KÁRMÁN

CYBER DEFENCE

ACCÉDER À LA RÉSILIENCE CYBER, SUR LA DURÉE_

Vous permettre de vous concentrer sur l'essentiel en offrant une protection complète contre les cyberattaques.

La question n'est plus « Allons-nous subir des cyberattaques ? », mais plutôt « Comment minimiser l'impact de ces attaques ? ».

Kármán Cyber Defence contribue à garantir la continuité des activités de ses clients.

« Il n'est plus seulement question de prévenir les violations de données. Il faut surtout en accélérer la détection. »

Philippe BACHA, Directeur Général

www.karmancyberdefence.com

KÁRMÁN
CYBER DEFENCE

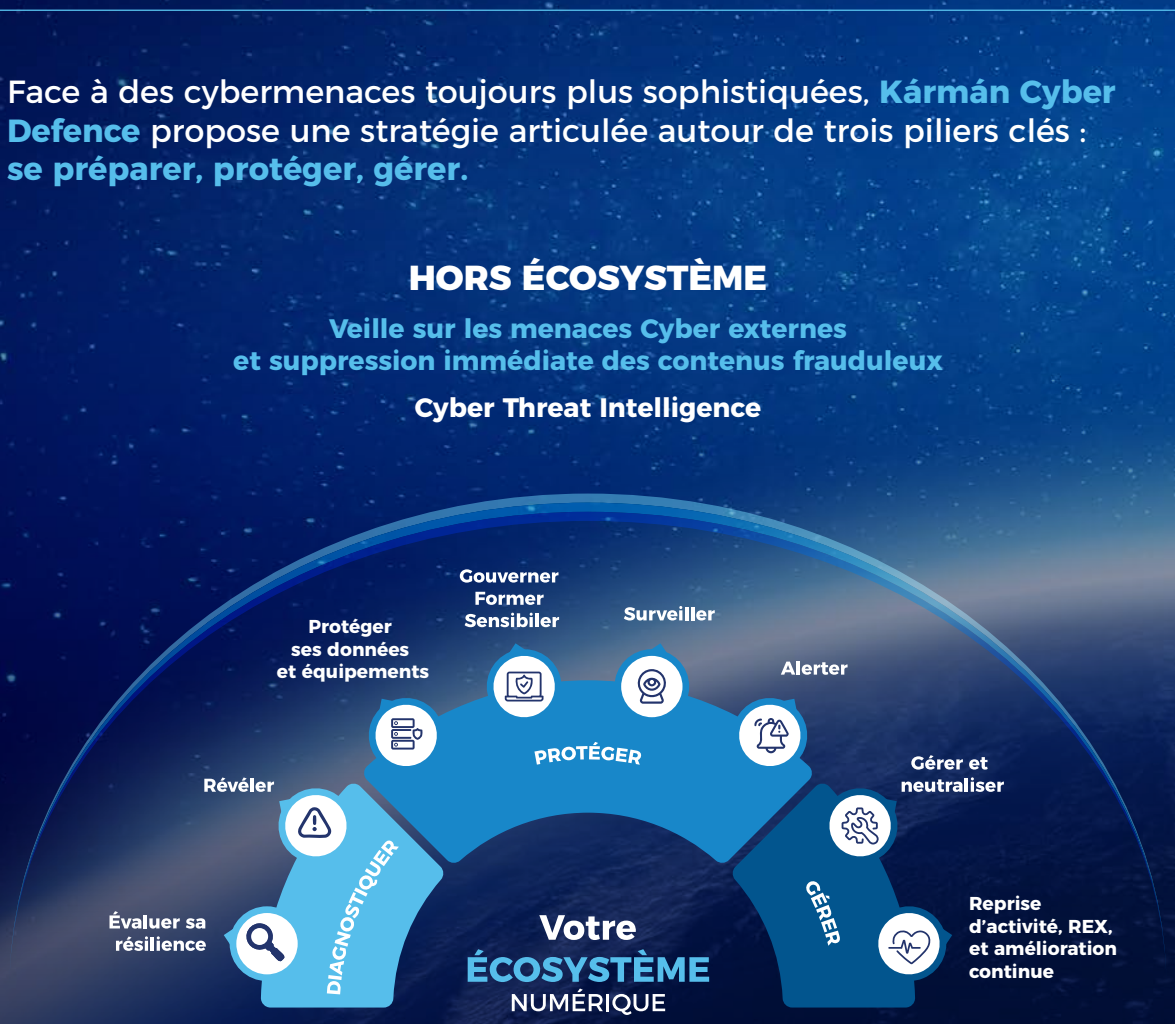
UNE APPROCHE GLOBALE, INTÉGRÉE & PERSONNALISABLE

Kármán Cyber Defence accompagne les entreprises dans la construction d'une cybersécurité résiliente et adaptée aux défis actuels. Son approche inclut :

- **L'identification des failles :** évaluation approfondie de la maturité cyber des organisations.
- **La mise en place de défenses solides :** sécurisation des infrastructures et formation continue des collaborateurs.
- **Une réaction efficace en cas d'incident :** limitation de l'impact et reprise rapide des activités.
- **L'anticipation des menaces externes :** détection proactive des risques avant qu'ils ne deviennent problématiques.

