cybervadis

CESIN

Panorama de la maturité en cybersécurité des entreprises françaises

Sommaire

Encart Méthodologique

La présente analyse s'appuie sur des évaluations de maturité cybersécurité, standardisées et vérifiées, menées par CyberVadis.

Le **référentiel** d'évaluation CyberVadis est un cadre hybride et évolutif. Il intègre les principaux standards internationaux (NIST CSF 2.0, ISO 27002:2022), les exigences des réglementations clés (NIS2, DORA) et s'adapte en continu à l'évolution des menaces et des pratiques, comme celles liées à l'IA.

Chaque évaluation est basée sur les réponses fournies par l'entreprise, qui doivent être systématiquement étayées par des preuves documentaires. La méthodologie analyse deux types de preuves complémentaires pour évaluer la maturité réelle :

- **Les preuves de définition :**
  Elles attestent que la mesure est formellement définie (ex: politiques de sécurité, procédures, schémas d'architecture, chartes).
- **Les preuves d'implémentation :**
  Elles démontrent que la mesure est techniquement et organisationnellement en place et fonctionnelle (ex: captures d'écran de configuration, extraits de journaux d'événements, inventaires, preuves d'utilisation de solutions techniques).

L'ensemble de ces preuves est ensuite **analysé** par une équipe d'experts en cybersécurité afin de valider la pertinence et la véracité des éléments fournis. Le framework d'évaluation est **adapté au contexte de chaque entreprise** (taille, secteur d'activité, exposition à la menace) en ajustant le périmètre des contrôles de sécurité applicables et attendus.
Cette approche contextuelle garantit que le **score** de maturité final est une juste représentation de la posture de sécurité d'une organisation au regard des risques qui lui sont propres.

Chaque contrôle de sécurité évalué se voit attribuer un score qui contribue au résultat global de l'évaluation.
Dans chaque thématique, on distingue des sujets élémentaires– qui couvrent les fondamentaux – et des sujets avancés. Un score inférieur à 550 indique une incapacité à démontrer la mise en œuvre des sujets élémentaires alors qu'un score supérieur à 850 confirme la mise en œuvre de nombreuses mesures de sécurité avancées. Le score final, calculé sur une échelle de 0 à 1000, positionne chaque entreprise sur l'un des cinq niveaux de maturité suivants : Mature (score supérieur à 850), Developed (Avancé) (700-849), Moderate (Modéré) (550-699), Basic (Basique) (400-549), et Insufficient (Insuffisant) (score inférieur à 400).

Executive Summary

L’analyse globale de la maturité en cybersécurité des entreprises françaises, évaluées par Cybervadis, confirme globalement des tendances qui pouvaient être attendues.

Premièrement, une corrélation significative entre l'assujettissement à la directive NIS 2 et la maturité est clairement établie, les entités régulées affichant une maturité supérieure.

Deuxièmement, un écart persistant entre la formalisation des politiques et leur mise en œuvre effective et vérifiable constitue un défi majeur pour toutes les catégories d'entreprises, particulièrement en ce qui concerne l'authentification forte, la gestion des appareils mobiles - smartphones et tablettes - et les tests de résilience opérationnelle.

Troisièmement, la taille de l'entreprise apparaît comme un facteur corrélé à la maturité, les plus grandes structures démontrant des pratiques plus robustes.

Enfin, des faiblesses spécifiques se concentrent sur la maîtrise de l'écosystème numérique et la capacité de monitoring et de détection des menaces.

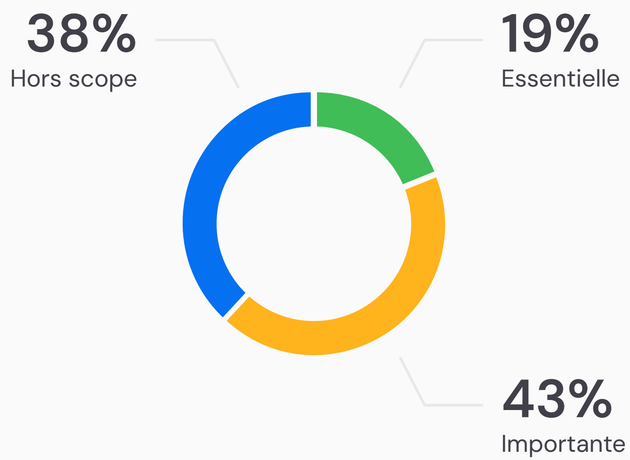
L’étude approfondit les objectifs qui nous ont paru révéler le plus d’enseignements ; n’hésitez pas à contacter CyberVadis pour échanger sur d’autres qui présentent un intérêt particulier pour vous.

Contexte de l'Étude

Le présent panorama
de la maturité en cybersécurité
des entreprises françaises
s'appuie sur l'analyse
de 1 049 évaluations réalisées
en France depuis 2023
par CyberVadis.

Les entreprises évaluées sont ainsi déjà intégrées à un dispositif de surveillance de la cybersécurité des tiers, porté par des organisations disposant d'une certaine maturité sur le sujet. Environ 62% de ces entreprises sont présumées* impactées par la directive NIS 2. L'échantillon comprenant plus de 15% des Grandes Entreprises françaises (GE), 250 Entreprises de Taille Intermédiaire (ETI) et plus de 700 Petites et Moyennes Entreprises (PME) et Très Petites Entreprises (TPE) est donc représentatif**.

