OPIIEC

Observatoire des métiers du Numérique,
de l'Ingénierie, du Conseil et de l'Evènement

RAPPORT D'ÉTUDE

ETUDE SUR LES BESOINS EN COMPETENCES, EMPLOIS ET FORMATIONS EN MATIERE DE CYBERSECURITE EN FRANCE

#Cybersécurité
#CyberTalent
#NIS2
#NouvellesTechnologies
#Offshoring

vendredi 11 avril 2025

NUMÉRIQUE

SOMMAIRE

Introduction

CONTEXTE ET OBJET DE LA MISSION

▲ L'Observatoire Paritaire des Métiers du Numérique, de l'Ingénierie, des Études et du Conseil (OPIIEC) a souhaité mener une étude approfondie sur les besoins en compétences, les emplois et les formations liés à la cybersécurité en France. Cette mission s'inscrit dans un contexte marqué par une augmentation significative des cybermenaces, la sophistication des attaques et l'émergence de nouvelles technologies telles que l'intelligence artificielle (IA).

L'OPIIEC, en tant qu'association loi 1901, fédère les organisations patronales SYNTEC et CINOV ainsi que les représentants syndicaux CFE/CGC/FIECI, CFDT/F3C, CGT, CFTC/MEDIA+ et FEC/FO. Ses actions s'articulent autour de trois axes principaux : l'état des lieux, la prospective et la communication sur les thématiques d'emploi et de formation.

▲ Un enjeu stratégique pour les entreprises :

La cybersécurité constitue un enjeu stratégique pour les entreprises françaises, qu'il s'agisse d'acteurs majeurs ou de petites structures. Ces entreprises doivent non seulement lutter contre des agressions malveillantes, mais aussi se préparer à des réglementations de plus en plus strictes, comme la directive européenne NIS2. Dans ce contexte, la formation et le développement des compétences apparaissent comme des leviers fondamentaux pour assurer la résilience des organisations face aux cybermenaces.

Cependant, malgré une offre de formation en plein essor, celle-ci reste fragmentée et manque de lisibilité, rendant indispensable une réflexion prospective sur les métiers et les compétences nécessaires à court et moyen terme

▲ Dans ce contexte, les objectifs de l'étude ont consisté à :

- **Analyser l'état des lieux** des besoins en compétences et formations dans le secteur de la cybersécurité.
- **Évaluer les enjeux prospectifs** liés à l'évolution des technologies et des pratiques en matière de cybersécurité.
- **Proposer un plan d'action** concret pour structurer l'offre de formation et accompagner les entreprises dans leur transition numérique sécurisée.

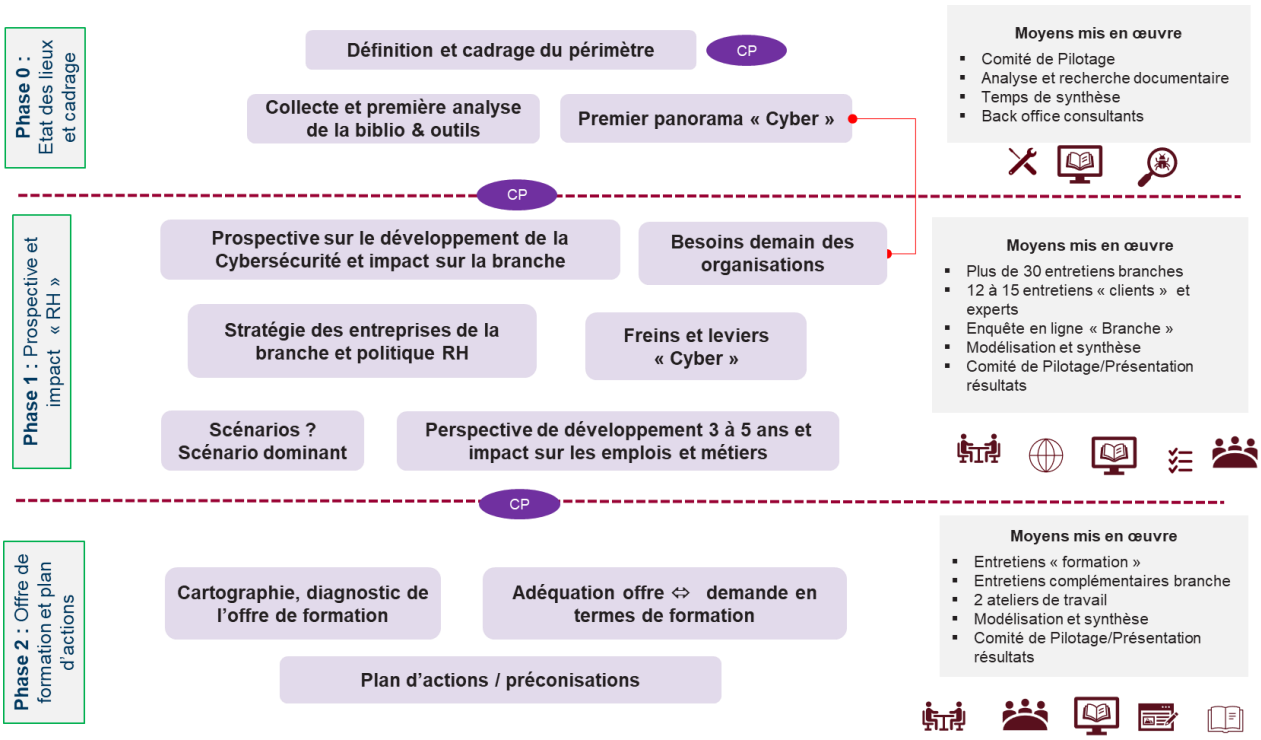
▲ La mission s'est déroulée en trois grandes étapes :

- **Phase 1 : État des lieux et cadrage** – Analyse documentaire, entretiens avec les acteurs de la branche et synthèse des besoins actuels.
- **Phase 2 : Prospective et impacts RH** – Étude des scénarios de développement à moyen terme et des enjeux en ressources humaines.
- **Phase 3 : Offre de formation et plan d'action** – Élaboration d'une stratégie de formation et recommandations pratiques pour accompagner les acteurs du secteur

La méthodologie adoptée est rappelée dans les lignes qui suivent et résumée dans le schéma méthodologique de bas de la page.

- La première phase s'est principalement appuyée sur une analyse documentaire approfondie pour s'imprégner du contexte et traiter toutes les données existantes.
- La deuxième phase de prospective autour des métiers et des compétences a largement mobilisé les acteurs de la filière. C'est ainsi 51 entretiens qualitatifs avec des acteurs de la branche de la cybersécurité qui ont été menées, complétés par des interviews avec une douzaine de clients de la branche. Les premiers constats ont par la suite été étayés par le lancement d'une enquête en ligne à destination des acteurs de la branche.
- La troisième étape fut dédiée à construire un plan d'action focalisé sur les questions « RH » en ayant préalablement analysé plus en profondeur l'offre de formation. Pour alimenter la réflexion, l'équipe de consultant a mené des entretiens complémentaires avec des acteurs de la formation et animé 2 ateliers de travail sur les enjeux et les pistes d'actions en lien avec l'emploi, le développement des compétences et la formation.

Schéma de l'intervention

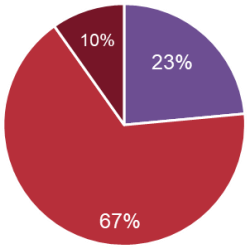


▲ L'échantillon des entretiens qualitatifs menés se décompose ainsi :

- 34 entretiens menés auprès d'entreprises du secteur de la cybersécurité.
- 12 entretiens menés auprès d'une diversité de clients du secteur, tant en termes de secteurs d'activité que de taille d'entreprises ;
- 5 entretiens menés après d'établissements de formation initiale ou continue.

Entretiens qualitatifs réalisés

Répartition des acteurs/structures interrogés

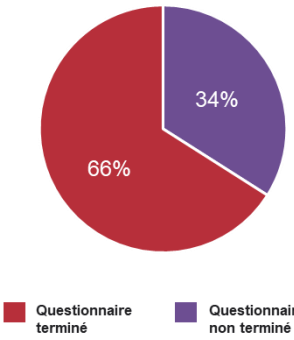


126 personnes contactées…

51 entretiens qualitatifs effectués

+ retours d'information de premier niveau

Enquête en ligne



Icône utilisée tout au long du rapport pour faire référence aux données extraites de l'enquête en ligne :

▲ Les questionnaires ont globalement été bien renseignés avec 66% des questionnaires entièrement complétés. Le panel de réponses permet ainsi de dégager des grandes tendances, bien qu'il convient de rester vigilant quant à la validité statistique des résultats. L'échantillon comporte une forte proportion d'ESN et d'éditeurs de logiciels (respectivement 38 % et 30 %). A noter que les répondants occupent pour plus de 80% une fonction de direction ou une fonction salariale (notamment RH), apportant de la crédibilité aux réponses obtenues (acteur au cœur des enjeux de la montée en compétences des salariés de l'entreprise).

▲ Pour une meilleure interprétation des résultats, il est nécessaire de rappeler les définitions des différentes activités et types d'entreprises présents dans l'échantillon. Ces précisions permettent d'apporter un cadre de référence pour mieux comprendre la typologie des répondants et la portée des réponses recueillies :

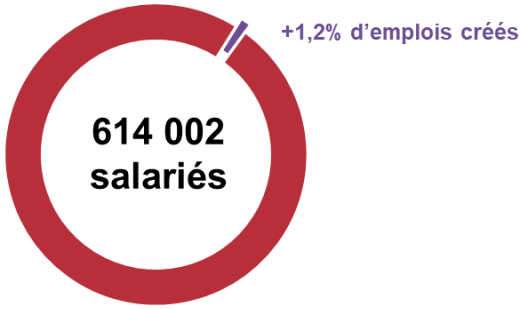
- Editeurs de logiciels : « Ils conçoivent, développent et commercialisent les programmes nécessaires au fonctionnement de tous les équipements numériques, qu'il s'agisse notamment de logiciels d'infrastructure ou de logiciels d'application. », Source : Numeum
- Entreprises de services numériques (ESN) : « Les Entreprises de Services du Numérique sont expertes dans le domaine des nouvelles technologies et du numérique. Elles peuvent englober plusieurs métiers (conseil, conception et réalisation d'outils, maintenance ou encore formation). Elles ont pour objectif principal d'accompagner une société cliente dans la réalisation d'un projet. Elles proposent des prestations qui sont destinées à améliorer le fonctionnement et les infrastructures internes de leurs clients, leurs outils et leurs process de gestion et d'administration.», Source : Numeum
- TPE (Très Petite Entreprise) : une entreprise de 0 à 9 salariés avec un chiffre d'affaires inférieur à 2 millions d'euros, Source : INSEE (rattaché au terme de microentreprise par l'Insee selon l'article 51 (n°2008-1354) de la loi de modernisation de l'économie)
- PME (Petite ou Moyenne Entreprise) : une entreprise de 10 à 249 salariés avec un chiffre d'affaires inférieur à 50 millions d'euros, Source : INSEE

CHIFFRES CLES DE LA « BRANCHE » / SECTEUR DU NUMERIQUE

- Les données présentées dans cette section sont issues des chiffres du numérique publiés par l'OPIIEC en mars 2025. Elles offrent un aperçu global de la **situation actuelle dans le secteur du numérique en France**, en mettant en lumière les dynamiques d'emploi, les évolutions des métiers et les compétences les plus recherchées. Ces chiffres permettent d'évaluer les tendances du marché, d'identifier les tensions en matière de recrutement et de mieux comprendre les besoins en compétences, notamment dans les domaines liés à la cybersécurité.

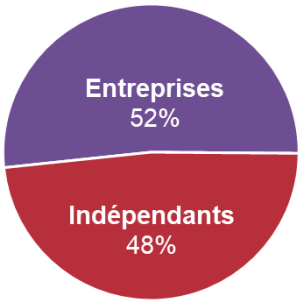
- Le secteur du numérique en 2024 continue de jouer un rôle central dans l'économie française avec 614 002 salariés enregistrés. On observe une **croissance de 1,2 % des emplois** créés malgré une baisse marquée de 9,0 % des offres d'emploi. Cette dynamique illustre un marché en mutation, porté par des besoins en compétences spécifiques et des évolutions rapides dans les technologies numériques.

NOMBRE D'EMPLOIS DU NUMÉRIQUE EN 2024

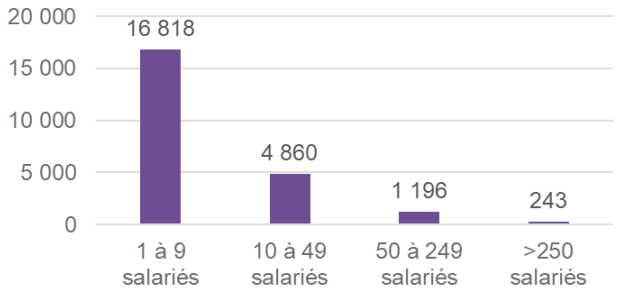


- Le paysage professionnel du numérique se répartit de manière équilibrée entre entreprises (52 %) et travailleurs indépendants (48 %). Cette répartition reflète la diversité des modèles économiques dans le secteur, avec une forte présence d'entreprises de petite taille. La majorité des structures comptent entre 1 et 9 salariés, ce qui met en lumière l'importance des TPE et PME dans l'écosystème numérique.

RÉPARTITION DES ETABLISSEMENTS ENTRE ENTREPRISES ET INDÉPENDANTS EN 2024



NOMBRE D'ENTREPRISES PAR TAILLES D'ENTREPRISES EN 2024



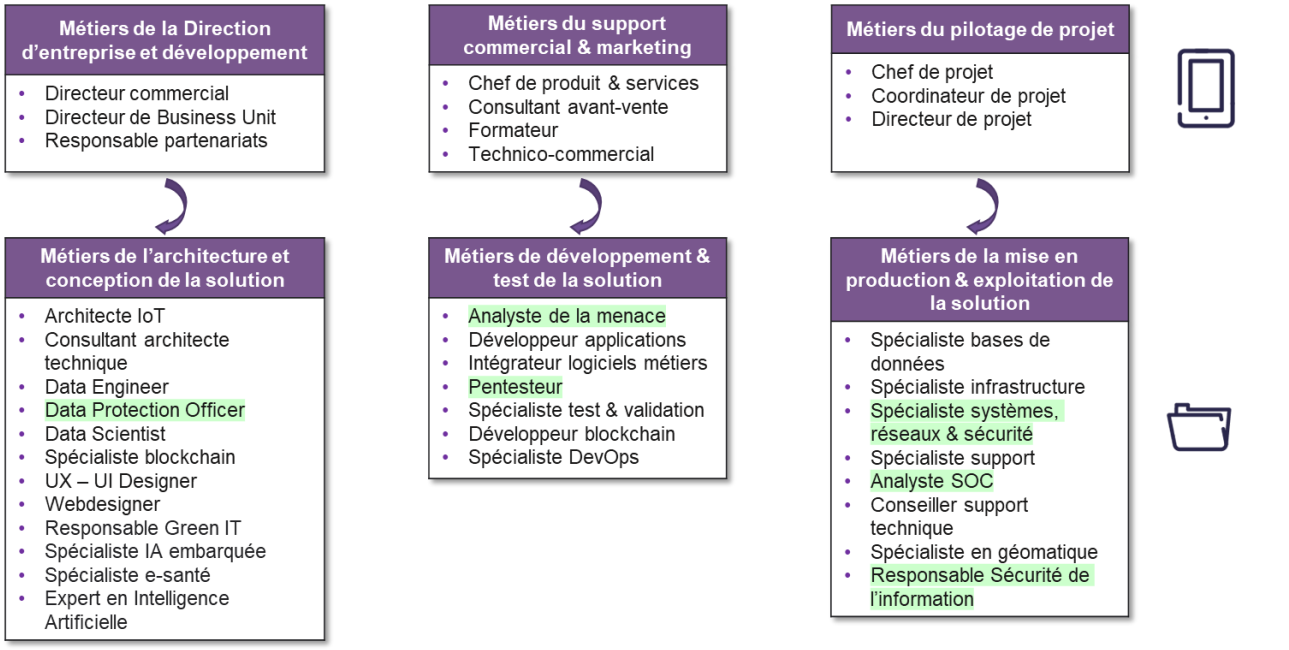
- Au-delà de la répartition des emplois et des structures, l'analyse met également en lumière les attentes des recruteurs en matière de compétences. Elles témoignent des priorités du secteur pour répondre aux défis technologiques et organisationnels actuels. Les compétences les plus recherchées dans le secteur sont liées à l'innovation, à la gestion de projets et à la conduite du changement. Piloter des projets complexes, concevoir des stratégies commerciales et encadrer des équipes figurent parmi les attentes prioritaires des recruteurs. Cependant, les statistiques **montrent peu de compétences spécifiquement identifiées en lien direct avec la cybersécurité**. Les besoins semblent davantage orientés vers la gestion d'infrastructures et de matériels informatiques, intégrant indirectement des volets liés à la cybersécurité dans la pratique. Ce constat interroge sur la visibilité et la **reconnaissance des compétences en cybersécurité dans les fiches de poste et les recrutements actuels**.

CARTOGRAPHIE DES METIERS DU NUMERIQUE (NOVEMBRE 2024)

- La cartographie des métiers du numérique, issue des travaux de l'OPIIEC et mise à jour en octobre 2024, dresse un panorama détaillé des fonctions et spécialités qui structurent ce secteur. Elle met en lumière les principaux rôles professionnels, allant de la direction d'entreprise au développement, en passant par la production et l'exploitation des solutions.

  Cette classification inclut d'ores et déjà des métiers directement liés à la cybersécurité (surlignés ci dessous), soulignant ainsi l'importance croissante de cette thématique dans l'écosystème numérique.

Cartographie OPIIEC des métiers du numérique / Rappel (source site internet)



- La cybersécurité, bien que souvent associée à des métiers spécifiques tels que l'analyste de la menace, le pentesteur, l'analyste SOC, et le responsable de la sécurité de l'information, englobe en réalité une gamme beaucoup plus large de rôles essentiels. Ces métiers, qui relèvent principalement de l'anticipation, la détection et la réponse aux cybermenaces, sont cruciaux dans le cadre de la sécurisation des systèmes numériques. La cybersécurité ne se limite donc pas seulement à ces postes techniques.
- En effet, des fonctions telles que la gouvernance, la gestion des risques, et la réponse aux incidents jouent également un rôle fondamental dans la gestion des enjeux sécuritaires. Ces expertises, bien que moins visibles dans cette première classification (détail dans la partie 2 .3 du présent document), sont tout aussi importantes pour assurer une protection globale et durable des infrastructures numériques. Ces rôles sont nécessaires pour garantir une approche systémique de la cybersécurité, allant au-delà des interventions techniques pour inclure des dimensions stratégiques et organisationnelles essentielles à la résilience des entreprises face aux cybermenaces.

PARTIE 1.
PANORAMA DE LA CYBERSECURITE

1.1.CYBERSECURITE : DEFINITION ET CHIFFRES CLES

1.1.1. DEFINITION

- La cybersécurité est un univers aux multiples dimensions qui englobe des aspects techniques, organisationnels, stratégiques et juridiques. Elle vise à protéger les systèmes d'information, les réseaux et les données contre les cyberattaques, tout en garantissant la confidentialité, l'intégrité et la disponibilité des informations. Cette section propose plusieurs définitions afin d'illustrer la diversité des approches et de mieux cerner les enjeux liés à la cybersécurité.

Les enjeux « **cyber** » vont bien au-delà des modalités techniques. La cybersécurité mobilise notamment la gestion des risques, le droit, les finances, la communication, etc.

Source : ANSSI

La cybersécurité va concerner les usages défensifs et offensifs des systèmes d'information. Elle prend en compte les contenants, utilisés pour l'échange de données, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques.

Source : Nicolas Arpagian (Expert)

Une approche de **cybersécurité** efficace offre de multiples niveaux de protection répartis sur les ordinateurs, les réseaux, les programmes ou les données que l'on a l'intention de sécuriser. Dans une entreprise, les personnes, les processus et la technologie doivent se compléter les uns les autres pour créer une protection efficace contre les cyberattaques.

Source : Cisco

La cybersécurité désigne l'ensemble des technologies, mesures et pratiques visant à protéger les systèmes informatiques, les réseaux et les données contre les cyberattaques

Source : Wikipédia

La cybersécurité vise à protéger les systèmes, les applications, les équipements informatiques, les données sensibles et les actifs financiers des individus et des organisations contre les virus informatiques, contre les attaques de ransomwares, sophistiquées et coûteuses, et plus encore.

Source : IBM

La cybersécurité : C'est l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, etc.

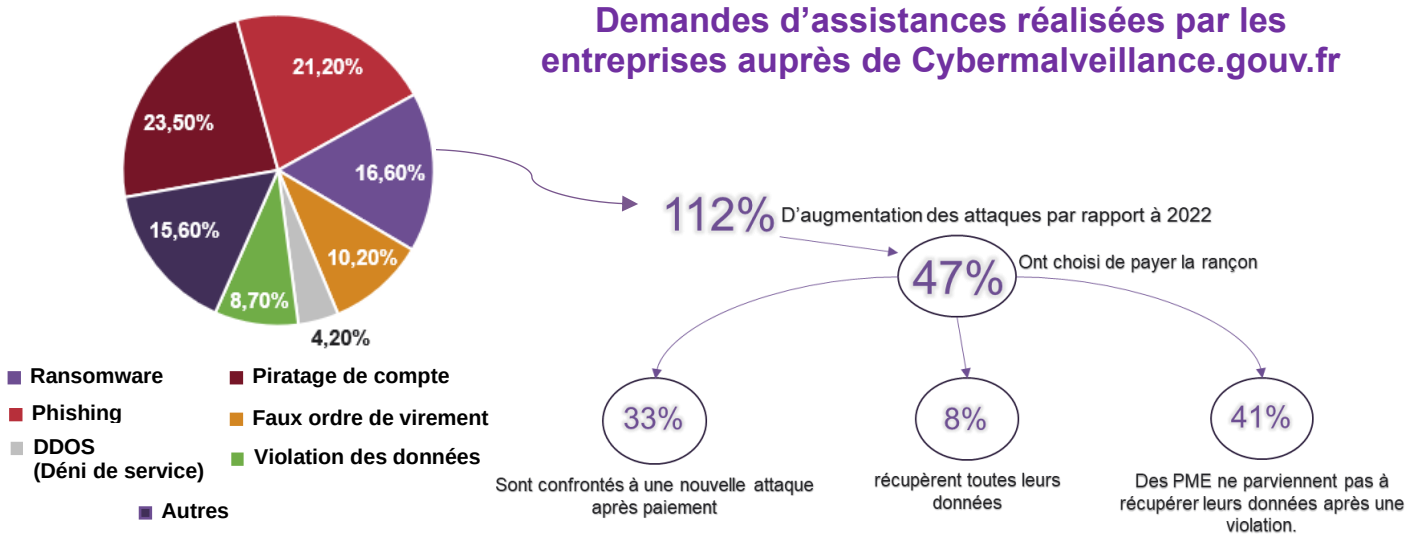
Source : Le Robert

- Les définitions supra montrent que la cybersécurité dépasse largement les aspects purement techniques pour intégrer des dimensions stratégiques, organisationnelles et juridiques essentielles. Par ailleurs, la cybersécurité ne se limite pas à de simples mesures défensives. Elle répond également sur des approches proactives, telles que le pentesting (simulations d'attaques), visant à anticiper et déjouer les cybermenaces. Le facteur humain rappelé dans deux des définitions supra demeure trop souvent relégué au second plan, alors même qu'il est un maillon essentiel dans la mise en œuvre des politiques de sécurité. La lecture des définitions met aussi en évidence la complexité croissante des enjeux liés à la cybersécurité, dans un monde toujours plus interconnecté. On notera enfin que les différentes définitions présentent un consensus sur son importance capitale à l'échelle mondiale.

1.1.2. CHIFFRES CLES DE LA CYBERSECURITE

ATTAQUES ET MENACES

- Cette section présente un panorama des principales menaces et incidents de cybersécurité signalés par les entreprises, basé sur les données de « Cybermalveillance.gouv.fr ». Ces chiffres illustrent l'ampleur croissante des cyberattaques, leurs impacts sur les organisations et les vulnérabilités les plus fréquemment exploitées. Ils soulignent également les comportements et décisions adoptés par les entreprises face à ces menaces, ainsi que les causes sous-jacentes des failles de sécurité.

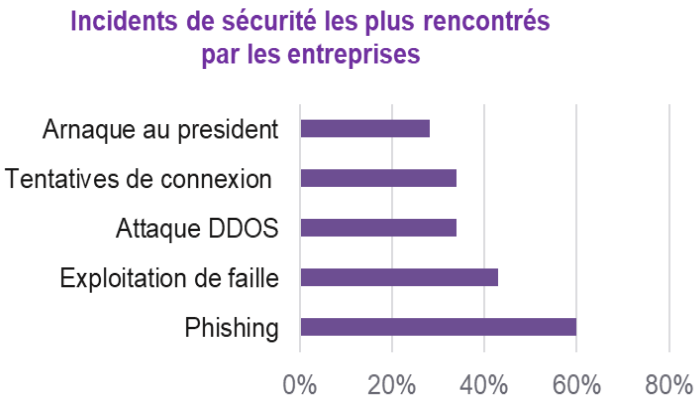


- Les ransomwares continuent de représenter une menace majeure pour les entreprises, avec une augmentation de 112 % des attaques par rapport à 2022. Cette hausse témoigne de l'intensification des tentatives d'extorsion, où les données sont prises en otage contre des rançons. Face à ces attaques, 47 % des entreprises ont choisi de payer la rançon, espérant récupérer leurs données. Néanmoins, 33 % d'entre elles ont été confrontées à une nouvelle attaque même après avoir payé, soulignant l'inefficacité de cette stratégie et le risque d'encourager davantage les cybercriminels.

  De plus, seulement 8 % des entreprises ayant payé ont réussi à récupérer l'intégralité de leurs données, laissant la majorité d'entre elles avec des pertes partielles ou irrécupérables. Ce constat est encore plus alarmant pour les PME, dont 41 % ne parviennent pas à restaurer leurs données après une violation, ce qui fragilise durablement leur activité et leur crédibilité.

- Les attaques par phishing, quant à elles, se classent parmi les incidents les plus fréquemment signalés par les entreprises. Exploitant majoritairement des failles humaines, elles soulignent l'impérieuse nécessité d'une sensibilisation accrue et d'une formation continue des employés afin de renforcer la résilience organisationnelle face à ces menaces.

- Les exploitations de failles et les attaques DDoS sont également des menaces fréquentes. En particulier, 90 % des attaques DDoS recensées sont désormais appuyées par des outils d'intelligence artificielle (IA), ce qui augmente leur efficacité et leur capacité à contourner les défenses traditionnelles. Cette automatisation croissante des attaques impose une adaptation rapide des stratégies de défense des entreprises.



▲ Près de 49 % des cyberattaques atteignent malheureusement leur objectif, ce qui démontre des vulnérabilités persistantes dans les systèmes d'information des entreprises. En 2023, on recensait environ 330 000 attaques réussies contre des PME, confirmant que ces structures sont particulièrement exposées aux menaces. 23 % des entreprises déclarent en outre avoir constaté une augmentation des attaques, tandis que 65 % ont subi des conséquences directes sur leurs opérations.

Les causes principales des failles de sécurité proviennent souvent de l'intérieur des organisations elles-mêmes. Parmi elles, on dénombre que :

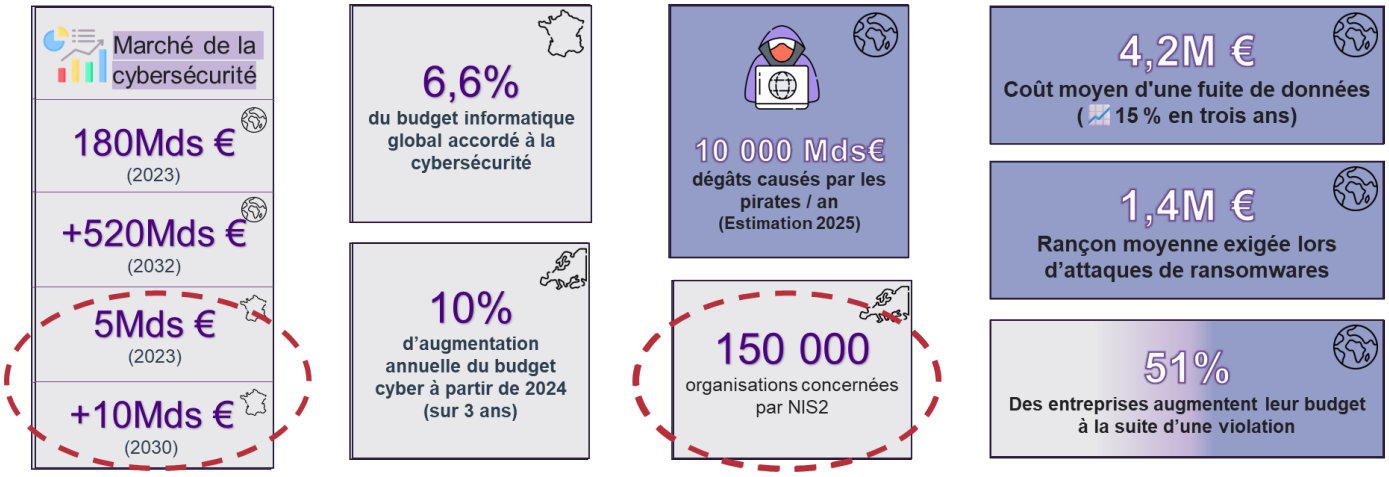
- 35 % des incidents sont liés à l'utilisation d'applications non approuvées, exposant les systèmes à des vulnérabilités non contrôlées.
- 34 % résultent de vulnérabilités résiduelles non corrigées, soulignant un manque de mises à jour et de gestion proactive des correctifs.
- 33 % sont attribués à des erreurs humaines, qu'il s'agisse de configurations mal réalisées ou d'erreurs de manipulation.

77% des répondant estiment être bien ou très bien informés des menaces de cybersécurité qui pèsent sur leur entreprise, mais seulement 66% estiment y être bien ou très bien préparés

MARCHE ET INVESTISSEMENTS AUTOUR DE LA CYBERSECURITE

▲ La cybersécurité est devenue un pilier existentiel pour les entreprises, soutenue par une croissance continue des budgets. En 2023, les dépenses mondiales en cybersécurité ont atteint 180 milliards d'euros, avec une projection à 520 milliards d'ici 2032. Cette hausse reflète la prise de conscience grandissante face aux pertes économiques estimées à 10 000 milliards d'euros par an d'ici 2025, causées par les cyberattaques.

Marché de la cybersécurité et Prévisions de croissance



▲ Au-delà des coûts directs, comme les rançons moyennes de 1,4 million d'euros et les 4,2 millions liés aux fuites de données, cette montée des investissements illustre une transformation vers une sécurité proactive. La directive européenne NIS2 impose en effet désormais à plus de 150 000 organisations d'adopter des standards renforcés, accélérant ainsi l'adoption de pratiques de conformité et de résilience.

RESSOURCES HUMAINES ET COMPETENCES

- La cybersécurité est aujourd'hui confrontée à une **pénurie de talents** et de compétences spécialisées, posant un défi majeur pour les entreprises qui doivent se protéger efficacement contre des menaces toujours plus complexes. Les besoins en expertise dans des domaines comme l'intelligence artificielle, la sécurité cloud et la criminalistique numérique sont en forte croissance, accentuant la pression sur le recrutement et la formation. Ce chapitre illustre les principaux constats en matière de ressources humaines dans le domaine de la cybersécurité

Ressources humaines liées à la cybersécurité / Chiffres clés

- La pénurie de talents en cybersécurité se constate à l'échelle mondiale, avec plus de 4 millions de postes non pourvus. En France, 15 000 postes devront être créés d'ici 2030 pour répondre à la demande croissante. Le ratio actuel de 1 expert pour 1 086 employés illustre un décalage important entre la demande de compétences spécialisées et l'offre de professionnels formés**,** (d'après certains expert, ce chiffre devrait plutôt être aux alentours des 1 expert pour 150 à 200 employés).
- La pénurie de talents toucherait 71 % des entreprises, entravant leur capacité à mettre en place des stratégies de cybersécurité efficaces. Seulement 25 % des postes en cybersécurité sont par ailleurs occupés par des femmes, révélant un déséquilibre de genre persistant et mettant en lumière un potentiel inexploité pour diversifier et renforcer les équipes.
- Selon les premiers diagnostics cybersécurité réalisés par Bpifrance, **47 % des entreprises ne disposent d'aucune personne spécifiquement dédiée à la cybersécurité**, et 17 % ne peuvent pas s'appuyer sur un responsable des systèmes d'information (DSI). Ce manque de moyen, logique compte tenu de la taille des entreprises, expose ces organisations à des risques considérables face à des menaces cyber croissantes car elles n'ont pas les ressources nécessaires pour anticiper et gérer les attaques.

L'ensemble de ces chiffres souligne l'urgence d'investir dans la formation et le développement des compétences pour pallier les lacunes actuelles. Ils appellent également à renforcer l'attractivité des métiers de la cybersécurité, notamment auprès des femmes notoirement sous-représentées, et à intégrer davantage de formations spécialisées pour répondre aux besoins émergents liés à l'IA et à la gestion des incidents. Une stratégie proactive de recrutement et de formation est essentielle pour garantir une résilience durable face aux cybermenaces.

1.2.CARTOGRAPHIE DES PARTIES PRENANTES ET CHAINE DE VALEUR

▲ La cybersécurité en France repose sur un **écosystème riche et diversifié**, impliquant des acteurs publics et privés. Ce réseau collaboratif joue un rôle central dans le développement et la consolidation des capacités de cybersécurité à l'échelle nationale.

Schéma des acteurs

▲ La **synergie entre les différents acteurs** de la cybersécurité s'avère cruciale pour créer un écosystème robuste et résilient en France**.** Si chacun d'eux assume un rôle distinct, c'est dans la complémentarité de leurs actions et la fluidité de leur coordination que réside l'efficacité d'une protection globale, capable de faire face à la montée en puissance des cybermenaces.

▲ Le cœur de l'écosystème est constitué des opérateurs suivants

- **Acteurs publics** : ils élaborent et appliquent les normes réglementaires pour structurer et harmoniser les pratiques de cybersécurité. Leur rôle est de garantir un cadre juridique et opérationnel clair pour l'ensemble des parties prenantes.
- **ESN, Conseil IT et éditeurs** : ces entreprises fournissent des solutions technologiques et des services de conseil pour accompagner les organisations dans l'implémentation et la gestion des systèmes de sécurité informatique.
- **Entreprises clientes** : ce sont les bénéficiaires finaux des solutions et des politiques de cybersécurité. Elles expriment des besoins variés en fonction de leur taille et de leur secteur d'activité.
- **Associations cyber** : elles contribuent à la sensibilisation, à la formation et au partage des bonnes pratiques. Leur rôle est également d'assurer la diffusion des informations et de promouvoir une culture de la cybersécurité.
- **Acteurs de la recherche** : ils jouent un rôle fondamental dans l'innovation et le développement de technologies avancées pour anticiper et contrer les cybermenaces.

▲ **Les normes et labels** constituent un pilier essentiel pour **garantir la qualité et l'efficacité des pratiques** de cybersécurité. Ils permettent d'établir des standards de référence et d'assurer la conformité des processus et des systèmes informatiques aux exigences légales et opérationnelles.

