

BJSecureID

Solution de Sécurité Identitaire Numérique

Fingerprinting

IA & LLM Souverain

IP Rep. & OWASP

Active Response

La fraude identitaire numérique — les chiffres

+340%

hausse des fraudes identitaires numériques en Afrique subsaharienne entre 2020 et 2024

63%

des fraudes contournent l'authentification classique sans être détectées par les systèmes en place

\$2.7B

pertes annuelles liées à la fraude d'identité numérique sur le continent africain

BJSecureID — Qu'est-ce que c'est ?

BJSecureID est une solution de détection et prévention de fraude identitaire numérique, développée par CNIN Bénin.

Elle attribue à chaque visiteur un UUID unique et un Trust Score (0–100) calculé en temps réel par IA.



IDENTIFIER

UUID unique par visiteur
Fingerprinting 18+ composants
Traçabilité cross-sessions



ANALYSER

LLM souverain CNIN
Annotations comportementales
JSON structuré strict



PROTÉGER

IP Reputation 3 providers
OWASP Top 10 temps réel
Blocklists automatiques



RÉPONDRE

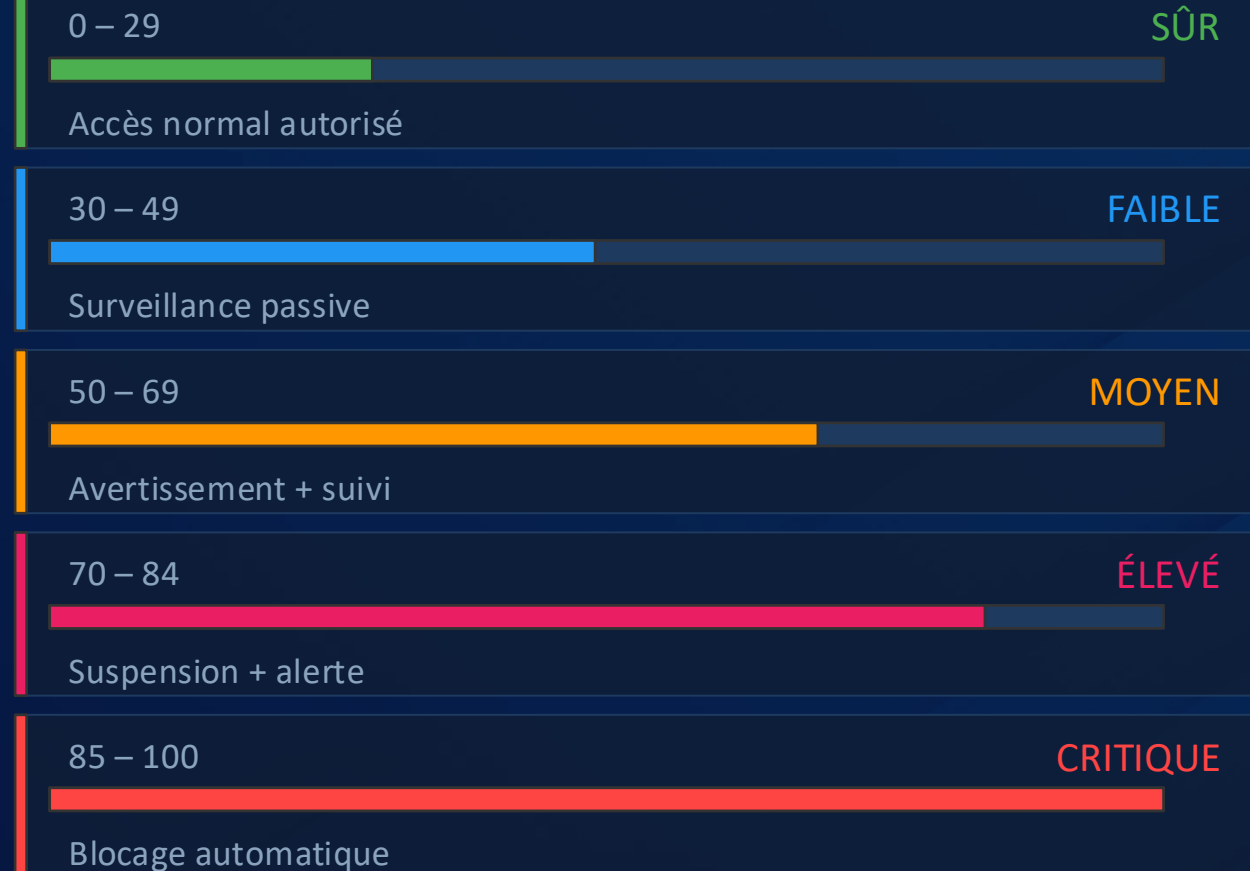
warn · suspend · block
Portée platform/entity/global
Webhooks temps réel

