INBONIS RATING
THE CREDIT RATING AGENCY FOR SME

ANALYSE DE LA FILIÈRE SÉCURITÉ INFORMATIQUE

Septembre 2022

INTRODUCTION

La **sécurité informatique** est une branche de la **technologie de l'information** qui protège l'intégrité des systèmes, des réseaux et des données informatiques et s'organise autour de trois piliers clés : le réseau, le hardware et le software. Les risques peuvent être de plusieurs ordres : virus, vers, chevaux de Troie, cyberattaques, attaques par invasion, vol d'identité et de données, devinette de mots de passe, interception des communications électroniques, défaillance des serveurs (pannes d'électricité et de climatisation) etc. Par ailleurs, les entreprises doivent adopter des solutions de sécurité informatique qui sont intégrées dès la phase de conception pour qu'elle soit à la fois proactive et réactive. Si la sécurité informatique traite de la protection et de l'intégrité des technologies de l'information, la **cybersécurité** se concentre sur la protection des données de l'extérieur de la ressource sur Internet. Ainsi, la sécurité informatique doit recouvrir plusieurs aspects :

La sécurité informatique **est devenue prioritaire** dans toutes les économies mondiales, au même niveau que les risques sanitaires, climatiques ou financiers. Par ailleurs, au niveau entreprise, les pertes financières peuvent être importantes, c'est pourquoi, il revient aux dirigeants et aux responsables informatiques d'intégrer pleinement la sécurité informatique dans leur stratégie d'entreprise.

PRINCIPALES MENACES INFORMATIQUES

VECTEURS DE MENACES

- Dispositifs mobiles
- IdO (Internet des Objets)
- Fournisseurs Cloud
- Ingénierie Sociale (activités malveillantes à des fins d'escroquerie)
- Tiers

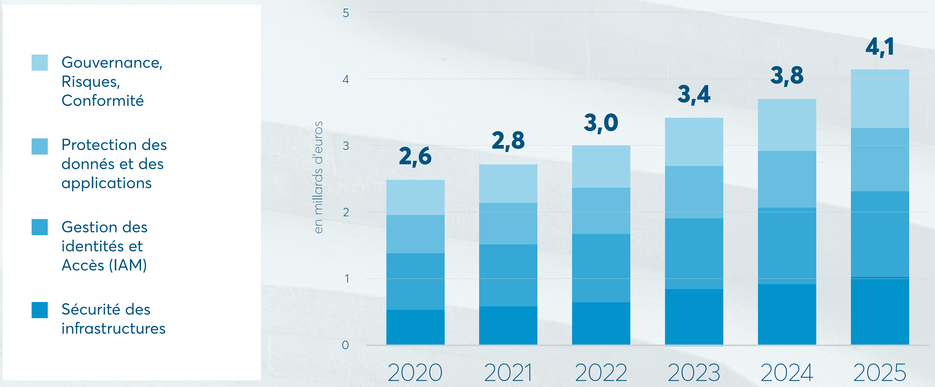
RESPONSABLES DES MENACES

- Cybercriminels
- Hackers/activistes
- États
- Employés (internes, actuels et anciens)
- Tiers et sous-traitants
- Concurrents

CHIFFRES CLÉS

En 2021, la filière de la sécurité informatique représentait 2,8 Md€, et devrait passer à 4,2 Md€ en 2025, soit une moyenne de +11% par an, et +1,4 Md€ en 4 ans. La sécurité informatique au sens large est la filière française la plus dynamique de l'industrie depuis une décennie.

EVOLUTION DU MARCHÉ DES SERVICES DE CYBERSÉCURITÉ 2020-2025



Les services autour de la **protection des données et applications** seront, avec les services autour de la **gouvernance**, des **risques** et de la **conformité**, les segments les plus porteurs. Les services liés à la cybersécurité des environnements Cloud vont quant à eux être en très forte croissance.

