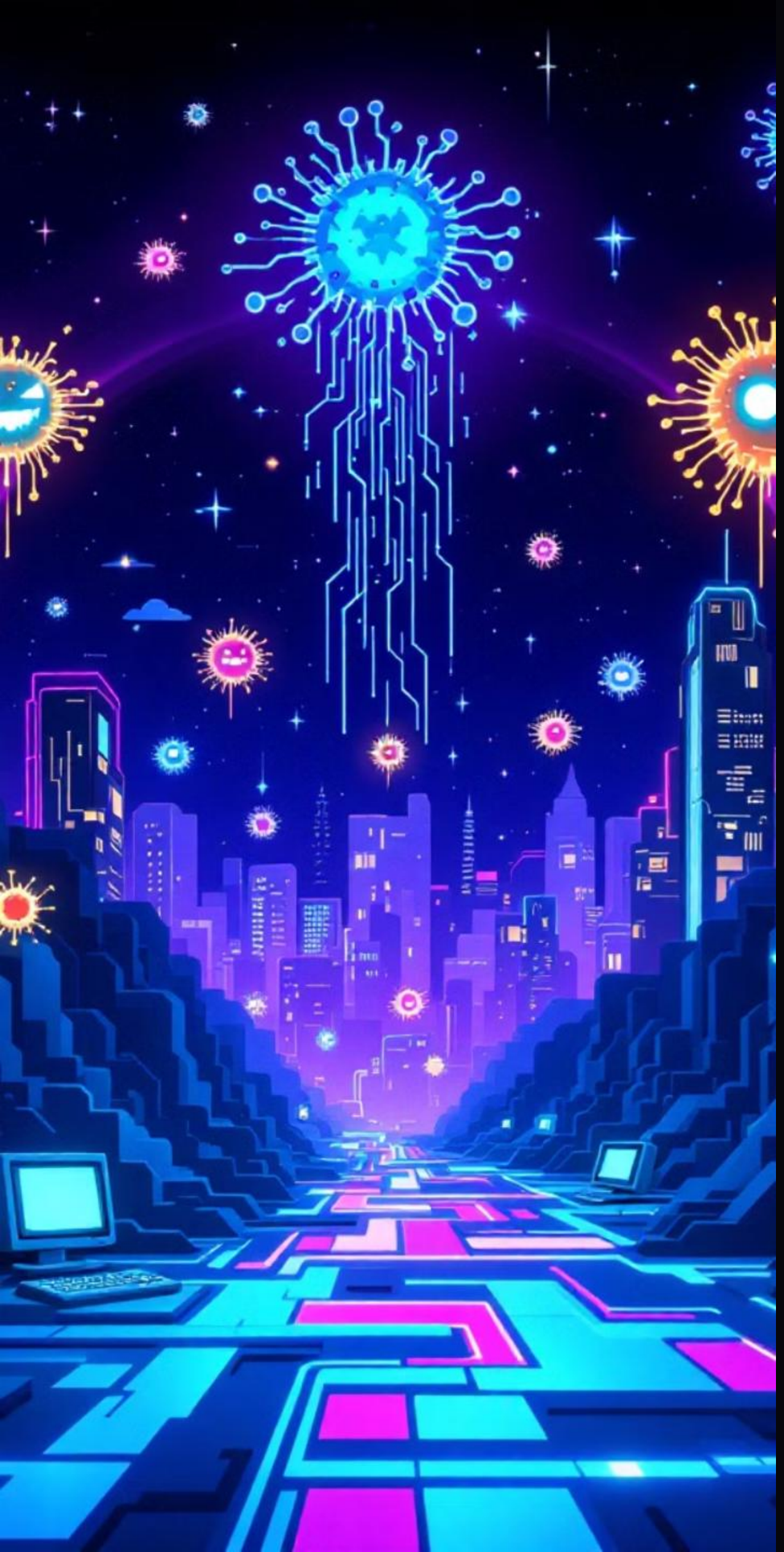
# Cybersécurité 2025 : Restons Protégés !

Bienvenue à cette présentation sur les tendances de cybersécurité pour 2025. Dans un monde numérique en constante évolution, comprendre les menaces émergentes est essentiel pour protéger votre entreprise.

