Présentation fonctionnelle

CyberShield

Auteur: Securas Technologies

Version: 1.1 Date: 11 Novembre 2025

Introduction

La présente présentation fonctionnelle a pour objectif de vous accompagner dans la découverte, la compréhension et l'utilisation des fonctionnalités de CyberShield, la solution SaaS de cybersécurité web développée par Securas Technologies.

Elle s'adresse à la fois aux utilisateurs finaux, souhaitant protéger leurs sites web, et aux distributeurs, chargés du déploiement et du suivi de la solution auprès de leurs clients.

À propos de CyberShield
CyberShield est une plateforme complète de sécurité web conçue pour assurer une protection en temps réel contre un large éventail de menaces, notamment :

- Les injections SQL (SQLi)
- Les attaques XSS (Cross-Site Scripting)
- Les bots malveillants et visiteurs suspects

Avantages de CyberShield

Commencez en 5 minutes

Déployez la solution en quelques minutes et commencez à protéger vos sites ou ceux de vos clients sans configuration complexe.

Facile à utiliser

Une interface intuitive qui facilite la gestion de la sécurité pour tous, particuliers comme distributeurs.

Contrôle et surveillance en temps réel

Détection et blocage instantanés des attaques pour garantir la sécurité de chaque site surveillé.

Alertes instantanées : Restez informé, restez en avance

Recevez des notifications en temps réel pour intervenir rapidement sur vos sites ou ceux que vous gérez.

1 solution – Sécurité multi-sites

Administrez plusieurs sites ou comptes clients depuis une seule plateforme centralisée.

Rentable

Des offres flexibles et avantageuses adaptées aux besoins des utilisateurs et à la croissance des distributeurs.

1. Tableau de bord centralisé

Le Tableau de bord centralisé (Dashboard) est le cœur de l'application CyberShield.
Il offre une vue d'ensemble claire et dynamique de la sécurité de vos sites web, tout en donnant aux distributeurs une supervision centralisée de tous les clients protégés.

Deux modes d'affichage s'adaptent à vos besoins :

- **Mode Facile** (Easy Mode) – Pour une expérience simplifiée et visuelle.
- **Mode Expert** (Expert Mode) – Pour une analyse technique détaillée.

Mode Facile (Easy Mode)

Conçu pour une lecture intuitive, le Mode Facile simplifie la sécurité en présentant les informations essentielles sous forme d'indicateurs visuels et de statistiques claires.

💡 **Idéal pour les utilisateurs finaux ou distributeurs souhaitant un suivi rapide et visuel de la sécurité.**

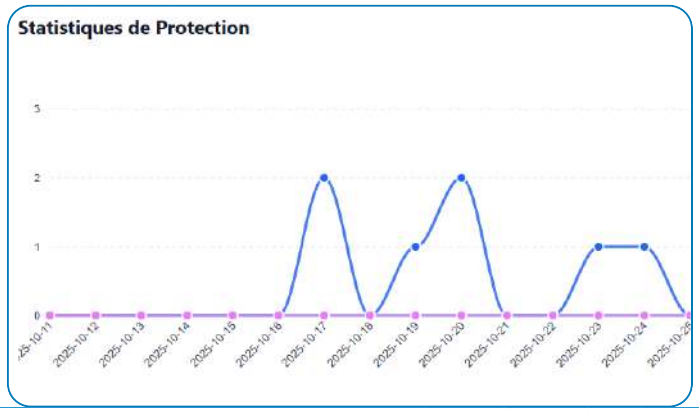
Vos outils de sécurité en un coup d'œil :

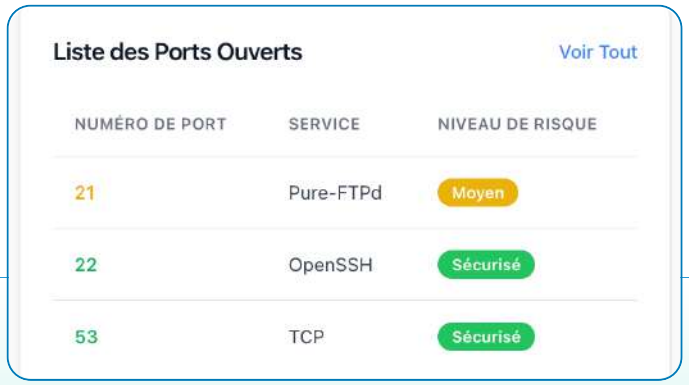
- **CyberShield Security:** Aperçu instantané du niveau de protection du site.
- **Centre de Protection Firewall :** Un accès direct pour activer ou désactiver vos protections selon vos besoins.
- **Statistiques simplifiées** : Cartes interactives des attaques bloquées, visiteurs suspects et menaces détectées par l'IA.

Mode Expert (Expert Mode)

Pensé pour les professionnels et partenaires techniques, le Mode Expert fournit des métriques avancées et des analyses en temps réel.

⚙ Conçu pour ceux qui veulent aller plus loin dans la compréhension et le pilotage de la sécurité web.