Classification NIS 2 présumée des entreprises



Classification des entreprises relevant ou non du périmètre NIS 2

	# GE	# ETI	# PME	# TPE	Total
Essentielle	35	164	0	0	199
Importante	28	78	343	0	449
Hors scope	9	21	127	244	401
Total	72	263	470	244	1 049

Catégorie	Effectif
TPE	< 25 personnes
PME	25 à 300 personnes
ETI	300 à 4 999 personnes
GE	≥ 5 000 personnes

(*) Les articles 2, 3 et 4 de la directive NIS 2, et en particulier les annexes I et II, ont permis - en prenant en compte la taille des entreprises et leur secteur d'activité - de définir une catégorisation présumée en Essentielles, Importantes et Hors scope.
(**) Afin de composer avec les segmentation de CyberVadis, dans le cadre de cette étude les typologies d'entreprises sont définies comme suit:

Précision sur l'approche de l'étude en lien avec la directive NIS 2.

Pour les besoins de cette étude, la maturité des entreprises est analysée au regard des objectifs de sécurité définis par l'ANSSI, relatifs à la transposition nationale des mesures de gestion des risques cyber requises par la directive NIS 2.

Il est important de préciser que si le référentiel CyberVadis couvre une part significative de ces contrôles, il ne prétend pas à une exhaustivité parfaite du framework de l'ANSSI. L'analyse offre donc une vue très représentative de la maturité NIS 2, mais ne constitue pas un audit de conformité formel.

Enseignements clés

Les entreprises françaises soumises à la directive NIS 2 présentent aujourd'hui une maturité cybersécurité nettement supérieure à celles qui en sont dispensées — et la taille de l'entreprise reste un déterminant fort du niveau de maturité.

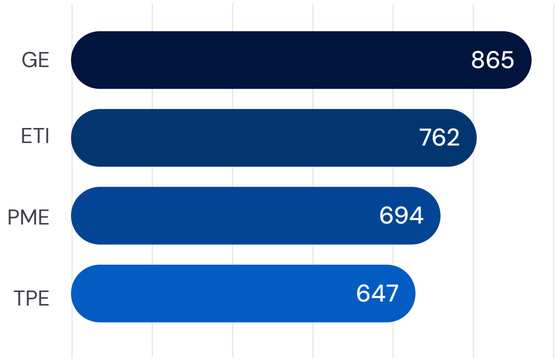
Notre analyse révèle une stratification intéressante de la maturité en cybersécurité au sein des entreprises françaises évaluées : les entités relevant du périmètre NIS2 (Essentielles et Importantes) affichent globalement une maturité supérieure par rapport à celles qui en sont exclues. Sans surprise, les entreprises Essentielles se distinguent comme les acteurs les plus performants, établissant une référence solide.

Ceci s'explique par le fait que la grande majorité d'entre elles, déjà régulées, ont initié depuis longtemps leur démarche sécurité.

Score global selon la classification NIS 2

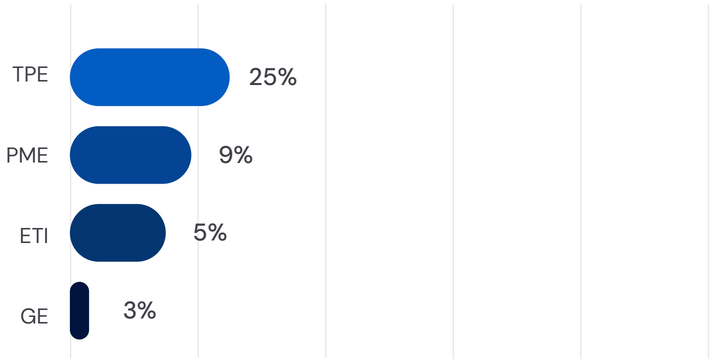
Parallèlement à cette distinction basée sur la directive NIS2, la maturité cyber est corrélée à la taille des entreprises. Les Grandes Entreprises obtiennent en moyenne un score de 865, suivies par les ETI (762), les PME (694) et les TPE (647), suggérant un lien entre les ressources et la robustesse des pratiques de cybersécurité.

Score global selon la catégorie d'entreprise



La posture cybersécurité des entreprises, entre deux évaluations (typiquement faite à 12 mois d'écart), s'est d'autant plus améliorée que leur niveau initial était faible. Ainsi les TPE, ou du moins celles d'entre elles qui ont pris conscience de leur niveau de maturité via l'évaluation initiale, progressent de 25% les PME de 19% et les ETI de 15%. Les dernières mesures plus complexes à mettre en place pour les GE déjà matures ne leur permettent pas de progresser autant (3% en moyenne).

Taux d'amélioration suite à réévaluation par catégorie d'entreprise : Entreprises françaises évaluées depuis 2023 (scores précédents vs scores actuels)



La maturité cybersécurité des entreprises françaises révèle des forces en particulier une gouvernance bien structurée, mais des faiblesses persistantes telles que la gestion des tiers, des accès distants et des configurations.

