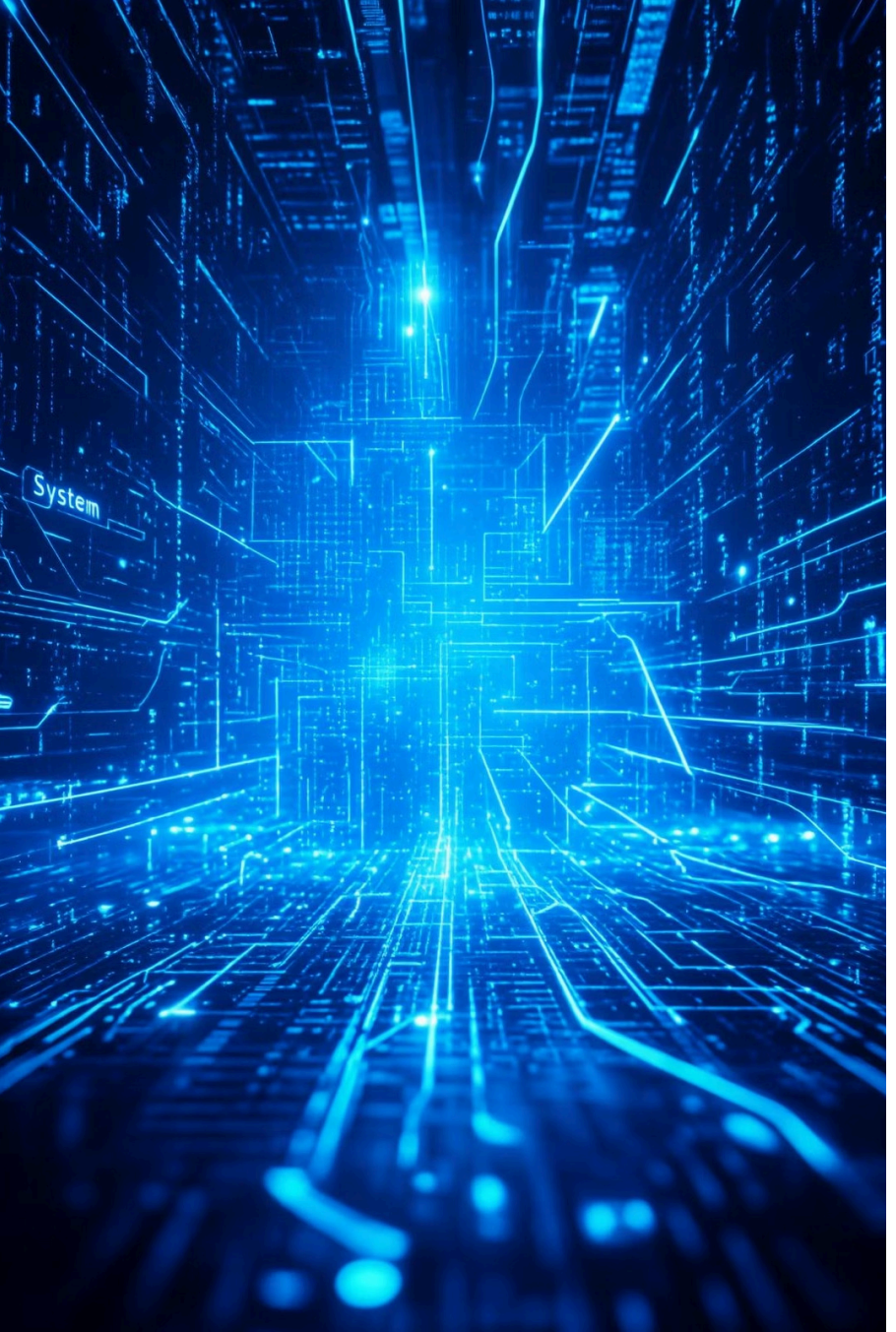
Les trois domaines du risque cyber

Le risque cyber représente la possibilité de pertes causées par des cyberattaques ou des compromissions de données.

Explorons les trois dimensions principales du risque numérique qui menacent nos organisations.

par Serge Houtain



Introduction au risque cyber

Définition

Ensemble des risques liés au numérique pouvant affecter les systèmes d'information et les données.

Évolution

Paysage des cybermenaces en mutation constante, avec des attaques de plus en plus sophistiquées.

Approche

Nécessité d'une compréhension holistique des risques pour une protection efficace.

Premier domaine: Les accidents

Incendies

Destruction des centres de données et perte d'informations critiques.

