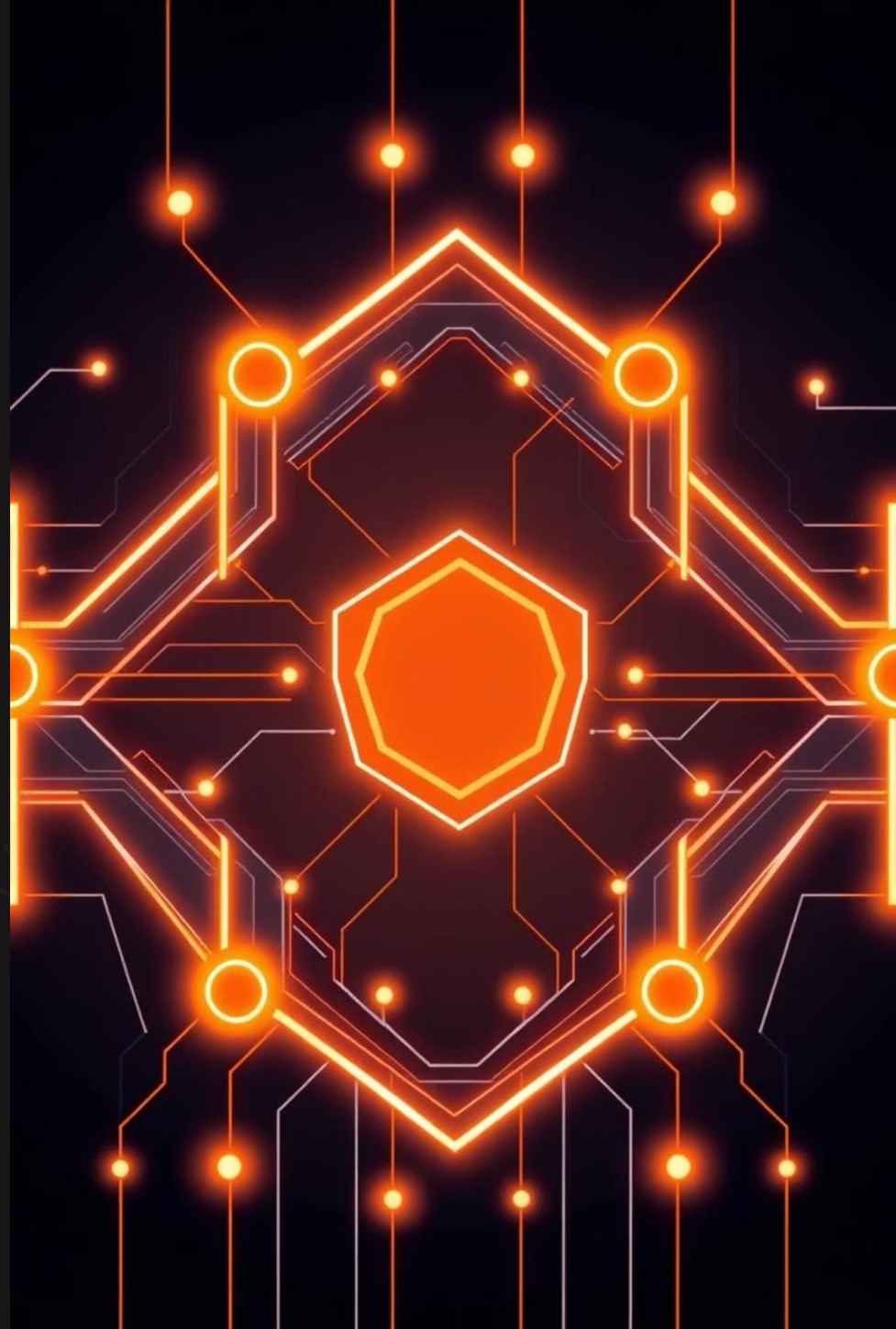
Sécurité et Cybersécurité des Réseaux Critiques

Directive NIS2 : Nouveaux enjeux pour les communications radio professionnelles

Danny Larbouillat
CISO/RSSI - SEE Telecom
CEO & Expert en Cybersécurité - ACOServices



Un Contexte de Menaces Croissantes

Les infrastructures critiques font face à une augmentation exponentielle des cyberattaques. La transformation numérique des systèmes radio vers l'IP expose de nouvelles vulnérabilités.