La maturité en cybersécurité des entreprises françaises varie selon les domaines. Les points forts concernent la gouvernance de la sécurité numérique et son intégration dans la gestion des ressources humaines, illustrant une attention croissante aux aspects organisationnels.

La gestion des incidents, également un point fort, témoigne d'une capacité à identifier les menaces et à y répondre. Le recensement des systèmes d'information pourtant particulièrement complexe dans les grandes organisations, révèle également une certaine maturité.

À l'inverse, des défis importants subsistent dans la maîtrise de l'écosystème numérique (partenaires, fournisseurs), la sécurisation des accès distants via appareils mobiles, et la configuration des systèmes d'information, qui restent des sources de vulnérabilité.

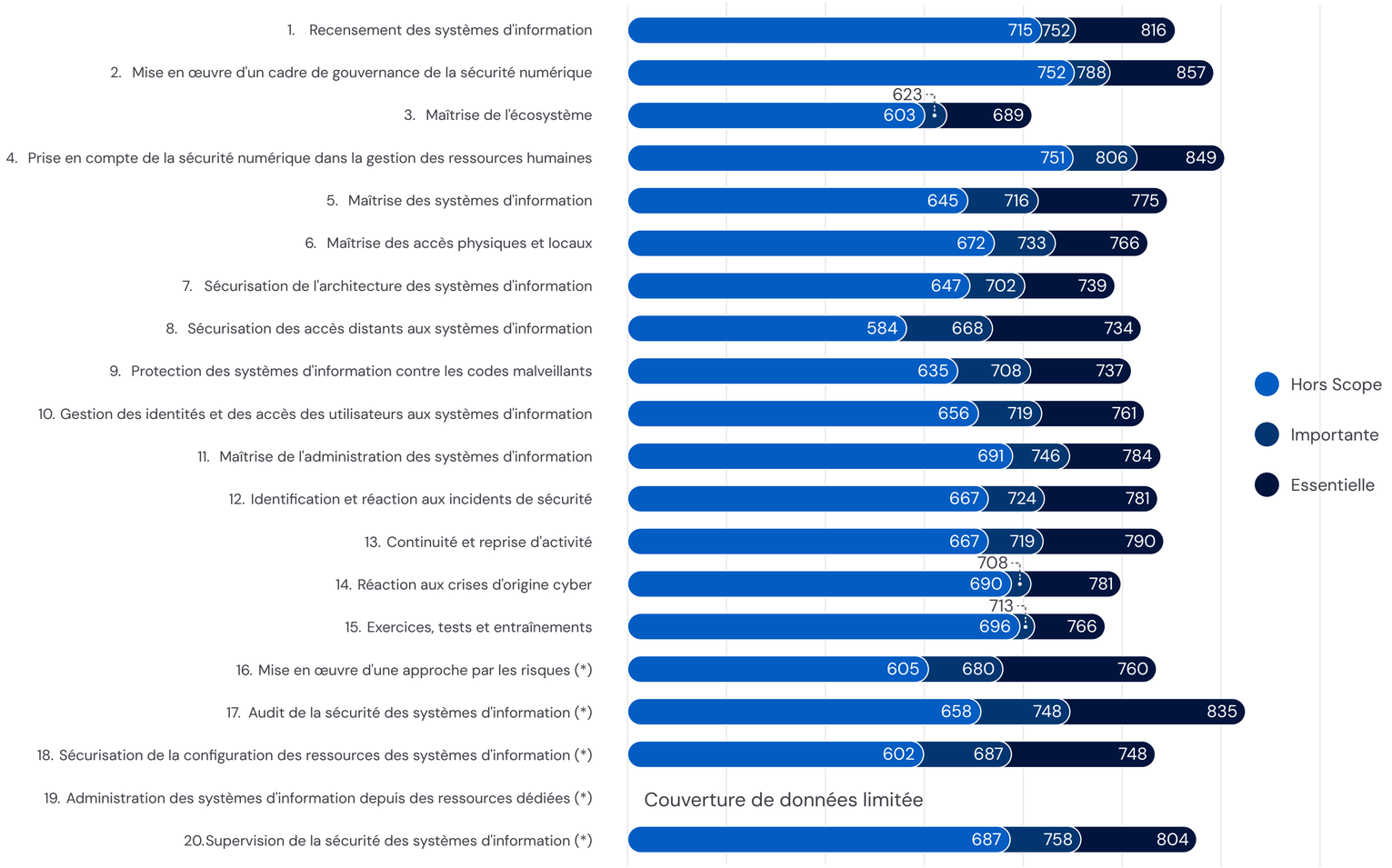
Score par objectifs de sécurité du référentiel ANSSI pour les entreprises assujetties à NIS 2

Les entreprises Essentielles affichent une avance significative sur des domaines critiques et exigés par l'ANSSI.

Dans chacun des domaines, les entreprises Essentielles sont en avance sur les entreprises Importantes, qui elles même sont en avance sur les entreprises hors du périmètre de la réglementation.

