CESIN : Les instantanés S2 2025

Les instantanées du CESIN du second semestre de 2025 s'appuient sur 11 mini-sondages hebdomadaires effectués auprès de ses membres du CESIN. Les panels varient entre 92 et 180 répondants avec une moyenne se situant à **136** répondants pour ce semestre.

A noter : il n'y avait pas de question sur les périodes estivales ni de vacances de fin d'année.

Les questions posées chaque semaine sont hétérogènes. Elles sont regroupées pour ce semestre selon 4 catégories : Les sujets qui ont fait l'actualité / Sécurité Applicative / Sensibilisation / Gouvernance.

Les sujets qui ont fait l'actualité

IA, LinkedIn et Microsoft

LinkedIn utilise depuis le 10 novembre 2025 les données des utilisateurs pour entraîner leurs modèles d'intelligence artificielle. Par ailleurs, Microsoft annonce maintenant qu'ils vont utiliser des données de LinkedIn, donc des données professionnelles et personnelles, à des fins d'entraînement de son IA.

Cette situation soulève des questions majeures sur la protection des données et le consentement éclairé. Les informations partagées sur LinkedIn, par exemple les parcours professionnels, les échanges, et aussi les contenus publiés peuvent ainsi alimenter des modèles d'IA sans que les utilisateurs en aient pleinement conscience. Pour les organisations, l'enjeu est double : protéger les données de leurs collaborateurs, mais aussi leurs propres informations stratégiques potentiellement exposées via les profils et activités de leurs équipes.

Pour éviter de laisser un tel consentement à LinkedIn et à Microsoft, il est possible, dans les deux cas, de s'opposer aux fonctionnalités d'entraînement d'IA en décochant une case dans LinkedIn ou Microsoft, Outlook ou Office 365. Mais cette option d'opposition reste discrète, et la question se pose : combien de RSSI en ont eu connaissance, et combien ont mis en place une politique globale au sein de leur organisation ?

140 membres ont répondu à la question [Q182] concernant leur connaissance de cette option d'opposition et sa mise en œuvre, à titre individuel et professionnel :

- **58%** le savaient, dont 49% s'y opposent et 9% ne s'y opposent pas ;
- **42%** ne le savaient pas, dont 30% vont s'y opposer et 12% non.

À titre professionnel, et pour votre organisation, le saviez-vous et qu'avez-vous mis en place ?

- **51%** le savaient :
  - 37% ne vont pas pousser une politique globale d'opposition ;
  - 5% ont poussé une politique globale d'opposition ;
  - 4% vont pousser une politique globale d'opposition ;
  - 5% vont pousser une politique globale d'opposition uniquement pour l'un ou l'autre (majoritairement pour Microsoft).
- **49%** ne le savaient pas : 23% vont préparer une politique globale d'opposition à pousser pour les salariés, les 26%, non.

La dépendance numérique : un livre blanc qui a fait l'actualité !

La dépendance numérique est devenue l'un des enjeux stratégiques majeurs pour les organisations. Entre multiplication des fournisseurs SaaS, concentration des infrastructures cloud chez quelques acteurs dominants, et chaînes d'approvisionnement technologiques mondialisées, les RSSI font face à des risques systémiques qui dépassent largement le périmètre traditionnel de la cybersécurité.

Cette dépendance se manifeste à plusieurs niveaux : dépendance vis-à-vis d'éditeurs étrangers pour les outils de sécurité eux-mêmes, concentration des données critiques chez un nombre restreint d'hébergeurs, impossibilité technique ou contractuelle de changer de prestataire sans coût prohibitif, perte de maîtrise sur les mises à jour et évolutions fonctionnelles... Autant de situations où l'organisation se retrouve captive, avec une marge de manœuvre réduite en cas de défaillance, de changement de politique tarifaire, ou de tensions géopolitiques.

Face à ces constats, le CESIN a souhaité produire un état des lieux collectif, documentant les pratiques, les leviers de réduction de la dépendance, et les arbitrages que les RSSI opèrent au quotidien entre autonomie stratégique et pragmatisme opérationnel.

Ce livre blanc, réalisé en partenariat avec le Forum International de la Cybersécurité (FIC), s'appuie sur les retours terrain des membres du CESIN et propose des pistes d'action concrètes pour mieux maîtriser cette dépendance sans renoncer aux bénéfices du numérique.

Le livre blanc sera disponible prochainement sur le site du CESIN : https://cesin.fr

Les incidents de sécurité SaaS en forte augmentation

Une entreprise américaine de sécurisation du SaaS souligne dans son rapport récent des lacunes majeures dans la sécurisation des environnements SaaS et la nécessité de protéger les applications

d'IA. « 91 % des organisations se disent confiantes quant à la sécurité de leurs solutions SaaS, pourtant 75 % d'entre elles ont subi un incident de sécurité (lié au SaaS). Ce décalage entre confiance et réalité révèle un problème majeur. »

L'explosion du SaaS dans les organisations a profondément transformé la surface d'attaque. Là où les applications étaient autrefois hébergées et maîtrisées en interne, elles sont désormais dispersées chez des dizaines, voire des centaines de fournisseurs tiers. Cette externalisation massive pose des défis inédits : gestion des accès, contrôle des configurations, visibilité sur les incidents, dépendance vis-à-vis des politiques de sécurité des éditeurs... Autant de zones grises qui échappent parfois au radar des RSSI.

Le paradoxe soulevé par cette étude américaine est frappant : une confiance élevée cohabite avec une sinistralité importante. Ce décalage interroge sur la perception des risques SaaS, souvent sous-estimés car externalisés, et sur la capacité réelle des organisations à surveiller, détecter et réagir face à des incidents qui se déroulent hors de leur infrastructure.

Les données de l'enquête sont basées sur une étude menée auprès de plus de 800 responsables de la sécurité aux États-Unis, au Royaume-Uni, en Allemagne, en Australie et au Japon, issus des secteurs de la finance, de la santé, de l'industrie manufacturière et des logiciels, dont les trois quarts travaillent dans des organisations de plus de 2 000 employés. Le rapport est disponible via : https://appomni.com/reports/state-of-saas-security/

Les utilisateurs français n'ayant pas été consultés lors de cette enquête, le CESIN a souhaité vérifier si les mêmes constats pouvaient être observés au sein de la communauté.

94 membres ont répondu à la question [Q185] concernant la validation ou non de ce constat au sein de leur propre organisation :

54% font le même constat, dont :

- 37% tout à fait, en observant une augmentation significative des incidents de sécurité liés aux applications SaaS qu'ils utilisent ;
- 6% en partie, car ils arrivent à bloquer en amont ;
- 11% en partie, car leurs fournisseurs SaaS réussissent à circonscrire l'incident.

- **46%** ne font pas le même constat, dont :
  - 32% indiquent que les incidents dans ce segment restent rares et qu'ils n'ont pas observé d'évolution récemment ;
  - 14% indiquent qu'ils n'ont jamais eu d'incidents avec leurs applications SaaS.

Sécurité applicative

Périmètre applicatif des RSSI

La taille du périmètre applicatif est un facteur déterminant de la surface d'attaque d'une organisation. Plus le nombre d'applications est élevé, plus la complexité de leur gestion et de leur sécurisation augmente.

Dans un contexte où les solutions SaaS se multiplient, où les équipes métiers déploient leurs propres outils, et où les environnements hybrides (IT et OT) coexistent, maintenir un inventaire à jour devient un défi quotidien pour les RSSI. Chaque application représente une porte d'entrée potentielle, un risque de fuite de données, ou un point de défaillance à surveiller.

Pourtant, la réalité du terrain montre une grande disparité entre les organisations : certaines gèrent quelques dizaines d'applications sur un périmètre maîtrisé, tandis que d'autres en comptent plusieurs milliers, réparties entre différents environnements, fournisseurs et niveaux de criticité. Cette hétérogénéité reflète non seulement la taille des structures, mais aussi leur maturité en matière de gouvernance applicative.

141 membres ont répondu à la question [Q178] concernant le nombre d'applications, y compris SaaS, présentes dans leur inventaire/cartographie sur l'ensemble du périmètre IT et OT de leur structure :

Parmi les **Grandes entreprises** :

- **6%** ont entre 0 et 100 applications ;
- **15%** ont entre 101 et 300 applications ;
- **24%** ont entre 301 et 600 applications ;
- **28%** ont entre 601 et 1000 applications ;
- **13%** ont entre 1001 et 1500 applications ;
- **4%** ont entre 1501 et 2000 applications ;
- **10%** ont plus de 2000 applications.

Parmi les **ETI** :

- **32%** ont entre 0 et 100 applications ;
- **42%** ont entre 101 et 300 applications ;
- **16%** ont entre 301 et 600 applications ;
- **6%** ont entre 601 et 1000 applications ;

- **1%** ont entre 1001 et 1500 applications ;
- **0%** ont entre 1501 et 2000 applications ;
- **3%** ont plus de 2000 applications.

Parmi les **TPE/PME** :

- **50%** ont entre 0 et 100 applications ;
- **50%** ont entre 101 et 300 applications.

Tests end-to-end et sécurité

À mesure que les chaînes CI/CD (Continuous Integration/Continuous Delivery) se généralisent, les tests end-to-end deviennent un enjeu clé pour assurer la qualité globale des livraisons, sans freiner l'agilité et sans omettre la sécurité. Pourtant, leur intégration reste un sujet de débat : entre coûts d'exécution, pertinence fonctionnelle et rôle dans la validation sécurité, les approches varient fortement d'une organisation à l'autre.