300%

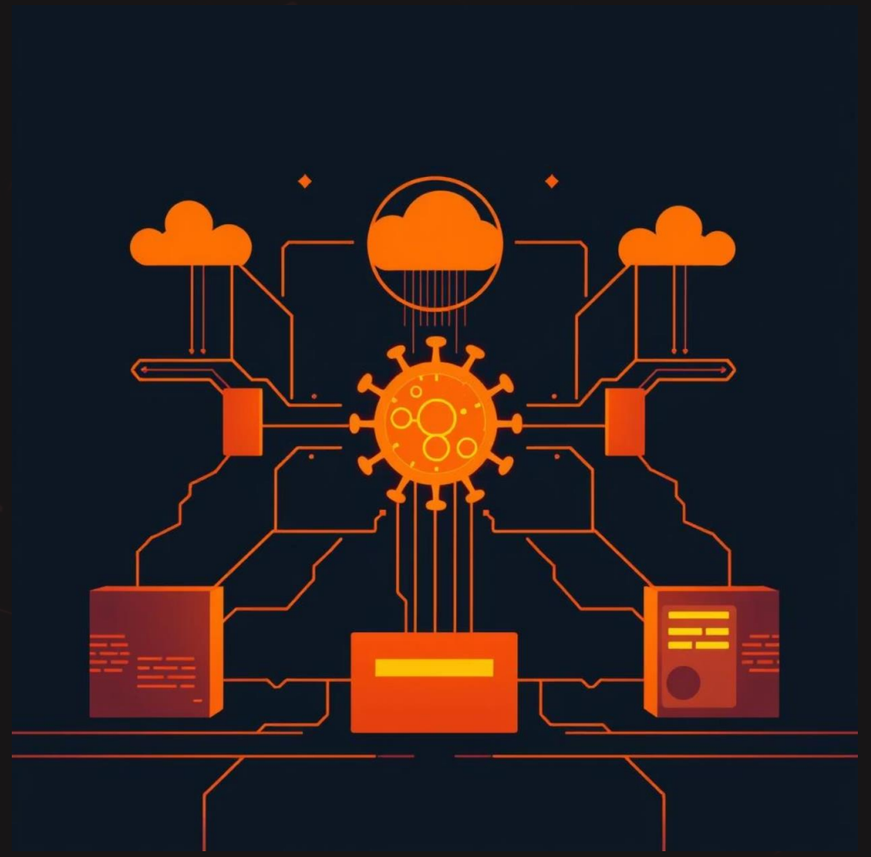
Hausse des incidents

Augmentation des cyberattaques contre les infrastructures en 3 ans

24h

Délai critique

Temps moyen de propagation d'une attaque sur réseau critique



Made with GAMMA

Qu'est-ce qu'un Réseau Critique ?

Les réseaux critiques sont les **systèmes de communication essentiels** au fonctionnement de la société et à la sécurité nationale.



Services d'Urgence

Réseaux PMR pour police, pompiers, SAMU - communications vitales en situation de crise



Infrastructures Énergétiques

Systèmes SCADA, réseaux OT/IT pour centrales et distribution électrique



Transport & Télécoms

Contrôle ferroviaire, aérien, maritime - connectivité essentielle aux citoyens

Made with GAMMA



Panorama des Menaces Actuelles

Menaces Étatiques

Espionnage, sabotage d'infrastructures stratégiques par des acteurs géopolitiques

Ransomware

Chiffrement et paralysie des systèmes critiques pour extorsion financière

Sabotage Interne

Menaces d'initiés, erreurs humaines, compromission des accès privilégiés

Made with GAMMA



Vulnérabilités Spécifiques aux Réseaux Critiques

Obsolescence Technologique

- Équipements radio anciens sans mises à jour
- Systèmes propriétaires difficiles à maintenir