Les entreprises Essentielles sont notamment bien plus matures que les autres dans la gouvernance de la sécurité, la gestion RH et l'audit, bénéficiant de leur expérience réglementaire. Des écarts notables apparaissent aussi sur des pratiques avancées (approche par les risques, supervision, audit, sécurisation des configurations), souvent difficiles à mettre en œuvre dans les petites structures, et que l'ANSSI n'attend que des entreprises Essentielles.

Score par objectifs de sécurité du référentiel ANSSI par classification NIS 2



Gouvernance et responsabilités cybersécurité : des fondations solides pour les Essentielles, un chemin important reste à parcourir pour les autres.

La gouvernance de la sécurité de l'information est globalement mature. Une grande majorité des entreprises, y compris hors NIS 2, ont initié une démarche formelle, portée possiblement par la pression croissante des audits et questionnaires de sécurité émis par leurs clients.

Les entreprises Essentielles se distinguent par leur capacité à définir une politique de sécurité claire et à structurer les rôles et responsabilités. Ce dernier point reste toutefois moins maîtrisé pour les plus petites structures, chez qui la séparation des responsabilités est souvent lacunaire.

La gouvernance n'est plus réservée aux seuls acteurs régulés, mais il faudra désormais renforcer la qualité de sa mise en œuvre chez les entreprises hors du périmètre et dans une moindre mesure chez les entreprises "Importantes".

Gouvernance sécurité

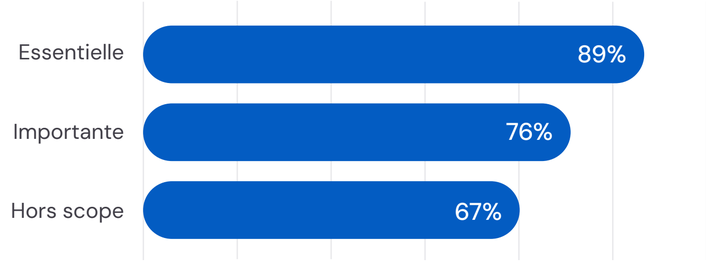
Politiques de sécurité : une formalisation maîtrisée, mais une validation managériale et diffusion aux utilisateurs encore fragmentées.

La majorité des entreprises Essentielles peuvent démontrer la formalisation, l'approbation, la révision périodique et la communication de leur politique générale de sécurité des systèmes d'information.

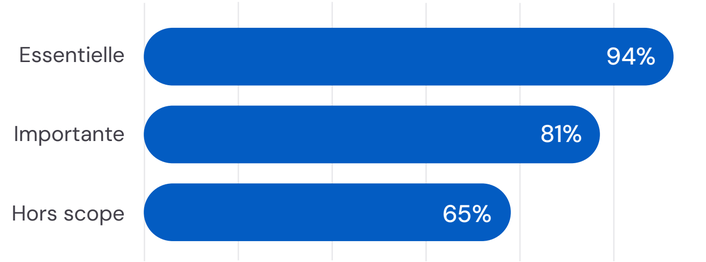
En revanche, de nombreuses entreprises Importantes et hors périmètre ont encore du mal à prouver que ce document est validé par le management et effectivement accessible à tous les utilisateurs.

Une politique de sécurité de l'information est formalisée

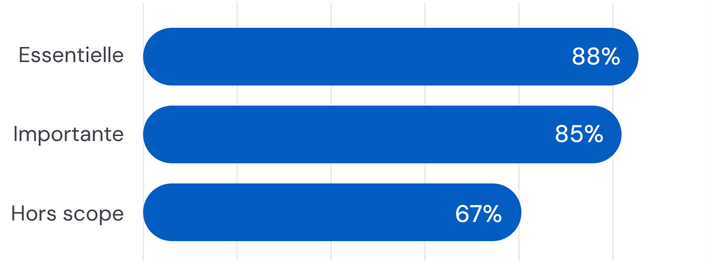
La politique est approuvée par la direction générale



