
PROJETS NOVATEURS
POUR 2026
AI

PROJETS GENERAUX EN 2026

AGENDA DES PROJETS

- 1) Copilote de gouvernance pour code IA et agents IA
- 2) Observabilité “anti-ruine” open standard pour PME et scale-ups
- 3) FinOps opérationnel pour cloud + IA + SaaS
- 4) Plateforme “Secure-by-Design” pour PME
- 5) DB Doctor universel : tuning + migration + drift + index advisor
- 6) Internal Developer Platform “lite” pour PME techniques
- 7) Sécurité supply-chain logicielle réellement exploitable
- 8) NOC/SOC autonome pour infrastructures Linux/web
- 9) “Modernisation factory” pour applications legacy
- 10) Infrastructure compliance-as-code pour PME européennes


COPILOTE DE GOUVERNANCE
POUR CODE IA ET AGENTS IA
AI
Secret Exposure
Test Coverage
RISK SCORE
AI COPILOT

1) Copilote de gouvernance pour code IA et agents IA

Idée : une plateforme qui surveille tout ce que les équipes produisent avec l'IA : code généré, prompts, dépendances introduites, secrets exposés, licences, tests manquants, hallucinations techniques, PR générées par agents.

Pourquoi c'est bankable : l'IA entre partout dans le dev, mais la qualité et la sécurité ne suivent pas au même rythme. Des équipes génèrent déjà une grande part de leur code avec l'IA, alors que beaucoup d'organisations n'ont pas de politique claire ni de contrôle sérieux sur ces usages. Il y a donc un vide énorme entre "on utilise l'IA" et "on la gouverne proprement". TechRadar +3

Le trou du marché : beaucoup d'outils codent, très peu **auditent et encadrent** vraiment l'IA de prod.

Clients : ESN, SaaS B2B, fintech, healthtech, équipes compliance.

Moat possible : moteur de règles, scoring de risque, replay d'actions des agents, branch protection intelligente.

OBSERVABILITÉ “ANTI-RUINE”

OPEN STANDARD POUR PME & SCALE-UPS

Prometheus · OpenTelemetry · Grafana

Puissante. Simple. Open Source. Maîtrisez vos coûts, pas l’inverse.

OBJECTIF

Offrir une observabilité complète, low-cost et open standard, sans exploser le budget.

ANTI-RUINE : MAÎTRISE DES COÛTS

- ✓ Réduction automatique du bruit & cardinalité
- ✓ Sampling intelligent & rétention optimisée
- ✓ Alertes utiles, pas de faux positifs
- ✓ Jusqu’à -60% sur les coûts d’observabilité

STACK 100% OPEN & INTEROPÉRABLE

Applications → OpenTelemetry (Traces, Metrics, Logs) → Prometheus (Stockage & Alerting) → Grafana (Visualisation)

DÉPLOYÉ EN QUELQUES MINUTES

Kubernetes, Docker, On-Prem ou Cloud

```
helm repo add obs https://observa.io/helm
helm install observa obs/observa --set tier=pme
```

BÉNÉFICES

- **-50 à -70%** vs solutions propriétaires
- **Déploiement rapide** & maintenance simplifiée
- **Zéro lock-in** Standards ouverts
- **Scalable** de 1 à 1M+ de métriques


OBSERVABILITÉ "ANTI-RUINE"
OPEN STANDARD POUR PME ET SCALE-UPS
OpenTelemetry
Prometheus

2) Observabilité “anti-ruine” open standard pour PME et scale-ups

Idée : une stack observabilité prête à l’emploi, basée sur OpenTelemetry/Prometheus, avec réduction automatique du bruit, optimisation des coûts, templates Kubernetes/Nginx/Postgres/MySQL/Redis, et migration hors des vendors trop chers.

Pourquoi c’est bankable : le marché veut de l’observabilité plus intelligente, moins chère et plus ouverte. Le coût, l’interopérabilité et l’évitement du lock-in sont devenus des critères centraux. Les standards ouverts comme Prometheus et OpenTelemetry prennent encore plus de poids en 2026. IBM +3

Le trou du marché : les grands outils existent, mais beaucoup de boîtes paient trop cher pour des dashboards qu’elles exploitent mal.

Clients : SaaS, e-commerce, hébergeurs, MSP, agences à forte volumétrie.

Version startup : “APM cost killer” + migration assistée + recommandations de sampling/rétention.


