

RAPPORT D'AUDIT EXÉCUTIF & CONFORMITÉ CRA / PQC

Cible auditée : FinTech-Pay-API (D:\aegis-ast\sample_target_repo) | Date : 2026-10-25 00:46 UTC | Moteur : 100% Déterministe Local (Zéro LLM)
Tatouage Légal Licence : CERTIFICAT B2B ENTERPRISE | Titulaire : FinTech SAS (SIREN 888999000) | Facture : INV-2026-001 | Postes : UNLIMITED

AEGIS TRUST SCORE	NOTE GLOBAL E	DETTE IA ANNUELLE	SURCÔÛT CLOUD FINOPS	STATUT RÉGLEMENTAIRE CRA
31.4 / 100	E	24,000.00 € / an	5,040.00 € / an	NON-CONFORME CRITIQUE

1. SYNTHÈSE FINANCIÈRE EXÉCUTIVE (IMPACT EN EUROS €)

Basé sur un TJM ingénieur de référence de 550 €/jour (68.75 €/h), l'analyse mathématique de 6 fichiers (196 lignes de code effectives, 10 fonctions) met en évidence les coûts cachés suivants :

Indicateur Financier & Opérationnel	Volume Détecté	Impact Mensuel	Impact Annuel (€)
Dettes de Maintenance IA (Clones AST, Complexité, Erreurs masquées)	3 clones AST, 5 try/catch muets	29.1 h (2,000.00 €)	24,000.00 € / an
Gaspillage Serveur / Cloud FinOps (Boucles O(N²) & Requêtes N+1)	1 boucles O(N²) (1 avec I/O DB)	420.00 € / mois	5,040.00 € / an
Exposition Réglementaire & Incident Cyber Resilience Act (UE 2024/2847)	5 bloqueurs critiques CRA	Risque d'audit / incident	188,000.00 €
Coût du Sprint de Remédiation Ciblée (Prompts AEGIS-AST inclus)	30 correctifs automatisés	39.4 heures ingé.	Investissement : 2,708.75 € (ROI x10.7)

2. ÉTAT DE CONFORMITÉ CYBER RESILIENCE ACT (SEPTEMBRE 2026 / DÉCEMBRE 2027)

Le Règlement Européen **Cyber Resilience Act (UE 2024/2847)** impose dès le **11 septembre 2026** l'obligation de notifier sous 24h toute vulnérabilité activement exploitée à l'ENISA/CSIRT, et dès le **11 décembre 2027** la fourniture d'un SBOM/CBOM machine-readable (CycloneDX 1.6), l'absence de failles connues à la mise sur le marché et l'état de l'art cryptographique.

Domaine d'Audit AEGIS-AST	Score / 100	Constat Technique Déterministe
1. Entropie IA & Clones AST (Weisfeiler-Lehman)	16.5 / 100	3 clones structurels AST, 5 blocs d'erreurs étouffés, 7 zombie imports, complexité cognitive moy. 7.0.
2. Bouclier Supply-Chain & Anti-Slopsquatting	20.0 / 100	2 packages hallucinés / slopsquatting (404 PyPI/npm), 1 dépendances fantômes, 14 CVE OSV.dev.
3. Conformité CRA, Secrets Shannon & PQC (NIST)	34.0 / 100	1 secrets à haute entropie (>4.2 bits/car.), 2 primitives cassées (MD5/SHA1), 2 primitives vulnérables à Shor (RSA/ECDSA).
4. Efficience FinOps & Complexité Algorithmique	80.0 / 100	1 boucles imbriquées O(N²) détectées dont 1 effectuant des requêtes DB/Réseau synchrones.

3. ANALYSE MATHÉMATIQUE D'ENTROPIE IA (CLONES AST & MASQUAGE D'ERREURS)

Fonction A (Fichier & Lignes)	Fonction B (Fichier & Lignes)	Similarité WL / SimHash	Empreinte AST Canonique
evaluate_cross_border_surcharge... kyc_compliance.py:8-41	compute_dynamic_merchant_fees... payment_gateway.py:15-48	100.0% Hash: f4c6e94c6f...	FunctionDef -> ARG -> ARG -> ARG -> ASSIGN -> VAR -> LIT_float -> ASSIGN ->...
evaluate_cross_border_surcharge... kyc_compliance.py:8-41	calculate_clearing_commission... sepa_settlement.py:8-41	100.0% Hash: f4c6e94c6f...	FunctionDef -> ARG -> ARG -> ARG -> ASSIGN -> VAR -> LIT_float -> ASSIGN ->...
compute_dynamic_merchant_fees... payment_gateway.py:15-48	calculate_clearing_commission... sepa_settlement.py:8-41	100.0% Hash: f4c6e94c6f...	FunctionDef -> ARG -> ARG -> ARG -> ASSIGN -> VAR -> LIT_float -> ASSIGN ->...