PRINCIPAUX SECTEURS QUI ALIMENTENT LA DEMANDE (FRANCE, 2021, %) :

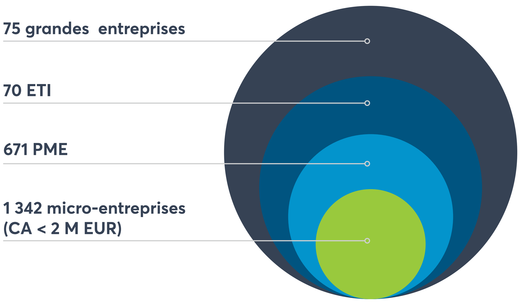
- Secteur public : 19%
- Banque/Finance/Assurance : 19%
- Énergie : 16%
- Transports : 8%

69% des organisations prévoient une hausse des dépenses liées à la sécurité informatique en 2022, versus 55 % en 2021. La prise de conscience du risque informatique gagne de plus en plus les ETI et PME, après avoir d'abord concerné les grands comptes.

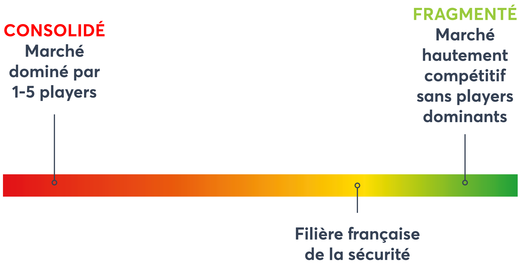
Le niveau de maturité cyber des grandes organisations françaises atteint seulement 46 %, et arrive donc en dessous de la moyenne. En s'appuyant sur les données des dernières cyberattaques traitées, un cabinet spécialisé de premier ordre a pu attribuer un niveau de maturité moyen aux organisations face à ce type d'attaque :

- La moyenne des grandes entreprises est de 54,5 %
- Le niveau moyen est de 46,2 %
- 30 % des organisations sont considérées en situation critique

STRUCTURATION DE L'OFFRE (FRANCE, 2021)



- Filière française fragmentée : 62% des entreprises de la sécurité informatique réalisent un CA < 2 M EUR
- L'entrée régulière de nouveaux acteurs renforce une compétitivité déjà intense
- Dominance de certains champions nationaux : Airbus, Orange, Thales, Atos



Il semble intéressant de se pencher sur une analyse SWOT de la filière de sécurité informatique afin de comprendre les dynamiques qui la traversent :

Forces

- Apparition continue de nouveaux produits disruptifs : IdO, IA, sécurité du Cloud, blockchain, 5G etc. qui augmentent la surface d'attaque globale
- Nouveaux services de résilience numérique (capacité à continuer à fonctionner en cas de panne, piratage etc.) : Zero Trust, architecture maillée de cybersécurité (CSMA) etc.
- Émergence du Security as a Service qui va bouleverser la structure de la concurrence avec une convergence entre logiciel et service