FOCUS SUR LE SECTEUR PUBLIC

▲ Le secteur public joue un rôle fondamental dans la structuration, la régulation et le financement des pratiques de cybersécurité en France. Ses interventions sont réparties en trois grandes catégories :

Trois rôles des intervenants publics

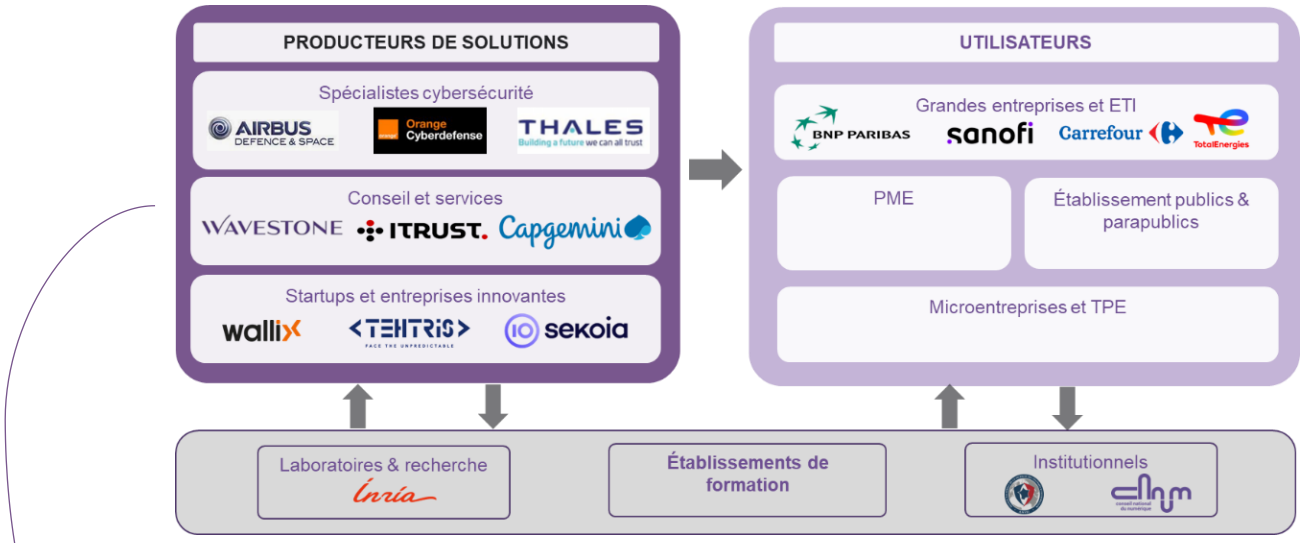
Parmi les principaux acteurs et leurs rôles dans la cybersécurité en France on recense entre autres :

- **Des institutions comme l'Assemblée Nationale, le sénat et l'union européenne** qui établissent des cadres légaux et des directives pour encadrer les pratiques et garantir la sécurité numérique.
- **Des organismes comme la direction Interministérielle du Numérique (DINUM), la SGDSN et le CNIL** qui définissent et harmonisent les normes et standards de cybersécurité.
- **Des organismes spécialisés comme l'AFNOR et l'ANSSI** qui délivrent des certifications pour garantir la conformité et la qualité des solutions adoptées.
- **Des entités comme l'Arcom, l'Arcep, Bpifrance et l'ANR** qui soutiennent la recherche, l'innovation et le déploiement de solutions de cybersécurité, en particulier pour les PME.

▲ Les institutions publiques jouent un rôle stratégique pour la cybersécurité en assurant une **coordination nationale pour anticiper et contrer les menaces**, tout en finançant la recherche et en soutenant l'innovation technologique. Leur action passe aussi notamment par l'élaboration de normes et de certifications qui harmonisent les pratiques et renforcent la confiance entre les acteurs, permettant ainsi une protection accrue et une meilleure préparation face aux cyberattaques.

FOCUS SUR LE SECTEUR PRIVE

▲ L'écosystème privé de la cybersécurité en France s'articule autour d'une structuration progressive et diversifiée. Il rassemble des concepteurs de solutions, des utilisateurs finaux ainsi que des acteurs de soutien, tels que des laboratoires de recherche et des institutions. Cette synergie favorise l'émergence de services adaptés à une large palette de besoins, qu'il s'agisse de grandes entreprises, de PME ou de TPE.



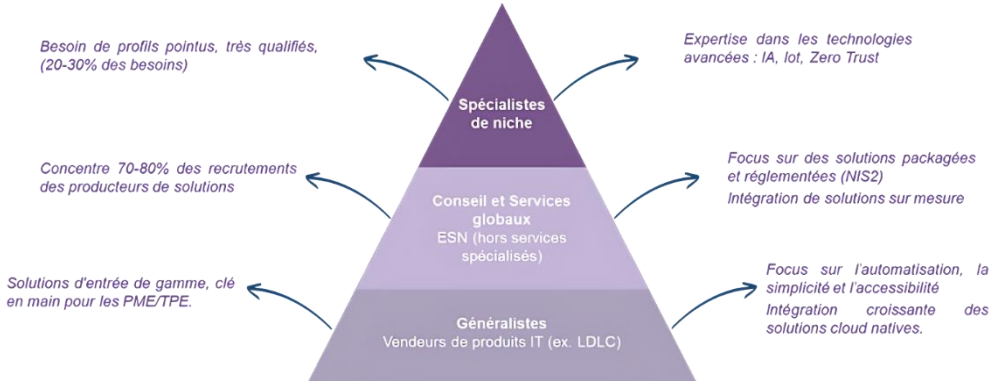
▲ On considère généralement que les producteurs de solutions se répartissent en quatre grandes catégories :

- **<u>Les acteurs du numérique</u> :** prestataires majeurs et généralistes offrant une gamme étendue de services.
- **Les acteurs traditionnels** : Fournisseurs d'équipements intégrant des solutions de cybersécurité dans leurs produits.
- **Les startups** : Innovateurs dynamiques développant des technologies spécifiques face aux menaces émergentes.
- **Des acteurs extérieurs** : Structures développant des solutions sur mesure pour leur propre usage ou leur commercialisation.

Cette diversité d'acteurs illustre la capacité du secteur à combiner expertise établie et agilité pour répondre aux défis croissants en cybersécurité.

▲ Le marché des producteurs de solutions montre également une polarisation croissante entre :

- **Des généralistes** : proposant des solutions standardisées et accessibles, particulièrement pour les PME et TPE.
- **Des conseils et services globaux** : axés sur l'intégration et l'adaptation des systèmes pour répondre aux besoins complexes des grandes organisations.
- **Des spécialistes de niche** : offrant des solutions avancées, intégrant des technologies émergentes comme l'intelligence artificielle, l'IoT et les approches Zero Trust.



FOCUS SUR LES ASSOCIATIONS ET LES ETABLISSEMENTS DE FORMATION

ROLE DES ASSOCIATIONS DANS L'ÉCOSYSTEME

▲ Les associations jouent un rôle prépondérant dans la **promotion et la structuration** de la cybersécurité en France. Elles agissent comme des plateformes d'échange et de collaboration en facilitant la mise en réseau des professionnels et des entreprises du secteur. En fédérant les acteurs autour de bonnes pratiques et de standards partagés, elles contribuent à renforcer la confiance numérique et à professionnaliser la filière.

▲ Ces associations assurent souvent trois fonctions clés :

- **La promotion et sensibilisation** : organisation d'événements, publications et campagnes de sensibilisation.
- **La mise en réseau** : création de communautés et forums pour favoriser les échanges d'expériences et d'expertises.
- **L'harmonisation des pratiques** : élaboration de standards communs pour garantir une sécurité uniforme et efficace.

DYNAMIQUE DES FORMATIONS

▲ **L'offre de formation en cybersécurité en France connaît une croissance significative** afin de répondre aux besoins diversifiés et évolutifs du marché. Elle couvre un large spectre, allant de la formation initiale, depuis le niveau Bac Pro jusqu'aux masters spécialisés (Bac+6), à des programmes de formation continue adaptés aux professionnels. Ces cursus sont conçus pour répondre aux exigences spécifiques des entreprises et des organisations, en intégrant les dernières avancées technologiques et réglementaires. En permettant aux professionnels d'acquérir ou de renforcer leurs compétences tout au long de leur carrière, cette offre de formation contribue à structurer et à professionnaliser la filière cybersécurité. Elle soutient ainsi l'innovation et renforce la résilience des entreprises face aux défis numériques croissants. Un panorama détaillé de cette offre de formation est présenté en partie 3, page 51PARTIE 351.

Principales formations mentionnées lors des entretiens (non exhaustif)

Cette synergie entre les associations et les formations contribue à renforcer l'écosystème de la cybersécurité en France. Elle garantit un développement cohérent des compétences et une mise à niveau continue des acteurs face aux nouveaux défis.

1.2.1. NORMES LEGISLATIONS ET CERTIFICATIONS

UN ENVIRONNEMENT NORMATIF ETOFFE

▲ Le cadre normatif participe à la structuration et l'amélioration continue des pratiques de cybersécurité au sein des organisations. Le tableau ci-dessous présente une sélection des principales normes internationales utilisées pour encadrer la gestion des risques, la sécurité de l'information et la protection des données. Ces normes fournissent des lignes directrices précieuses pour établir des systèmes de gestion, assurer la conformité réglementaire et renforcer la résilience face aux cybermenaces.

Normes	Objet	Proximité avec l'étude
ISO 22301	• Spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de la continuité d'activité (SMCA).	■■■■■
ISO 27001	• Spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI). • Aide les organisations à protéger leurs informations sensibles de manière systématique et économique.	■■■■■
ISO 27002	• Fournit des lignes directrices pour les contrôles de sécurité de l'information basés sur les meilleures pratiques de gestion de la sécurité. • Norme complémentaire qui décrit des mesures de sécurité précises à mettre en œuvre.	■■■■□
ISO 27005	• Spécifie les lignes directrices pour la gestion des risques liés à la sécurité de l'information dans le cadre de l'ISO/IEC 27001. Elle aide à identifier et gérer les risques.	■■■■□
ISO 27017	• Offre des lignes directrices spécifiques pour la sécurité de l'information dans les services de cloud computing	■■■■□
ISO 27018	• Complémentaire à l'ISO/IEC 27017, cette norme se concentre sur la protection des informations personnelles dans les environnements de cloud computing, alignée sur des exigences réglementaires telles que le RGPD.	■■■■□
ISO 29100	• Fournit un cadre pour protéger la vie privée en s'assurant que les pratiques relatives aux données personnelles respectent les principes de confidentialité.	■■■□□
ISO 31000	• Fournit un cadre pour la gestion des risques, applicable à tout type d'organisation (Management du risque).	■■■□□
ISO 62443	• Fournit un cadre pour sécuriser les systèmes industriels, tels que les systèmes de contrôle industriels (ICS), en mettant l'accent sur la protection contre les cybermenaces et la résilience des infrastructures critiques.	■■■■□

Légende : ■■■■■ Cohérence maximale

▲ **La norme ISO 27001** est incontournable en cybersécurité, car elle définit les exigences pour établir, maintenir et améliorer un système de management de la sécurité de l'information (SMSI). Elle aide les organisations à protéger leurs données sensibles, à gérer les risques de manière systématique et à se conformer aux exigences réglementaires comme le RGPD. Au-delà du renforcement de la résilience face aux cybermenaces, elle offre un cadre structuré favorisant l'amélioration continue et constitue un atout pour la crédibilité et la compétitivité des entreprises.

FOCUS SUR LA DIRECTIVE NIS 2

▲ La directive NIS 2, adoptée en octobre 2022 par le Parlement européen, vise à renforcer la cybersécurité au sein de l'Union Européenne. En France, un texte de transposition a été présenté en conseil des ministres le 15 octobre 2024 et devra être voté au Parlement, bien qu'aucune date précise n'ait encore été définie. Cette nouvelle directive succède à la directive NIS de 2016 qui avait introduit des règles communes pour la cybersécurité des opérateurs de services essentiels. Son objectif principal est de renforcer la résilience des réseaux et des systèmes d'information dans l'Union Européenne, face à une augmentation constante des cybermenaces.

OBJECTIFS CLES DE LA DIRECTIVE NIS 2

▲ La directive NIS 2 repose sur plusieurs objectifs majeurs. Elle prévoit tout d'abord un élargissement du champ d'application en couvrant un nombre plus important de secteurs critiques tels que la santé, l'énergie, les transports et les infrastructures numériques. Elle introduit par ailleurs une *nouvelle classification*, distinguant les "Entités essentielles" et les "Entités importantes" pour mieux adapter les exigences de sécurité à chaque catégorie.

Ensuite, un renforcement des obligations est imposé aux entreprises et aux administrations publiques. Cela inclut une gestion plus stricte des risques de cybersécurité, en mettant l'accent sur la protection des chaînes d'approvisionnement. La directive impose aussi des délais précis pour signaler les incidents majeurs : 24 heures pour une détection initiale et 72 heures pour une notification complète.

NIS 2 vise enfin à établir une **harmonisation européenne** en créant un cadre commun pour une réponse coordonnée et plus efficace aux cybermenaces au sein des États membres de l'Union Européenne.

(Secteurs critiques en annexe p.8888)

IMPACTS POUR LES ENTREPRISES

▲ Les entreprises seront directement impactées par des obligations renforcées. Elles devront adopter des mesures de gestion des risques plus strictes et améliorer leurs capacités d'audit, de surveillance et de contrôle afin d'assurer leur conformité avec la directive.

En parallèle, la directive prévoit un panel de sanctions et de contrôles pour garantir l'application rigoureuse des nouvelles règles. Les entreprises non conformes s'exposeront à des amendes pouvant atteindre 10 millions d'euros ou 2 % de leur chiffre d'affaires mondial, ce qui représente une pression financière significative. Des **audits réguliers et renforcés** seront imposés par les autorités compétentes, augmentant les exigences en matière de conformité et de sécurité. Les organisations devront également produire des **reportings détaillés** sur la gestion des risques et les mesures de sécurité mises en place, ce qui impliquera une révision des processus internes.

Enfin, en cas de non-conformité persistante, les entreprises risqueront d'être exclues des marchés critiques, soulignant ainsi l'importance stratégique d'une mise en conformité rapide et efficace.

La directive NIS 2 marque une étape décisive dans l'harmonisation et le renforcement des mesures de cybersécurité en Europe. Elle impose aux entreprises des exigences accrues en matière de gestion des risques, tout en introduisant des sanctions sévères pour garantir leur application. Cette réglementation oblige les acteurs concernés à revoir et à améliorer leurs pratiques afin de répondre aux nouvelles menaces et de renforcer leur résilience face aux cyberattaques.

DES CERTIFICATIONS DEVELOPPEES PAR CERTAINES INSTITUTIONS OU ACTEURS PRIVES POUR APPRECIER LEURS FOURNISSEURS

▲ Les certifications en cybersécurité jouent un rôle essentiel pour garantir la qualité et la fiabilité des prestataires et des services utilisés par les entreprises. Elles permettent d'évaluer et de valider les compétences, les pratiques et les technologies mises en œuvre afin d'assurer un niveau élevé de protection contre les menaces numériques. Ce cadre normatif renforce la confiance des entreprises envers leurs fournisseurs tout en assurant des standards rigoureux et adaptés aux exigences croissantes en matière de sécurité.

Voici quelques certifications regroupées en trois catégories principales : celles portant sur les services, celles axées sur les compétences, et celles dédiées aux produits :

Certifications	Objet	Proximité avec l'étude
PASSI (ANSSI)	Qualification pour les prestataires d'audit qui attestent de leur capacité à effectuer des audits de sécurité.	■■■■■
PDIS (ANSSI)	Qualification pour les services de détection d'incidents de sécurité.	■■■■■
PACS (ANSSI)	Destinée aux prestataires qui réalisent des audits de cybersécurité. Elle vise à garantir que ces prestataires respectent des normes élevées de compétence et de qualité lors de leurs interventions	■■■■■
PRIS (ANSSI)	Atteste des compétences des prestataires en matière de réponse aux incidents de sécurité informatique, incluant le pilotage technique, l'analyse système, l'analyse réseau et l'analyse de codes malveillants.	■■■■■
SecNumCloud (ANSSI)	Destiné aux services cloud qui respectent des exigences strictes de sécurité pour la protection des données sensibles, notamment pour les opérateurs d'importance vitale.	■■■■■
CSNA (STORMSHIELD)	Atteste des compétences en configuration et en gestion des dispositifs de sécurité réseau.	■■■■■
PAMS (ANSSI)	Destinée aux fournisseurs de matériels de sécurité, garantit le respect des standards de sécurité rigoureux par leurs produits.	■■■■■
EAL	Certification internationale attestant du niveau de sécurité des produits informatiques	■■■■□
CISSP (ISC2)	Reconnue internationalement et atteste des compétences en gestion, conception et mise en œuvre de programmes de sécurité de l'information dans une organisation.	■■■■□
CRA	Atteste des compétences en gestion des risques et en mise en œuvre de stratégies de résilience en cybersécurité	■■■■□

■ Certification de services ■ Certification de compétences ■ Certification de produits

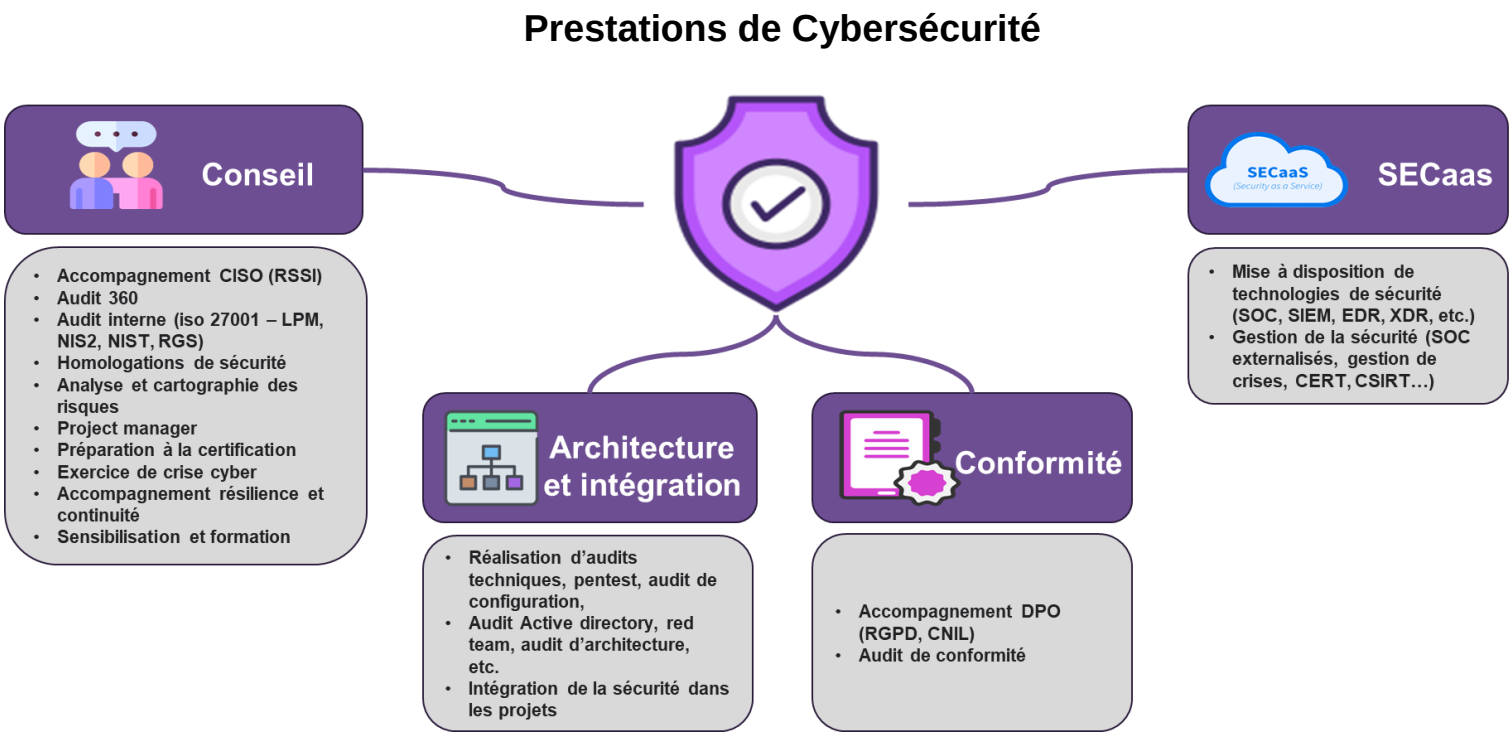
Légende : ■■■■■ Cohérence maximale

▲ Ces certifications participent activement à la professionnalisation et à la structuration du secteur de la cybersécurité. Elles favorisent l'adoption de pratiques de sécurité éprouvées et l'amélioration continue des processus au sein des organisations. En outre, la préférence française pour les certifications validées par l'État, comme celles délivrées par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), témoigne d'une volonté de garantir un cadre strict, harmonisé et souverain.

1.2.2. TYPE DE PRESTATIONS « CYBERSECURITE » CONFIEES AUX ENTREPRISES DE LA BRANCHE

▲ La représentation ci-dessous des prestations en cybersécurité repose sur une première analyse établie à partir des échanges réalisés avec les acteurs du secteur. Elle illustre la diversité des services proposés par les entreprises spécialisées pour répondre aux besoins croissants de protection, de conformité et de résilience face aux cybermenaces.

Les prestations identifiées couvrent plusieurs domaines clés, allant du conseil stratégique et des audits de sécurité, à l'intégration technique et à la gestion de la conformité réglementaire. Elles englobent également des solutions avancées sous forme de services externalisés (SECaaS), garantissant une surveillance continue et des réponses rapides aux incidents. Cette cartographie permet d'avoir une vision globale des compétences et des solutions mobilisables pour accompagner les organisations dans la sécurisation de leurs systèmes d'information.



1.3. TENDANCES ET PERSPECTIVE D'EVOLUTION

1.3.1. CYBERSECURITE & TENDANCES MACROECONOMIQUES

L'analyse des tendances macroéconomiques et des facteurs d'évolution en cybersécurité repose sur une approche PESTEL, permettant d'examiner les influences politiques, économiques, sociales, technologiques et légales. Ce cadre d'analyse met en lumière les dynamiques clés qui façonnent le secteur et oriente les stratégies adoptées par les entreprises pour répondre aux défis émergents en matière de sécurité numérique.

POLITIQUE ET LEGAL

- Instabilité et tension géopolitiques, **guerre cyber**
- Mise en place de directives comme **NIS2** qui impose des normes de cybersécurité plus strictes pour les entreprises
- Renforcement des lois sur la protection des données, comme le RGPD, qui obligent les entreprises à adopter des mesures de sécurité adéquates
- Accord entre les pays pour partager des informations sur les cybermenaces et renforcer la sécurité collective

ECONOMIQUE

- **Digitalisation toujours croissante de l'économie**
- Croissance des budgets consacrés à la cybersécurité.
- Augmentation **des pertes financières** dues aux cyberattaques, impactant **particulièrement les PME**
- Forte demande pour les professionnels de la cybersécurité, avec des **pénuries de compétences** dans le secteur
- Intégration quasi systématique d'une composante cyber dans l'offre des ESN

SOCIAL

- **Renforcement des initiatives de sensibilisation** à la cybersécurité au sein des entreprises, formant les salariés à reconnaître les menaces
- Augmentation de la méfiance des consommateurs envers les technologies numériques
- Changement des comportements des utilisateurs vers une plus grande prudence en matière de partage de données et d'utilisation des technologies
- **Faible évolution du nombre de femmes** dans les métiers de la cybersécurité malgré des efforts (et dans le numérique en général)
- Baisse globale de la **qualité de la formation initiale en mathématiques, un prérequis** critique qui reste trop peu mis en avant

TECHNOLOGIQUE

- **Diversité et complexité croissante** des systèmes d'information, logiciel et matériel
- Amélioration de la capacité de différents systèmes, logiciels et dispositifs à fonctionner ensemble de manière cohérente
- Développement de nouvelles technologies comme l'**IA** et l'apprentissage automatique pour détecter et prévenir les cybermenaces, ou encore **le numérique quantique** qui va pousser à repenser les solutions et systèmes face aux puissances de calcul démultipliées
- Émergence de solutions de cybersécurité basées sur le cloud, offrant flexibilité et scalabilité
- De manière plus générale, des **évolutions technologiques majeures** dans le secteur du numérique, à fort impact sur la cybersécurité (IA, Cloud, Quantique, Blockchain, IOT…)

ZOOM SUR LES FACTEURS LES PLUS STRUCTURANTS

En approfondissement de l'analyse PESTEL**, le tableau infra propose un focus sur les facteurs les plus structurants** qui influencent directement les stratégies de cybersécurité des entreprises. Ce zoom met en évidence les principaux moteurs de transformation et leurs impacts sur l'organisation des acteurs de la branche.

Principaux facteurs d'évolution	Impact sur les entreprises de la branche et actions menées
Croissance des budgets consacrés à la cybersécurité	• Hausse de la demande en solutions et services de cybersécurité. • Augmentation des opportunités pour les ESN spécialisées dans le domaine.
Mise en place de directives renforcées (ex. NIS2, RGPD)	• Obligation de mise en conformité, augmentant la demande en expertise juridique et technique. • Complexité accrue pour les TPE/PME. • Obligation de gestion des compétences.
Digitalisation toujours croissante de l'économie	• Accélération des besoins en cybersécurité pour protéger les infrastructures numériques, mais également les systèmes embarqués. • Augmentation des risques liés à l'exposition des données et des systèmes critiques en ligne.
Évolutions technologiques majeures *Cf. page suivante*	• Développement de nouvelles solutions basées sur l'IA, la blockchain et le cloud notamment • Besoin également d'anticiper les menaces issues des technologies émergentes comme le quantique.
Instabilité et tensions géopolitiques	• Renforcement des investissements en cyberdéfense.… • Nécessité d'adopter des stratégies plus robustes contre les cyberattaques, et à plus grande échelle.

▲ Quelques phénomènes repérés en page précédente **certes plus marginaux dans leur impact** méritent des commentaires complémentaires :

- La baisse globale du niveau en mathématiques n'est pas de nature à faciliter les recrutements en Cybersécurité. La maîtrise de cette discipline fait partie du socle de compétences demandé par une majorité de postes liés à la cybersécurité
- Les perspectives de réduction potentielle du CIR (Crédit d'impôt recherche) ont également interpellé certains acteurs interrogés. Cette baisse possible des incitations financières signifierait le cas échéant le ralentissement des travaux de recherche sur des sujets clés de cybersécurité (ex. crypto, quantique…)

FOCUS SUR LES FACTEURS TECHNOLOGIQUES

▲ **Le développement rapide des technologies numériques entraîne une transformation des besoins en cybersécurité**. Ce tableau présente les principaux facteurs d'évolution technologiques et leur impact sur les entreprises, en mettant en évidence la nécessité d'adapter les pratiques de sécurité face à des innovations comme l'IoT, l'IA, la blockchain et les technologies quantiques. À travers ces tendances, les entreprises doivent anticiper des besoins croissants en compétences spécialisées, en automatisation des processus et en intégration de nouvelles normes pour assurer leur résilience face aux cybermenaces.

Principaux facteurs d'évolution technologiques	Niveau d'impact	Échéance	Impact sur les entreprises de la branche et actions menées
SAAS : bascule de solutions « on premise » vers du SAAS	■■■■□	Court terme	• Evolution d'un réseau « physique » de SI, à une surveillance de flux, digital. Besoin d'adaptation des équipes internes et des prestations
IoT (Internet of Things, objets connectés)	■■■■□	Court terme	• Développement de l'IoT, une déclinaison du phénomène de digitalisation croissante décrit en page précédente • Développement d'expertises sur l'IoT et de prestations dédiées • Augmentation importante à venir des besoins
IA (Intelligence artificiel)	■■■■■	Court/Moyen terme	• Evolution des outils • Risque de détourner des budgets autrefois dédiés à la cybersécurité en cas d'arbitrage • Intégration de la cybersécurité dans les produits IA dès la conception (bydesign) • Poursuite de l'automatisation de certains processus • Baisse des besoins en profils peu expérimentés
Informatique quantique	■■■■■	Long terme	• Développement et intégration de nouvelles compétences et de profils capable de travailler et comprendre cette technologie • Evolution des solutions et systèmes développés pour prendre en compte le nouveau paradigme • Intégration du quantique comme outil demain
Blockchain	■■■■■	Long terme	• Création de standards interopérables pour faciliter la collaboration entre différents systèmes blockchain. Mise en place de solutions de sécurité adaptées pour protéger les actifs numériques et les données décentralisées. • Adoption de solutions blockchain dans les systèmes financiers, avec une réduction des coûts de transaction et une amélioration de la vitesse de traitement.

Légende : ■■■■■ Impact maximal

Compte tenu de la maturité respective des technologies listées, les impacts ne se matérialiseront pas à la même échéance. Par exemple l'intégration massive de l'IA dans les processus pousse déjà à ajuster des systèmes de défense alors que les technologies quantiques commencent juste à questionner les experts de la cybersécurité.

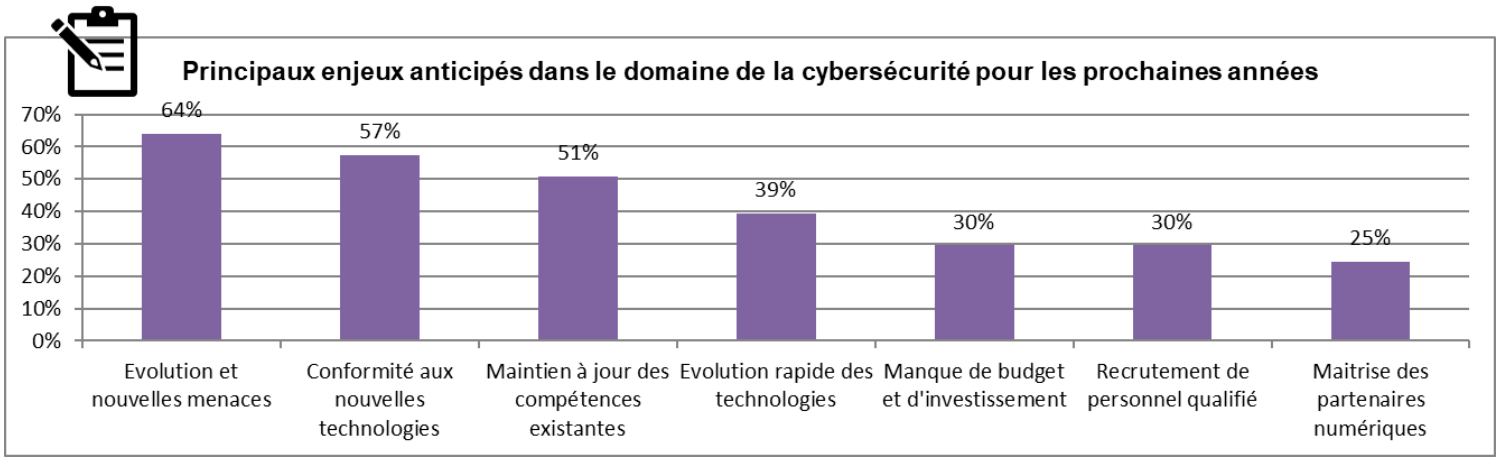
TENDANCES CLES : SYNTHESE

- La cybersécurité évolue dans un contexte de **sensibilisation accrue des individus et des organisations**, entraînant une hausse notable des budgets dédiés à la protection des systèmes d'information. Parallèlement, le **renforcement des exigences réglementaires** vise à mieux prévenir les cyberattaques et à imposer des sanctions plus strictes aux entités qui ne respecteraient pas les normes en vigueur.

  La **transformation numérique de l'économie**, combinée à l'essor rapide des nouvelles technologies, **accentue les besoins en sécurisation des données et des infrastructures**. Cette dynamique impose une adaptation constante des approches et des outils pour faire face à des menaces en perpétuelle évolution. Conscientes pour certaines des enjeux, les entreprises adoptent une approche plus structurée de leurs stratégies de cybersécurité, en développant des partenariats et en organisant leurs ressources internes pour faire face à ces nouveaux défis.

  Ces évolutions entraînent également une **demande croissante en ressources humaines et en compétences spécialisées**. La diversification des profils recherchés et l'augmentation du volume de recrutements attendus soulignent l'urgence d'une montée en compétence pour accompagner les mutations du secteur et répondre efficacement aux enjeux futurs.

- Les résultats de l'enquête en ligne menée auprès des acteurs du secteur corroborent les tendances identifiées via les entretiens qualitatifs. Ces retours mettent en lumière les défis liés à la conformité réglementaire et au manque de talents qualifiés. L'évolution rapide des technologies apparaît de plus comme un enjeu central, nécessitant une veille continue et une capacité d'adaptation renforcée pour les entreprises.



Les interviewés s'inquiètent parfois des investissements sous-jacents pour sécuriser à l'avenir leur système d'information et pointent par conséquent la question financière au cœur des enjeux.

CE QU'IL FAUT RETENIR

1. **La cybersécurité est multidimensionnelle, couvrant des aspects techniques, organisationnels, stratégiques et juridiques. Elle vise à protéger les données, réseaux et systèmes contre les cyberattaques tout en garantissant leur confidentialité, intégrité et disponibilité.**

2. **Les attaques par ransomware, phishing et DDoS augmentent considérablement, posant des défis majeurs. La réglementation (RGPD, NIS2) impose des obligations strictes, nécessitant une conformité accrue et des investissements en cybersécurité. La branche pourra tirer profit de ces stimuli.**

3. **Les entreprises déplorent une forte pénurie de professionnels qualifiés. Plus de 15 000 postes devront être créés en France d'ici 2030, et seulement 25 % des effectifs en cybersécurité sont des femmes, révélant un potentiel inexploité pour diversifier et renforcer les équipes.**

4. **La cybersécurité repose sur un réseau d'acteurs publics et privés, comprenant des régulateurs, des entreprises technologiques, des associations et des centres de recherche. Cette collaboration assure une réponse globale et cohérente aux cybermenaces.**

5. **Des normes comme ISO 27001 et des certifications telles que PASSI ou SecNumCloud jouent un rôle clé pour structurer les pratiques de sécurité et garantir la conformité réglementaire et technique.**

6. **L'essor des nouvelles technologies (IA, IoT, blockchain, quantique) transforme les besoins en cybersécurité, nécessitant des approches adaptées et des compétences spécifiques pour répondre aux défis émergents.**

PARTIE 2.
PROSPECTIVE METIERS ET COMPETENCES AUTOUR DE LA THEMATIQUE CYBERSECURITE

2.1.MATURITE DES ENTREPRISES ET PRATIQUES CYBERSECURITE

2.1.1. APPROCHES ET BESOINS EN CYBERSECURITE

PROFIL TYPE DES ENTREPRISES ET STRATEGIE

▲ La cybersécurité s'avère désormais un enjeu stratégique pour les entreprises, qui doivent adapter leurs approches en fonction de leur maturité et de leur engagement face aux cybermenaces. Si certaines organisations adoptent des stratégies proactives, en investissant massivement dans les technologies, la recherche et le développement, d'autres se contentent de réagir, limitant leurs actions à des réponses ponctuelles ou imposées par la réglementation. On déplorera qu'un nombre significatif d'entreprises reste encore vulnérable, faute de plan clair ou de ressources dédiées, exposant ainsi leurs systèmes à des risques majeurs. Cette hétérogénéité de niveaux de préparation souligne la nécessité d'une sensibilisation accrue, d'un renforcement des compétences et d'une structuration des pratiques pour faire face aux défis croissants liés à la sécurité numérique.

Stratégie adoptée	Entreprises de la branche	Entreprises « clientes » et organisation
« Très proactif »	• Investissements massifs dans des technologies avancées, des experts et de la recherche et développement. • Développement de solutions de sécurité innovantes à la pointe du secteur. • Collaboration avec des organismes gouvernementaux pour anticiper les menaces et élaborer des solutions à long terme.	• Investissement dans des logiciels et services de sécurité avancés comme des systèmes de détection d'intrusion, des firewalls de nouvelle génération, etc. • Formation d'équipes spécialisées en cybersécurité en interne pour gérer les risques et être autonomes.
« Opportuniste » (Approche ad hoc)	• Adaptation, en réaction à la demande du marché, de l'offre existante sans trop d'investissement interne. • Modification des produits pour inclure des fonctionnalités de sécurité, sans aller au-delà de ces ajouts.	• Adoption d'une stratégie plus flexible, permettant de sous-traiter la sécurité à des prestataires externes plutôt que de la gérer en interne. • Investissement uniquement en réponse à un problème ou dans le cadre d'une réglementation obligatoire, sans stratégie à long terme.
« Attentiste »		• Absence de plan stratégique clair pour gérer la cybersécurité, avec utilisation possible d'outils obsolètes ou mal configurés, exposant ainsi aux cyberattaques. • Mise en place de solutions temporaires pour répondre aux menaces immédiates, sans réelle coordination ni stratégie.
« Réfractaire »		• Absence de prise de conscience des risques de cybersécurité, sans mise en place de mesures de protection, même basiques.

VISION DES FREINS ET MOTIVATIONS POUR DEVELOPPER LA CYBERSECURITE

▲ La cybersécurité s'impose aujourd'hui comme un enjeu prioritaire pour les entreprises, poussées à renforcer leurs stratégies face à des menaces croissantes et des environnements numériques en constante évolution. Cette prise de conscience s'accompagne toutefois de motivations variées et de freins persistants, qu'il s'agisse d'obligations réglementaires, de contraintes budgétaires ou d'un besoin accru de compétences techniques. Les deux schémas ci-dessous mettent successivement en évidence les éléments de vision commune entre entreprises de la branche et organisations clientes puis les différences de perception.