Nous explorerons ensemble les nouvelles menaces qui se profilent à l'horizon, ainsi que les stratégies pour y faire face efficacement. La cybersécurité est une responsabilité partagée, et votre vigilance constitue la première ligne de défense.

upinfo



# Un Paysage Cyber en Constante Évolution

### Passé

Menaces simples et facilement identifiables

### Présent

Attaques sophistiquées et ciblées

### Futur (2025)

Menaces alimentées par l'IA et technologies avancées

Le paysage de la cybersécurité évolue à un rythme sans précédent. Les menaces d'aujourd'hui sont déjà plus sophistiquées que celles d'hier, et cette tendance s'accélérera d'ici 2025. Notre objectif est de comprendre ces nouvelles menaces pour mieux vous protéger.

Il est essentiel d’ identifier les risques émergents et d’ adopter les comportements qui renforceront notre sécurité au quotidien.

# L'IA dans la Cybersécurité : Une Double Lame

## L'IA comme outil d'attaque

- Phishing et spearphishing perfectionnés
- Malwares sophistiqués et adaptatifs
- Automatisation des attaques
- IA générative pour tromper systèmes et employés

## L'IA comme outil de défense

- Détection des menaces en temps réel
- Automatisation des réponses
- Identification des faux positifs
- Priorisation des menaces critiques

L'intelligence artificielle représente à la fois notre plus grand défi et notre meilleur allié en matière de cybersécurité. Les cybercriminels l'utilisent pour créer des attaques plus convaincantes et automatisées, tandis que nous l'employons pour renforcer nos défenses.

**Actions concrètes :** Soyez vigilants face aux emails et communications suspectes. Méfiez-vous des demandes inhabituelles, même si elles semblent provenir de sources connues.

# Attention aux Illusions : L'Ère des Deepfakes

## Qu'est-ce qu'un deepfake ?

Contenu audio et vidéo hyperréaliste généré par l'IA, capable d'imiter parfaitement une personne réelle.

## Risques pour l'entreprise

Fraude financière, usurpation d'identité des dirigeants, atteinte à la réputation de l'entreprise.

## Méthodes d'attaque

Appels vidéo falsifiés, messages vocaux contrefaits, manipulation d'image pour l'ingénierie sociale.

Les deepfakes représentent une menace croissante pour les entreprises. Ces technologies permettent de créer des contenus audio et vidéo si réalistes qu'il devient difficile de distinguer le vrai du faux.

**Actions concrètes :** Validez systématiquement l'authenticité des communications audio et vidéo, surtout pour les demandes sensibles. Mettez en place des protocoles de vérification et des flux de validation pour les informations critiques.

# Protéger l'écosystème : Les Risques

### Infiltration

Logiciels malveillants via des mises à jour légitimes

### Propagation

Exploitation des relations de confiance entre partenaires

### Impact

Compromission de multiples organisations en une seule attaque

Certaines attaques ciblent vos fournisseurs et partenaires pour atteindre indirectement votre entreprise. Ces attaques sont particulièrement dangereuses car elles exploitent les relations de confiance établies entre organisations.

**Actions concrètes :** Soyez vigilants quant aux demandes provenant de sources externe. Signalez toute activité suspecte et mettez en place des procedures de verification, en particulier dès que cela concerne des demandes d' informations liées à vos accès ou password.

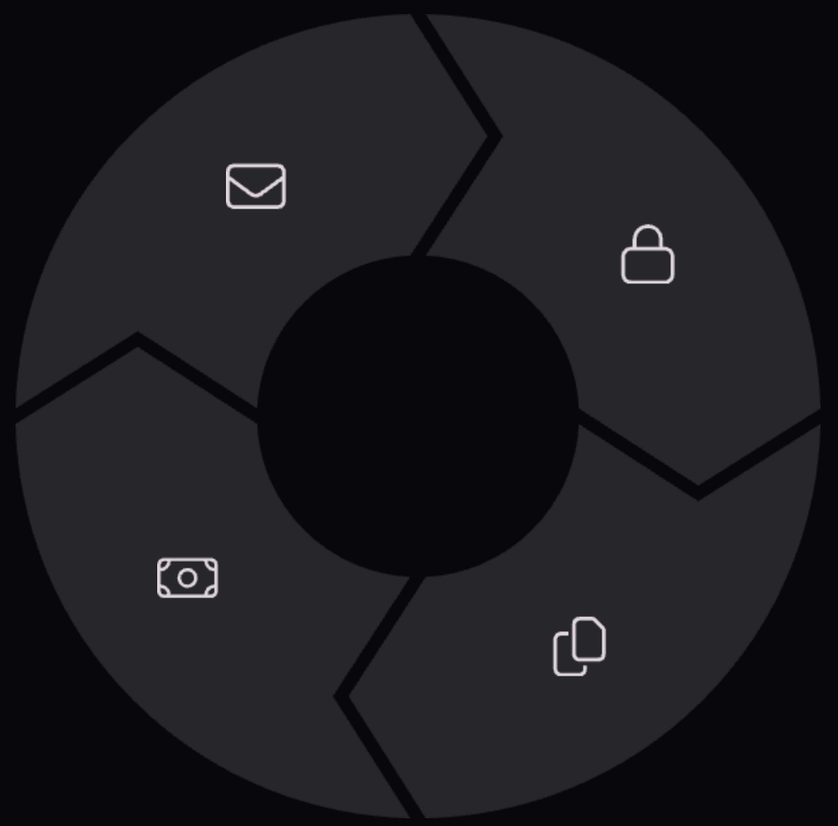
# Le Ransomware : Une menace persistante

