

PÔLE D'EXCELLENCE CYBER

Observatoire de la performance cybersécurité du secteur spatial

Novembre 2026

Région Bretagne

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Edito



Antoine Hautin
Vice-Président du Pôle d'Excellence Cyber

Faire de la cyber résilience spatiale une ambition collective.

Le spatial est devenu l'un des piliers de notre autonomie stratégique. Communications, navigation, observation de la Terre : nos sociétés, nos économies et nos capacités de défense dépendent chaque jour davantage des infrastructures spatiales. Dans un contexte de tensions géopolitiques accrues, leur caractère dual, à la fois civil et militaire, en fait des actifs stratégiques autant que des cibles potentielles.

L'essor du New Space, la multiplication des acteurs et l'interconnexion croissante des systèmes élargissent la surface d'attaque. Face à des menaces qui dépassent les frontières et les périmètres industriels, l'enjeu n'est plus seulement de protéger chaque infrastructure, mais de garantir la sécurité et la résilience de l'ensemble des services spatiaux essentiels.

Cette ambition exige de décloisonner les expertises et de fédérer les énergies. C'est la conviction qui a présidé à la création, avec IRISPACE, du groupe de travail « Cyberdéfense du domaine spatial » du Pôle d'Excellence Cyber. En rapprochant les communautés spatiale et cyber, nous souhaitons structurer une dynamique durable de partage des connaissances, d'expérimentation et de recommandations opérationnelles.

Cet observatoire en constitue une première traduction concrète. En apportant un éclairage objectif sur l'exposition numérique de 170 entreprises du secteur, il établit un premier état de référence pour identifier les fragilités, orienter les priorités et mesurer les progrès.

Notre ambition est claire : transformer cette connaissance partagée en actions concrètes, pour renforcer durablement la cyber-résilience et la souveraineté spatiale française et européenne.

Mesurer la maturité cyber pour éclairer les décisions stratégiques.

Satellites, infrastructures au sol et chaînes d'approvisionnement forment un écosystème complexe, dont la sécurité conditionne la continuité de services critiques, civils comme militaires.

Face à l'évolution des menaces, la connaissance objective du niveau de maturité cyber des organisations constitue un préalable indispensable à toute stratégie de renforcement de la résilience. C'est dans cette perspective que Board of Cyber a contribué aux travaux du groupe « Cyberdéfense du domaine spatial », en apportant une lecture structurée des pratiques de cybersécurité des organisations participantes.

Cet observatoire permet d'identifier des tendances, de mettre en perspective les niveaux de maturité et de faire émerger des priorités d'action. Car renforcer la cybersécurité spatiale suppose d'abord de savoir où se situent les risques, de mesurer les progrès accomplis et de concentrer les efforts là où ils produiront le plus d'impact.



Sylvain Lefeuvre
Directeur de Board of Cyber



Introduction

Dans un contexte de tensions géopolitiques croissantes et de dépendance accrue aux capacités spatiales, la cybersécurité des infrastructures orbitales et terrestres constitue un enjeu stratégique de souveraineté, de résilience et de continuité des services. La diversité des acteurs, l'interconnexion des systèmes et les spécificités technologiques du secteur appellent une approche collective, capable de rapprocher les expertises spatiales et cyber.

C'est dans cette perspective que le Pôle d'excellence cyber (PEC) et IRISPACE ont annoncé, en mars 2026, la création du **groupe de travail « Cyberdéfense du domaine spatial ».** Copilotée par Nicolas Bellec, coordinateur d'IRISPACE, et Antoine Hautin, Vice-Président du PEC et Secrétaire Général & VP Défense d'Almond, cette initiative fédère des acteurs industriels, académiques et institutionnels autour de trois ambitions : **structurer une communauté pluridisciplinaire, formuler des recommandations opérationnelles et développer des outils d'expérimentation en cybersécurité spatiale.**

Le présent observatoire s'inscrit dans cette dynamique. Construit à partir des évaluations réalisées avec **Security Rating® de Board of Cyber** sur le panel étudié dans le cadre du groupe de travail, il analyse la performance cybersécurité observable depuis Internet des organisations étudiées et met en évidence leurs principales expositions ainsi que les priorités d'amélioration.