La politique est révisée périodiquement

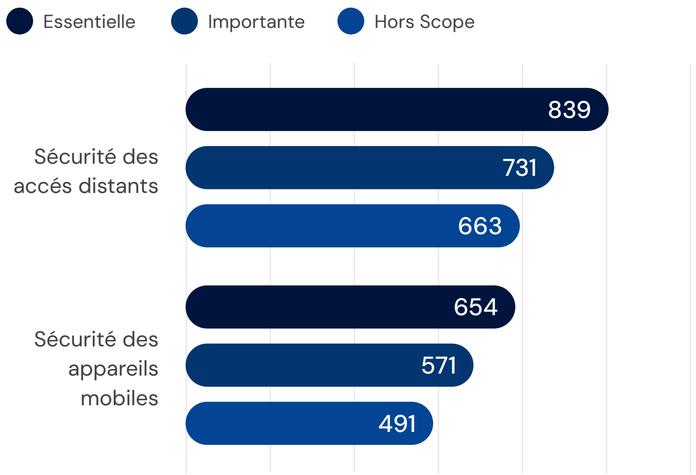


La politique est communiquée aux utilisateurs

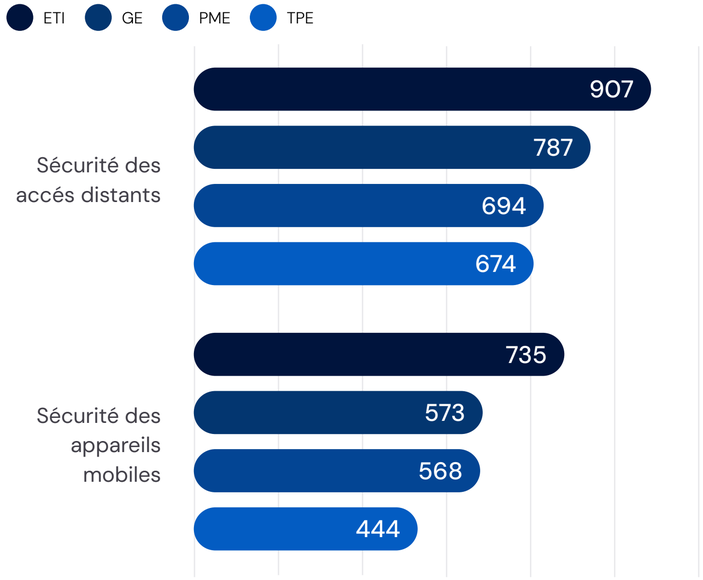


Sécurité des accès distants : une maîtrise relative mise à mal par la faiblesse de la gestion des appareils mobiles.

La sécurisation des accès à distance, dont l'importance est largement reconnue depuis la pandémie, constitue un des domaines les mieux maîtrisés. Toutefois, la gestion des appareils mobiles utilisés pour accéder aux ressources de l'entreprise est identifiée comme le maillon faible, bien qu'elle soit d'une importance primordiale car vecteur d'un volume croissant d'accès.



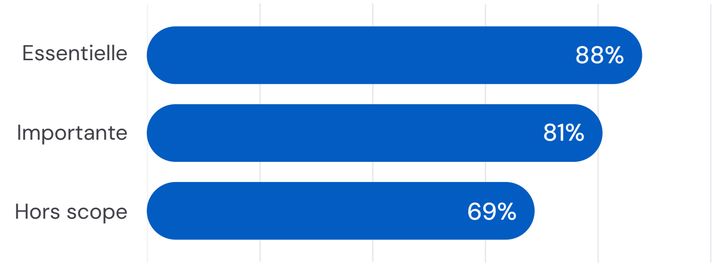
A noter qu'une analyse par taille d'entreprise révèle que cette faiblesse des entreprises Essentielles sur la sécurité des appareils mobiles est en réalité portée majoritairement par les ETI et moins par les GE qui tout en ayant de la marge de progression sont raisonnablement matures.



Accès distants : la formalisation des mesures s'affirme, un défi persistant hors NIS 2

La capacité à démontrer la formalisation des mesures de sécurisation des accès à distance varie selon la classification NIS 2. Près de 90% des entreprises essentielles sont en mesure de prouver qu'elles ont formalisé leurs processus et contrôles, ce qui atteste d'une démarche bien établie. Cette capacité diminue chez les entreprises importantes (81%) et chute pour les organisations hors du périmètre NIS2 (69%).

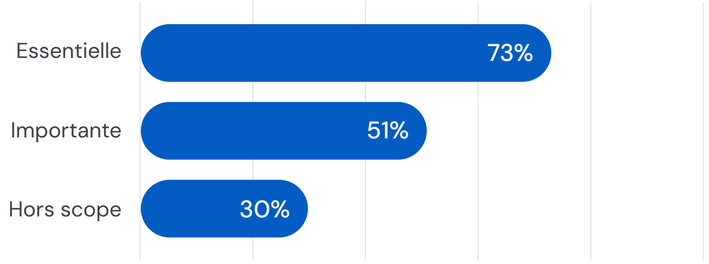
Une politique de sécurisation des accès à distance est formalisée



Authentification forte des accès distants : un impératif sécuritaire encore insuffisamment adressé.

L'adoption de méthodes d'authentification forte pour les accès à distance se révèle un véritable défi pour les organisations. Si près des trois quarts des entreprises Essentielles (73%) démontrent l'emploi de l'authentification forte, ce chiffre tombe à 51% pour les entreprises importantes et à un niveau plus faible encore pour les organisations hors du périmètre NIS2. Ce constat met en lumière un axe d'amélioration très important, avec 70% des entreprises non régulées ne pouvant prouver leur conformité.

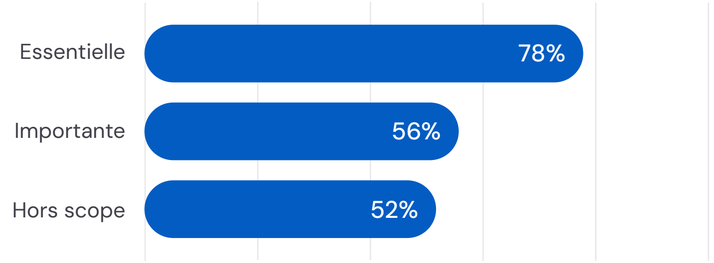
Les accès distants sont protégés par des mécanismes d'authentification forte



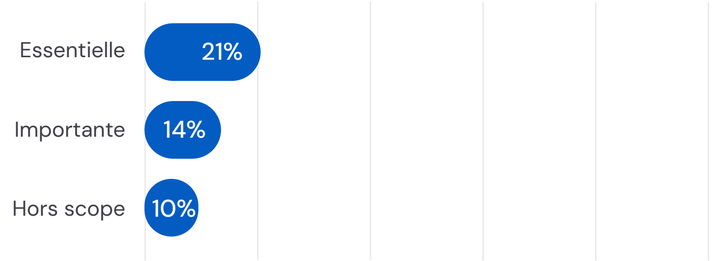
Sécurité des appareils mobiles : des politiques raisonnablement établies mais très peu d'implémentation effective.