Protocoles Non Sécurisés

- TETRA, Modbus sans chiffrement
- Communications en clair interceptables

Cloisonnement Insuffisant

- Convergence OT/IT mal maîtrisée
- Passerelles non sécurisées vers internet

Made with GAMMA

Directive NIS2 : Le Nouveau Cadre Européen



18

Secteurs Couverts

Énergie, transport, santé, télécoms, services numériques

10M€

Amendes Maximales

Ou 2% du CA annuel mondial pour les manquements

La Directive NIS2 est en vigueur **depuis le 18 octobre 2024**, renforçant drastiquement les obligations de

Made with GAMMA

Obligations Clés de la Directive NIS2

01

Gouvernance et Gestion des Risques

Direction générale responsable, politique de sécurité documentée, évaluation régulière, chaîne logistique

02

Mesures Techniques Obligatoires

Chiffrement, authentification multi-facteurs, segmentation réseau, sauvegarde

03

Signalement d'Incidents

Déclaration sous 24h des incidents importants (significatifs) aux autorités compétentes

04

Audits et Contrôles

Supervision régulière, tests de pénétration, certification de la conformité

Made with GAMMA

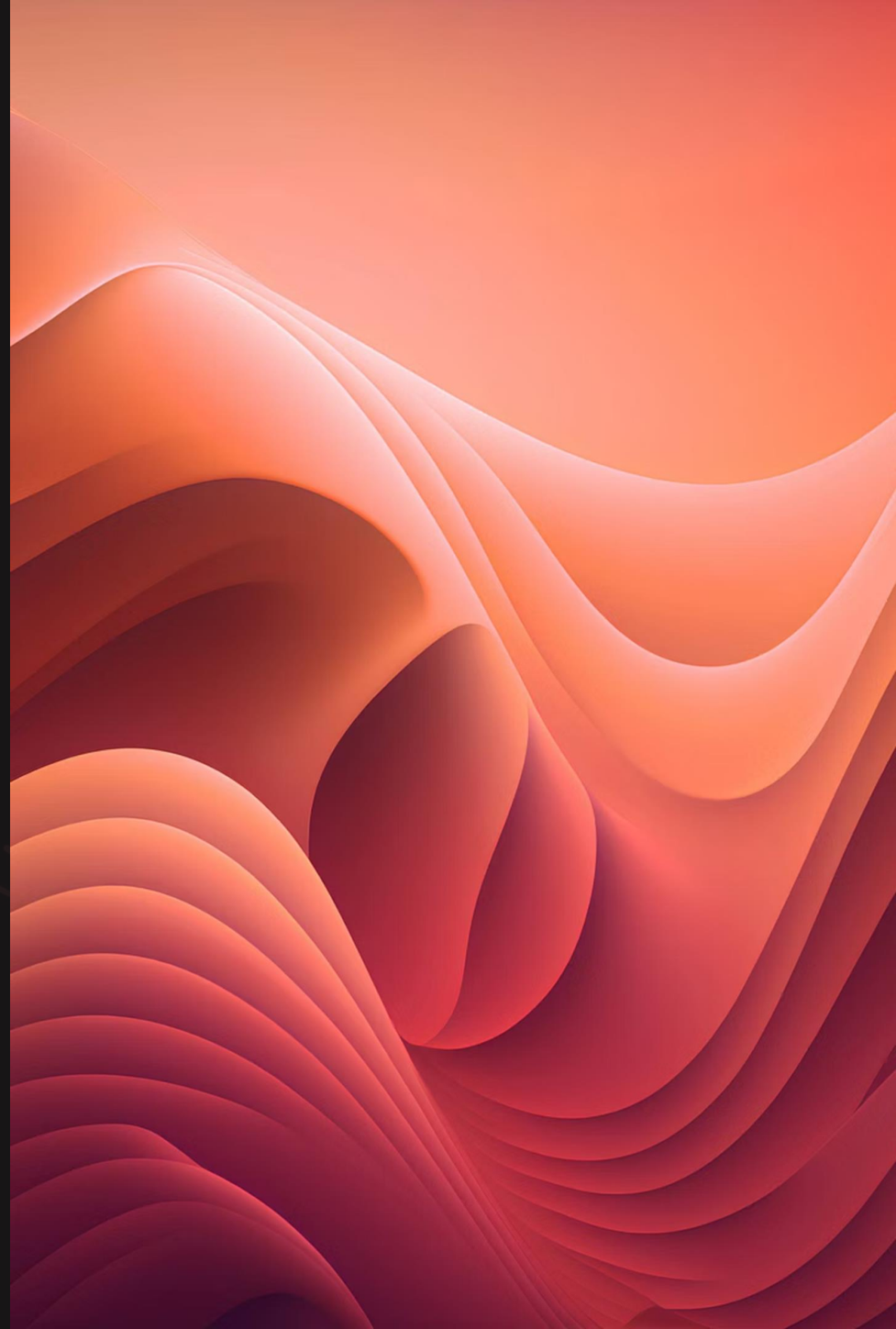
Logique et du bon sens

Pourquoi faire compliqué quand on peut faire simple !

Pourquoi faire simple quand on peut faire compliqué !

Pourquoi faire compliqué quand on peut faire encore plus compliqué !

Se conformer = gérer la complexité !