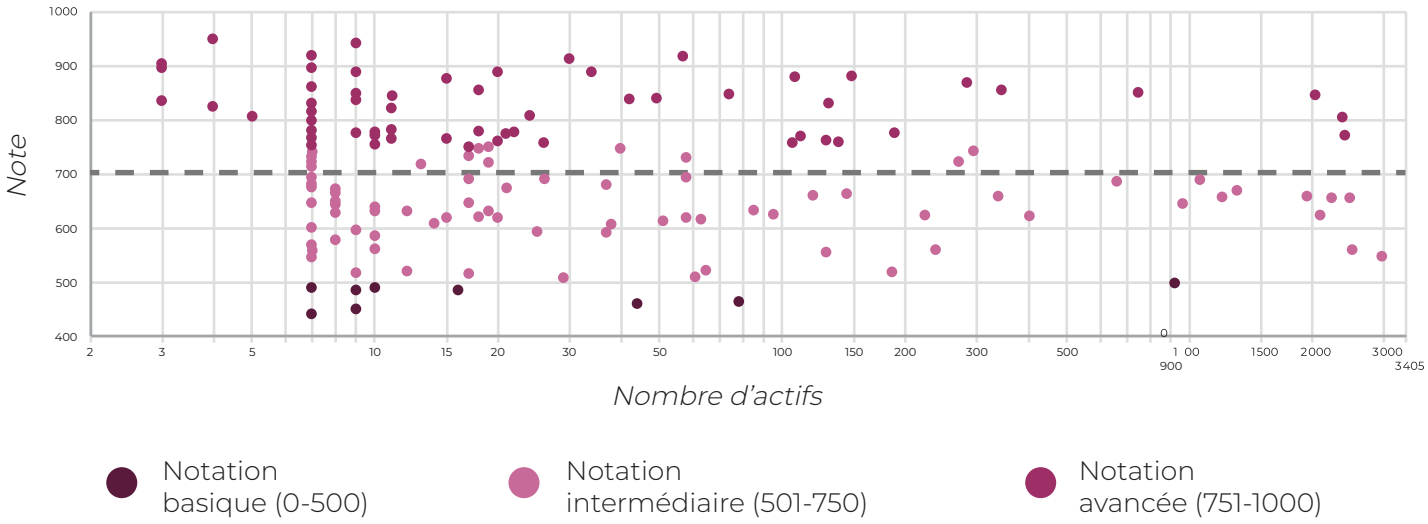
À travers les résultats présentés, cet observatoire vise à **identifier les tendances, les disparités et les axes de progression** au sein du panel étudié. Il constitue une première base d'analyse pour alimenter les réflexions du groupe de travail, orienter ses travaux et contribuer à l'élévation collective du niveau de cybersécurité de la filière spatiale.

Note de rédaction : les résultats décrivent l'exposition numérique visible depuis Internet. Ils ne constituent pas un audit des systèmes internes, des satellites ou de l'ensemble des infrastructures spatiales, ni une mesure représentative de toute la filière.

Présentation du panel étudié

Le panel réunit des sociétés dont les empreintes numériques diffèrent fortement. Ce premier graphique permet de situer cette diversité en matérialisant les 170 sociétés selon leur nombre d'actifs et leur note cyber.

Chaque point représente une société. Sa position horizontale indique le nombre d'actifs observés depuis Internet ; sa position verticale correspond à sa note de cybersécurité. Plus le point est haut, meilleure est la note.



La dispersion des points invite à examiner les constats à l'échelle de chaque société. Le nombre d'actifs renseigne sur le périmètre observé et sur le volume potentiel de travail. Les priorités de correction dépendent ensuite de la nature et de la gravité des problèmes relevés.

Méthodologie d'analyse

Security Rating® analyse l'ensemble des vecteurs d'exposition externe d'une organisation, articulés en deux grandes catégories :

Mesures de contrôle : ce qui est exposé et comment c'est protégé
- **Surface d'attaque** : cartographie des actifs exposés sur Internet (sous-domaines, ports ouverts, services accessibles)
- **Messagerie** : configuration des enregistrements SPF, DKIM, DMARC et exposition des serveurs de messagerie
- **Web TLS/SSL** : qualité et validité des certificats, protocoles supportés, configurations à risque
- **Contrôle de sécurité** : présence et configuration des mécanismes de protection essentiels

Mesures de performance : comment l'organisation réagit aux menaces
- **Vulnérabilités** : CVE connues détectées sur les actifs exposés, avec niveau de sévérité
- **Performances de mise à jour** : cadence de patching sur chaque niveau de criticité (ex : < 5 jours pour les failles critiques)
- **Indicateurs CTI** (Cyber Threat Intelligence) : présence dans des blacklists, IP ou domaines compromis détectés, fuites de données ou d'identifiants liés à l'organisation

Des profils contrastés selon les axes d'évaluation

Avec une note moyenne de 705 sur 1 000, le panel compte 161 sociétés de maturité intermédiaire ou avancée, contre 9 de maturité basique. Ces résultats constituent une base encourageante pour engager des améliorations ciblées, dont la rapidité de mise en œuvre dépendra des problèmes identifiés.