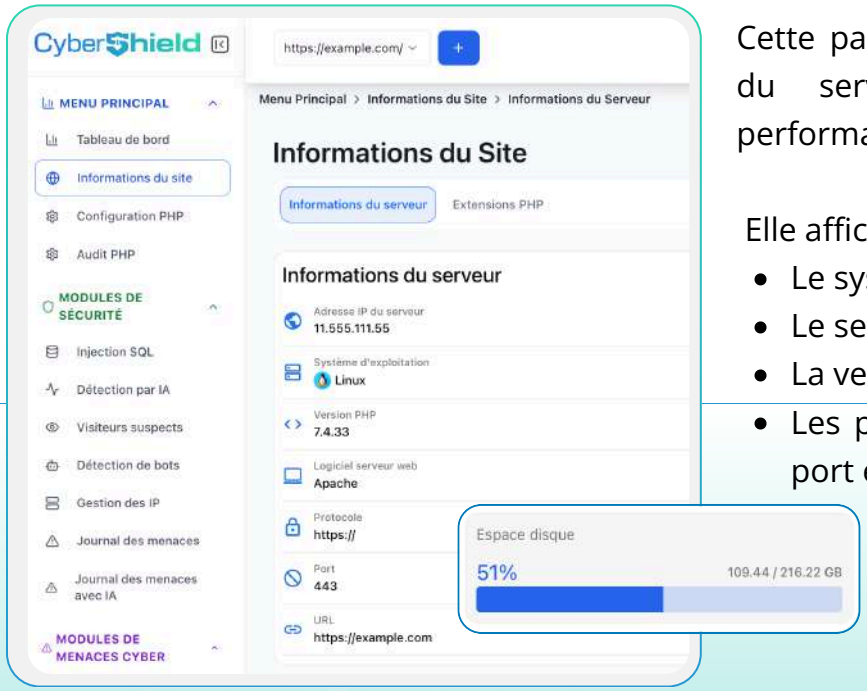
Indicateurs clés :

- **Aperçu des attaques :** suivi des menaces détectées (SQLi, XSS, bots, IA).
- **Statistiques de trafic :** volume et tendances des requêtes sur différentes périodes.
- **Indicateurs de sécurité :** vulnérabilités, ports ouverts et comportements suspects.
- **Filtrage avancé :** analyse ciblée par période ou catégorie de risque.

2. Informations du Site

La section Informations du Site offre une vision complète de l'environnement technique du site web protégé.
Elle permet à l'utilisateur comme au distributeur de mieux comprendre la configuration serveur et de prévenir les erreurs.

Informations du Serveur



Cette partie regroupe les données essentielles du serveur, utiles pour le suivi des performances et la compatibilité du site.

Elle affiche notamment :

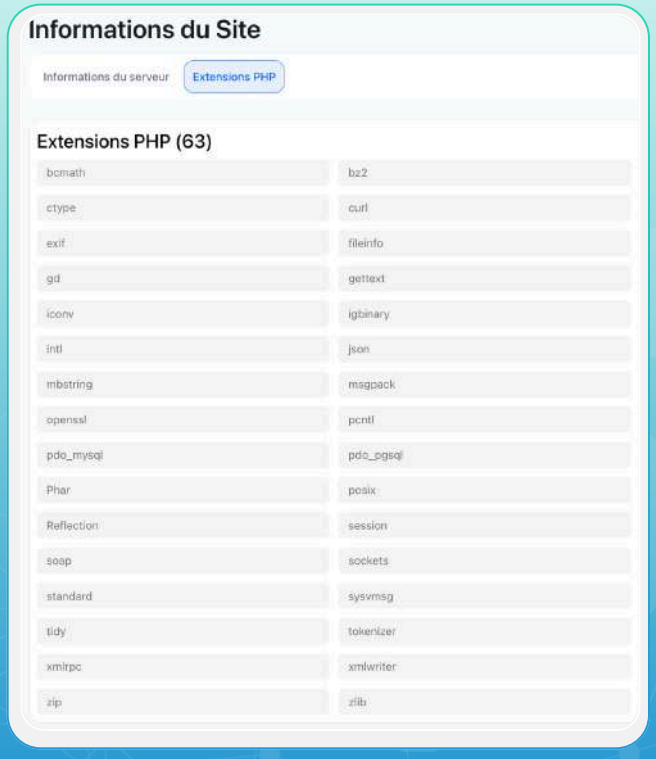
- Le système d'exploitation et sa version.
- Le serveur web utilisé (Apache, Nginx, etc.).
- La version de PHP installée.
- Les paramètres clés comme l'adresse IP, le port et l'espace disque.

Un outil pratique pour identifier rapidement les risques de configuration et assurer la stabilité du site.

Extensions PHP

Cette section répertorie les extensions PHP actives du serveur.

Cela vous permet de vérifier rapidement si les extensions requises pour le site sont présentes.



3. Configuration PHP

La section Configuration PHP permet de visualiser et d'analyser les paramètres PHP actifs sur le serveur.

Elle aide à garantir la sécurité, détecter les faiblesses et optimiser les performances des sites protégés par CyberShield.

Une configuration PHP bien paramétrée réduit considérablement les risques de vulnérabilités et améliore la stabilité de votre environnement web.

💡 **Un outil essentiel pour les utilisateurs souhaitant renforcer leur protection, et pour les distributeurs assurant un suivi technique fiable.**

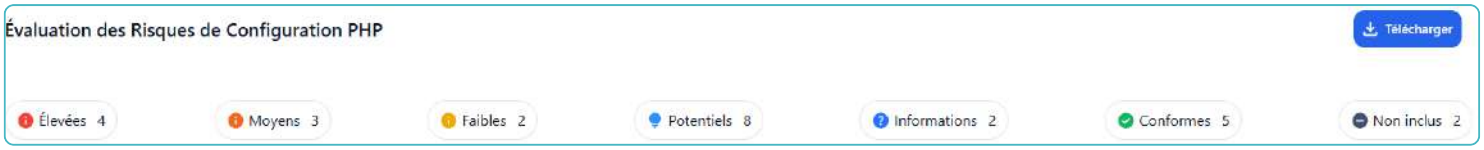
Fonctions clés

- **Contrôle des paramètres de sécurité :** vérifiez que les directives recommandées sont bien appliquées.
- **Détection des configurations à risque :** identifiez rapidement les paramètres susceptibles d'exposer votre site.
- **Optimisation des performances :** ajustez la configuration PHP pour un fonctionnement fluide et rapide.

