Cybersécurité : KPMG à vos côtés

Notre offre Cybersécurité

Octobre 2021

kpmg.fr

Les axes de notre offre

CYBER IN THE BOARDROOM

Accompagner les directions générales dans la mise sous contrôle des risques Cyber.

TRANSFORMATION DE LA FONCTION CYBER

Accompagner les entreprises dans la mise en place d'une fonction Cybersécurité « World Class ».

SÉCURISATION DE LA TRANSFORMATION NUMÉRIQUE

Aider les entreprises et les métiers à sécuriser, et donc à accélérer, leur transformation numérique.

CYBER RÉSILIENCE

Aider les entreprises à se défendre opérationnellement via des contrôles préventifs, détectifs, curatifs, et la mise à l'épreuve continue de ces contrôles.

Notre offre Cybersécurité

01

VOTRE DÉFI

La technologie rend beaucoup de choses possibles, mais « possible » ne veut pas toujours dire « sûr ».

02

NOTRE RÉPONSE

KPMG peut vous aider à anticiper l'avenir, à aller plus vite et disposer d'une longueur d'avance grâce à des technologies robustes et fiables.

03

POURQUOI KPMG ?

Les professionnels de KPMG sont à vos côtés et vous apporte une combinaison d'expertises technologiques, de connaissance approfondie des métiers et des secteurs pour vous aider à protéger et à développer votre entreprise en répondant à des enjeux potentiellement divergents :

- Résilience et agilité
- Sérénité malgré le risque
- Opportunités malgré les menaces

04

NOTRE AMBITION COMMUNE

Ensemble, nous créons un monde numérique de confiance, pour que vous puissiez repousser les limites du possible.

Cyber in the boardroom

VOS ENJEUX

Les impacts des risques Cyber pouvant être critiques pour les entreprises, les directions générales doivent être assistées pour mettre les risques Cyber sous contrôle, via :

- L'identification et la compréhension des risques Cyber les plus critiques,
- La définition de stratégies de gestion des risques Cyber,
- Le déploiement de programmes de réduction ou de transfert des risques Cyber, et de mise en conformité aux lois et règlements dans le domaine Cyber.

NOS SERVICES

- Évaluation / benchmark de la maturité Cybersécurité de l'entreprise
- Apport d'expertise Cybersécurité aux Conseils d'administration, sensibilisation des dirigeants
- Cartographie globale des menaces, réglementations et risques Cybersécurité, identification des « crown jewels »
- Audit de la fonction Cybersécurité
- Construction de la roadmap Cybersécurité
- Définition d'une fonction Cybersécurité d'excellence
- Mise en place d'une Cyber assurance
- Conception et suivi de programmes de mise en conformité réglementaire (GDPR, LPM/OIV, SWIFT, NIS, HDS, PCI-DSS, PSD2, etc.)
- Simulation de Cybercrises
- Due-diligence Cybersécurité lors d'une acquisition

Transformation de la fonction Cyber

VOS ENJEUX

La fonction Cybersécurité est aujourd'hui reconnue comme un élément critique dans la capacité des entreprises à protéger leur cœur d'activité contre les risques Cyber.

Dans un contexte de transformation numérique des entreprises, elle doit accompagner les métiers et l'ensemble de l'entreprise, et leur fournir des services ou solutions de sécurité de qualité, efficaces et transparents.

Elle doit en outre permettre à la Direction Générale, sur la base d'éléments factuels, de s'assurer que les risques Cyber sont sous contrôle.

NOS SERVICES

- Analyse de risques Cybersécurité (entreprise / IT / projet)
- État des lieux du niveau de Cybersécurité du SI (ISO27002)
- Audits et tests d'intrusions, Red Teaming, cartographie des points de présence sur Internet
- Construction et implémentation de programmes de Cybersécurité
- Mise en place de SMSI (ISO27xxx) et assistance à la certification ISO27001
- Définition et adaptation de gouvernances, politiques, processus, procédures et guidelines Cybersécurité
- Prise en compte de la sécurité dans les méthodologies projet (incluant Agile / DevOps)
- Sensibilisation, formation et accompagnement Cybersécurité (VIP, IT, métiers, développeurs)
- Choix et déploiement d'outils / services / solutions de Cybersécurité (architectures Internet, DRP, SOC, SIEM, IAM, IDS/IPS, DLP, anti-APT, anti-DDoS, Bug Bounty, SIRP)
- Optimisation du pilotage et du reporting de la fonction Cybersécurité (KPI, tableaux de bord)
- Implémentation de programme de mise en conformité réglementaire (GDPR, LPM, SWIFT, NIS, HDS, PCI-DSS, PSD2..)
- Audit du niveau de Cybersécurité de tiers (fournisseurs, prestataires, hébergeurs dont cloud)

Sécurisation de la transformation numérique

VOS ENJEUX

Les métiers se sont emparés de la transformation numérique et sont très actifs dans le domaine des nouveaux services en ligne, des objets connectés et solutions basées sur des technologiques innovantes comme la blockchain.

