



Présentation fonctionnelle

# Cyber<sup>5</sup>Shield



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 :**

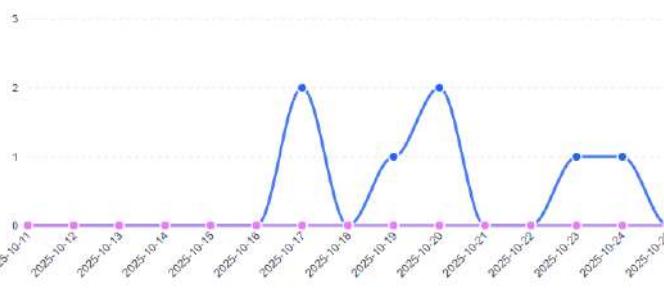
- **CyberShield Security:** Aperçu instantané du niveau de protection du site.
- **Centre de Protection Firewall :** Un accès direct pour activer ou désactiver vos protections selon vos besoins.
- **Statistiques simplifiées :** Cartes interactives des attaques bloquées, visiteurs suspects et menaces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

## Statistiques de Protection



## Évaluation des Risques de Configuration

### PHP

● Élevées	2
● Moyens	5
● Faibles	1
● Potentiels	6
● Informations	3
● Conformes	6
● Non inclus	2

[Voir les Détails](#)

## Tableau de bord

[Mode Facile](#) [Mode Expert](#)

### Mode Expert Actif

Affichage d'informations techniques détaillées et de métriques avancées.

## Liste des Ports Ouverts

[Voir Tout](#)

NUMÉRO DE PORT	SERVICE	NIVEAU DE RISQUE
21	Pure-FTPd	Moyen
22	OpenSSH	Sécurisé
53	TCP	Sécurisé

## Aperçu des vulnérabilités

[Voir les détails](#)

16 vulnérabilités trouvées



● Critique: 2  
● Elevé: 5  
● Moyen: 8  
● Faible: 1

## 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

The screenshot shows the CyberShield dashboard with the 'Informations du Site' section selected. Under 'Informations du serveur', it lists:

- Adresse IP du serveur: 11.555.111.55
- Système d'exploitation: Linux
- Version PHP: 7.4.33
- Logiciel serveur web: Apache
- Protocole: https://
- Port: 443
- URL: https://example.com

A callout box highlights the 'Espace disque' (Disk Space) section, which shows 51% usage of 109.44 / 216.22 GB.

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.

### Informations du Site

Informations du serveur	Extensions PHP
<b>Extensions PHP (63)</b>	
<small>bcmath curl ctype fileinfo exif gettext gd iconv json mbstring msgpack openssl pcntl pdo_mysql pdo_pgsql Phar posix Reflection session soap sockets standard sysvmsg tidy tokenizer xmlrpc xmlwriter zip zlib</small>	

# 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.

Directive	Valeur
System	Linux chevre.c2switch.net 4.18.0-553.50.1.lve.el8.x86_64 #1 SMP Thu Apr 17 19:10:24 UTC 2025 x86_64
Build Date	Jul 9 2025 08:26:49

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

openssl					
Directive	Valeur				
OpenSSL support	enabled				
OpenSSL Library Version	OpenSSL 1.1.1w 11 Sep 2023				
OpenSSL Header Version	OpenSSL 1.1.1w 11 Sep 2023				
Openssl default config	/opt/alt/openssl11/etc/pki/tls/openssl.cnf				
openssl.cafile	<table border="1"> <thead> <tr> <th>Local</th> <th>Master</th> </tr> </thead> <tbody> <tr> <td>no value</td> <td>no value</td> </tr> </tbody> </table>	Local	Master	no value	no value
Local	Master				
no value	no value				
openssl.capath	<table border="1"> <thead> <tr> <th>Local</th> <th>Master</th> </tr> </thead> <tbody> <tr> <td>no value</td> <td>no value</td> </tr> </tbody> </table>	Local	Master	no value	no value
Local	Master				
no value	no value				

## 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.

**Évaluation des Risques de Configuration PHP**

Élevées 4
 Moyens 3
 Faibles 2
 Potentiels 8
 Informations 2
 Conformes 5
 Non inclus 2

### 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.

AUDIT PHP	DESCRIPTIONS	CRITÈRES	RECOMMANDATIONS
Élevées	Version PHP Vérifie si votre version de PHP est > 8.0	La version de PHP est très ancienne	S'il vous plaît mettre à jour PHP dès que possible. ...

