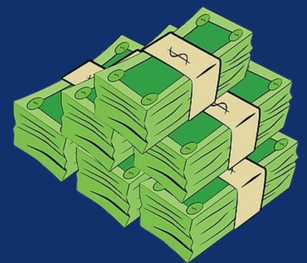
EUROBANK DIGITAL

Présenté par
VOUBOU KLETT GUEWEN(RSSI)



COMMENT EUROBANK DIGITAL PEUT-ELLE ASSURER SA CONFORMITÉ AUX RÉGLEMENTATIONS EUROPÉENNES TOUT EN RENFORÇANT SA RÉSILIENCE CYBER POUR SÉCURISER SON EXPANSION ET MAINTENIR LA CONFIANCE DE SES CLIENTS ?

1. CONTEXTE ET PERIMETRE

EuroBank Digital, fondée en 1999 et basée à Francfort, est un acteur majeur du secteur financier numérique européen. Avec 6 500 employés et un chiffre d'affaires de 2,2 milliards d'euros, notre croissance est rapide et nos objectifs stratégiques pour les cinq prochaines années sont ambitieux :

Ces objectifs s'accompagnent de contraintes significatives, notamment une forte dépendance au cloud, une surveillance rigoureuse de la Banque Centrale Européenne, et le traitement de données bancaires et biométriques extrêmement sensibles. Notre équipe IT/Cyber de 220 personnes et notre budget de 18 M€ en cybersécurité sont dédiés à la construction d'une stratégie SSI robuste pour naviguer dans cet environnement complexe.

2.UN CADRE REGLEMENTAIRE DANSE

EuroBank Digital opère dans un environnement réglementaire particulièrement strict. La conformité n'est pas seulement une obligation mais un point fort afin d’être crédible et de garder une confiance avec nos clients.

- **RGPD:** Protection des données personnelles, notamment bancaires et biométriques. Nécessité de prouver la capacité à répondre rapidement aux droits des clients (ex: droit à l'effacement).
- **DORA:** Renforcement de la résilience opérationnelle, encadrement des prestataires critiques (cloud) et tests réguliers de continuité d'activité.
- **NIS 2:** Classée entité essentielle, nous devons mettre en place des mesures strictes de gestion des risques et signaler tout incident majeur sous 24h.
- **AI Act & ISO 42001:** Encadrement de l'utilisation de l'IA en particulier pour les systèmes à haut risque comme la biométrie ou la détection de fraude.

3.Risques Majeurs pour EuroBank Digital

L'expansion numérique d'EuroBank Digital s'accompagne de risques accrus. Une identification claire de ces menaces est essentielle pour développer une stratégie de défense efficace.

- **Cyberattaques Externes :** Attaques DDoS, ransomwares (type LockBit), et campagnes de phishing ciblant nos clients sont des menaces persistantes.
- **Dépendance au Cloud :** Une défaillance chez un fournisseur cloud critique pourrait entraîner l'interruption des transactions bancaires à l'échelle européenne, affectant des millions de clients.
- **Risques Réglementaires :** Le non-respect des réglementations telles que le RGPD ou DORA peut entraîner des amendes de plusieurs millions d'euros, impactant directement notre rentabilité.
- **Risques Réputationnels :** Une fuite de données bancaires peut éroder la confiance des clients et entraîner une fuite massive de capitaux, menaçant la stabilité de la banque.

4.STRATEGIE

Court terme (0-6mois): La première phase de notre stratégie vise à consolider nos bases de sécurité et à obtenir des résultats rapides et mesurables. Ces actions sont cruciales pour établir une posture de sécurité solide.

1

Mise à jour de la PSSI
Alignement avec ISO 27001 et NIS 2 pour une gouvernance de sécurité moderne.

2

Améliorer des capacités de détection (ex: lecture des logs pour identifier une attaque DDoS en temps réel).

3

Plan de Gestion de Crise
Mise en place et test de scénarios concrets (ex: simulation d'indisponibilité totale du cloud pendant 48h).

4

Campagnes de Sensibilisation
Phishing simulé et formations ciblées pour les employés sur la protection des données clients.

Moyen terme (6-24mois): Cette période se concentre sur l'intégration de pratiques de sécurité avancées et la formalisation de notre engagement envers la conformité et la résilience.

Certification ISO 27001

Pour notre crédibilité auprès des régulateurs et partenaires.

Zero Trust Architecture

Authentification multi-facteurs biométriques, segmentation réseau, contrôle.

Sécurité Cloud

Audits indépendants et intégration de DORA.

Comité Éthique IA

Supervision des projets IA (détection de fraude) pour assurer transparence plus que clair

Long terme (24-32mois): La dernière phase de notre stratégie vise à consolider notre leadership en cybersécurité par l'innovation et une conformité préventive en anticipant les défis futurs.