FinOps OPÉRATIONNEL
POUR CLOUD + IA + SaaS
Cloud Costs
SaaS Costs
OBJECTIF
ANTI-RUINE :
MATTRISE DES COÛTS
-9,275 € économisé / mois
FinOps
Coûts Mensuels
45,732 €
Projected
63.000 €
-17,580 €
économisé / mois
TOP SERVICES COÛTEUX
Compute 41%
Data Processing 23%
GPU 18%
PostgreSL 9%
TOP ANOMALIES
Inactivité GPU 100
TOP ETEIGERS
10 instances éteintes
45,732 €
Righislzing
→-9,275 économisé / mois
Auto-Extinction
→ 3,612 € économisé / mois
TOP ANOMALIES
Inactivité GPU 100
aws
Azure
Google Cloud
AI
Stack

3) FinOps opérationnel pour cloud + IA + SaaS

Idée : un outil qui relie coûts cloud, coûts LLM, coûts GPU, coûts SaaS, coûts observabilité, et qui propose des actions concrètes : rightsizing, extinction auto, anomalies, showback, budgets par équipe, simulation avant déploiement.

Pourquoi c'est bankable : le FinOps ne porte plus seulement sur le cloud public ; il s'étend au SaaS et à l'IA. En 2025, 63 % des répondants disent déjà gérer la dépense IA, et la responsabilité FinOps s'élargit. data.finops.org +2

Le trou du marché : beaucoup d'outils voient les coûts, mais peu transforment cela en **actions automatiques exploitables par les équipes techniques**.

Clients : startups qui scalent, plateformes SaaS, équipes data/AI, CTO/VP Eng.

Très bon angle : lier coûts à la télémétrie réelle et au trafic réel, pas juste à la facture.


PLATEFORME “SECURE-BY-DESIGN” POUR PME
Simplifiez la sécurité des PME. Efficace. Complète. Abordable.
Serveurs & IAM
srv01.acme.local
pierre@acme : MFA desactivé
Audit Config
8 failles (2 critiques)
Patching
17 mises à jour manquantes
Scan Secrets
3 secrets exposés
État de Sécurité
Attention
7 le 24 items
58
Attention
Patching
DASHBOARD SÉCURITÉ
Vue d'ensemble
Agents
Serveurs
Scan IAM
Conformité
Secrets
Playbooks
#1: Remédiation Serveur srv01
Corriger
74
Corriger
Compliance
4 Alerte(s) critique(s)
BENÉFICES
Durcissement Serveur & IAM automatique
Scan secrets, configuration & patching
Playbooks & conformites pour une sécurité continue
aws
Linux
SaaS

4) Plateforme “Secure-by-Design” pour PME

Idée : une plateforme de sécurité simple qui assemble en un seul endroit : durcissement serveur, IAM de base, audit de config, scan secrets, patching, backup checks, score de posture, playbooks d’incident, conformité minimale.

Pourquoi c’est bankable : la demande sécurité des PME est forte, mais leur maturité réelle reste faible. Les rapports montrent un écart massif entre confiance et préparation réelle ; en parallèle, CISA pousse fortement une approche “secure by design”. cisa.gov +3

Le trou du marché : l’offre est souvent soit trop pauvre, soit trop “enterprise”, soit trop éclatée.

Clients : PME, cabinets, e-commerce, MSP, boîtes industrielles légères.

Version rentable : abonnement récurrent + agent Linux/Windows + tableau de bord + alerting.

DB Doctor universel : Tuning + Migration + Drift

Optimisez vos bases PostgreSQL, MySQL, Oracle, SQL Server...

5) DB Doctor universel : tuning + migration + drift + index advisor

Idée : un "médecin" des bases relationnelles qui analyse PostgreSQL, MariaDB/MySQL, Oracle, SQL Server : plans d'exécution, index inutiles/manquants, schémas divergents, migrations cassées, cardinalités trompeuses, lenteurs ORM, et propose des correctifs.

Pourquoi c'est bankable : les bases restent le cœur du SI, mais le tuning fin et les migrations sûres restent des compétences rares. Le manque de talents tech freine l'exécution, ce qui rend les outils d'assistance hautement monétisables.

linuxfoundation.o... +1

Le trou du marché : il existe des outils dispersés, mais peu de solutions unifiées pensées pour les équipes qui n'ont pas un DBA senior à plein temps.

