

Plus forts ensemble !

La notion de souveraineté gagne du terrain dans les entreprises : près de 8 décideurs IT sur 10 considèrent aujourd'hui que l'enjeu est important pour leurs organisations*. Le gouvernement vient également de lancer « Je choisis la French Tech » avec l'objectif de multiplier par deux le volume de commandes des grandes entreprises aux start-up de la French Tech. Mais qu'en est-il en pratique ?

C'est la raison d'être de ce baromètre lancé par Hexatrust avec la Fédération Française de Cybersécurité auprès de certains de leurs membres : s'assurer que cette prise de conscience se traduit dans les faits par des comportements d'achat souverain chez les grandes entreprises en matière de solutions de cybersécurité et de cloud. L'objectif est ainsi de distinguer les « bons élèves », ceux qui jouent le jeu, non de dénoncer les moins bons. Et pour cela, rien de plus révélateur que les comportements en matière d'achat !

Acheter souverain, ce n'est pas acheter plus cher des solutions moins performantes auprès d'acteurs français. C'est concilier à la fois les exigences de performance opérationnelle et de coût avec la volonté de développer un écosystème français numérique puissant, conforme à nos valeurs et à nos intérêts, seul capable de nous permettre de répondre en même temps aux enjeux de cybersécurité opérationnelle et de résilience. Acheter souverain, ce n'est pas non plus refuser d'acheter des solutions non françaises.

Dans une économie mondialisée, l'auto-suffisance technologique n'existe pas. Il s'agit en revanche de privilégier, à performance et coût identiques des solutions françaises, en particulier pour les composants les plus critiques de nos systèmes d'information.

Mais pour pouvoir grandir et répondre aux besoins de nos clients, les éditeurs que nous sommes ont besoin avant toute chose de contrats, tant publics que privés. Les grandes entreprises doivent à cet égard jouer un rôle clé, au départ pour nous permettre d'éprouver nos solutions autour de leurs cas d'usage, mais aussi pour nous permettre d'atteindre des tailles critiques. Bien sûr, les obstacles existent : éclatement des solutions, scalabilité insuffisante, manque d'interopérabilité etc. Mais les solutions à ces défis existent et nous ne pourrions les résoudre que tous ensemble, start-up, PME, ETI et grands groupes. C'est à cette condition que les objectifs du Plan Cybersécurité lancé par le Président de la République en 2021 (tripler le chiffre d'affaires du secteur et créer 37 000 emplois d'ici 2025) seront atteints !

Jean-Noël de Galzain Président d'Hexatrust
David Ofer Président de la Fédération Française de Cybersécurité

*Enquête menée par Jamespot, éditeur français de solutions collaboratives en novembre 2022

Les 20 sociétés françaises qui achètent le plus de solutions souveraines

Classement des entreprises françaises du SBF 120 en fonction du nombre de contrats signés avec les éditeurs français membres d'Hexatrust et de la FFCYBER

- | | | | |
|----|--|----|---|
| 01 |  | 03 |  |
| 02 |  | 05 |  |
| 04 |  | 07 |  |
| 06 |  | 09 |  |
| 08 |  | 11 |  |
| 10 |  | 13 |  |
| 12 |  | 15 |  |
| 14 |  | 17 |  |
| 16 |  | 19 |  |
| 18 |  | | |
| 20 |  | | |

en partenariat avec



Baromètre de la souveraineté numérique

2023

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY



en partenariat avec



Ce baromètre exploite les résultats d'une enquête conduite en partenariat avec l'École de Guerre Économique auprès d'un panel de 25 entreprises membres d'Hexatrust et de la Fédération française de cybersécurité du 15/06/2023 au 31/07/2023. Cette enquête a pour objectif de classer les entreprises de l'indice boursier **SBF 120 en fonction du nombre de contrats** (à l'exclusion des démonstrateurs et *Proof of Concept*) passés auprès de fournisseurs de solutions de cybersécurité et de numérique de confiance membres d'Hexatrust et de la Fédération Française de Cybersécurité.

Points clés

Alors qu'elles éprouvent souvent des difficultés à contractualiser avec des start-up et PME (les obstacles étant principalement la scalabilité et la praticité des solutions ainsi que la pérennité des structures), **les grandes entreprises joignent de plus en plus la pratique à la théorie en matière de souveraineté numérique.**

Le nombre de contrats (hors démonstrateurs et *Proof of Concept*) signés par les grands groupes avec les éditeurs français de cybersécurité et de solutions *cloud* progresse ainsi depuis quelques années. **Outre la popularisation de la notion de souveraineté numérique, cette évolution dans les comportements d'achat s'explique aussi par la maturité croissante des solutions françaises, tant au plan technique et opérationnel qu'en termes marketing.** Ces solutions sont aujourd'hui non seulement performantes mais aussi compétitives.