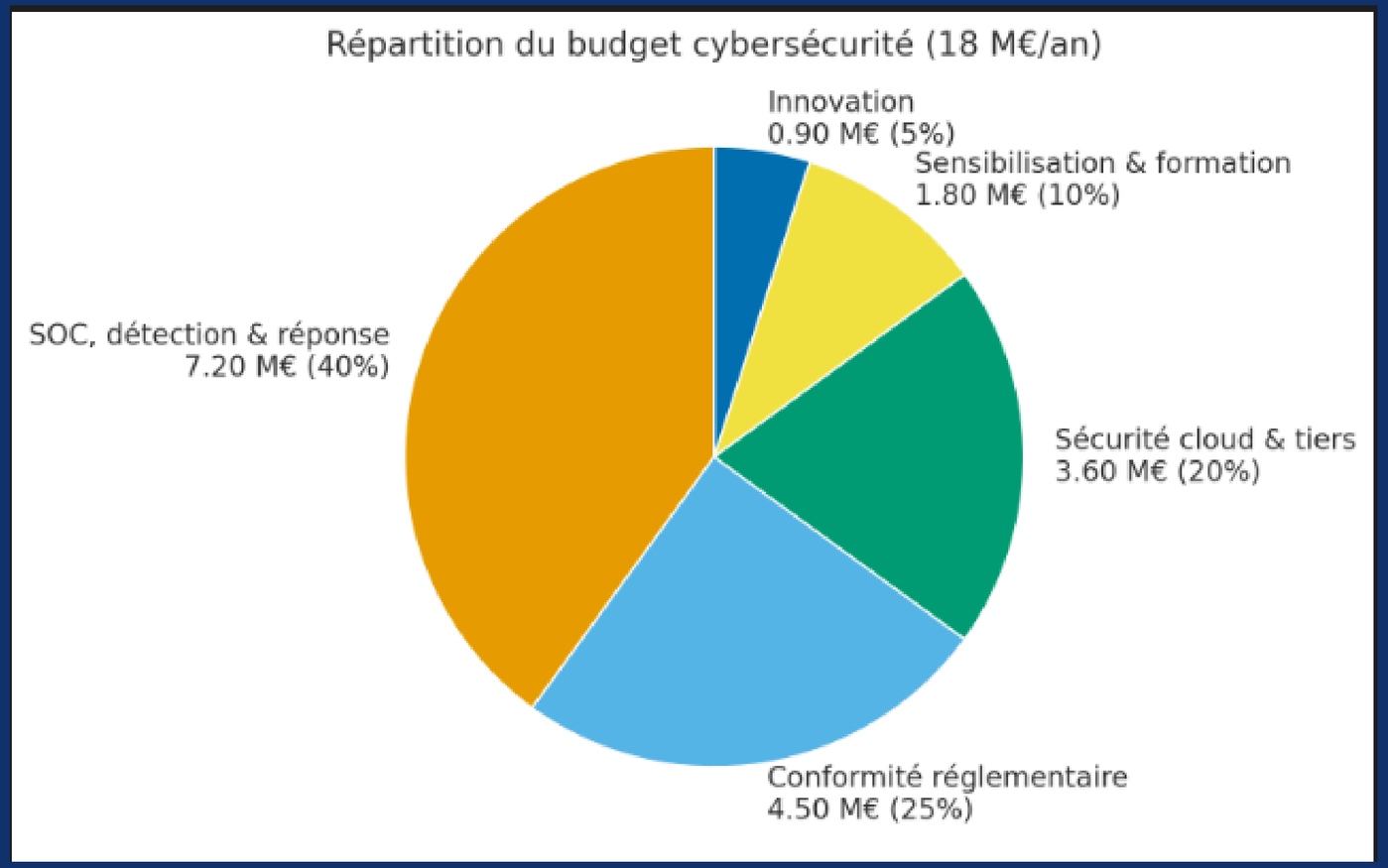
Programme de Bug Bounty Européen : Lancement d'un programme pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées.

Certification ISO 42001 : Obtenir cette certification pour assurer une gouvernance responsable et éthique de l'IA.

Conformité Cyber Resilience Act : Mise en conformité de tous les services numériques internes et externes pour garantir la sécurité dès la conception.

Intégration Green IT : Optimisation des data centers et réduction de l'empreinte carbone du cloud avec le Pacte Vert européen.

4.BUDGET ET ALLOCATION DES RESSOURCES


Répartition du budget cybersécurité (18 M€/an)
Innovation
0.90 M€ (5%)
Sensibilisation & formation
1.80 M€ (10%)
Sécurité cloud & tiers
3.60 M€ (20%)
Conformité réglementaire
4.50 M€ (25%)
SOC, détection & réponse
7.20 M€ (40%)

CONCLUSION:

La stratégie SSI présentée permettra à EuroBank Digital de transformer la cybersécurité d'une obligation réglementaire en un véritable avantage concurrentiel. Nous avons pour objectif:

- Respecter toutes les exigences réglementaires européennes (RGPD, NIS 2, DORA, CRA, AI Act).
- Renforcer notre résilience face aux cyberattaques.
- Sécuriser notre expansion européenne et nos innovations (crypto-actifs, IA).
- Maintenir la confiance des clients, des investisseurs et des régulateurs.

En adoptant cette approche proactive et intégrée, EuroBank Digital sera mieux positionnée pour prospérer dans un paysage numérique en constante évolution tout en garantissant sécurité et confiance pour tous nos stakeholders.

MERCI