SOCIÉTÉS ÉVALUÉES
170

MOYENNE DES NOTES
705/1000

MATURITÉ

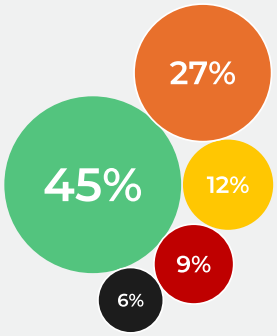


Basique : 9
Intermédiaire : 98
Avancé : 63

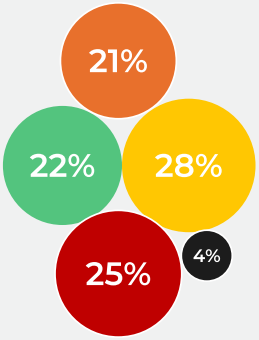
La note globale résume des résultats qui peuvent varier sensiblement d'un domaine technique à l'autre. Leur lecture détaillée permet de préciser les priorités. La prédominance des maturités intermédiaire et avancée doit ainsi être rapprochée des résultats par axe. Elle ne permet pas de déduire, à elle seule, l'effort ou le délai nécessaire aux corrections.

Chaque encart présente la répartition des sociétés entre les classes A à E pour un domaine évalué. Les pourcentages inscrits dans les bulles indiquent la part du panel dans chaque classe. A correspond aux 10 % les mieux classés dans le référentiel global de Board of Cyber, tandis que E correspond aux 10 % les moins bien classés. Une même société peut obtenir des classements différents selon les domaines.

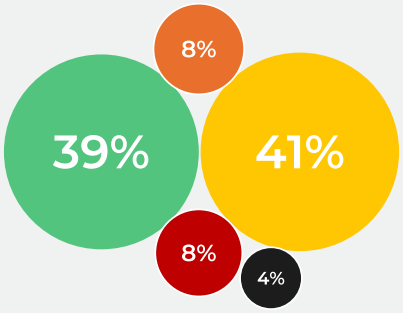
SURFACE D'ATTAQUE



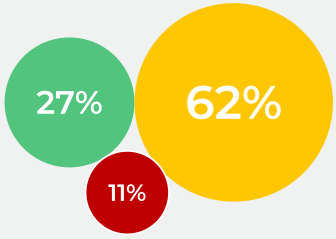
MESSAGERIE



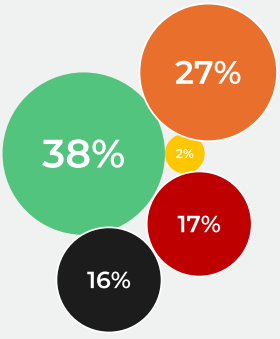
WEB TLS/SSL



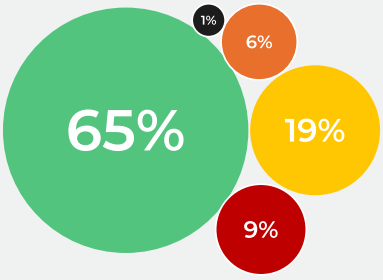
CONTRÔLE DE SÉCURITÉ



VULNÉRABILITÉS



PERFORMANCE DE MISE À JOUR



A B C D E

Une moyenne proche du référentiel global tous secteurs confondus

La comparaison au référentiel global - c'est à dire à la moyenne des sociétés évaluées tous secteurs confondus - permet de situer le panel et de distinguer les domaines sur lesquels les écarts sont les plus marqués.