Les tests de sécurité dans les chaînes CI/CD représentent un équilibre délicat. D'un côté, leur automatisation complète promet rapidité et couverture systématique ; de l'autre, certaines organisations privilégient une approche plus sélective, réservant ces tests à des moments clés du cycle de développement ou les externalisant pour bénéficier d'expertises spécialisées. Entre ces deux extrêmes, beaucoup d'équipes cherchent encore leur modèle, confrontées à des contraintes de ressources, de compétences ou de maturité DevSecOps.

92 membres ont répondu à la question [Q180] concernant la gestion de l'intégration des tests de sécurité dans leurs chaînes CI/CD (ou chaînes de livraison) *(plusieurs réponses étaient possibles)* :

Parmi les **Grandes entreprises** :

- **56%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **22%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **16%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée) ;
- **2%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **29%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **7%** ont répondu « Autre ».

Parmi les **ETI** :

- **34%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **23%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **29%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée);
- **14%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **37%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **6%** ont répondu « Autre ».

Parmi les **TPE/PME** :

- **33%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **25%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **17%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée) ;
- **8%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **25%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **8%** ont répondu « Autre ».

Processus DevSecOps

Au-delà des démarches d'Intégration de la Sécurité dans les Projets (ISP), l'intégration de la sécurité dans les processus de développement (DevSecOps) est un enjeu clé pour garantir la robustesse des applications. La revue de code, les tests automatisés et les audits de sécurité sont des étapes essentielles pour prévenir les vulnérabilités en amont.

Le DevSecOps repose sur un principe simple : la sécurité ne doit plus être un verrou de fin de cycle, mais un fil rouge qui traverse toutes les étapes du développement. Cela implique de déployer des outils automatisés capables de détecter les failles au plus tôt, de former les développeurs aux bonnes pratiques sécuritaires, et de créer une culture de collaboration entre les équipes dev, sécurité et opérations. Pourtant, la réalité du terrain montre une maturité variable : certaines organisations ont pleinement intégré ces pratiques dans leurs pipelines CI/CD, tandis que d'autres en sont encore à des approches plus traditionnelles, basées sur des audits ponctuels ou des tests manuels.

L'enjeu n'est pas seulement technique : il est aussi culturel et organisationnel. Faire évoluer les processus de développement vers le DevSecOps nécessite d'embarquer les équipes, de lever les résistances, et de démontrer la valeur ajoutée de cette approche dans un contexte où la vitesse de livraison reste une priorité forte.

114 membres ont répondu à la question [Q184] concernant les pratiques mises en place pour intégrer la sécurité tout au long du cycle de développement et lors des audits *(plusieurs réponses étaient possibles)* :

- **77%** assurent un suivi de vulnérabilités dans le cadre de la gestion de la dette technique ;
- **75%** conduisent des audits de sécurité réguliers sur les applications ou les infrastructures ;
- **70%** utilisent des outils d'analyse statique et dynamique du code pour détecter les vulnérabilités ;
- **67%** intègrent la sécurité dès la phase de développement (DevSecOps) ;
- **51%** favorisent une collaboration étroite entre les équipes dev, sécurité et opérationnelle ;
- **48%** ont déployé des tests de sécurité automatisés dans le pipeline CI/CD ;
- **39%** proposent une formation continue des développeurs sur les principes de sécurité ;
- **33%** pratiquent une revue de code systématique avec un focus sur les bonnes pratiques sécuritaires ;
- **13%** déploient des sandbox ou environnements de test pour évaluer les risques ;
- **11%** ont répondu « Autre » : certaines équipes combinent tests externes (pentests, bug bounties), revues de code, outils automatisés (SAST/DAST, SCA) et formations, tandis que d'autres déclarent une absence totale de mesures ou une faible implication (sous-traitance, peu de développement). Des projets d'amélioration (revues de code, programmes de formation, intégration de la DSSI) sont en cours, mais l'application reste inégale selon les contextes.

Une ressource proposée par Matthieu Grall pourrait vous intéresser : https://github.com/matthieu-grall/management_systems/blob/main/Structure/08.%20Op%C3%A9rations/5.%20ORGA/08%20-%20PRO%20-%20Int%C3%A9grer%20la%20protection%20des%20donn%C3%A9es%20dans%20les%20projets%20-%20TLP%20AMBER.md

Sensibilisation

Actions de sensibilisation

Une action ponctuelle de sensibilisation, telle que le Cybermois, ne suffit pas à transformer durablement les comportements. Au-delà d'un certain point, les messages peinent à capter l'attention et à maintenir l'engagement des collaborateurs, malgré la répétition ou la multiplication des formats, surtout quand le métier de ces derniers s'éloigne beaucoup du monde « technique », « cyber », « informatique ».

La sensibilisation à la cybersécurité rencontre un plafond de verre : après quelques campagnes, les mêmes messages sont ignorés, les mêmes formats lassent, et l'effet de saturation s'installe. Les collaborateurs deviennent imperméables, non par mauvaise volonté, mais par surcharge informationnelle ou par manque de lien direct avec leur quotidien professionnel. Pour les équipes marketing, RH, ou commerciales, les enjeux cyber peuvent sembler abstraits, lointains, voire secondaires face à leurs priorités métier.

159 membres ont répondu à la question [Q176] concernant les approches mises en place au sein de leur organisation pour dépasser ce plafond de verre et ancrer une culture cybersécurité vivante et participative dans la durée *(plusieurs réponses étaient possibles)* :

Parmi les **Grandes entreprises** :

- **52%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **50%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **46%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **46%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;
- **40%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **33%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **31%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;
- **27%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;
- **27%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;

- **25%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **23%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **15%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **10%** ont mis en place une autre action ;
- **6%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).

Parmi les **ETI** :

- **43%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **37%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **36%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **34%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **33%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;
- **30%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;
- **28%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **28%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **21%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **19%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **19%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;
- **16%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;

- **9%** ont mis en place une autre action ;
- **7%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).

Parmi les **TPE/PME** :

- **55%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **42%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **39%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **39%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;
- **37%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **37%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **26%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **21%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;
- **18%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;
- **16%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **13%** ont mis en place une autre action ;
- **11%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **3%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;
- **3%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).

A noter : les réponses « Autre » incluent notamment des programmes structurés (formations régulières, campagnes de phishing, plateformes dynamiques, Cyberdays, incitations/sanctions,

implication du COMEX et d'un Cyber Culture Manager) ainsi que des initiatives plus ponctuelles (charte, contenus ludiques type CyberFlix). Toutefois, certaines organisations n'ont aucune démarche proactive, souvent faute d'engagement de la direction ou de moyens.

Moyens pour la sensibilisation

Après vous avoir demandé votre avis sur des approches pour briser le plafond de verre en matière de sensibilisation, nous allons nous intéresser cette semaine aux moyens pour y arriver.

Si les approches stratégiques définissent la direction avec l'animation continue, la personnalisation mais aussi avec la gamification, les moyens constituent la boîte à outils concrète pour les mettre en œuvre. Modules e-learning, campagnes de phishing, escape games, démonstrations techniques, talks d'experts... l'éventail est large, et chaque organisation compose son propre mix en fonction de ses ressources, de sa culture, et de son niveau de maturité.

Certains moyens se sont imposés comme des standards : les tests de phishing outillés et les modules e-learning figurent désormais dans la quasi-totalité des programmes de sensibilisation. D'autres, plus ambitieux ou coûteux comme les journées thématiques, les serious games, les talks d'experts, restent l'exclusivité des grandes structures dotées de budgets et d'équipes dédiées. Entre ces deux extrêmes, les organisations de taille intermédiaire cherchent souvent à maximiser l'impact avec des moyens limités, en privilégiant des formats hybrides ou en mutualisant les efforts avec d'autres fonctions (RH, communication interne).

158 membres ont répondu à la question [Q177] concernant les différents moyens de sensibilisation à la cybersécurité mis en œuvre au sein de leur organisation *(plusieurs réponses étaient possibles)* :

Parmi les **Grandes entreprises** :

- **89%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **86%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;
- **80%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **50%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **46%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **38%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;

- **36%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **32%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **32%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **27%** ont mis en œuvre des démonstrations concrètes ;
- **20%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne) ;
- **11%** ont mis en œuvre d'autres moyens.

Parmi les **ETI** :

- **80%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **77%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **72%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;
- **44%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **35%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **30%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;
- **25%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **25%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **23%** ont mis en œuvre des démonstrations concrètes ;
- **17%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **15%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne) ;

- **4%** ont mis en œuvre d'autres moyens.

Parmi les **TPE/PME** :

- **77%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **71%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **55%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;
- **35%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **26%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **26%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;
- **19%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **16%** ont mis en œuvre des démonstrations concrètes ;
- **16%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **13%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **10%** ont mis en œuvre d'autres moyens ;
- **6%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne).

A noter : les réponses « Autre » incluent notamment des modules ou ateliers ludiques hors parcours RH, des interventions interactives via bot Teams ou en présentiel, la communication des scores de tests phishing jusqu'au Comex pour créer une émulation, et la diffusion de supports pratiques (plaquette des règles d'or, formations légales ou en direct).

Gouvernance

Recruter en cybersécurité : quelles pratiques dans un marché sous tension ?

Le recrutement en cybersécurité, qu'il s'agisse de profils opérationnels, de gouvernance ou de direction ne se limite pas à l'analyse de CV, de lettres de motivation ou aux informations trouvées sur LinkedIn. Dans un marché très tendu, chaque organisation développe ses propres leviers : méthodologie, posture, intuition, culture d'équipe...

Les RSSI développent des approches hybrides, mêlant réseau professionnel, recruteurs spécialisés, marque employeur, et pari sur le potentiel. Certains misent sur la cooptation et la proximité communautaire, d'autres sur des parcours de formation internes pour faire émerger des talents non labellisés. L'enjeu : identifier non pas le profil parfait sur le papier, mais celui qui saura s'intégrer, grandir, et tenir dans la durée.