4. Audit PHP

L'Audit PHP est un outil intelligent qui analyse automatiquement la configuration PHP du serveur afin de détecter les risques de sécurité potentiels.

Il fournit une évaluation claire de votre configuration PHP et des recommandations précises pour renforcer la sécurité du site.



Principaux atouts de l'Audit PHP

- **Évaluation instantanée** des paramètres de sécurité avec un score global et un classement par niveau de criticité (Critique, Élevé, Modéré, Bon).
- **Liste détaillée des configurations à risque,** accompagnée de recommandations correctives simples et exploitables.
- **Suivi visuel clair** grâce à des indicateurs et graphiques facilitant la priorisation des actions.

5. Modules de Sécurité

Les modules de sécurité sont le cœur de CyberShield.
Ils assurent une protection en temps réel contre les attaques web et offrent un contrôle simple et centralisé pour les utilisateurs et distributeurs.

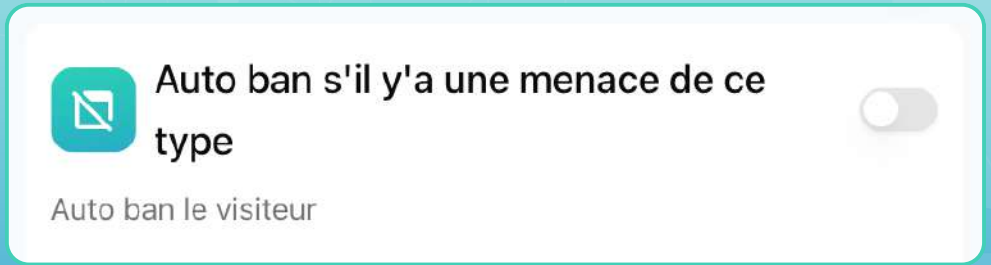
Injection SQL (SQL Injection)

Ce module protège votre site contre les attaques SQL et XSS, qui visent à manipuler les bases de données ou exécuter du code malveillant.

Il agit automatiquement pour détecter, bloquer et consigner toute tentative d'intrusion.

Fonctions clés:

- **Activation globale**
  active toutes les protections en un clic.
- **Alertes e-mail & mobiles :**
  notification instantanée lors d'une tentative d'attaque.
- **Journalisation:**
  enregistrement détaillé des tentatives.
- **Bannissement automatique:**
  blocage immédiat des IP malveillantes.



Détection par IA (Detection by AI)

Ce module exploite l'intelligence artificielle pour identifier les attaques sophistiquées qui échappent aux méthodes de détection classiques.

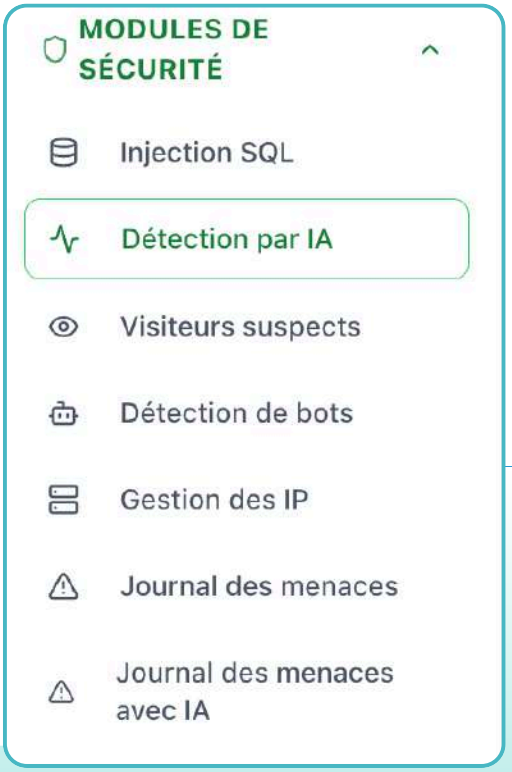
Grâce à l'apprentissage automatique, il reconnaît les nouvelles variantes d'injections SQL et d'attaques XSS, garantissant une protection toujours à jour.

Fonctions clés:

- **Détection SQL par IA**
  Identifie les attaques SQL complexes via IA.

- **Détection XSS par IA**
  Repère les attaques XSS avancées et les comportements suspects.

- **Alertes intelligentes**
  Notifications instantanées par e-mail ou mobile, journalisation automatique et bannissement des IP malveillantes.



💡 **Une protection évolutive qui apprend en continu pour détecter les menaces émergentes avant qu'elles ne vous atteignent.**

Visiteurs Suspects

Ce module surveille et bloque les visiteurs provenant de sources suspectes, telles que des proxys, des VPN, le réseau Tor ou des adresses IP à mauvaise réputation.

Fonctions clés:

- **Détection des visiteurs suspects :**

  Identifie et bloque automatiquement les visiteurs présentant un comportement malveillant (scans, tentatives d'exploitation, accès non autorisés, etc.).

Détection des Bots

Ce module est spécialisé dans l'identification et le blocage des bots malveillants, tout en autorisant les bots légitimes comme ceux des moteurs de recherche.