Traits communs entre la branche et ses clients

MOTIVATIONS	FREINS / LIMITES
✓ Multiplication des attaques et des risques liés aux nouvelles technologies => **coûts engendrés** ✓ Contraintes réglementaires de plus en plus forte (NIS 2, DORA…) ✓ Besoin d'intégrer l'IA et l'IoT pour la sécurité des systèmes ✓ Cybersécurité en forte croissance, accentuant la criticité de la gouvernance des données pour une gestion d'entreprise efficace. ✓ Partenaires et parties prenantes de l'organisation exprimant attentes et demandes (clients, co-traitants, etc.).	✓ Contraintes budgétaires, processus chronophage… et pas de conscience, preuve tangible du ROI ✓ Pénurie de profils ✓ Manque de compétences techniques ✓ Manque de formation initiale adaptée aux besoins en cybersécurité ✓ Manque de sensibilisation des collaborateurs ✓ Difficulté de rétention des talents en cybersécurité ✓ Place délicate du RSSI avec une influence limitée dans les décisions stratégiques de l'entreprise, compliquant la valorisation des enjeux de cybersécurité au sein de la direction.

▲ Au-delà des éléments partagés entre les différentes organisations, des spécificités émergent selon leur positionnement et leur rôle. Les entreprises de la branche adoptent souvent une approche orientée vers l'innovation technologique et la gestion des risques, tandis que les entreprises clientes se concentrent davantage sur la protection des données, la conformité réglementaire et la continuité d'activité.

Spécificités branche ≠ Spécificités « clients »

Motivations	Freins / limites
✓ Gains en efficacité opérationnelle grâce à une meilleure gestion des risques ✓ Pression des sous-traitants et des partenaires pour renforcer la sécurité ✓ Nécessité d'intégrer l'IA dans les systèmes de sécurité pour les grandes entreprises	✓ Manque de visibilité et de lisibilité des offres de formation en cybersécurité ✓ Complexité des compétences techniques à maîtriser, avec peu d'outils de formation adaptés aux évolutions ✓ Besoin accru de profils spécialisés capables de sécuriser les systèmes industriels et les infrastructures critiques

Motivations	Freins / limites
✓ Gains / moindres pertes économiques ✓ Besoin de protection des données clients pour maintenir la confiance et la réputation ✓ Conformité aux exigences de sécurité imposées par les partenaires ou les régulateurs ✓ Besoin de continuité d'activité pour éviter les interruptions de service ✓ Pression accrue pour adopter les pratiques de cybersécurité "by design" dans les projets ✓ Meilleure gouvernance des données pour améliorer l'efficacité des process internes	✓ Manque de sensibilisation et d'engagement des équipes dirigeantes ✓ Défaut d'identification des bons profils en capacité de les accompagner au sein des ESN ✓ Manque de temps en interne pour déployer des projets n'étant pas cœur d'activité (dont la cyber) ✓ Collaborateurs n'ayant pas / peu d'appétence à changer de comportement ✓ Externalisation fréquente de la cybersécurité avec les résistances classiques (sentiment de perte de contrôle)

SEGMENTATION DES APPROCHES ET BESOINS CLIENTS

▲ La maturité des organisations en matière de cybersécurité varie considérablement en fonction de la taille et du secteur d'activité. Cette hétérogénéité s'explique par des niveaux d'exposition, des ressources disponibles et des contraintes réglementaires spécifiques à chaque type d'acteurs. Le schéma suivant met en lumière ces différences en classifiant les entreprises selon leur taille et leur secteur, tout en identifiant les approches et les besoins distincts qui en découlent.

ETI / GROUPE

- Distinction entre ETI au niveau de maturité variable (souvent avancé mais dépend de la sensibilité des dirigeants) et grands groupes, souvent avancés sur la question et disposant de moyens conséquents (équipes dédiées, détachement de consultants d'ESN à temps plein auprès d'eux…)

PME

- Sensibilisation croissante aux enjeux de cybersécurité, mais des entreprises souvent limitées par les moyens financiers.
- Recours à des RSSI externes pour une gestion de la cybersécurité à temps partiel.

TPE

- Sensibilisation et compétences souvent limitées en cybersécurité
- Peu de ressources pour développer des systèmes de cybersécurité robustes
- Forte dépendance aux prestataires externes pour les besoins cyber

Service

- Services financiers / assurance soumis à des réglementations plus fortes, par obligation bien outillés sur le sujet
- Services de télécommunications relativement avancés sur le sujet (criticité de la cybersécurité pour leur cœur d'activité)

Secteur public

- Administrations centrales (ministères régaliens : Défense, Intérieur, etc.) érigeant les problématiques cyber comme une priorité et investissant massivement
- Collectivités locales et établissements de santé souvent plus démunis (manque de moyens, pas de priorité portée à la cybersécurité)

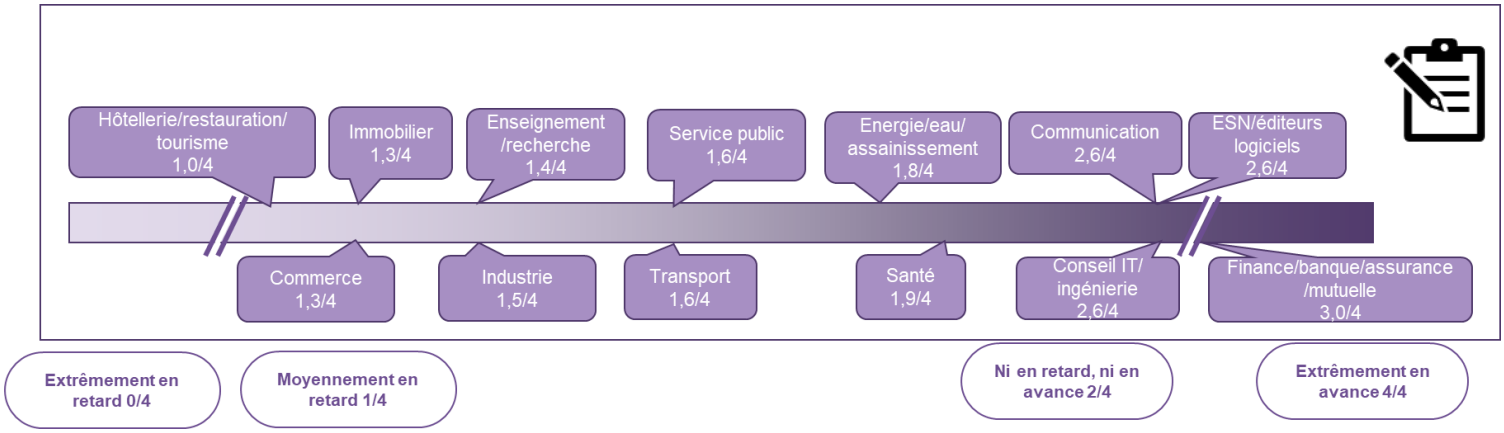
Industrie

- Industries manufacturières, secteur des transports et de l'énergie (hors grands groupes : EDF, RATP, SNCF..) globalement en retard
- Sujet de la cybersécurité des systèmes embarqués / de l'informatique industrielle à forte criticité, qui touche particulièrement les acteurs industriels

Analyse détaillée par secteurs d'activité en page suivante

▲ Les petites entreprises, comme les TPE et certaines PME, apparaissent plus vulnérables en raison d'un manque de ressources et de compétences dédiées, ce qui les rend fortement dépendantes des prestataires externes pour leurs besoins en cybersécurité. À l'inverse, **les grands groupes** et certaines ETI adoptent des **stratégies plus avancées, avec des équipes dédiées et des budgets conséquents**, leur permettant d'imposer des règles de sécurité strictes à leurs partenaires. Enfin, une évolution notable se dessine avec un repositionnement de la branche vers des prestations d'expertise et d'accompagnement, visant à répondre aux besoins stratégiques croissants des clients.

▲ L'étude met en perspective la perception des participants à l'enquête en ligne quant à la maturité des divers secteurs d'activité économique face aux défis de la cybersécurité. Les résultats révèlent des situations très disparates dans les niveaux de préparation et d'adaptation, oscillant entre les secteurs les plus avancés et ceux jugés en retrait. Ces perceptions ont été corroborées et approfondies à travers des entretiens qualitatifs.



▲ Les secteurs tels que la **finance, les banques**, les assurances et les mutuelles apparaissent **comme les plus avancés**, bénéficiant d'une forte régulation et d'exigences strictes en matière de sécurité. Ces domaines ont intégré la cybersécurité comme un enjeu stratégique, engageant des investissements importants sur la protection des données et la gestion des risques.

À l'inverse, des secteurs comme **l'hôtellerie, le tourisme ou l'immobilier** accuseraient un retard inquiétant, principalement en raison de ressources limitées et d'une Sensibilisation moindre à la cybersécurité. Ces secteurs semblent encore percevoir la cybersécurité comme un enjeu secondaire, ce qui les expose à des vulnérabilités accrues.

Entre ces deux extrêmes, d'autres secteurs tels que l'industrie, le transport et l'énergie affichent une maturité intermédiaire. Ces secteurs, bien qu'en phase de transition, doivent encore renforcer leurs compétences et leurs infrastructures pour faire face à des menaces de plus en plus sophistiquées.

Enfin, les **secteurs des technologies de l'information (ESN, éditeurs de logiciels) et du conseil se** positionnent comme des acteurs clés dans l'accompagnement des autres industries, jouant un rôle moteur dans l'innovation et la diffusion des bonnes pratiques en cybersécurité.

2.1.2. STRATEGIES D'ACHAT

PRESTATIONS DE CYBERSECURITE

▲ La nature des stratégies d'achats en matière de cybersécurité repose sur plusieurs variables structurantes, notamment la **taille de l'entreprise, la criticité de ses activités et la récurrence des besoins**. Les grandes entreprises tendent à internaliser en partie leurs besoins en cybersécurité afin de garantir un contrôle direct et d'instaurer des pôles internes dédiés. À l'inverse, les entreprises de taille intermédiaire et les TPE/PME privilégient souvent des partenariats avec des prestataires spécialisés ou se contentent de stratégies d'achats opportunistes, ciblées sur des interventions spécifiques telles que l'audit ou la réponse aux incidents. Les tendances futures en matière d'internalisation ou externalisation de la cybersécurité conditionnent largement les perspectives de développement des emplois dans la branche. Les scénarios prospectifs explicités dans la suite du rapport prennent en considération ce phénomène

La cybersécurité, par la complexité et la singularité des enjeux qu'elle soulève, exige une étude minutieuse des processus à l'œuvre au sein des activités de l'entreprise. L'identité propre à chaque organisation, façonnée par sa culture du risque et son niveau de maturité numérique, imprime une marque décisive sur ses pratiques d'achat. À cela s'ajoutent la cadence et la régularité des besoins exprimés, qu'ils relèvent d'interventions ponctuelles ou d'un suivi continu, ainsi que la nature des actions envisagées—qu'elles soient préventives ou curatives—autant de paramètres qui guident et modulent les choix opérés.

Face à la technicité croissante du domaine, les entreprises doivent souvent **faire appel à des compétences externes**. L'offre de prestataires est variée, allant des **ESN** (Entreprises de Services du Numérique) classiques, qui offrent des solutions IT globales mais parfois limitées en expertise cyber, aux ESN spécialisées, capables de fournir des services pointus et adaptés. Certaines entreprises adoptent **un modèle hybride, combinant des solutions IT générales avec des interventions spécifiques d'experts cyber**. Ce modèle se révèle particulièrement pertinent pour les PME grâce à sa flexibilité et à l'optimisation des coûts qu'il propose.

La mobilisation de ressources externes repose fréquemment sur des modalités telles que **l'expertise à temps partagé** ou le recours à des freelances, permettant aux entreprises de s'adapter à leurs besoins ponctuels sans supporter le coût **d'un** expert dédié à temps plein. Cette approche optimise les ressources tout en assurant un niveau de protection adapté aux menaces actuelles.

Le temps partagé : flexibilité et optimisation des coûts

- Concept : le temps partagé permet aux entreprises d'accéder à un expert cybersécurité (ex. RSSI) à temps partiel
- Avantage : solution idéale pour les entreprises de taille moyenne ou PME, ce modèle alliant expertise et optimisation des coûts
- Objectif : bénéficier de conseils et de suivi en cybersécurité sans engager un expert à temps plein

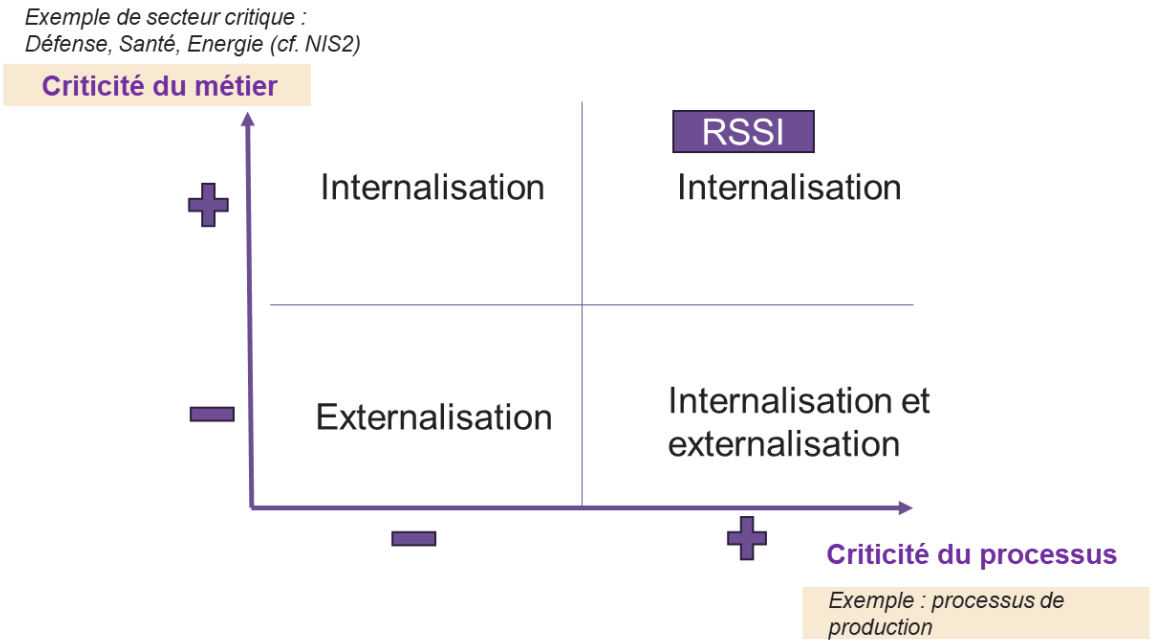
Les organisations construisent par ailleurs des stratégies d'achats distinctes selon le contexte d'intervention, accompagnement attendu : **curatif ou préventif.**

L'approche curative concerne sur la gestion des crises et la remise en état des systèmes après un incident. Elle inclut des actions telles que la récupération des données et la gestion des situations critiques. À l'opposé, l'approche préventive vise à anticiper les risques par la mise en place de mesures proactives, incluant des audits réguliers, des formations et une surveillance continue des infrastructures.

INTERNALISATION VS EXTERNALISATION

▲ S'agissant des arbitrages entre internalisation et externalisation ; les stratégies types observées au sein des organisations résultent souvent d'un croisement entre leur secteur d'activité et les processus spécifiques qu'elles doivent gérer. Parmi les nombreuses variables entrant en ligne de compte, la criticité du métier d'une part et l'importance du processus concerné dans l'entreprise d'autre part, guident souvent les choix de d'internalisation « make » ou d'externalisation « buy ».

Matrice d'Aide à la Décision : Internalisation vs Externalisation



Au-delà de ces deux composantes structurantes, d'autres variables peuvent expliquer le degré de recours aux prestations extérieures :

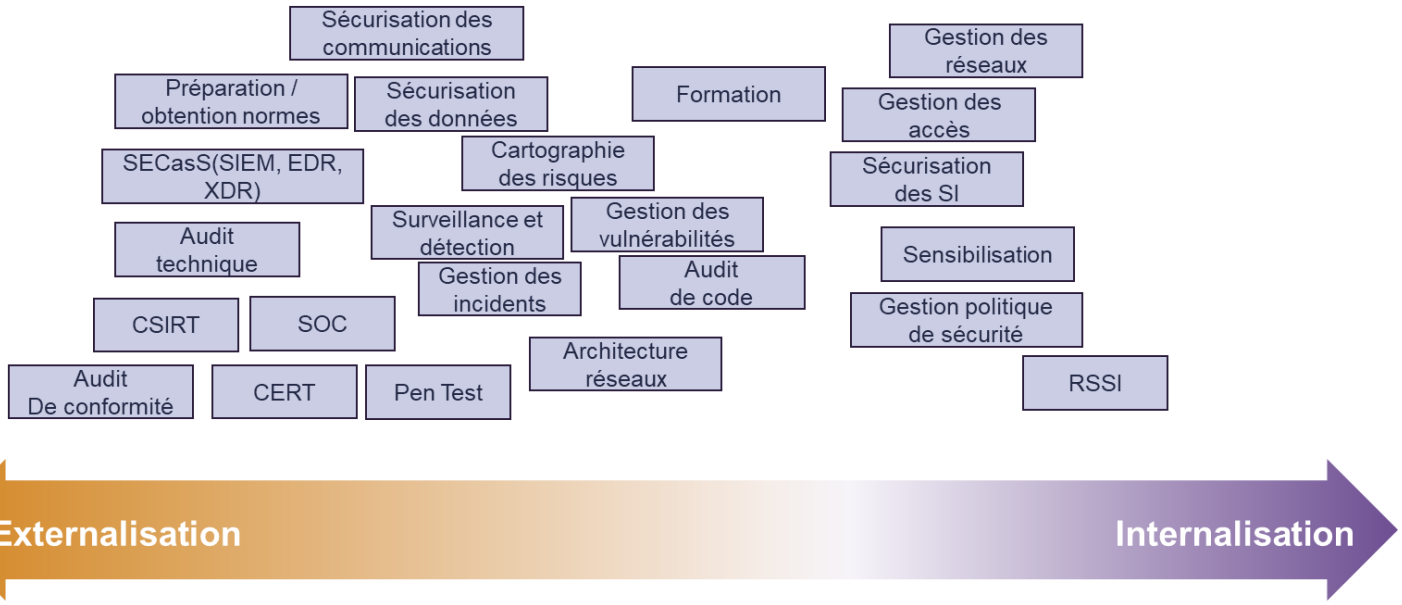
- Taille de l'entreprise
- ADN, culture
- Fréquence et récurrence du besoin…etc.

Dans le cadre des décisions d'externalisation, ce sont principalement les entreprises de la branche qui tirent parti de ces opportunités. Ce modèle contribue à renforcer l'écosystème économique sectoriel en s'appuyant sur des services spécialisés tels que l'audit et le conseil en IT, les prestations fournies par des ESN, ainsi que l'acquisition d'outils et de logiciels dédiés à la cybersécurité.

Illustration des pratiques d'externalisation

- L'externalisation est une pratique courante adoptée par différents types d'organisations pour répondre à des besoins spécifiques. Les collectivités y ont souvent recours en raison de contraintes budgétaires, tandis que les grands groupes l'utilisent comme solution temporaire, le temps de former leurs équipes et d'internaliser les compétences nécessaires. Par ailleurs, face à l'évolution des exigences réglementaires, telles que NIS2, DORA et REC, certaines entreprises privilégient l'externalisation pour s'adapter plus rapidement et efficacement. Les éditeurs de logiciels, quant à eux, externalisent fréquemment pour absorber les pics de charge qui dépassent les capacités de leurs équipes internes (sous-traitance de capacité). Enfin, lorsque la gestion de certains services devient trop complexe en interne, comme c'est souvent le cas pour un Security Operations Center (SOC), l'externalisation apparaît comme une solution pragmatique et efficiente.

Répartition des Activités en Cybersécurité : Externalisation vs Internalisation



- Les décisions d'externalisation concernent notamment des prestations spécialisées, telles que les audits techniques, la gestion des vulnérabilités ou la surveillance des incidents, souvent confiées à des experts externes pour des raisons de flexibilité et d'optimisation des coûts. En parallèle, l'internalisation se justifie pour des aspects nécessitant un contrôle direct et stratégique, comme la gestion des réseaux ou la sensibilisation des équipes. Cette dualité reflète un équilibre recherché par les entreprises pour conjuguer expertise pointue et maîtrise des coûts.
- Les dynamiques à l'œuvre révèlent une montée en compétences au sein des organisations clientes, qui, tout en consolidant leur expertise interne, continuent de solliciter des prestataires externes pour répondre à des besoins ciblés et spécifiques. L'essor de l'externalisation dans certains cas repose sur des considérations économiques, comme le recours à une main-d'œuvre à moindre coût en Europe de l'Est pour des prestations de qualité équivalente. Ce sujet est développé au paragraphe suivant

MODELE ECONOMIQUE DES PRESTATIONS CYBER : QUID DE L'OFFSHORING ?

▲ L'offshoring, ou délocalisation des activités vers des pays étrangers, constitue une pratique courante dans le domaine de la cybersécurité. Son décryptage permettra d'évaluer les besoins futurs en compétences et en emploi au sein de la branche (périmètre des activités en France).

RAPPEL DE LA NOTION D'OFFSHORING

▲ **L'offshoring** se définit comme un transfert d'activités, qu'il s'agisse de production, de services ou d'autres fonctions, vers un pays étranger. Ce « déplacement » d'activité vise plusieurs objectifs, tels que la réduction des coûts grâce à une **main-d'œuvre moins onéreuse** et à des avantages fiscaux. Il permet également d'accéder à des **compétences spécifiques disponibles localement et d'ouvrir l'entreprise à de nouveaux marchés**.

Dans le domaine du numérique, plusieurs modèles d'offshoring se distinguent. La sous-traitance simple repose sur la réduction des coûts grâce à l'utilisation de main-d'œuvre étrangère. Le **nearshoring,** quant à lui, consiste en une délocalisation vers des pays proches, tels que ceux du Maghreb ou d'Europe de l'Est, afin de limiter les décalages horaires et de faciliter la communication.

Le marché français de **l'externalisation informatique représente plus de 25 milliards d'euros en 2024***. Si cette pratique était initialement limitée au développement de logiciels, elle englobe désormais la maintenance des systèmes, le support technique et la gestion des réseaux. Elle couvre ainsi aujourd'hui la quasi-totalité des maillons de la chaîne de valeur numérique.

OFFSHORING ET CYBERSECURITE : OPPORTUNITES ET PRATIQUES

▲ L'offshoring présente de nombreuses opportunités pour la cybersécurité. Il offre un accès à des experts à des coûts compétitifs et permet une **couverture des fuseaux horaires** grâce au modèle "follow the sun", facilitant un support continu 24/7. Cette approche réduit également les délais de développement et de maintenance des solutions cyber.

Dans la pratique, **l'offshoring s'applique à des activités variées**, telles que les audits de cybersécurité, la gestion des incidents à distance par des équipes offshore, et le développement de solutions anti-cyberattaques par des centres spécialisés délocalisés.

La mise en œuvre d'une politique d'offshoring demande plusieurs précautions. Les risques liés à la sécurité des données sensibles sont à considérer, notamment en raison de réglementations spécifiques comme le Cloud Act aux États-Unis, le Patriot Act ou encore la loi chinoise PIPL sur la protection des informations personnelles. De plus, la gestion interculturelle et la collaboration à distance nécessitent des ajustements organisationnels. Les coûts cachés associés à la délocalisation doivent également être pris en compte, sans oublier les organisations ad hoc requises pour assurer un pilotage efficace des partenaires étranger : formations spécifiques, maîtrise de l'anglais…etc.

Illustration des pratiques

▲ L'offshoring est une pratique largement utilisée dans **plusieurs secteurs** pour optimiser les coûts et accéder à des compétences spécifiques. Dans le secteur bancaire, il est courant d'externaliser des prestations de tests d'intrusion (pentest) afin de renforcer la sécurité des systèmes d'information. De même, certaines entreprises de services numériques (ESN) spécialisées en cybersécurité externalisent des services d'infogérance et de centres opérationnels de sécurité (SOC). Les sociétés de conseil en cybersécurité recourent également à l'offshoring pour des prestations de pentest, garantissant ainsi une expertise pointue tout en maîtrisant les coûts. Par ailleurs, certaines ESN établissent des **centres d'expérience digitale à l'étranger**, comme à Bangalore, afin de bénéficier d'un vivier de talents qualifiés. Des accords de coopération, tels que celui entre la France et le Maroc, facilitent enfin le développement de projets web offshore, favorisant une collaboration internationale efficace et compétitive.

***Source : Statista**

VERBATIM AUTOUR DE LA CYBERSECURITE

Dans le cadre de notre étude, nous avons recueilli plusieurs témoignages marquants. Voici un extrait particulièrement révélateur de l'état d'esprit des opérateurs :

BRANCHE

Perception

« Nous relevons trois grands enjeux stratégiques pour la cybersécurité demain : l'aspect économique, c'est-à-dire donner confiance aux entreprises pour qu'elles se cyber-sécurisent ; l'aspect technologique avec l'apparition de l'IA et la pénurie de talents ralentissant le développement cyber »

« Il y a une véritable prise de conscience, mais les moyens manquent toujours pour les petites structures »

Freins et motivations

« La règlementation européenne est une bonne chose, car elle oblige les entreprises à faire le minimum syndical, et donc à grandir en matière de cybersécurité »

« Les gens ont un prisme restreint de la cybersécurité, il faut réussir à comprendre que c'est un tout, pas juste un service »

« Les besoins en matière de cybersécurité des grands donneurs d'ordres industriels sont énormes, et le cadre réglementaire récent ne va que renforcer ces besoins. Beaucoup de structures, notamment PME et ETI ne sont pas prêtes et devront être accompagnées pour monter en maturité sur le sujet. »

Actions demain

« Il y a une énorme pénurie de talents dans la cybersécurité, nombre qu'on estime à 400 000 personnes pour la France. Le véritable enjeu est donc de former des gens, et de ne pas réduire la cybersécurité à de la réalisation de Pen Test »

« La cybersécurité c'est comme la santé, les technologies ce sont comme les médicaments, mais il faut beaucoup plus que ça, des règles d'hygiène à chaque étape, des professionnels… Le faire comprendre est très complexe »

CLIENTS

Perception

« On demande parfois au client d'être plus au fait et plus compétent sur la cybersécurité que les intégrateurs de solution, or ce n'est pas comme cela que ça devrait fonctionner »

« L'informatique industrielle est en retard, historiquement tout était basé sur la prévention des défaillances de ces systèmes, sans intégrer les questions de malveillance. C'est un changement de culture qui va prendre de longues années »

« La montée en compétence de l'écosystème des grands groupes est le gros sujet des années actuelles et à venir »

Freins et motivations

« En général, beaucoup de nos clients privés et publics ne nous importunent pas avec ces problématiques cyber, mais nous sentons qu'il y a une demande croissante de chiffrement des données… etc. qui nous obligent à investir »

« Beaucoup de secteurs réglementés commencent à demander des prestations cyber de plus en plus pointues et ne trouvent pas en face l'offre de solution pertinente pour répondre à leurs besoins »

« Beaucoup de clients ne sont pas à l'aise avec le cloud mais ne peuvent pas s'en passer et de plus, n'ayant pas les équipes internes, ils doivent externaliser par contrainte »

Actions demain

« Nous allons continuer à réaliser ponctuellement des audits cyber pour adapter notre feuille de route et nos actions en la matière »

« Nous renforçons le suivi de nos fournisseurs sur la cyber »

« Dans les années à venir, nous allons renforcer la sensibilisation et la diffusion des bonnes pratiques auprès de l'ensemble de nos collaborateurs, à travers la formation »

2.2.POLITIQUE « RH » EN LIEN AVEC LA CYBERSECURITE

2.2.1. BESOINS ET STRATEGIES DE RECRUTEMENT

POLITIQUE RH EN LIEN AVEC LE DEVELOPPEMENT DE LA CYBERSECURITE

- L'évolution constante des enjeux liés à la cybersécurité impose des politiques de ressources humaines très agiles, imposant des ajustements organisationnels, une optimisation des processus internes et un développement ciblé des compétences pour faire face aux nouvelles menaces et exigences réglementaires.

CHANGEMENT ORGANISATIONNEL (TYPE ORGANIGRAMME)

- Le développement de la cybersécurité nécessite une montée en compétence transverse. Cette problématique, désormais partagée entre plusieurs départements tels que la DSI, les ressources humaines, le service juridique et le commercial, exige une meilleure collaboration interne pour garantir une approche intégrée. Les RSSI doivent de surcroît être davantage intégrés aux comités de direction ou comités exécutifs afin d'assurer que la cybersécurité soit systématiquement prise en compte dans les décisions stratégiques. Certaines entreprises créent ainsi des cellules cybersécurité dédiées pour renforcer leurs capacités dans le domaine. Ces équipes peuvent être internalisées ou externalisées auprès de partenaires spécialisés, en fonction des besoins et des ressources disponibles.

ÉVOLUTIONS DES PROCESSUS INTERNES

- La gestion des risques cyber impose aux entreprises de mieux formaliser leurs processus internes en matière de gestion des risques. Les grandes structures mettent en place des politiques spécifiques pour gérer les incidents, notamment des plans de continuité et de reprise d'activité, afin d'assurer une réponse rapide et efficace en cas de crise. Par ailleurs, l'utilisation d'outils collaboratifs sécurisés se généralise, en particulier dans les contextes de télétravail ou de mobilité, afin de faciliter la collaboration tout en maintenant un haut niveau de sécurité. Les organisations déploient dorénavant des campagnes de sensibilisation généralisée d'envergure afin de réduire les erreurs humaines, qui sont souvent à l'origine des cyber-incidents.

POLITIQUE DE FORMATION

- En matière de formation, les entreprises privilégient une approche continue pour accompagner l'évolution des compétences. La mise en place de programmes de formation réguliers répond aux besoins spécifiques identifiés et garantit une montée en compétence durable. Les **certifications spécialisées** sont particulièrement recherchées, en visant des accréditations reconnues qui renforcent la crédibilité et les compétences des équipes. De plus, l'utilisation accrue des plateformes d'e-learning permet de plus aux collaborateurs de se former en ligne sur des outils techniques et sur les réglementations en vigueur, favorisant ainsi un apprentissage flexible et accessible. Pour compléter la palette des outils et occasions de montée en compétences, les entreprises organisent parfois des **événements immersifs tels que des hackathons ou des simulations d'attaques** pour plonger les équipes dans des situations réelles et leur permettre de développer des réflexes adaptés face aux cybermenaces.

CYBERSECURITE ET POLITIQUE DE RECRUTEMENT

DIVERSITE DES METIERS ET BESOINS EN RECRUTEMENT

▲ La cybersécurité englobe une grande diversité de métiers et nécessite l'adaptation des stratégies de recrutement pour répondre à des besoins variés. Les entreprises doivent ainsi combiner des interventions techniques, telles que les analystes SOC et les pentesters, avec des profils stratégiques comme les architectes de sécurité et les consultants en conformité. Une attention particulière se porte ainsi sur les talents capables de tisser un lien harmonieux entre compétences techniques (cyber), aptitudes organisationnelles (gestion de crise, audits, conformité) et qualités comportementales, indispensables pour relever des enjeux transversaux et complexes.

APPROCHES CURATIVE ET PREVENTIVE DANS LE RECRUTEMENT

▲ Les stratégies de recrutement en cybersécurité suivent les deux grands pans d'actions préalablement cités : approche curative et approche préventive. Pour gérer les interventions en urgence les organisations privilégient le recrutement de profils expérimentés, avec une attention particulière aux professionnels ayant entre trois et cinq ans d'expérience. Elles s'orientent également vers des profils en reconversion, issus du monde industriel et la priorité aux compétences opérationnelles, capables d'agir rapidement. En parallèle, l'approche préventive vise à anticiper les menaces en recrutant des experts capables de sécuriser les infrastructures et de développer des stratégies de sécurité à long terme. Ces profils sont formés pour analyser les risques, assurer la conformité et gérer les accès de manière proactive.

STRATEGIES DE SOURCING ET INTEGRATION DES TALENTS

▲ Pour faire face aux besoins croissants en compétences spécialisées, les entreprises adoptent différentes stratégies de sourcing et d'intégration des talents. Le recrutement via des Entreprises de Services du Numérique (ESN) demeure un levier fréquemment usité. Les entreprises dépendent fortement de ces prestataires pour répondre aux besoins urgents en compétences, notamment par l'apport de profils spécialisés. Ce système repose sur une communication fluide entre les consultants des ESN et les postes internes dans les organisations clientes.

Les entreprises recrutent également des profils à distance (nearshore et offshore) pour des tâches opérationnelles, telles que la surveillance et la gestion des SOC. Cette approche offre plusieurs avantages déjà évoqués, notamment la réduction des coûts et la couverture des fuseaux horaires.

COLLABORATION ET INITIATIVES POUR ATTIRER LES TALENTS

▲ Pratique courante dorénavant, les entreprises investissent pour attirer les talents dès leur formation. Le renforcement des liens avec les écoles d'ingénieurs et les universités permet de repérer et d'attirer les jeunes talents dans le domaine de la cybersécurité. La création de passerelles facilite l'intégration des jeunes diplômés dans ces métiers.

Pour identifier les talents potentiels, les événements de type Hackathons et simulations d'attaques permettent de tester les compétences et d'évaluer la capacité des participants à réagir face à des cybermenaces. La participation à des forums et salons de recrutement joue également un rôle important pour sensibiliser aux opportunités de carrière dans la cybersécurité.

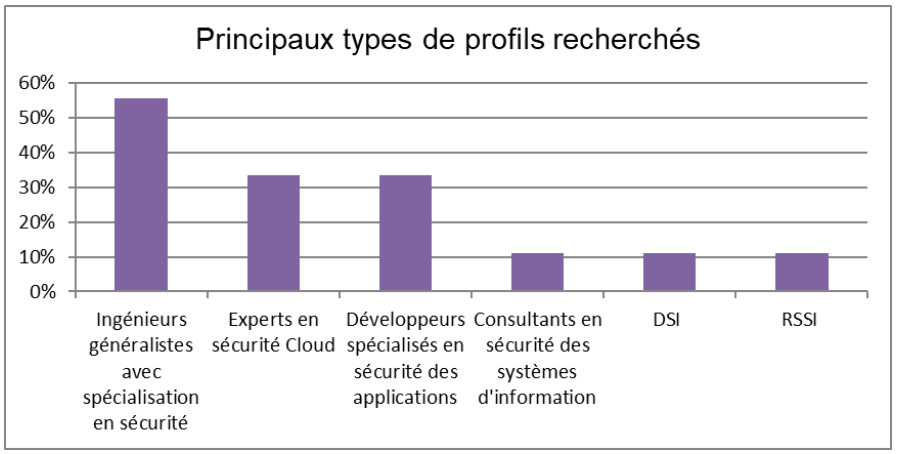
Près de** 70% des répondants estiment avoir besoin de recruter au moins une personne **dédiée à la cyber sécurité dans les trois prochaines années
Parmi eux,** 30 % ont actuellement des postes vacants **et rencontrent des difficultés à les combler

Des éléments, confirmés, étayés par l'analyse des offres d'emploi autour de la thématique de Cybersécurité (cf. page 40)

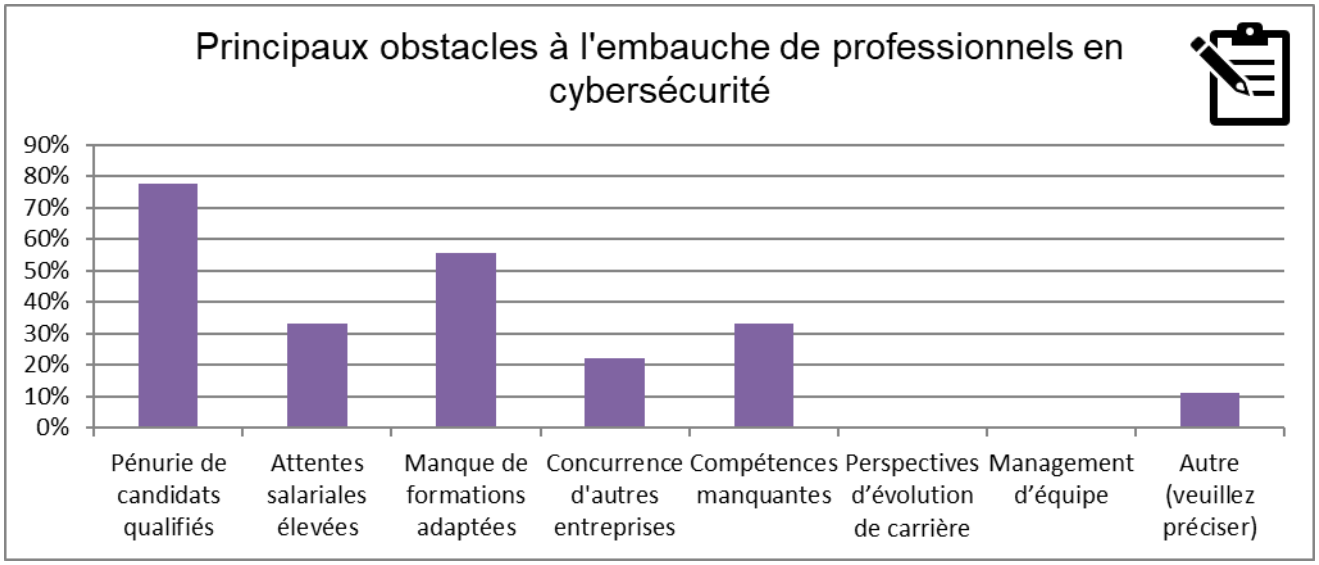
PROFILS RECHERCHES ET DEFIS DE RECRUTEMENT

- La digitalisation rapide de l'économie génère une demande croissante en compétences spécialisées en cybersécurité. Les difficultés de recrutement ont été observées tout au long de l'année 2024, accentuées bien sûr pour les profils les plus recherchés

- Les ingénieurs généralistes spécialisés en sécurité représentent la catégorie de profils la plus sollicitée, témoignant d'un besoin accru pour des compétences polyvalentes capables de couvrir plusieurs aspects de la cybersécurité. En complément, les experts en sécurité Cloud et les développeurs spécialisés en sécurité des applications figurent parmi les profils les plus demandés. Cette tendance reflète l'importance grandissante des infrastructures cloud et des solutions logicielles sécurisées dans les stratégies des entreprises.