Clients : agences, SaaS B2B, infogérance, équipes Django/Rails/Node/Java.

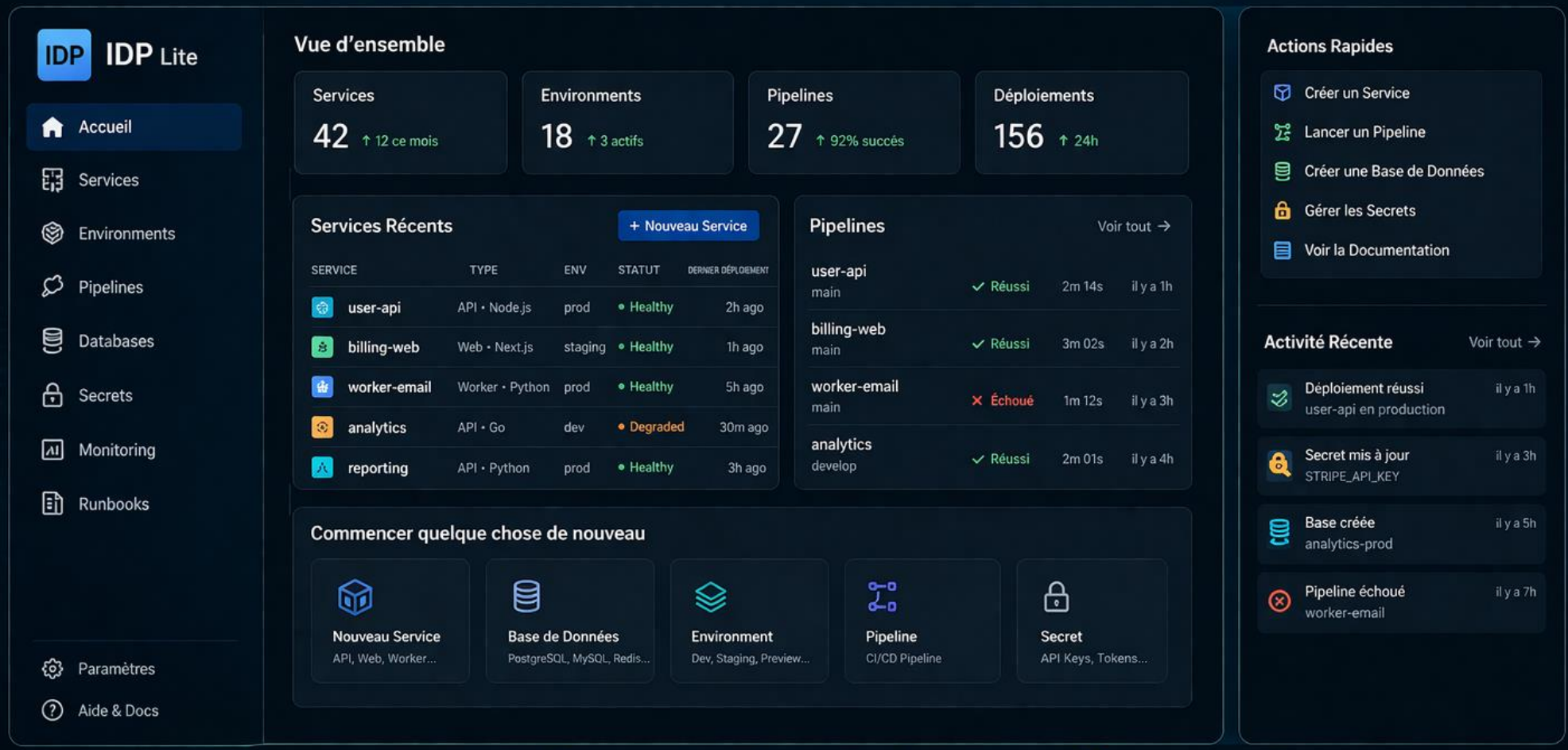
Très bon angle : brancher cela à CI/CD pour valider les migrations avant prod.

INTERNAL DEVELOPER PLATFORM "LITE"

POUR PME TECHNIQUES

La puissance d'une IDP. Sans la complexité. 100% orientée productivité développeur.