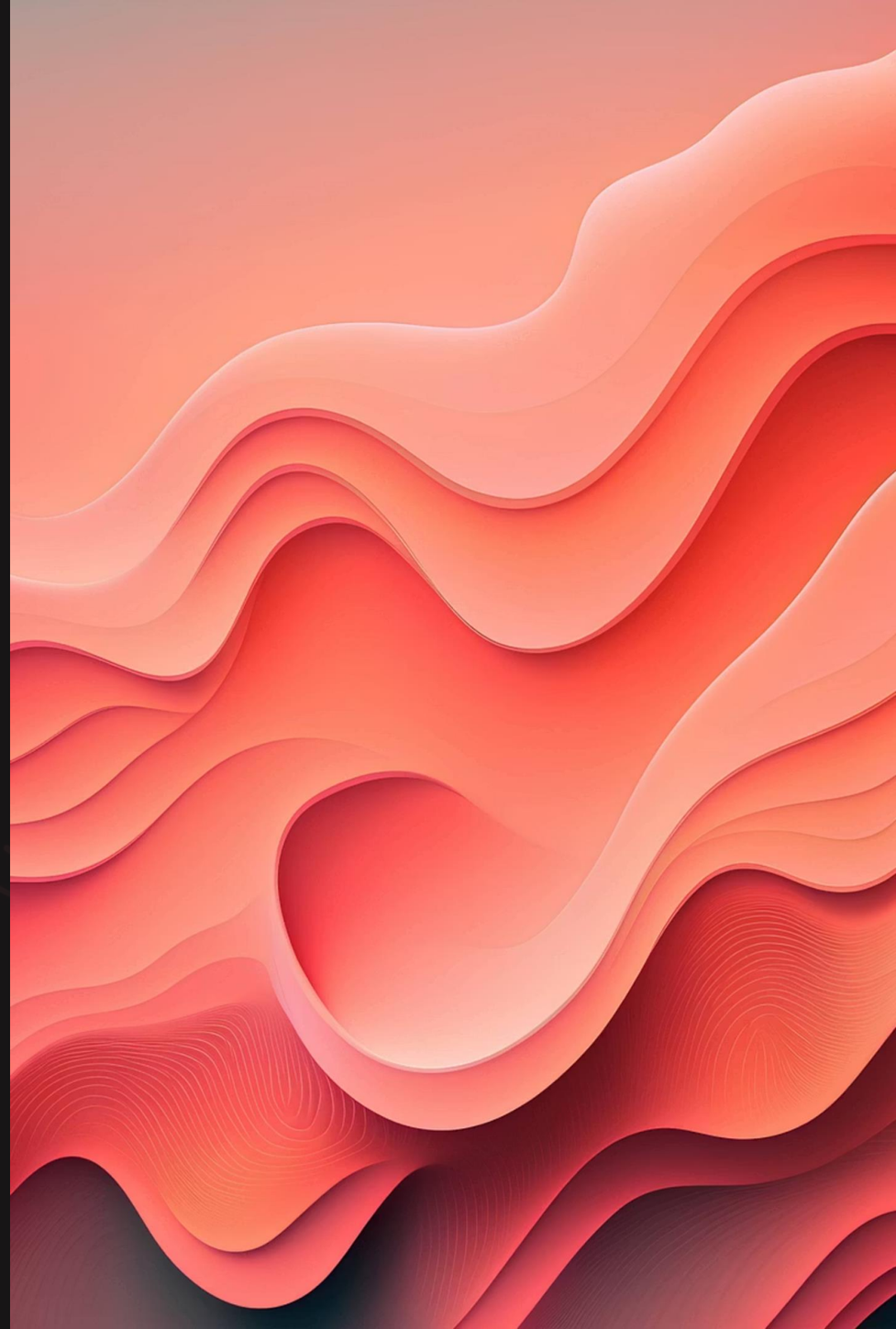
Logique et du bon sens

NIS2 - Article 21 §1

Les entités essentielles et importantes prennent les **mesures** techniques, opérationnelles et organisationnelles

appropriées et proportionnées

pour gérer les **risques** qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.



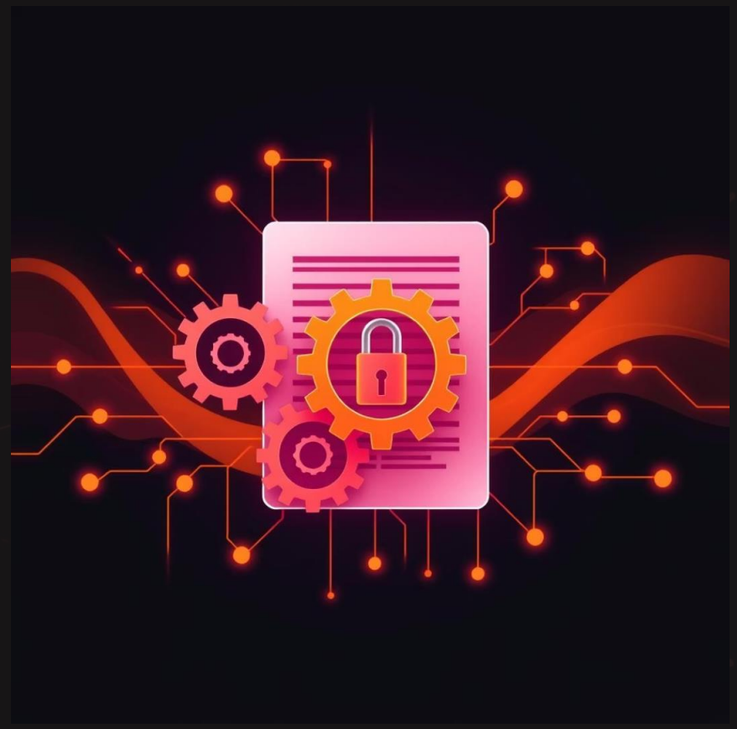
Mesures liées à la Directive NIS2 —> ... > 200



4 Mesures (J. Easterly)
(4 indicateurs)

98 % des menaces

Principe de précautionTolérance zéro



Entre 50 et 65 Mesures
18 indicateurs (100% NIS2)

> 99,..% des menaces

Conformité légale (Directive)Eviter les pénalités



> 200 mesures

> 99,99..% des menaces

Filtrer : Applicable ? Pertinente ? Réaliste ? Risque acceptable ?Principe de proportionnalité

Made with GAMMA

Recommandations Pratiques pour Réseaux PMR & 4G/5G

Audit de Sécurité

Évaluation complète des vulnérabilités radio, 4G/5G et IP, cartographie des actifs **critiques**