- **La pénurie de candidats qualifiés** constitue, d'après les répondants à l'enquête, le principal obstacle au recrutement dans le domaine de la cybersécurité. Ce constat plaide pour un investissement accru dans la formation et dans des initiatives visant à attirer de nouveaux talents. Les attentes salariales élevées et l'inadéquation des formations disponibles limitent par ailleurs les capacités de recrutement, en particulier pour les PME, rendant la sécurisation des compétences un enjeu stratégique pour les entreprises.



2.2.2. ANALYSE DU MARCHE DE L'EMPLOI, ANNONCE JOBFEED (BY textkernel)

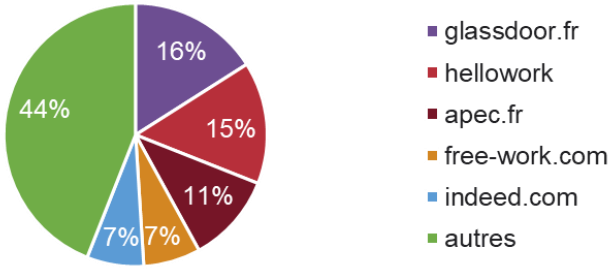
▲ L'exploitation de base de données type Jobfeed fournit des éléments intéressants pour appréhender la réalité des recrutements opérés sur la thématique cybersécurité par les entreprises de la filière numérique. Cet outil s'appuie sur un recensement exhaustif des offres d'emplois publiées en France. Un système de requête permet d'extraire, sur des temporalités définies, la volumétrie des offres d'emploi sur un poste en particulier. L'extraction a été réalisé en décembre 2024.

▲ Selon cette source, **34 652 emplois** ont été créés entre septembre 2022 et décembre 2024, dont **16 025 postes** destinés aux profils Bac +4/+5, représentant la majorité de la demande des employeurs.

Parmi les professions les plus recherchées arrivent par ordre de priorité :

- Ingénieur en cybersécurité (2 068 annonces)
- Consultant (1 660 annonces)
- Administrateur réseau (1 273 annonces)
- Chef de projet informatique (1 082 annonces)
- Chef de projet (1 248 annonces)
- Architecte système (797 annonces)
- Ingénieur Système (673 annonces)
- Responsable sécurité informatique (275 annonces)

LES JOBBOARDS LES PLUS UTILISÉS



▲ Le profil le plus recherché est généralement de niveau Bac +5, avec **12 270 annonces**, suivi de **4003 annonces** pour un Bac +2, **1 784 annonces** pour un Bac +3, **1 797 annonces** pour un Bac +4/+5, et **798 annonces** pour un niveau Bac.

▲ A noter que les offres d'emploi sont principalement localisées en **Île-de-France** avec **17 887 annonces**, suivies de la région **AURA** avec **4 247 annonces** et de la région **PACA** avec **3 151 annonces**.

Sur le champ très spécifique de la cybersécurité, les 7 principaux employeurs directs repérés sont :

- Atos (2 278)
- Sopra (1 430)
- Orange Group (820)
- Capgemini (741)
- Bouygues Telecom (720)
- Inetum Computing Inc. (642)
- Devoteam (634)

2.3.IMPACT DE LA CYBERSECURITE SUR LES METIERS ET LES COMPETENCES AU SEIN DE LA BRANCHE

2.3.1. CARTOGRAPHIE DES METIERS DE LA CYBERSECURITE

INTRODUCTION SUR LA CARTOGRAPHIE DES METIERS & COMPETENCES

UN PANEL DES METIERS PROPRES A LA CYBERSECURITE ECLECTIQUE ET EN CONSTANTE EVOLUTION

- La cybersécurité regroupe un ensemble très diversifié de métiers répartis en quatre grandes familles, offrant une flexibilité d'organisation et d'évolution (cf. page suivante). On retrouve bon nombre des métiers chez les prestataires de services comme chez les clients, certains postes spécifiques restant l'apanage des sociétés du numérique. L'évolution rapide du panel de métiers traduit la nouvelle dimension prise par la thématique au sein des organisation et suit le rythme rapide des évolutions technologiques touchant le numérique.

UNE CARTOGRAPHIE DES METIERS NUMERIQUES DEJA IMPREGNEE DU DEVELOPPEMENT DE LA CYBERSECURITE

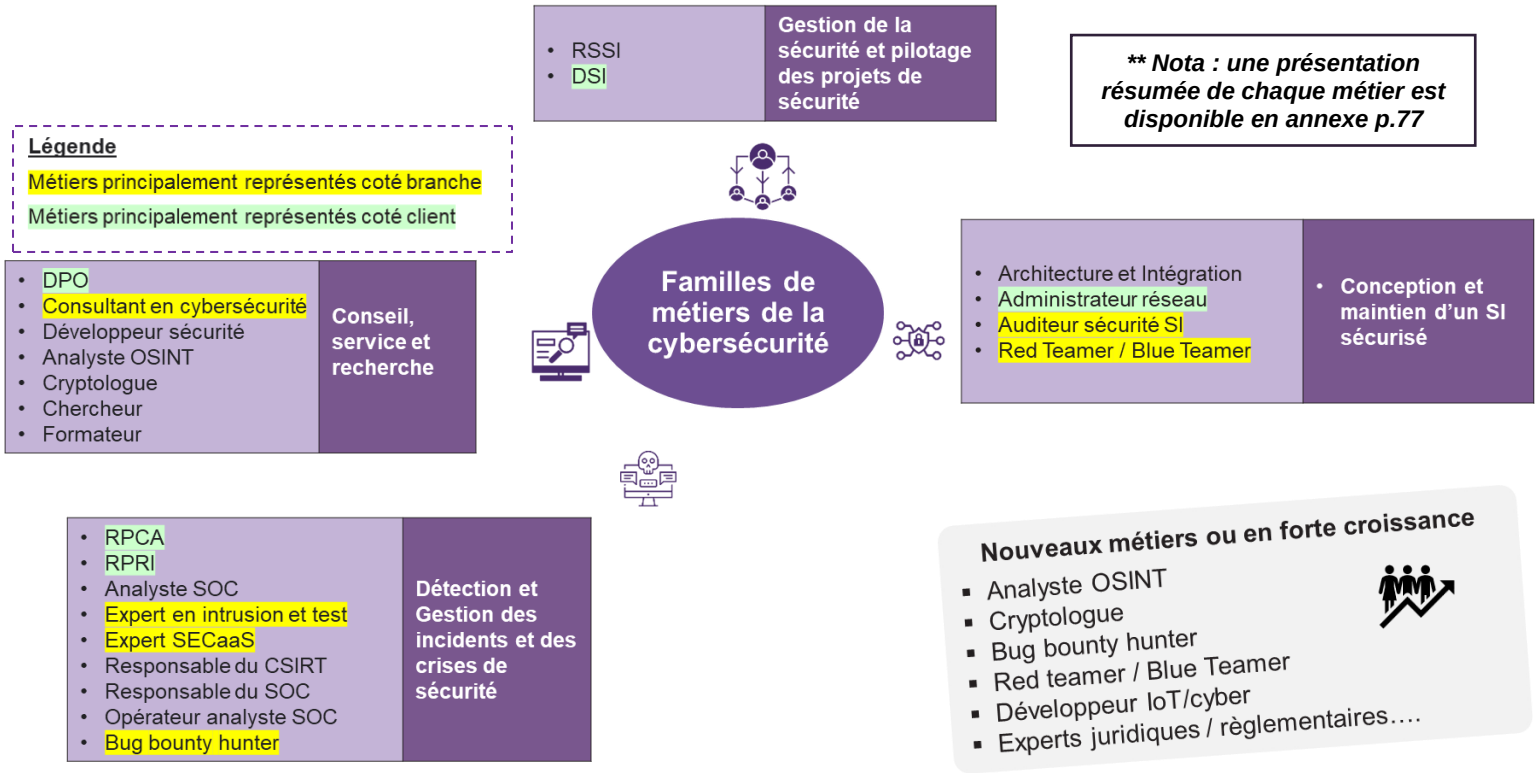
- Certains des métiers liés à la cybersécurité figurent déjà dans la cartographie « OPIIEC » 2024.
- La cartographie actuelle n'intègre pas cependant tous les métiers émergents qui prennent une importance croissante au sein des ESN et des éditeurs de logiciels.
- Les métiers traditionnels du numérique déjà référencés au sein de la cartographie se transforment pour intégrer davantage les exigences de la cybersécurité. Selon les familles de rattachement, ils sont diversement impactés par le phénomène.

DES IMPACTS SUR LE PANEL DES COMPETENCES AU SEIN DES ENTREPRISES DE LA BRANCHE

- L'empreinte de la cybersécurité se manifeste de manière plus ou moins forte selon les métiers, influençant directement le quotidien des salariés et des prestataires. Certains postes sont **au cœur du bon fonctionnement des systèmes de sécurité informatique**, tandis que d'autres, plus éloignés, nécessitent d'acquérir un **socle initial de compétences**. Le degré de maîtrise attendu varie selon les profils et les niveaux d'expertise. Par ailleurs, l'évolution des technologies entraîne l'émergence de nouvelles compétences clés, essentielles pour suivre les transformations du secteur.
- Au-delà des compétences techniques, les recruteurs accordent une grande importance à des **compétences transversales**. Celles-ci incluent une culture économique étendue, une connaissance approfondie des processus métiers et une maîtrise des outils informatiques avec une approche globale et stratégique. Ces qualités s'avèrent indispensables pour accompagner l'évolution des pratiques et des technologies en cybersécurité.

LES METIERS DE LA CYBERSECURITE

La cartographie des métiers de la cybersécurité schématisée ci-dessous a été réalisée en collaboration avec des experts du domaine et enrichie progressivement au fil des entretiens menés avec des **professionnels du secteur. Elle met en lumière la diversité et la spécialisation croissante des compétences requises pour** répondre aux défis de sécurité actuels. D'autres référentiels existent pour représenter les métiers de la cybersécurité. Parmi eux, la cartographie du Campus Cyber se distingue en proposant une approche intégrée reliant métiers et compétences. Elle tend à s'imposer comme une référence du secteur, permettant d'harmoniser les parcours professionnels et de mieux répondre aux besoins en compétences des entreprises et des institutions.



▲ La cybersécurité couvre un **large éventail de métiers**** qui répondent aux besoins variés des entreprises et des organisations. Ces métiers sont répartis entre des rôles davantage présents « côté client » et d'autres plus représentés « côté branche », offrant ainsi une complémentarité essentielle pour assurer une couverture complète des enjeux de sécurité. Les métiers côté client relèvent en particulier de la sécurisation des environnements spécifiques et la réponse aux besoins opérationnels, tandis que les profils côté branche jouent souvent un rôle d'expertise, de conseil et d'interface entre les différents acteurs.

La cybersécurité est marquée par l'émergence de nouveaux métiers et une demande croissante pour des compétences spécialisées. Parmi ces métiers en forte croissance, se positionnent les **analystes OSINT, les cryptologues, les bug bounty hunters, ainsi que les red et blue teamers**. Ces profils répondent à des besoins spécifiques tels que l'analyse des menaces, la gestion des incidents et la protection des systèmes critiques.

D'abord réservés aux services de Police et Gendarmerie, les métiers de l'investigation numérique (Investigateur cyber criminalité et investigations Forensic) s'ouvrent aujourd'hui au secteur privé avec des nouveaux métiers tels que les Threat intelligence analysts qui identifient et tracent, entre autres, les données volées sur le Darkweb/Deepweb.

Les experts en cybersécurité s'orientent de plus en plus vers des spécialisations pointues, qu'il s'agisse de l'intrusion, de la gestion de crise ou encore de la cryptologie. Toutefois, cette expertise ne saurait se cantonner aux seules compétences techniques. Elle requiert également une maîtrise approfondie des enjeux de gestion, de la réglementation en vigueur et de l'analyse des risques, autant de savoirs indispensables pour répondre aux exigences toujours plus élevées des entreprises

Les **évolutions technologiques rapides impliquent une interaction constante entre métiers présents côté client et ceux côté branche**. Cette collaboration permet d'aligner les stratégies et de garantir une sécurité optimale sur l'ensemble des processus. Les métiers du conseil, comme les consultants en cybersécurité, opèrent pour faciliter la coordination et la mise en œuvre des politiques de sécurité.

2.3.2. IMPACT SUR LA CARTOGRAPHIE DES METIERS

▲ En dehors des métiers directement liés à la cybersécurité, toutes les professions du numérique sont concernées par les enjeux de sécurité, nécessitant une montée en compétences généralisée. Les tableaux ci-dessous, fondés sur la classification « OPIIEC » des métiers du numérique, permettent d'appréhender l'impact de ces transformations

Direction d'entreprise et développement	Impact	Commentaires
Directeur de Business Unit	■■■□□	**Des fonctions devant impulser les changements de pratiques en interne comme en externe** • Mise en œuvre de stratégies cybersécurité en interne sur les process/produits • Sensibilisation des équipes • Choix de positionnement « Cyber » de l'entreprise / avantage compétitif ? (déclinaison d'une offre?)
Directeur commercial	■■□□□	
Responsable partenariats	■□□□□	

Pilotage de projet	Impact	Commentaires
Chef de projet	■■■□□	**Prise en compte de la cybersécurité dans les projets** • Travail étroit avec les équipes techniques et les spécialistes cybersécurité • Renforcement de l'analyse des risques pour inclure des audits et des tests de pénétration. • S'assurer du développement d'un projet dans les règles du cyberbydesign
Coordinateur de projet	■■■□□	
Directeur de projet	■■□□□	

Support commercial et marketing	Impact	Commentaires
Formateur	■■■■□	**Support commercial et marketing devant agir de pair avec la direction pour faciliter la commercialisation** • Adaptation a minima des messages marketing (rassurer le client) • Déclinaison d'une offre pour les entreprises positionnées sur le sujet • Anticipation des objections clients • Soutien avant-vente
Consultant avant-vente	■■■■□	
Chef de produit & services	■■□□□	
Technico-commercial	■■□□□	

Développement et test de la solution	Impact	Commentaires
Développeur blockchain	■■■■□	**Intégration systématique des enjeux cyber dans le cœur de ces métiers** • Mise en place de codage sécurisé pour éviter les failles exploitables • Inclusion systématique de tests de pénétration et d'audits de sécurité • Besoin d'interaction constante entre développeurs, testeurs et experts cybersécurité
Spécialiste DevSecOps	■■■■□	
Analyste de la menace		
Développeur applications	■■□□□	
Intégrateur logiciels métiers	■■□□□	
Pentesteur		
Spécialiste test et validation	■■□□□	

Légende : ■■■■■ Impact maximal

Architecture et conception de la solution	Impact	Commentaires
Spécialiste e-santé	■■■■■	**Une famille de métiers logiquement fortement impactée et de nouveaux besoins en « ETP » à prévoir** • Focus sur la sécurité dès la conception • Besoin croissant d'expertise en blockchain, IoT et Intelligence Artificielle pour anticiper les menaces spécifiques à ces technologies • Importance de conformité réglementaire
Architecte IoT	■■■■□	
Consultant architecte technique	■■■■□	
Data Engineer	■■■■□	
Data Protection Officer		
Data Scientist	■■■■□	
Spécialiste blockchain	■■■■□	
Spécialiste IA embarquée	■■■■□	
Expert en Intelligence Artificielle	■■■■□	
UX – UI Designer	■■□□□	
Webdesigner	■■□□□	
Responsable Green IT	■□□□□	

Mise en production et exploitation de la solution	Impact	Commentaires
Spécialiste bases de données	■■■□□	**Métiers liés à l'infrastructure et aux systèmes mis à rude épreuve** • Gestion proactive des incidents • Surveillance continue • Connaissance des solutions cloud et des outils d'automatisation essentielle
Spécialiste en géomatique	■■■□□	
Spécialiste infrastructure	■■□□□	
Spécialiste systèmes, réseaux et sécurité		
Analyste SOC		
Conseiller support technique	■□□□□	
Responsable sécurité de l'information		
Spécialiste support	■□□□□	

Légende : ■■■■■ Impact maximal

▲ La transformation numérique et l'essor des menaces cyber imposent ainsi **une mutation profonde des métiers du numérique**. Il faut dorénavant appréhender la cybersécurité comme un enjeu transversal dans toutes les fonctions, allant de la conception à l'exploitation des solutions technologiques.

Cette évolution entraîne des ajustements majeurs au niveau des compétences, avec une demande accrue pour des profils techniques et spécialisés, tels que les développeurs, analystes de sécurité, et experts en infrastructures. En parallèle, des métiers plus généralistes doivent également s'adapter en intégrant des pratiques de gestion des risques et de conformité réglementaire.

L'impact est particulièrement marqué dans les domaines où **l'innovation technologique est rapide, comme l'intelligence artificielle, la blockchain et l'IoT**. Ces secteurs nécessitent des compétences avancées pour anticiper les menaces émergentes et intégrer des mécanismes de sécurité dès la phase de conception.

FOCUS SUR LES METIERS CYBER/VOLUMETRIE EN JEU

▲ Les **besoins en talents dans le domaine de la cybersécurité s'annoncent important à l'horizon 2028**. Cette montée en puissance s'explique par la sophistication croissante des menaces, l'accélération de la transformation numérique et le renforcement des exigences réglementaires. Certains profils, à l'instar des consultants, des développeurs spécialisés en sécurité et des analystes SOC, se révèlent particulièrement recherchés. Parallèlement, l'accent est mis sur le développement de compétences à la fois pointues et transversales, indispensables pour garantir la protection des infrastructures critiques et assurer une gouvernance adaptée aux défis émergents. **Les deux tableaux infra pointent quelques modulations**.

Dans les tableaux ci -dessous, le nombre de cases indique la croissance annuelle prévue des emplois :

■ (0-3%), ■■ cases (4-7%), ■■■ (8-10%) et ■■■■ (+10%).

Métiers de la cybersécurité	Croissance Emploi Horizon 2028	Besoins quantitatifs / commentaires
RSSI	■■■■	• Besoins croissants dans les grandes entreprises et les secteurs critiques. • Recrutement urgent pour garantir une gouvernance efficace face aux menaces. • Manque de profils formés avec des compétences transversales en gestion et en cybersécurité.
Consultant en cybersécurité	■■■■	• Très demandé, particulièrement dans les ESN. • Recrutement ponctuel pour des missions spécifiques ou des audits réguliers. • Profils très variés, pouvant se spécialiser sur des sujets plus spécifiques (cryptologie, gouvernance, cloud...)
Développeur sécurité	■■■■	• Besoin important avec l'adoption du DevSecOps. • Formation insuffisante pour combiner développement et sécurité.
Analyste OSINT	■■■□	• Profils recherchés pour surveiller les cybermenaces et collecter des informations dans les SOC et CERT. • Demande en hausse avec l'utilisation croissante d'outils de veille et d'analyse.
RPCA	■■■■	• Demande soutenue pour garantir la continuité d'activité dans les industries critiques. • Souvent combiné avec des obligations réglementaires liées à la gestion des crises.
RPRI	■■■■	• Profils nécessaires pour anticiper et gérer la reprise des infrastructures informatiques après des incidents. • Formation limitée pour répondre à ces besoins spécifiques.
DPO	■■■□	• En hausse depuis l'entrée en vigueur du RGPD. • Expertise en protection des données et maîtrise des enjeux réglementaires. • Besoin de formations pratiques en lien avec des outils technologiques.
Analyste SOC	■■□□	• Très forte demande pour surveiller et répondre aux incidents en temps réel. • Externalisation fréquente vers des SOC mutualisés pour répondre aux besoins des PME.
DSI	■□□□	• Besoins modérés, mais essentiel pour les entreprises transformant leur stratégie IT en intégrant la cybersécurité. • Besoins à court/moyen terme pour des secteurs en pleine transition numérique. • Souvent en lien avec les industries réglementées (santé, finance).
Cryptologue	■■□□	• Volume faible, mais stratégique pour les organisations manipulant des données sensibles. • Majoritairement présent dans les secteurs de la défense et de la finance.

Métiers de la cybersécurité	Croissance Emploi Horizon 2028	Besoins quantitatifs / commentaires
Administrateur réseau	■■■□	• Rôle clé pour assurer la sécurité des infrastructures réseau, surtout dans le cloud. • Évolution des compétences nécessaires pour répondre aux nouvelles menaces.
Expert en intrusion et test	■■■□	• Profils essentiels pour évaluer les failles des systèmes via des tests d'intrusion. • Tendance à l'offshoring intra-européen du métier de Pentester (pour les tests « basiques »)
Responsable du CSIRT	■■■□	• Nécessaire pour coordonner les réponses aux incidents dans les entreprises de grande taille. • Demande accrue dans les secteurs critiques pour structurer les équipes cyber.
Responsable du SOC	■■■□	• Indispensable pour superviser les opérations des SOC internes et gérer les analystes. • Profils expérimentés rares sur le marché.
Bug bounty hunter	■■□□	• Recrutement ponctuel pour tester des systèmes critiques via des plateformes spécialisées. • Très peu de formations académiques disponibles pour ce rôle.
Architecture et Intégration	■■□□	• Profils recherchés pour intégrer la cybersécurité dès la conception des projets IT. • Particulièrement critique dans les projets nécessitant une sécurité "by design" (majorité des projets portés aujourd'hui).
Auditeur sécurité SI	■■■■	• Demande constante pour évaluer la conformité des systèmes et répondre aux normes réglementaires. • Profils nécessaires pour les audits réguliers, souvent externalisés. • Un nombre restreint d'auditeurs certifiés, souvent accompagnés par des consultants
Red teamer / Blue Teamer	■■■□	• Red team : Profils techniques essentiels pour simuler des attaques avancées. • Blue team : Profils défensifs recherchés pour anticiper et contrer les cyberattaques.
Offre SECaaS	■■□□	• Augmentation des besoins pour mutualiser les solutions de cybersécurité. • Profils souvent externalisés vers des centres spécialisés ou ESN.

Légende : ■■■■ = Forte croissance

Les prévisions ci-dessus intègrent les gains de productivité attendus et l'impact de l'offshoring sur les besoins en ressources humaines à l'échelle nationale.

La méthodologie utilisée pour déterminer les besoins RH à horizon 2028 est détaillée dans la partie 4.2, dédiée aux scénarios prospectifs.

QUELLES COMPETENCES DEMAIN POUR DEPLOYER LA CYBERSECURITE ?

▲ Le domaine de la cybersécurité rassemble une large palette de compétences, **couplant des aptitudes comportementales poussées (soft-skills) avec des compétences techniques et technologiques avancées**. Les soft-skills englobent des qualités comme la gestion de projets, la communication et l'adaptabilité, nécessaires pour collaborer efficacement et gérer les situations complexes. Les compétences techniques, quant à elles, incluent des savoir-faire spécifiques comme la maîtrise des normes, les tests d'intrusion ou encore l'analyse des cyberattaques, essentiels pour implémenter et maintenir des systèmes de sécurité robustes. Les trois tableaux ci-dessus visualisent les compétences majeures en isolant volontairement par convenance celles liés à des évolutions technologiques éminemment structurantes (intelligence artificielle, l'IoT, la blockchain et la 5G…). Un panorama détaillé et complet de 66 compétences identifiées est disponible en annexe p.92 pour approfondir si besoin l'analyse.

Soft-skills

- **Comprendre** les **interactions transverses** de la cybersécurité avec **les métiers de l'organisation**
- Savoir **écouter les besoins**, agir en toute discrétion et retranscrire correctement les besoins exprimés
- S'adapter à l'évolution rapide de l'environnement de la cybersécurité en faisant preuve de **curiosité** pour rester à jour face aux nouvelles menaces et technologies
- Être capable de **sensibiliser et acculturer de manière itérative les équipes non techniques** aux enjeux de la cybersécurité et d'expliquer les concepts complexes de manière simple
- Savoir gérer et réagir de manière efficace et rapide aux incidents de sécurité [**mitigation des incidents**]
- **Communiquer** efficacement à l'oral et à l'écrit, avec une maîtrise du français et de l'anglais
- Pouvoir mener un projet de cybersécurité et manager une équipe [**gestion de projets cyber**]

Compétences « techniques »

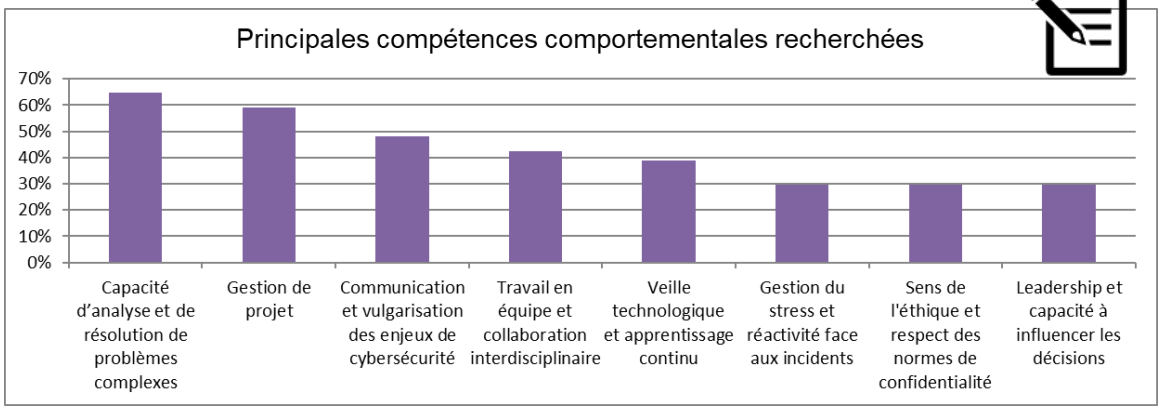
- Maîtriser les **techniques d'attaque** pour tester la résilience des systèmes. [***Mitre att&ck]***
- Maîtriser les différentes normes I**SO 27000**, **NIS2…,** appliquer les exigences des qualifications professionnelles (**PRIS**, **PASSI**, **PAMS**, etc.), et intégrer les labels associés comme **SecNumCoud** pour assurer la conformité
- Coder en tenant compte des bonnes pratiques de sécurité pour réduire les vulnérabilités dès la conception des logiciels [**Secure by design**]
- Développer une expertise en tests de pénétration et en chasse aux failles de sécurité dans les systèmes [***pentesting et bug bounty]***
- **Évaluer la robustesse des systèmes** et identifier les points faibles
- Maîtriser la gouvernance de la cyber de l'information afin d'assurer la cohérence de la politique de sécurité du SI.
- **Comprendre l'architecture globale** des systèmes pour anticiper les vulnérabilités potentielles
- Analyser a posteriori une cyberattaque [***analyse forensic***]
- Élaborer des procédures de **gestion de crise**, en y intégrant des aspects décisionnels
- Mettre en œuvre une **approche SOAR** (Security Orchestration, Automation and Response) au sein des entreprises
- Comprendre les métiers et **environnements dans lesquels les systèmes s'appliquent** pour intégrer les besoins **dès le développement**, par exemple pour l'IoT, avec une compréhension de la fonction utile d'une ligne de production.
- Disposer d'une **double compétence sûreté des process / cybersécurité**, pour intervenir sur des problématiques de cybersécurité industrielle

Compétences liées aux nouvelles technologies

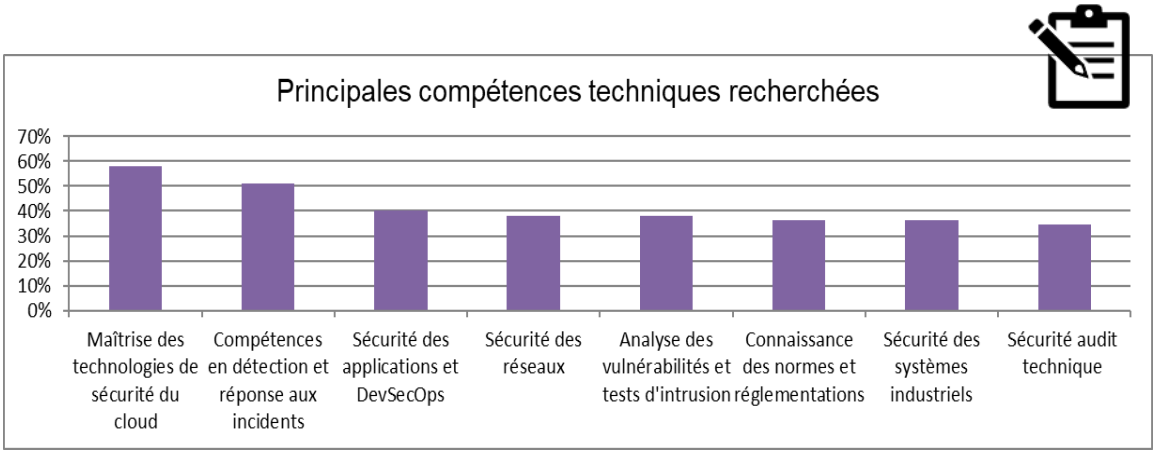
- Protéger les systèmes contre les **attaques automatisées** propulsées **par l'intelligence artificielle** et comprendre les impacts de l'informatique quantique sur les algorithmes de **cryptographie**
- **Sécuriser les dispositifs IoT**, qui représentent une faille critique pour de nombreuses industries (ex. santé, énergie)
- **Connaître les mécanismes de sécurité dans la blockchain**, en particulier pour l'authentification et la gestion des identités
- Maîtriser les **infrastructures cloud** et **identifier les failles potentielles** dans la chaîne de **fournisseurs** et **prestataires** (supply chain security)
- Comprendre **les vulnérabilités associées à la 5G**, notamment dans les secteurs critiques comme les transports ou la santé

COMPETENCES CLES RECHERCHEES POUR LA CYBERSECURITE

▲ Les compétences comportementales occupent une place centrale dans la constitution d'équipes polyvalentes capables d'évoluer dans des **environnements complexes et dynamiques**. Une importance particulière est accordée à la collaboration et à la communication, reflétant une prise de conscience croissante des enjeux humains liés à la cybersécurité. Par ailleurs, les attentes en matière **de leadership et d'éthique** traduisent une évolution des profils recherchés vers des **fonctions stratégiques et décisionnelles**, nécessitant des qualités de gestion et d'influence pour faire face aux défis contemporains



▲ L'évolution rapide des **technologies émergentes, telles que le cloud et DevSecOps**, redéfinit les priorités techniques dans le recrutement. La diversité des compétences techniques recherchées illustre le besoin croissant d'une approche globale et intégrée en cybersécurité. Cette tendance répond à **des menaces de plus en plus sophistiquées et ciblées**, imposant aux professionnels d'acquérir une expertise pointue pour assurer une protection efficace. Cette montée en compétences se heurte toutefois à plusieurs freins, notamment le manque de budgets dédiés, l'insuffisance de spécialisations dans les formations disponibles, le temps limité consacré à l'apprentissage et l'absence de formations certifiantes. Ces contraintes freinent l'adaptation aux nouveaux enjeux et complexifient l'accès aux qualifications nécessaires.



Principaux freins cités à la montée en compétences sont :

- Le manque de budget dédié à la formation,
- Le manque de spécialisation des formations disponibles
- Le manque de temps alloué à la formation
- Le manque de formations certifiantes

CE QU'IL FAUT RETENIR

1. **Les entreprises adoptent des stratégiques très diverses face aux menaces cyber : certaines investissent massivement dans la sécurité (approche proactive), tandis que d'autres privilégient des réponses ponctuelles (approche réactive) ou restent vulnérables par manque de ressources.**

2. **Les motivations au développement de la cybersécurité incluent la pression réglementaire, la croissance des attaques et la nécessité d'intégrer l'IA et l'IoT. Les freins, quant à eux, sont majoritairement liés aux contraintes budgétaires, au manque de compétences, et à la difficulté d'attirer et de retenir les talents.**

3. **Les secteurs comme la finance et l'assurance sont perçus comme étant plus avancés en cybersécurité, tandis que d'autres, comme l'hôtellerie et l'immobilier, accusent un retard en raison de ressources limitées. Plus généralement les TPE, se sentant faussement à l'abri, cumulent du retard.**

4. **Les grandes entreprises ont tendance à internaliser leurs besoins en cybersécurité pour partie tout en mobilisant des prestataires numériques, tandis que les PME privilégient l'externalisation pour réduire les coûts. L'externalisation via des ESN ou l'offshoring est courante pour des prestations spécifiques comme les tests d'intrusion ou la gestion des incidents.**

5. **Les besoins en compétences sont en forte croissance, avec des profils recherchés comme les analystes SOC, les experts en intrusion et les développeurs spécialisés.**

6. **La cybersécurité impacte l'ensemble des métiers du numérique, nécessitant des compétences techniques et comportementales. L'émergence de nouveaux métiers liés à la sécurité des infrastructures cloud, à la gestion des risques et aux technologies comme l'IA et la blockchain reflète l'évolution des besoins.**

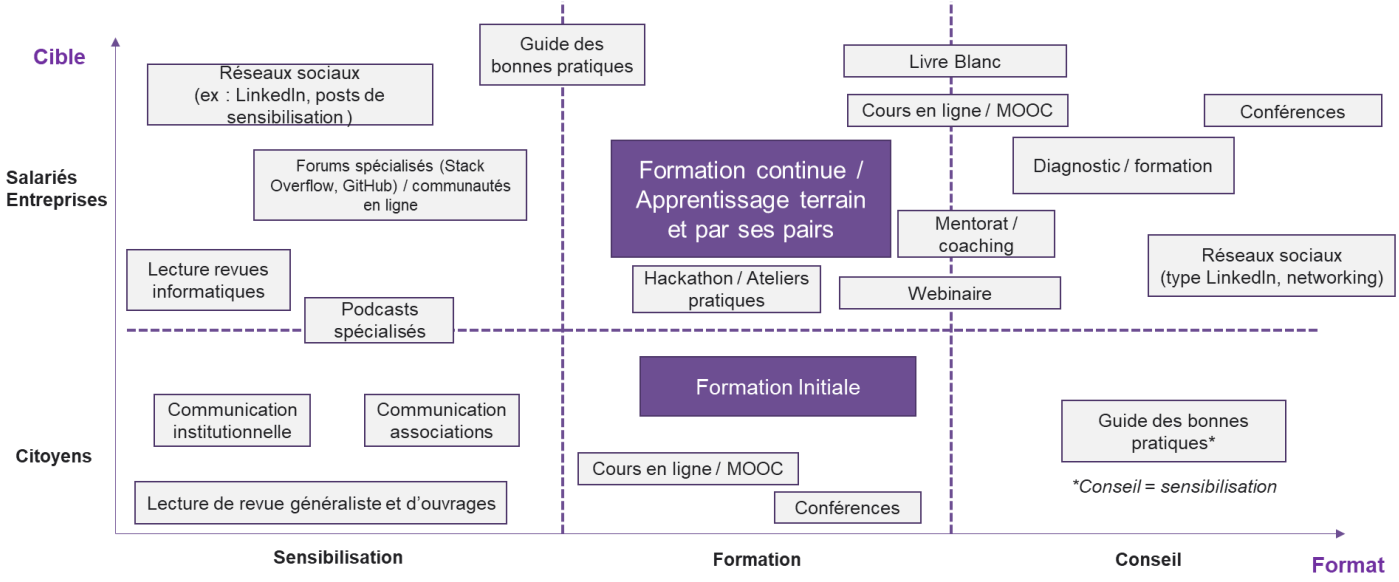
7. **Les principales compétences recherchées couvrent un large éventail, des soft-skills (gestion de projet, communication) aux compétences techniques (tests d'intrusion, sécurité cloud). Les obstacles à la formation se manifestent à travers le coût inhérent, le manque de temps disponible et l'absence de spécialisations véritablement adaptées aux besoins du secteur.**

PARTIE 3. OFFRE DE FORMATION EN LIEN AVEC LA CYBERSECURITE

3.1.MODALITE D'ACQUISITION DE COMPETENCES CYBERSECURITE ET PLACE DE LA FORMATION

▲ Le renforcement des compétences en cybersécurité repose sur un éventail de dispositifs variés, finement adaptés aux exigences spécifiques des entreprises, des employés et des citoyens. Il s'incarne à travers des actions de sensibilisation, des formations initiales et continues, ainsi que des dispositifs de conseil et d'accompagnement. Cette montée en compétences s'appuie aussi sur une palette d'outils tels que les cours en ligne, les webinaires, les hackathons, les guides de bonnes pratiques ou encore les réseaux sociaux professionnels. Cette diversité d'approches illustre la nécessité d'allier théorie et pratique afin de mieux armer chacun face aux défis concrets du terrain.