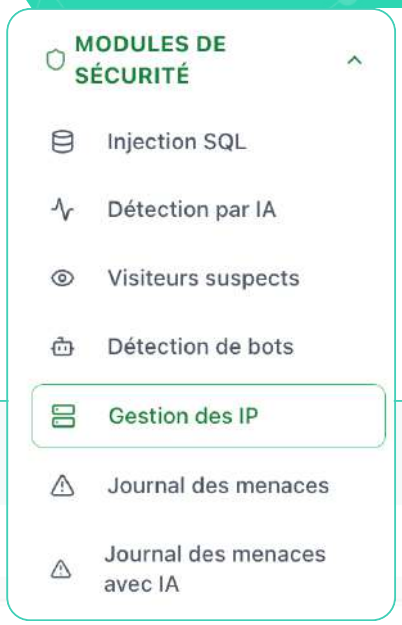
Fonctions clés:

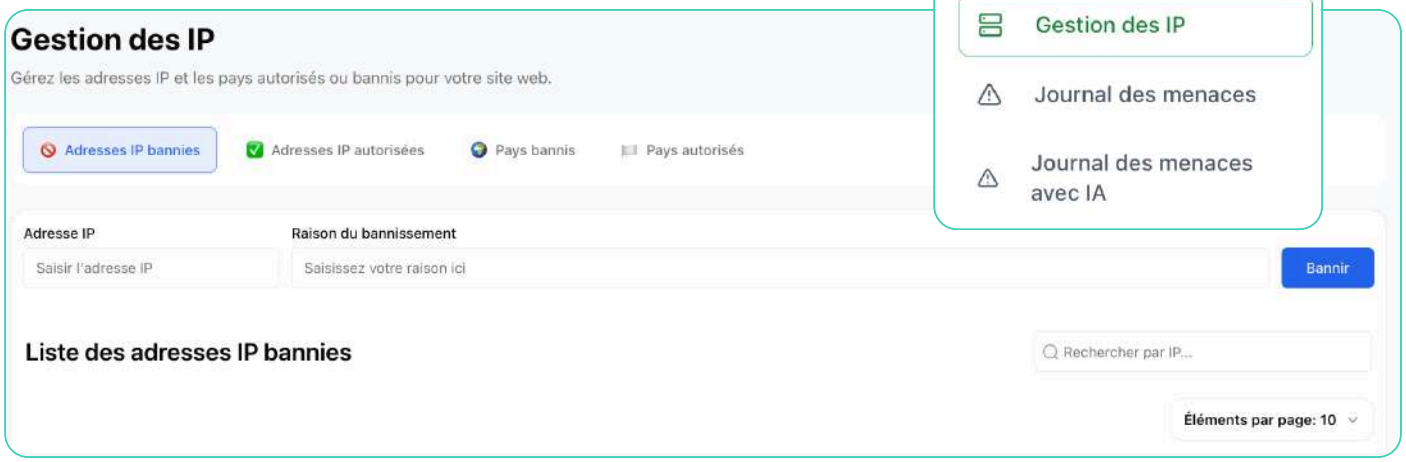
- **Détection des mauvais bots :**
  Bloque les bots connus pour être malveillants.
- **Détection des faux bots :**
  Identifie les bots qui se font passer pour des bots légitimes (par exemple, un faux Googlebot).
- **Protection contre le spam :**
  Bloque les bots qui tentent de poster du spam dans les commentaires ou les formulaires.

Gestion des IP & Pays

Ce module offre un contrôle complet des accès réseau dans les environnements protégés par CyberShield.

Il permet de bloquer les sources suspectes et de définir les zones de confiance selon les besoins de sécurité.





- **Blocage des IP malveillantes**

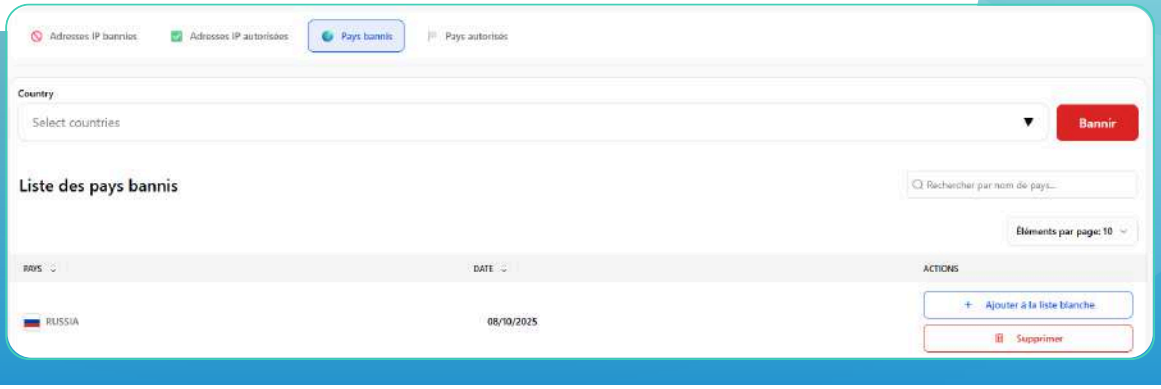
Détection et blocage automatiques des adresses IP suspectes, avec ajout manuel possible et suivi en temps réel.

- **Filtrage par pays (Geo-Blocking)**

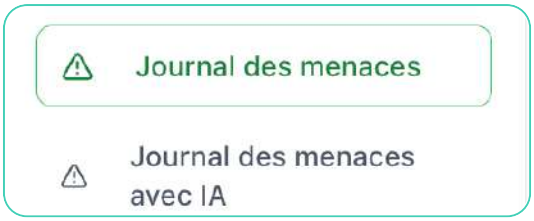
Autorisez ou interdisez l'accès depuis certains pays pour renforcer la sécurité ou limiter les connexions à des zones spécifiques.

- **Adresses et régions de confiance**

Ajoutez les IP ou pays fiables (bureaux, partenaires, serveurs internes) pour garantir un accès continu et sécurisé.