- **Déploiement en quelques clics** — Templates, GitOps, Preview envs
- **Self-Service** — Services, Bases, Secrets, Jobs
- **Standardisation** — Best practices intégrées
- **Observabilité intégrée** — Logs, Metrics, Alerts
- **CI/CD natif** — Pipelines as Code



Backstage · PORT · Kubernetes · GitOps · Terraform · OpenTelemetry · Prometheus

- **Léger & Rapide** — Setup en < 30 minutes
- **Open Source First** — Pas de lock-in
- **Conçu pour les PME** — 10 à 200 développeurs
- **Évolutif** — Grandit avec vous

6) Internal Developer Platform “lite” pour PME techniques

Idée : une IDP légère qui simplifie déploiement, création de services, secrets, jobs, bases, monitoring, runbooks, environnements preview, CI/CD.

Pourquoi c’est bankable : la platform engineering continue de monter, et les équipes veulent standardiser l’infra et améliorer la productivité dev. Gartner est souvent cité sur la forte progression des équipes plateforme, et les rapports 2025–2026 confirment que les priorités restent la standardisation et l’expérience développeur. Platform Enginee... +4

Le trou du marché : les grandes IDP sont souvent trop lourdes, trop chères ou trop complexes pour les structures de 10 à 200 développeurs.

Clients : scale-ups, ESN produit, boîtes multi-projets.

Positionnement idéal : “Backstage/Port/K8s power without the enterprise burden.”

SÉCURITÉ SUPPLY-CHAIN LOGICIELLE

Réellement Exploitable

Protégez vos dépendances logicielles. Évaluez et bloquez intelligemment les risques.

- Carte interactive des dépendances
- Remontée des menaces exploitables
- Analyse provenance
- Blocage automatique si risque avéré

harfs Python Tirivy

node React .NET aws docker GitHub Jenkins snyk

7) Sécurité supply-chain logicielle réellement exploitable

Idée : un produit qui cartographie dépendances, provenance, SBOM, signatures, packages à risque, conteneurs, secrets, transitive dependencies, et qui bloque intelligemment les mises en prod risquées.

Pourquoi c'est bankable : en 2025, OWASP a mis les échecs de supply chain logicielle très haut dans les risques majeurs. Avec la montée des dépendances open source et des builds automatisés, ce sujet devient structurel. owasp.org +3

Le trou du marché : beaucoup d'outils scannent, peu aident vraiment à **décider vite** avec un score de risque compréhensible par un CTO de PME.

Clients : SaaS, fintech, devtools, éditeurs logiciels.

Moat : scoring orienté exploitation réelle, pas simple avalanche de CVE.

NOC/SOC AUTONOME POUR INFRASTRUCTURES LINUX/WEB

Surveille. Détecte. Corrige. Sans équipe dédiée 24/7.

SOURCES SURVEILLÉES

- **Nginx / Apache** — Logs, erreurs, latence
- **SSH** — Auth, échecs, bruteforce
- **CPU / RAM / IO** — Saturation, anomalies
- **PostgreSQL / MySQL** — Connexions, lenteurs, locks
- **Réseau** — Anomalies, ports, latence
- **Système** — Services, processus, mises à jour

DÉTECTIONS AUTOMATIQUES

- **Anomalies réseau** — Pics, scans, comportements suspects
- **Floods & attaques L7** — Détection d'abus / surcharges
- **Changements système** — Packages, configs, utilisateurs
- **Problèmes applicatifs** — 5xx, latence DB, saturation
- **Comportements suspects** — Bruteforce, élévation de privilèges

STATUT GLOBAL

92 /100

SANTÉ INFRA

Stable

HÔTES	ALERTES 24H	MTTR RÉDUIT
48	3 ↓-68%	-74%

Fonctionne 24/7
Sans intervention humaine

ACTIONS AUTOMATIQUES (contrôlées & auditables)

CONFINER UNE IP MALVEILLANTE
Ajout firewall (ufw/iptables)
Automatique & réversible

PROTÉGER CONTRE BRUTEFORCE SSH
Bannissement temporaire
Fail2ban piloté par IA

REDÉMARRER UN SERVICE KO
systemd runbook safe
Seuils & fenêtres de maintenance

DRAINER TRAFIC EN CAS DE FLOOD
Rules Nginx / WAF / Rate limit
Préserve la disponibilité

EXEMPLE D'INCIDENT RÉSOLU

ALERTE	ACTION IA	RÉSULTAT
Flood sur /login + 1200 req/s détectées	Activation rate limit Nginx + blocage IP sources	Service protégé Aucun impact utilisateur

Détecté 14:32:10 • Corrigé 14:32:45 • Impact évité

POURQUOI C'EST BANKABLE

- **Manque de temps, compétences et personnel** — Les équipes veulent de l'automatisation utile, pas plus d'alertes.
- **Besoin confirmé par le marché** — La "data/cloud/network security" est un besoin prioritaire, mais la disponiblité des talents freine l'exécution.
- **Vrai vide du marché** — Passerelle manquante entre fail2ban artisanal et SOC/SIEM hors de prix.