Modalités d'acquisitions de compétences



Panorama de la formation & Thématiques Cyber

	FORMATION INITIALE	FORMATION CONTINUE				
Type de structure	Grandes Ecoles et universités	Autoformation	Entreprises conseil	ESN	Grandes Ecoles & universités	Associations
Modalités	Thématique abordée dans des cursus classiques type licence ou master	Modules de formation Livre blancs/ verts Articles	Modules de formations Ateliers allant de la sensibilisation à l'expertise technique en mettant en place des feuilles de route	Modules de formations Ateliers allant de la sensibilisation à l'expertise technique en mettant en place des feuilles de route	MOOC En classe ou à distance	Format divers
Public cible	Etudiants / Stagiaires / Alternants	Tout public	Salariés d'une entreprise	Salariés d'une entreprise	Tout public	Tout public
Compétences développées	Curiosité intellectuelle Méthodologie d'apprentissage et de travail Savoir-être Compréhension des sujets généraux Culture générale (entreprise…)	Compétences techniques Savoir-être	Compétences techniques Savoir-être	Compétences techniques	Compétences techniques	Compétences techniques Compréhension générale du sujet

▲ La transformation numérique et la crise sanitaire ont accentué la nécessité de faire évoluer l'offre de formation, en intégrant des formats adaptés au télétravail et à la transmission interne des connaissances.

75% des répondants affirment proposer des formations en cybersécurité à leurs salariés, et confirment les modalités retenues

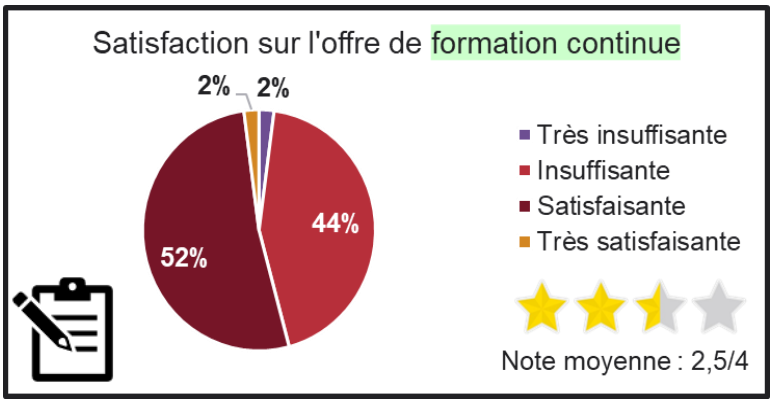
3.2. PERCEPTION DE L'OFFRE DE FORMATION PAR LES ENTREPRISES

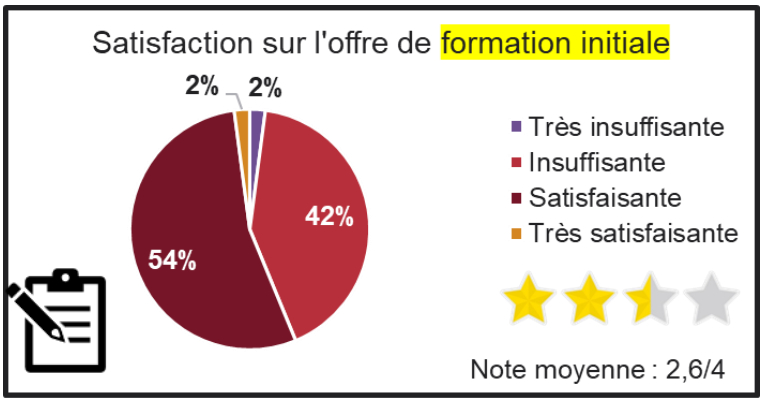
- L'essor des formations en cybersécurité s'inscrit en réponse à une demande en constante croissance. Ce développement repose sur une offre plurielle, allant des cursus académiques aux modules en ligne, en passant par des certifications spécialisées. Toutefois, des axes d'amélioration subsistent : mieux accompagner les PME et ETI, intégrer les avancées technologiques émergentes et renforcer des compétences transversales essentielles, telles que la gestion de crise et les techniques de communication
- La perception de l'offre de formation en cybersécurité s'avère contrastée. Si ces parcours couvrent un large spectre de besoins, ils laissent entrevoir des attentes insatisfaites sur des aspects cruciaux tels que la sécurité des applications, la conformité réglementaire ou la gestion des incidents. Parmi les défis majeurs à relever figurent un déficit de technicité dans certains programmes, des contenus parfois trop théoriques ou, à l'inverse, excessivement spécialisés, limitant ainsi une approche à la fois globale et pragmatique. Cette situation souligne l'urgence d'adapter l'offre de formation afin de mieux répondre aux exigences du marché et aux évolutions technologiques

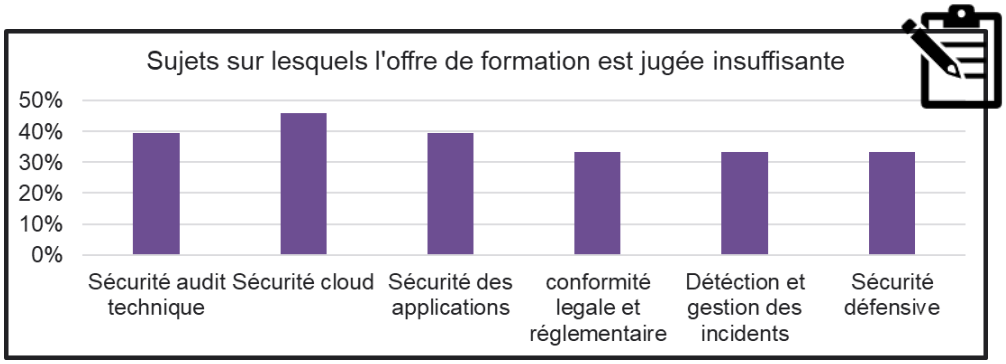
Synthèse perception des entreprises

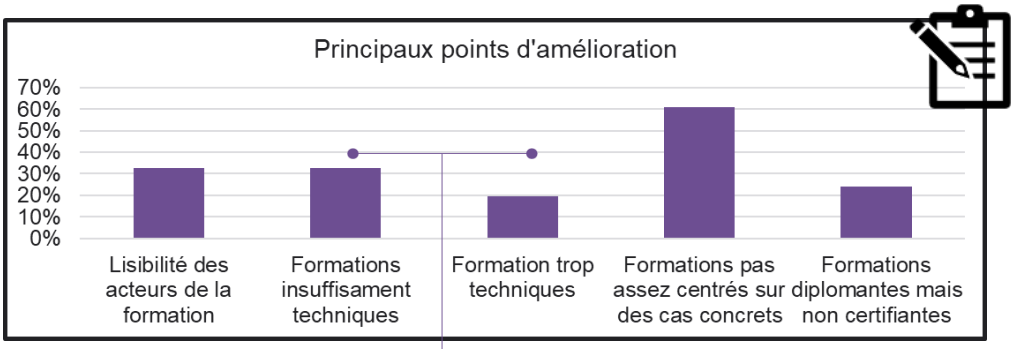
	POINTS POSITIFS	AXES D'AMÉLIORATION
	• **Existence de programmes en cybersécurité dans certaines grandes écoles d'ingénieurs et universités (Telecom Paris, Ecole polytechnique etc.)** • **Nombreux profils issus de Masters en Relations Internationales ou en Sciences Politiques, de plus en plus ciblés par les ESN** • **Multiplication des parcours de formation initiale à dominante cybersécurité (BTS, Bachelor, BUT, Master…)** • **Intégration croissante des soft skills dans les formations initiales en cybersécurité, répondant à la nécessité de compétences en communication, collaboration et gestion de crise.**	• **Manque de formations adaptées aux besoins spécifiques des PME et ETI (surtout pour les compétences transversales en cybersécurité)** • **Programmes souvent trop techniques, et pas assez centrés sur la gouvernance et l'analyse de risques** • **Insuffisance de formations intégrant les nouvelles technologies (IA, IoT, Blockchain, Quantique…) et les enjeux réglementaires** • **Formations intégrant trop peu les Soft Skills (relation client, capacité de vulgarisation, communication écrite et orale)** • **Augmentation importante de formations en alternance. Des étudiants qui ont souvent du mal à se trouver une entreprise…** • **…et des rythmes d'alternance proposés par les écoles incompatibles avec la réalité d'une entreprise et des projets cyber menés** • **Manque de pragmatisme face aux évolutions des besoins du marché** • **…de niveau parfois trop hétérogène (manque de lisibilité, utilisation du terme cybersécurité dans une démarche « marketing »)**
	• **Disponibilité de formations en ligne et de modules e-learning adaptés à l'autodidacte** • **Nombreuses formations certifiantes (en gouvernance, sécurité cloud, etc.) pour des compétences spécifiques** • **Accès à des formations de qualité en partenariat avec des organismes comme SANS Institute et l'ANSSI**	• **Offre de formation parfois peu lisible, notamment pour les formations avancées et spécialisées** • **Difficultés pour certaines entreprises (notamment TPE et PME) d'accéder aux formations pointues, faute de budget**
 Autres leviers	• **Initiatives d'associations et clubs de cybersécurité (ex. CESIN, Hexatrust) pour sensibiliser et échanger** • **Création de forums, séminaires et événements pour favoriser l'apprentissage en continu et le networking** • **Programmes de reconversion pour attirer des profils non techniques vers la cybersécurité** • **Plateformes de formations sectorielles (ex. Campus Atlas) pour faciliter l'accès aux compétences clés avec des tarifs négociés**	• **Formations diplômantes mais pas certifiantes** • **Formations pas assez centrées sur des cas concrets**

▲ Les résultats de l'enquête en ligne confirment cette photographie synthétique de l'offre de formation. Les graphiques ci-après reprennent les principaux résultats de l'enquête en ligne









Une contradiction apparente, commentaire :

- Illustration de la grande diversité des formations nécessaires et attendues autour de la Cyber…
- …des formations parfois un peu « légères » sur le contenu technique et les impacts des nouvelles technologies
- …des formations trop techniques ne donnant pas une vision holistique du sujet

3.3.PANEL DES FORMATIONS PROPOSEES

▲ L'examen de l'offre de formation débouche sur un inventaire très consistant de formations disponibles à l'échelle nationale. Pour bâtir la base l'équipe a procédé dans un premier temps à une recherche approfondie par mots-clés sur internet et sur des plateformes spécialisées telles celles du Carif Oref. D'autre part, des entretiens menés auprès de professionnels du secteur ont enrichi cette analyse par une perspective plus qualitative.

Les formations en cybersécurité ont été classées selon plusieurs critères afin de mieux identifier les offres disponibles. Cette classification repose sur la typologie des organismes proposant ces formations, incluant les universités, les écoles, les organismes de formation continue, les ESN, les cabinets de conseil et les associations. Elle tient également compte du niveau des apprenants, qu'ils soient débutants ou intermédiaires, et de la possibilité d'obtenir une certification officielle à l'issue de la formation.

Actuellement, **plus de 1 000 solutions de formation sont référencées,** couvrant sur le papier tout le spectre des besoins. Elles incluent des formations initiales, qui bien que non spécifiques à la cybersécurité, intègrent certains aspects liés à la discipline. De nombreuses formations continues, comprenant des modules spécifiques, sont également proposées par des écoles, des universités et des organismes de formation continue. En complément, des formations continues à forte visibilité sont offertes par des ESN, des cabinets de conseil et divers autres acteurs. Certaines associations proposent également des programmes adaptés pour compléter ces parcours.

Extrait de la base de formation

Intitulé de la formation	Nom du porteur / organisme	Typologie d'organisme	Principal thématique Cyber de la formation	Certification	Niveau
Cybersécurité et hacking éthique	Cyberini	Organisme de formation continue	Hacking éthique, tests d'intrusion	Oui	Débutant - intermédiaire
CompTIA S+ : les bases de la cybersécurité	Oo2 formations	Organisme de formation continue	Fondamentaux de la cybersécurité	Oui	Débutant
Analyste Cybersécurité SOC	OpenClassrooms	MOOC	Cybersécurité, analyse SOC	oui	Débutant à avancé
Cybersécurité - essentials et fullstack	Jedha	Organisme de formation continue	Sécurité informatique, Pentest	oui	Débutant à avancé
Expert en gouvernance de la sécurité des réseaux et des systèmes - BC02 Conduire un projet de cybersécurité	Télécom SudParis	Université, école et formation initiale	Gouvernance de la cybersécurité	oui	Niveau avancé, professionnels
Responsable cybersécurité	Orsys	Organisme de formation continue	Gestion des systèmes de cybersécurité	oui	Niveau intermédiaire à avancé
Fondamentaux techniques de la cybersécurité	HS2 - Herve Schauer Securite	Organisme de formation continue	Principes techniques de la cybersécurité	oui	Niveau intermédiaire à avancé
Socle technique de la cybersécurité	Deloitte	Conseil	Cybersécurité technique, bases essentielles	oui	Débutants et reconversion
Master Cybersecurity	Ecole polytechnique	Université, école et formation initiale	Cybersécurité avancée et analyse de systèmes	oui	Niveau Bac+5
Master Cybersécurité	EPITA	Université, école et formation initiale	Cybersécurité, ingénierie des systèmes	oui	Niveau Bac+5
Mastère spécialisé en ingénierie de la cybersécurité	ECOLE NATIONALE SUPERIEURE MINES - TELECOM Lille Douai	Université, école et formation initiale	Cybersécurité, ingénierie des systèmes	oui	Niveau Bac+5

Une cartographie plus exhaustive des formations est accessible sur le site internet de l'OPIIEC.

50% des répondant affirment qu'ils solliciteraient l'OPCO Atlas pour des formations en cybersécurité

PRINCIPALES FORMATIONS CITEES LORS DES ENTRETIENS

▲ Le panorama des principales formations en cybersécurité mises en avant par les entreprises lors des entretiens constitue un complément très utile à l'inventaire complet évoqué en page précédente. Elle distingue les formations initiales, dispensées par des écoles d'ingénieurs et d'universités, des formations professionnelles proposées par des organismes spécialisés et des associations. Ce recensement reflète la diversité des parcours disponibles pour répondre aux besoins croissants en compétences et accompagner les professionnels dans leur montée en expertise. Il met également en lumière les institutions les plus citées pour leur capacité à offrir a priori des cursus adaptés aux exigences du secteur.

Formations les plus fréquemment citées en entretien

Formation initiale

- Ecole polytechnique
- ENSIBS (Université Bretagne Sud) / CyberSkills4All
- ENSTA
- EPITA
- ESAIP Angers
- ESLIV
- IAE Paris Science
- ISEN Lille (Junia)
- Mines de Nancy
- Telecom Paris
- UBS (Rennes)
- Université de Lorraine

Formation professionnelle (organisme et asso.)

Formations et modules proposés par :

- Ecole 2600
- Edugroup
- Evoluteam (Soft Skills)
- HS2
- Orsys
- SANS institue

▲ Les profils issus des écoles d'ingénieurs en formation initiale sont particulièrement prisés par les entreprises, notamment pour leur capacité à associer une expertise généraliste en architecture et réseaux avec une spécialisation en cybersécurité. Les grandes écoles, telles que Telecom Paris, Mines de Nancy et ENSTA, sont fréquemment citées pour leur excellence dans la formation de ces profils. On observe cependant une **visibilité croissante des écoles spécialisées en cybersécurité,** telles qu'ESISAR Valence, qui répondent à des besoins plus pointus du secteur.

▲ En matière de formation continue, plusieurs organismes se distinguent comme des références incontournables dans le domaine. Des organismes tels que HS2, SANS Institute et Orsys sont reconnus pour leurs programmes adaptés et modulaires. Cependant, les politiques de formation varient selon les entreprises, **certaines optant pour des formations entièrement externalisées tandis que d'autres préfèrent des modules plus internalisés**. Cette diversité permet aux entreprises d'adopter des stratégies de formation alignées sur leurs besoins spécifiques et leurs ressources internes.

CE QU'IL FAUT RETENIR

1. **Les compétences en cybersécurité s'acquièrent à travers divers dispositifs de formation, allant des cursus initiaux et continus aux certifications spécialisées, en passant par des outils dynamiques tels que les webinaires, les hackathons et les plateformes e-learning. Cette diversité favorise un apprentissage progressif et adapté aux évolutions constantes du domaine.**

2. **Bien que l'offre soit perçue comme riche et variée, des lacunes persistent, notamment pour les PME et ETI qui peinent à accéder à des formations adaptées. Les programmes sont parfois jugés trop techniques ou insuffisamment centrés sur la gouvernance, la gestion des risques et les compétences transversales.**

3. **Les nouvelles technologies (IA, IoT, blockchain, quantique) nécessitent des formations spécifiques pour accompagner leur adoption sécurisée. Ces domaines restent cependant encore peu couverts dans les programmes actuels, engendrant un décalage avec les besoins réels du marché.**

4. **L'intégration des soft-skills, comme la communication et la gestion de crise, devient une priorité pour répondre aux besoins croissants de polyvalence et d'adaptabilité. Ces compétences demeurent encore parfois sous-représentées dans la majorité des cursus.**

5. **Les écoles d'ingénieurs et les universités jouent un rôle clé dans la formation initiale, tandis que des organismes spécialisés comme SANS Institute, Orsys et HS2 dominent la formation continue avec des programmes certifiants (liste non exhautive bien entendu). Les formations restent souvent difficiles d'accès pour les petites entreprises en raison de leur coût ou de leur format peu flexible, peu adaptée à la PME**

6. **Des initiatives de reconversion sont développées pour attirer des profils non techniques et espérons-le plus féminins vers la cybersécurité, mais des efforts restent nécessaires pour rendre ces parcours plus accessibles et mieux adaptés aux attentes des entreprises.**

PARTIE 4. DEVELOPPEMENT DE LA CYBERSECURITE : SYNTHESE ET RECOMMANDATIONS

4.1.SYNTHESE ET ENJEUX

ANALYSE SWOT

▲ L'ensemble des données et des analyses présentées tout au long du rapport est résumé dans le tableau ci-dessous. L'approche SWOT offre une vision synthétique des forces, faiblesses, opportunités et menaces identifiées dans le domaine de la cybersécurité, mettant en lumière les principaux enjeux stratégiques et opérationnels auxquels la branche doit faire face.

FORCES	FAIBLESSES
▪ Un écosystème proactif : structures publiques et association de références ▪ Des guides techniques et outils de sensibilisation nombreux ▪ Les mesures de soutien aux PME pour renforcer leur cybersécurité (exemple des diagnostics cyber en partie subventionnés) ▪ L'émergence de conseil et acteurs du numérique spécialisés Cyber… ▪ …. complétant la présence de fleurons historiques dans le domaine (Thales, Orange, etc.) ▪ Une offre efficace et efficiente de RSSI à temps partagé ▪ **La structuration en cours de pôles cyber dans les grandes organisations** ▪ **La qualité et la diversité de la formation** ▪ **La diversité des formats de formation / sensibilisation** ▪ **Des certifications en place sur la cybersécurité** ▪ **L'ouverture à la Cyber du catalogue Campus Atlas**	▪ La capacité à investir massivement au sein de la branche et chez les clients sur le thème de la cybersécurité ▪ **La pénurie de talents dans le secteur du numérique…** ▪ **…et des difficultés de recrutement particulièrement marquées dans la cybersécurité** ▪ **L'attractivité, image et compréhension de la réalité et diversité des métiers cyber : « truc de geek »** ▪ **Le foisonnement et le manque de lisibilité de l'offre de formation** ▪ **L'intégration en temps des évolutions technologiques dans la formation cyber (Cloud, blockchain, IOT, IA …)**
OPPORTUNITES	**MENACES**
▪ La prise de conscience grandissante des organisations et des citoyens ▪ Les préoccupations autour de l'intelligence économique et souveraineté nationale ▪ L'accélération de la pression réglementaire chez les clients (et risques financiers / amendes) Ex. : NIS2 ▪ La digitalisation croissante – tous pans de l'économie - et l'impératif absolu de cybersécurité ▪ La pression croissante des grandes organisations en direction de leurs fournisseurs, maillons faibles dans le dispositif ▪ **Le développement généralisé d'une offre cyber (a minima) par les entreprises du numérique en direction de leur client** ▪ **De nouvelles technologies au service de la cybersécurité**	▪ La hausse de la cybercriminalité et les tensions géopolitiques ▪ Une croissance économique « molle » et des contraintes « administratives / improductives » supplémentaires sur les TPE ▪ La Cybersécurité vu comme un coût et non comme une opportunité ou un axe de différenciation par les entreprises ▪ **Les limites de l'appareil de formation actuel pour couvrir les besoins de demain (quantitatifs et qualitatifs)** ▪ **Un manque d'attractivité persistant des métiers de la cybersécurité ?**

■ **Items au cœur des problématiques des ressources humaines**

PRINCIPAUX ENJEUX IDENTIFIES

ENJEU 1 : POURSUIVRE LA SENSIBILISATION AUTOUR DE LA CYBERSECURITE

- Il est d'une importance capitale de diffuser largement les enjeux de la cybersécurité, en particulier auprès des très petites et moyennes entreprises. Pour ce faire, les clubs d'entreprises, les pôles et les clusters constituent des vecteurs privilégiés de sensibilisation et d'accompagnement.
  Par ailleurs, une communication soutenue sur les menaces cybernétiques les plus critiques s'impose, afin d'éveiller les consciences et d'instaurer une vigilance accrue face aux risques grandissants.
  Enfin, il est essentiel d'adapter les offres de services en cybersécurité aux réalités financières et organisationnelles propres aux PME. Seule une approche sur mesure leur permettra d'affronter efficacement les défis d'un monde numérique en perpétuelle évolution.

ENJEU 2 : RENFORCER L'ATTRACTIVITE DES METIERS DE LA CYBERSECURITE

- Il est essentiel d'élargir la sensibilisation aux multiples facettes des métiers de la cybersécurité, souvent réduits, dans l'imaginaire collectif, aux seules disciplines du Pen Test ou de la cyber-offensive. Il convient de mettre en lumière la richesse et la diversité de ces professions, encore méconnues du grand public.
  Par ailleurs, il est pertinent d'identifier et d'attirer de jeunes talents issus de formations habituellement éloignées de la cybersécurité, telles que les Instituts d'études politiques, les écoles de management ou encore les cursus en relations internationales. Cette ouverture permettra d'apporter de nouvelles perspectives et d'enrichir la filière.
  Dans cette même dynamique, les fiches métiers « Cyber », déjà recensées dans la cartographie de l'OPIIEC, méritent d'être ajustées et valorisées afin de mieux refléter l'évolution constante du secteur.
  Enfin, il est impératif d'accorder une attention particulière à la féminisation des métiers de la cybersécurité. Diversifier les profils, encourager l'accès des femmes à ces carrières et promouvoir une vision plus inclusive de la filière contribueront à façonner un écosystème plus équilibré et innovant.

ENJEU 3 : FAIRE EVOLUER ET DIVERSIFIER L'OFFRE DE FORMATION INITIALE

- L'évolution des formations en cybersécurité doit reposer sur une approche favorisant le croisement des compétences entre les métiers traditionnels et les spécialisations cyber. Il s'agit d'intégrer, de manière fluide et naturelle, des modules dédiés à la cybersécurité au sein des cursus existants. Par exemple, les ingénieurs industriels pourraient être formés à des briques cyber adaptées aux spécificités de secteurs comme l'Internet des objets ou les systèmes embarqués, répondant ainsi aux défis croissants de la sécurisation de ces technologies.
  Par ailleurs, il est crucial de mieux appréhender les enjeux de gouvernance dans les formations actuelles. Trop souvent négligées, ces problématiques revêtent pourtant une importance stratégique face aux évolutions réglementaires et aux nouvelles exigences du secteur.
  Enfin, l'intégration plus systématique de certifications reconnues, telles que celles délivrées par CISCO ou Ethical Hacker, s'impose comme un levier clé d'employabilité et de professionnalisation. Cette démarche devrait être encouragée dès la formation initiale, afin d'ancrer les compétences cyber dans des standards reconnus et opérationnels.

ENJEU 4 : FAIRE EVOLUER, DIVERSIFIER L'OFFRE DE FORMATION CONTINUE

- L'offre de formation continue en cybersécurité doit être repensée en profondeur pour mieux s'adapter aux besoins en constante évolution des entreprises et aux avancées technologiques. Il est essentiel de remplacer les modules devenus obsolètes par des formations alignées les nouvelles menaces et les cadres réglementaires émergents, tels que NIS2 ou DORA, garantissant ainsi une mise régulière des compétences.
  Par ailleurs, la diversification des formats pédagogiques représente un levier indispensable pour favoriser une montée en compétence à la fois efficace et flexible. Le développement des formations hybrides, des modules courts certifiants, de l'apprentissage en ligne et des mises en situation pratiques permettra de répondre d'une façon plus fine aux contraintes des professionnels tout en optimisant l'acquisition des savoirs.
  Enfin, l'intégration de nouveaux contenus spécialisés, tels que la cybersécurité appliquée à l'Internet des objets, à l'intelligence artificielle ou encore aux technologies quantiques, est cruciale. En anticipant ces enjeux stratégiques, l'offre de formation se positionnera comme un moteur d'innovation et de résilience face aux défis à venir.

4.2.SCENARIOS PROSPECTIFS DE DEVELOPPEMENT DE LA CYBERSECURITE

PROJECTIONS SUR L'EMPREINTE DE LA CYBER : ELEMENTS DE METHODE

RAPPEL DES OBJECTIFS DE LA MODELISATION

- Une des objectifs centraux de cette étude consiste à projeter les emplois directement liés à la cybersécurité au sein de la branche en aboutissant à une estimation globale des effectifs de la filière cyber à l'horizon 2030 tenant compte des dynamiques actuelles et des tendances émergentes. Il s'agit de prévisions à moyen terme visant à anticiper l'évolution des besoins en compétences et en formations afin d'accompagner au mieux la transformation du secteur et d'assurer une adéquation optimale entre l'offre et la demande en matière de talents spécialisés.

LA MOBILISATION DE SOURCES MULTIPLES

- L'étude s'appuie tout d'abord sur une recherche documentaire approfondie, capitalisant notamment sur plusieurs sources d'information crédibles (Xerfi, Statista, Exaegiss, ANSII, insee)

  Des entretiens qualitatifs ont été en parallèle conduits auprès d'experts et de professionnels du secteur, permettant d'enrichir les données théoriques avec les perspectives issues du terrain. Enfin, les résultats d'enquêtes en ligne ont enfin été exploités garantissant ainsi une vision aussi exhaustive que pertinente des dynamiques à l'œuvre.

METHODES ET ETAPES DU RAISONNEMENT

- Dans un premier temps, il s'est agi d'estimer les effectifs dédiés de la cybersécurité en 2024

  La démarche a ensuite consisté à simuler des projections de croissance puis à élaborer des scénarios prospectifs décrivant les évolutions du secteur. Sur cette base, des prévisions ont été établies concernant les dynamiques des métiers de la cybersécurité au sein des entreprises de la branche.

  Au-delà de ces considérations purement quantitatives, l'étude s'attarde également sur les répercussions de ces transformations pour les organisations existantes, en s'appuyant notamment sur la cartographie actualisée de l'OPIIEC au 1er décembre 2024. Cette étape, dont les résultats sont détaillés en page 44, adopte une approche résolument qualitative, mettant en lumière les impacts organisationnels et les enjeux stratégiques que soulèvent ces mutations.

DES HYPOTHESES DISCRIMINANTES POUR L'APPRECIATION DE L'IMPACT

- L'évaluation s'appuie sur plusieurs hypothèses structurantes. En premier lieu, elle prend en considération l'intensification des menaces en matière de cybersécurité, un phénomène qui façonne profondément les besoins en expertise et en protection.

  La deuxième hypothèse repose sur l'évolution des cadres réglementaires, dont les exigences croissantes influencent directement la demande en compétences spécialisées et redéfinissent les obligations des acteurs du secteur.

  Enfin, une analyse approfondie du modèle économique des prestations en cybersécurité a permis d'identifier les dynamiques spécifiques du marché, notamment en ce qui concerne les stratégies d'externalisation et les modalités d'offshoring, dont l'essor pourrait remodeler la répartition des emplois et des compétences à l'échelle internationale.

PRESENTATION DE L'APPROCHE PAR SCENARIOS ET MAPPING

SYNTHESE DE L'ANALYSE DES VARIABLES STRUCTURANTES

▲ Un consensus se dégage sur la **croissance des besoins en cybersécurité**, alimentée par l'intensification des menaces et la prise de conscience des pouvoirs publics. Des débats persistent cependant sur l'ampleur de ce phénomène dans les années à venir. Les progrès technologiques pourraient par exemple augmenter notoirement la productivité et modérer la croissance des emplois.

Les organisations adoptent des **stratégies diversifiées pour répondre à ces besoins** (cf. page 32), mixant internalisation et externalisation des prestations et compétences. Cette diversité d'approches s'exprime également dans le choix des modalités de réalisation des prestations, avec des questionnements sur l'offshoring.

VARIABLES STRUCTURANTES POUR LA CONSTRUCTION DES SCENARIOS

▲ Deux dimensions clés ont été retenues pour structurer les scénarios. Chacune d'entre elles est un indice composite de plusieurs paramètres :

- **Variable 1 : Croissance des activités cyber et effectifs liés en France**

  Cette dimension évalue la croissance des activités liées à la cybersécurité. Elle prend en compte plusieurs phénomènes :

  - La progression des attaques et le renforcement des menaces.
  - L'ampleur de la digitalisation des processus et de l'économie.
  - L'adoption des innovations technologiques et des nouvelles solutions cyber.
  - La pression réglementaire et les contraintes en matière de sécurité.
  - La capacité des organisations à assurer la continuité des opérations face aux cyberattaques.

  L'examen de l'ensemble des variables converge vers une forte probabilité de croissance soutenue des besoins en cybersécurité d'ici 2030. Cette dynamique s'explique par l'intensification des menaces, le durcissement des exigences réglementaires et l'accélération de la digitalisation des processus, autant de facteurs qui redessinent en profondeur le paysage de la cybersécurité.

  Ces tendances préfigurent une demande croissante en compétences et en services spécialisés, destinés à jouer un rôle central dans l'accompagnement de cette transformation et la sécurisation des environnements numériques de demain.

- **Variables 2 : Degré d'externalisation des actions cyber au profit des entreprises de la branche et des emplois en France**

  Cette variable cherche à apprécier la part des effectifs en France dédiés à la réalisation demain des prestations, elle prend en compte **:**

  - La prédisposition des entreprises, organisations de tous types à déléguer ces activités « cyber » aux prestataires de la branche.
  - Le taux d'offshoring des prestations au sein de la filière numérique.

  Les stratégies adoptées par les entreprises en matière de cybersécurité varient sensiblement en fonction de leur taille et leur trajectoire historique. Cependant, une tendance générale émerge en faveur d'une plus grande flexibilité et d'une expertise renforcée dans les approches curatives, ce qui conduit à un recours accru aux services des acteurs du numérique.

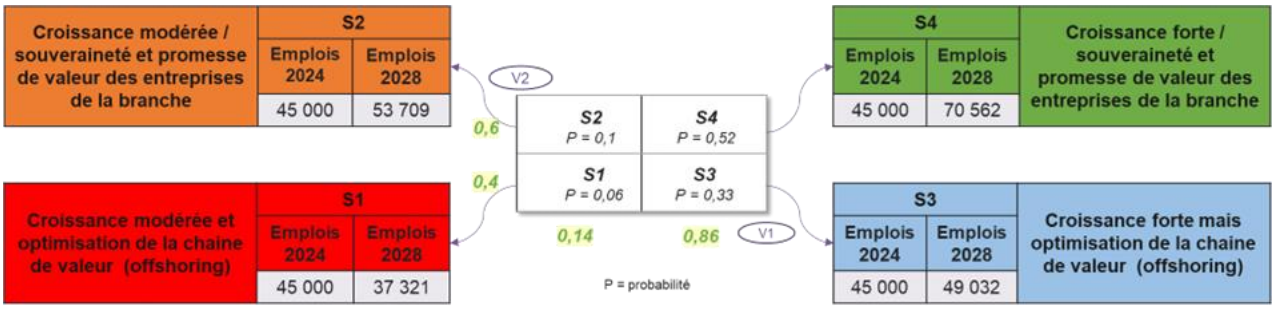
  Dans ce contexte, les organisations sont incitées à consolider leurs équipes internes dédiées à la cybersécurité, tout en s'appuyant sur des prestataires spécialisés pour répondre à des besoins spécifiques et ponctuels. Concernant l'offshoring, les pratiques restent hétérogènes, fortement influencées par l'histoire des ETI et des grands groupes. Toutefois, les impératifs de sécurité et les enjeux de souveraineté devraient limiter une externalisation massive des compétences cyber à l'international, incitant les entreprises à privilégier des modèles plus hybrides et maîtrisés.

4 SCENARIOS PROPOSES AU CROISEMENT DES VARIABLES V1 ET V2

▲ **Quatre scénarios** résultent mécaniquement du croisement des variables « V1 » et « V2 »

- Par simplification, deux valeurs extrêmes sont utilisées pour anticiper la croissance des activités cyber (V1).
- Deux scénarios opposés sont aussi proposés pour l'externalisation (V2) :
  - **Cas favorable :** Forte externalisation vers des prestataires numériques situés en France, avec peu ou pas d'offshoring.
  - **Cas défavorable :** Faible externalisation des compétences cyber par les organisations et une pratique d'offshoring modérée mais organisée dans les ESN.

Ces scénarios permettent d'explorer différents avenirs possibles pour l'évolution des besoins en cybersécurité, en tenant compte des stratégies adoptées demain par les entreprises et des dynamiques du marché.



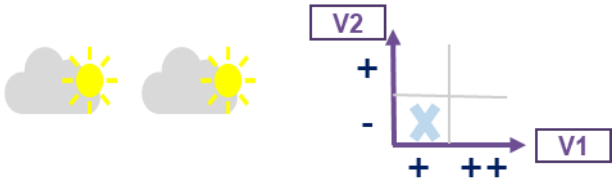
Le scénario S4, le plus probable, table sur des **perspectives de croissance significatives**, soutenues par une montée en compétences et un encadrement réglementaire limitant l'offshoring.

IMPACTS GENERIQUES POUR LA BRANCHE (COMMUNS AUX SCENARIOS)

▲ Quel que soit le scénario d'évolution envisagé, **plusieurs tendances majeures** se profilent pour la filière :

- Une augmentation significative des besoins en formation, tant en termes de volume que de fréquence, afin de maintenir les compétences à jour face aux nouveaux défis et poursuivre la sensibilisation à tous les niveaux des organigrammes.
- L'émergence de nouveaux métiers, notamment au sein des entreprises les plus innovantes et ambitieuses du secteur.
- Une montée en compétences généralisée au sein des entreprises du numérique, portée par l'évolution des menaces et des réglementations.
- Le déploiement de politiques renforcées de sensibilisation et d'éducation aux enjeux de la cybersécurité, à tous les niveaux organisationnels.
- Une adoption accrue des technologies émergentes – intelligence artificielle, cloud, IoT – pour offrir des réponses adaptées aux défis croissants de la cybersécurité.

SCENARIO 1



DESCRIPTION DU SCENARIO

- Dans ce scénario, bien que les préoccupations en matière de cybersécurité demeurent vives, plusieurs facteurs viennent **tempérer la progression des besoins**. Les organisations adoptent une approche plus intégrée, internalisant progressivement les compétences essentielles tout en s'appuyant sur des expertises internes renforcées et des solutions optimisées pour faire face aux défis cyber.

  Dans ce contexte, les entreprises du numérique se positionnent comme des acteurs incontournables d'un marché en pleine expansion, mais évoluant au sein d'une **chaîne de valeur rationalisée et optimisée**. Ce modèle privilégie l'efficacité des processus et la réactivité des services, garantissant ainsi une réponse plus agile et adaptée aux attentes des clients.

ÉLEMENTS DECLENCHEURS ET FAITS GENERATEURS

- La dynamique de ce scénario repose sur une lutte efficace contre les cybermenaces, soutenue par une pression réglementaire qui impose l'internalisation des compétences. Des accords internationaux facilitent le contrôle et la sanction des actes malveillants, renforçant la sécurité globale.

  La digitalisation des processus progresse avec des solutions intégrant des sécurités natives dès leur conception. Par ailleurs, la taylorisation et la rationalisation des tâches, combinées à une gestion optimisée de la chaîne de valeur des ESN, favorisent une approche réfléchie et mesurée de l'offshoring.

