

Sécurité de l'infrastructure d'hébergement

La plateforme est hébergée sur une infrastructure **Plesk** bénéficiant de plusieurs niveaux de protection visant à assurer la disponibilité des services, la sécurité des données et la résistance face aux attaques courantes.

Les principales mesures de sécurité mises en œuvre sont les suivantes :

- **Serveur dédié sous Plesk** administré et maintenu régulièrement.
- **Chiffrement des communications** via HTTPS/TLS.
- **Pare-feu applicatif (WAF)** et mécanismes de filtrage des requêtes.
- **Imunify360** assurant une protection avancée contre les logiciels malveillants, les attaques web, les tentatives d'exploitation de vulnérabilités et les comportements suspects.
- **Fail2Ban** avec plusieurs règles de protection permettant le bannissement automatique des adresses IP présentant un comportement anormal (tentatives répétées, erreurs, dépassements de seuils, etc.).
- **Protection Nginx** contre les surcharges et attaques applicatives grâce à des mécanismes de limitation :
 - du nombre de connexions simultanées par adresse IP ;
 - du nombre de requêtes par seconde ;
 - des accès répétés à une même ressource.
- **Surveillance des journaux** permettant la détection des comportements anormaux et l'adaptation des règles de protection.
- **Mises à jour régulières** du système d'exploitation, de Plesk, de PHP et des composants logiciels.
- **Isolation des sites** et gestion indépendante des services PHP-FPM.
- **Sauvegardes régulières** permettant la restauration rapide des services en cas d'incident.

L'ensemble de ces mécanismes permet de limiter les risques liés aux attaques automatisées (robots, scans, brute force, déni de service applicatif, exploitation de vulnérabilités connues) tout en maintenant un haut niveau de disponibilité des services.

Les mécanismes de sécurité sont régulièrement adaptés en fonction des menaces observées et des retours d'exploitation, afin de maintenir un niveau de protection cohérent avec l'évolution des risques.