CLIENTS CIBLÉS

Hébergeurs · PME · MSP · E-commerce · Plateformes web à petit staff infra

MODÈLE TRÈS MONÉTISABLE

SELF-HOSTED — Vous hébergez
- Licence par hôte / volume
- Idéal pour tech teams & souveraineté

MANAGED — Recommandé — Nous hébergeons
- Abonnement mensuel / périmètre
- Mises à jour, tuning, assistance incl.

Agent léger — Déploiement en 5 min
IA corrélation multi-signaux — Moins d'alertes, plus de signal
Remédiations sûres & auditables — Contrôles, rollbacks, logs
Disponible 24/7 — Réduit MTTR et charge on-call

Linux · Nginx · PostgreSQL · MySQL · Fail2ban · systemd

NOC/SOC AUTONOME
POUR INFRASTRUCTURES LINUX/WEB

Surveillance 24/7. Détection intelligente. Remédiation contrôlée.

Nginx • SSH • CPU/RAM/IO • Postgres/MySQL • Réseau • Système

AGENT LÉGER

Installé en 2 minutes

- Collecte & corrélation locale
- Faible empreinte
- File d'attente résiliente

Linux Docker ~ 30MB RAM

Logs & Métriques

TLS sécurisé

BACKEND INTELLIGENT

Corrélation • Détection d'anomalies • Automatisation

- **Détection IA** — Behavior & baselines
- **Scoring de Risque** — Priorisation
- **Remédiations** — Playbooks
- **Apprentissage** — Continu

Alertes & Actions

Canaux

ACTIONS CONTRÔLÉES

Automatiser en toute sécurité

- Redémarrer un service
- Bloquer une IP (fail2ban)
- Rotation de logs
- Basculer un backend

Dry-run • Validation • Rollback

TABLEAU DE BORD

Vue NOC/SOC en temps réel

12	3	99.98%
SERVEURS En ligne	ALERTES Critiques	DISPONIBILITÉ 24h

1.2s MTTR (moy. 24h)

SANTÉ INFRASTRUCTURE

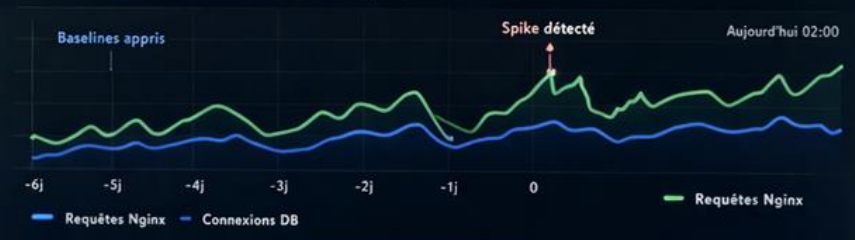
(moy. 5 min)

CPU	23%
RAM	45%
IO Wait	2%
Réseau	18 Mbps

ALERTES RÉCENTES

HEURE	HÔTE	SOURCE	ALERTE	RISQUE	STATUT
10:42:11	web-01	Nginx	↑ 5xx erreurs	Élevé	Résolue
10:37:55	db-01	PostgreSQL	Connexions anormales	Moyen	En cours
10:22:18	app-02	Système	Charge CPU > 90%	Élevé	Résolue
10:15:03	web-02	SSH	Bruteforce détecté	Critique	Bloquée

DÉTECTION IA – ANOMALIES (7 derniers jours)



PLAYBOOK EXÉCUTÉ

#PB-SSH-BRUTEFORCE — Succès

10:15:03 • web-02

- Détection : 12 échecs SSH / 1 min
- Action : IP 203.0.113.45 bloquée
- Règle fail2ban appliquée
- Notification envoyée

Durée : 4.2s — Voir le détail

DÉPLOIEMENT & PRICING

SELF-HOSTED

Votre infra. Vos données.

Licence simple
Mises à jour incl.

