Imunify AV : détecter des virus qui auraient infectés votre site web et les nettoyer

Imunify AV (Antivirus) est une solution de sécurité informatique développée par **CloudLinux**, une société spécialisée dans les solutions pour les environnements d'hébergement web et de serveurs.

2 versions différentes : la version gratuite **ImunifyAV** et la version encore plus puissante **ImunifyAV+**.

Imunify AV est conçu pour protéger les serveurs web et les sites web contre les menaces et les attaques malveillantes, notamment les logiciels malveillants, les virus, les chevaux de Troie, les vers et autres types de cybermenaces.

Les principales fonctionnalités et avantages d'Imunify AV incluent :

- **Détection et suppression de malwares :** Imunify AV analyse en permanence les fichiers et les processus sur le serveur à la recherche de codes malveillants ou de fichiers infectés. Il peut détecter et nettoyer les infections pour empêcher la propagation de logiciels malveillants.
- **Analyse en temps réel :** l'outil surveille activement l'activité en temps réel sur le serveur, ce qui lui permet de réagir rapidement aux menaces émergentes et de bloquer les attaques potentielles.
- **Heuristique avancée :** Imunify AV utilise des algorithmes heuristiques avancés pour détecter les nouvelles variantes de logiciels malveillants et de menaces, même si elles n'ont pas encore été répertoriées dans les bases de données de signatures.
- **Protection proactive :** il peut bloquer automatiquement les adresses IP malveillantes ou les comportements suspects, ce qui aide à prévenir les attaques avant même qu'elles ne se produisent.
- **Rapports et notifications :** Imunify AV fournit des rapports et des notifications détaillés sur les activités malveillantes détectées, ce qui permet aux administrateurs de serveurs de suivre les actions prises et de prendre des mesures correctives.
- **Intégration avec d'autres outils de sécurité :** il peut être utilisé en conjonction avec d'autres outils de sécurité pour une protection plus complète du serveur et des sites web.

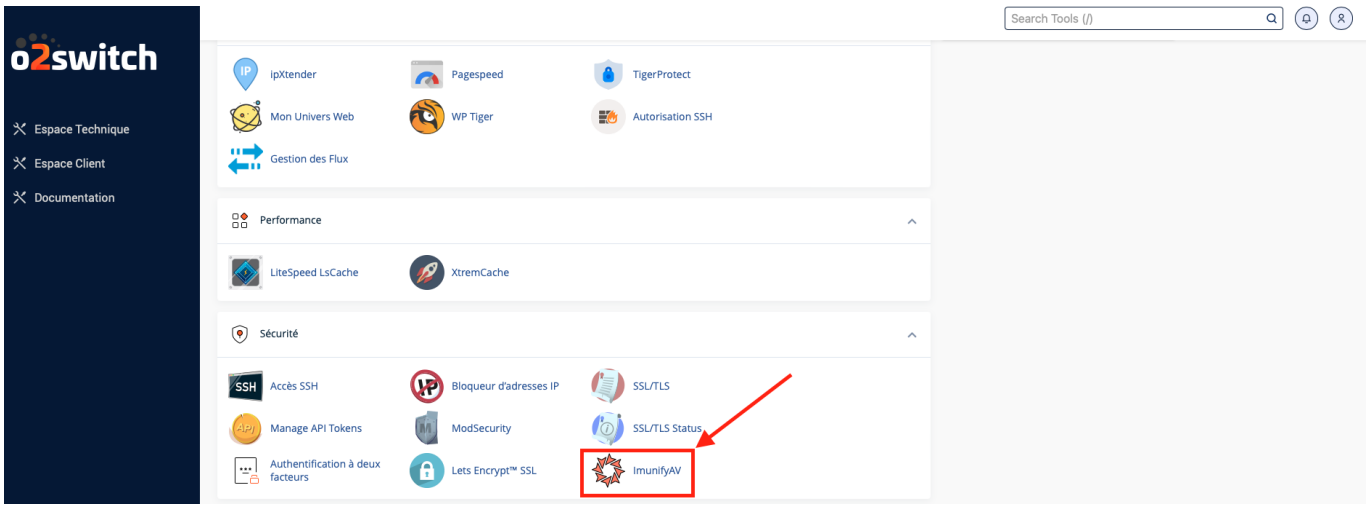
Remarque : Imunify AV prend en charge de nombreux CMS, dont **WordPress** qui fait partie des cibles favorites des pirates.

Imunify AV est notamment disponible chez l'hébergeur web **o2switch**, au niveau de votre **cPanel**.

Recherchez une section ou une icône liée à la sécurité, à la gestion des antivirus ou à **Imunify AV**.