Blocs de Masquage Silencieux d'Erreurs ('AI Error Masking') :

Fichier & Ligne	Langage	Anti-Pattern Détecté	Diagnostic & Impact CRA
frontend_checkout.ts:8	TypeScript/JavaScript	catch (e) { /* empty */ }	Bloc catch vide étouffant silencieusement toutes les exceptions JavaScript/TypeScript.
frontend_checkout.ts:15	TypeScript/JavaScript	catch (e) { /* empty */ }	Bloc catch vide étouffant silencieusement toutes les exceptions JavaScript/TypeScript.
kyc_compliance.py:49	Python	except Bare Except (All Exceptions): pass...	Masquage silencieux total d'exception (Bare Except (All Exceptions)) via 'pass'. Les erreurs d'exécution...
payment_gateway.py:61	Python	except Exception: pass	Masquage silencieux total d'exception (Exception) via 'pass'. Les erreurs d'exécution sont étouffées...
sepa_settlement.py:55	Python	except Exception: return None	Retour silencieux (None) sur exception (Exception) sans journalisation structurée ni propagation d'e...

4. BOUCLIER SUPPLY-CHAIN : SLOPSQUATTING, PHANTOM DEPS & CVE (OSV.DEV)

Package / Composant	Écosystème	Type d'Alerte Supply-Chain	Détail & Preuve
py-quantum-sepa-validator	PyPI	SLOPSQUATTING / HALLUCINATION IA (4...)	ALERTE CRITIQUE SLOPSQUATTING : Le package 'py-quantum-sepa-validator' (PyPI) N'EXISTE PAS sur le re...
stripe-ai-fraud-shield-sdk	npm	SLOPSQUATTING / HALLUCINATION IA (4...)	ALERTE CRITIQUE SLOPSQUATTING : Le package 'stripe-ai-fraud-shield-sdk' (npm) N'EXISTE PAS sur le re...
fastapi==0.109.0	PyPI	CVE : CVE-2024-24762	FastAPI is a web framework for building APIs with Python 3.8+ based on standard Python type hints. W...
pyyaml==5.3.1	PyPI	CVE : CVE-2020-14343	Improper Input Validation in PyYAML
cryptography==42.0.5	PyPI	CVE : GHSA-537c-gmf6-5ccf	Vulnerable OpenSSL included in cryptography wheels
cryptography==42.0.5	PyPI	CVE : CVE-2024-12797	Vulnerable OpenSSL included in cryptography wheels
cryptography==42.0.5	PyPI	CVE : GHSA-h4gh-qq45-vh27	pyca/cryptography has a vulnerable OpenSSL included in cryptography wheels
cryptography==42.0.5	PyPI	CVE : CVE-2026-69249	python-cryptography: Duplicate self-signed intermediates can cause exponential path-building
cryptography==42.0.5	PyPI	CVE : CVE-2026-34073	cryptography has incomplete DNS name constraint enforcement on peer names
cryptography==42.0.5	PyPI	CVE : CVE-2026-26007	cryptography Vulnerable to a Subgroup Attack Due to Missing Subgroup Validation for SECT Curves

axios==1.6.7	npm	CVE : CVE-2026-44494	axios Vulnerable to Full Man-in-the-Middle via Prototype Pollution Gadget in `config.proxy`
axios==1.6.7	npm	CVE : CVE-2026-44495	axios Vulnerable to Credential Theft and Response Hijacking via Prototype Pollution Gadget in Config...
axios==1.6.7	npm	CVE : CVE-2025-62718	Axios has a NO_PROXY Hostname Normalization Bypass that Leads to SSRF
axios==1.6.7	npm	CVE : CVE-2026-42044	Axios: Invisible JSON Response Tampering via Prototype Pollution Gadget in `parseReviver`
axios==1.6.7	npm	CVE : CVE-2026-67313	Axios: Excessive recursion in formDataToJSON can cause denial of service

5. CERTIFICAT D'INVENTAIRE CRYPTOGRAPHIQUE (CBOM POST-QUANTIQUE & SECRETS)

Emplacement	Type de Secret Détecté	Entropie Shannon H(X)	Aperçu Masqué
payment_gateway.py:12	Stripe Live Secret Key	5.0433 bits/car. (Seuil 4.2)	sk_liv...1t0U