Coupures d'électricité

Interruptions des services numériques essentiels.

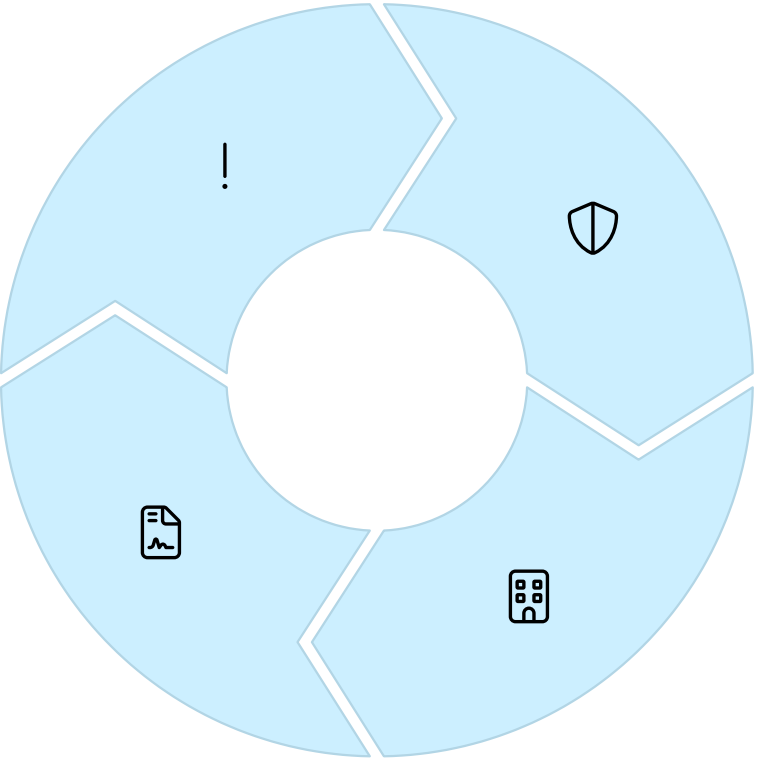
Dégâts des eaux

Endommagement des équipements et des infrastructures informatiques.

Impact des accidents sur la sécurité

Perturbation

Interruption des activités sans intention délibérée de nuire.



Vulnérabilités

Failles de sécurité créées pendant les interruptions.

Plans

Nécessité de stratégies de continuité d'activité robustes.

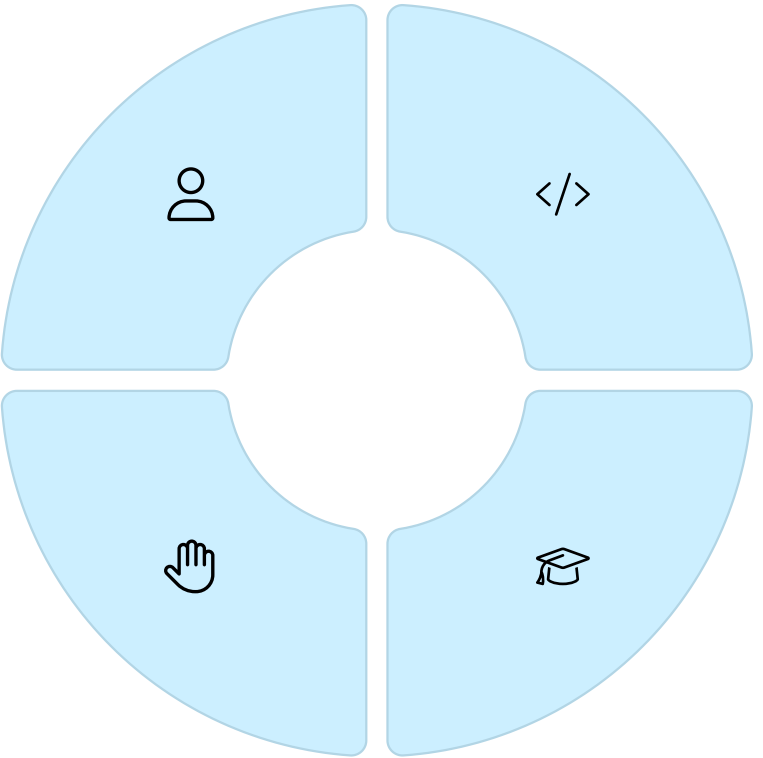
Infrastructures

Défaillances des systèmes critiques de l'organisation.

Deuxième domaine: Le facteur humain

Négligence

Actions involontaires compromettant la sécurité des systèmes.