  D'autres facteurs, tels que l'intégration de l'intelligence artificielle au service de la cybersécurité et l'amélioration des outils et logiciels, contribuent également à limiter les besoins cyber.

IMPACT SUR LA BRANCHE : POINTS NOTOIRES ET SPECIFIQUES

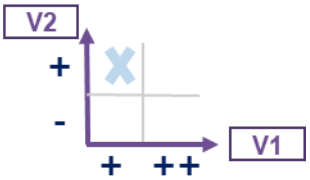
- Ce scénario se caractérise par une baisse constante des effectifs en France, conséquence directe d'une rationalisation des ressources et d'une internalisation progressive des compétences clés. La formation reste principalement orientée vers les nouvelles technologies pour accompagner la transformation numérique, mais avec des volumes moindres qu'envisagé dans des scénarios plus optimistes.

  Une large diffusion des compétences fondamentales en cybersécurité à l'ensemble des salariés est toutefois observée, permettant de compenser partiellement la réduction des effectifs spécialisés.

FACTEURS ENDOGENES A LA BRANCHE

- Certains facteurs internes influence de manière décisive ce scénario. Dans un marché moins dynamique avec une forte pression sur les prix, les prestataires explorent des solutions d'offshoring.

  Dans ce contexte, les ESN et les indépendants du numérique conservent cependant une place stratégique en comblant les lacunes existantes et en apportant un soutien aux organisations pour sécuriser leurs environnements numériques.



SCENARIO 2

DESCRIPTION DU SCENARIO

- Ce scénario repose sur une **croissance modérée des besoins en cybersécurité**, soutenue par une légère diminution des menaces et des exigences réglementaires. Cette évolution est portée par des projets de transformation numérique à petite échelle. Dans ces scénario, **l'externalisation bénéficie principalement aux les ESN (**Entreprises de Services du Numérique) afin de pallier le manque de compétences internes et optimiser les coûts. Le recours à l'offshoring reste très limité et raisonné.

  Les ESN se positionnent alors comme des partenaires stratégiques dans la gestion des risques cyber, mettant l'accent sur des offres locales et personnalisées. Ainsi, les entreprises du numérique deviennent des experts en cybersécurité au service de clients avertis, évoluant dans un marché plus mature et stabilisé.

ÉLEMENTS DECLENCHEURS ET FAITS GENERATEURS

- Ce scénario repose sur plusieurs facteurs clés. La progression modérée des menaces cyber concerne principalement les PME et les structures moins exposées, tandis que la digitalisation continue à avancer. Dans ce contexte, les projets se concentrent essentiellement sur des impératifs de mise en conformité et des besoins spécifiques, tels que la sécurisation des environnements cloud et la gestion des accès, traduisant une approche pragmatique et ciblée des enjeux de cybersécurité.

  Par ailleurs, une pression économique incite les entreprises à réduire leurs coûts en externalisant leurs activités non stratégiques. Cependant, elles préfèrent maintenir un contrôle local pour les aspects sensibles, réduisant ainsi l'attrait pour l'offshoring. Des réglementations favorisent enfin la souveraineté numérique et la protection des données locales, renforçant l'intérêt pour des solutions de proximité.

IMPACT SUR LA BRANCHE : POINTS NOTOIRES ET SPECIFIQUES

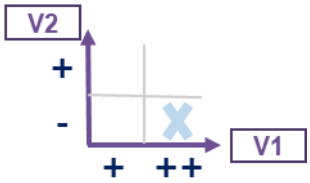
- La montée en puissance des ESN répond aux besoins des organisations publiques et privées grâce à des offres standardisées mais flexibles. Cette dynamique s'accompagne d'une demande concentrée sur des services de proximité, tels que les audits ponctuels, la mise à jour des systèmes et les services SOC locaux.

  Les acteurs de la branche développent une spécialisation sur des niches, comme la cybersécurité pour les PME ou les services publics. Cette approche, bien qu'exigeant moins de volumes en termes d'emplois, garantit néanmoins une expertise de qualité.

  Les solutions locales et régionales prévalent sur les tentations d'offshoring, réduisant les partenariats internationaux au profit d'une gestion de proximité. Enfin, la formation se concentre sur des compétences immédiatement opérationnelles, telles que la cybersurveillance, la conformité et les outils standards.

FACTEURS ENDOGENES A LA BRANCHE

- Plusieurs éléments internes renforcent la probabilité de ce scénario. Les entreprises adoptent une approche commerciale adaptée aux petites structures avec des offres « packagées » et standardisées. Les efforts se concentrent sur la proximité géographique des services pour maintenir la confiance des clients.
- Les propositions de valeur locale sont renforcées pour rivaliser avec les prestataires internationaux. Par ailleurs, bien que les investissements restent limités, ils sont ciblés sur des outils collaboratifs et des processus simplifiés, répondant spécifiquement aux besoins des clients locaux.



SCENARIO 3

DESCRIPTION DU SCENARIO

- Ce scénario repose sur une **forte croissance des besoins en cybersécurité**, alimentée par des menaces permanentes et un enjeu devenu stratégique pour les grandes entreprises et organisations publiques. Face à ces défis, les acteurs de la branche se repositionnent pour soutenir les **entreprises qui choisissent en partie d'internaliser leurs activités cyber** tout en s'appuyant avec discernement sur des prestataires de la branche

  Les entreprises de la branche se positionne pour former et accompagner les équipes internes, tout en apportant des expertises complémentaires sur des besoins spécialisés. Elles proposent également des offres offshores compétitives pour les activités non stratégiques. Cette approche hybride permet de concilier internalisation et sécurité, tout en bénéficiant d'un soutien à distance grâce à l'offshoring.

  Dans ce cadre, les entreprises du numérique se positionnent comme des partenaires essentiels pour renforcer la sécurité de clients avertis et mieux contrer les dangers permanents.

ÉLEMENTS DECLENCHEURS ET FAITS GENERATEURS

- Ce scénario est alimenté par plusieurs déclencheurs clés. Tout d'abord, un climat géopolitique tendu pousse les grandes entreprises à renforcer la protection de leurs données sensibles et de leurs activités stratégiques. Ensuite, la poursuite de la digitalisation des processus impose des exigences accrues en cybersécurité, avec une volonté de contrôler davantage les systèmes d'information en interne.

  En revanche, la concurrence internationale dans les technologies avancées, telles que l'intelligence artificielle, la cryptographie quantique et DevSecOps, incite à l'externalisation de certaines ressources pour réduire les coûts tout en maintenant un haut niveau de sécurité.

IMPACT SUR LA BRANCHE : POINTS NOTOIRES ET SPECIFIQUES

- La branche fait face à une augmentation croissante mais modérée pour des formations sur mesure destinées aux équipes internes des entreprises clientes. Cette tendance s'accompagne d'une demande accrue de **certifications et d'accréditations** visant à garantir la qualité des services offshore tout en respectant les normes internationales de cybersécurité.

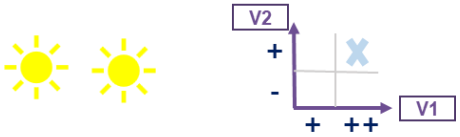
  Les acteurs du secteur se spécialisent de plus en plus, proposant des solutions d'accompagnement hybrides, qui combinent soutien aux équipes internes (formation, outils et audits) et partenariats offshores pour des missions nécessitant une forte expertise technique ou une faible criticité**.**

  Enfin, la branche tend à se structurer autour de grands partenariats internationaux. Les ESN et grandes entreprises numériques jouent un rôle clé en tant que coordinateurs globaux, assurant la gestion des ressources offshore et internes pour une couverture de sécurité optimisée

FACTEURS ENDOGENES A LA BRANCHE

- Plusieurs éléments internes viennent renforcer la probabilité de ce scénario. Les entreprises développent de nouvelles certifications et labels pour garantir la qualité des services offshore. Les équipes commerciales s'adaptent en proposant des offres hybrides, intégrant à la fois l'internalisation des compétences et l'option d'offshoring, afin de répondre aux besoins variés de leurs clients.

  En parallèle, des plateformes collaboratives sont mises en place pour intégrer efficacement les ressources offshores aux systèmes internes des clients. Ces outils facilitent la gestion des opérations et des compétences en cybersécurité, offrant ainsi une approche plus fluide et collaborative entre les équipes locales et distantes.



SCENARIO 4

DESCRIPTION DU SCENARIO

- Ce scénario est sous-tendu par une **forte croissance des besoins en cybersécurité, provoquée** par la multiplication des menaces permanentes et un enjeu stratégique devenu incontournable pour les pouvoirs publics. Face à cette situation, les acteurs du secteur adaptent leur offre de services pour répondre à un marché de plus en plus tendu, en proposant des solutions à la fois performantes et attractives.
- Cette dynamique encourage une **externalisation accrue des activités cybersécurité vers des entreprises spécialisées,** capables de recruter des experts hautement qualifiés et de fournir des services réactifs et adaptés aux exigences du marché. Ces entreprises se positionnent comme des "gardiens providentiels" de la sécurité numérique, jouant un rôle central dans la protection des organisations contre des menaces cyber croissantes et de plus en plus complexes. L'expertise des entreprises de la branche du numérique devient indispensable pour naviguer dans un environnement numérique de plus en plus risqué.

ÉLEMENTS DECLENCHEURS ET FAITS GENERATEURS

- Ce scénario repose sur plusieurs facteurs clés qui alimentent la dynamique de croissance des besoins en cybersécurité. D'abord, le maintien d'un climat géopolitique tendu, accentué par l'intensification des cyber-guerres, constitue un élément majeur déclencheur. Face à des attaques informatiques toujours plus sophistiquées et ciblées, entreprises et gouvernements intensifient leurs efforts pour sécuriser leurs infrastructures critiques.
- Ensuite, la digitalisation rapide des activités et des processus au sein des organisations **amplifie la dépendance aux systèmes d'information**. Chaque interruption, qu'elle soit liée à une cyberattaque ou une défaillance technique, peut entraîner un arrêt total des opérations, avec des conséquences financières et stratégiques majeures
- Enfin, l'innovation technologique continue, en particulier avec l'**émergence de nouvelles technologies comme l'intelligence artificielle, la cryptographie quantique et d'autres avancées, impose la mise en place de nouvelles stratégies de défense**. Ces technologies, bien qu'innovantes, apportent également de nouveaux vecteurs de vulnérabilité qu'il est crucial de sécuriser. Dans ce contexte, l'externalisation de certaines expertises spécialisées, notamment dans des domaines de pointe, devient une solution incontournable pour renforcer la résilience des systèmes face à des menaces toujours plus complexes et sophistiquées.

IMPACT SUR LA BRANCHE : POINTS NOTOIRES ET SPECIFIQUES

- Dans cette hypothèse, la branche est confrontée à des **besoins très importants en matière de recrutement et de formation,** afin de répondre à la montée en puissance des enjeux cyber. Une accélération des formations sur les nouvelles technologies s'impose pour garantir un niveau de compétence suffisant parmi les salariés.
- Par ailleurs, la diffusion d'une culture cyber et d'un socle de connaissances de base auprès de tous les collaborateurs devient primordiale. Enfin, des partenariats solides avec des Entreprises de Services du Numérique se développent.

FACTEURS ENDOGENES A LA BRANCHE

- Certains éléments internes à la branche favorisent également la survenance de ce scénario. Il s'agit notamment de l'intégration de nouvelles offres et de la montée en compétence des équipes commerciales, devenues plus persuasives sur le volet cyber. La valorisation de la marque employeur et l'attractivité des avantages proposés aux salariés jouent également un rôle clé dans le recrutement des talents nécessaires. Ce dernier point s'appuie non seulement sur des profils techniques issus des formations spécialisées, mais aussi sur des talents provenant d'autres parcours, voire de reconversion, contribuant à élargir la base des compétences disponibles.

4.3. PRECONISATIONS

Pour faire face aux défis croissants en cybersécurité, trois grands axes d'intervention émergent pour renforcer la filière et sécuriser nos activités. Ils font échos aux enjeux présentés plus en amont dans le document

- **La sensibilisation**, visant à mieux faire connaître les enjeux cyber auprès des entreprises et des salariés/ citoyens
- **L'attractivité des métiers**, pour diversifier les profils et attirer de nouveaux talents vers ces professions en tension ;
- L'offre de formation, essentielle pour adapter les compétences aux évolutions du secteur. Cette dernière se décline en **formation initiale,** intégrant la cybersécurité dès les cursus académiques, et en **formation continue**, permettant aux professionnels de monter en compétence face aux nouvelles menaces et technologies.

:

Axe 1 : Poursuivre la sensibilisation autour de la cybersécurité
Renforcer les campagnes de sensibilisation dans les entreprises, les acteurs publics et les établissements de formation à travers des événements, webinaires et supports pédagogiques accessibles.
Lancer des campagnes d'acculturation et de formation à destination des jeunes pour les sensibiliser et susciter des vocations.
Mettre en place des attestations de niveau de maîtrise en cybersécurité, à l'instar des certifications TOEIC et TOEFL.
Diffuser la connaissance et la culture cyber au sein des PME, via les grands donneurs d'ordres.

Axe 2 : Renforcer l'attractivité des métiers de la Cybersécurité
Promouvoir la diversité des métiers du cyber en mettant en avant des parcours variés (techniques, stratégiques, juridiques, gestion des risques…) et en valorisant les valeurs fondamentales de la cybersécurité.
Renforcer la visibilité des formations et des débouchés dès le lycée et dans l'enseignement supérieur via des forums, hackathons et partenariats avec les écoles.
Sensibiliser les prescripteurs de formation (enseignants, médiateurs, éducateurs jeunesse...) aux métiers de la cybersécurité afin d'orienter les jeunes vers ces carrières.
Favoriser l'inclusion et la diversité dans la filière cyber en mettant en avant des parcours inspirants et en développant des actions ciblées de communication (ex. : femmes & cybersécurité).
Valoriser les évolutions de carrière en cybersécurité et promouvoir les possibilités de reconversion vers les métiers du cyber.
Communiquer sur les métiers et parcours de la cybersécurité via les réseaux sociaux fréquentés par les jeunes.

Axe 3 : Faire évoluer, diversifier l'offre de formation initiale
Intégrer la cybersécurité dans tous les cursus IT (informatique, ingénierie, data science, etc.) comme une compétence transverse et incontournable.
Développer des spécialisations en cybersécurité au sein des grandes écoles et universités, en mettant l'accent sur des parcours professionnalisants.
Créer des formations hybrides (Management + Cyber, Droit + Cyber, Responsable Produit + Cyber, Qualité + Cyber…) pour s'adapter à l'évolution des besoins des entreprises.
Intégrer des certifications professionnelles reconnues dès la formation initiale (CEH, ISO 2700X…)

Axe 4 : Faire évoluer, diversifier l'offre de formation continue
Mettre en place des parcours de reconversion vers la cybersécurité pour répondre à la pénurie de talents et attirer des profils issus d'autres domaines.
Faciliter l'accès à des formations modulaires adaptées aux professionnels (e-learning, formations courtes, bootcamps) en mettant en place un socle de connaissance commun à toutes les formations.
Proposer des formations adaptées aux différents niveaux de maîtrise en cybersécurité, avec un parcours de progression et une validation régulière des acquis.
Intégrer des mises en situation pratiques et des exercices de simulation (red teaming, gestion de crise cyber) dans les formations continues, selon le principe de l'AFEST.
Promouvoir les certifications (RNCP, ISO) et favoriser le choix de formations certifiantes.
Développer des formations spécialisées en cybersécurité appliquée aux nouvelles technologies (sécurité de l'IA, cybersécurité des systèmes quantiques, IoT sécurisé…).
Étoffer le catalogue CampusAtlas avec de nouvelles thématiques : IoT/5G, quantique, formation spécifique pour dirigeants, nouvelles réglementations (NIS2, DORA…).

Chaque axe est détaillé plus en profondeur dans les pages suivantes, les actions phares font en outre l'objet d'une fiche action dédiée. Il appartiendra aux instances paritaires de prioriser davantage les actions notamment celles relevant des axes 3 et 4.

1 ▲ Axe 1 : Poursuivre la sensibilisation autour de la cybersécurité

Les actions retenues au titre de la sensibilisation sont récapitulées dans le tableau ci-après. Elles mobilisent une diversité d'acteurs au-delà de l'OPIIEC et de l'Opco Atlas, incluant la branche, les syndicats, les pôles et clusters. Bien que certaines actions dépassent les prérogatives directes de l'OPIIEC et de l'Opco Atlas, elles semblent essentielles pour renforcer les compétences en cybersécurité et structurer une réponse efficace face aux défis croissants du secteur.

Proposition d'actions	Précisions
Renforcer les campagnes de sensibilisation dans les entreprises, les acteurs publics et les établissements de formation à travers des événements, webinaires et supports pédagogiques accessibles.	✓ Importance de diversifier les supports et d'adapter le discours selon les publics
Ajouter / modifier des intitulés de métier sur la cartographie Opiiec	✓ DevSecOps, administrateur réseau, DSI, Soc manager, RPCA/RPRA
Lancer des campagnes d'acculturation et de formation à destination des jeunes pour les sensibiliser et susciter des vocations.	✓ Jeux, Mise en situation etc.. . Des classes primaires au collège
Mettre en place des attestations de niveau de maîtrise en cybersécurité, à l'instar des certifications TOEIC et TOEFL.	✓ Une façon « d'institutionnaliser » la cybersécurité
Diffuser la connaissance et la culture cyber au sein des PME, via les grands donneurs d'ordres.	✓ Mobiliser les grandes entreprises comme relais pour sensibiliser et former les PME aux enjeux de la cybersécurité

Les actions de sensibilisation contribueront aussi à conforter l'attractivité des métiers de la cybersécurité

2 ▲ Axe 2 : Renforcer l'attractivité des métiers de la Cybersécurité

Complémentaires au sujet de la sensibilité, les actions de promotion de l'attractivité des métiers de la cybersécurité consisteront pour partie à lutter contre les préjugés, stéréotypes et mettre en lumière la diversité des profils. Sur le scénario de croissance retenu, les besoins de recrutement seront en effet significatifs.

Proposition d'actions	Précisions
Promouvoir la diversité des métiers du cyber en mettant en avant des parcours variés (techniques, stratégiques, juridiques, gestion des risques…) et en valorisant les valeurs fondamentales de la cybersécurité.	✓ Mettre davantage en lumière les métiers liés à la gouvernance et à l'organisation. La défense, la sécurité, la loyauté et la souveraineté sont des marqueurs forts des métiers du cyber.
Renforcer la visibilité des formations et des débouchés dès le lycée et dans l'enseignement supérieur via des forums, hackathons et partenariats avec les écoles.	
Sensibiliser les prescripteurs de formation (enseignants, médiateurs, éducateurs jeunesse...) aux métiers de la cybersécurité afin d'orienter les jeunes vers ces carrières.	
Favoriser l'inclusion et la diversité dans la filière cyber en mettant en avant des parcours inspirants et en développant des actions ciblées de communication (ex. : femmes & cybersécurité).	✓ Intégrer des témoignages de professionnels issus de divers horizons et des modèles de réussite pour favoriser l'identification.
Valoriser les évolutions de carrière en cybersécurité et promouvoir les possibilités de reconversion vers les métiers du cyber.	✓ De nombreux exemples de reconversion réussie peuvent être mis en avant pour illustrer ces opportunités.
Communiquer sur les métiers et parcours de la cybersécurité via les réseaux sociaux fréquentés par les jeunes.	✓ Privilégier les plateformes comme Instagram et TikTok. Possibilité de prise en charge par Atlas pour la valorisation des métiers.

3 Axe 3 : Faire évoluer, diversifier l'offre de formation initiale

Pour optimiser l'offre de formation initiale en cybersécurité, plusieurs actions concrètes ont été identifiées. Celles-ci visent principalement à mieux intégrer la cybersécurité dans les cursus existants, à développer des spécialisations adaptées aux besoins des entreprises et à promouvoir des formations hybrides associant cybersécurité et autres domaines stratégiques. L'objectif est de structurer une offre plus lisible et accessible, tout en assurant une montée en compétences progressive des futurs professionnels du secteur.

Proposition d'actions	Précisions
Intégrer la cybersécurité dans tous les cursus IT (informatique, ingénierie, data science, etc.) comme une compétence transverse et incontournable.	✓ Modules Cyber obligatoires si possible, pour assurer une base commune de compétences.
Développer des spécialisations en cybersécurité au sein des grandes écoles et universités, en mettant l'accent sur des parcours professionnalisants.	✓ Besoin d'une réflexion plus approfondie sur les spécialisations à proposer et leur articulation avec le marché de l'emploi.
Créer des formations hybrides (Management + Cyber, Droit + Cyber, Responsable Produit + Cyber, Qualité + Cyber…) pour s'adapter à l'évolution des besoins des entreprises.	✓ Les profils à double compétence sont très prisés. Une première certification cyber pourrait compléter la formation initiale, suivie à terme par un double diplôme.
Intégrer des certifications professionnelles reconnues dès la formation initiale (CEH, ISO 2700X…)	

4 Axe 4 : Faire évoluer, diversifier l'offre de formation continue

Pour accompagner l'évolution rapide des besoins en cybersécurité, le développement de l'offre de formation continue est essentiel. Les actions proposées visent à faciliter l'accès des professionnels à des parcours adaptés, à intégrer des mises en situation pratiques et à renforcer la reconnaissance des certifications. Elles prennent en compte la diversité des niveaux de maîtrise et l'émergence de nouvelles technologies, afin d'assurer une montée en compétences continue et alignée avec les attentes des entreprises du secteur.

Proposition d'actions	Précisions
Mettre en place des parcours de reconversion vers la cybersécurité pour répondre à la pénurie de talents et attirer des profils issus d'autres domaines.	✓ Des actions similaires existent déjà dans le numérique. Il serait pertinent d'envisager des campagnes spécifiques pour la cybersécurité.
Faciliter l'accès à des formations modulaires adaptées aux professionnels (e-learning, formations courtes, bootcamps) en mettant en place un socle de connaissance commun à toutes les formations.	✓ Difficulté à mobiliser les salariés pour des formations longues. Une solution serait d'intégrer ces formations dans des parcours de montée en compétences en entreprise.
Proposer des formations adaptées aux différents niveaux de maîtrise en cybersécurité, avec un parcours de progression et une validation régulière des acquis.	✓ S'inspirer des référentiels existants (ex. Lean management avec les certifications Green Belt, Black Belt).
Intégrer des mises en situation pratiques et des exercices de simulation (red teaming, gestion de crise cyber) dans les formations continues, selon le principe de l'AFEST.	✓ Le dispositif AFEST est déjà utilisé par l'OPCO Atlas. Il permet une formation immersive chez les clients et partenaires.
Promouvoir les certifications (RNCP, ISO) et favoriser le choix de formations certifiantes.	✓ Nota : ISO 27001 pouvant s'adapter aux PME
Développer des formations spécialisées en cybersécurité appliquée aux nouvelles technologies (sécurité de l'IA, cybersécurité des systèmes quantiques, IoT sécurisé…).	
Étoffer le catalogue CampusAtlas avec de nouvelles thématiques : IoT/5G, quantique, formation spécifique pour dirigeants, nouvelles réglementations (NIS2, DORA…).	✓

CE QU'IL FAUT RETENIR

1 Face à l'augmentation constante des cyberattaques et à l'émergence de nouvelles menaces, la **cybersécurité est devenue un enjeu stratégique** pour les entreprises et les institutions. il est essentiel de renforcer les compétences des professionnels du secteur. La formation continue apparaît comme une nécessité incontournable pour assurer une protection efficace des systèmes et garantir une résilience accrue face aux cybermenaces.

2 Le secteur de la cybersécurité **devrait connaître une croissance soutenue**, avec des prévisions d'augmentation du marché pouvant atteindre 15 % par an. Des interrogations subsistent sur la répartition demain des emplois entre les entreprises françaises et l'externalisation vers d'autres marchés.

3 Alors que la demande en experts en cybersécurité ne cesse de croître, les entreprises peinent à recruter les profils nécessaires. Il devient donc primordial **d'attirer de nouveaux talents vers ces métiers**, de proposer des parcours de formation adaptés et de fidéliser les professionnels déjà en poste.

4 Si la cybersécurité **ne bouleverse pas radicalement les métiers actuels du numérique, elle en modifie en profondeur les exigences.** L'intégration de mesures de protection et de conformité devient incontournable dans de nombreux domaines, l'adaptation des pratiques professionnelles à ces nouvelles contraintes est désormais une priorité.

5 Les métiers de la cybersécurité requièrent un **large éventail de compétences**, mêlant expertise technique, capacité d'analyse stratégique et maîtrise des réglementations en vigueur. Au-delà des connaissances en cryptographie, sécurité cloud ou audit informatique, les professionnels doivent être en mesure de comprendre les enjeux métiers, d'anticiper les risques et de communiquer efficacement sur les problématiques de cybersécurité.

6 Avec plus de **900 formations répertoriées en cybersécurité, l'offre actuelle est riche, fragmentée et peu lisible**. Il est nécessaire d'améliorer la structuration des parcours, de renforcer la lisibilité des certifications et d'assurer une meilleure articulation entre formations initiales et continues, afin d'offrir des cursus véritablement adaptés aux exigences du marché.

7 Pour répondre aux défis actuels et futurs, la cybersécurité doit être **intégrée dès les premiers niveaux d'apprentissage.** Tous les cursus en informatique et en ingénierie devraient inclure une composante cybersécurité, tandis que des **spécialisations approfondies devraient être proposées dans les grandes écoles et universités**. Cette approche permettrait de former des experts directement opérationnels à la sortie de leurs études.

8 Les professionnels devront monter en compétences « Cyber » tout au long de leur carrière. Le développement de formations modulaires, **l'intégration de certifications reconnues** et la mise en place **d'exercices pratiques immersifs** sont autant de leviers à activer pour garantir une montée en compétence efficace et adaptée aux besoins du marché.

9 Les métiers de la **cybersécurité souffrent encore d'un déficit d'image**, souvent perçus comme trop techniques ou réservés à une élite de spécialistes. Pourtant, **la diversité des parcours possibles** – mêlant aspects techniques, stratégiques, juridiques ou encore liés à la gestion des risques – démontre que ces professions sont accessibles à un public bien plus large. Mieux communiquer sur ces opportunités contribuera à séduire de nouveaux profils de salariés.

10 La cybersécurité représente un **enjeu de souveraineté nationale**. Le développement des compétences en France est essentiel pour limiter la dépendance aux prestataires étrangers et garantir la protection des infrastructures critiques. La structuration de la filière, le soutien aux initiatives de formation et l'implication des entreprises dans la montée en compétences sont des impératifs pour **renforcer l'autonomie et la résilience du pays face aux menaces numériques**.

ANNEXES

- Glossaire
- Sources
- Resultats de l’enquete en ligne
- Donnees et analyses complementaires

GLOSSAIRE

MOT	DÉFINITION
CERT	Computer Emergency Response Team (Équipe de Réponse aux Urgences Informatiques)
CISSP	Certified Information Systems Security Professional
CNIL	Commission Nationale de l'Informatique et des Libertés
CRA	Cyber Risk Assessment (Évaluation des Risques Cyber)
CSIRT	Computer Security Incident Response Team (Équipe de Réponse aux Incidents de Sécurité Informatique)
CSNA	Cyber Security National Authority (Autorité Nationale de la Cybersécurité)
DDOS	Distributed Denial of Service (Déni de Service Distribué)
DevOps	Development and Operations (Développement et Opérations)
DORA	Digital Operational Resilience Act (Loi sur la Résilience Opérationnelle Numérique)
DPO	Data Protection Officer (Délégué à la Protection des Données)
DSI	Directeur des Systèmes d'Information
EAL	Evaluation Assurance Level
EDR	Endpoint Detection and Response (Détection et Réponse sur les Terminaux)
ESN	Entreprise de Services du Numérique
IA	Intelligence Artificielle
IOT	Internet of Things (Internet des Objets)
MOOC	Massive Open Online Course (Cours en Ligne Ouvert et Massif)
NIS	Network and Information Systems (Réseaux et Systèmes d'Information)
OSINT	Open Source Intelligence (Renseignement en Sources Ouvertes)
PACS	Prestataires d'Agrément de Confiance Sécurisée
PAMS	Privileged Access Management Systems (Systèmes de Gestion des Accès Privilégiés)
PASSI	Prestataires d'Audit de la Sécurité des Systèmes d'Information

MOT	DÉFINITION
PDIS	Prestataires de Détection des Incidents de Sécurité
PENTEST	Test d'intrusion
PRIS	Prestataires de Réponse aux Incidents de Sécurité
RGPD	Règlement Général sur la Protection des Données
RPCA	Responsable du Plan de Continuité des Activités
RPRI	Responsable du Plan de Reprise Informatique
RSSI	Responsable de la Sécurité des Systèmes d'Information
SAAS	Software as a Service (Logiciel en tant que Service)
SECaaS	Security as a Service (Sécurité en tant que Service)
SIEM	Security Information and Event Management (Gestion des Informations et Événements de Sécurité)
SOC	Security Operations Center (Centre d'Opérations de Sécurité)
UX/UI	User Experience / User Interface (Expérience Utilisateur / Interface Utilisateur)
XDR	Extended Detection and Response (Détection et Réponse Étendues)

SOURCES

PRINCIPALES SOURCES UTILISEES

- OPIIEC - LES FORMATIONS ET LES COMPÉTENCES EN FRANCE SUR LA CYBERSÉCURITÉ
- CESIN - Etude sur la rémunération et le positionnement organisationnel des responsables cybersécurité
- L'Usine Nouvelle - Près de la moitié des TPE et PME françaises s'estiment trop peu protégées
- L'Usine Nouvelle - Cybersécurité ; Victimes de stress excessif des RSSI songent à changer de poste
- L'Usine Nouvelle - La pénurie de talents en cybersécurité, une épine dans le pied des entreprises françaises
- L'Usine Nouvelle - Les entreprises françaises résistent aux cyberattaques mais peinent à respecter la réglementation
- Campus Cyber / ANSSI / CISA - Référentiel de métiers cyber
- **ATLAS – Formations ATLAS**
- OPIIEC: https://www.opiiec.fr/secteur/numerique
- EY : https://www.ey.com/fr_fr/news/2023/09/barometre-future-ready-de-la-transformation-des-eti
- Cybermalveillance.gouv.fr : https://entreprendre.service-public.fr/actualites/A17303
- Stormshield : https://www.stormshield.com/fr/actus/cybersecurite-chiffres-cles-statistiques-2023/
- Bpifrance : https://bigmedia.bpifrance.fr/nos-actualites/cybersecurite-que-disent-les-chiffres-de-2023-2024
- Ellisphere : https://www.ellisphere.com/cybersecurite-en-entreprise-bilan-2023-et-tendances-2024/
- CESIN : https://cesin.fr/articles-slug/?slug=2060-9%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN
- Ambient.IT : https://www.ambient-it.net/statistiques-cybersecurite/
- Fortune business insight : https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
- Xerfi : https://www.xerfi.com/presentationetude/le-marche-de-la-cybersecurite_SAE24
- Rothschild : https://www.rothschildandco.com/fr/actualites/publications/2024/03/wm-thematic-insights-frontieres-numeriques-la-cybersecurite/
- Wavestone : https://www.wavestone.com/fr/insight/benchmark-cyber-2024-la-maturite-cyber-des-grands-groupes-progresse-lentement-en-depit-de-nouveaux-challenges/
- L'Opinion : https://www.lopinion.fr/economie/risque-cyber-les-4-chiffres-clefs-qui-alertent-sur-2024-la-tribune-de-laurent-celerier-et-arthur-chen
- ISC2 : https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look

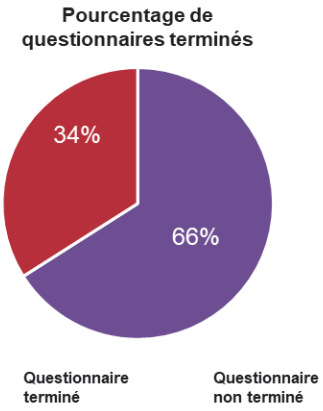
PRESENTATION DETAILLEE DES METIERS

MÉTIER	PROFIL	ACTIVITÉ
RSSI	Bac+5, grandes écoles, ingénieur système et réseaux	Responsable de la sécurité des systèmes d'information et de la conduite de la politique de sécurité des systèmes d'information de l'organisation
DSI	Bac+5, école d'ingénieur, informatique	Direction de projets
DPO	Juriste, école informatique	Conformité légale et règlementaire (RGPD, CNIL)
Consultant en cybersécurité	Bac+5, grandes écoles, ingénieur	Conseils et accompagnement des entreprises sur la cybersécurité
DevSecOps	Ingénieur, master informatique	Assure l'intégration d'une couche de sécurité native dans la conception de logiciels, progiciels, outils de cybersécurité.
Analyste OSINT	Grandes écoles, anciens militaires, anciens cadres forces de sécurité intérieure	Collecte, analyse et interprétation de données ouvertes (open source intelligence) et donc publiques afin d'identifier d'éventuelles menaces.
Cryptologue	Expert en sécurité informatique	Supervise la stratégie de sécurité cryptographique d'une entreprise
RPCA	Responsable conformité, direction générale,	Responsable du plan de continuité informatique
RPRI	Dsi, rssi	Responsable du plan de reprise informatique
Analyste SOC	Master en informatique, expert en sécurité informatique	Surveille, détecte, analyse et répond aux incidents de sécurité en temps réel
Expert en intrusion et test	Master en informatique, expert en sécurité informatique	Contrôle la sécurité des réseaux informatiques en opérant des tests d'intrusion. Identifie les vulnérabilités afin de pouvoir les corriger.
Expert SECasS	Intégrateur, architecte, développeur	Gère les services managés pour le compte des clients de son organisation (edr, xdr, siem, etc…)
Responsable CSIRT	Master en informatique, expert en sécurité informatique, ingénieur système et réseaux	Responsable d'une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information d'une organisation
Responsable du SOC	Master en informatique, expert en sécurité informatique, ingénieur système et réseaux	Planifie et organise les opérations quotidiennes du Security Operation Center (SOC). Il supervise et gère l'équipe de sécurité opérationnelle.
Bug bounty hunter	Bac+ scientifique	Trouver des bogues et des failles de sécurité dans les systèmes d'information.
Spécialiste architecture et intégration	Intégrateur, architecte, développeur	Conception de l'architecture fonctionnelle, logicielle et technique. Pilotage de l'intégration des différentes composantes matérielles et logicielles si système d'information. Elaboration de la documentation d'exploitation associée à l'application.
Administrateur réseau	Intégrateur, architecte, développeur	Assure la circulation des informations dans l'entreprise et sécurise le réseau. Gère l'accès des utilisateurs au réseau de l'entreprise en identifiant les différents comptes et droits d'accès des utilisateurs et des comptes de services.

Auditeur sécurité SI	Bac+5	Effectue des inspections pour évaluer les vulnérabilités des systèmes informatiques, rédige des rapports d'analyse, propose des recommandations, assure une veille technologique, forme les entités concernées et contrôle l'application des procédures de sécurité.
Red Teamer / Blue Teamer	Intégrateur, architecte, développeur	Missionnés afin de tenter de mettre en défaut la sécurité du système d'information cible.