Autre point positif : **les grandes entreprises identifiées dans ce classement appartiennent à des secteurs très divers.** Sont ainsi représentés

la banque avec Crédit Agricole (en 1^{ère} position), BNP Paribas et Société Générale, traditionnellement gros acheteurs de solutions de cybersécurité, l'industrie (avec Airbus, en 2^e position, Dassault, Thales ou Alstom), les télécommunications (avec Orange, en 4^e position), les entreprises de services numériques (avec Sopra Steria, en 9^e position, et Atos, à la 10^e place), l'énergie (avec Engie ou Totalenergies) ou encore le luxe (avec LVHM, en 15^e position). Apparaissent enfin des entreprises dans lesquelles l'Etat est actionnaire comme ADP (3^e position) ou FDJ (14^e position).

Malgré ces tendances encourageantes, le nombre moyen de contrats signés par les entreprises du panel auprès des grandes entreprises reste relativement faible (4,3). Leur montant apparaît aussi relativement faible. Par ailleurs, les entreprises du SBF 120 apparaissant aux 20 premières places de ce classement sont principalement des très grandes entreprises (8 sur 10 d'ailleurs appartiennent ainsi à l'indice CAC 40).

Louis Fleuret,
Directeur-adjoint, La French Tech

QUEL EST L'OBJECTIF DU PROGRAMME « JE CHOISIS FRENCH TECH » ?

- ▶ **Doubler la commande publique et privée** en direction des start-ups à l'horizon 2027
- ▶ **500 entreprises partenaires** d'ici fin 2023, 5000 en 2027

Ces ambitions sont nées du double constat que la diffusion des technologies des start-up dans nos administrations et nos entreprises est indispensable pour que chacun bénéficie de ces innovations, et que le soutien aux revenus est un levier indispensable pour développer l'écosystème French Tech.

QUELS SONT LES ENGAGEMENTS PRIS PAR LES ENTREPRISES PARTENAIRES DU PROGRAMME ?

255 entreprises (dont 108 grands groupes) se sont engagées à choisir la French Tech. Elles sont divisées en deux catégories :

- ▶ Les entreprises « partenaires », qui s'engagent à doubler leurs achats start-ups à l'horizon 2027
- ▶ Les entreprises « soutien », qui prennent des engagements de moyens pour soutenir les initiatives de La French Tech (désignation d'un référent start-up, mise en place d'un processus d'achat accéléré, doublement du nombre de start-ups référencées en tant que fournisseurs, organisation d'événements)

Certains membres d'Hexatrust figurent parmi ces entreprises. Atempo et Vade Secure se sont engagées en tant qu'entreprises « partenaires » et Docaposte et Inetum participent en tant qu'entreprises « soutiens ». Nous sommes ravis de constater que notre intérêt pour ce programme est partagé par nos membres et, sans nul doute, de nombreux autres viendront grossir les rangs.

La souveraineté numérique, une composante clé du numérique responsable

Loreline DESCORMIERS,
Chief of Staff, WALLIX Group

COMMENT DÉFINIR LA RESPONSABILITÉ NUMÉRIQUE DES ENTREPRISES ?

Les technologies numériques induisent des bouleversements humains, économiques, sociétaux, éthiques, géopolitiques, environnementaux, juridiques. Les entreprises doivent donc intégrer à leur pilotage une stratégie numérique responsable.

Le but est de mettre en place des pratiques respectant un certain nombre de principes et valeurs liés à la conception, la réalisation, la commercialisation, la promotion, l'exploitation de processus, services et produits intégrant du numérique. C'est un élément clé de la confiance de tous les usagers pour un numérique transparent, sécurisé et durable, et donc le développement de nouveaux usages de confiance.

QUELLES SONT LES GRANDES COMPOSANTES DE CETTE RESPONSABILITÉ ?

On peut distinguer :

- ▶ La responsabilité environnementale liée à l'empreinte carbone du numérique
- ▶ La responsabilité éthique liée aux algorithmes et à l'intelligence artificielle
- ▶ La responsabilité réglementaire liée à la cybersécurité et à la protection de la vie privée
- ▶ La responsabilité sociétale relative à l'ouverture des données, à la transformation des modes de travail, à l'achat responsable et à la souveraineté numérique

La « Responsabilité Numérique des Entreprises » (RNE) doit appréhender la transition numérique au regard de ces enjeux et s'inscrire dans la stratégie RSE des entreprises.

La RNE s'exerce dans des champs nombreux liés à l'usage des moyens informatiques et digitaux dont disposent les entreprises et notamment dans le cadre d'une politique d'achat de services et produits numériques de confiance.

L'avenir des organisations passe par un usage du numérique transparent et rassurant pour tous.