MOYENNES DES NOTES

705 Panel GT Cyber spatial

725 Panel Global

-20 pts | -2,8%

MÉDIANE DES NOTES

708,5 Panel GT Cyber spatial

735 Panel Global

-26,5 pts | -3,6%

DISPERSION DES NOTES

393 à 950

Panel GT Cyber spatial
Ecart-type : 117 pts
Moitié centrale : 625 à 778

Par axe d'analse, écart en points entre le Panel étudié par le GT Cyber spatial et le Global évalué par Board of Cyber.

Surface d'attaque	Contrôle de sécurité	Messagerie	Web TLS/SSL	Vulnérabilités	Performances de mise à jour
-29 pts	**-34 pts**	**-47 pts**	**-7 pts**	**-67 pts**	**+148 pts**
Global : 847 Panel GT : 818	Global : 581 Panel GT : 547	Global : 751 Panel GT : 704	Global : 795 Panel GT : 788	Global : 714 Panel GT : 647	Global : 710 Panel GT : 858

Mesures de contrôle
Ecart moyen : -29,3 pts

Mesures de performance
Ecart moyen : +40,5 pts

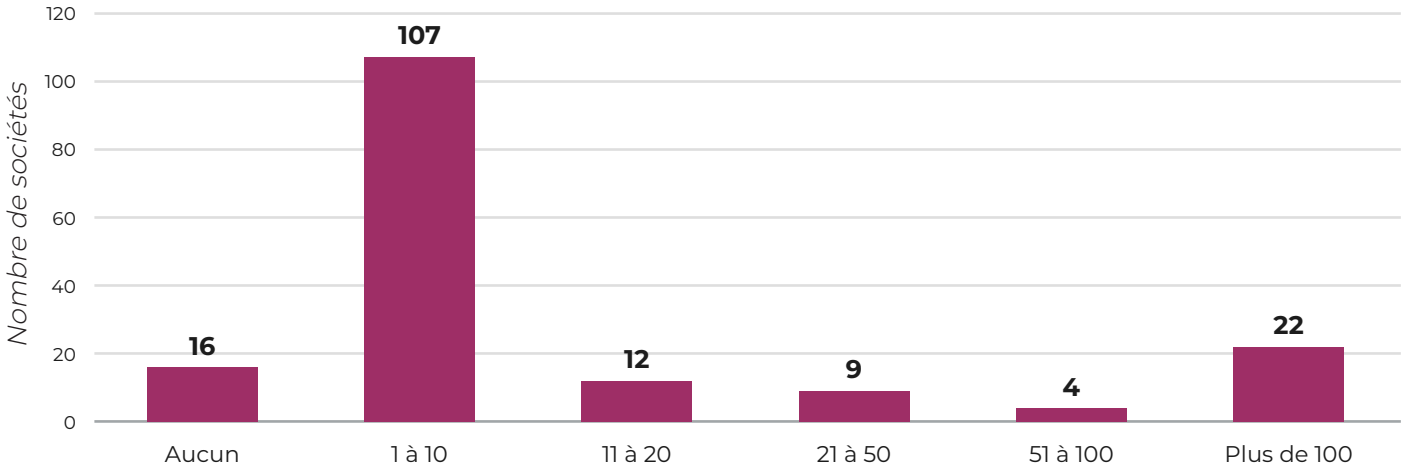
La moyenne du panel se situe 20 points sous celle du référentiel global. Cet écart masque toutefois une dispersion importante : les notes s'échelonnent de 393 à 950. Le résultat collectif recouvre donc des situations et des besoins de correction très différents.

Les écarts les plus défavorables concernent les vulnérabilités et la messagerie, tandis que la performance de mise à jour dépasse nettement le référentiel. Ce contraste invite à examiner les technologies et les configurations concernées : un bon résultat sur un axe peut coexister avec des fragilités sur un autre.

Une maturité encourageante et des corrections encore nécessaires

La présence de problèmes élevés ou critiques dans 91 % des entreprises montre que la note globale doit être complétée par une lecture des expositions concrètes. Ici, chaque société apparaît dans une seule tranche, selon le nombre de problèmes de sévérité élevée ou critique détectés. Le graphique renseigne sur le volume des constats, mais ne permet pas, à lui seul, d'en déduire la gravité précise ou la difficulté de correction.