Cette stratégie est renforcée par une veille continue en **Cyber Threat Intelligence (CTI)** et **Digital Risk Protection (DRP)**, assurant une couverture exhaustive du cycle de sécurité.

Face à des cybermenaces toujours plus sophistiquées, **Kármán Cyber Defence** propose une stratégie articulée autour de trois piliers clés : **se préparer, protéger, gérer.**



DIAGNOSTIQUER

Évaluation de la maturité cyber

Objectif : Évaluer le niveau de préparation face aux cyberattaques (gouvernance, processus, protection technique).

Bénéfices :
- Meilleure visibilité pour orienter les efforts et budgets.
- Anticipation des menaces pour éviter les crises coûteuses.

Audit d'architecture et de configuration

Objectif : Vérifier la bonne configuration des infrastructures et serveurs pour éviter les failles.

Bénéfices :
- Réduction des risques d'intrusion liés à une mauvaise configuration.
- Amélioration de la stabilité et de la documentation de l'architecture.

Tests d'intrusion et Pentests

Objectif : Simuler des attaques pour identifier et corriger les failles de sécurité.

Bénéfices :
- Prévention des incidents en corrigeant les failles avant exploitation.
- Sensibilisation des équipes aux risques réels.

Planification et gouvernance

Objectif : Mettre en place une organisation et des politiques claires pour gérer la cybersécurité.

Bénéfices :
- Meilleure gestion grâce à des rôles et des indicateurs clairs.
- Passage d'une gestion réactive à une stratégie structurée.

Communication des résultats et engagement exécutif

Objectif : Présenter un rapport de synthèse aux dirigeants pour valider les mesures de sécurité.

Bénéfices :
- Soutien financier facilité grâce à une meilleure compréhension des enjeux.
- Mobilisation des équipes métiers et IT.

PROTÉGER

Mise en place des mesures de sécurité recommandées

Objectif : Déployer outils, processus et ressources pour renforcer la protection quotidienne.

Bénéfices :
- Réduction immédiate des risques grâce à des défenses modernes.
- Amélioration de la culture de sécurité grâce à une meilleure formation des collaborateurs.

Gouvernance, conformité & SMSI (ISMS)

Objectif : Mettre en place un Système de Management de la Sécurité de l'Information (SMSI) conforme aux normes (ISO 27 001, ANSSI).

Bénéfices :
- Crédibilité renforcée grâce à une éventuelle certification.
- Adaptation continue des règles de sécurité pour une gestion proactive.

Surveillance proactive et défenses avancées

Objectif : Suivre en continu le SI pour détecter rapidement les anomalies et prévenir les attaques.

Bénéfices :
- Réactivité accrue pour limiter les dommages en cas d'incident.
- Renforcement de la confiance des clients grâce à une surveillance efficace.

GÉRER

Gestion d'incidents

Objectif : Réagir rapidement et efficacement en cas d'incident pour limiter les dommages et identifier la cause.

Bénéfices :
- Réduction des dégâts (éviter l'arrêt de la production ou une fuite de données).
- Renforcement de la confiance des équipes et des clients.

Plans de reprise d'activité (PRA/PCA)

Objectif : Relancer rapidement l'activité après un sinistre pour limiter les pertes financières et d'image.

Bénéfices :
- Continuité de service assurée grâce à une reprise rapide.
- Résilience des équipes, qui savent comment réagir sans panique.

Retour d'expérience et amélioration continue

Objectif : Tirer des leçons de chaque incident pour améliorer en continu le niveau de sécurité.

Bénéfices :
- Adaptation constante face à l'évolution des menaces.
- Appropriation des bonnes pratiques par les équipes.

Le SOC

Votre première ligne de défense proactive

Un **SOC (Security Operations Center)** est un centre d'opérations de sécurité qui surveille, détecte et répond aux menaces informatiques en temps réel. Il est composé d'experts en cybersécurité qui utilisent des outils avancés pour analyser en continu les événements de sécurité et protéger les infrastructures IT et Cloud contre les cyberattaques. Un SOC efficace permet d'anticiper les attaques, de limiter les impacts des incidents et de garantir la conformité aux normes de sécurité.

Kármán Cyber Defence, l'expertise au service de votre SOC

Grâce à son savoir-faire et ses solutions de pointe, Kármán Cyber Defence accompagne les entreprises dans la mise en place et l'optimisation de leur SOC avec des technologies avancées pour une surveillance et une réponse aux menaces en temps réel.