Quant à l'évaluation, elle cristallise les débats : faut-il privilégier les soft skills (communication, gestion du stress, rigueur) ou les hard skills (tests techniques, CTF, exercices pratiques) ? Faut-il faire confiance à l'intuition des opérationnels ou s'appuyer sur des grilles structurées ? La réponse varie fortement d'une organisation à l'autre, reflétant autant des contraintes de moyens que des cultures de recrutement profondément ancrées.

113 membres ont répondu à la question [Q174] en deux volets : les approches les plus efficaces pour recruter en cybersécurité, et les méthodes d'évaluation de la qualité d'un candidat *(plusieurs réponses étaient possibles)* :

Parmi les **Grandes entreprises** :

- **84%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **47%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **44%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise) ;
- **44%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **42%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **33%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;
- **11%** ont mentionné d'autres approches, notamment le reskilling interne ou le réseau.

Parmi les **ETI** :

- **64%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **48%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise) ;

- **40%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **40%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;
- **38%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **33%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **2%** ont mentionné d'autres approches, notamment la chasse directe sur les réseaux sociaux.

Parmi les **TPE/PME** :

- **56%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;
- **44%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **44%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **38%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **38%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **25%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise).

Et comment évaluez-vous la qualité d'un candidat ?

Parmi les **Grandes entreprises** :

- **89%** pratiquent une préqualification approfondie par des opérationnels avant RH ;
- **51%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **51%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **38%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **5%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques) ;
- **9%** évaluent autrement, via la préqualification par des opérationnels après les RH, ainsi que des repères comme les certifications (ex. CISSP), les évaluations internes et le portrait numérique.

Parmi les **ETI** :

- **86%** pratiquent une préqualification approfondie par des opérationnels avant RH ;
- **55%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **52%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **31%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **7%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques) ;
- **2%** évaluent autrement, via des entretiens techniques et opérationnels afin d'évaluer les vrais acquis fondamentaux techniques.

Parmi les **TPE/PME** :

- **81%** pratiquent une préqualification approfondie par des opérationnels avant RH ;
- **56%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **44%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **13%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **13%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques).

Plan Stratégique et schéma directeur Cyber

La cybersécurité, c'est savoir gérer le temps court de l'opérationnel, de la réponse à incident et du maintien en condition de sécurité. C'est aussi le temps long des plans stratégiques et des schémas directeurs permettant de se fixer une ambition, une cible qui se décline ensuite en trajectoire(s) de projets.

Le plan stratégique ou schéma directeur cyber est l'outil qui matérialise cette vision long terme. Il pose un cap, priorise les investissements, structure les projets, et permet de justifier les arbitrages budgétaires. Pourtant, sa formalisation reste inégale : certaines organisations y voient un exercice indispensable de gouvernance, d'autres le jugent trop rigide dans un contexte mouvant où les menaces, les technologies et les priorités métier évoluent en permanence.

La tension entre planification et agilité se reflète dans les pratiques : durée couverte, fréquence de mise à jour, niveau de formalisation... Autant de paramètres qui varient fortement selon la taille, la maturité, et la culture des organisations.

148 membres ont répondu à la question [Q175] concernant la formalisation et la gestion de leur plan stratégique ou schéma directeur cyber :

Parmi les **Grandes entreprises** :

- **86%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **14%** considèrent que « c'est comme le temps, ça change tout le temps ».

Parmi les **ETI** :

- **73%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **27%** considèrent que « c'est comme le temps, ça change tout le temps ».

Parmi les **TPE/PME** :

- **57%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **43%** considèrent que « c'est comme le temps, ça change tout le temps ».

Votre plan stratégique/schéma directeur est élaboré sur...

Parmi les **Grandes entreprises** :

- **82%** couvrent 2 à 3 ans ;
- **16%** couvrent plus de 4 ans
- **2%** couvrent moins de 2 ans.

Parmi les **ETI** :

- **70%** couvrent 2 à 3 ans ;
- **17%** couvrent plus de 4 ans ;
- **13%** couvrent moins de 2 ans.

Parmi les **TPE/PME** :

- **58%** couvrent 2 à 3 ans ;
- **33%** couvrent moins de 2 ans ;
- **9%** couvrent plus de 4 ans.

Faites-vous une mise à jour régulière de votre plan stratégique ?

Parmi les **Grandes entreprises** :

- **79%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **21%** ne réalisent pas cette mise à jour régulièrement.

Parmi les **ETI** :

- **69%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **31%** ne réalisent pas cette mise à jour régulièrement.

Parmi les **TPE/PME** :

- **55%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **45%** ne réalisent pas cette mise à jour régulièrement.

Choix des outils de sécurité IT

Le choix des outils de sécurité IT (EDR, SIEM, IAM, DLP, etc.) est un enjeu clé pour les organisations. Identifier qui détient réellement cette responsabilité permet de mieux comprendre la place du RSSI dans l'organisation et son impact sur la stratégie de cybersécurité.

Dans certaines organisations, le RSSI dispose d'une autonomie pleine et entière : il pilote, choisit, et assume. Dans d'autres, la décision est partagée avec la DSI, les équipes techniques, voire les Achats ou la Direction Générale. Entre ces deux extrêmes, une zone grise peuplée de modèles hybrides, de décisions collégiales, d'arbitrages au cas par cas, et de rapports de force implicites. La gouvernance du choix des outils est un révélateur intéressant de la maturité cyber d'une organisation, mais aussi de la place réelle et pas seulement affichée du RSSI dans l'organigramme.

Cette diversité de modèles reflète des réalités organisationnelles très contrastées : taille de la structure, rattachement du RSSI, culture de décision centralisée ou distribuée, maturité de la fonction sécurité, poids relatif de la DSI, etc.

160 membres ont répondu à la question [Q179] concernant l'acteur qui prend principalement les décisions relatives au choix des outils de sécurité IT au sein de leur organisation :

Parmi les **Grandes entreprises** :

- **35%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **34%** : décisions prises par le RSSI (si hors DSI) ;
- **12%** : décisions prises par la DSI ;
- **6%** : décisions prises par le RSSI (intégré à la DSI) ;
- **1%** : décisions prises au cas par cas selon les outils ;
- **0%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;
- **12%** ont répondu « Aucun de ces cas » car les décisions sont majoritairement collégiales ou partagées entre plusieurs acteurs : CISO/RSSI, DSI, équipes techniques et parfois la Direction des Achats. Dans certains cas, la décision relève du CISO Groupe ou de la holding, tandis que d'autres évoquent une répartition par domaine (Identify/Protect/Govern/Detect) ou une implication du COMEX en cas d'arbitrage.

Parmi les **ETI** :

- **43%** : décisions prises par le RSSI (si hors DSI) ;
- **22%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **17%** : décisions prises par la DSI ;
- **9%** : décisions prises par le RSSI (intégré à la DSI) ;
- **3%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;
- **3%** : décisions prises au cas par cas selon les outils ;
- **3%** ont répondu « Aucun de ces cas » car les décisions sont majoritairement collégiales ou partagées entre plusieurs acteurs : CISO/RSSI, DSI, équipes techniques et parfois la Direction des Achats. Dans certains cas, la décision relève du CISO Groupe ou de la holding, tandis que d'autres évoquent une répartition par domaine (Identify/Protect/Govern/Detect) ou une implication du COMEX en cas d'arbitrage.

Parmi les **TPE/PME** :

- **43%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **35%** : décisions prises par le RSSI (si hors DSI) ;
- **13%** : décisions prises par le RSSI (intégré à la DSI) ;
- **5%** : décisions prises par la DSI ;
- **4%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;
- **0%** : décisions prises au cas par cas selon les outils ;
- **0%** ont répondu « Aucun de ces cas ».

Fidélisation des talents

Dans un marché aussi mouvant que la cybersécurité, garder ses talents est un enjeu au même titre que les recruter. Au-delà du salaire, ce sont l'environnement, les perspectives, la reconnaissance ou encore la mission qui peuvent aussi faire la différence.

Le levier salarial, bien que nécessaire, ne suffit plus. Les profils cyber recherchent aujourd'hui un équilibre global : qualité de vie au travail, reconnaissance, sentiment d'utilité, perspectives d'évolution, autonomie, formation continue... Autant de dimensions qui, cumulées, composent une « expérience collaborateur » attractive et différenciante.

Les RSSI ne contrôlent pas tous ces leviers : la politique salariale est du ressort de la DRH ou de la Direction Générale, la flexibilité télétravail dépend de la culture d'entreprise, les mobilités internes sont conditionnées par les opportunités, etc.

Ils peuvent cependant agir sur l'ambiance d'équipe, la reconnaissance du travail accompli, l'inclusion dans les réflexions stratégiques, et la création d'un cadre de travail où chacun se sent écouté, valorisé, et challengé.

180 membres ont répondu à la question [Q181] concernant les actions ou leviers utilisés pour favoriser la rétention des profils cyber dans leurs équipes *(plusieurs réponses étaient possibles)* :

- **68%** s'appuient sur l'ambiance d'équipe et la reconnaissance quotidienne ;
- **63%** offrent de la flexibilité (télétravail, gestion du temps, politique de congé, droit à la déconnexion...) ;
- **59%** proposent un parcours de formation et de montée en compétences continue ;
- **51%** cultivent la culture de la mission / sentiment d'utilité dans l'organisation ;

- **44%** favorisent l'inclusion dans les réflexions stratégiques sécurité ;
- **40%** pratiquent des revues salariales (augmentation, primes, avantages, ...) ;
- **38%** organisent des feedbacks réguliers et entretiens de suivi non formels ;
- **31%** assurent la clarté sur les perspectives d'évolution (experte, managériale, transverse) ;
- **14%** proposent la mobilité interne vers d'autres rôles ou entités ;
- **13%** ont répondu « Autre » et utilisent notamment d'autres leviers tels que le cadre de vie, la récurrence des opportunités proposées, un cadre de réduction des irritants (désamorçage des conflits, rotation des tâches à faible valeur ajoutée, diversification des tâches, développement de l'automatisation...) ; certains n'ont rien mis en place.