Journal des Menaces

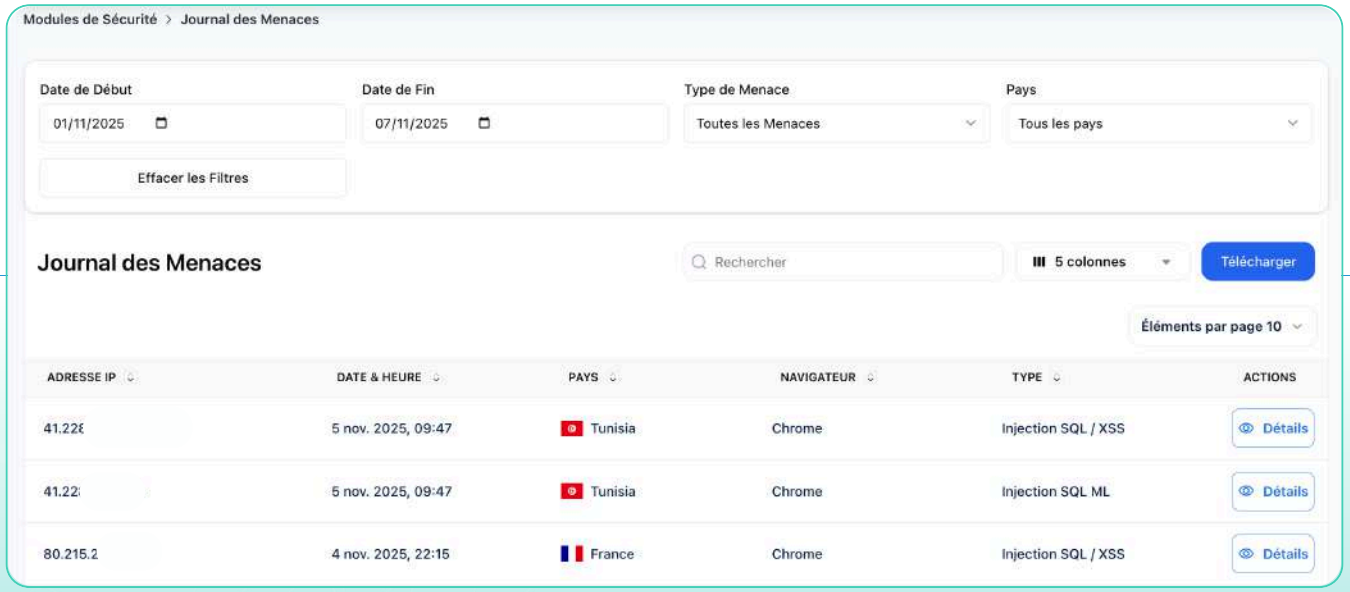


Le Journal des Menaces centralise l'ensemble des activités malveillantes détectées par les différents modules de CyberShield.

C'est un outil essentiel pour surveiller les attaques bloquées, analyser leur origine et améliorer la stratégie de protection.

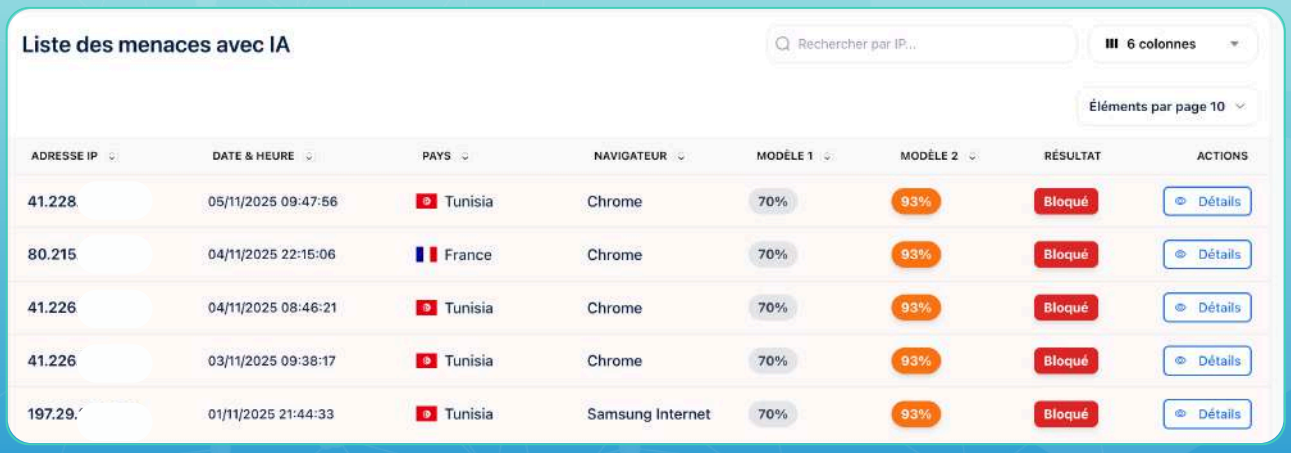
Journal des Menaces Standard

Présente la liste chronologique des menaces détectées par les modules classiques (SQLi, XSS, bots, visiteurs suspects, etc.).



Journal avec IA

Cette vue exploite les modules d'intelligence artificielle pour identifier les attaques complexes ou émergentes.



6. Modules de Cybermenaces

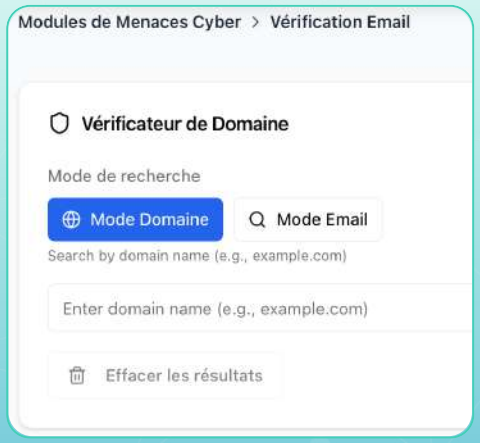
Les modules de cybermenaces complètent la protection en offrant des outils d'analyse proactive et de veille externe.