### Infection

Via phishing, vulnérabilités ou accès compromis

### Chiffrement

Données rendues inaccessibles



### Rançon

Demande de paiement pour récupération

### Vol de données

Double extorsion: chiffrement et menace de publication

Le ransomware reste l'une des menaces les plus persistantes et dévastatrices pour les entreprises. Les attaquants ont développé des tactiques plus sophistiquées, comme la double extorsion qui combine le chiffrement des données avec leur vol.

**Actions concrètes :** Ne jamais cliquer sur des liens ou ouvrir des pièces jointes provenant de sources inconnues. Signalez immédiatement toute demande de rançon ou tout fichier chiffré suspect.
La mise en place d'un service SOC permet la surveillance 24/7 de la cybersécurité par des professionnels.

# Chiffres Clés : La Cybersécurité en 2025

La menace cyber évolue rapidement. Ces chiffres révèlent l'ampleur des défis à venir.

85%

Attaques IA

Des cyberattaques utiliseront l'intelligence artificielle d'ici 2025

11.5M

Postes vacants

Déficit mondial de professionnels en cybersécurité

10.5T

Coût global

Impact financier estimé des cyberattaques d'ici 2025

24.5B

Appareils IoT

Connectés et vulnérables aux nouvelles menaces

Ces prévisions soulignent l'importance d'une stratégie de défense proactive et d'une sensibilisation constante de tous les collaborateurs.