ANNEXES

QUESTION DE LA SEMAINE : DETAIL DES RESULTATS (graphiques)

[Q174] Recruter en cybersécurité : quelles pratiques dans un marché sous tension ? Quelles sont selon vous les approches les plus efficaces pour recruter en cybersécurité ?

Parmi les **Grandes entreprises** :

- **84%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **47%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **44%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise) ;
- **44%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **42%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **33%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;
- **11%** ont mentionné d'autres approches, notamment le reskilling interne ou le réseau.

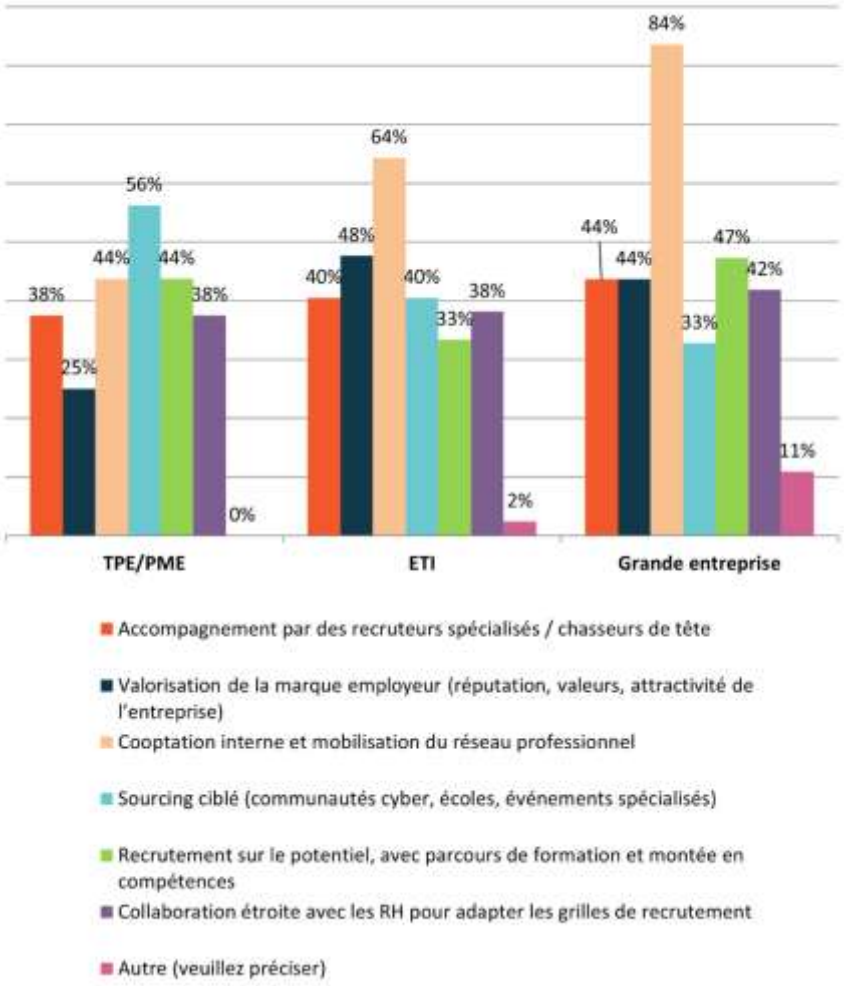
Parmi les **ETI** :

- **64%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **48%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise) ;
- **40%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **40%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;
- **38%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **33%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **2%** ont mentionné d'autres approches, notamment la chasse directe sur les réseaux sociaux.

Parmi les **TPE/PME** :

- **56%** recrutent sur le potentiel, avec parcours de formation et montée en compétences ;

- **44%** s'appuient sur l'accompagnement par des recruteurs spécialisés / chasseurs de tête ;
- **44%** privilégient la collaboration étroite avec les RH pour adapter les grilles de recrutement ;
- **38%** utilisent la cooptation interne et la mobilisation du réseau professionnel ;
- **38%** pratiquent le sourcing ciblé (communautés cyber, écoles, événements spécialisés) ;
- **25%** valorisent la marque employeur (réputation, valeurs, attractivité de l'entreprise).



Et comment évaluez-vous la qualité d'un candidat ?

Parmi les **Grandes entreprises** :

- **89%** pratiquent une préqualification approfondie par des opérationnels avant RH ;

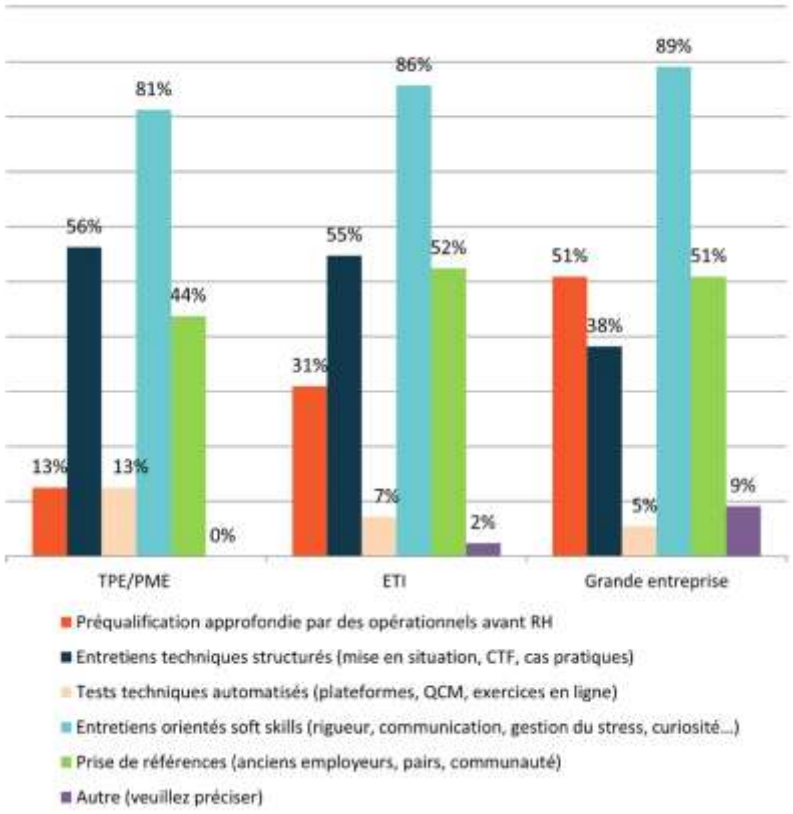
- **51%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **51%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **38%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **5%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques) ;
- **9%** évaluent autrement, via la préqualification par des opérationnels après les RH, ainsi que des repères comme les certifications (ex. CISSP), les évaluations internes et le portrait numérique.

Parmi les **ETI** :

- **86%** pratiquent une préqualification approfondie par des opérationnels avant RH ;
- **55%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **52%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **31%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **7%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques) ;
- **2%** évaluent autrement, via des entretiens techniques et opérationnels afin d'évaluer les vrais acquis fondamentaux techniques.

Parmi les **TPE/PME** :

- **81%** pratiquent une préqualification approfondie par des opérationnels avant RH ;
- **56%** effectuent une prise de références (anciens employeurs, pairs, communauté) ;
- **44%** utilisent des tests techniques automatisés (plateformes, QCM, exercices en ligne) ;
- **13%** privilégient des entretiens orientés soft skills (rigueur, communication, gestion du stress, curiosité...) ;
- **13%** mettent en place des entretiens techniques structurés (mise en situation, CTF, cas pratiques).



[Q175] Plan Stratégique et schéma directeur Cyber : Avez-vous formalisé un plan stratégique/schéma directeur Cyber pour votre organisation ?

Parmi les **Grandes entreprises** :

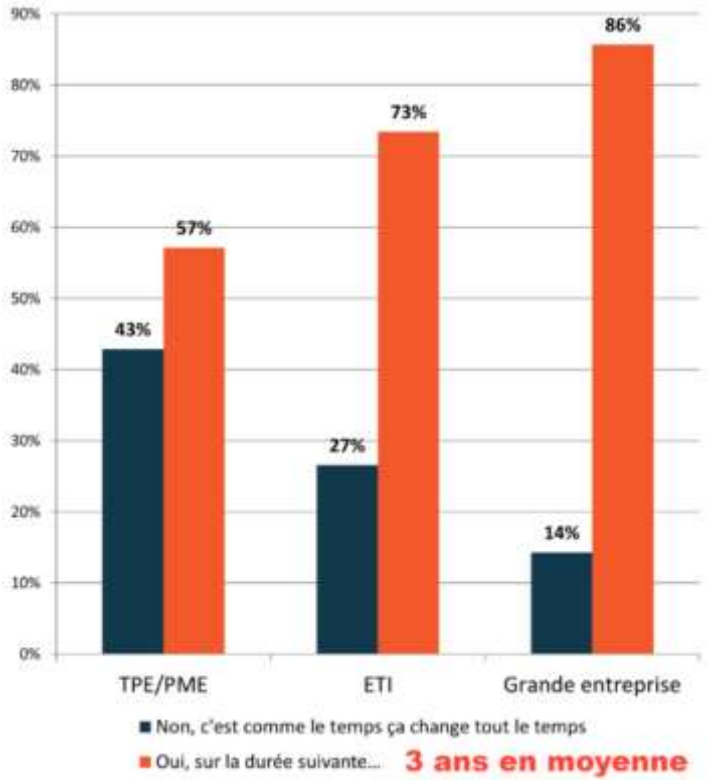
- **86%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **14%** considèrent que « c'est comme le temps, ça change tout le temps ».