Moyens	php.ini -> assert.active	-
Moyens	php.ini -> disable_classes	-
Moyens	php.ini -> session.use_strict_mode	-
Faibles	php.ini -> expose_php	-
Faibles	php.ini -> max_execution_time	-
Potentiels	Suhosin Vérifie si le Suhosin-Extension est chargé	

# 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.

### MODULES DE SÉCURITÉ

#### Injection SQL

- ⚡ Détection par IA
- 👁️ Visiteurs suspects
- 🤖 Détection de bots
- 🌐 Gestion des IP
- ⚠️ Journal des menaces
- ⚠️ Journal des menaces avec IA



Auto ban s'il y'a une menace de ce type



Auto ban le visiteur

# 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.

## MODULES DE SÉCURITÉ

Injection SQL

**Détection par IA**

Visiteurs suspects

Détection de bots

Gestion des IP

Journal des menaces

Journal des menaces avec IA

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

### Détection par IA

Activer tout

Activer la notification par e-mail pour ce type de menaces

Activer le log de ce type d'attaque

Auto bannir s'il y a une menace de ce type

Recevoir une notification par e-mail

Enregistrer dans le log

Auto bannir le visiteur

### Activer la détection SQLi avec IA

Activer la détection des attaques SQLi avec IA

### Activer les alertes mobiles pour cette menace

Recevoir une notification push lors de la détection d'une attaque SQLi avec IA

# 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.).

## MODULES DE SÉCURITÉ

Injection SQL

Détection par IA

**Visiteurs suspects**

Détection de bots

Gestion des IP

Journal des menaces

Journal des menaces avec IA

# 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.

## MODULES DE SÉCURITÉ

Injection SQL

Détection par IA

Visiteurs suspects

**Détection de bots**

Gestion des IP

Journal des menaces

Journal des menaces avec IA

## 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.

## Gestion des IP

Gérez les adresses IP et les pays autorisés ou bannis pour votre site web.

Adresses IP bannies
 Adresses IP autorisées
 Pays bannis
 Pays autorisés

Adresse IP	Raison du bannissement	
Saisir l'adresse IP	Saisissez votre raison ici	<button>Bannir</button>

**Liste des adresses IP bannies**

ADRESSE IP	PAYS	RAISON	DATE
103.1	The Netherlands	Tentative de SQLi AI	25/03/2024 12:57:20
104.1	United States	Utilisation d'un proxy	25/03/2024 05:41:16

ADRESSE IP	PAYS	RAISON	DATE
103.1	The Netherlands	Tentative de SQLi AI	25/03/2024 12:57:20
104.1	United States	Utilisation d'un proxy	25/03/2024 05:41:16

### • 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.

Adresses IP bannies
 Adresses IP autorisées
 Pays bannis
 Pays autorisés

Country		
Select countries		<button>Bannir</button>

**Liste des pays bannis**

PAYS	DATE	ACTIONS
RUSSIA	08/10/2025	<a href="#">Ajouter à la liste blanche</a> <a href="#">Supprimer</a>

# 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.).

Modules de Sécurité > Journal des Menaces

Date de Début	Date de Fin	Type de Menace	Pays
01/11/2025	07/11/2025	Toutes les Menaces	Tous les pays
<button>Effacer les Filtres</button>			