Identification & Score de Confiance

18+ Composants collectés par le SDK

Canvas Hash	WebGL Hash
User-Agent	Écran / DPI
Timezone	Polices système
Plugins	Mémoire RAM
Cœurs CPU	Langue / Locale
Touch	Do Not Track
AudioContext	Platform
Battery API	Connection type
WebRTC leak	Cookies

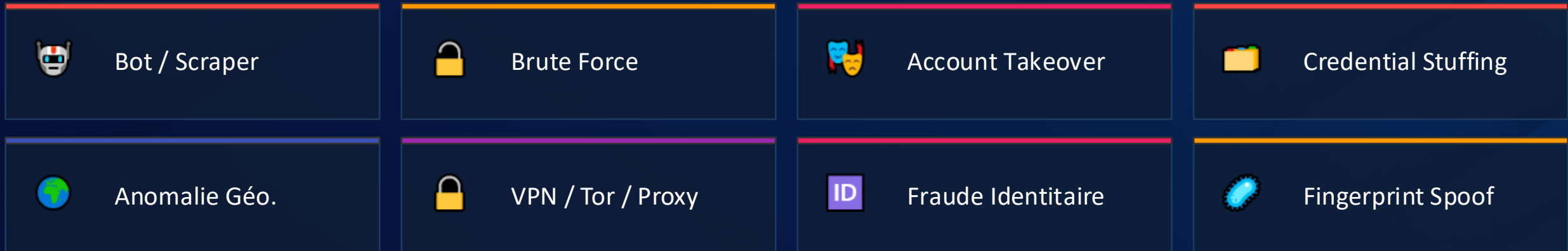
Trust Score 0 → 100 — Niveaux



Analyse Comportementale par Intelligence Artificielle



Menaces détectées



Protection Multi-Couches — IP & Web

Réputation IP — Waterfall 3 providers

Blocklist Locale



FireHOL · Spamhaus · TOR exits · feeds AbuseIPDB
Mise à jour automatique via scheduler Laravel

AbuseIPDB



Signalements communautaires mondiaux
Fraud score · Pays · ISP · historique abus

IPQualityScore



Score fraude + flags VPN / Tor / Proxy / Bot
Détection comportement abusif récent

BJ ANIP — Lookup NPI (registre identité, non IP reputation)

OWASP Top 10 — Détection Active

A01 Broken Access Control

A02 Cryptographic Failures

A03 SQL / Code Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable Components

A07 Auth & Session Failures

A08 Software Integrity Failures

A09 Logging & Monitoring Failures

A10 SSRF

Scan synchrone + analyse IA asynchrone si détection positive

Réponse Automatique & Gestion des Menaces



WARN

- Alerte dans le dashboard
- Aucune action utilisateur
- Surveillance renforcée

Score \geq seuil warn



SUSPEND

- Visiteur suspendu 24h
- Alerte critique créée
- Webhook envoyé

Score \geq seuil suspend



BLOCK

- Blocage permanent
- HTTP 403 renvoyé au SDK
- Propagation selon scope

Score \geq seuil block

PORTÉE DU BLOPAGE



PLATFORM

Limité à la plateforme d'origine



ENTITY

Étendu à toutes les plateformes de l'entité



GLOBAL

National — toutes les plateformes BJSecureID

Intégration en 3 lignes — SDK JavaScript



MODE PASSIF

- Collecte silencieuse de l'empreinte
- UUID visiteur en callback JS
- Trust Score retourné
- Aucun webhook
- Zéro modification infra



MODE ACTIF

- Webhooks temps réel bidirectionnels
- Partage profils cross-plateformes
- Synchro SSO natif
- Notifications blocage immédiates
- API bidirectionnelle

• • • bjsecure-integration.html

```
<!-- 1. Inclure le SDK -->
<script src="https://bjsecureid.bj/sdk/bjsecure.js"></script>
<!-- 2. Initialiser -->
<script>
  BJSecure.init({ apiKey: 'VOTRE_CLE_API',
    onReady: (d) => console.log('UUID:', d.visitor_uuid, '| Score:', d.trust_score) });
</script>
```