Primitive	Classification NIST / ANSSI	Emplacement	Plan de Migration Post-Quantique (FIPS 203/204)
AES-256-GCM	SÛR / POST-QUANTUM READY	crypto_vault.py:6	Conforme ANSSI & NIST Post-Quantique (résistant à l'algorithme de Grover avec clé 256 bits).
RSA-1024/2048	VULNÉRABLE AU QUANTIQUE	crypto_vault.py:15	Vulnérable à l'algorithme de Shor sur calculateur quantique (Store Now, Decrypt Later). Planifier la migration...
ECDSA / Secp256k1 / ...	VULNÉRABLE AU QUANTIQUE	crypto_vault.py:21	Courbes elliptiques classiques vulnérables à l'algorithme de Shor d'ici 2030-2035. Préparer l'agilité cryptogr...
SHA-256/512	SÛR / POST-QUANTUM READY	crypto_vault.py:30	Hachage cryptographique robuste résistant aux attaques quantiques de Grover.
AES-256-GCM	SÛR / POST-QUANTUM READY	crypto_vault.py:31	Conforme ANSSI & NIST Post-Quantique (résistant à l'algorithme de Grover avec clé 256 bits).
AES-256-GCM	SÛR / POST-QUANTUM READY	crypto_vault.py:32	Conforme ANSSI & NIST Post-Quantique (résistant à l'algorithme de Grover avec clé 256 bits).
MD5	INTERDIT / CASSÉ	payment_gateway.py:55	Collisions triviales (CWE-328). Remplacer immédiatement par SHA-256 ou SHA3-256.
SHA1	INTERDIT / CASSÉ	sepa_settlement.py:48	Cassé par attaque SHattered (CWE-328). Interdit par l'ANSSI et le NIST. Migrer vers SHA-256/SHA-512.

6. TOP 10 DES URGENCES DE REFACTORISATION IA (PLAN D'ACTION)

ID	Sévérité	Catégorie	Action Chirurgicale Prioritaire
SURG-CLONE-01	HIGH	Déduplication AST (Weisfe...	Unifier le clone structurel 'evaluate_cross_border_surcharge... Cible : kyc_compliance.py:8-41 & payment_gateway.py:15-48
SURG-CLONE-02	HIGH	Déduplication AST (Weisfe...	Unifier le clone structurel 'evaluate_cross_border_surcharge... Cible : kyc_compliance.py:8-41 & sepa_settlement.py:8-41
SURG-CLONE-03	HIGH	Déduplication AST (Weisfe...	Unifier le clone structurel 'compute_dynamic_merchant_fee' &... Cible : payment_gateway.py:15-48 & sepa_settlement.py:8-41
SURG-ERR-01	CRITICAL	Correction AI Error Maski...	Supprimer le masquage silencieux 'catch (e) { /* empty */ }'... Cible : frontend_checkout.ts:8-8
SURG-ERR-02	CRITICAL	Correction AI Error Maski...	Supprimer le masquage silencieux 'catch (e) { /* empty */ }'... Cible : frontend_checkout.ts:15-15
SURG-ERR-03	CRITICAL	Correction AI Error Maski...	Supprimer le masquage silencieux 'except Bare Except (All Ex... Cible : kyc_compliance.py:49-50
SURG-ERR-04	CRITICAL	Correction AI Error Maski...	Supprimer le masquage silencieux 'except Exception: pass' da... Cible : payment_gateway.py:61-62
SURG-ERR-05	HIGH	Correction AI Error Maski...	Supprimer le masquage silencieux 'except Exception: return N... Cible : sepa_settlement.py:55-56
SURG-SLOP-01	CRITICAL	Urgence Anti-Slopsquattin...	Éliminer le package halluciné 'py-quantum-sepa-validator' (P... Cible : requirements.txt:5 / manifeste
SURG-SLOP-02	CRITICAL	Urgence Anti-Slopsquattin...	Éliminer le package halluciné 'stripe-ai-fraud-shield-sdk' (... Cible : package.json (dependencies) / manifeste

SURG-CVE-01	HIGH	Remédiation CVE (OSV.dev)	Corriger CVE-2024-24762 sur fastapi==0.109.0 Cible : requirements.txt:2
SURG-CVE-02	CRITICAL	Remédiation CVE (OSV.dev)	Corriger CVE-2020-14343 sur pyyaml==5.3.1 Cible : requirements.txt:4
SURG-CVE-03	HIGH	Remédiation CVE (OSV.dev)	Corriger GHSA-537c-gmf6-5ccf sur cryptography==42.0.5 Cible : requirements.txt:6
SURG-CVE-04	LOW	Remédiation CVE (OSV.dev)	Corriger CVE-2024-12797 sur cryptography==42.0.5 Cible : requirements.txt:6
SURG-CVE-05	MODERATE	Remédiation CVE (OSV.dev)	Corriger GHSA-h4gh-qq45-vh27 sur cryptography==42.0.5 Cible : requirements.txt:6