MILLENIUM RISK

Nos services

Millenium Risk

NOS SERVICES

01 Évaluation des risques

02 Diagnostic de maturité

03 Définition et mise en place de la gouvernance

04 Gestion des risques tiers

05 Gestion de la continuité des activités

06 Post-mortem

07 Mise en conformité

08 Formation et sensibilisation

Pourquoi évaluer les risques en cybersécurité ?

Protection des actifs

Sécuriser les données et les systèmes contre les cyberattaques.

Conformité réglementaire

Répondre aux exigences légales et normatives.

Préparation aux incidents

Identifier les vulnérabilités et atténuer les impacts des menaces.

Réduction des coûts

Prendre des mesures proactives pour éviter les pertes financières dues à des attaques.

Évaluation des risques

Identification des Actifs et des Menaces

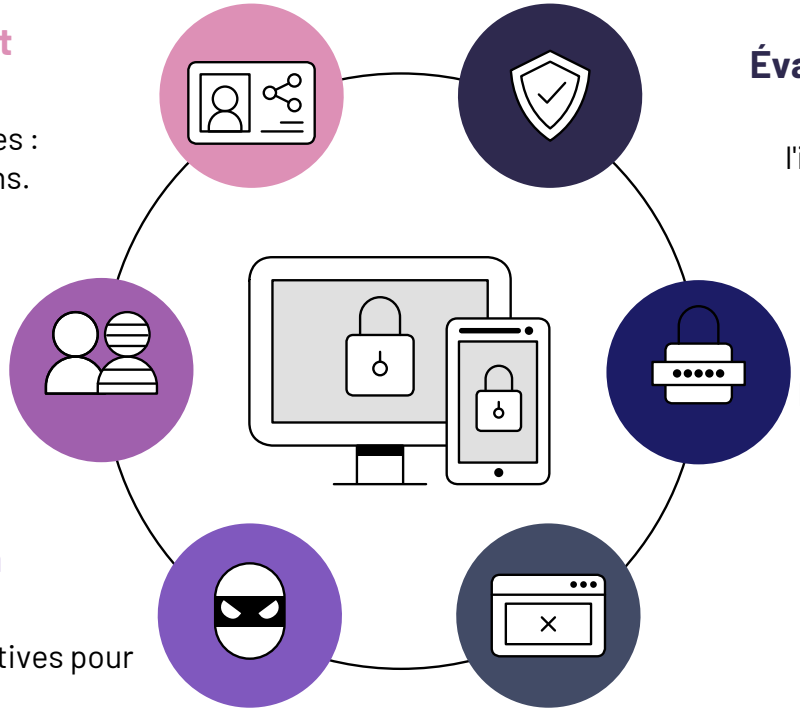
Cartographie des actifs critiques : données, systèmes, applications.

Suivi et Réévaluation

Mise en place d'un suivi pour évaluer l'évolution des risques et des contrôles.

Recommandations et Plan d'Action

Proposition de mesures correctives pour atténuer les risques identifiés.



Évaluation des Vulnérabilités

Analyse des points faibles dans l'infrastructure, les processus et les technologies.

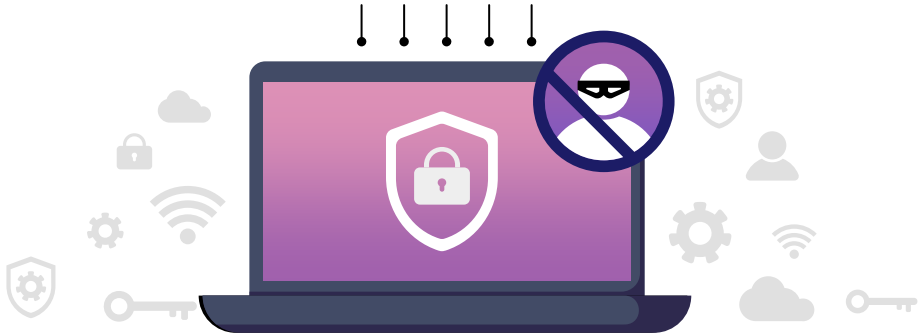
Analyse d'Impact et Probabilité

Évaluation de l'impact potentiel des menaces identifiées et de leur probabilité d'occurrence.

Évaluation des Contrôles Existants

Vérification de l'efficacité des contrôles de sécurité en place.

Diagnostic de Maturité



Évaluation Initiale

Identification des parties prenantes et des risques spécifiques

Analyse de la Maturité

Évaluation basée sur des frameworks de maturité reconnus

Évaluation des Domaines Clés

Analyse des domaines critiques

Recommandations

Rapport détaillant les résultats du diagnostic et les recommandations

Amélioration Continue

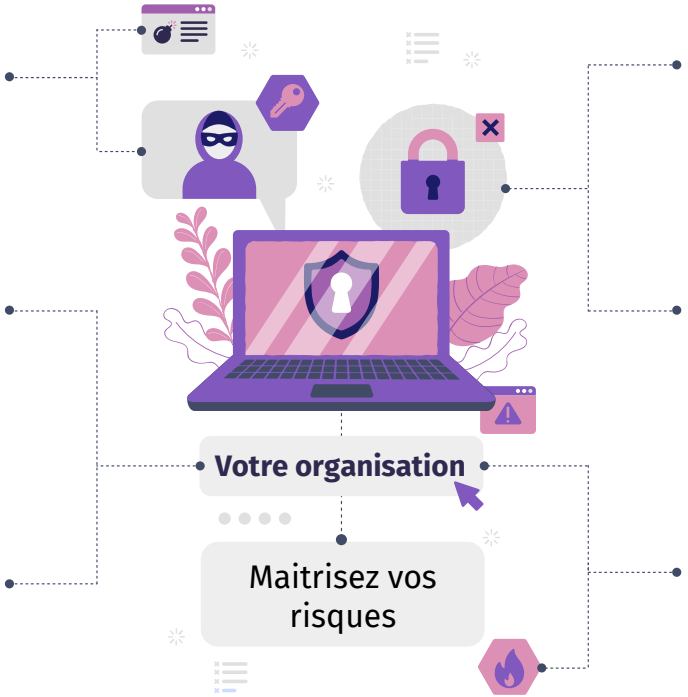
Proposition d'un plan de mise en œuvre des recommandations et d'un suivi