Parmi les **ETI** :

- **73%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **27%** considèrent que « c'est comme le temps, ça change tout le temps ».

Parmi les **TPE/PME** :

- **57%** ont formalisé un plan stratégique/schéma directeur sur 3 ans en moyenne ;
- **43%** considèrent que « c'est comme le temps, ça change tout le temps ».



Votre plan stratégique/schéma directeur est élaboré sur...

Parmi les **Grandes entreprises** :

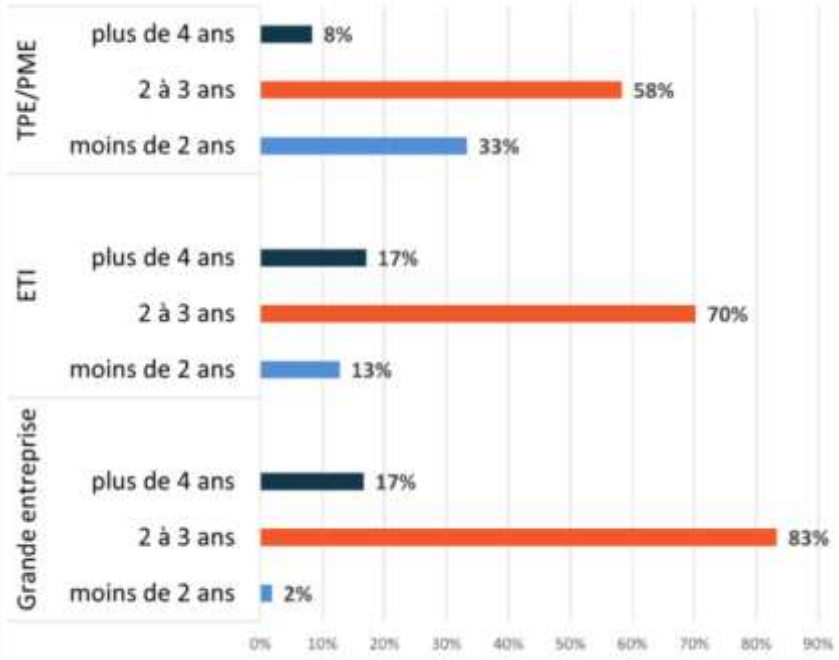
- **2%** couvrent moins de 2 ans ;
- **82%** couvrent 2 à 3 ans ;
- **16%** couvrent plus de 4 ans.

Parmi les **ETI** :

- **13%** couvrent moins de 2 ans ;
- **70%** couvrent 2 à 3 ans ;
- **17%** couvrent plus de 4 ans.

Parmi les **TPE/PME** :

- **33%** couvrent moins de 2 ans ;
- **58%** couvrent 2 à 3 ans ;
- **9%** couvrent plus de 4 ans.



Faites-vous une mise à jour régulière de votre plan stratégique ?

Parmi les **Grandes entreprises** :

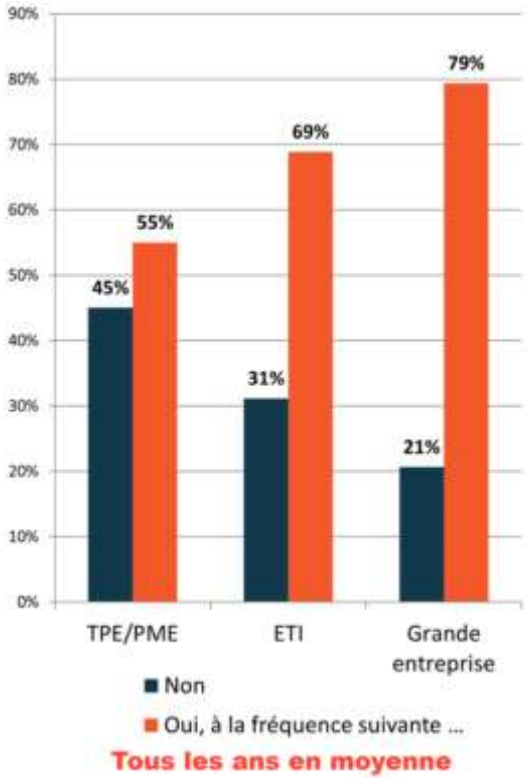
- **79%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **21%** ne réalisent pas cette mise à jour régulièrement.

Parmi les **ETI** :

- **69%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **31%** ne réalisent pas cette mise à jour régulièrement.

Parmi les **TPE/PME** :

- **55%** mettent à jour, tous les ans en moyenne, leur plan stratégique ;
- **45%** ne réalisent pas cette mise à jour régulièrement.



[Q176] Actions de sensibilisation : Dans votre organisation, quelles approches avez-vous mis en place pour dépasser ce plafond de verre et ancrer une culture cybersécurité vivante et participative dans la durée ? *(plusieurs réponses étaient possibles)*

Parmi les **Grandes entreprises** :

- **52%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **50%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **46%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **46%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;

- **40%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **33%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **31%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;
- **27%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;
- **27%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;
- **25%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **23%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **15%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **10%** ont mis en place une autre action ;
- **6%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).

Parmi les **ETI** :

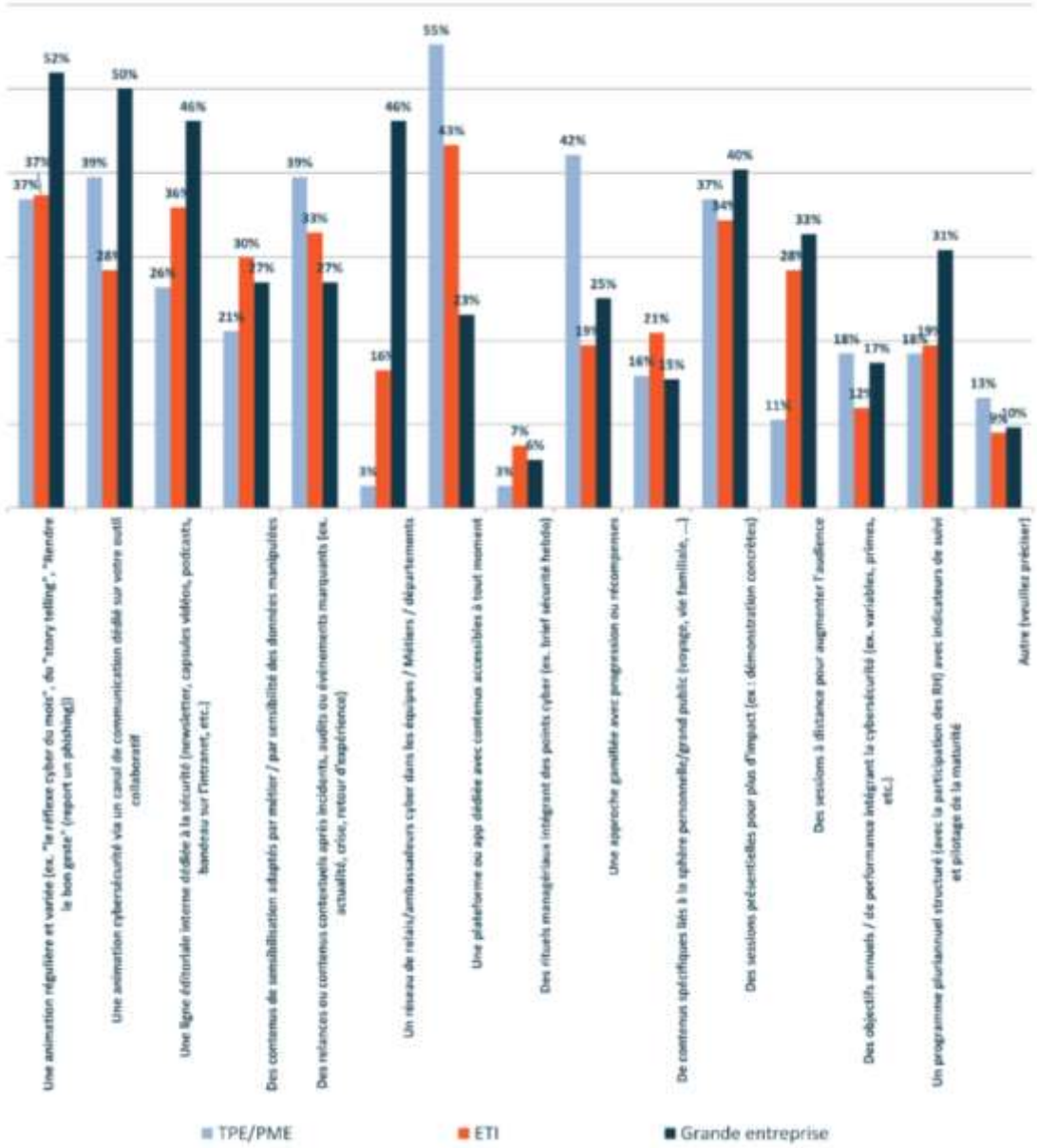
- **43%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **37%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **36%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **34%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **33%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;
- **30%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;

- **28%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **28%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **21%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **19%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **19%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;
- **16%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;
- **9%** ont mis en place une autre action ;
- **7%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).

