CALIALABS

CEREBRO ENGINEERING SERIES

RPT-2025-03

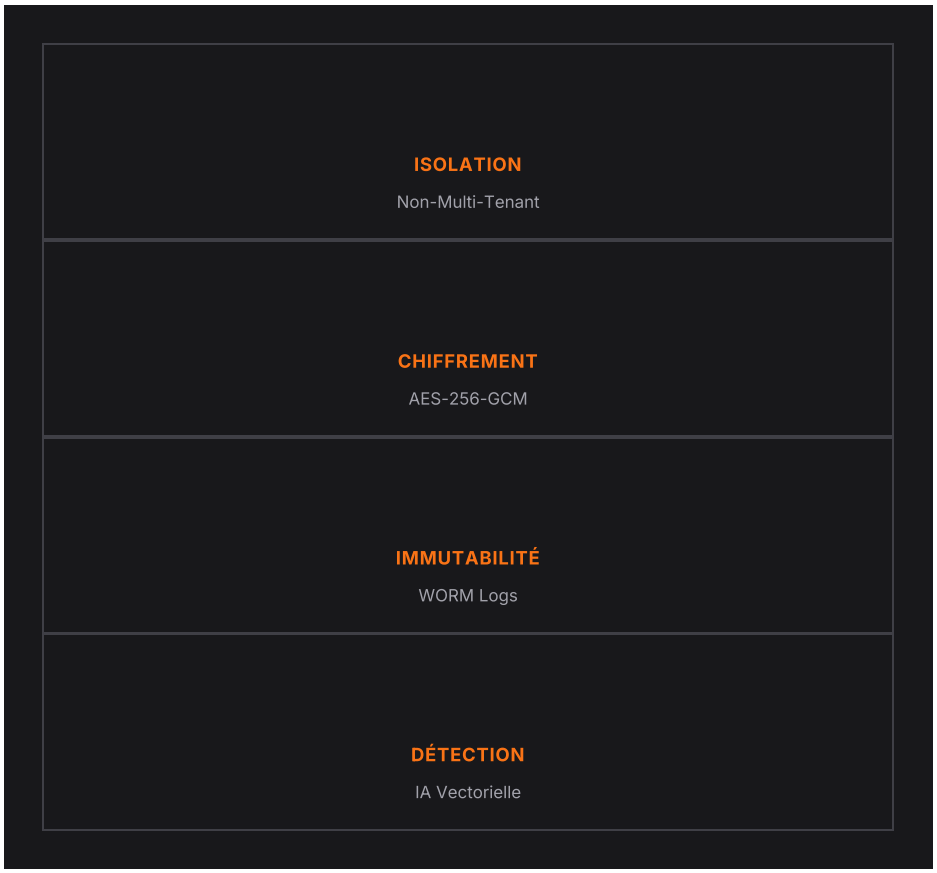
Novembre 2025

PUBLIC / TECHNIQUE

/// ARCHITECTURE

SÉCURISATION DES FLUX SMTP EN ENVIRONNEMENT HOSTILE

Standard Zero-Trust pour les communications financières critiques (Tier-1). Focus : Sécurité Offensive & Défensive.



1. CONTEXTE : L'ENVIRONNEMENT HOSTILE

Dans une banque de niveau Tier-1, les flux SMTP ne sont pas de simples messages, ce sont des vecteurs de données financières. L'environnement "hostile" désigne ici l'Internet public, où les communications transitent par des réseaux non-maîtrisés.

Le défi pour le CISO est double : assurer la **confidentialité absolue** (chiffrement) et l'**intégrité vérifiable** (audit) de chaque paquet.

2. ISOLEMENT : L'HÉRÉSIE DU MULTI-TENANT

> **⚠ Risque de Fuite Latérale**
>
> Dans une architecture mutualisée, une erreur de configuration IAM ou une faille hyperviseur peut exposer les données d'un client A à un client B (Cross-Tenant Leak).

2.2. Le Standard CEREBRO : Isolation Totale

→ **Instances SMTP réservées**: Aucun partage de file d'attente ou de CPU.

→ **Stockage cloisonné**: Bases de données isolées logiquement et physiquement.

→ **Segmentation réseau**: VPC dédié pour chaque institution.

> **Principe de Sécurité**
>
> Chaque tenant est considéré comme un périmètre de confiance hostile pour les autres.

3. CHIFFREMENT : DÉFENSE EN PROFONDEUR

3.1. Au Repos (At-Rest)

ALGORITHME

`AES-256-GCM (Galois/Counter Mode)`

Assure confidentialité + intégrité. Rotation automatique avant le seuil critique de 2^{32} opérations (NIST SP 800-38D).

3.2. En Transit

PROTOCOLE

`TLS 1.3 STRICT ONLY`

Interdiction des protocoles obsolètes. Élimination des ciphers faibles de TLS 1.2.

4. INTÉGRITÉ & IMMUTABILITÉ (WORM)

L'auditabilité ne se négocie pas. Pour satisfaire les contrôles ACPR, les journaux d'activité doivent être infalsifiables.

STOCKAGE

`WORM (Write Once, Read Many)`

Même un administrateur Root ne peut pas altérer une trace d'audit. Les logs deviennent preuve numérique recevable.

5. DÉTECTION : LA FIN DU REGEX

Les systèmes basés sur des expressions régulières sont obsolètes. CEREBRO utilise une **analyse sémantique vectorielle** : projection des emails dans un espace vectoriel dense, détection par "distance sémantique" plutôt que par mots-clés.

> **Résultat**
>
> Détection des menaces Zero-Day et compréhension du contexte (ex: distinction entre un envoi de RIB légitime et une exfiltration).

CONCLUSION

La sécurisation des flux SMTP en environnement hostile exige un changement de paradigme. L'architecture CEREBRO abandonne la confiance implicite pour une vérification cryptographique continue. En combinant isolation physique, chiffrement militaire et intelligence vectorielle, elle transforme le canal email en une forteresse informationnelle.