Ils aident à détecter les fuites de données, évaluer les services exposés et identifier les vulnérabilités critiques sur les systèmes connectés.

Vérification d'Email

Cette option permet de vérifier si des adresses ou domaines ont été compromis dans des fuites de données publiques.

Cet outil aide à prévenir l'exploitation d'identifiants exposés appartenant à des équipes internes ou partenaires.



Deux modes disponibles :

- **Mode Domaine :** Recherche toutes les adresses compromises associées à un domaine.
- **Mode Email :** Vérifie si une adresse spécifique apparaît dans une base de fuite connue.

💡 **Utile pour évaluer le niveau d'exposition numérique des organisations gérées.**

Vérification des Services

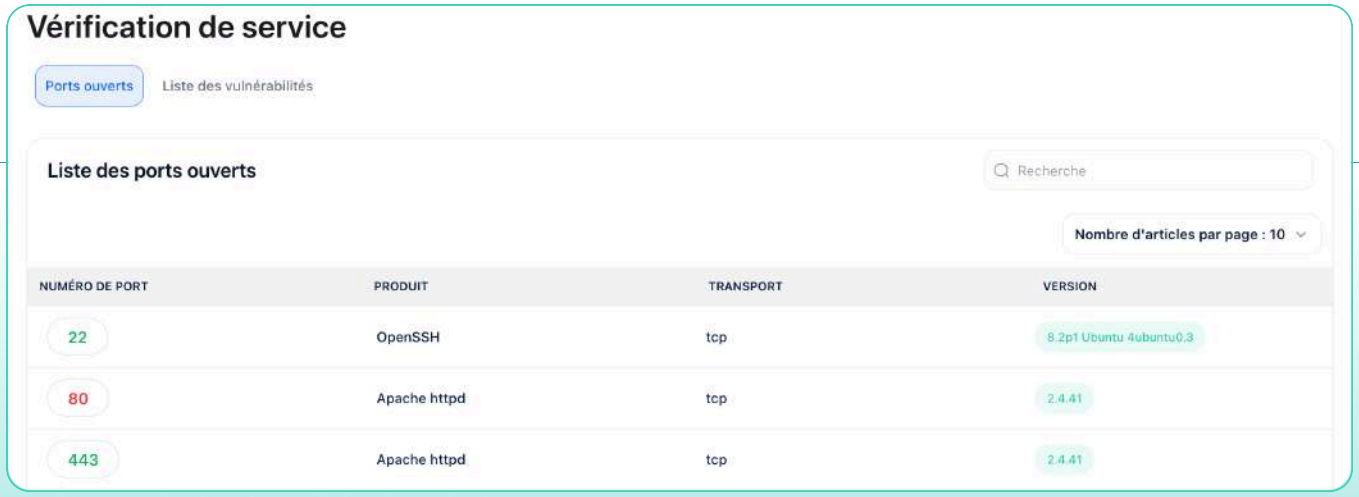
Ce module aide à analyser les serveurs et services en ligne pour identifier les ports ouverts et les vulnérabilités connues (CVE) associées.

Chaque port détecté est évalué selon sa criticité et relié à des bases de données de sécurité internationales.

Fonctions clés:

Ports ouverts :
Liste les services actifs, protocoles et versions détectées.

Vulnérabilités associées :
Fournit une évaluation des risques par niveau (faible à critique) avec lien CVE.