Parmi les **TPE/PME** :

- **55%** ont mis en place une plateforme ou app dédiée avec contenus accessibles à tout moment ;
- **42%** ont mis en place une approche gamifiée avec progression ou récompenses ;
- **39%** ont mis en place une animation cybersécurité via un canal de communication dédié sur leur outil collaboratif ;
- **39%** ont mis en place des relances ou contenus contextuels après incidents, audits ou événements marquants (ex. actualité, crise, retour d'expérience) ;
- **37%** ont mis en place une animation régulière et variée (ex. « le réflexe cyber du mois », du « story telling », « Rendre le bon geste » (report un phishing)) ;
- **37%** ont mis en place des sessions présentielles pour plus d'impact (ex : démonstrations concrètes) ;
- **26%** ont mis en place une ligne éditoriale interne dédiée à la sécurité (newsletter, capsules vidéos, podcasts, bandeau sur l'intranet, etc.) ;
- **21%** ont mis en place des contenus de sensibilisation adaptés par métier / par sensibilité des données manipulées ;
- **18%** ont mis en place des objectifs annuels / de performance intégrant la cybersécurité (ex. variables, primes, etc.) ;

- **16%** ont mis en place des contenus spécifiques liés à la sphère personnelle/grand public (voyage, vie familiale, ...) ;
- **13%** ont mis en place une autre action ;
- **11%** ont mis en place des sessions à distance pour augmenter l'audience ;
- **3%** ont mis en place un réseau de relais/ambassadeurs cyber dans les équipes / Métiers / départements ;
- **3%** ont mis en place des rituels managériaux intégrant des points cyber (ex. brief sécurité hebdo).



[Q177] Moyens pour la sensibilisation : Quels sont les différents moyens de sensibilisation à la cybersécurité que vous avez mis en œuvre au sein de votre organisation ? *(plusieurs réponses étaient possibles)*

Parmi les **Grandes entreprises** :

- **89%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **86%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;
- **80%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **50%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **46%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **38%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;
- **36%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **32%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **32%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **27%** ont mis en œuvre des démonstrations concrètes ;
- **20%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne) ;
- **11%** ont mis en œuvre d'autres moyens.

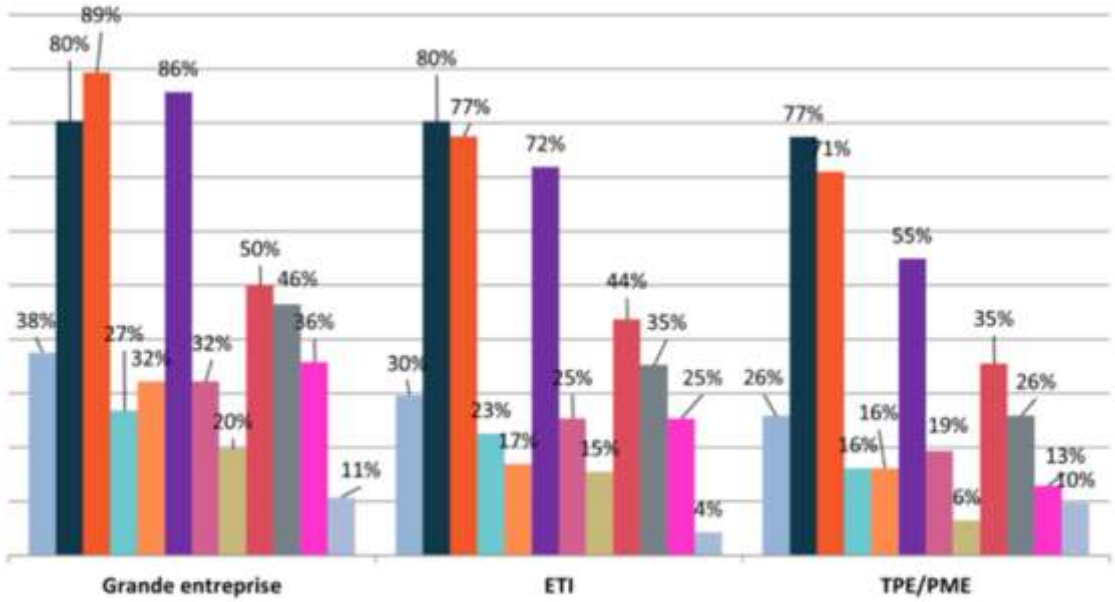
Parmi les **ETI** :

- **80%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **77%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **72%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;
- **44%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **35%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **30%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;
- **25%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **25%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **23%** ont mis en œuvre des démonstrations concrètes ;
- **17%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **15%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne) ;
- **4%** ont mis en œuvre d'autres moyens.

Parmi les **TPE/PME** :

- **77%** ont mis en œuvre des tests de faux phishing « outillés » pour simuler des attaques et mesurer les réactions via un outil ;
- **71%** ont mis en œuvre des modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber) ;
- **55%** ont mis en œuvre des campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos) ;

- **35%** ont mis en œuvre des mini exercices de gestion de crise ou d'incidents de cybersécurité ;
- **26%** ont mis en œuvre une intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.) ;
- **26%** ont mis en œuvre des tests de faux phishing « maison » pour simuler des attaques et mesurer les réactions ;
- **19%** ont mis en œuvre des journées cybersécurité ou semaines thématiques ;
- **16%** ont mis en œuvre des démonstrations concrètes ;
- **16%** ont mis en œuvre des escape games, « serious game », challenges ou quiz internes avec jeu concours ;
- **13%** ont mis à disposition la base de connaissance (communicable) de la cybersécurité ;
- **10%** ont mis en œuvre d'autres moyens ;
- **6%** ont mis en œuvre des talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne).



- Des tests de faux phishing "maison" pour simuler des attaques et mesurer les réactions
- Des tests de faux phishing "outillés" pour simuler des attaques et mesures les réactions via un outil
- Modules e-learning / microlearning intégrés au parcours RH, avec des modules ou des thématiques dédiées selon le Métier du collaborateur (exemple : sensibilisation / formation des développeurs à la cyber)
- Démonstrations concrètes
- Escape games, "serious game", challenges ou quiz internes avec jeu concours
- Campagnes de communication régulières avec diffusion d'un contenu spécifique ou séries thématiques (affiches, newsletters, vidéos)
- Journées cybersécurité ou semaines thématiques
- Talks d'experts (ANSSI, Cybermalveillance.gouv.fr, assureurs, etc.) pouvant faire des retours d'expérience d'incidents anonymisés ou d'incidents en interne (par des experts en interne)
- Mini exercice de gestion de crise ou d'incidents de cybersécurité
- Intégration de la sensibilisation dans les processus métier (onboarding, achats, etc.)
- Mise à disposition de la base de connaissance (communicable) de la cybersécurité
- Autre (veuillez préciser)

[Q178] Périmètre applicatif des RSSI : Combien d'applications, y compris Saas, avez-vous dans votre inventaire/cartographie sur l'ensemble du périmètre IT et OT de votre structure ?

Parmi les **Grandes entreprises** :

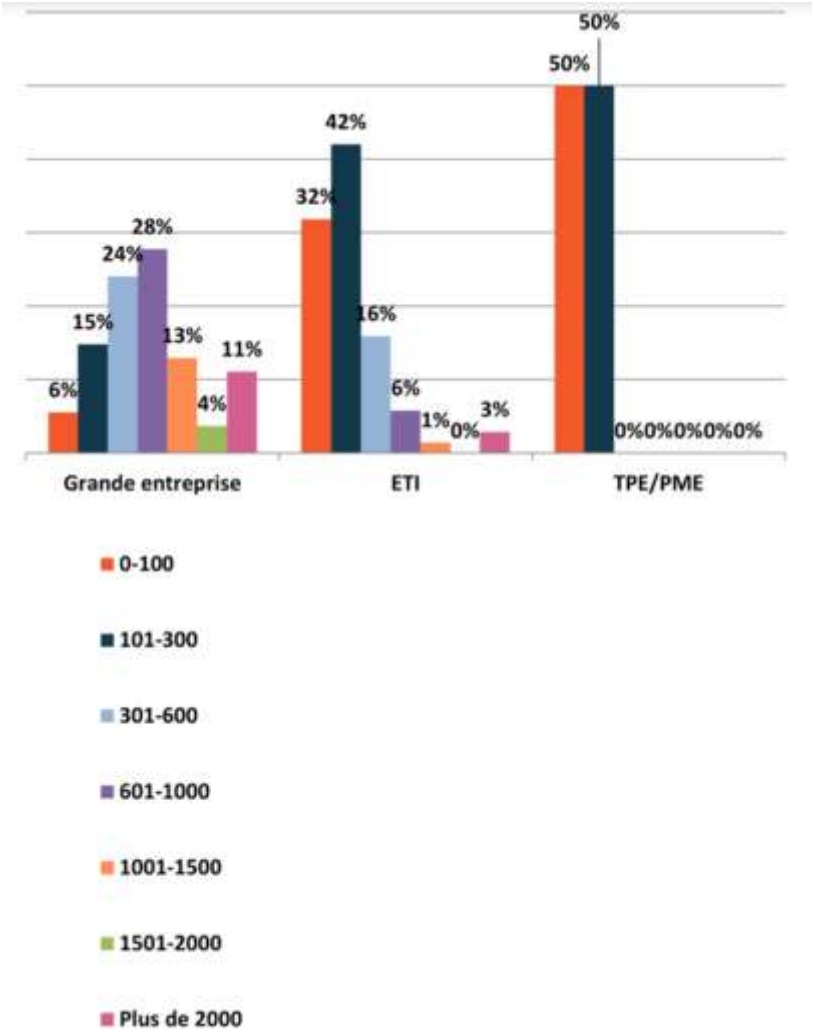
- **6%** ont entre 0 et 100 applications ;
- **15%** ont entre 101 et 300 applications ;
- **24%** ont entre 301 et 600 applications ;
- **28%** ont entre 601 et 1000 applications ;
- **13%** ont entre 1001 et 1500 applications ;
- **4%** ont entre 1501 et 2000 applications ;
- **10%** ont plus de 2000 applications.