MANAGÉ

Clé en main 24/7

Hébergement
+ Support

POUR QUI ?

Hébergeurs • PME • MSP
E-commerce • Plateformes web

POURQUOI ÇA MARCHE ?

Automatisation utile.
Pas juste des alertes.

VIDE DU MARCHÉ

Plus simple que le SIEM.
Plus puissant que fail2ban.

TRÈS MONÉTISABLE

Self-hosted + Managé
Upsell MSP

8) NOC/SOC autonome pour infrastructures Linux/web

Idée : un agent + backend qui surveille logs Nginx, SSH, CPU/RAM/IO, Postgres/MySQL, anomalies réseau, floods, changements système, comportements suspects, et applique des remédiations contrôlées.

Pourquoi c'est bankable : les équipes manquent de temps, de compétences et de personnel ; elles veulent de l'automatisation utile, pas juste des alertes. Les besoins les plus cités dans les compétences sécurité restent data/cloud/network security, alors que la disponibilité des talents reste un frein. Fortinet +2

Le trou du marché : entre fail2ban artisanal et solutions SIEM/SOC hors de prix, il y a un vrai vide.

Clients : hébergeurs, PME, MSP, e-commerce, plateformes web à petit staff infra.

Très monétisable : version self-hosted + version managée.

9) “Modernisation factory” pour applications legacy

Idée : une usine logicielle qui prend une vieille appli Django/PHP/Java/.NET/Node et fournit : audit, cartographie, tests de non-régression, sécurité, conteneurisation, migration DB, observabilité, découpage progressif.

Pourquoi c’est bankable : les entreprises doivent moderniser sans réécrire. L’IT spending continue d’augmenter, mais le talent reste rare, ce qui favorise les plateformes qui accélèrent la remise à niveau des systèmes existants. gartner.com +1

Le trou du marché : trop de cabinets vendent du conseil, pas assez livrent une vraie chaîne industrialisée semi-automatique.

Clients : ETI, éditeurs historiques, administrations, industrie.

Angle fort : IA + analyseur statique + générateur de patchs + benchmark avant/après.

10) Infrastructure compliance-as-code pour PME européennes

Idée : un produit qui transforme sécurité/configuration/hébergement en contrôles concrets : backups testés, rétention, chiffrement, journaux, droits, segmentation, politiques, preuve d'exécution, export audit.

Pourquoi c'est bankable : la demande pour des plateformes cloud sectorielles et orientées résultats métier progresse, et la conformité reste un domaine douloureux parce que trop manuel et trop coûteux. gartner.com +2

Le trou du marché : les PME veulent être "suffisamment conformes" sans acheter une usine à gaz.

Clients : santé légère, RH, SaaS B2B, legaltech, agences manipulant données clients.

Très bon angle : "compliance evidence engine" branché à serveurs, DB, stockage et CI/CD.

Mon classement brut par potentiel business

Si je devais te donner les 5 plus prometteurs en création de valeur, je mettrais :

1. Gouvernance du code IA / agents IA
2. Observabilité low-cost open standard
3. FinOps cloud + IA + SaaS
4. Secure-by-design pour PME
5. DB Doctor universel

Pourquoi eux ? Parce qu'ils cumulent quatre qualités rares :
demande mondiale, douleur immédiate, budget déjà ouvert, et offre encore imparfaite. Cette conclusion est une **inférence stratégique** à partir de la hausse des dépenses IT/cloud, de l'expansion du FinOps, de la montée de la platform engineering, du poids de l'IA dans le code, et du décalage persistant entre adoption et maîtrise opérationnelle. gartner.com +5

Là où je pense que les “places vides” sont les plus réelles

Les vraies places vides ne sont pas dans le “faire encore un outil de plus”. Elles sont ici :

- rendre enterprise-grade quelque chose d’enfin accessible aux PME
- remplacer du service humain coûteux par de l’automatisation crédible
- prendre 5 outils compliqués et en faire 1 produit simple
- supprimer le lock-in vendeur
- mettre l’IA au service d’un métier infra/sécu/DB précis, pas en mode gadget

MON AVIS POUR 2026-2027

- Compte tenu de nos profils respectifs :
  - Nous crédibles sur 4 axes

- DB Doctor universel
- NOC/SOC autonome Linux + Nginx + DB
- Secure-by-design platform pour PME
- FinOps/Observability optimizer

Parce que ce sont des sujets très techniques, à forte barrière d'entrée, où une vraie expérience systèmes/serveurs/DB fait la différence. Et ce sont aussi des domaines où l'IA peut t'aider à construire un produit ambitieux plus vite que des équipes classiques.