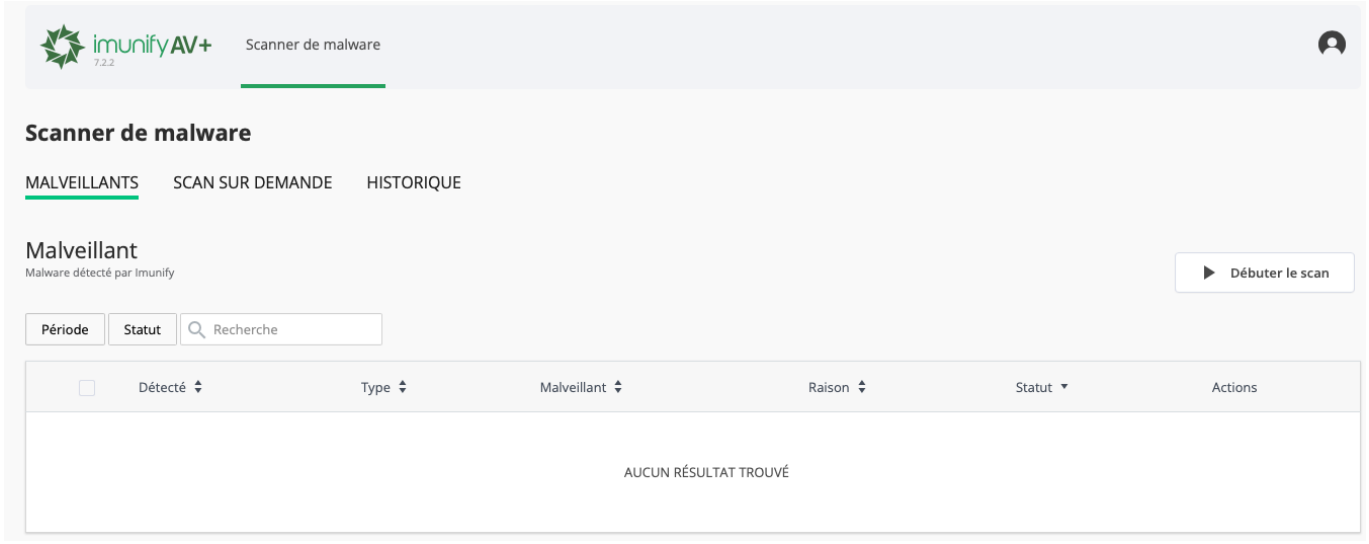
Ces noms peuvent varier en fonction de la configuration spécifique de **cPanel**.

Cliquez sur l'icône ou l'option correspondante pour accéder à l'interface **Imunify AV**.



Dans l'interface **Imunify AV**, recherchez une option ou un bouton permettant de lancer un scan.

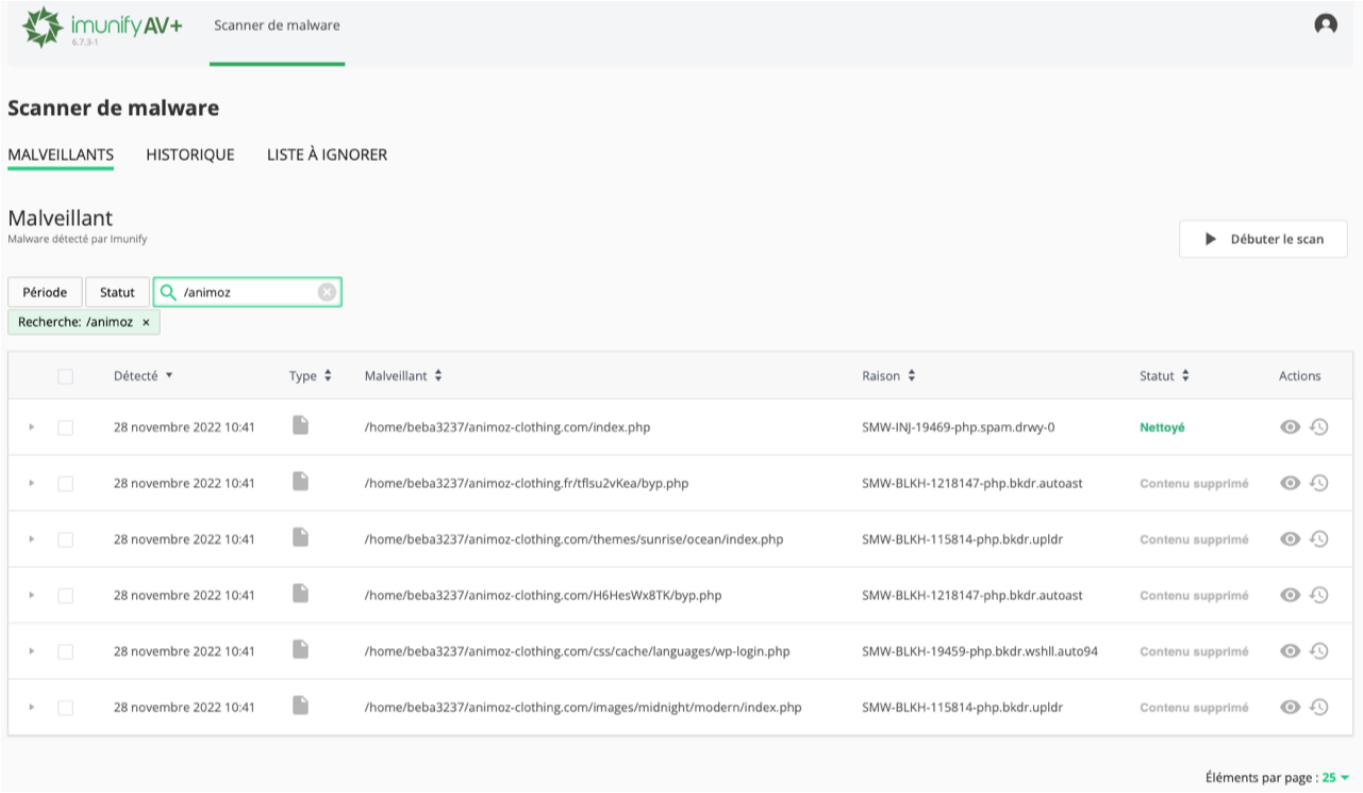
Il peut s'agir d'une option pour analyser tout le serveur, une partie spécifique du serveur ou un domaine particulier.



Attendez que le scan se termine.

Le temps nécessaire dépendra de la taille du serveur et de la quantité de données à analyser.

Une fois le scan terminé, vous devriez recevoir des résultats indiquant s'il y a eu des détections de logiciels malveillants ou d'autres problèmes.



Si Imunify AV a détecté des fichiers malveillants sur votre serveur, il est important de nettoyer rapidement ces fichiers pour protéger votre système et vos données (onglet Actions).