Parmi les **ETI** :

- **32%** ont entre 0 et 100 applications ;
- **42%** ont entre 101 et 300 applications ;
- **16%** ont entre 301 et 600 applications ;
- **6%** ont entre 601 et 1000 applications ;
- **1%** ont entre 1001 et 1500 applications ;
- **0%** ont entre 1501 et 2000 applications ;
- **3%** ont plus de 2000 applications.

Parmi les **TPE/PME** :

- **50%** ont entre 0 et 100 applications ;
- **50%** ont entre 101 et 300 applications.



[Q179] Choix des outils de sécurité IT : Dans votre organisation, qui prend principalement les décisions concernant le choix des outils de sécurité IT ?

Parmi les **Grandes entreprises** :

- **35%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **34%** : décisions prises par le RSSI (si hors DSI) ;
- **12%** : décisions prises par la DSI ;
- **6%** : décisions prises par le RSSI (intégré à la DSI) ;
- **1%** : décisions prises au cas par cas selon les outils ;
- **0%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;

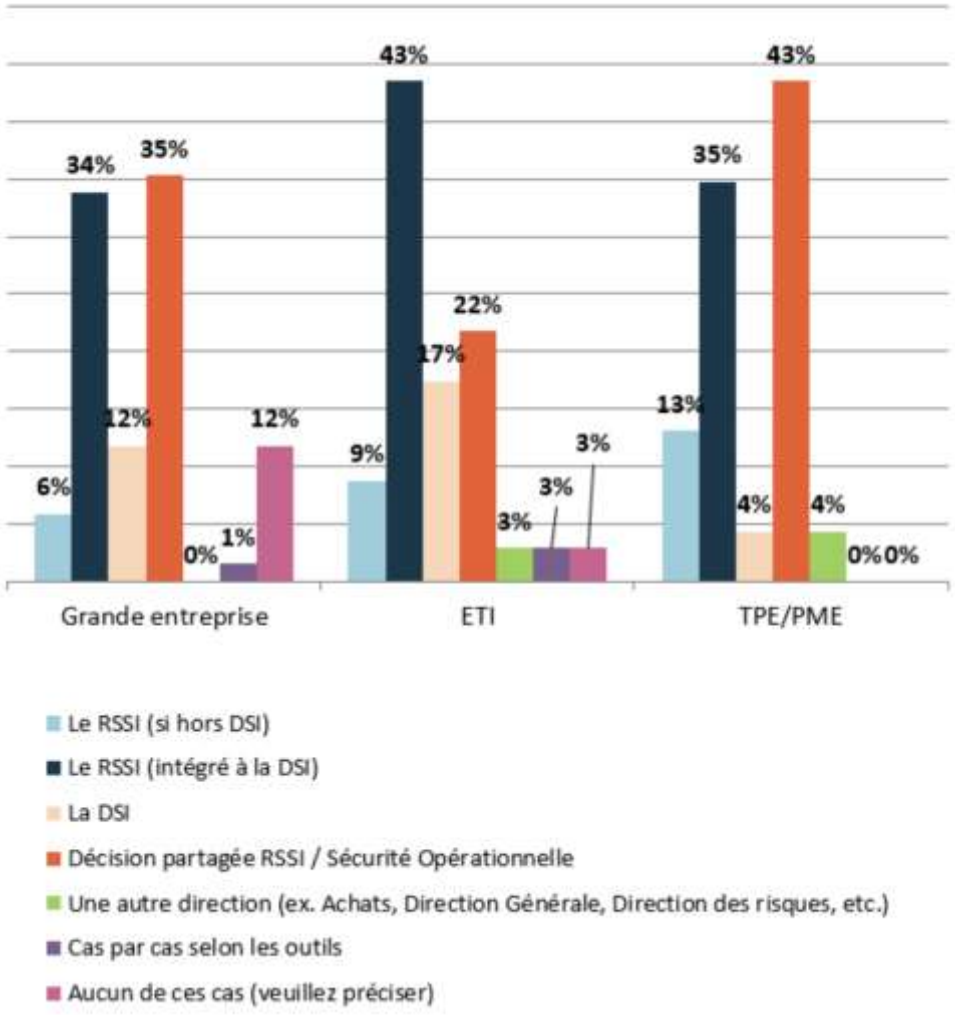
- **12%** ont répondu « Aucun de ces cas » car les décisions sont majoritairement collégiales ou partagées entre plusieurs acteurs : CISO/RSSI, DSI, équipes techniques et parfois la Direction des Achats. Dans certains cas, la décision relève du CISO Groupe ou de la holding, tandis que d'autres évoquent une répartition par domaine (Identify/Protect/Govern/Detect) ou une implication du COMEX en cas d'arbitrage.

Parmi les **ETI** :

- **43%** : décisions prises par le RSSI (si hors DSI) ;
- **22%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **17%** : décisions prises par la DSI ;
- **9%** : décisions prises par le RSSI (intégré à la DSI) ;
- **3%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;
- **3%** : décisions prises au cas par cas selon les outils ;
- **3%** ont répondu « Aucun de ces cas » car les décisions sont majoritairement collégiales ou partagées entre plusieurs acteurs : CISO/RSSI, DSI, équipes techniques et parfois la Direction des Achats. Dans certains cas, la décision relève du CISO Groupe ou de la holding, tandis que d'autres évoquent une répartition par domaine (Identify/Protect/Govern/Detect) ou une implication du COMEX en cas d'arbitrage.

Parmi les **TPE/PME** :

- **43%** : décision partagée RSSI / Sécurité Opérationnelle ;
- **35%** : décisions prises par le RSSI (si hors DSI) ;
- **13%** : décisions prises par le RSSI (intégré à la DSI) ;
- **5%** : décisions prises par la DSI ;
- **4%** : décisions prises par une autre direction (ex. Achats, Direction Générale, Direction des Risques, etc.) ;
- **0%** : décisions prises au cas par cas selon les outils ;
- **0%** ont répondu « Aucun de ces cas ».



[Q180] Tests end-to-end et sécurité : Comment gérez-vous l'intégration des tests de sécurité dans vos chaînes CI/CD (ou chaînes de livraison) ? *(plusieurs réponses étaient possibles)*

Parmi les **Grandes entreprises** :

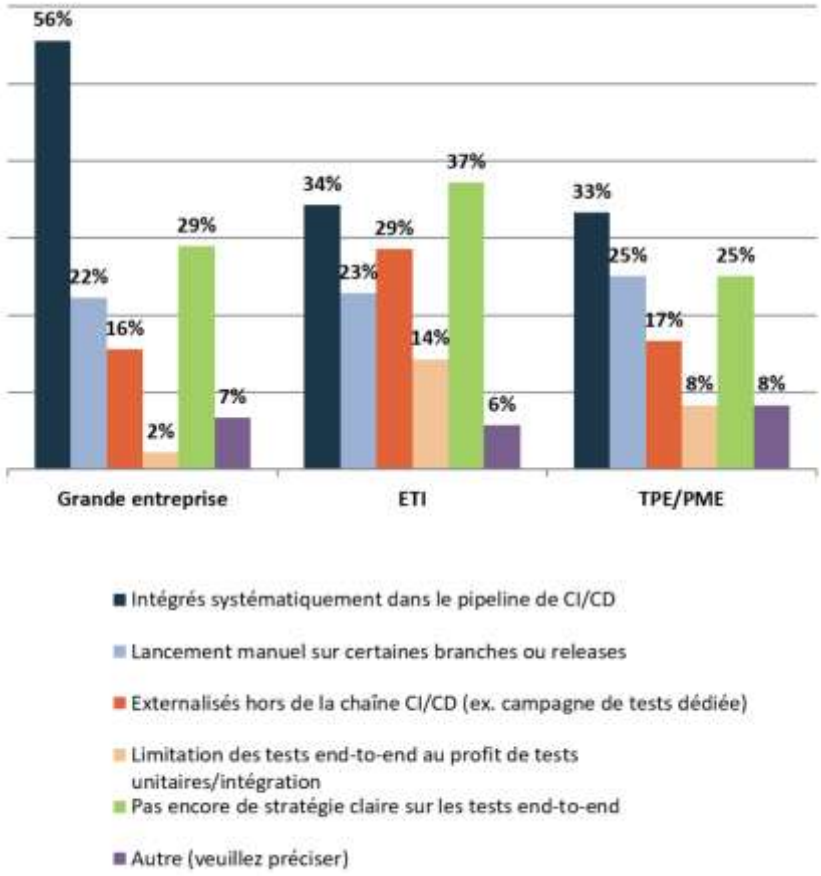
- **56%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **22%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **16%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée) ;
- **2%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **29%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **7%** ont répondu « Autre ».

Parmi les **ETI** :

- **34%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **23%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **29%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée) ;
- **14%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **37%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **6%** ont répondu « Autre ».

Parmi les **TPE/PME** :

- **33%** les intègrent systématiquement dans le pipeline de CI/CD ;
- **25%** ont mis en place un lancement manuel sur certaines branches ou releases ;
- **17%** externalisent ces tests de sécurité hors de la chaîne CI/CD (ex. campagne de tests dédiée) ;
- **8%** limitent les tests end-to-end au profit de tests unitaires/intégration ;
- **25%** n'ont pas encore de stratégie claire sur les tests end-to-end ;
- **8%** ont répondu « Autre ».