Faiblesses

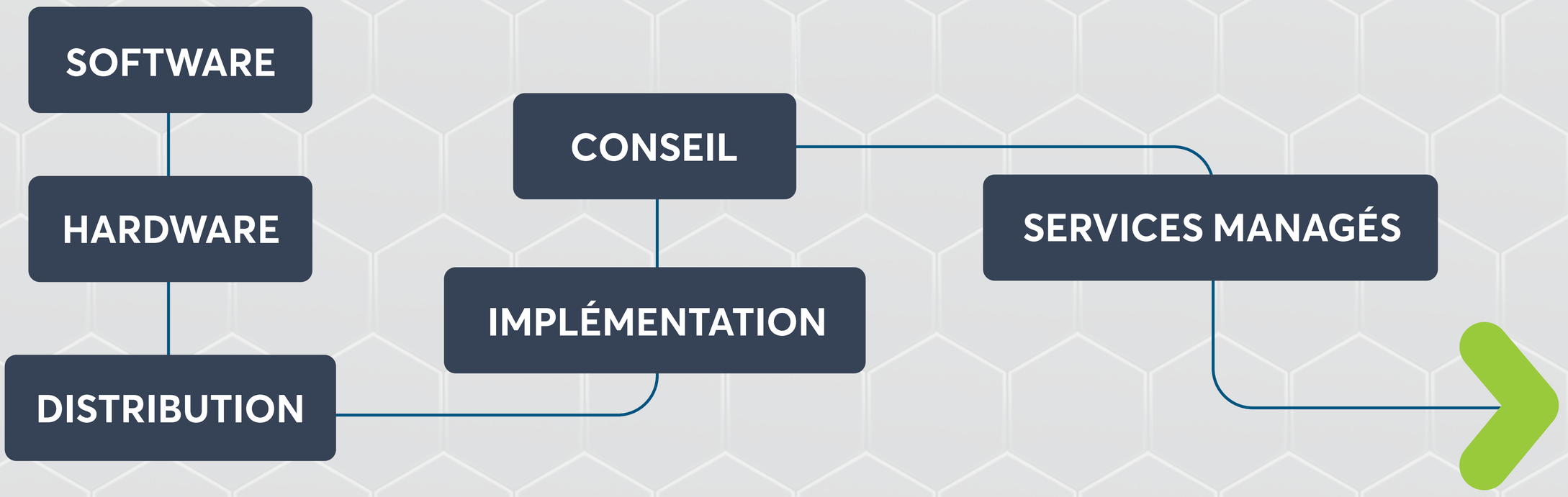
- Limitations des capacités humaines, avec une insuffisance du nombre d'experts et de personnes formées :
  - Au niveau mondial, 4 millions de postes sont restés vacants en 2021. En France, il existe une pénurie de formation professionnelle et de véritables difficultés pour recruter des ingénieurs spécialisés dans la sécurité informatique
  - Fuite de nombreux chercheurs français vers les universités américaines
- Structuration de la filière : prise de contrôle de jeunes pousses tricolores par des groupes étrangers
- En cas de défaillance individuelle de l'un des intervenants de la filière : pertes de CA, discrédit qui affecterait négativement l'ensemble de la filière
- Manque de visibilité et de reconnaissance de l'offre auprès des clients

Opportunités

- Environnement de plus en plus complexe et sophistiqué et phénomènes apparus récemment qui se sont installés dans nos habitudes : télétravail, avec des investissements majeurs concentrés sur la sécurisation des flux, explosion des plateformes de e-commerce et bond des paiements en ligne etc.
- Durcissement au niveau européen (RGPD etc.) avec un renforcement des exigences de sécurité imposées aux secteurs privé et public (services administratifs, infrastructures hospitalières, énergétiques, aériennes ...)
- Investissements nationaux importants à travers plusieurs initiatives :
  - Priorité nationale via le plan d'investissement France 2030 avec entre autres une injection de 200 M€ en fonds propres dans les start-up et PME de la sécurité informatique, une triplication du CA du secteur, et la création de 37 000 emplois d'ici 2025
  - Incubateur ouvert en 2019 dédié à favoriser l'innovation en offrant un hébergement, l'accès à des données d'intérêt cyber et la capacité à tester les solutions avec des experts et des opérationnels du ministère des Armées

Menaces

- Recrudescence des attaques commanditées par des États, même si la France fait partie des pays les plus sûrs au monde en matière de résilience face aux attaques
- Paralysie totale de l'activité, perturbations de la production, pertes financières, atteintes à l'image… qui peuvent précipiter certaines sociétés au redressement judiciaire



Domaines d'intervention

Software

- Sécurité des applications – du Cloud – des données
- Gestion des identités et des accès
- Protection des infrastructures
- Plateformes opérationnelles
- Gestion des risques