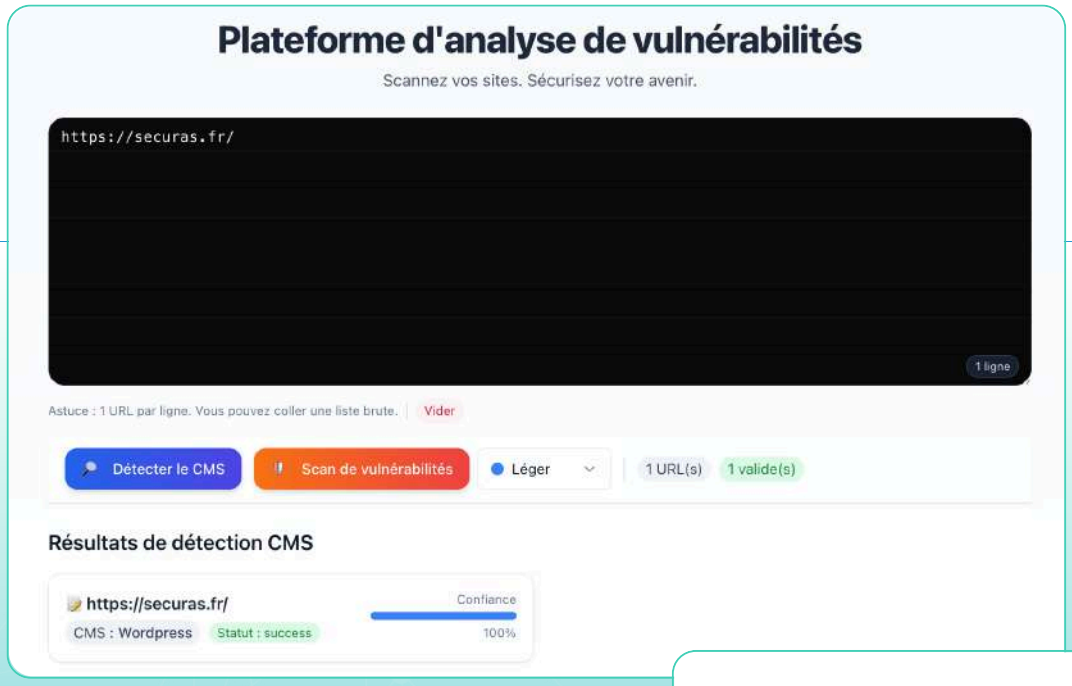
Scanner de CMS

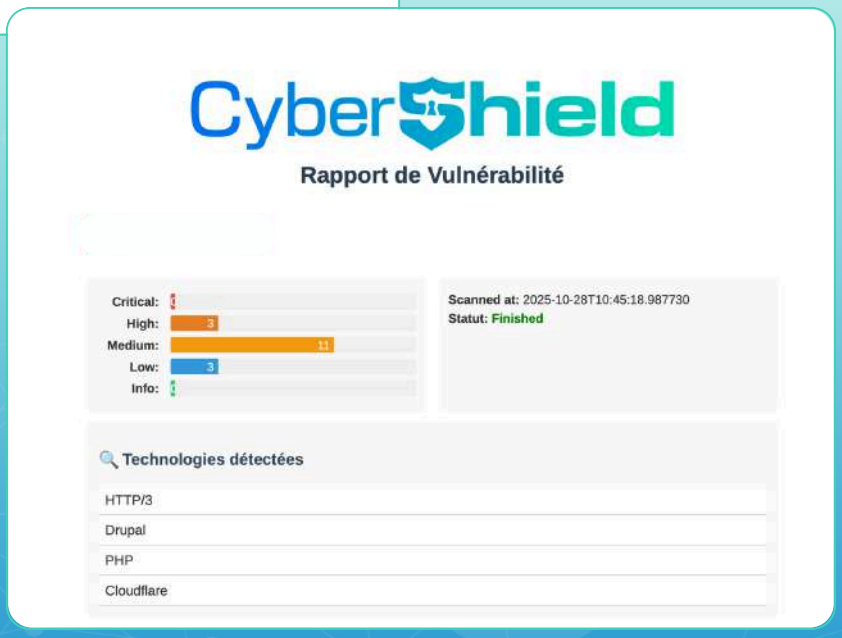
Analyse les sites web externes pour identifier le CMS utilisé (WordPress, Joomla, Drupal, etc.) et les vulnérabilités connues associées.

Il s'appuie sur une base de signatures enrichie et des algorithmes d'IA pour détecter les failles dans les noyaux, thèmes et plugins.

Fonctions clés:

- Détection automatique du CMS et de sa version.
- Scan de vulnérabilités ciblé basé sur les CVE publiques.



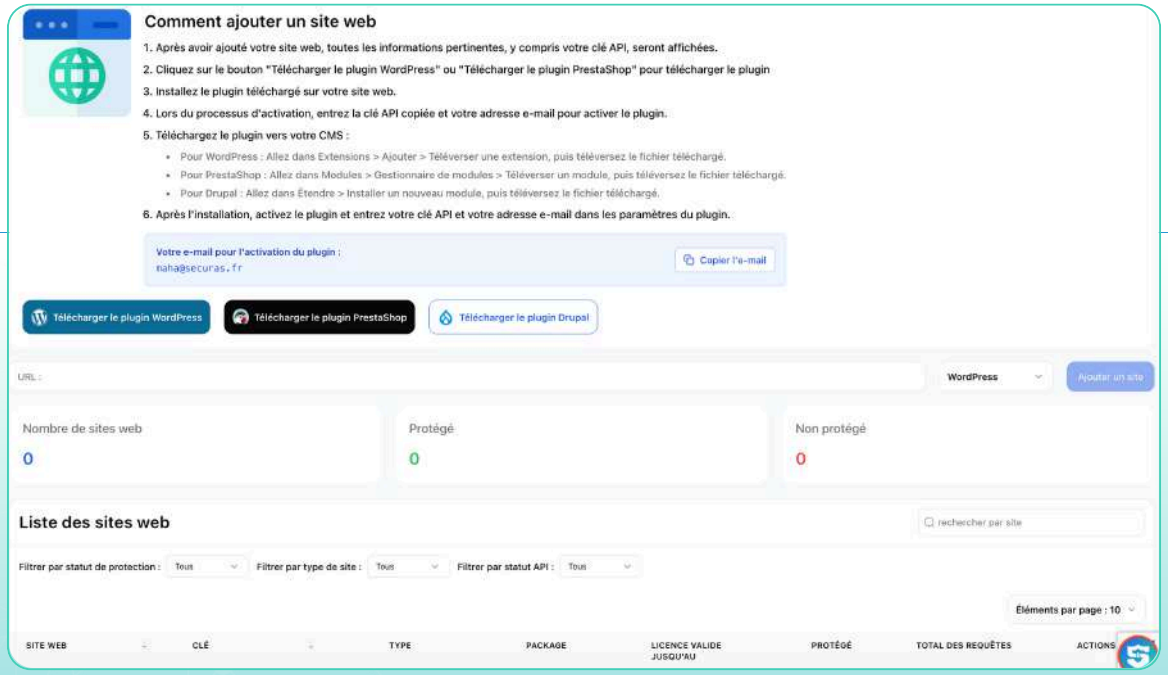


8. Options

Cette section regroupe les principaux paramètres de configuration de compte CyberShield, incluant la gestion des sites web, des préférences du compte et le reporting.

Liste des Sites Web

Cette interface vous permet de gérer les sites protégés par CyberShield : ajout, configuration et installation des plugins nécessaires à la connexion avec la plateforme.