# Sécuriser le monde connecté : Les risques liés à l'IoT

### Caméras de sécurité

Souvent vulnérables aux accès non autorisés

### Appareils mobiles

Point d'entrée potentiel vers le réseau principal

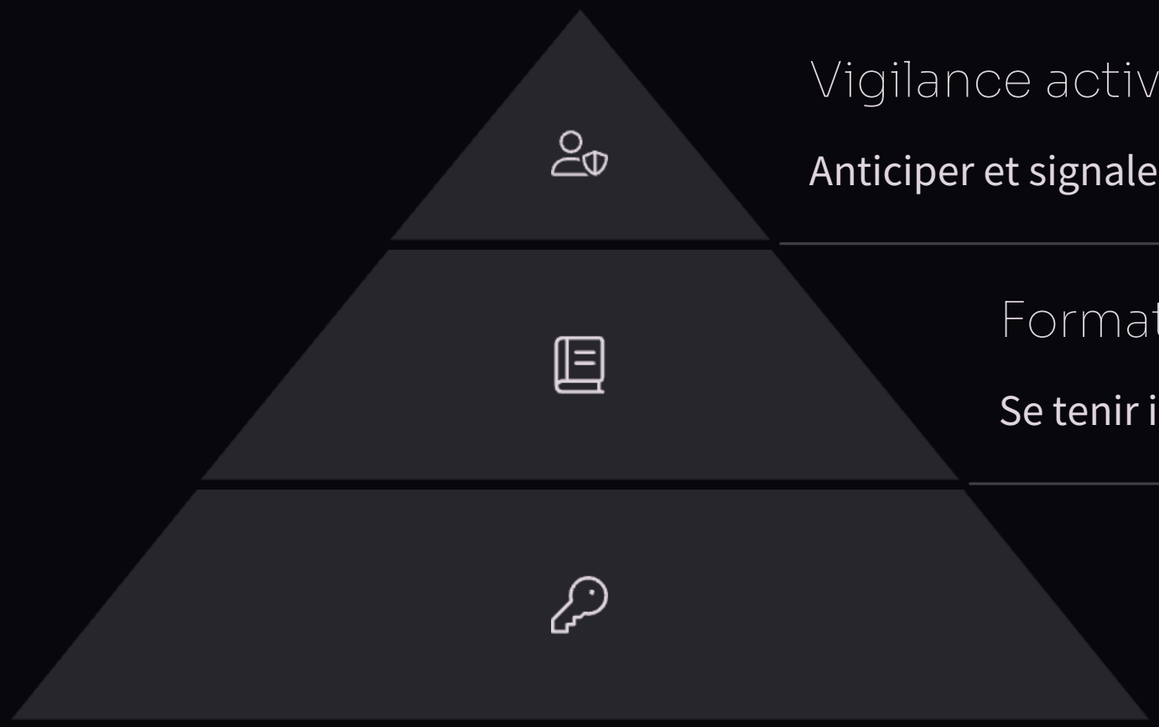
### Imprimantes

Rarement mise à jour et souvent négligée

La prolifération des objets connectés (IoT) dans l'entreprise crée de nouveaux vecteurs d'attaque. Ces appareils, souvent conçus avec la fonctionnalité comme priorité plutôt que la sécurité, peuvent devenir des points d'entrée vers notre réseau.

**Actions concrètes :** Soyez conscients des appareils IoT connectés au réseau de l'entreprise. Signalez tout comportement étrange des appareils connectés et évitez toute installation sans étudier le critère de sécurité.

# La Cybersécurité :
# Le rôle de chacun est essentiel



Vigilance active

Anticiper et signaler les menaces

Formation continue

Se tenir informé des nouvelles menaces

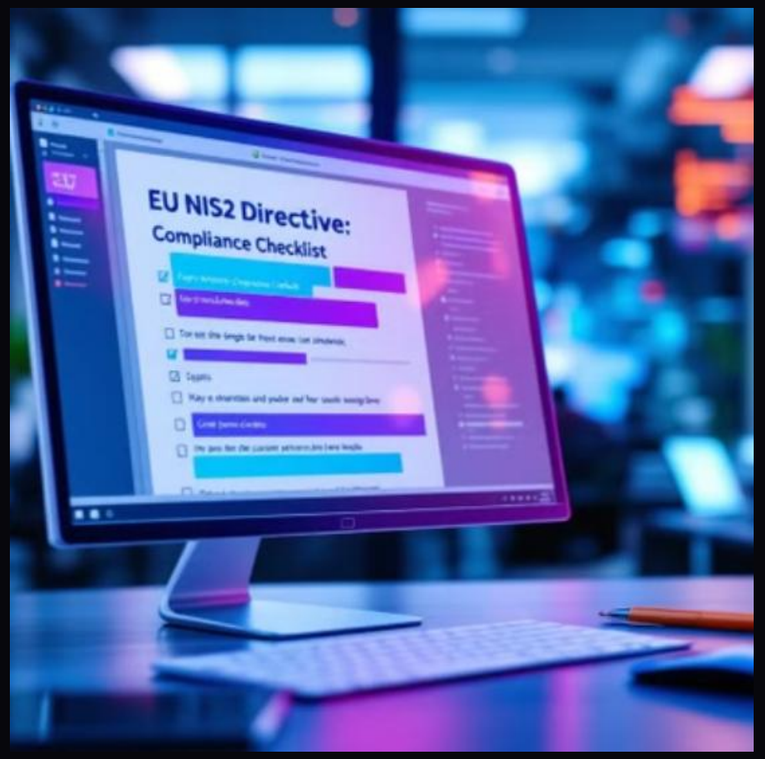
Bonnes pratiques

Mots de passe forts, authentification à deux facteurs

L'humain reste la première ligne de défense contre les cyberattaques. L'ingénierie sociale, comme le phishing et les arnaques par email professionnel (BEC), cible directement les employés pour contourner les défenses techniques.

**Actions concrètes :** Toujours vérifier l'expéditeur et le contenu des emails et messages. En cas de doute, ne pas agir et contacter le service informatique. Adoptez les bonnes pratiques de sécurité au quotidien.

# Se conformer pour sécuriser : les nouvelles réglementations





Les réglementations comme NIS2 et DORA imposent de nouvelles obligations aux entreprises en matière de cybersécurité. Ces cadres réglementaires visent à renforcer la résilience numérique à l'échelle européenne et à garantir une meilleure protection des données.

La conformité à ces réglementations n'est pas seulement une obligation légale, mais aussi un moyen d'améliorer notre posture de sécurité globale. Les sanctions en cas de non-conformité peuvent être significatives.

**Actions concrètes :** Comprendre que la conformité réglementaire est une responsabilité collective. Soyez attentifs aux communications concernant les nouvelles directives de sécurité.