Feuille de route Cybersécurité

Ces dernières années, le nombre d'incidents liés à la cybercriminalité et à la perte de données a augmenté en flèche. Alors que par le passé, les cyberattaques visaient principalement les grandes organisations, elles prennent désormais aussi pour cible des organisations et des administrations publiques de plus petite taille. Ces incidents passent de plus en plus souvent inaperçus ou ne sont détectés que plusieurs mois plus tard.

Quels sont les maillons faibles dans votre système de sécurité ? Et quels sont les risques pour votre organisation ?

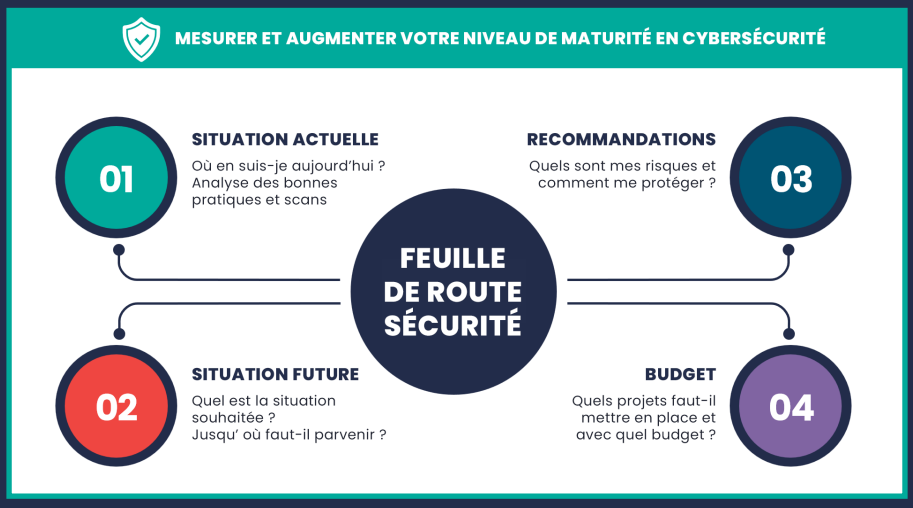
La Feuille de route Cybersécurité vous permet de répondre à ces questions, en définissant une stratégie de sécurité claire et proactive pour votre organisation. Avec vos collaborateurs, nous prenons toutes les mesures de protection appropriées. Nous auditons vos systèmes existants, nous interprétons les résultats pour vous et nous établissons un plan d'approche pour vous aider à vous armer contre la cybercriminalité.

inetum realdolmen
Positive digital flow

Pourquoi établir une feuille de route Cybersécurité ?

Vos données, vos applications et vos utilisateurs se décentralisent au fur et à mesure que vos collaborateurs gagnent en mobilité et que votre environnement informatique se complexifie. Les criminels innovent, les menaces évoluent sans cesse et dans ce contexte, la sécurité des données devient un véritable enjeu.

En tant que CIO ou responsable informatique, vous pouvez utiliser la feuille de route pour mesurer et cartographier le niveau de maturité actuel de la sécurité de votre environnement informatique. Vous pouvez ensuite l'intégrer à votre stratégie de sécurité ou l'utiliser comme stratégie à part entière. Elle forme dans ce cas la base de la sécurité de votre environnement informatique pour les années à venir.



Notre méthode

1. Réunion de lancement pour définir ensemble vos objectifs
2. Audit et collecte d'informations sur votre infrastructure informatique, avec un scan des vulnérabilités et une analyse des risques AD
3. Organisation d'ateliers avec les parties prenantes sur la base de nos Security Baselines Inetum-Realdolmen, pour évaluer le niveau de maturité actuel de la sécurité dans votre organisation
4. Présentation et remise de votre feuille de route cybersécurité personnalisée

Les Security Baselines d'Inetum-Realdolmen couvrent l'ensemble de votre environnement informatique

- **Reposent sur de bonnes pratiques reconnues au niveau mondial (NIST, CIS, ISO...) et l'expérience d'Inetum-Realdolmen**
- **18 thématiques différentes, dont la gestion des actifs, la protection des données, la défense de l'infrastructure et la gestion de la réponse aux incidents, avec 170 bonnes pratiques au total**
- **Subdivision en 3 niveaux en fonction de la complexité : Standard, Advanced et Premium**

Votre feuille de route personnalisée reprend les points forts de votre organisation, ses points faibles et les conséquences possibles pour chaque thématique de sécurité. Nous formulons des recommandations pour atténuer ou neutraliser les risques identifiés. Nous vous aidons à établir une liste des priorités et nous vous expliquons en détail les actions à entreprendre. Nous vous fournissons pour chaque recommandation une description concrète, le risque encouru et son impact, le niveau de priorité et une estimation budgétaire, le tout de façon aussi pragmatique que possible. L'ensemble du projet dure en moyenne 3 à 4 semaines. Tout dépend des disponibilités des différentes parties prenantes et de la taille de votre organisation.

Vous souhaitez en savoir plus sur la Feuille de route Cybersécurité ?

Nos experts sont à votre écoute pour toute question et suggestion

info@inetum-realdolmen.world

+32 2 801 55 55