Définition et mise en place de la gouvernance

Analyse des Besoins et Objectifs

Définition des Politiques et Cadres de Gouvernance

Structuration des Responsabilités et Rôles



Mise en Œuvre des Processus et Contrôles

Suivi et Reporting

Amélioration Continue

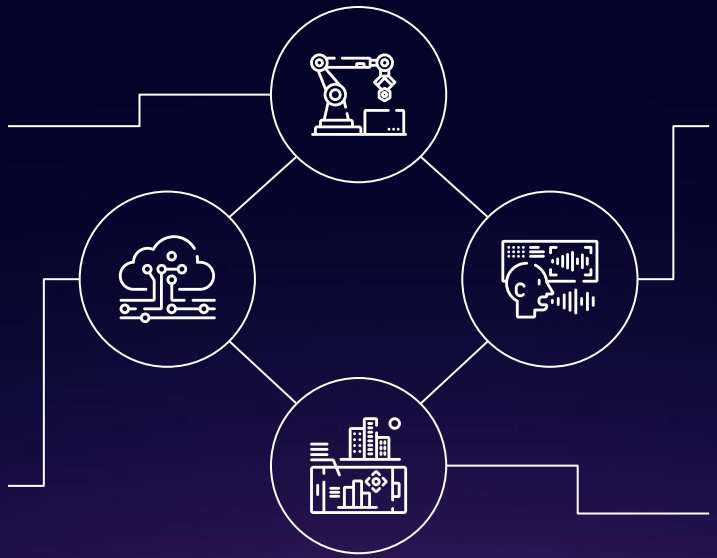
Pourquoi gérer les risques tiers en cybersécurité ?

Multiplication des connexions

Les tiers peuvent être des points d'entrée pour des cyberattaques.

Réduction des risques

Minimisation de l'exposition aux risques liés aux tiers (fournisseurs, partenaires, prestataires de services cloud, etc.).



Responsabilité partagée

Les violations de données peuvent être causées par des partenaires qui ne respectent pas les mêmes standards de sécurité.

Conformité réglementaire

Certaines normes exigent de prendre en compte la sécurité des tiers (ex. : GDPR, ISO 27001).

Gestion des Risques-Tiers

01

Identification des Tiers et Évaluation des Risques

Recensement des tiers critiques et identification des risques associés à chaque partenariat (fournisseurs, prestataires, etc.).

02

Évaluation des Contrôles de Sécurité des Tiers

Vérification des contrôles de sécurité en place chez les tiers (p.ex., normes ISO, SOC 2, audits de sécurité).

03

Gestion des Contrats et des Accords

Élaboration de clauses de cybersécurité dans les contrats et accords de service avec les tiers (p.ex., NDA, clauses de sécurité, SLA, etc.).

04

Surveillance Continue et Réévaluation

Détection proactive des nouvelles menaces et vulnérabilités via des audits périodiques et des outils de surveillance.

05

Plan de Réponse aux Incidents et Communication

Élaboration d'un plan de réponse aux incidents en cas de violation de sécurité impliquant un tiers.

Gestion de la continuité des activités

Analyse d’Impact sur les Activités (BIA)

Plan de Continuité des Activités (PCA)

Plan de Reprise d’Activité (PRA)

Plan de Test de Continuité des Activités

Plan de Communication en Cas de Crise

Post-Mortem cyber

01 Analyse Post-Incident

- Rapport d'Incident & de Communication
- Estimation des repercussions

02 Plan d'Amélioration & Leçons Apprises

- Document des leçons apprises de l'incident, des améliorations possibles dans les processus, les outils, et les formations.

03 Mise à jour des Politiques de Sécurité

- Politique de Sécurité des Systèmes d'Information (PSSI)
- Plan de Continuité des Activités (PCA)
- Plan de Reprise des Activités (PRA)

04 Plan de Test et de Validation des Correctifs

- Test à l'aide de scénario de crise probable
- Amélioration continue

Mise en Conformité

Évaluation Initiale

Analyse des exigences réglementaires applicables à votre organisation.

Élaboration d'un plan détaillé pour atteindre et maintenir la conformité.

Plan de Conformité

Mise en œuvre

Application des actions correctives, mise à jour des politiques et des processus.

Évaluation continue et audits réguliers pour vérifier la conformité.

Audit de suivi

Formation & Sensibilisation

Formation

Elle est essentielle pour garantir la protection des systèmes d'information et des données sensibles au sein d'une organisation. Face à l'évolution constante des menaces cyber, il est crucial que tous les employés, à tous les niveaux, soient formés pour reconnaître les risques, adopter de bonnes pratiques de sécurité et réagir efficacement en cas d'incident.

Sensibilisation

Elle permet de cultiver une conscience collective des risques informatiques et des comportements à adopter pour les minimiser. En sensibilisant les employés aux menaces comme le phishing, les malwares ou les violations de données, on les équipe pour reconnaître et éviter ces attaques avant qu'elles n'affectent les systèmes de l'entreprise.

MILLENIUM RISK

Maitrisez vos risques liés à la cybersécurité

www.millenium-risk.fr