Nombre de sociétés selon leur nombre de problèmes de sévérité élevée ou critique



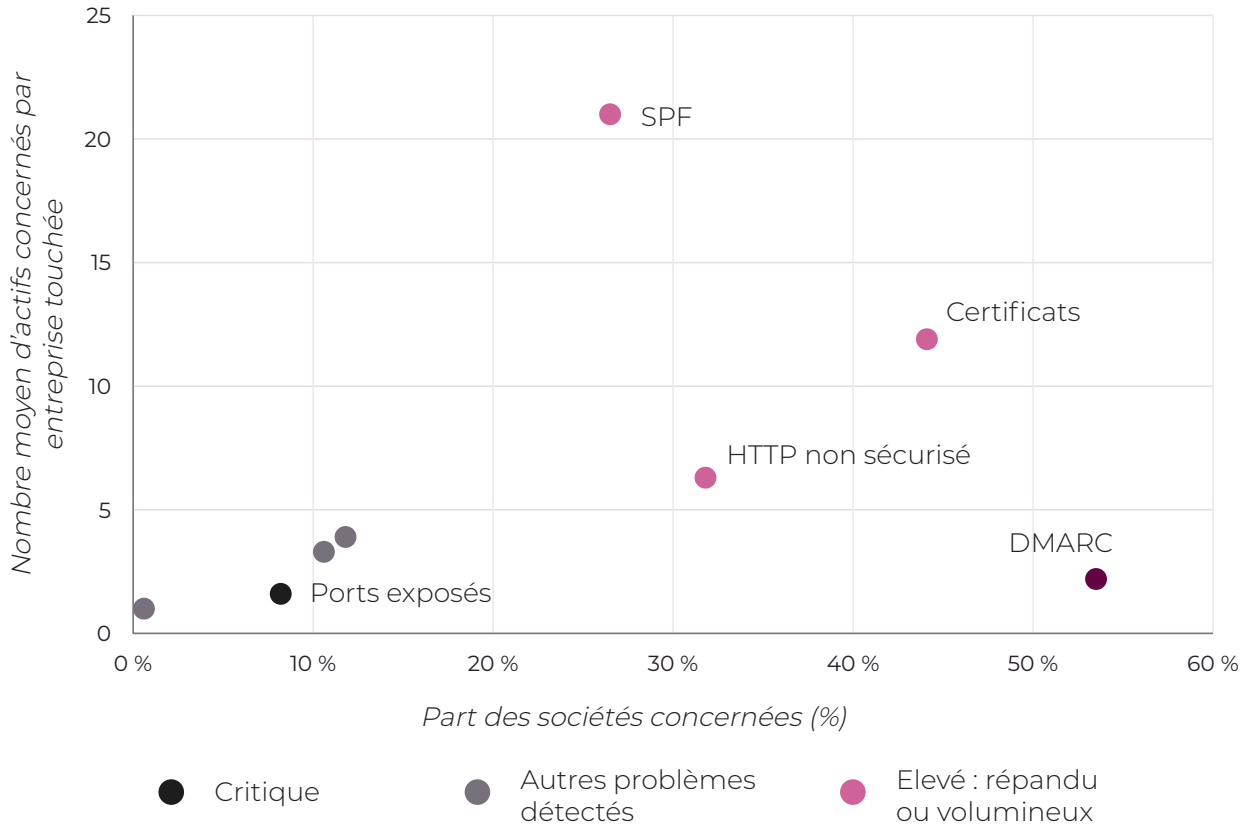
La majorité du panel présente entre un et dix problèmes de ces niveaux de sévérité. À l'autre extrémité, 22 entreprises dépassent cent constats. Ces situations appellent des réponses différentes : des corrections ciblées pour les unes, une organisation du traitement à plus grande échelle pour les autres.

Le nombre de constats ne suffit cependant pas à déterminer l'urgence. Un seul service critique exposé peut justifier une intervention prioritaire. À l'inverse, un volume élevé peut résulter d'une même configuration reproduite sur plusieurs actifs.

La progression devra donc être appréciée à travers la réduction des problèmes les plus graves, leur résorption dans chaque entreprise et leur éventuelle réapparition. Les 16 entreprises sans problème de ces niveaux constituent un repère à la date de mesure, dans le périmètre observé.

Adapter les priorités à la gravité et à l'étendue des problèmes

Problèmes élevés et critiques : part des sociétés touchées et actifs concernés par société touchée



● CRITIQUE

Ports exposés : 14 sociétés, 23 actifs.

La correction est une priorité.

● LE PLUS RÉPANDU

Défauts de configuration de messagerie DMARC : 54% des sociétés.