Les avantages clés

- **Surveillance continue et détection en temps réel :** Analyse avancée des événements de sécurité pour identifier et neutraliser les menaces avant qu'elles ne causent des dommages.
- **Threat Hunting en temps réel :** Exploration approfondie des artefacts collectés pour identifier des schémas d'attaques basés sur MITRE ATT&CK®.
- **Network Detection and Response (NDR) :** Surveillance du trafic réseau pour détecter les comportements suspects et prévenir les intrusions.
- **Gestion proactive des vulnérabilités :** Identification et correction rapide des failles de sécurité pour limiter les risques d'exploitation.
- **Analyse comportementale avancée (UEBA) :** Détection des anomalies grâce à l'intelligence artificielle et au machine learning pour repérer les comportements suspects.
- **Orchestration et automatisation (SOAR) :** Automatisation des réponses aux incidents pour accélérer la remédiation et améliorer l'efficacité du SOC.
- **Connectivité universelle :** Intégration fluide avec toutes les sources de données (APIs, logs, formats personnalisés, événements HTML).
- **Flexibilité et évolutivité :** Adaptation aux environnements hybrides, Cloud et On-Premise, avec une gestion dynamique des ressources.
- **Traitement de données optimisé :** Prétraitement des événements pour réduire le bruit et optimiser le stockage des logs.
- **Conformité et reporting automatisé :** Génération rapide de rapports conformes aux normes ISO 27 001, PCI DSS et autres réglementations.

+100
sources de logs intégrées.

+50 000
événements par seconde traités en temps réel.

+500
règles d'alerte intégrées.

+50
intégrations avec des sources de renseignement sur les menaces tierces.

CTI & DRP

LA VEILLE EN DEHORS DE L'ÉCOSYSTÈME

Kármán Cyber Defence propose une **plateforme avancée de Cyber Threat Intelligence et de protection contre les risques numériques** conçue pour neutraliser les activités de piratage dès leur origine. Dans un contexte de transformation numérique, les menaces ne se limitent plus aux systèmes internes des entreprises : elles s'étendent désormais aux environnements cloud, au télétravail et aux réseaux sociaux.

Cyber Threat Intelligence (CTI)

- Surveillance du Dark Web pour détecter les fuites de données et surveiller les activités d'APT.
- Collecte d'indicateurs de compromission (hashes de malwares, adresses IP malveillantes, vulnérabilités critiques).
- Intégration des standards MISP/STIX/TAXII pour enrichir les analyses dans le SIEM et au sein du SOC.

Digital Risk Protection (DRP)

- Protection de la marque via la détection de typosquatting, de phishing et de sites frauduleux.
- Mise en œuvre de procédures DMCA et coordination avec les hébergeurs/registrars pour le retrait de contenus illicites.
- Gestion de crise avec élaboration d'une stratégie de communication et de mesures juridiques adaptées.

Témoignages clients

BANQUE MULTI RÉGIONALE
CHALLENGE SOCMINT & ANTI-PHISHING

PROBLÈME :

Les clients de la banque ont été touchés par des tentatives de fraude externe par le biais d'attaques de phishing et d'escroquerie sur les réseaux sociaux.

CEO, CFO et CTO souffraient d'usurpation d'identité.

Des données sensibles ont été divulguées par des fuites involontaires.

PLAN D'ACTION :

Adoption d'une approche proactive pour améliorer la sécurité de l'entreprise au lieu de simplement réagir aux attaques.

Mise en œuvre d'un balayage 24 heures sur 24 du Web, Deep Web et Dark Web.

Scan en temps réel pour surveiller en permanence l'empreinte numérique de la marque sur toutes les plateformes de médias sociaux.

RÉSULTATS :

- Désactivation de + de 500 faux groupes WhatsApp et membres malveillants.
- Détection & alerte des clients pour la désactivation de + de 2 500 cartes de crédit divulguées.
- Réduction des activités malveillantes de 99 % sur 2 ans.
- Rapports hebdomadaires et mensuels réguliers.

ENTREPRISE SECTEUR SANTÉ MULTI RÉGIONALE
MALWARE DARK WEB DATA LEAKAGE

PROBLÈME :

Les données des clients et des employés ont été compromises et vendues sur le Dark/Deep Web.

Les enquêtes initiales menées par des tiers n'ont montré aucun signe de compromission de l'environnement du client. Pourtant, leur marque et leur présence en ligne ont été considérablement affectées.

PLAN D'ACTION :

24 heures sur 24, 7 jours sur 7, scan du Web, Deep Web et Dark Web de 10 000 000 identifiants.

Analyse de la fuite de données.

Détection et alerte du client.

RÉSULTATS :

- Les malwares récoltaient des identifiants venant d'ailleurs (courriels personnels et comptes de réseaux sociaux) et ne ciblaient pas spécifiquement l'entreprise.
- Le client a demandé à ses clients de modifier leurs informations d'identification et les a alertés de l'attaque ciblant leurs appareils personnels.
- L'image de l'entreprise a été restaurée et améliorée.

KÁRMÁN

CYBER DEFENCE

KÁRMÁN CYBER DEFENCE

1, allée des Écureuils | 69380 Lissieu, France
+33 (0)4 72 54 88 58 | info@karmancyberdefence.com | www.karmancyberdefence.com