Le meilleur projet n'est pas forcément le plus "sexy". C'est celui où :
la douleur est récurrente, le ROI est démontrable, et le client peut payer en abonnement mensuel.

PROJETS SECURITE

Ce qui est bankable pour nous

Les meilleurs axes sont :

1. NetGuard / NOC-SOC autonome pour Linux, Nginx, SSH, DB
2. Secrets & config exposure guardian
3. Crypto/RSA/PQC inventory + migration advisor
4. Supply-chain / dependency risk control pour PME
5. Secure-by-design platform pour PME techniques

Ce qui l'est beaucoup moins

Je n'irais **pas** en priorité sur :

- un antivirus classique
- un EDR "full endpoint enterprise"
- un nouveau chiffrement "révolutionnaire" sans standardisation
- un produit purement "RSA plus fort"
- un SIEM généraliste géant

1 NETGUARD

1) NetGuard : oui, franchement bankable

Pourquoi j'y crois

Entre :

- le petit script artisanal type fail2ban,
- les quelques règles nftables faites maison,
- et les plateformes SOC/SIEM hors de prix,

il y a un **vide énorme**.

Les PME, hébergeurs modestes, infogérances, e-commerces, SaaS, agences, n'ont ni les moyens ni les équipes pour opérer un vrai SOC. En même temps, elles ont des serveurs Linux, Nginx, SSH, DB, logs web, pics de connexions, scans, brute force, floods, erreurs de config, clés/API mal gérées. CISA insiste justement sur le fait que les petites structures sont exposées mais manquent d'outils et d'organisation adaptés. cisa.gov +2

Le bon positionnement

Pas "encore un firewall".

Pas "encore un SIEM".

“Autonomous Security Operations for Linux/Web infra”

Concrètement :

- agent léger Linux
- collecte logs Nginx/SSH/systemd/Postgres/MySQL
- détection : brute force, scan, anomalie trafic, erreur 5xx anormale, exfil probable, secrets exposés dans conf
- actions contrôlées : ban IP, ban subnet, rate limit, escalade, kill process suspect, alerte Telegram/Slack/mail
- tableau de bord web propre
- historique, preuves, score de confiance
- mode simulation avant mode blocage

Pourquoi c’est vendable

Parce que tu vends :

- du **temps gagné**
- du **risque évité**
- de la **simplicité**
- une **alternative réaliste** aux outils enterprise

Mon avis brutal

C'est probablement le projet sécurité n°1 pour nous.

Tu as déjà la culture Linux/Nginx/réseau/DB. Et là, l'IA peut aider sur :

- classification d'événements
- corrélation
- explication des alertes
- suggestion de remédiation
- génération de règles

2 Secrets & config exposure guardian

2) Secrets & config exposure guardian : très bankable

Ça, je pense que c'est **énorme** et sous-estimé.

Le vrai problème

Les équipes exposent :

- clés API
- tokens
- mots de passe dans `.env`
- confs Nginx/Django/Node mal fermées
- buckets mal configurés
- variables sensibles dans CI/CD
- dumps DB en clair
- certificats mal suivis
- permissions trop larges

Et en pratique, beaucoup de boîtes ne veulent pas acheter une usine à gaz enterprise pour ça.

OWASP 2025 place toujours très haut la **Security Misconfiguration** et les **Cryptographic Failures**, ce qui confirme que les problèmes les plus fréquents sont encore souvent des erreurs concrètes d'implémentation et de configuration.

Le bon produit

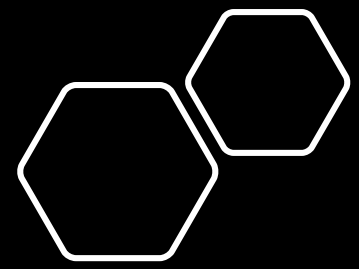
Pas juste un scanner Git.