● VOLUMINEUX

SPF (943 actifs) pour 26% des sociétés

Certificats (889 actifs) pour 44% des sociétés

Comprendre les problèmes détectés :

- **Ports exposés** : points d'accès à des services informatiques accessibles depuis Internet. Certains sont nécessaires au fonctionnement des systèmes, mais une exposition mal maîtrisée peut faciliter une attaque.
- **DMARC** : mécanisme de protection des domaines contre leur usurpation dans les e-mails. Une configuration insuffisante peut faciliter certaines tentatives d'hameçonnage.
- **SPF** : mécanisme permettant d'identifier les serveurs autorisés à envoyer des e-mails pour un domaine. Une mauvaise configuration fragilise l'authentification des messages.
- **Certificats numérique** : éléments utilisés notamment pour authentifier les services et sécuriser les échanges. Des certificats expirés, invalides ou mal configurés peuvent compromettre la confiance ou la sécurité des connexions.
- **HTTP non sécurisé** : ommunications web dépourvues de la protection apportée par HTTPS, susceptibles d'exposer les données échangées à l'interception ou à la modification.

Ce graphique permet de distinguer trois dimensions complémentaires : la gravité des problèmes détectés, leur diffusion au sein du secteur et leur concentration sur les actifs numériques des entreprises concernées.

Chaque point représente une catégorie de problème. Plus il se situe à droite, plus le problème touche une part importante des entreprises du panel. Plus il est haut, plus le nombre moyen d'actifs numériques concernés par entreprise touchée est élevé. La couleur apporte une indication complémentaire sur la criticité ou la nature des problèmes identifiés.

Des expositions critiques qui nécessitent une intervention ciblée. Les ports exposés classés critiques concernent 14 entreprises et 23 actifs. Il s'agit de services accessibles depuis Internet présentant une exposition jugée particulièrement sensible. Bien que peu répandus à l'échelle du panel, ces problèmes appellent une qualification et, lorsque le risque est confirmé, une correction prioritaire.

Des faiblesses de configuration largement partagées. Les défauts de configuration DMARC concernent 54 % des entreprises. Ce mécanisme de sécurité de la messagerie contribue à protéger les noms de domaine contre leur usurpation lors de l'envoi d'e-mails frauduleux. Sa mauvaise configuration constitue ainsi un enjeu transversal, sur lequel des recommandations communes et le partage de bonnes pratiques pourraient produire des bénéfices à l'échelle du secteur.

Des problèmes qui affectent un grand nombre d'actifs au sein des organisations. Les anomalies SPF et de certificats se distinguent par leur volume : respectivement 943 et 889 actifs concernés. SPF participe à l'authentification des serveurs autorisés à envoyer des e-mails pour un domaine, tandis que les certificats numériques jouent notamment un rôle dans l'authentification et la sécurisation des communications. La multiplication des anomalies sur ces éléments peut révéler des difficultés de configuration, de gestion ou de maintien en condition de sécurité d'un patrimoine numérique étendu.