Dans ce contexte, il est vital pour les entreprises de prendre en compte les risques Cyber dès le début de ces projets, sous peine d'être confronté à des failles de sécurité dont les conséquences pourront être très significatives, tant pour les clients que pour les collaborateurs.

NOS SERVICES

- Sensibilisation des métiers aux risques cyber
- Analyse des risques Cybersécurité relative à un SI/application/service en ligne/app mobile, objet connecté (IoT)/infrastructure
- Test de la sécurité et de la résilience de SI métier/applications/ services en ligne/objets connectés (IoT)/infrastructures, via des tests d'intrusion/revue de configuration/audit de code/audit d'architecture
- Mise en conformité GDPR, LPM/OIV, SWIFT, NIS, HDS, PCI-DSS/PSD2 sur un périmètre métier (analyse de risque, adaptation des processus métier / IT, mise en place des mesures de sécurité, homologation et reporting)
- Amélioration de la cyber résilience d'un processus métier ou d'un service vendu à des clients B2B/B2C (BIA, PRA/PCA, dispositifs anti- DDoS, threat intelligence, SOC métier, gestion de crise, forensic, etc.)
- Sécurisation des SI industriels/SCADA (diagnostic, analyse de risque, plan de sécurisation, organisation, gestion du changement, etc.)
- Intégration de solutions métiers (dont cloud) dans les dispositifs et politique de sécurité de l'entreprise
- Sécurisation d'applications métier (SAP, Oracle)
- Étude des vulnérabilités dans les nouvelles technologies (blockchain, impression 3D, IoT, IA, ZigBee, etc.)
- Audit du niveau de Cybersécurité de tiers (fournisseurs, prestataires, hébergeurs dont cloud)

Cyber résilience

VOS ENJEUX

Les Cyber menaces se transforment, devenant de plus en plus innovantes, mutantes et agiles.

Les attaquants peuvent attendre le moment propice pendant des mois, et frapper en quelques minutes.

Pour rester dans la course face à des attaquants professionnalisés, créatifs et efficaces, le dispositif de Cybersécurité doit s'adapter en permanence, gagner en réactivité et assurer la résilience des processus métier au-delà de la protection de l'IT.

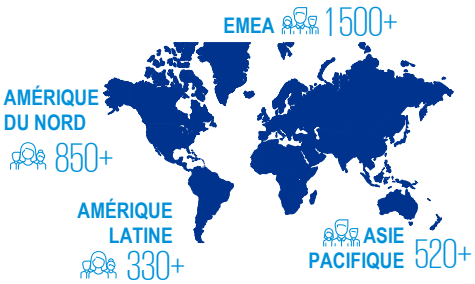
NOS SERVICES

- Revue de la cyber résilience de l'entreprise ou d'un processus métier
- Tests de sécurité sur des infrastructures, réseaux, applications, services web, etc. via des tests d'intrusion (black/grey/white box), audits de code, audits d'architecture, revues de configuration, audits de sécurité physique
- Tests d'intrusion « Red Team » et « PurpleTeam », campagnes de phishing et de social engineering
- Mise à l'épreuve et test d'efficacité des dispositifs de sécurité : SOC, dispositifs anti-DDoS, dispositifs anti-APT
- Revue des habilitations, y compris sur l'analyse des chemins de compromission d'Active Directory
- Accompagnement à la définition de stratégies de tests (tests d'intrusion, scans de vulnérabilités, bug bounty, etc.)
- Conception d'architectures techniques et de processus métiers résilients par rapport aux cyber menaces
- Réponse aux incidents Cybersécurité, gestion de crise, simulation de crise, forensic et reverse-engineering
- Durcissement de technologies et composants du SI, rédaction de guides de sécurisation
- Analyse de l'évolution des menaces, Threat Intelligence

Nos atouts

Une signature reconnue dans le monde entier

Une présence mondiale, avec un réseau de 110 associés et plus de 3200 experts dédiés à la Cybersécurité et la Privacy dans 50 pays



Pour la troisième année consécutive, KPMG leader mondial en Cybersécurité

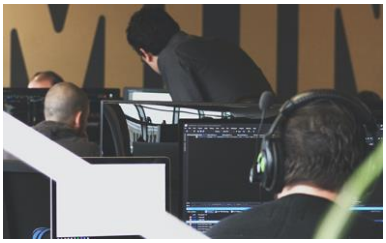
selon l'étude Forrester 2019

KPMG classé parmi les leaders mondiaux en Cyber Sécurité par ALM Intelligence

Nos capacités

Laboratoire Cyber Sécurité

KPMG a construit dans ses locaux parisiens un laboratoire dédié à la Cyber Sécurité. Cet environnement sécurisé est un espace de travail collaboratif facilitant le partage de connaissances et permettant à nos consultants de se former sur de nouvelles technologies, de simuler des environnements particuliers et d'augmenter leur niveau d'expertise technique.