Code défectueux

Erreurs de programmation créant des vulnérabilités exploitables.

Mauvaises manipulations

Erreurs opérationnelles compromettant l'intégrité des systèmes.

Formation inadéquate

Manque de connaissances en sécurité chez les collaborateurs.

Manifestations du facteur humain

70%

Erreurs humaines

Part du risque cyber attribuable au facteur humain.

43%

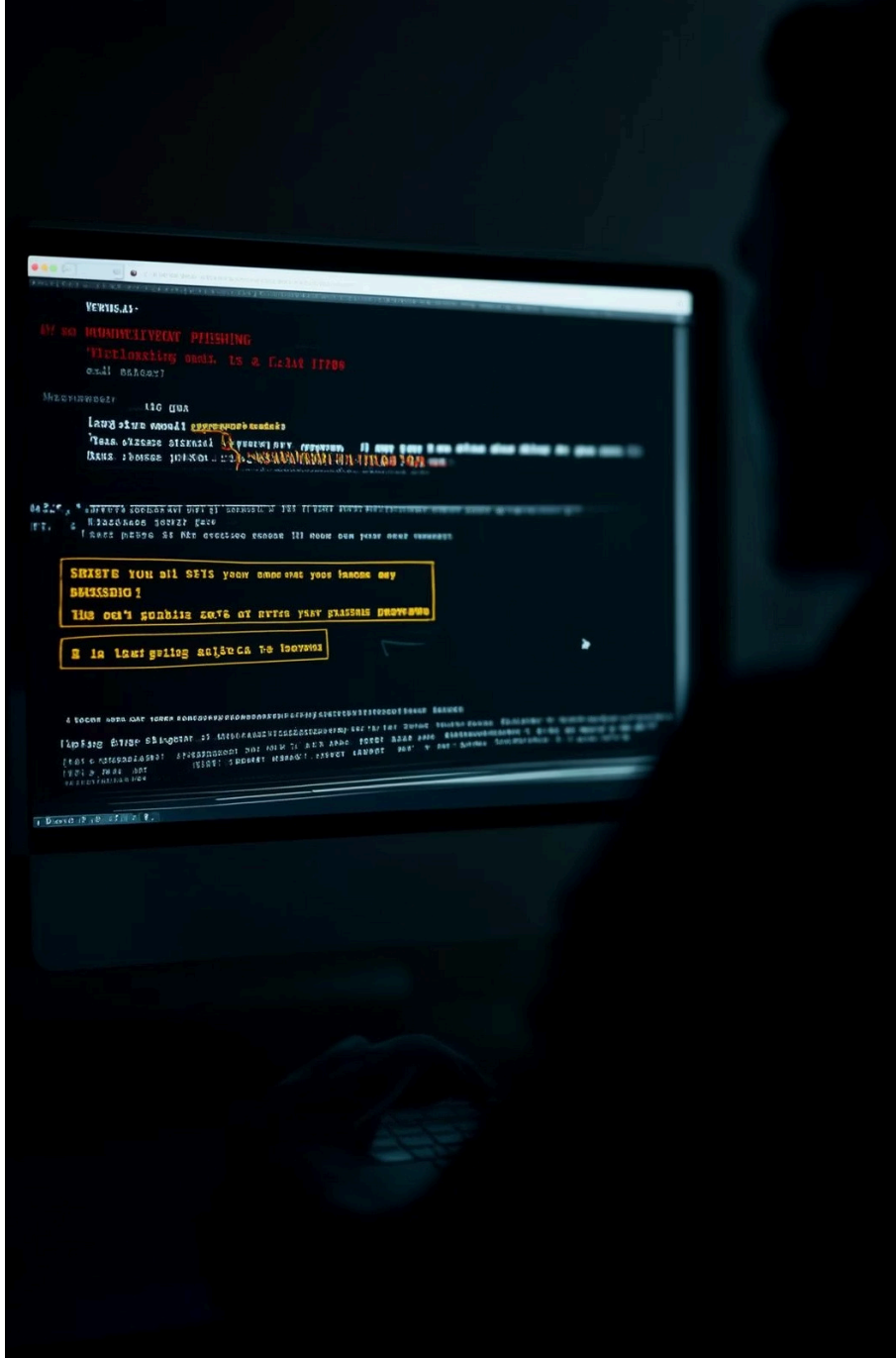
Phishing réussi

Employés cliquant sur des liens malveillants.