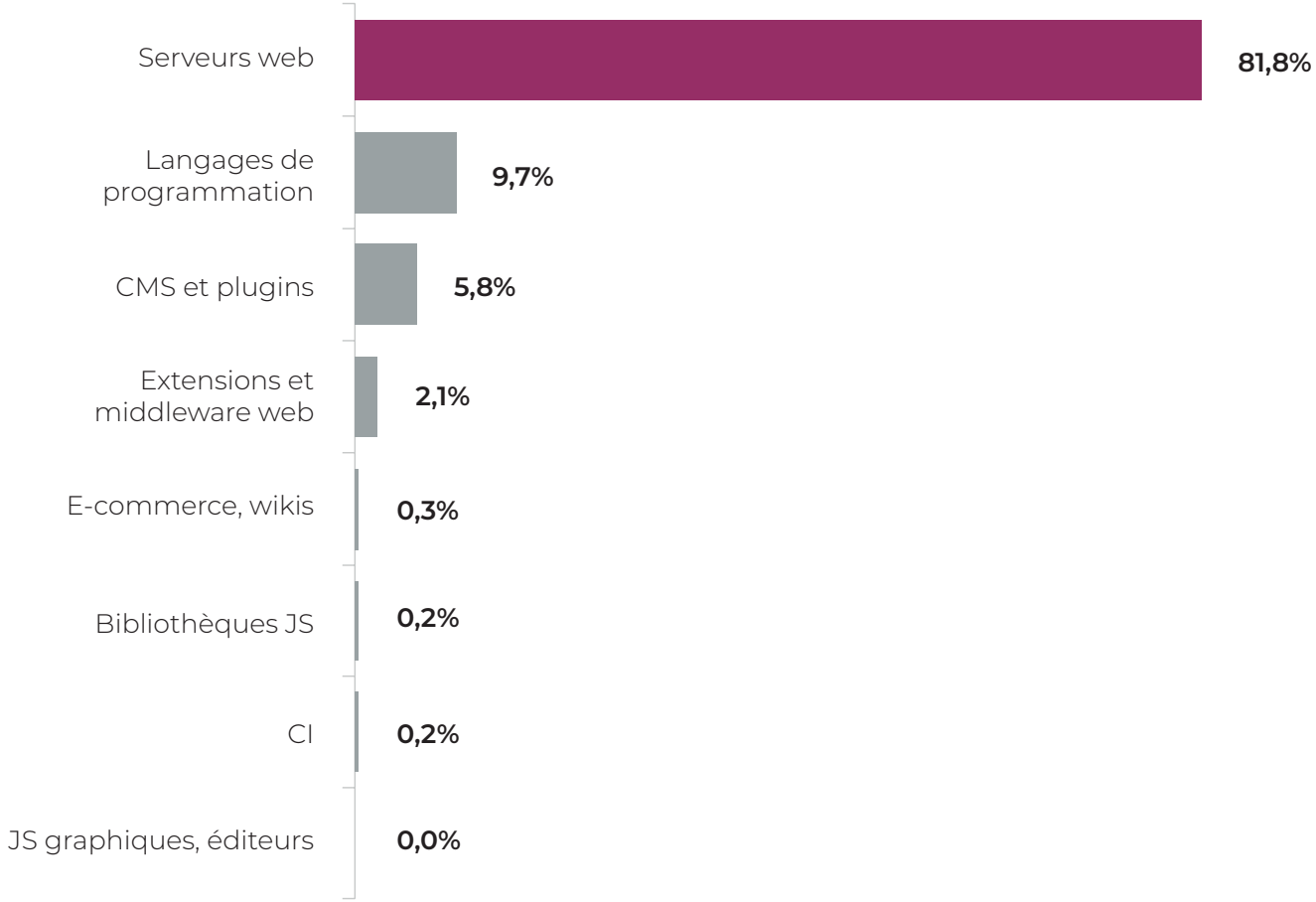
Ces constats invitent à différencier les réponses : intervention ciblée sur les expositions critiques, recommandations communes face aux faiblesses largement répandues, et actions coordonnées de remédiation lorsque de nombreux actifs sont concernés.

Au-delà des vulnérabilités individuelles, cette lecture met en évidence l'intérêt d'une démarche collective de surveillance et d'amélioration continue de la sécurité numérique du secteur spatial.

Concentrer les premières revues sur les serveurs web

Les serveurs web représentent 81,8 % des vulnérabilités potentielles critiques recensées. Cette concentration désigne un premier périmètre de vérification technique.

Part de chaque catégorie dans les 12 967 vulnérabilités potentielles critiques (%)



SERVEURS WEB

82%

des vulnérabilités critiques (10 601 sur 12 967), présente chez 42 % des sociétés du panel du GT.

AUTRES VULNÉRABILITÉS

Bibliothèques JS : 41 % des sociétés mais 30 problèmes critiques seulement (0,2 %).

Langages et CMS : 46 % et 37 % de leurs vulnérabilités sont critiques.

La revue des versions détectées et des correctifs effectivement appliqués doit permettre de confirmer les vulnérabilités pertinentes pour chaque environnement. Cette qualification est nécessaire avant d'organiser les mises à jour et de fixer les priorités de traitement.

Les autres catégories pèsent moins dans le total, mais peuvent concerner des services essentiels pour une entreprise. Leur priorité doit également tenir compte de l'exposition et de l'usage des actifs.

Organiser les corrections et vérifier leurs effets

01. SOUS 72H

Fermer les expositions critiques.

Ports exposés, LDAP anonyme, interface d'admin

Fermer, filtrer ou placer derrière un pare-feu. Si exposé depuis longtemps, renouveler les identifiants et examiner les journaux.

02. SOUS 30 JOURS

Messagerie, certificats et HTTP.

Configurer DMARC et SPF ou supprimer les enregistrement MX.