**Journal des Menaces**

ADRESSE IP	DATE & HEURE	PAYS	NAVIGATEUR	TYPE	ACTIONS
41.228	5 nov. 2025, 09:47	🇹🇳 Tunisia	Chrome	Injection SQL / XSS	<button>Détails</button>
41.22	5 nov. 2025, 09:47	🇹🇳 Tunisia	Chrome	Injection SQL ML	<button>Détails</button>
80.215.2	4 nov. 2025, 22:15	🇫🇷 France	Chrome	Injection SQL / XSS	<button>Détails</button>

## Journal avec IA

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

Liste des menaces avec IA

ADRESSE IP	DATE & HEURE	PAYS	NAVIGATEUR	MODÈLE 1	MODÈLE 2	RÉSULTAT	ACTIONS
41.228	05/11/2025 09:47:56	🇹🇳 Tunisia	Chrome	70%	93%	Bloqué	<button>Détails</button>
80.215	04/11/2025 22:15:06	🇫🇷 France	Chrome	70%	93%	Bloqué	<button>Détails</button>
41.226	04/11/2025 08:46:21	🇹🇳 Tunisia	Chrome	70%	93%	Bloqué	<button>Détails</button>
41.226	03/11/2025 09:38:17	🇹🇳 Tunisia	Chrome	70%	93%	Bloqué	<button>Détails</button>
197.29.	01/11/2025 21:44:33	🇹🇳 Tunisia	Samsung Internet	70%	93%	Bloqué	<button>Détails</button>

# 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.

## MODULES DE MENACES CYBER

- Vérification d'email
- Vérification de service
- Scanner CMS

## 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.

Modules de Menaces Cyber > Vérification Email

### Vérificateur de Domaine

Mode de recherche

Mode Domaine

Mode Email

Search by domain name (e.g., example.com)

Enter domain name (e.g., example.com)

Effacer les résultats

### 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.

### Vérification de service

[Ports ouverts](#) [Liste des vulnérabilités](#)

**Liste des ports ouverts**

Recherche :  Nombre d'articles par page : 10

NUMÉRO DE PORT	PRODUIT	TRANSPORT	VERSION
22	OpenSSH	tcp	8.2p1 Ubuntu 4ubuntu0.3
80	Apache httpd	tcp	2.4.41
443	Apache httpd	tcp	2.4.41

Modules de Menaces Cyber > Vérification de Service > Vulnérabilités

### Vérification de service

[Ports ouverts](#) [Liste des vulnérabilités](#)

**Évaluation des vulnérabilités**

Total 78

**Vulnérabilités par niveau de risque**

Niveau de risque	Nombre de vulnérabilités
Faible	3
Moyen	24
Élevé	34
Critique	17

**Top 5 des vulnérabilités (Cliquez pour agrandir)**

Top 5 des CVE	Score CVSS
CVE-2022-22720	9.8
CVE-2020-33476	9.8
CVE-2020-38474	9.8
CVE-2022-31813	9.8
CVE-2021-39275	9.8

# 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.

### Plateforme d'analyse de vulnérabilités

Scannez vos sites. Sécurisez votre avenir.

1 ligne

Astuce : 1 URL par ligne. Vous pouvez coller une liste brute. | [Vider](#)

[Déetecter le CMS](#) [Scan de vulnérabilités](#) [Léger](#) 1 URL(s) 1 valide(s)

#### Résultats de détection CMS

 <a href="https://securas.fr/">https://securas.fr/</a>	Confiance 100%
CMS : Wordpress	Statut : success

# CyberShield

## Rapport de Vulnérabilité

Scanned at: 2025-10-28T10:45:18.987730  
Statut: Finished

**Vulnérabilités**

Critical: 1
High: 3
Medium: 11
Low: 3
Info: 1

**Technologies détectées**

- HTTP/3
- Drupal
- PHP
- Cloudflare

# 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.

SITE WEB	CLÉ	TYPE	PACKAGE	LICENCE VALIDE JUSQU'AU	PROTÉGÉ	TOTAL DES REQUÊTES	ACTIONS

### 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**