RESULTATS DE L'ENQUETE EN LIGNE

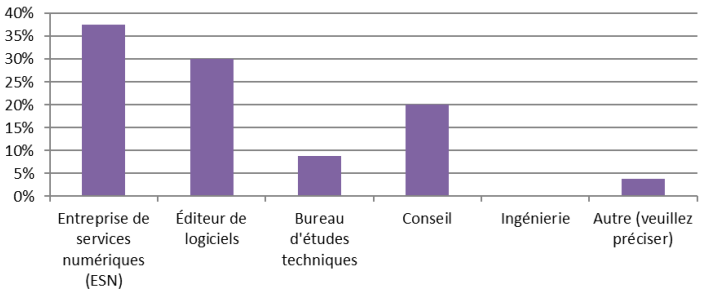
- Enquête en ligne publiée le 23 octobre 2024 et « fermée » le 2 décembre 2024
  - Envoyée aux entreprises contacts de l'OPIIEC du secteur du numérique au sens large (ESN, Editeurs de Logiciel, Conseil en IT).
  - Deux relances opérées par les services d'Atlas
  - Relai de certains clusters et informations par la voie de Linkedin
- 82 répondants à l'enquête
  - Des entreprises de toutes tailles, représentatives des profils constatés dans le secteur du Numérique
  - Un bon taux de renseignement du questionnaire
  - Une majorité de répondant appartenant à la « Direction » de l'entreprise
- 26 questions répartis en 6 parties
  - Partie 1 : Point sur l'activité de l'entreprise
  - Partie 2 : Maturité et perception du marché
  - Partie 3 : Cybersécurité au sein de l'entreprise
  - Partie 4 : Recrutement en cybersécurité au sein de l'entreprise
  - Partie 5 : Perception de la formation initiale et continue
  - Partie 6 : Coordonnées du répondant



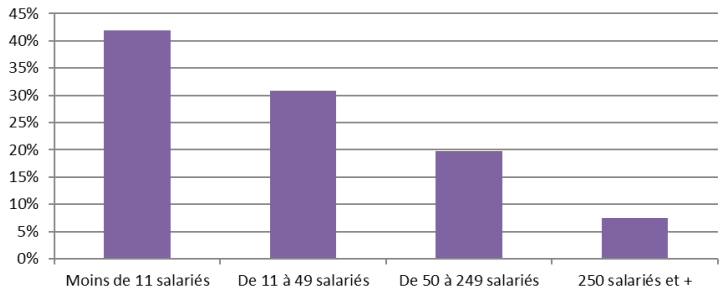
Commentaires

- Un nombre important de répondants, un bon niveau de fiabilité des phénomènes observés
- Une majorité d'acteurs ayant répondu (xx%) appartenant à une TPE et PME
- Un pourcentage correct de questionnaires « achevés », totalement remplis par les répondants

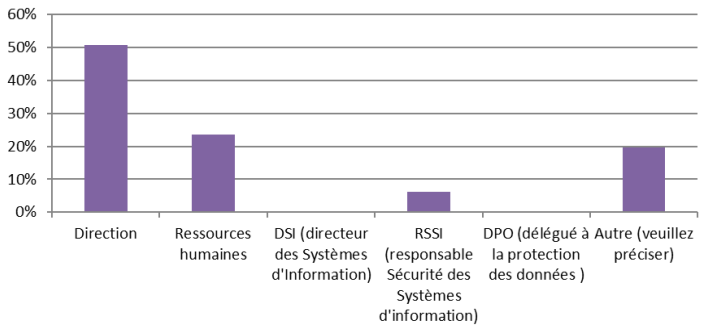
Quelle est l'activité principale de votre entreprise ?



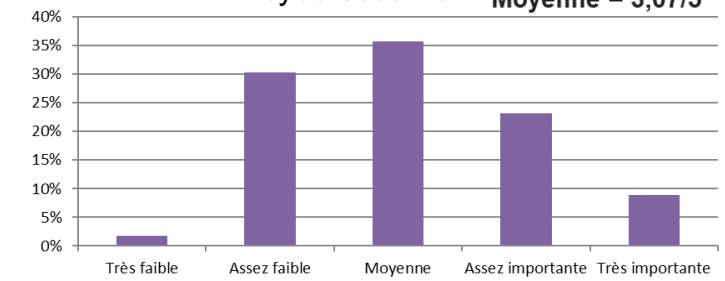
Quelle est la taille de votre structure (en ETP)



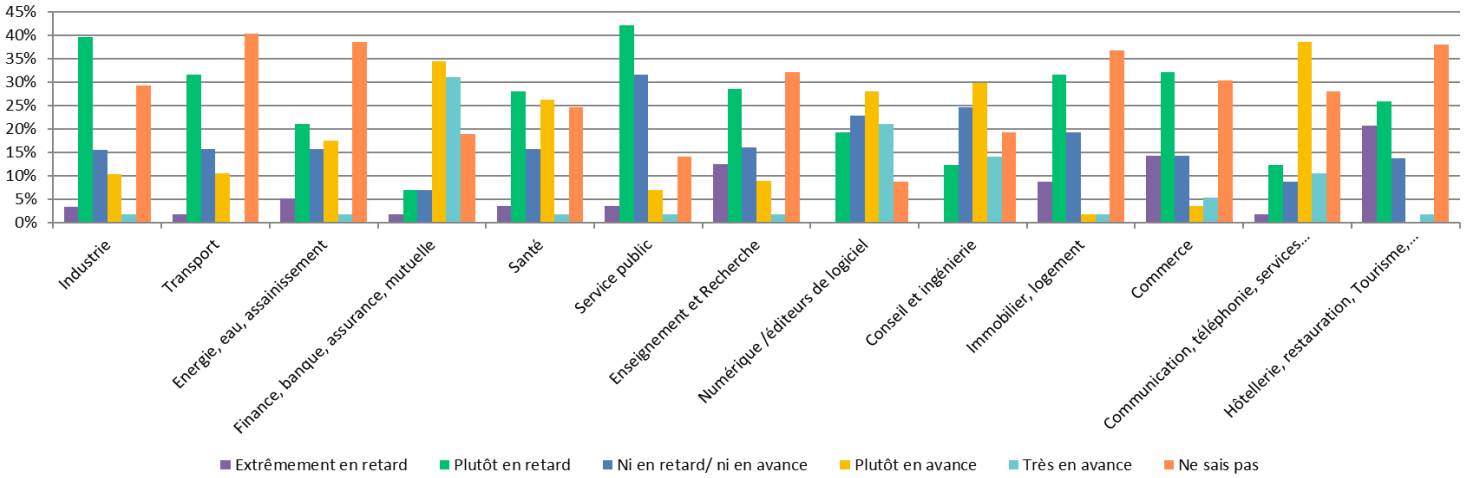
Quel poste occupez-vous ?



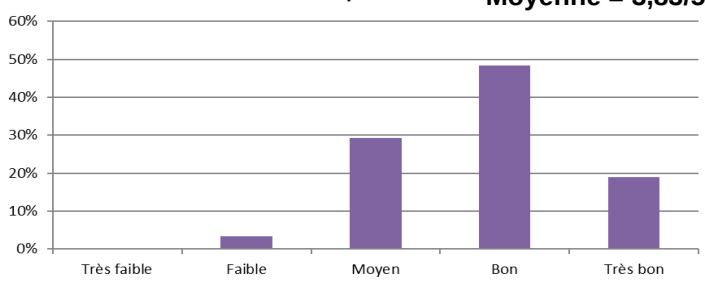
Selon vous, quelle est la maturité globale de vos clients sur la thématique de la cybersécurité ? Moyenne = 3,07/5



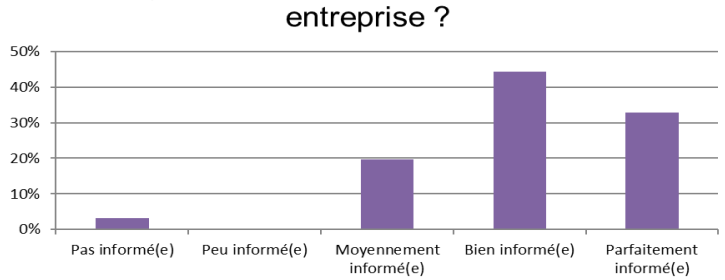
Comment jugez-vous la préparation et l'anticipation des secteurs suivants sur les sujets de cybersécurité ?

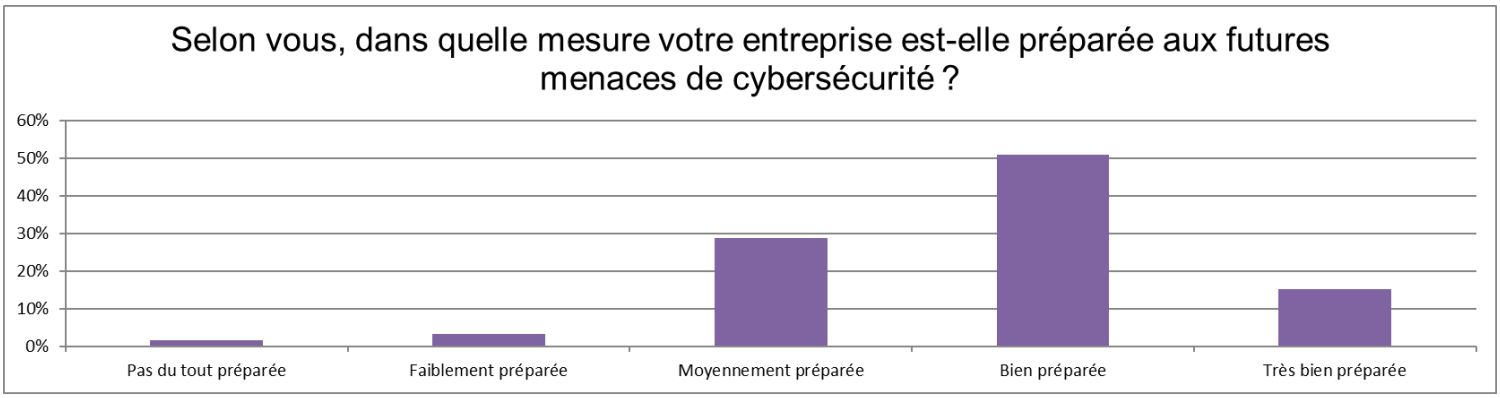


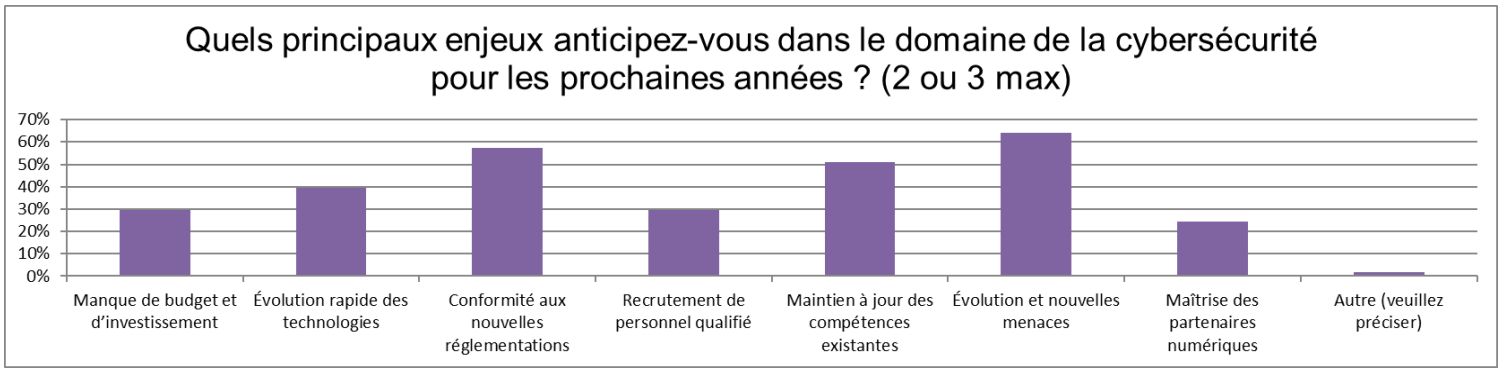
Comment évaluez-vous le niveau actuel de maturité en cybersécurité dans votre entreprise ? Moyenne = 3,83/5

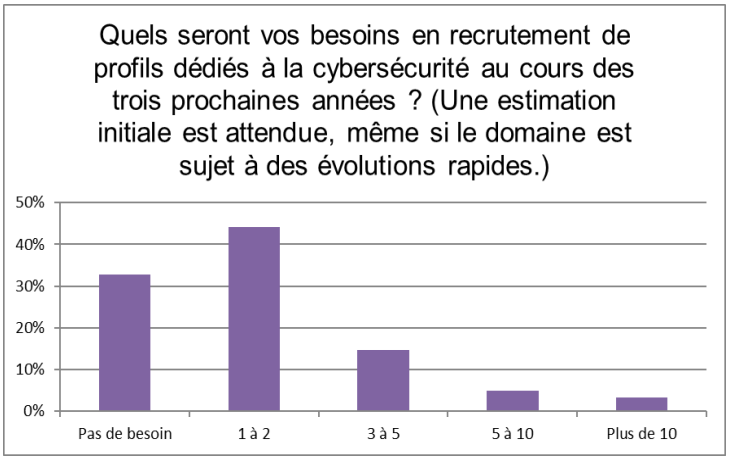


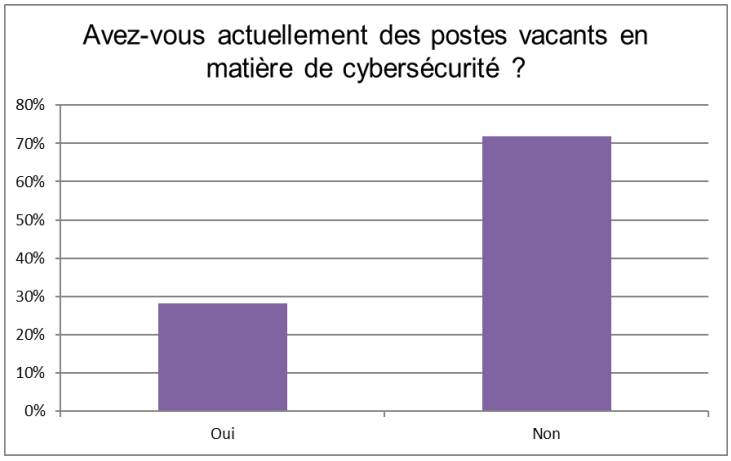
Dans quelle mesure êtes-vous informé personnellement des menaces de cybersécurité qui pèsent sur votre entreprise ?

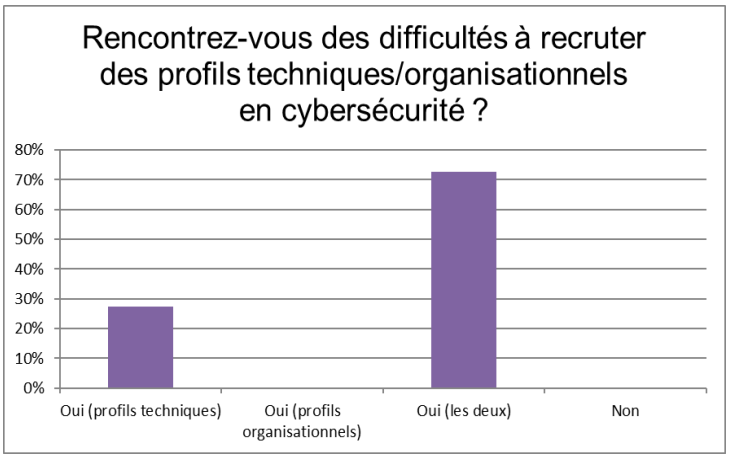


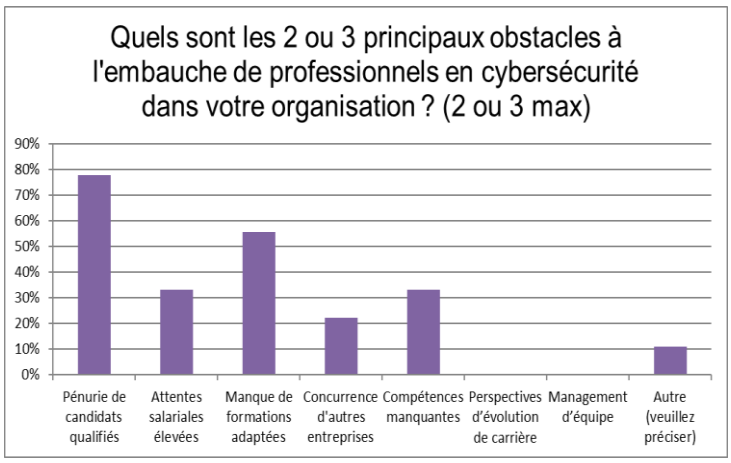

Selon vous, dans quelle mesure votre entreprise est-elle préparée aux futures menaces de cybersécurité ?
60%
50%
40%
30%
20%
10%
0%
Pas du tout préparée
Faiblement préparée
Moyennement préparée
Bien préparée
Très bien préparée

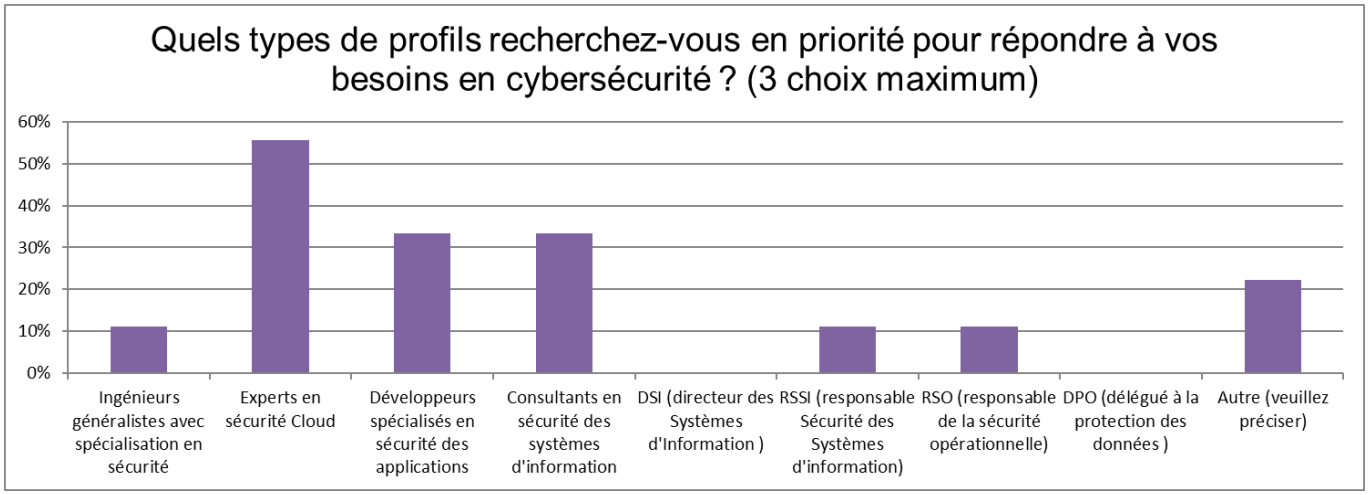

Quels principaux enjeux anticipez-vous dans le domaine de la cybersécurité pour les prochaines années ? (2 ou 3 max)
70%
60%
50%
40%
30%
20%
10%
0%
Manque de budget et d'investissement
Évolution rapide des technologies
Conformité aux nouvelles réglementations
Recrutement de personnel qualifié
Maintien à jour des compétences existantes
Évolution et nouvelles menaces
Maîtrise des partenaires numériques
Autre (veuillez préciser)

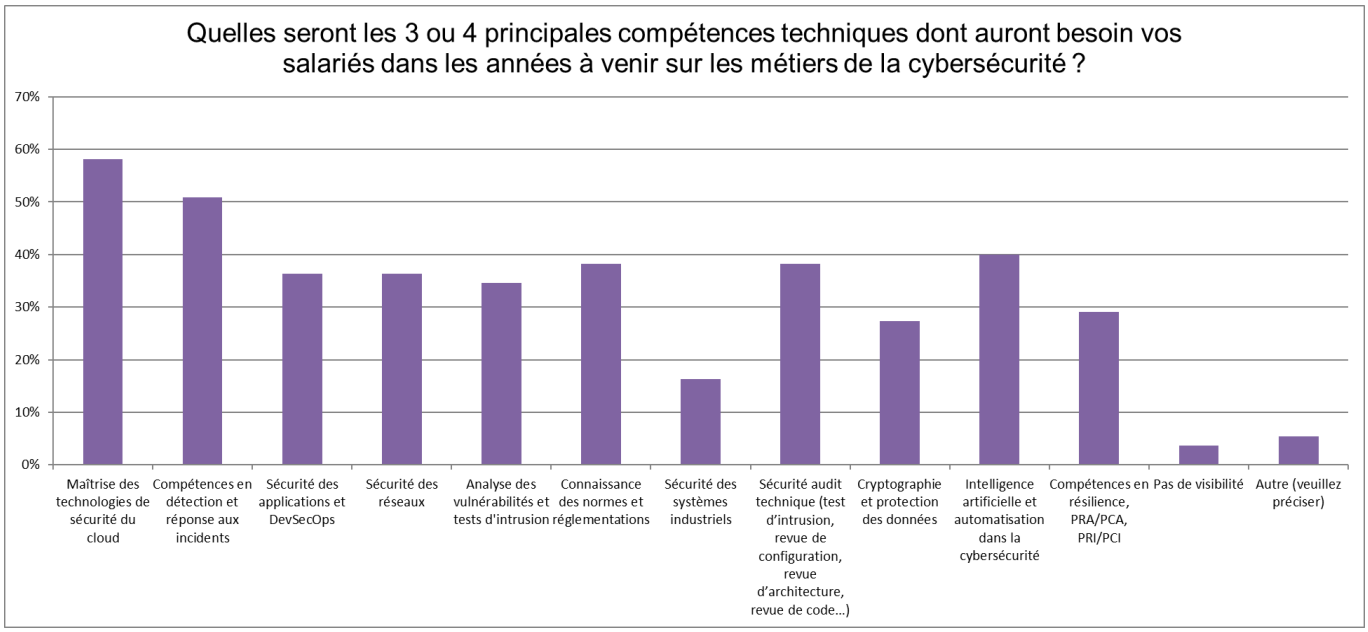

Quels seront vos besoins en recrutement de profils dédiés à la cybersécurité au cours des trois prochaines années ? (Une estimation initiale est attendue, même si le domaine est sujet à des évolutions rapides.)
50%
40%
30%
20%
10%
0%
Pas de besoin
1 à 2
3 à 5
5 à 10
Plus de 10

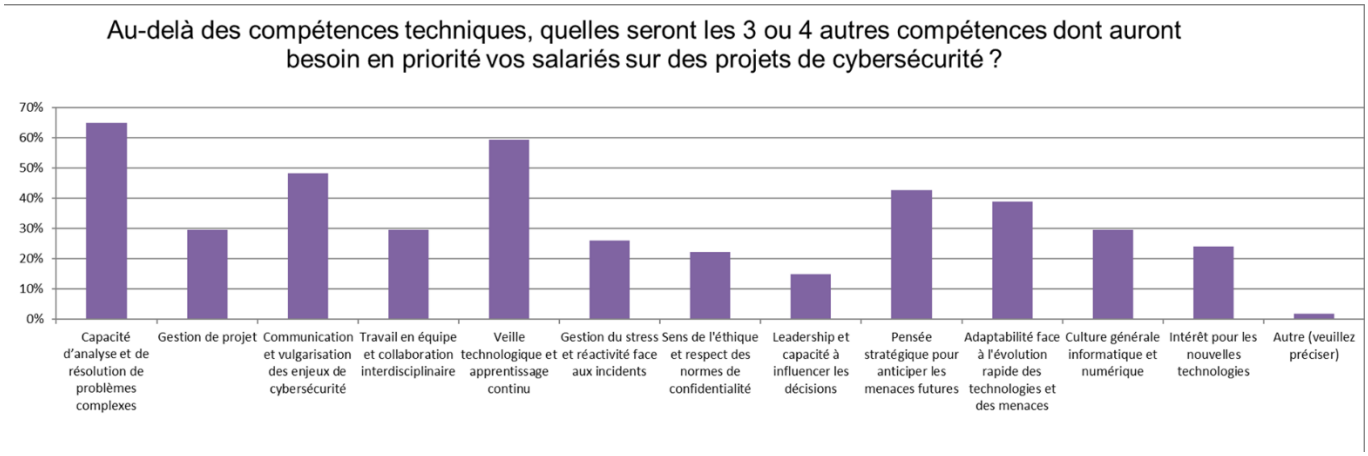

Avez-vous actuellement des postes vacants en matière de cybersécurité ?
80%
70%
60%
50%
40%
30%
20%
10%
0%
Oui
Non

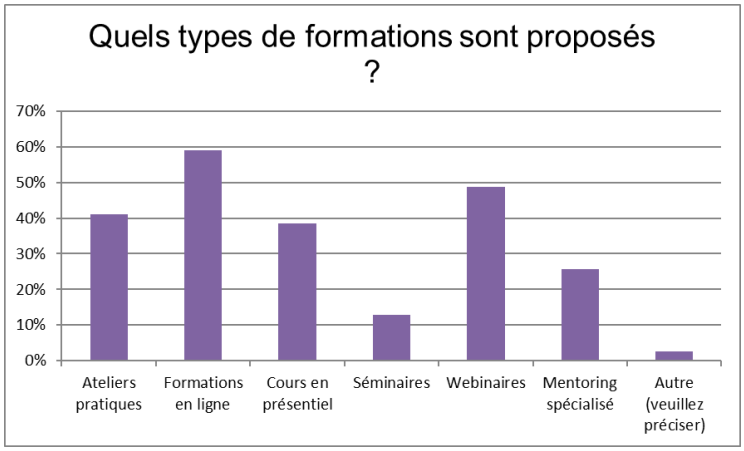

Rencontrez-vous des difficultés à recruter des profils techniques/organisationnels en cybersécurité ?
80%
70%
60%
50%
40%
30%
20%
10%
0%
Oui (profils techniques)
Oui (profils organisationnels)
Oui (les deux)
Non

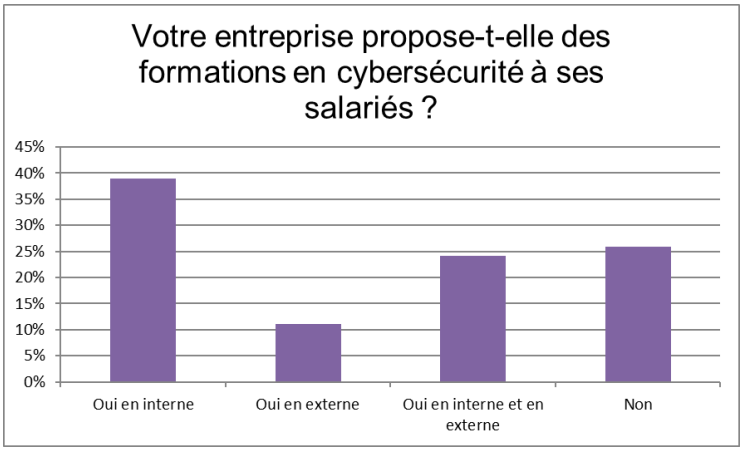

Quels sont les 2 ou 3 principaux obstacles à l'embauche de professionnels en cybersécurité dans votre organisation ? (2 ou 3 max)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Pénurie de candidats qualifiés
Attentes salariales élevées
Manque de formations adaptées
Concurrence d'autres entreprises
Compétences manquantes
Perspectives d'évolution de carrière
Management d'équipe
Autre (veuillez préciser)

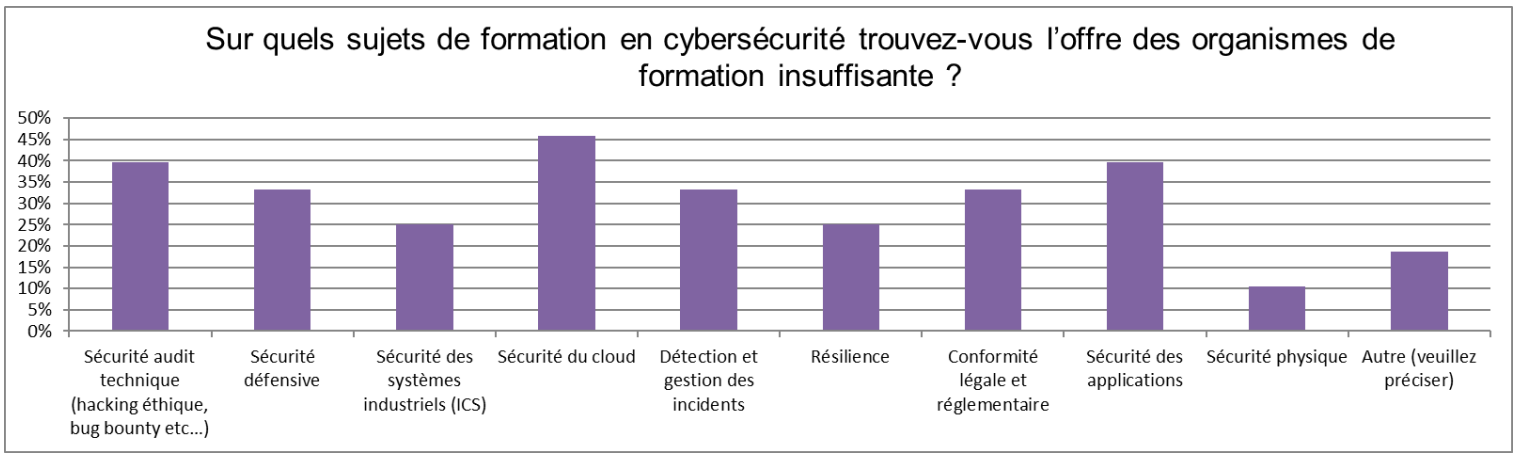

Quels types de profils recherchez-vous en priorité pour répondre à vos besoins en cybersécurité ? (3 choix maximum)
60%
50%
40%
30%
20%
10%
0%
Ingénieurs généralistes avec spécialisation en sécurité
Experts en sécurité Cloud
Développeurs spécialisés en sécurité des applications
Consultants en sécurité des systèmes d'information
DSI (directeur des Systèmes d'Information)
RSSI (responsable Sécurité des Systèmes d'information)
RSO (responsable de la sécurité opérationnelle)
DPO (délégué à la protection des données)
Autre (veuillez préciser)

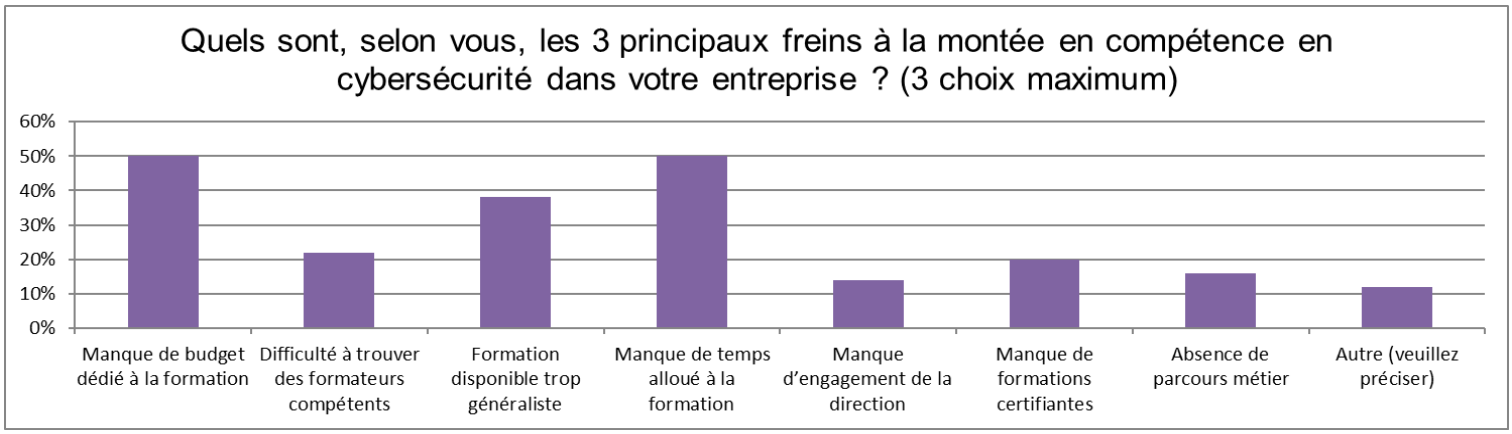

Quelles seront les 3 ou 4 principales compétences techniques dont auront besoin vos salariés dans les années à venir sur les métiers de la cybersécurité ?
70%
60%
50%
40%
30%
20%
10%
0%
Maîtrise des technologies de sécurité du cloud
Compétences en détection et réponse aux incidents
Sécurité des applications et DevSecOps
Sécurité des réseaux
Analyse des vulnérabilités et tests d'intrusion
Connaissance des normes et réglementations
Sécurité des systèmes industriels
Sécurité audit technique (test d'intrusion, revue de configuration, revue d'architecture, revue de code...)
Cryptographie et protection des données
Intelligence artificielle et automatisation dans la cybersécurité
Compétences en résilience, PRA/PCA, PRI/PCI
Pas de visibilité
Autre (veuillez préciser)

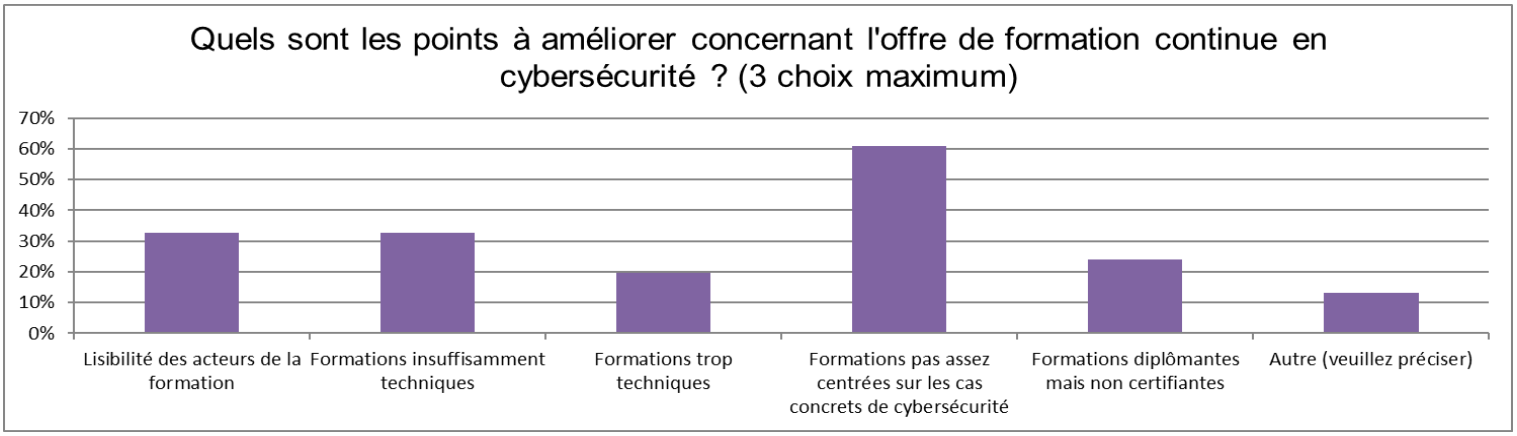

Au-delà des compétences techniques, quelles seront les 3 ou 4 autres compétences dont auront besoin en priorité vos salariés sur des projets de cybersécurité ?
70%
60%
50%
40%
30%
20%
10%
0%
Capacité d'analyse et de résolution de problèmes complexes
Gestion de projet
Communication et vulgarisation des enjeux de cybersécurité
Travail en équipe et collaboration interdisciplinaire
Veille technologique et apprentissage continu
Gestion du stress et réactivité face aux incidents
Sens de l'éthique et respect des normes de confidentialité
Leadership et capacité à influencer les décisions
Pensée stratégique pour anticiper les menaces futures
Adaptabilité face à l'évolution rapide des technologies et des menaces
Culture générale informatique et numérique
Intérêt pour les nouvelles technologies
Autre (veuillez préciser)

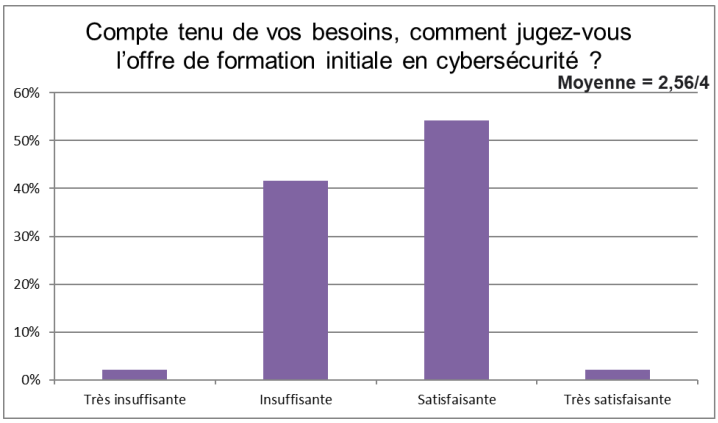

Quels types de formations sont proposés ?
70%
60%
50%
40%
30%
20%
10%
0%
Ateliers pratiques
Formations en ligne
Cours en présentiel
Séminaires
Webinaires
Mentoring spécialisé
Autre (veuillez préciser)

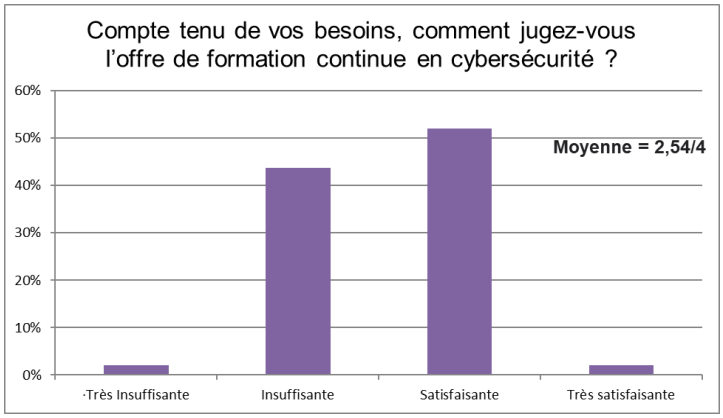

Votre entreprise propose-t-elle des formations en cybersécurité à ses salariés ?
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
Oui en interne
Oui en externe
Oui en interne et en externe
Non