La formalisation d'une politique de gestion de la flotte d'appareils mobiles est bien démontrée par les entreprises Essentielles (78%), mais cette capacité diminue pour les Importantes (56%) et les Hors périmètre (52%).
En revanche, la capacité à prouver l'utilisation d'authentifications fortes pour les accès aux ressources de l'entreprise via ces appareils est très limitée pour toutes les catégories (21% pour Essentielles, 14% Importantes, 10% Hors périmètre). Les politiques sont formalisées mais peu implémentées. Ce décalage s'explique en partie par des contraintes sociales, techniques et économiques : dans de nombreuses entreprises, les employés utilisent leurs téléphones personnels — seuls ou en parallèle d'un téléphone professionnel — limitant ainsi l'implémentation effective des contrôles.

Une politique de gestion des appareils mobiles est formalisée

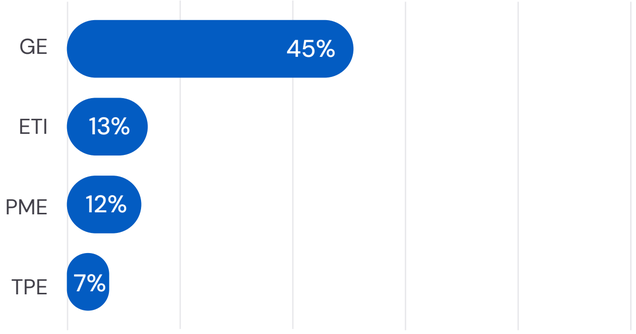


L'authentification forte pour l'accès aux ressources via les appareils mobiles est implémentée



L'analyse par taille d'entreprise montre que près de la moitié des GE peuvent démontrer l'usage de l'authentification forte pour l'accès aux ressources via les appareils mobiles.
En revanche, les ETI affichent un niveau similaire à celui des PME, bien en deçà de celui des GE.

L'authentification forte pour l'accès aux ressources via les appareils mobiles est implémentée

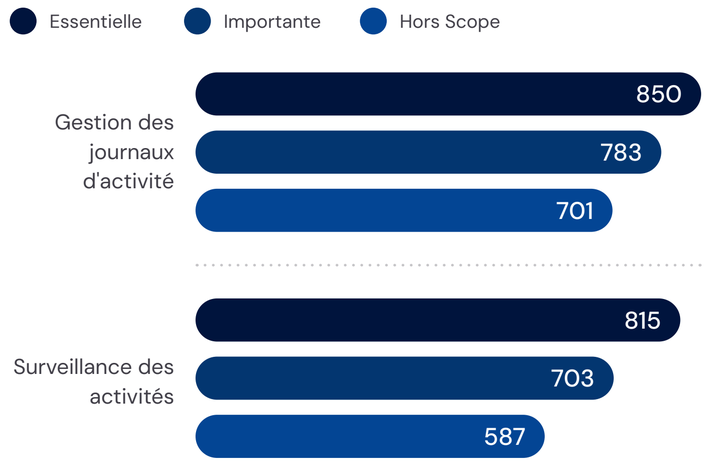


Au-delà de la sécurisation des accès, la résilience opérationnelle se révèle être un pilier majeur pour la continuité des activités des organisations.

Journalisation et monitoring : exploiter les logs, un palier difficile.

Si la journalisation des activités (logging) est globalement bien maîtrisée, son exploitation à des fins de détection reste plus limitée. En effet, passer du simple logging à un monitoring efficace, fondé sur l'analyse et la corrélation en temps réel, nécessite des outils avancés et une expertise souvent centralisée au sein d'un SOC. Un dispositif compliqué à mettre en œuvre, en particulier pour les entités hors scope, souvent plus petites, qui sont confrontées à des contraintes budgétaires, mais aussi à un déficit de sensibilisation et de compréhension des solutions existantes. Pourtant, la mise en place d'un dispositif de surveillance capable d'identifier les signaux faibles et de déclencher des alertes précoces est essentielle pour améliorer la capacité de détection et réduire les temps de réaction face aux incidents.