Hardware

- Équipements de sécurité des réseaux
- Sécurité
- Équipements/systèmes de sécurité biométrique

Distribution

- Distribution de logiciels ou de matériel de sécurité informatique aux usagers finaux, à des revendeurs ou à des structures fournisseurs de services de cybersécurité B2B

Conseil

- Stratégie cyber et risques
- Conseil et recherche
- Tests, évaluation, conformité et audit, design de processus opérationnels et outils cyber, digital forensic, gestion de projets cyber et renforcement des effectifs
- Recherche sur les vulnérabilités et menaces, développement des standards de sécurité, travaux académiques, formation professionnelle etc.

Implémentation

- Conception du déploiement
- Services d'intégration
- Développement

Services managés

- Solutions managées
- Gestion des dispositifs
- Menaces et vulnérabilités
- Services de cybersécurité virtuels
- Formations

Pour plus d'informations sur les différentes entreprises évoluant sur ce segment de marché, veuillez-vous référer à la matrice sectorielle.

Le montant total des transactions réalisées dans le monde au cours de l'année 2021 pour l'acquisition d'entreprises spécialistes de cybersécurité s'élève à **77,5 Md€**, versus 19,7 Md€ l'année précédente. Le montant des transactions enregistrées au cours de l'année 2021 est largement porté par des **opérations de très grande ampleur.** Les petites entités ayant développé une **technologie innovante** sont également très convoitées par les investisseurs et les grandes entreprises souhaitant développer ou renforcer une partie de leurs services.

Parmi les raisons qui expliquent la forte appétence de la part des investisseurs capital venture et entreprises spécialisées pour les sociétés cyber, se trouve la **digitalisation de l'économie,** la crise sanitaire accélérant la dématérialisation de nombreux process, avec pour corollaire un besoin accru de contrôle et de sécurité des systèmes.

Par ailleurs, tout comme les enjeux et risques ESG, **l'évaluation des risques de cybersécurité** a pris une importance croissante dans la **phase de due diligence** lors d'opérations de M&A. Elle vise à ajuster l'**évaluation de la valeur de l'entreprise cible**, en prenant en compte les risques cybersécurité (interruption ou perturbation de l'activité, fuite de données…), et en analysant leurs éventuels impacts sur les revenus, la part de marché et la réputation, ou encore les coûts de remédiation et les sanctions règlementaires. Si ces éléments ne sont pas traités à leurs justes valeurs, les conséquences pourraient alors être coûteuses :

- Risques cyber non maîtrisés
- Investissements CAPEX et dépenses non budgétés
- Absence de synergies entre le métier et la stratégie IT
- Manque de préparation pour faire face à une crise IT
- Modèle opérationnel IT obsolète ne s'intégrant pas avec la nouvelle structure

+ Niveau de récurrence des contrats signés
+ Taux d'attrition
+ Protection des infrastructures en place
+ Éventuel upsell réalisé
+ Stratégie en place afin de contrer le taux de roulement élevé des employés hautement qualifiés

SUJETS MATÉRIELS ET CONCEPTS CLÉS

Pour le secteur de la sécurité informatique, les sujets ESG jugés prioritaires en termes de matérialité et les concepts qui y sont associés sont les suivants :

1. Les **pratiques professionnelles** incluent des aspects comme le nombre de salariés et de travailleurs non-salariés, la captation et rétention des employés, l'équilibre entre vie professionnelle et vie privée, la qualité des contrats (couverts par une convention collective, contrats à durée indéterminée ou déterminée, durée, rémunération etc.).

2. L'**adaptation** fait référence à la mitigation de la vulnérabilité des systèmes ou territoires au dérèglement climatique, par des actions diminuant les impacts effectifs du changement climatique, ou améliorant les capacités de réponse des sociétés et de l'environnement.

3. La **transparence envers les parties prenantes** fait référence aux directives relatives à la publication d'informations en matière de durabilité des entreprises, la collecte de données non financières, la traçabilité, les systèmes de technologie de l'information, et la transparence avec les parties prenantes.