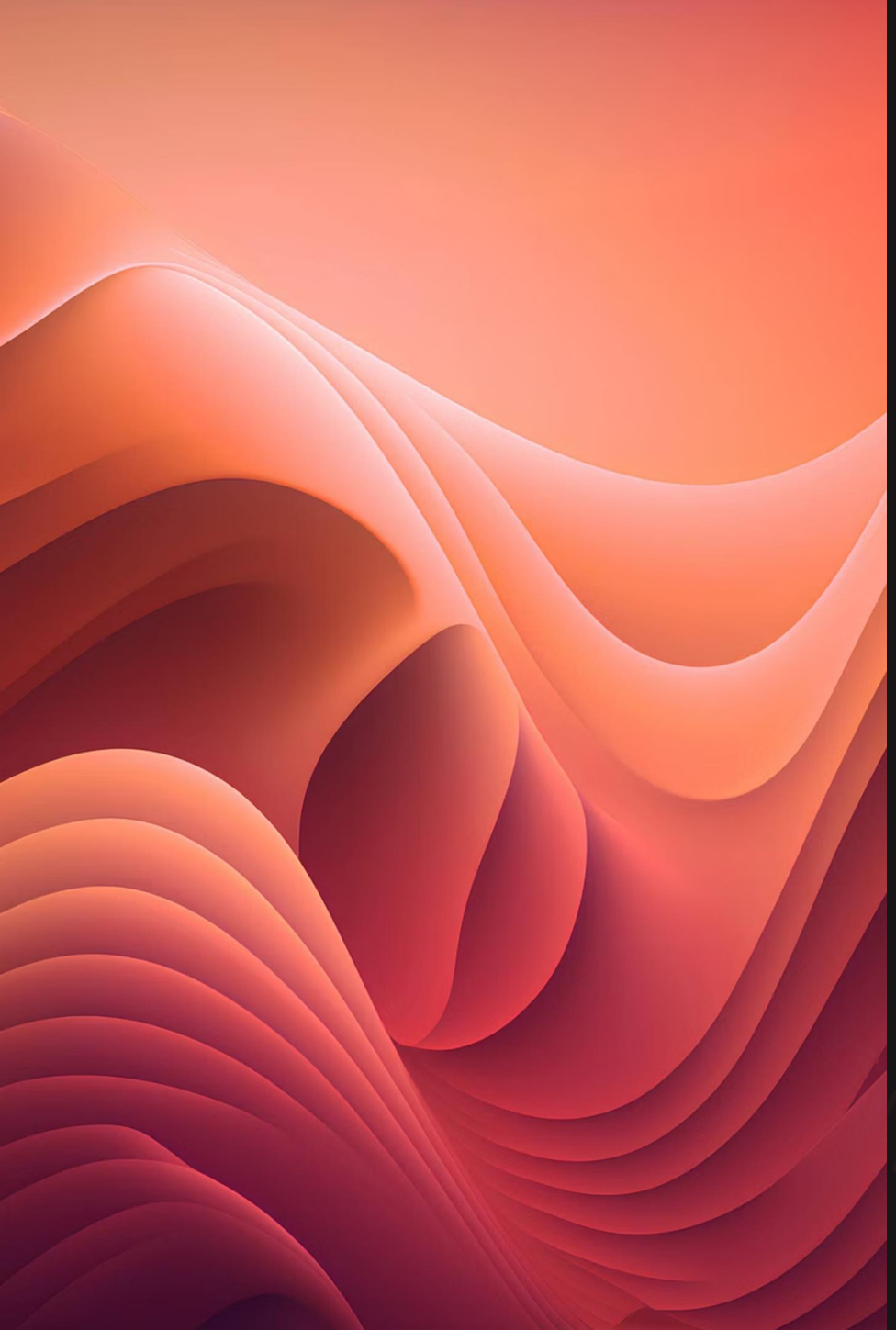
Cloisonnement Réseau

Séparation physique et logique, firewalls dédiés, zones DMZ pour l'interconnexion

Supervision Temps Réel

SOC dédié, détection d'anomalies, **alertes** automatisées sur les incidents





Plan d'Actions

1

Court Terme (3 mois)

- Cartographie des actifs critiques :
- Formation équipes techniques
- Mise à jour firmware équipements

2

Moyen Terme (6 mois)

- Déploiement chiffrement bout-en-bout
- Segmentation réseau avancée
- Procédures incident response

3

Long Terme (12 mois)

- Certification conformité NIS2
- Architecture Zero Trust
- Résilience opérationnelle

Made with GAMMA

L'Heure de l'Action

NIS2 représente une **opportunité unique de structurer la cybersécurité de vos réseaux critiques**.

La conformité n'est plus une option, c'est un **impératif stratégique**.

Coopération Technique

Rapprocher équipes IT, OT et métiers pour une approche intégrée

Investissement Prioritaire

Budget dédié à la modernisation et sécurisation des infrastructures

Expertise Spécialisée

Accompagnement par des professionnels de la cybersécurité industrielle

Made with GAMMA

Merci

Questions et échanges

Made with GAMMA