Qualifié PASSI*

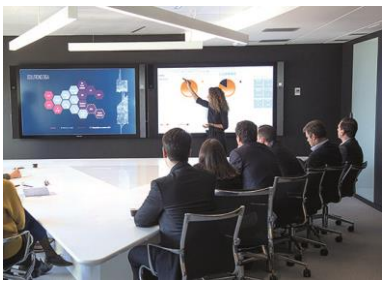
KPMG est qualifié PASSI* par l'ANSSI, ce qui atteste :

- des compétences des auditeurs en charge des audits de sécurité
- de la déontologie des auditeurs,
- de la protection et de la confidentialité des données, rapports et documents échangés
- d'une méthodologie d'audit de sécurité appropriée pour les audits de sécurité

Insights Center

L'Insights Center, un espace collaboratif unique dédié à l'accompagnement de nos clients, notamment sur des enjeux de Cyber Sécurité, propose 3 parcours :

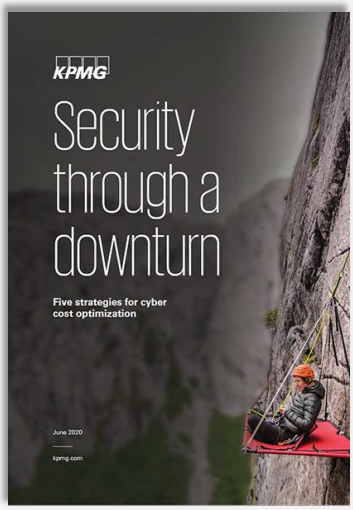
- Awareness cyber,
- Co-Construction (par exemple de cartographie des risques cyber)
- et Simulation de crise cyber.

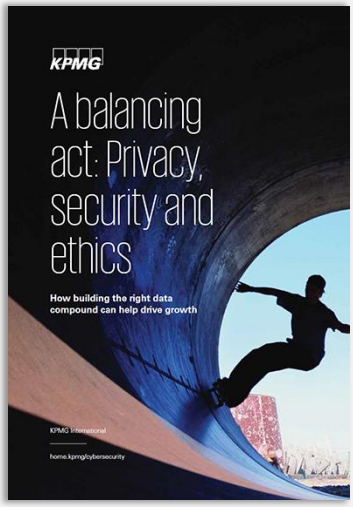


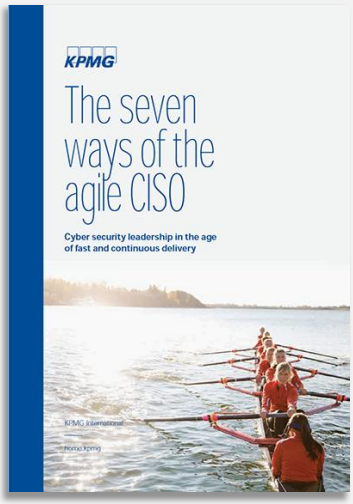
** Les activités faisant l'objet de la qualification PASSI sont les suivantes : audit organisationnel et physique, audit d'architecture, audit de configuration, audit de code source, tests d'intrusion. Toutes nos activités d'audit de sécurité des SI ne sont pas qualifiées PASSI.*

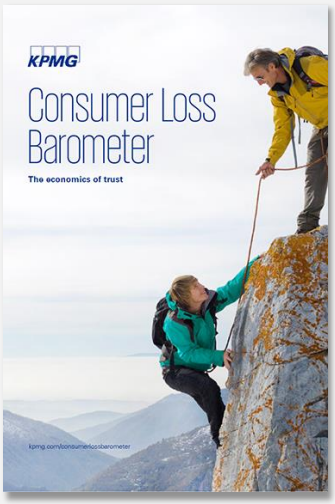
Attestation de qualification N° : 20118. Date de prise : lundi 23 novembre 2020. Fin de validité : dimanche 24 septembre 2023. Version : 3

Nos publications









Contacts

Vincent Maret
Associé
Responsable de l'offre Cybersécurité et Protection des données personnelles

Mob: +33 6 17 12 22 13
Email: vmaret@kpmg.fr

Faycal El Belghami
Associé
Responsable de l'offre Cybersécurité Banques et assurances

Mob: +33 7 77 31 21 60
Email: felbelghami@kpmg.fr

Guillaume Rablat
Directeur
Responsable de l'offre CyberDefense

Mob: +33 6 61 57 21 43
Email: grablat@kpmg.fr

kpmg.fr