



Cybersécurité : La rançon peut attendre !

Notre offre de services dédiée aux secteurs
Financier (banque et assurance) et Public

Contexte et enjeux de la cybersécurité

Toutes les organisations, administrations et entreprises, de toutes tailles et de tous secteurs, sont exposées aux risques cyber et peuvent être victimes d'attaque telles que le **sabotage**, **l'espionnage**, l'atteinte à l'image, la **cybercriminalité** pour ne citer que quelques exemples.

Les menaces se sont multipliées lors de la dernière crise sanitaire et des attaques faisant appel à d'autres technologies comme l'intelligence artificielle sont annoncées.

Parmi vos enjeux prioritaires pour maintenir à un niveau acceptable la sécurité de votre système d'information (SI) et maîtriser vos risques, vous devez, principalement, veiller à :

- **Maintenir en permanence la conformité des SI face aux référentiels normatifs et aux enjeux réglementaires** (ISO 27001, ISO 22301, LPM, RGS, RGPD, HDS, Directive NIS, SWIFT, PCI DSS, DORA, NIST, EIOPA,...),
- **Tester la résilience du SI, évaluer les risques cyber et les impacts sur l'activité en amont des crises** pour être en mesure de concentrer les efforts de défense sur les points critiques de l'activité,
- **Disposer d'éléments factuels et indépendants pour communiquer efficacement vis-à-vis des parties prenantes** (Direction générale, investisseurs, clients, partenaires...).

Une approche modulaire et adaptée

Grant Thornton assiste les entreprises dans toutes les dimensions de leur projet. Forts de leur expérience, d'une approche unique et d'une méthodologie éprouvée en sécurité des systèmes d'information, nos experts **vous accompagnent aussi bien sur des sujets stratégiques, qu'opérationnels et tactiques.**

Nos engagements

- ▷ **Vérifier votre conformité aux réglementations**, normes et standards applicables et la comparer aux meilleures pratiques du secteur,
- ▷ **Evaluer la performance de votre dispositif** de cybersécurité,
- ▷ Emettre des **recommandations afin d'améliorer votre dispositif** en ciblant les axes de travail prioritaires pour une meilleure attribution des ressources,
- ▷ Vous **Accompagner pour une communication pertinente et adaptée** auprès des parties prenantes de votre organisation (opération de levée de fonds, introduction en bourse...).

Notre offre

1. Gouvernance, Risques et Conformité de la Cybersécurité

- Evaluation de la conformité réglementaire (RGPD, RGS, LPM, NIS, HDS, SWIFT, PCI DSS, DORA, etc.),
- Conseil en réglementation pour la direction et l'exécutif,
- RSSI (responsable de la sécurité des systèmes d'information) *as a Service*,
- Analyse de risques,
- *Co-sourcing* et *outsourcing* de l'audit de cybersécurité,
- Revue des fonctions / services informatiques gérés ou de sécurité externalisés.

2. Stratégie et mise en œuvre de la cybersécurité

- Evaluation de la maturité cyber par rapport aux principales normes (ISO 27001/27002, NIST CSF, Guides ANSSI, etc.),
- Préparation à la certification ISO 27001,
- Conception et développement de stratégie cyber,
- Mise en œuvre de programme cyber.

3. Evaluation technique de la sécurité

- Diagnostic de cybersécurité,
- *Due diligence* cyber,
- Evaluation de la vulnérabilité,
- Test d'intrusion,
- Evaluation de la sécurité des applications, des infrastructures et réseaux, des mobiles,
- Revue sécurisée de code,
- Cybersurveillance.

4. Simulation d'attaque

- *Red Teaming*,
- Test d'attaque en situation réelle,
- Campagne de *phishing*.

6. Formation

- Sensibilisation générale à la cybersécurité,
- Sensibilisation ciblée pour le conseil d'administration et la direction.

5. Réponse aux incidents et investigation numérique

- Réponse aux incidents et confinement,
- Analyse et évaluation des violations / compromissions.



Notre expertise, certifiée

Nos collaborateurs possèdent de nombreuses certifications dont :

PECB LEAD PEN TEST PROFESSIONAL

CEH Certified Ethical Hacker

ITIL Foundation V3

CERTIFIED FRAUD EXAMINER

ISO

CISA Certified Information Systems Auditor An ISACA® Certification

OSCP security

PECB LEAD FORENSICS EXAMINER

CISSP

CMMI

CHFI Computer Hacking Forensic INVESTIGATOR

Nos atouts

- ▶ Une expertise sectorielle pointue vous assurant des conseils sur mesure et une opérationnalisation d'exception,
- ▶ Un laboratoire de sécurité intégré à nos locaux pour réaliser des tests d'intrusion, évaluer les solutions de sécurité du marché et établir des comparatifs de produits existants,
- ▶ Une présence territoriale forte dans toutes les métropoles régionales et un réseau international de premier plan.

France



210 M€
de chiffre d'affaires
en 2021



5^{ème}
pays du réseau



60 %
du chiffre d'affaires
en Conseil



23
bureaux



2 105
collaborateurs



125
associés

Monde



6,6 Mds\$
de chiffre d'affaires
en 2021



130
pays



730
bureaux



62 000
collaborateurs



3 535
associés

Vos interlocuteurs

Alexis GRIN

Associé, Cybersécurité
(ISO 27001 LA)

T +33 (0) 1 41 25 91 64

E Alexis.grin@fr.gt.com

Abdel Farid ALE

Directeur Cybersécurité
(CEH, CHFI, CISA, ISO 27001 LA, Lead
Pen Pest Professional,
Lead Forensics Examiner)

E Abdel-farid.ale@fr.gt.com

Frank William NZOUE TOM

Directeur Cybersécurité et IT Risks (CISA,
ISO 27001 LA, ISO 27005 RM)

E Frank.nzouetom@fr.gt.com



grantthornton.fr    

Agnès de Ribet

Associée, en charge du *Marketing*,
de la *Communication*

et du *Business Development*

T +33 (0) 1 41 25 85 85

E agnes.deribet@fr.gt.com

« Grant Thornton » est la marque sous laquelle les cabinets membres de Grant Thornton délivrent des services d'Audit, de Fiscalité et de Conseil à leurs clients et / ou, désigne, en fonction du contexte, un ou plusieurs cabinets membres. Grant Thornton France est un cabinet membre de Grant Thornton International Ltd (GTIL). GTIL et les cabinets membres ne constituent pas un partenariat mondial. GTIL et chacun des cabinets membres sont des entités juridiques indépendantes. Les services professionnels sont délivrés par les cabinets membres.

GTIL ne délivre aucun service aux clients. GTIL et ses cabinets membres ne sont pas des agents. Aucune obligation ne les lie entre eux : ils ne sont pas responsables des services ni des activités offerts par les autres cabinets membres.

© 2022 Grant Thornton. Tous droits réservés. Impression sur papier provenant de forêts gérées durablement. Ne pas jeter sur la voie publique.

Crédit photo : shutterstock (photographies retouchées).