4. La **diversité et égalité** comprend l'égalité de traitement et des chances, et l'inclusion de toutes les personnes.

5. La **santé et sécurité du consommateur et de l'utilisateur** inclut la sécurité des produits destinés à la consommation.

- **Conflits de priorités : comment conciliez-vous l'utilisation des données utilisateurs afin de proposer des services aux clients et générer des revenus avec le respect de la vie privée associé aux données collectées ?**
- **Subissez-vous vous-même des cyberattaques ou vols de données par des concurrents ?**
- **De nombreux fournisseurs sont localisés dans des pays avec des coûts moindres, aux réglementations et protection des travailleurs limitées : comment gérez-vous ce risque ?**

- **Blockchain** : Mode de stockage et de transmission de données sous forme de blocs liés les uns aux autres et protégés contre toute modification.
- **CA** : Chiffre d'Affaires.
- **CSMA** : Carrier Sense Multiple Access (Écoute d'un Support à Accès Multiple), ou ensemble de protocoles d'accès à un média.
- **IA** : Intelligence Artificielle.
- **IdO** : Internet des Objets.
- **M** : Million.
- **Md** : Milliard.
- **RGPD** : Règlement Général sur la Protection des Données.
- **SaaS** : Software as a Service, soit un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur.
- **Security as a Service** : Technique qui vise à offrir une solution de sécurité informatique externalisée via le Web et non plus en interne.
- **Sécurité du Cloud** : S'assurer que tous les services et données qui résident sur un Cloud seront protégés contre toute violation ou attaque de disponibilité, d'intégrité et de confidentialité.
- **Zero Trust** : Approche de la conception et de la mise en œuvre des systèmes informatiques, en réduisant la confiance implicite.

PROPRIÉTÉ INTELLECTUELLE

Les informations et données incluses dans le présent document sont la propriété d'Inbonis et sont protégées par le droit d'auteur. Pour reproduire, transmettre, transférer, diffuser, traduire, revendre ou stocker en vue d'une utilisation ultérieure à ces fins les informations et les données contenues dans le présent document, il convient de contacter Inbonis, à moins qu'Inbonis n'ait préalablement et expressément autorisé l'utilisation, la reproduction, le transfert, le stockage et/ou la diffusion totale ou partielle du présent rapport.

MÉTHODOLOGIE

Pour l'élaboration du présent document, Inbonis a eu accès à des sources publiques (gratuites et payantes), ainsi qu'à des données quantitatives et qualitatives issues de sa propre base de données.

Les données quantitatives présentées et relatives aux entreprises retenues à titre d'exemple sont issues d'un travail d'échantillonnage indicatif mené sur plusieurs sociétés sélectionnées par code NAF (extraction INPI), sur lesquelles Inbonis a réalisé un travail de sélection et de tri, en fonction des informations disponibles et de critères de taille entre autres, à la date d'émission de ce rapport. Ainsi, ce travail d'échantillonnage pourrait découler sur des résultats différents en fonction de la date d'extraction, des données disponibles à cette même date, et des critères retenus pour cette sélection.

Le présent rapport n'est pas régi par le Règlement (CE) N°1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit. Il ne constitue en aucun cas un avis sur la solvabilité des entreprises prises comme référence dans l'échantillon statistique. Il a été préparé par Inbonis à la demande expresse du destinataire pour son usage exclusif et selon ses conditions.

Les informations et conclusions contenues dans le présent rapport sont fournies à titre indicatif seulement et ne constituent en aucun cas un conseil en investissement ni une recommandation juridique, fiscale ou autre.

ANALYSE DE LA FILIÈRE SÉCURITÉ INFORMATIQUE

INBONIS RATING
THE CREDIT RATING AGENCY FOR SME

+33 685 24 63 95
info@inbonis.com

inbonis.com