Mais une plateforme qui vérifie :

- dépôts
- serveurs
- fichiers `.env`
- Docker/K8s manifests
- CI/CD
- reverse proxies
- permissions de fichiers
- certificats / expiration / algorithmes
- présence de secrets dans logs ou backups

Avec :

- scoring
- alertes
- auto-remediation guidée
- rapport auditable
- mode multi-tenant MSP



3 Crypto/RSA/PQC inventory + migration advisor

3) Crypto/RSA/PQC inventory + migration advisor

Là il faut être très honnête :

faire une "nouvelle crypto" = non

faire un produit de migration et d'inventaire crypto = oui

Les organisations commencent sérieusement à préparer la transition post-quantique. Gartner dit clairement que la cryptographie post-quantique pousse les organisations à identifier, gérer et remplacer les méthodes de chiffrement traditionnelles, avec priorité à la crypto-agilité. IBM et Deloitte tiennent le même discours : il faut inventorier les actifs cryptographiques et préparer la migration dès maintenant, car c'est un chantier pluriannuel. gartner.com +4

Là où le business existe

Pas dans "on invente un RSA du futur".

Mais dans :

- découverte des usages crypto dans le SI
- cartographie des certificats, TLS, SSH, JWT, libs crypto, signatures
- score de dette crypto
- détection des algorithmes faibles/legacy
- aide à la migration PQC/crypto-agile
- tests d'impact applicatif

Le bon slogan

“Know where your cryptography lives before you migrate it.”

Pourquoi c’est crédible pour nous

Parce que c’est un sujet d’architecture, d’inventaire, d’analyse, d’automatisation, pas de recherche académique pure.

Mon avis

Bankable en B2B, surtout si on le pense comme un **advisor technique** et pas comme un “nouvel algo miracle”.

4) Supply-chain dependency risk control

4) Supply-chain / dependency risk control

OWASP 2025 a mis les **Software Supply Chain Failures** dans le Top 3, ce qui est très significatif. owasp.org +1

Le problème réel

Toutes les équipes dépendent de :

- PyPI
- npm
- images Docker
- GitHub Actions
- libs transitive
- artefacts build
- pipelines CI/CD

Mais la plupart des outils :

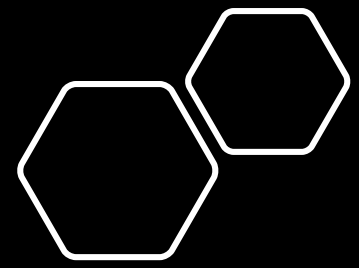
- spamment de faux positifs
- noient l'utilisateur
- ne donnent pas de décision claire

Le bon angle pour nous

Ne pas faire "encore un scanner CVE".

Faire :

- scoring de risque exploitable
- dépendances réellement chargées en prod
- priorité business
- blocage intelligent en CI/CD
- explication claire du risque
- vue par stack : Django, Python, Node, containers



Mon avis

Oui, mais plus concurrentiel.

Il faut un angle fort, par exemple :

- ultra-spécialisation Python/Django
- ou orientation PME/scale-up
- ou couplage supply-chain + runtime evidence

5) Secure-by-design platform pour PME

5) Secure-by-design platform pour PME

CISA pousse explicitement le “Secure by Design”, et il y a une vraie demande pour des solutions qui rendent les bonnes pratiques réellement applicables, pas seulement documentées. cisa.gov +2

Ce que ça deviendrait

Une plateforme qui centralise :

- audit config serveur
- durcissement Linux
- MFA / IAM minimum
- patch visibility
- backup verification
- secrets hygiene
- surface d’exposition
- score de posture
- preuves pour audit client

Pourquoi c’est fort

Parce que les petites et moyennes structures veulent être :

- plus sûres
- plus crédibles
- plus conformes

  sans recruter un RSSI + un SOC + un consultant cloud + un expert IAM.

MARCHES PEU PORTEUR

Là où il est déconseille franchement d’aller

- **A) Antivirus classique**
- **B) EDR complet**
- **C) “Nouveau RSA” ou nouvelle crypto propriétaire**
- **D) SIEM généraliste**

Mon classement honnête pour nous, en 2026

Top 1 — NetGuard

Le plus naturel pour toi, le plus différenciable, le plus vendable en mode B2B récurrent.

Top 2 — Secrets / Config Exposure Guardian

Très concret, très monétisable, plus simple à livrer en MVP.

Top 3 — Crypto Inventory / PQC Migration Advisor

Très bon angle premium, plus stratégique, plus “haut de gamme”.

Top 4 — Secure-by-Design Platform PME

Excellent si tu veux une plateforme plus large.

Top 5 — Supply-chain Security for Python/Web stacks

Bon marché, mais plus concurrentiel.