Renouveler ou corriger les certificats, supprimer l'utilisation de HTTP non sécurisé.

03. SOUS 90 JOURS

Mettre à jour les technologies utilisées.

Serveurs web, langages et CMS

Commencer par les serveurs web, qui portent 82 % des vulnérabilités critiques.

04. EN CONTINU

Surveiller et vérifier.

Noter régulièrement la maturité externe pour suivre la montée en maturité des sociétés du GT Cyber Spacial.

Les échéances donnent un cadre de mobilisation aux équipes. Pour chaque constat, le pilotage doit préciser l'actif concerné, le responsable du traitement et la preuve attendue pour vérifier la correction. Cette organisation permet de suivre l'avancement et de rendre visibles les difficultés qui nécessitent un arbitrage.

Le calendrier reste à adapter à la gravité des problèmes et aux contraintes d'exploitation. Une situation critique confirmée doit être prise en charge sans attendre l'échéance générale de sa catégorie.

Le suivi des corrections alimentera les prochaines évaluations. Il permettra de rapprocher les actions engagées des changements observés et d'identifier les problèmes persistants ou récurrents.

Focus : traiter une exposition critique

Exposition (exemples courants)	Risque	Remédiation
Accès distants : RDP, SMB, Telnet, VNC	Prise de contrôle à distance, rebond vers le SI, point d'entrée des ransomwares	Fermer au pare-feu, accès via VPN ou ZTNA, MFA
Bases de données : MySQL, PostgreSQL, MongoDB, Redis, Elasticsearch	Lecture ou vol de données, parfois sans authentification	Filtrer par IP, écoute sur le réseau interne, activer l'authentification
Interfaces d'administration : API Docker, Kubernetes, panneaux d'admin CMS	Prise de contrôle de l'hôte ou du cluster	Retirer d'Internet, liste d'IP autorisées, bastion
SSH ouvert à tous avec mot de passe	Attaque par force brute	Clés uniquement, restriction d'IP, bastion
Serveur LDAP accessible anonymement	Énumération des utilisateurs et des groupes, base pour du phishing	Désactiver le bind anonyme, restreindre l'accès réseau

Le tableau présente des exemples de situations et de mesures possibles. Leur application dépend du service, de son usage et des exigences de continuité. Chaque entreprise doit confirmer le constat et identifier le responsable capable de mettre en œuvre la mesure adaptée.

Le traitement est achevé lorsque la réduction de l'exposition est vérifiée. La conservation d'une trace du constat initial, de la modification et du contrôle réalisé permet d'en rendre compte et d'éviter qu'une même situation ne se reproduise.

Le suivi collectif pourra ainsi porter sur le nombre d'expositions critiques restantes et sur les délais de traitement. L'objectif présenté dans le support est leur résorption sous 30 jours, avec une première prise en charge rapide.

Les premières corrections doivent se prolonger dans les pratiques de gestion : tenir l'inventaire à jour, attribuer les responsabilités et contrôler régulièrement les configurations. Leur efficacité se mesure aussi à la capacité de prévenir la réapparition des problèmes.

Une démarche collective au service de la filière spatiale

Cet observatoire s'inscrit dans les travaux du GT Cyber spatial du Pôle d'Excellence Cyber et d'IRISPACE, copiloté par Nicolas Bellec, Coordinateur d'IRISPACE, et Antoine Hautin, Secrétaire Général & VP Défense d'Almond et vice-président du Pôle d'Excellence Cyber. Construit à partir des évaluations réalisées avec Security Rating® de Board of Cyber, il apporte un état de référence pour orienter les actions et suivre la progression du panel dans le temps.

Crédits

Cadre des travaux : Pôle d'Excellence Cyber et IRISPACE
Copilotage : Nicolas Bellec et Antoine Hautin
Évaluation et données : Hawa Diallo et Luc Delpha, Board of Cyber — Security Rating®
Conception graphique et mise en page : Manon Bliguet
Données arrêtées au 6 octobre 2026 · Édition octobre 2026

Droits et reproduction

© 2026 — Pôle d'Excellence Cyber. Les textes, données, illustrations, marques et logotypes restent soumis aux droits de leurs titulaires respectifs. Toute citation doit mentionner le titre de l'observatoire, son édition et la source des données : Board of Cyber — Security Rating®.

PÔLE D'EXCELLENCE
CYBER