Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

Cybervadis dévoile le panorama de la maturité en cybersécurité des entreprises françaises

une étude exclusive de CyberVadis, réalisée en partenariat avec le CESIN

Paris, le 30 septembre 2025 -- CyberVadis publie aujourd'hui un panorama inédit de la maturité en cybersécurité des entreprises françaises, mené en partenariat avec le CESIN, club des experts de la sécurité de l'information et du numérique. Le panorama se base sur plus de 1000 évaluations, réalisées en France depuis 2023, documentées et vérifiées.

L'étude dresse un état des lieux objectif de la posture de cybersécurité des organisations (grandes entreprises, ETI, PME et TPE), et révèle que si la maturité des entreprises françaises progresse, elle reste cependant inégale. La régulation tire les grandes entreprises vers le haut, tandis que PME et TPE peinent encore à transformer leurs politiques de sécurité en pratiques concrètes.

Le score présenté dans l'étude CyberVadis est un indicateur de maturité cyber. Chaque organisation est notée de 300 à 1000 points. Un score basé sur des preuves documentaires et vérifié par des experts, qui traduit concrètement son degré de maturité cyber. Le résultat positionne ainsi chacune d'entre elles entre insuffisance (sous 400 points) et mature (au delà de 850 points).

La maturité progresse plus vite sous l'effet d'un cadre interne et/ou réglementaire

Le premier enseignement est sans appel, les organisations dites « Essentielles » présentent une maturité supérieure, avec un score moyen de 817, contre 652 pour les entreprises hors de ce périmètre. Les grandes entreprises déjà soumises à des exigences réglementaires, ou sectorielles, affichent un niveau particulièrement élevé (865/1000). Cette avance confirme le rôle structurant des cadres existants, qui tire la maturité vers le haut.

La taille, facteur clé de maturité… mais pas de progrès

La taille demeure un facteur déterminant. Sans surprise, plus les structures sont importantes, plus elles disposent de ressources pour déployer des dispositifs robustes. Les scores sont de 865 pour les grandes entreprises, 762 pour les ETI, 694 pour les PME et 647 pour les TPE. En revanche, les plus petites structures sont celles qui progressent le plus vite lorsqu'elles s'engagent. +25% pour les TPE entre deux évaluations, contre seulement +3% pour les grandes entreprises déjà matures. La dynamique est encourageante mais fragile, et vient confirmer la nécessité d'accompagner PME et ETI dans leur montée en maturité.

Un fossé entre formalisation et implémentation

Selon l'adage *« du dire au faire, au milieu il y a la mer »*, l'étude révèle un décalage majeur entre politiques de sécurité formalisées et implémentation effective. En effet, si de nombreuses organisations sont en capacité de rédiger des politiques et procédures, elles peinent encore à démontrer leur application opérationnelle. On constate par exemple que près des trois quarts (73%) des organisations essentielles font usage de l'authentification forte (MFA) pour les accès distants, et cette proportion tombe à 51% pour les entreprises importantes, et à moins de 30% pour celles hors du champ NIS 2.

Le smartphone, porte d'entrée oubliée

Si la sécurisation des accès distants est globalement bien maîtrisée, la gestion des appareils mobiles est un véritable un talon d'Achille. 78% des entreprises essentielles ont formalisé une politique de gestion des mobiles, tandis que 21% seulement démontrent l'usage d'une authentification forte sur ces appareils. Ce décalage est lié notamment à l'utilisation d'outils personnels (BYOD), qui expose les organisations à des risques accrus.

Détection et surveillance, les logs ne suffisent pas

La journalisation est largement pratiquée, mais peu d'organisations franchissent le pas du monitoring temps réel et de la corrélation d'événements, faute de moyens et d'expertise, en particulier chez les entités hors NIS 2. Or, sans détection efficace, la capacité de réaction reste limitée.

La supply chain cyber reste le maillon faible

La sécurisation des tiers apparaît comme l'un des points les plus préoccupants. 85% des entreprises essentielles insèrent des clauses contractuelles de sécurité, mais seules 24% des entreprises hors NIS 2 procèdent à une évaluation effective de leurs partenaires. Cet écart met en évidence une faille béante dans la résilience globale de l'écosystème.

Frank Van Caenegem, administrateur du CESIN et Chief Information Security Officer EMEA de Schneider Electric, précise et alerte : « *Les programmes de gestion des risques tiers sont mis en place pour accompagner les partenaires, et doivent être animés par une démarche collaborative de l'amélioration de l'écosystème. Il ne s'agit pas de noyer les fournisseurs sous des questionnaires qui ne sont qu'un reflet partiel de leur maturité et de leur résilience, au risque de les détourner d'une sécurité plus agile. L'enjeu est*

désormais que les entreprises allègent leurs demandes en fonction des statuts NIS 2 des fournisseurs. »

« *Il faut aussi préciser que l'évaluation de la maturité en cybersécurité ne doit pas s'arrêter aux fournisseurs de rang 1, c'est toute la chaîne de sous-traitance qui doit être passée au crible. »,* ajoute **Estelle Tchigique-Boyer, Group CISO de CNP Assurances.**

L'étude relève aussi des points forts, comme une gouvernance de la cybersécurité de plus en plus structurée, même hors NIS 2, l'intégration progressive de la sécurité dans les ressources humaines, ou encore des processus de gestion des incidents largement établis qui témoignent d'une capacité à identifier les menaces et à y répondre (96% des essentielles, 85% des importantes, 67% des hors scope).

Parmi les fragilités persistantes observées, l'étude pointe des plans de continuité d'activité rarement testés, des audits et tests d'intrusion réguliers encore peu répandus hors NIS 2, et aussi une difficulté des PME et ETI à sécuriser leurs configurations et à déployer une approche par les risques.

« L*es grandes entreprises affichent des pratiques robustes, mais le défi des prochaines années sera d'élever les milliers de PME et d'ETI au même niveau. C'est la condition pour que la cybersécurité progresse à l'échelle du pays* », souligne **Thibault Lapédagne, VP Research de CyberVadis.** « *Les entreprises essentielles, pour partie déjà régulées avant NIS 2, disposent d'une avance certaine. Désormais, ce sont des dizaines de milliers d'acteurs importants qui devront engager ou poursuivre une mise en conformité exigeante, et en particulier sur la gestion des tiers, point névralgique de la résilience de tout l'écosystème.* », ajoute-t-il.

Pour **Alain Bouillé, délégué général du CESIN** *« L'étude CyberVadis apporte une vision factuelle et vérifiée. Elle constitue un outil unique pour éclairer les décideurs, mettre en évidence les priorités d'action et porter un plaidoyer collectif en faveur d'un renforcement de la cybersécurité en France. »*

L'étude complète est disponible via https://bit.ly/42fsGLA

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.
www.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 rassemble plus de 1 200 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

Pour en savoir plus **www.cesin.fr**