Détection et réponse aux événements de sécurité

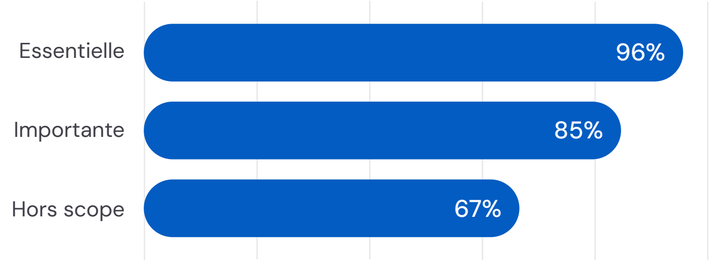


Gestion des incidents : une capacité globalement structurée.

Le processus de gestion des incidents est globalement bien établi : 96 % des entreprises Essentielles, 85 % des Importantes et 67 % des entités hors NIS 2 en démontrent l'existence, témoignant d'une capacité de réaction organisée face aux incidents.

Cependant, le niveau de maturité de ces processus reste hétérogène, allant de procédures élémentaires à des dispositifs plus avancés. La mise en œuvre régulière d'exercices permettrait de renforcer l'efficacité opérationnelle, bien que cette démarche reste difficile à déployer à grande échelle, notamment dans les grandes organisations.

Un processus de gestion des incidents est formalisé

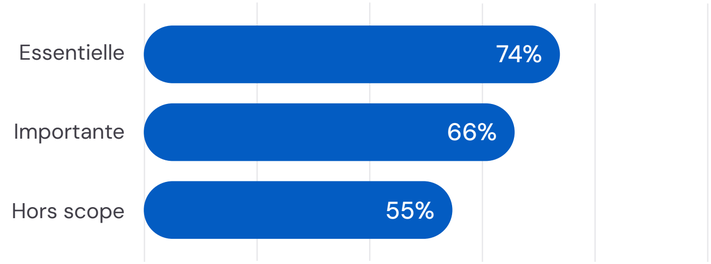


Résilience opérationnelle : un écart entre planification et exécution.

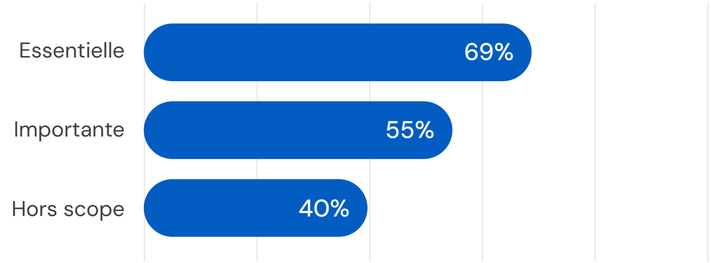
Les sauvegardes sont globalement bien mises en œuvre, avec des politiques formalisées et des processus en place dans la majorité des entreprises. Toutefois, la capacité à démontrer leur exécution régulière, ainsi que la réalisation de tests d'intégrité et de restauration, reste plus limitée, en particulier hors du périmètre NIS2.

Une politique de gestion des sauvegardes est formalisée

Des sauvegardes périodiques des données sont réalisées

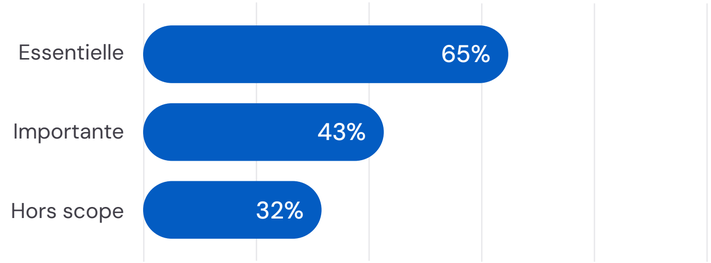


Des tests de restauration ou de vérification d'intégrité des sauvegardes sont effectués périodiquement



Les plans de continuité d'activité sont généralement documentés, en revanche leur mise à jour régulière et, surtout, la réalisation de tests concrets demeurent peu fréquentes. Les entreprises importantes et celles hors scope affichent une maturité intermédiaire. Toutefois, elles ne sont pas soumises aux exigences de continuité d'activité définies par l'ANSSI, ce qui limite l'investissement dans la mise en œuvre de pratiques plus robustes.

Un plan de continuité d'activité est formalisé et maintenu à jour



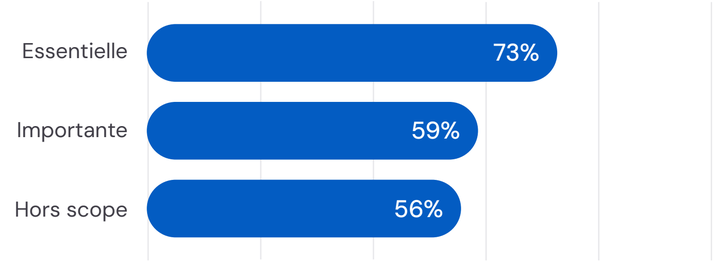
Vérification et assurance de la sécurité : l'impératif de la réalisation effective des audits.

Les entreprises Essentielles se distinguent par une bonne maîtrise des audits de sécurité : 73 % d'entre elles ont formalisé une méthodologie dédiée et 72% ont mis en œuvre, de façon régulière, des audits et des tests d'intrusion.