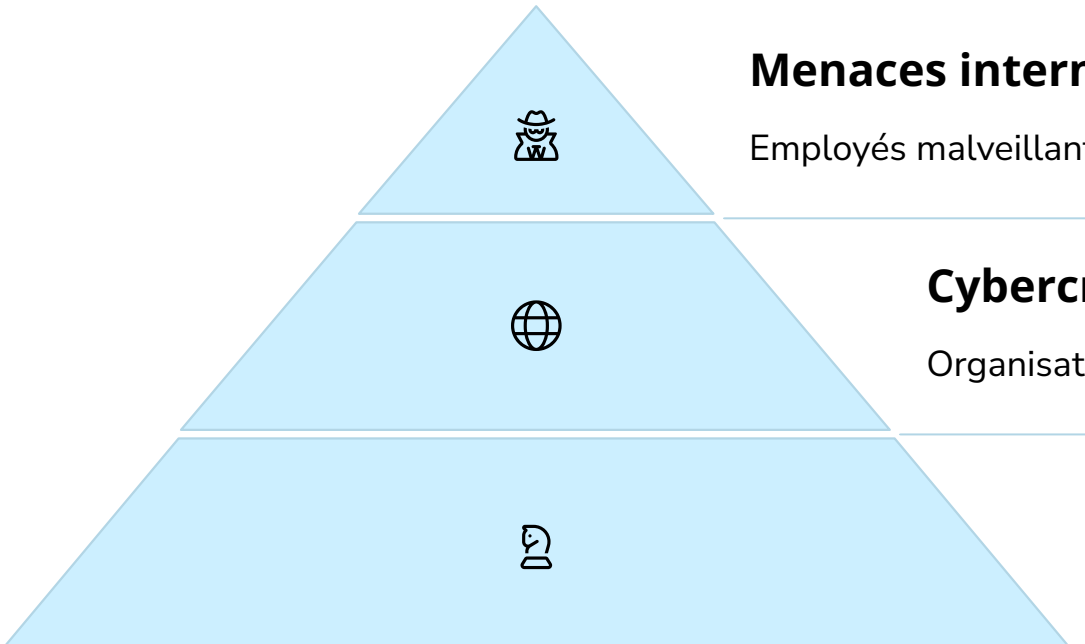
56%

Configurations erronées

Systèmes mal paramétrés créant des vulnérabilités.



Troisième domaine: La malveillance



Menaces internes

Employés malveillants ou compromis.

Cybercriminalité

Organisations criminelles ciblant les entreprises.

Actes délibérés

Attaques planifiées visant les systèmes d'information.

Principales cyberattaques

Rançongiciel

Cryptage des données avec demande de rançon pour leur récupération.

Vol de données

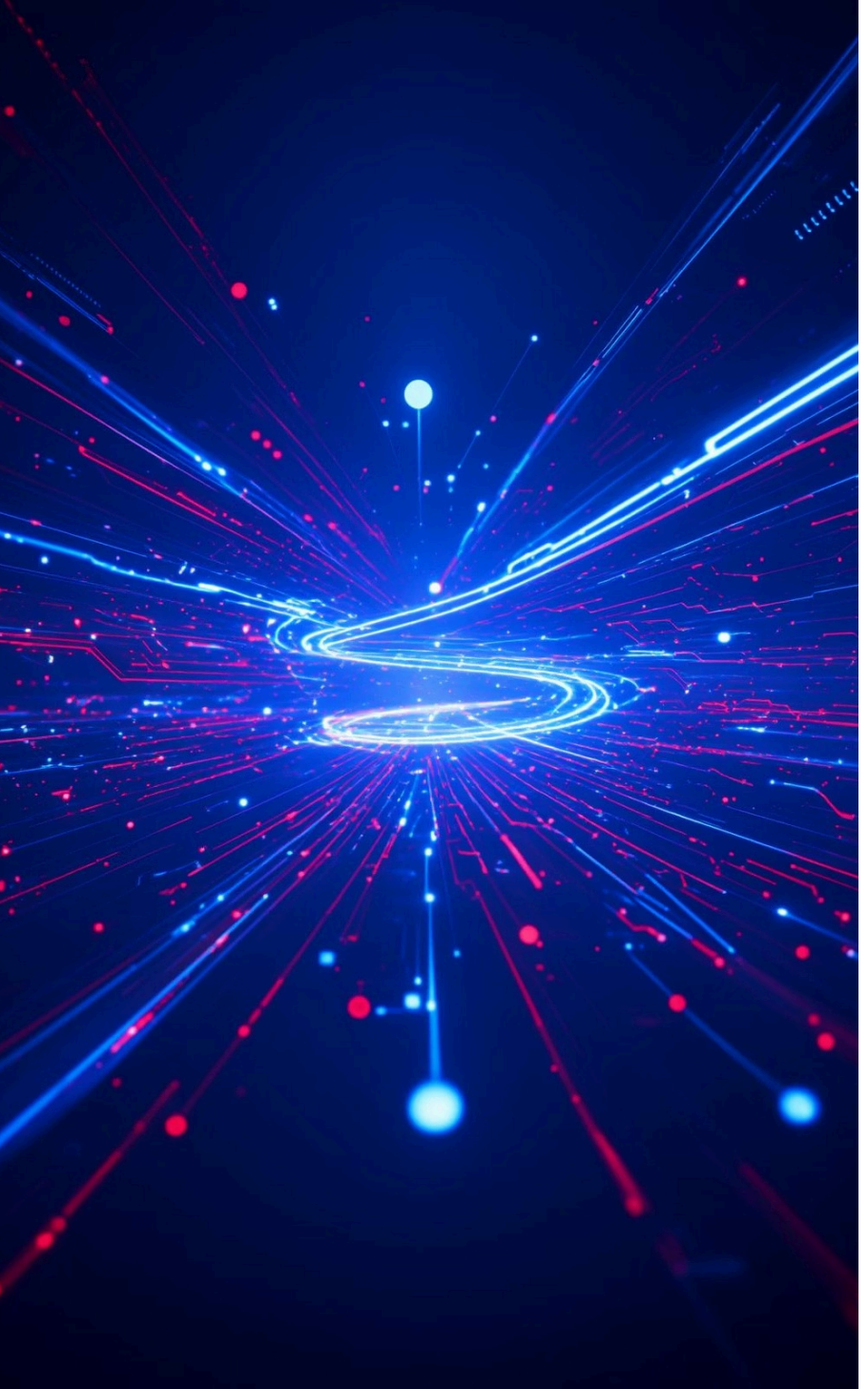
Extraction d'informations sensibles à des fins malveillantes.

