous fournissons un rapport résumant les problèmes de sécurité identifiés, leurs scores de risque et les mesures que nous recommandons en priorité. Notre rapport vous aide ainsi à résoudre en premier les problèmes de sécurité les plus critiques.

## Que se passe-t-il après notre scan de vulnérabilité ?

Seule une **approche proactive** de la cybersécurité peut vous apporter une réponse adaptée à vos défis de sécurité. Autrement dit, les vulnérabilités dans votre centre de données doivent être détectées et traitées avant que des criminels ne les exploitent à mauvais escient.

On pourrait croire que nous enfonçons des portes ouvertes, mais la dure réalité montre que vous êtes malheureusement toujours plus vulnérable que vous ne le pensez. **C'est pourquoi il est important d'identifier toutes les failles possibles par le biais de scans réguliers.** Ce **scan des vulnérabilités** est la première étape nécessaire dans un processus beaucoup plus large de la **gestion des vulnérabilités**. Ce processus comprend également :

- **une évaluation** approfondie des risques liés à chaque vulnérabilité ;
- **une priorisation** des vulnérabilités identifiées ;
- l'élaboration d'un plan **pour remédier à temps à toutes les vulnérabilités.**

Inetum-Realdolmen dispose de toute l'expertise nécessaire pour vous conseiller et vous apporter son aide technologique au cours de ces différentes étapes.

### ENVIE D'EN SAVOIR PLUS ?

Nos experts se tiennent à votre disposition pour répondre à toutes vos questions, idées et suggestions. Ils se feront également un plaisir de vous informer sur les autres services d'Inetum-Realdolmen : [info@inetum-realdolmen.world](mailto:info@inetum-realdolmen.world)