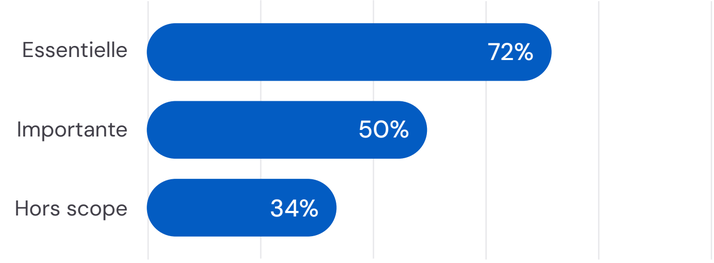
À l'inverse, les entreprises Importantes et, plus encore, celles hors scope présentent des fragilités, tant dans la structuration que dans l'exécution de ces démarches. Le déficit de mise en œuvre est particulièrement marqué pour les entités hors scope.

Pour ces dernières, le décalage entre l'intention - souvent affichée dans les plans - et la réalité opérationnelle souligne un enjeu majeur : transformer les démarches de planification en pratiques concrètes pour renforcer efficacement la posture de cybersécurité.

La méthodologie des audits de sécurité est spécifiée et documentée



Des tests d'intrusion et des audits de sécurité sont réalisés régulièrement



Pratiques de sécurité des tiers : prise de conscience certaine mais encore trop peu d'évaluations.

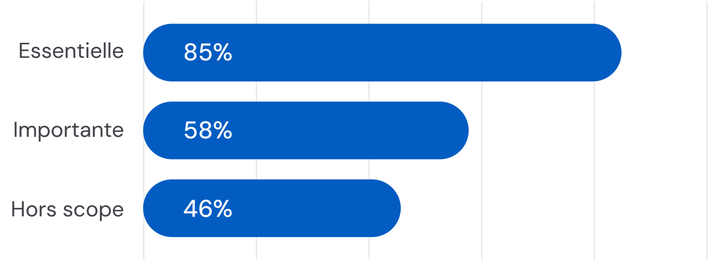
La directive NIS 2 place la sécurisation des partenaires au cœur des enjeux, mais sa mise en œuvre reste difficile pour de nombreuses entreprises françaises. Si l'insertion de clauses contractuelles est devenue courante, elle demeure largement insuffisante pour réduire de manière concrète les risques liés aux tiers. Le véritable enjeu est de dépasser le simple engagement juridique pour instaurer une évaluation active et continue des risques liés aux tiers.

- **Clauses contractuelles :**
  L'intégration d'exigences de sécurité dans les contrats est en place chez 85 % des entreprises Essentielles, chez 58 % des Importantes et 46 % des Hors scope. Cette relative maturité du processus contractuel, en particulier dans les entreprises les plus structurées, s'explique probablement par l'héritage des efforts de conformité au RGPD, qui ont déjà renforcé les pratiques de gestion contractuelle avec les tiers.

- **Politique d'évaluation des fournisseurs :**
  Leur existence est globalement homogène (67 % Essentielles et Importantes, 58 % Hors scope), ce qui traduit une volonté de structurer l'approche.

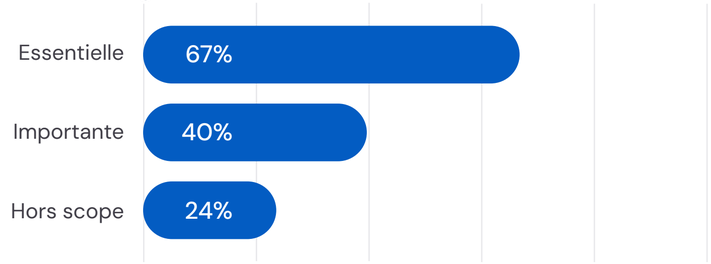
- **Evaluation des fournisseurs :**
  C'est sur la vérification effective des partenaires que le fossé se creuse : 67 % des Essentielles y parviennent, contre seulement 40 % des Importantes et 24 % des Hors scope.

Les contrats incluent des exigences en matière de sécurité



Une politique formalise l'évaluation des risques liés aux tiers

Une due diligence est mise en œuvre



À propos de CyberVadis

CyberVadis est un éditeur de solutions SaaS dédié à l'évaluation des risques de cybersécurité liés aux tiers. La mission de CyberVadis est de permettre aux entreprises de sécuriser leur écosystème en réduisant les cybermenaces de manière plus intelligente, plus rapide et plus fiable.

CyberVadis s'appuie sur une méthodologie rigoureuse validée par des analystes experts en cybersécurité et basée sur les principaux référentiels de sécurité (NIST Cybersecurity, ISO 27001 et le RGPD) pour fournir des évaluations fiables. Avec plus de 100 collaborateurs et une présence dans 9 bureaux à travers le monde, CyberVadis opère à l'échelle mondiale, évaluant des organisations dans plus de 110 pays. CyberVadis compte parmi ses clients des entreprises internationales de premier plan, des sociétés de taille intermédiaire, des petites et moyennes entreprises et de très petites entreprises.

cybervadis.com

Contact Presse :
marketing@cybervadis.com

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation et de promotion de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique, et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber, Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur. Le CESIN compte plus de 1 200 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

cesin.fr

Contact Presse :
vloquet@alx-communication.com