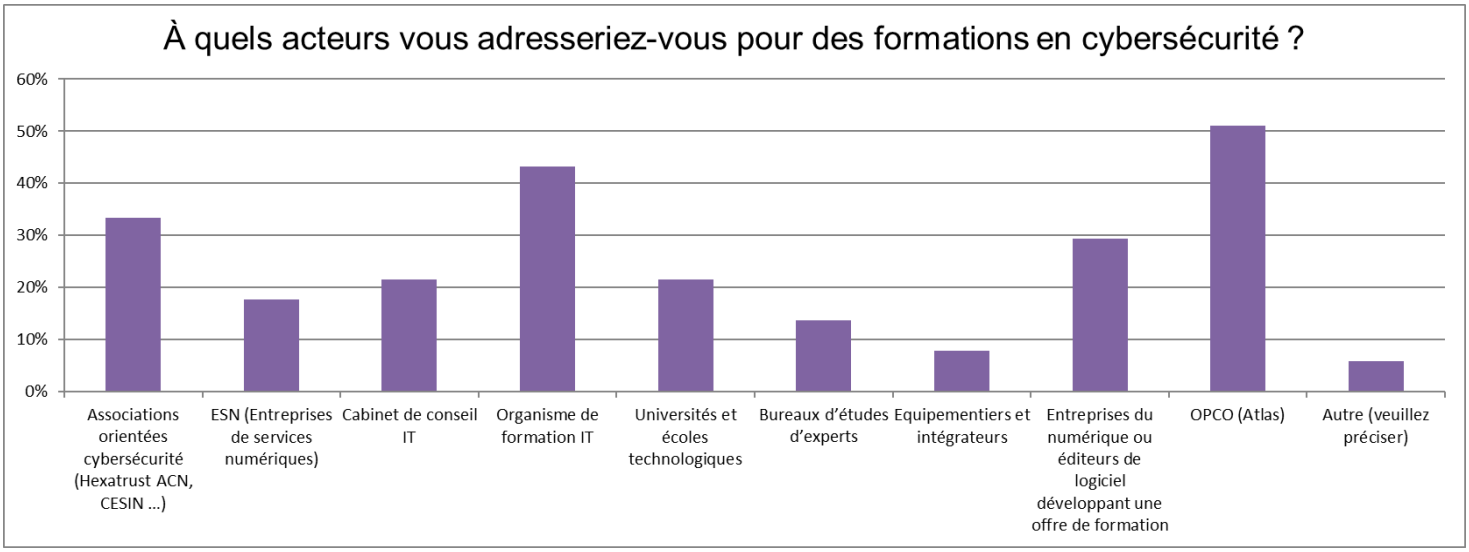

Sur quels sujets de formation en cybersécurité trouvez-vous l'offre des organismes de formation insuffisante ?
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
Sécurité audit technique (hacking éthique, bug bounty etc...)
Sécurité défensive
Sécurité des systèmes industriels (ICS)
Sécurité du cloud
Détection et gestion des incidents
Résilience
Conformité légale et réglementaire
Sécurité des applications
Sécurité physique
Autre (veuillez préciser)


Quels sont, selon vous, les 3 principaux freins à la montée en compétence en cybersécurité dans votre entreprise ? (3 choix maximum)
60%
50%
40%
30%
20%
10%
0%
Manque de budget dédié à la formation
Difficulté à trouver des formateurs compétents
Formation disponible trop généraliste
Manque de temps alloué à la formation
Manque d'engagement de la direction
Manque de formations certifiantes
Absence de parcours métier
Autre (veuillez préciser)

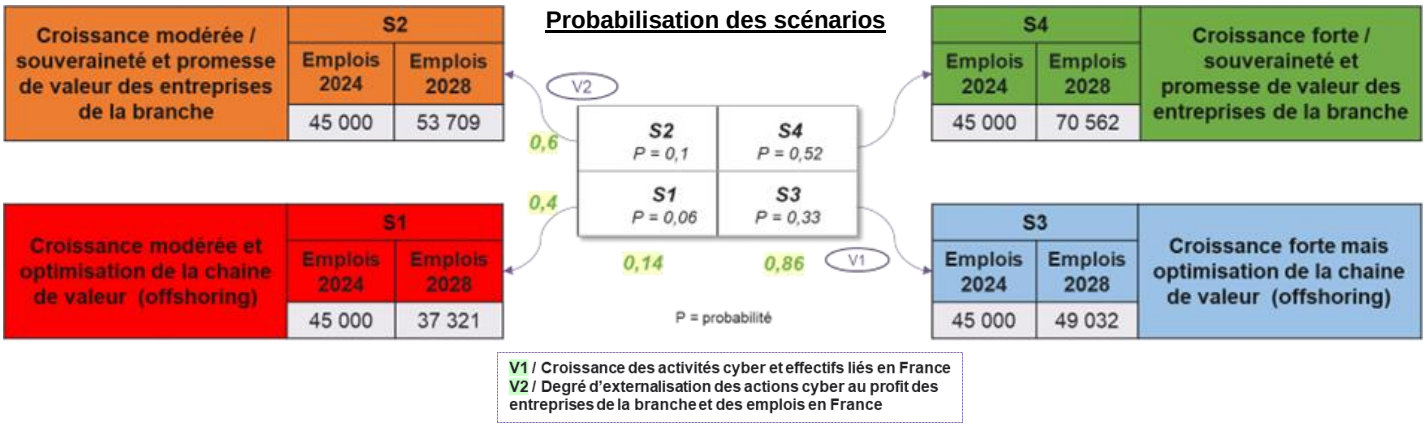

Quels sont les points à améliorer concernant l'offre de formation continue en cybersécurité ? (3 choix maximum)
70%
60%
50%
40%
30%
20%
10%
0%
Lisibilité des acteurs de la formation
Formations insuffisamment techniques
Formations trop techniques
Formations pas assez centrées sur les cas concrets de cybersécurité
Formations diplômantes mais non certifiantes
Autre (veuillez préciser)


Compte tenu de vos besoins, comment jugez-vous l'offre de formation initiale en cybersécurité ?
Moyenne = 2,56/4
60%
50%
40%
30%
20%
10%
0%
Très insuffisante
Insuffisante
Satisfaisante
Très satisfaisante


Compte tenu de vos besoins, comment jugez-vous l'offre de formation continue en cybersécurité ?
Moyenne = 2,54/4
60%
50%
40%
30%
20%
10%
0%
·Très Insuffisante
Insuffisante
Satisfaisante
Très satisfaisante


À quels acteurs vous adresseriez-vous pour des formations en cybersécurité ?
60%
50%
40%
30%
20%
10%
0%
Associations orientées cybersécurité (Hexatrust ACN, CESIN ...)
ESN (Entreprises de services numériques)
Cabinet de conseil IT
Organisme de formation IT
Universités et écoles technologiques
Bureaux d'études d'experts
Equipementiers et intégrateurs
Entreprises du numérique ou éditeurs de logiciel développant une offre de formation
OPCO (Atlas)
Autre (veuillez préciser)

IMPACT / CHIFFRES CLES PAR SCENARIO



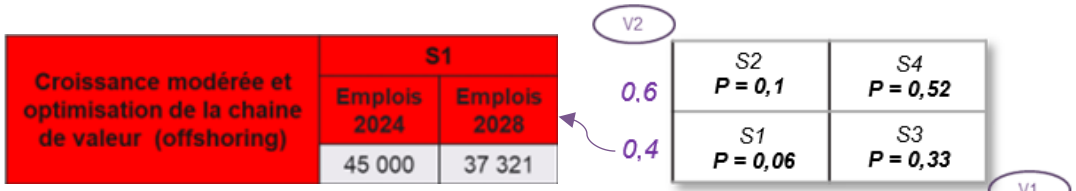
V1 / Croissance des activités cyber et effectifs liés en France
V2 / Degré d'externalisation des actions cyber au profit des entreprises de la branche et des emplois en France

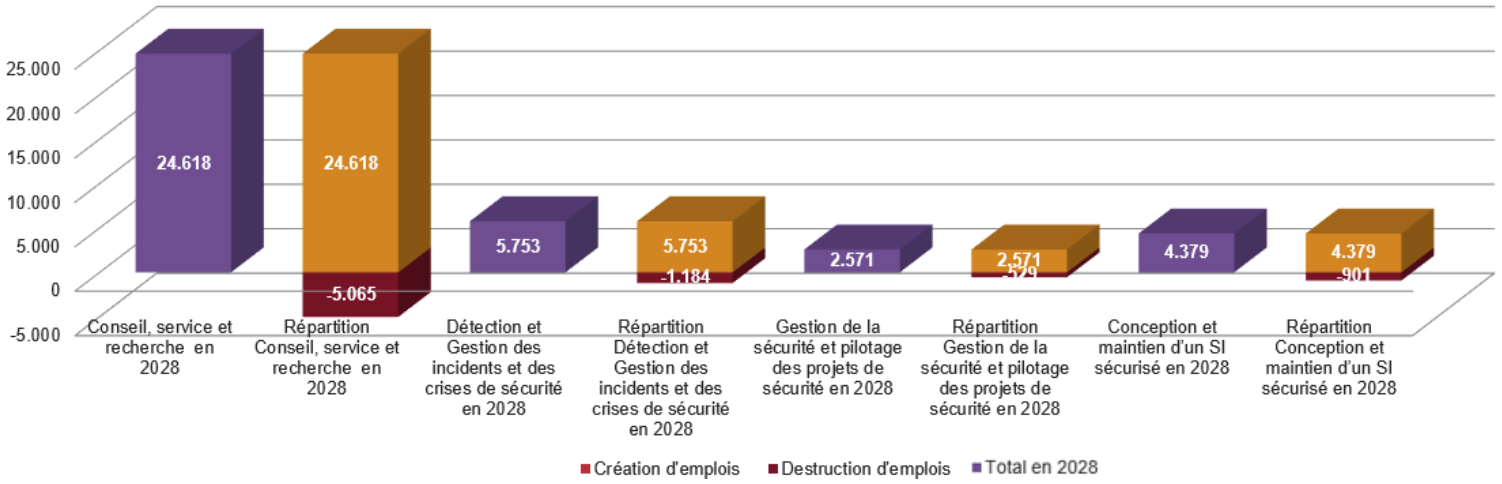
			2024	2025	2026	2027	2028	2029	2030	2031	TCAM 2028
P= 0,042	S1	Filière / Métiers Cyber	101 219	104 196	107 261	110 415	113 663	117 006	120 447	101 219	2,2%
		Branche	42 397	40 633	38 942	37 321	35 768	34 279	32 853	42 397	-4,6%
P= 0,098	S2	Filière / Métiers Cyber	101 219	104 196	107 261	110 415	113 663	117 006	120 447	101 219	2,2%
		Branche	46 437	48 744	51 166	53 709	56 378	59 179	62 120	46 437	4,5%
P= 0,258	S3	Filière / Métiers Cyber	101 219	114 119	128 664	145 062	163 551	184 396	207 897	101 219	9,4%
		Branche	42 397	44 502	46 712	49 032	51 467	54 022	56 705	42 397	2,2%
P= 0,602	S4	Filière / Métiers Cyber	101 219	114 119	128 664	145 062	163 551	184 396	207 897	101 219	9,4%
		Branche	46 437	53 386	61 376	70 562	81 122	93 263	107 221	46 437	11,9%

Métiers	Total Emplois retenu	% branche	ETP 2024
RSSI	5 000	40%	2 000
DSI	5 500	20%	1 100
DPO	30 000	21%	6 300
Consultant en cyber	20 000	100%	20 000
Développeur sécurité	4 500	50%	2 250
Analyste OSINT	2 000	50%	1 000
Cryptologue	266	50%	133
RPCA	3 000	10%	300
RPRI	3 000	10%	300
Analyste SOC	5 000	50%	2 500
Expert en intrusion et test	500	90%	450
Expert SECasS	2 500	100%	2 500
CERT	173	50%	87
R SOC	1 000	50%	500
Bug bounty hunter	300	100%	300
Administrateur réseau	15 500	20%	3 000
Auditeur sécurité SI	1 300	100%	1 300
Red teamer / blue teamer	980	100%	980
Formateur en cybersécurité	700	0%	0
Chercheur en cybersécurité	500	0%	0

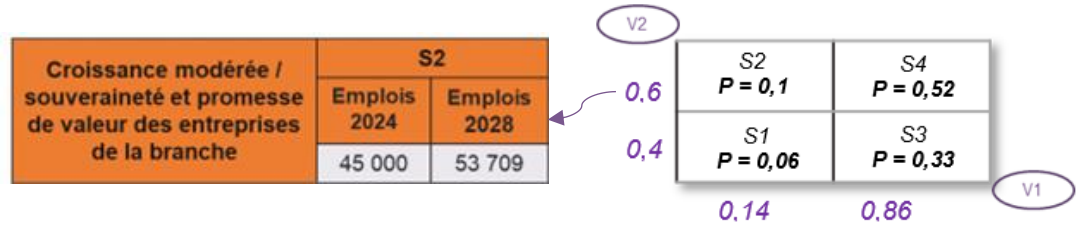
DONNEES ET ANALYSES COMPLEMENTAIRES

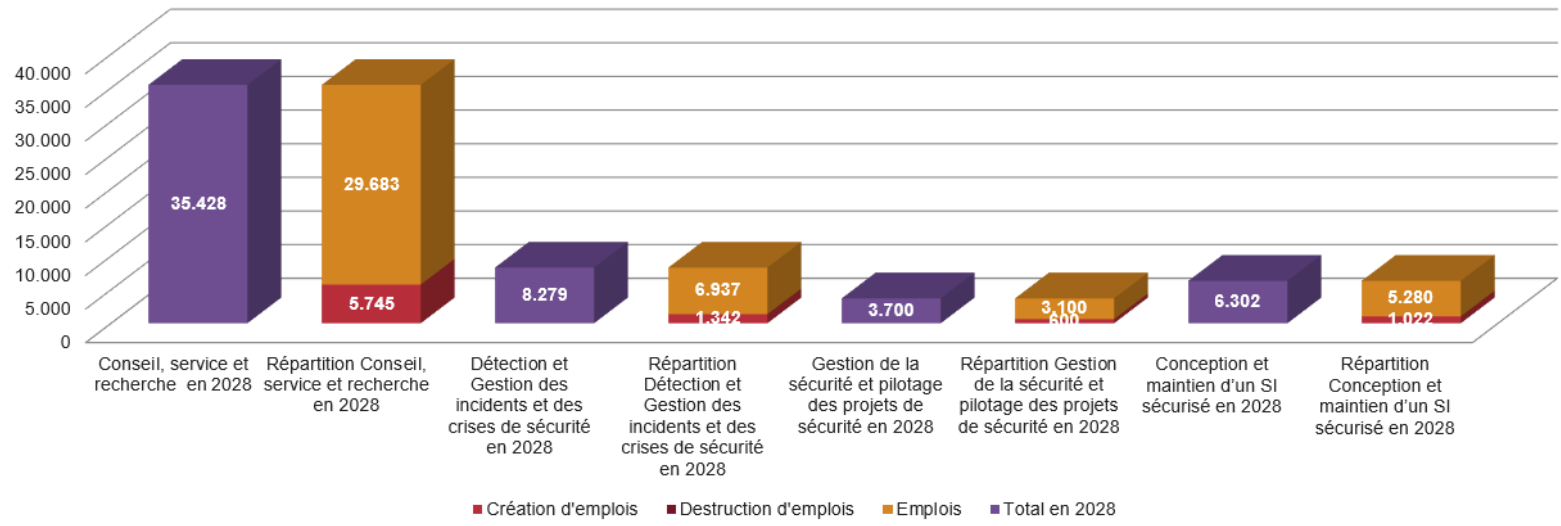
IMPACT / CHIFFRES CLES SCENARIO 1



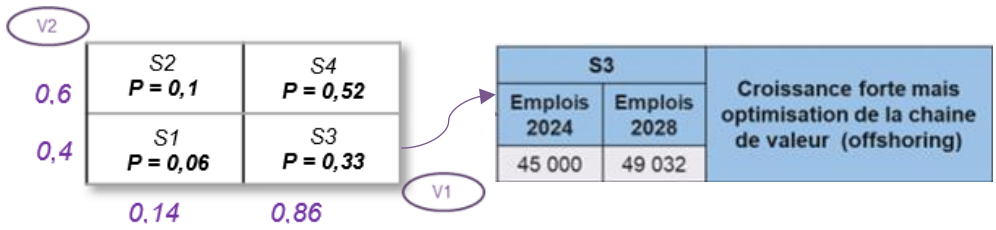


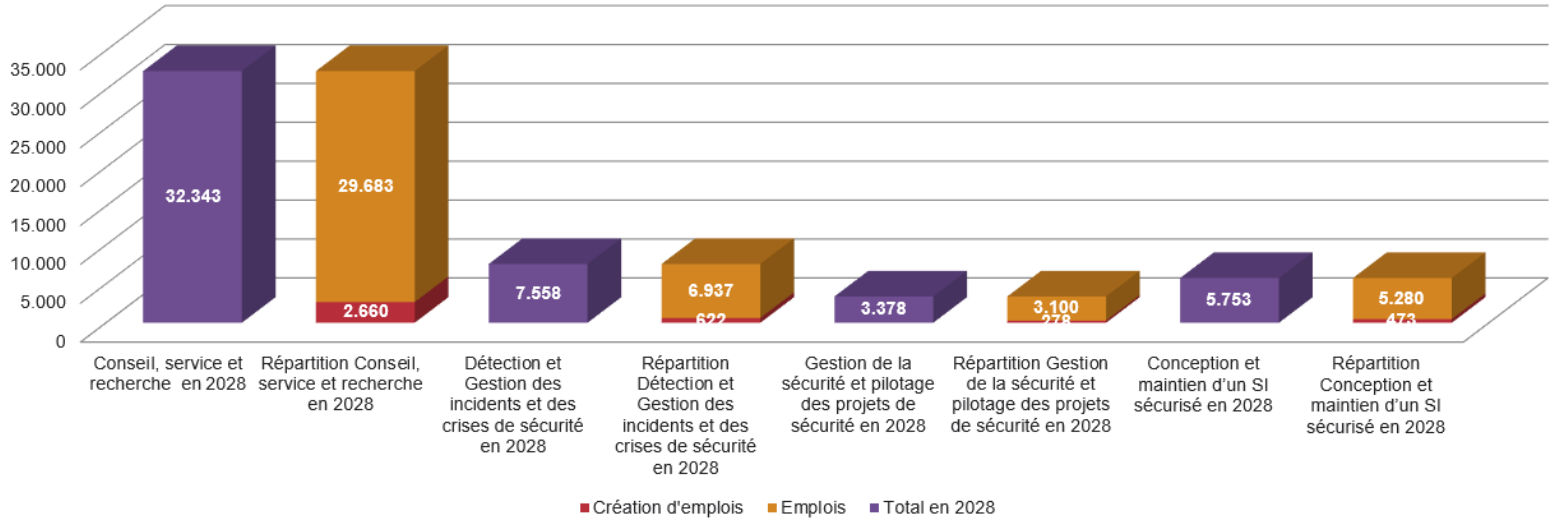
IMPACT / CHIFFRES CLES SCENARIO 2



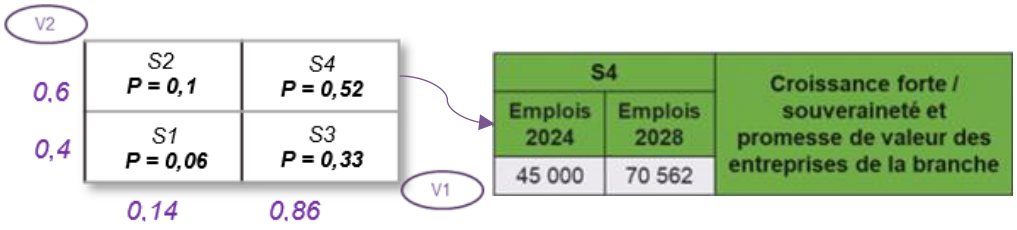


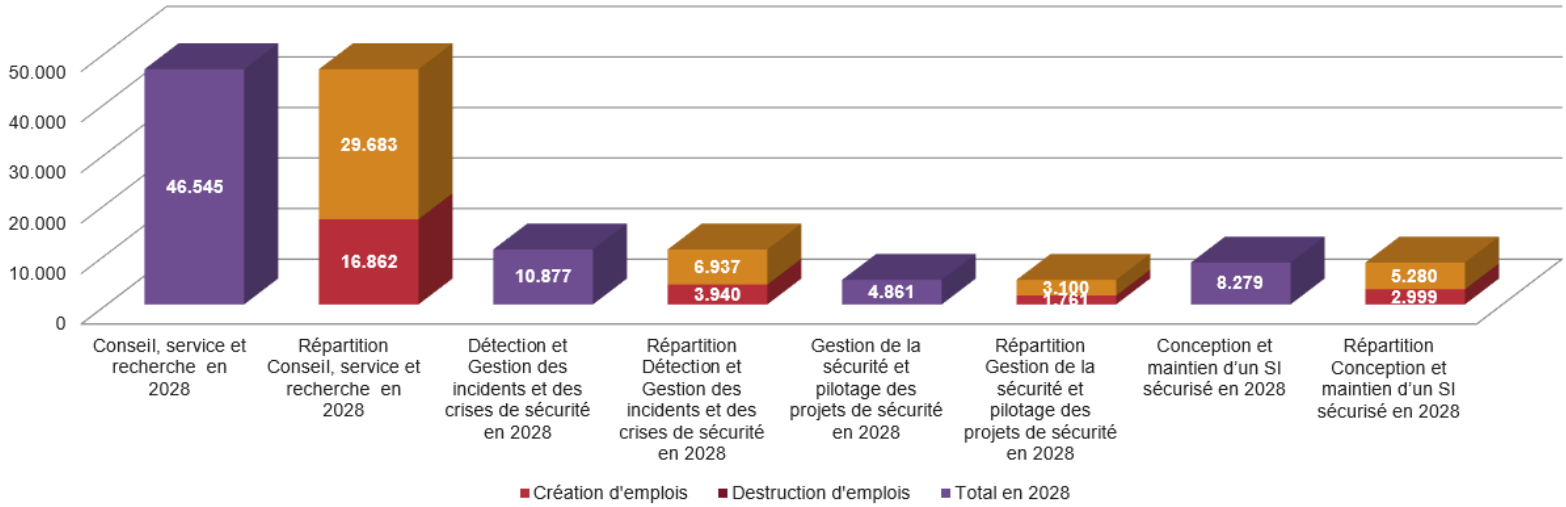
IMPACT / CHIFFRES CLES SCENARIO 3



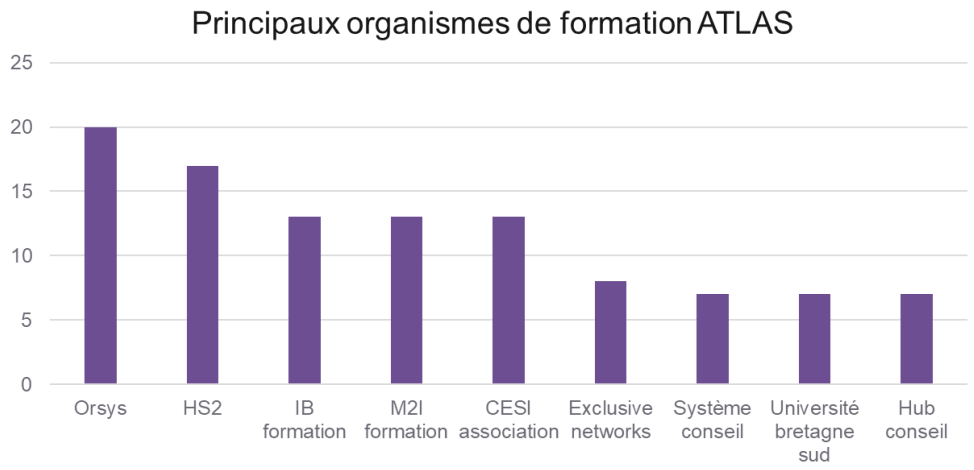


IMPACT / CHIFFRES CLES SCENARIO 4





FOCUS SUR LES FORMATIONS ATLAS



SECTEURS CRITIQUES NIS2

▲ DIRECTIVE (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022 :

- https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2555&qid=1710163571116

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	—Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil [(1)], qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		—Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		—Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		—Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		—Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil [(2)]
		—Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944
		—Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	—Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil [(3)]
	c) Pétrole	— Exploitants d'oléoducs

		—Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		—Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil [4]
	d) Gaz	—Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil [5]
		—Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		—Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE
		—Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
		—Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		—Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		—Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	—Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	—Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) nº 300/2008 utilisés à des fins commerciales
		—Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil [6], aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) nº 1315/2013 du Parlement européen et du Conseil [7], et entités exploitant les installations annexes se trouvant dans les aéroports
		—Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) nº 549/2004 du Parlement européen et du Conseil [8]
	b) Transports ferroviaires	—Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil [9]
		—Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	—Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) nº 725/2004 du Parlement européen et du Conseil [10], à l'exclusion des navires exploités à titre individuel par ces sociétés
		—Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil [11], y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) nº 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports
		—Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil [12]

	d)Transports routiers	—Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission [(13)] chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		—Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil [(14)]
3.Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil [(15)]
4.Infrastructures des marchés financiers		—Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil [(16)]
		—Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) nº 648/2012 du Parlement européen et du Conseil [(17)]
5. Santé		—Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil [(18)]
		—Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil [(19)]
		—Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil [(20)]
		—Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21
		—Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil [(21)]
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil [(22)], à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil [(23)], à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8.Infrastructure numérique		— Fournisseurs de points d'échange internet
		—Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		— Registres de noms de domaine de premier niveau
		— Fournisseurs de services d'informatique en nuage
		— Fournisseurs de services de centres de données
		— Fournisseurs de réseaux de diffusion de contenu
		— Prestataires de services de confiance

		— Fournisseurs de réseaux de communications électroniques publics
		— Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (interentreprises)		— Fournisseurs de services gérés — Fournisseurs de services de sécurité gérés
10. Administration publique		— Entités de l'administration publique des pouvoirs publics centraux définies comme telles par un État membre conformément au droit national
		— Entités de l'administration publique au niveau régional définies comme telles par un État membre conformément au droit national

BASE COMPETENCES

▲ Cette base de compétences en cybersécurité a été élaborée afin de structurer et classifier les principales expertises requises dans le domaine. Pour une meilleure lisibilité et exploitation, ces compétences ont été regroupées en blocs thématiques qui reflètent les différents aspects et enjeux du secteur.

- Le Bloc A regroupe les compétences liées aux activités opérationnelles et stratégiques en cybersécurité, telles que la **gestion des incidents et des crises de sécurité, la gestion de la sécurité et le pilotage des projets de sécurité, la conception et le maintien d'un SI sécurisé, et les aspects de Gouvernance-Risque-Compliance (GRC)**
- Le Bloc B, quant à lui, regroupe les compétences techniques et transversales essentielles pour l'analyse et la mise en œuvre des stratégies de sécurité.

Bloc A	BLOC B	Compétences
Gestion des incidents et des crises de sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Capacité à analyser et comprendre le comportement des logiciels malveillants pour les neutraliser
Gestion des incidents et des crises de sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Enquêter sur les incidents de sécurité et récupérer des preuves numériques
Gestion des incidents et des crises de sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Participer aux réseaux de détection de malware en partageant les failles découvertes et prenant en compte celles des autres
Gestion des incidents et des crises de sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Compétence en reverse engineering pour analyser des malwares ou comprendre des systèmes sans documentation
Gestion des incidents et des crises de sécurité	autres/ divers	Avoir le sens du détail afin d'identifier les vulnérabilités subtiles ou des signes d'attaque
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Pouvoir planifier, exécuter et finaliser des projets dans le respect des délais et des budgets
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Savoir identifier et gérer les besoins et attentes des différentes parties prenantes
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Savoir conduire des initiatives de changement notamment lors de l'implémentation de nouvelles technologies
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Présenter et vendre des solutions de cybersécurité aux clients potentiels
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Connaissance du marché de la cybersécurité pour orienter les efforts marketing et commerciaux
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Savoir établir et maintenir des relations de confiance avec les clients
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Développer et mettre en œuvre une stratégie de cybersécurité l'échelle de l'entreprise
Bloc A	**BLOC B**	**Compétences**
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Savoir allouer efficacement les ressources financières de l'entreprise
Gestion de la sécurité et pilotage des projets de sécurité	autres/ divers	Savoir former et sensibiliser les employés à la cybersécurité
Conception et maintien d'un SI sécurisé	autres/ divers	Capacité à concevoir une architecture de sécurité robuste pour protéger les infrastructures informatiques

Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Capacité à analyser des situations complexes et à identifier des solutions logiques et efficaces
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Résolution rapide de problèmes
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Savoir expliquer des concepts techniques complexes à un public non technique
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Savoir collaborer avec différentes personnes/départements
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Être capable de s'adapter rapidement aux nouvelles technologies
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Capacité à travailler sous pression, notamment lors d'incidents informatiques
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Savoir remettre en question les hypothèses et analyser les informations de manière critique
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Maintenir une attitude professionnelle et éthique dans la gestion des informations sensibles et des systèmes de sécurité
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Avoir un désir constant d'apprendre et de se tenir au courant des dernières tendances en cybersécurité
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Leadership
Gestion de la sécurité et pilotage des projets de sécurité	Compétences Transversales et Personnelles	Capacité à trouver des solutions innovantes
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Comprendre les concepts de base des réseaux (TCP/IP,DNS,VPN,pare-feu ...)
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Connaissance des systèmes de détection et de prévention des intrusions (IDS/IPS)
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Configurer et sécuriser les VPN pour protéger les communications
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Comprendre et appliquer les normes et réglementations en matière de sécurité
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Connaissance des environnements clouds et des mesures de sécurité spécifiques à ceux-ci
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Protéger les bases de données contre les attaques
Conception et maintien d'un SI sécurisé	Concepts de Base des Réseaux et de la Sécurité	Maîtriser des technologies de virtualisation et des mesures de sécurités associées (Vmware,Hyper-V)
Bloc A	**BLOC B**	**Compétences**
Gestion de la sécurité et pilotage des projets de sécurité	Cryptographie et Sécurité des Données	Savoir comment les, données, sont chiffrées et déchiffrées pour assurer la confidentialité, l'intégrité et l'accessibilité des informations (triade CIA)
Conception et maintien d'un SI sécurisé	Cryptographie et Sécurité des Données	Connaissance des méthodes pour sécuriser le développement et le déploiement des applications
Gouvernance-Risque-Compliance (GRC)	Gestion des Risques	Capacité à identifier, évaluer et gérer les risques liés à la sécurité de l'information
Gouvernance-Risque-Compliance (GRC)	Gestion des Risques	Evaluer les risques liés au projet et mettre en place des mesures d'atténuation

Gouvernance-Risque-Compliance (GRC)	Gestion des Risques	Comprendre les risques liés au marketing numérique (gestion de données client)
Conception et maintien d'un SI sécurisé	Programmation et Automatisation	Compétences en en scripting (Python,Powershell...)
Conception et maintien d'un SI sécurisé	Programmation et Automatisation	Connaissance des spécificités et défis de la sécurisation des objets connectés (IoT)
Gouvernance-Risque-Compliance (GRC)	Gestion de la sécurité dans un système d'exploitation	Maîtriser les systèmes d'exploitation, y compris la gestion des comptes, des autorisations et des correctifs de sécurité
Conception et maintien d'un SI sécurisé	Systèmes d'Exploitation et Gestion des Accès	Comprendre comment gérer les identités numériques et les accès aux ressources sensibles
Gestion de la sécurité et pilotage des projets de sécurité	Tests de Sécurité et Évaluation des Vulnérabilités	Compétence pour effectuer des tests de sécurité et identifier les vulnérabilités dans les systèmes
Gouvernance-Risque-Compliance (GRC)	Compétences Transversales et Personnelles	Avoir une compréhension complète des activités de l'entreprise pour ne pas être enfermé dans une approche uniquement "cyber"
Gestion de la Sécurité et Pilotage des Projets de Sécurité	Compétences Transversales et Personnelles	Savoir écouter les besoins, agir en toute discrétion et retranscrire correctement les besoins exprimés
Gouvernance-Risque-Compliance (GRC)	Compétences Transversales et Personnelles	S'adapter à l'évolution rapide de l'environnement de la cybersécurité en faisant preuve de curiosité pour rester à jour face aux nouvelles menaces et technologies.
Gestion de la Sécurité et Pilotage des Projets de Sécurité	Compétences Transversales et Personnelles	Être capable de sensibiliser les équipes non techniques aux enjeux de la cybersécurité et d'expliquer les concepts complexes de manière simple.
Gestion des Incidents et des Crises de Sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Savoir gérer et réagir de manière efficace et rapide aux incidents de sécurité (mitigation des incidents).
Gestion de la Sécurité et Pilotage des Projets de Sécurité	Compétences Transversales et Personnelles	Communiquer efficacement à l'oral et à l'écrit, avec une maîtrise du français et de l'anglais.
Gestion de la Sécurité et Pilotage des Projets de Sécurité	Compétences Transversales et Personnelles	Pouvoir mener un projet et manager une équipe (gestion de projets cyber)
Conception et Maintien d'un SI Sécurisé	Cryptographie et Sécurité des Données	Protéger les systèmes contre les attaques automatisées propulsées par l'intelligence artificielle et comprendre les impacts de l'informatique quantique sur les algorithmes de cryptographie.
Conception et Maintien d'un SI Sécurisé	Cryptographie et Sécurité des Données	Sécuriser les dispositifs IoT, qui représentent une faille critique pour de nombreuses industries (ex. santé, énergie).
Conception et Maintien d'un SI Sécurisé	Cryptographie et Sécurité des Données	Connaître les mécanismes de sécurité dans la blockchain, en particulier pour l'authentification et la gestion des identités.
Gouvernance-Risque-Compliance (GRC)	Concepts de Base des Réseaux et de la Sécurité	Maîtriser les infrastructures cloud et identifier les failles potentielles dans la chaîne de fournisseurs et prestataires (supply chain security).
Conception et Maintien d'un SI Sécurisé	Concepts de Base des Réseaux et de la Sécurité	Comprendre les vulnérabilités associées à la 5G, notamment dans les secteurs critiques comme les transports ou la santé.
Conception et Maintien d'un SI Sécurisé	Tests de Sécurité et Évaluation des Vulnérabilités	Maîtriser les techniques d'attaque pour tester la résilience des systèmes.
Gouvernance-Risque-Compliance (GRC)		Maîtriser les normes ISO 27000, NIS2, EBIOS, PRIS, PASSI, PAMS, etc., et les labels associés comme SEC INCLOUD pour assurer la conformité
Bloc A	**BLOC B**	**Compétences**
Conception et Maintien d'un SI Sécurisé	Programmation et Automatisation	Coder en tenant compte des bonnes pratiques de sécurité pour réduire les vulnérabilités dès la conception des logiciels. (Secure by design)
Conception et Maintien d'un SI Sécurisé	Tests de Sécurité et Évaluation des Vulnérabilités	Développer une expertise en tests de pénétration et en chasse aux failles de sécurité dans les systèmes (pentesting et bug bounty)
Gouvernance-Risque-Compliance (GRC)	Gestion des Risques	Évaluer la robustesse des systèmes et identifier les points faibles.
Gestion des Incidents et des Crises de Sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Comprendre les méthodes d'attaque des cybercriminels pour mieux défendre les systèmes. (Mitre att&ck)
Gouvernance-Risque-Compliance (GRC)	Gestion des Risques	Comprendre l'architecture globale des systèmes pour anticiper les vulnérabilités potentielles

Gestion des Incidents et des Crises de Sécurité	Analyse de Logiciels Malveillants et Réponse aux Incidents	Analyser a posteriori une cyberattaque (analyse forensic)
Gestion des Incidents et des Crises de Sécurité	Gestion des Risques	Élaborer des procédures de gestion de crise, en y intégrant des aspects décisionnels
Gestion de la Sécurité et Pilotage des Projets de Sécurité	Programmation et Automatisation	Mettre en œuvre une approche SOAR (Security Orchestration, Automation and Response) au sein des entreprises
Gouvernance-Risque-Compliance (GRC)	Systèmes d'Exploitation et Gestion des Accès	Comprendre les métiers et environnements dans lesquels les systèmes s'appliquent pour intégrer les besoins dès le développement, par exemple pour l'IoT, avec une compréhension de la fonction utile d'une ligne de production.

OPIIEC

CONTACT :

CATINAT Alexandra
Chef de projets Prospective
OPIIEC
25, quai Panhard et Levassor
75013 PARIS
opiiec@opiiec.fr

RÉALISATION :

KATALYSE
10, rue Charles Brunellière
44100 Nantes
https://www.katalyse.com/

ÉTUDE REALISÉE AVEC LE SOUTIEN DE L'OPCO ATLAS