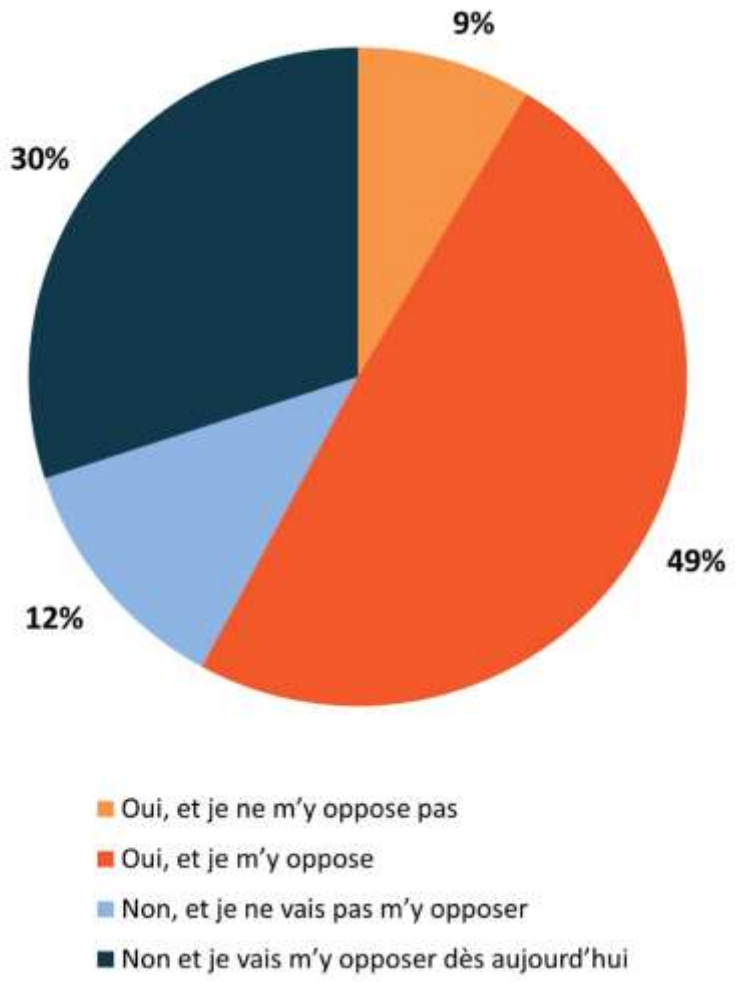
[Q181] Fidélisation des talents : Quelles actions ou leviers utilisez-vous pour favoriser la rétention des profils cyber dans vos équipes ? *(plusieurs réponses étaient possibles)*

- **68%** s'appuient sur l'ambiance d'équipe et la reconnaissance quotidienne ;
- **63%** offrent de la flexibilité (télétravail, gestion du temps, politique de congé, droit à la déconnexion...) ;
- **59%** proposent un parcours de formation et de montée en compétences continue ;
- **51%** cultivent la culture de la mission / sentiment d'utilité dans l'organisation ;
- **44%** favorisent l'inclusion dans les réflexions stratégiques sécurité ;
- **40%** pratiquent des revues salariales (augmentation, primes, avantages, ...) ;
- **38%** organisent des feedbacks réguliers et entretiens de suivi non formels ;
- **31%** assurent la clarté sur les perspectives d'évolution (experte, managériale, transverse) ;

- **14%** proposent la mobilité interne vers d'autres rôles ou entités ;
- **13%** ont répondu « Autre » et utilisent notamment d'autres leviers tels que le cadre de vie, la récurrence des opportunités proposées, un cadre de réduction des irritants (désamorçage des conflits, rotation des tâches à faible valeur ajoutée, diversification des tâches, développement de l'automatisation...) ; certains n'ont rien mis en place.

[Q182] IA, LinkedIn et Microsoft : À titre individuel, aviez-vous connaissance de l'option d'opposition ?

- **58%** le savaient, dont 49% s'y opposent et 9% ne s'y opposent pas ;
- **42%** ne le savaient pas, dont 30% vont s'y opposer et 12% non.



À titre professionnel, et pour votre organisation, le saviez-vous et qu'avez-vous mis en place ?

- **51%** le savaient, dont :
  - 37% ne vont pas pousser une politique globale d'opposition ;
  - 5% ont poussé une politique globale d'opposition ;
  - 4% vont pousser une politique globale d'opposition ;

- 5% vont pousser une politique globale d'opposition uniquement pour l'un ou l'autre (majoritairement pour Microsoft).

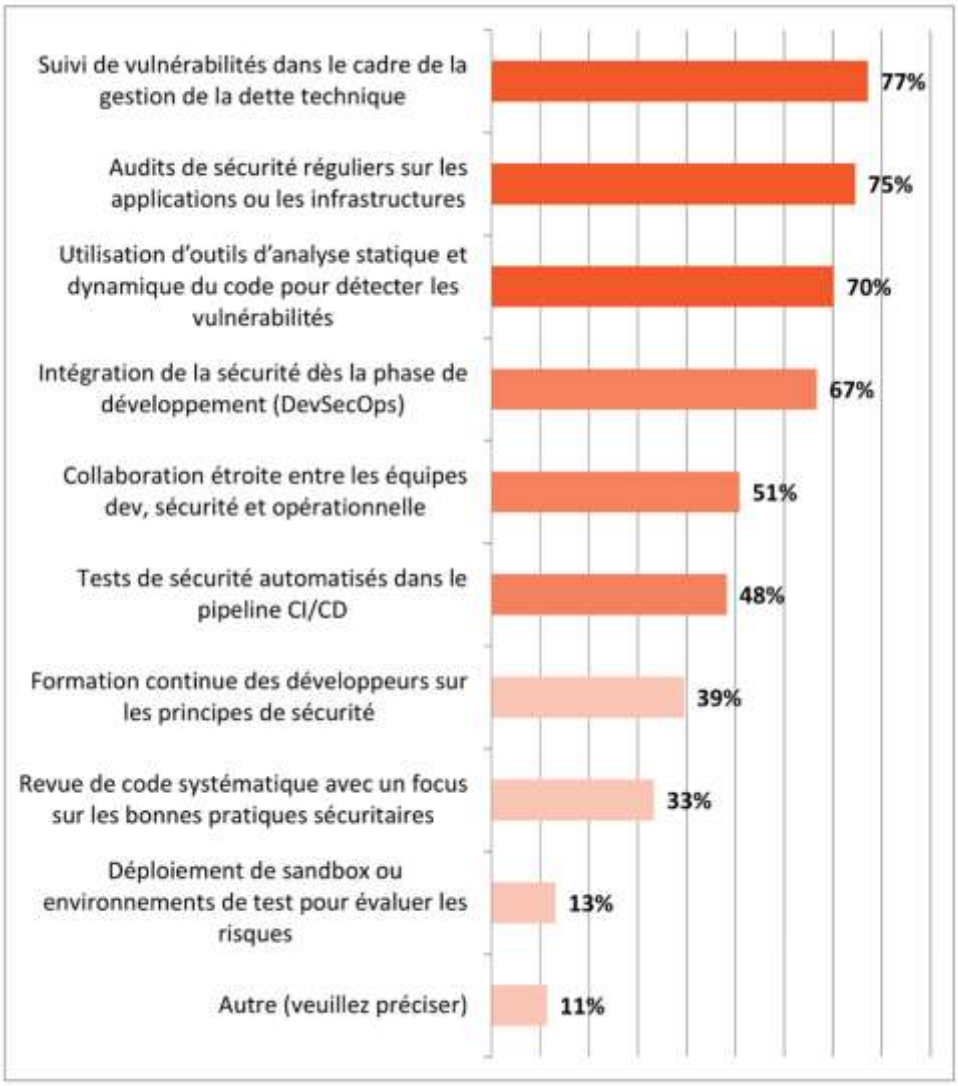
♦ **49%** ne le savaient pas, dont 23% vont préparer une politique globale d'opposition à pousser pour les salariés et 26% non.

[Q183] Livre blanc Dépendance Numérique

Le livre blanc est disponible sur le site du CESIN : ici

[Q184] Processus DevSecOps Quelles pratiques mettez-vous en place pour intégrer la sécurité tout au long du cycle de développement et lors des audits ? *(plusieurs réponses étaient possibles)*

- **77%** assurent un suivi de vulnérabilités dans le cadre de la gestion de la dette technique ;
- **75%** conduisent des audits de sécurité réguliers sur les applications ou les infrastructures ;
- **70%** utilisent des outils d'analyse statique et dynamique du code pour détecter les vulnérabilités ;
- **67%** intègrent la sécurité dès la phase de développement (DevSecOps) ;
- **51%** favorisent une collaboration étroite entre les équipes dev, sécurité et opérationnelle ;
- **48%** ont déployé des tests de sécurité automatisés dans le pipeline CI/CD ;
- **39%** proposent une formation continue des développeurs sur les principes de sécurité ;
- **33%** pratiquent une revue de code systématique avec un focus sur les bonnes pratiques sécuritaires ;
- **13%** déploient des sandbox ou environnements de test pour évaluer les risques ;
- **11%** ont répondu « Autre » : certaines équipes combinent tests externes (pentests, bug bounties), revues de code, outils automatisés (SAST/DAST, SCA) et formations, tandis que d'autres déclarent une absence totale de mesures ou une faible implication (sous-traitance, peu de développement). Des projets d'amélioration (revues de code, programmes de formation, intégration de la DSSI) sont en cours, mais l'application reste inégale selon les contextes.



[Q185] Actions Les incidents de sécurité SaaS en forte augmentation : De votre côté, avez-vous fait le même constat que cette enquête ?

- **54%** font le même constat, dont :
    - 37% tout à fait, en observant une augmentation significative des incidents de sécurité liés aux applications SaaS qu'ils utilisent ;
    - 6% en partie, car ils arrivent à bloquer en amont ;
    - 11% en partie, car leurs fournisseurs SaaS réussissent à circonscrire l'incident.
- **46%** ne font pas le même constat, dont :

- 32% indiquent que les incidents dans ce segment restent rares et qu'ils n'ont pas observé d'évolution récemment ;
- 14% indiquent qu'ils n'ont jamais eu d'incidents avec leurs applications SaaS.