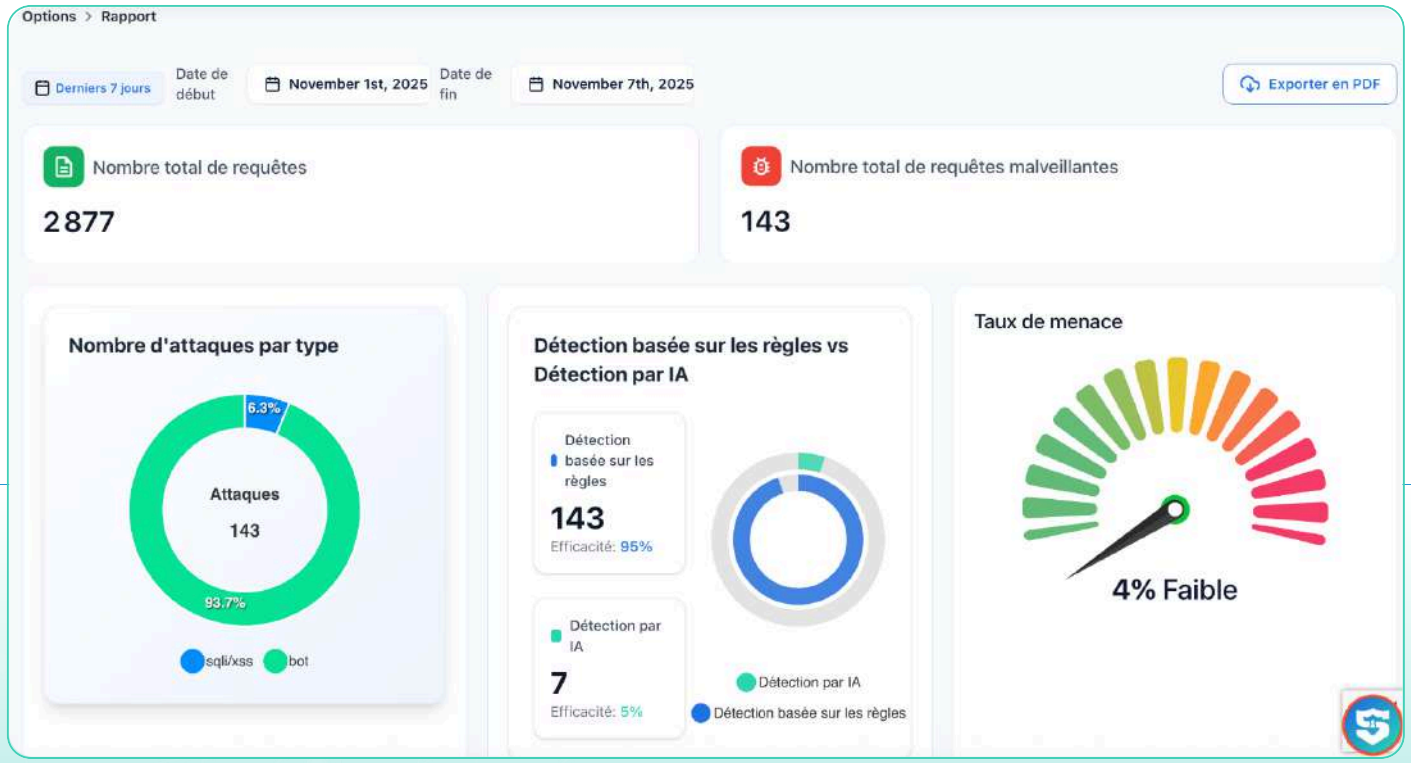


Fonctionnalités clés :

- **Ajouter un nouveau site :** saisissez l'URL, sélectionnez le type de CMS (WordPress, PrestaShop, Drupal) et le forfait associé.
- **Installation guidée :** téléchargez et installez le plugin correspondant à votre CMS via les instructions affichées.
- **Clé d'API :** une clé unique est générée pour activer le plugin et relier votre site à la plateforme.
- **Vue Distributeur :** basculez entre vos sites personnels et ceux de vos clients.

Reporting et Statistiques

Le module de reporting offre une vue complète sur l'activité et la sécurité de vos sites, facilitant l'analyse et la prise de décision.



Indicateurs clés :

- Nombre total de requêtes et requêtes malveillantes détectées.
- Répartition des attaques (SQLi, XSS, bots, etc.).
- Comparatif Détection IA / Détection par règles pour mesurer l'efficacité des moteurs de sécurité.
- Taux global de menace, exprimé sous forme d'indicateur visuel (faible, moyen, élevé).
- Export en PDF pour archivage ou partage des rapports avec vos clients.

Conclusion

Ce document présente l'ensemble des fonctionnalités clés de CyberShield et démontre comment chaque module contribue à renforcer la cybersécurité et la résilience digitale.

En combinant simplicité d'usage et technologies avancées, CyberShield permet aux entreprises et partenaires distributeurs d'assurer une protection continue contre les menaces web.

💡 **Une seule plateforme, une vision complète de la sécurité.**

À propos de nous

Securas Technologies est une entreprise spécialisée dans la cybersécurité et la protection des actifs numériques.

Nous accompagnons les organisations et distributeurs dans la mise en place de solutions fiables pour détecter, prévenir et répondre efficacement aux cybermenaces.

Nos services couvrent :

- L'analyse proactive des vulnérabilités et la sécurisation continue des systèmes.
- La surveillance en temps réel et la réponse rapide aux incidents.
- L'assistance technique pour garantir la disponibilité et la performance de vos solutions.

Pour toute question ou tout problème, n'hésitez pas à contacter le support de CyberShield.

SECURAS