Compromission des emails

Usurpation d'identité pour des fraudes financières.

Attaques zero-day

Exploitation de vulnérabilités inconnues des éditeurs.



Tendances émergentes en cybercriminalité

Attaques de la chaîne d'approvisionnement

Compromission des fournisseurs pour atteindre les cibles principales.

IA malveillante

Utilisation de l'intelligence artificielle pour créer des attaques sophistiquées.

Menaces quantiques

Vulnérabilités liées à l'avènement de l'informatique quantique.

Risques IoT

Exploitation des failles dans les objets connectés.

Stratégies de protection

Identification

Cartographie des actifs numériques et évaluation des risques associés.

Protection

Mise en place de contrôles de sécurité adaptés aux menaces identifiées.

Détection

Surveillance continue et identification rapide des incidents.

Réaction

Procédures de réponse aux incidents pour minimiser l'impact.

Récupération

Processus de restauration des systèmes après un incident.

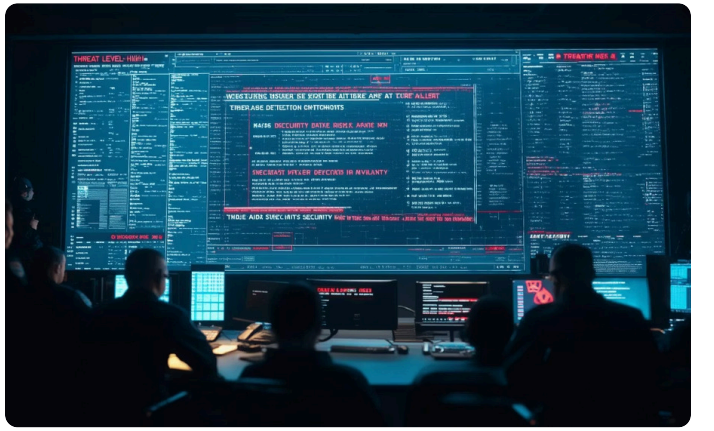
Mesures préventives essentielles

Formation

Sensibilisation régulière de tous les collaborateurs aux bonnes pratiques.

Plans de continuité

Stratégies détaillées pour maintenir les opérations en cas d'incident.



Surveillance

Détection proactive des comportements suspects dans les systèmes.

Conclusion: Une approche intégrée

Intégration

Adresser simultanément les trois domaines du risque cyber.

Évolution

Adaptation constante face aux menaces changeantes.

Protection

Dispositifs de sécurité adaptés à chaque type de risque.

Stratégie

La cybersécurité comme enjeu majeur pour toute organisation.