Communiqué de presse

AL'X COMMUNICATION - Véronique Loquet
+33 668 427 968 vloquet@alx-communication.com

Étude VOC : seulement 7,6 % des entreprises corrigent les vulnérabilités critiques en moins de 24 heures

I-TRACING, 1er pure player européen de la cybersécurité accompagnant plus de 600 entreprises dans la gestion des risques cyber à travers le monde, et le CESIN, Club des Experts de la Sécurité de l'Information et du Numérique, publient aujourd'hui les résultats de leur étude sur la gestion des Vulnerability Operations Centers (VOC).

Les VOC permettent de structurer la détection des vulnérabilités selon une approche proactive, en associant outils, processus et expertise humaine, dans le but de mieux appréhender le risque, d'optimiser la priorisation et le traitement des failles.
Menée auprès de plus de 250 RSSI membres du CESIN, cette enquête révèle des lacunes persistantes dans la gestion des vulnérabilités, malgré un contexte marqué par l'élargissement de la surface d'exposition et l'intensification de la menace.

L'étude met en lumière un décalage structurel. Car si les organisations disposent de plus en plus de capacités de détection et de priorisation, elles peinent encore à aligner leurs capacités opérationnelles avec le rythme réel d'exploitation des vulnérabilités par les attaquants.

L'intégralité des résultats de cette étude, basée sur un sondage de 21 questions, sont détaillés dans le Livre Blanc « Gestion des vulnérabilités : Comment réduire votre exposition aux cyberattaques ? », dévoilés à l'occasion du Forum InCyber Europe le 1 avril 2026. Il vise à identifier les stratégies mises en place par les RSSI, à quantifier leurs préoccupations et les défis rencontrés, ainsi qu'à proposer des solutions concrètes pour optimiser la cybersécurité des entreprises.

Des équipes cybersécurité en surrégime

Le premier constat de l'étude porte sur la charge de travail des équipes cybersécurité : 56 % des répondants estiment manquer de personnel qualifié pour faire face à la masse de

vulnérabilités, dont 51 % sont jugées trop critiques pour être ignorées. Alors que 80 % des attaques exploitent des vulnérabilités traditionnelles, on remarque que les services peinent davantage à gérer les vulnérabilités dites “Shift-left” (conteneurs, code, dépendances logicielles). Ainsi, seuls 56 % des failles liées aux conteneurs, 57 % des failles dans le code et 48 % des failles de dépendances logicielles sont traitées. Sous cette charge de travail croissante, les VOC rencontrent encore des difficultés à intégrer pleinement les pratiques DevSecOps dans leurs programmes.

Cette situation traduit une tension croissante entre l'augmentation continue de la surface d’attaque, et la capacité réelle des équipes à absorber la remédiation dans des délais compatibles avec la menace.

« La pénurie de ressources humaines et l’augmentation des cyberattaques obligent les entreprises à repenser leur approche. Il ne s’agit plus seulement de prioriser les risques, mais aussi de mieux répartir la charge de travail pour éviter l’épuisement des équipes. » souligne **Laurent Besset, Directeur Général Adjoint et Cyberdéfense chez I-TRACING.**

Un impact direct sur la détection et le traitement des vulnérabilités critiques

L’étude montre que près de 9 RSSI sur 10 déclarent disposer d’un processus clair et opérationnel. Toutefois, si près de 85 % utilisent au moins deux outils pour le suivi des vulnérabilités, 15 % d’entre eux en utilisent 5 ou plus. Elle met en évidence une disparité méthodologique et de moyens alloués par les entreprises qui engendre une multiplicité d’approches : la moitié des répondants (51 %) s’appuient sur des outils d’IT Services Management (ITSM) pour le suivi de la remédiation, 66 % exploitent directement leur outil de détection, près d’un quart gèrent les vulnérabilités via des fichiers partagés (24 %), mais encore 22 % fonctionnent sans tableau de bord ni outil dédié, ce qui complique la mesure de l’efficacité des actions.

L’étude démontre que cette hétérogénéité des pratiques reflète un manque de convergence des modèles opérationnels. Cela limite la capacité des organisations à industrialiser le traitement des vulnérabilités et à en piloter efficacement la remédiation.

Ces différences se répercutent sur les délais de traitement des vulnérabilités critiques. Si les failles sont exploitées dans les 24 à 48 heures en moyenne, seules 7,6 % d’entre elles sont corrigées en moins de 24 heures. Ainsi, la moitié des entreprises déclarent parvenir à les corriger en moins de 7 jours, un délai souvent imposé par les Politiques de Sécurité des Systèmes d'Information (PSSI), mais rarement respecté. Cette situation s’explique notamment par un manque d’alignement entre les exigences des PSSI et les capacités opérationnelles, ainsi que par la jeunesse des démarches VOC dans les processus des entreprises.

Ce décalage met en évidence un enjeu central pour les organisations, car elles ne sont plus

confrontées à un problème de visibilité sur les vulnérabilités, mais à un problème de capacité à agir dans le temps court, imposé par les attaquants.

L'étude met également en évidence que seules 2 entreprises sur 5 ont mis en place un processus transverse, capable d'agréger les données et de prioriser les actions de manière unifiée. Cette fragmentation des outils et des méthodes venant ralentir la remédiation.

« La gestion des vulnérabilités ne peut pas reposer sur des outils isolés ou des processus cloisonnés. Une approche unifiée et contextualisée est indispensable pour réduire efficacement les risques. » insiste **Fabrice Bru, Président du CESIN.**

Aujourd'hui, le défi n'est plus uniquement de détecter ou de prioriser les vulnérabilités. Il réside en la capacité de les corriger avant qu'elles soient exploitées. Cela suppose une transformation des organisations, des processus et de la gouvernance, au-delà des seuls outils.

Un manque d'automatisation et de maturité dans les entreprises

L'étude souligne que les lacunes en matière de gestion des vulnérabilités dépendent des moyens organisationnels, technologiques et financiers des entreprises. Cependant des pistes d'amélioration émergent de l'analyse menée par I-TRACING et le CESIN. Les méthodologies de cybersécurité intègrent progressivement l'intelligence artificielle (IA) dans les processus, même si son adoption reste encore timide. Pourtant l'IA représente un atout majeur pour l'automatisation des tâches répétitives, synthétiser les rapports de vulnérabilités, clarifier les messages d'alerte et générer des recommandations adaptées.

Un autre levier d'amélioration réside dans la montée en maturité des entreprises face aux enjeux de cybersécurité. En structurant davantage leurs services dédiés, tant en effectifs qu'en outils, les organisations renforcent leurs capacités à faire face aux risques. Parallèlement, le secteur poursuit son évolution vers une standardisation des outils et des données, favorisant ainsi l'émergence de méthodologies plus uniformes et efficaces.

In fine, les démarches de type VOC apparaissent moins comme une évolution technique que comme une réponse organisationnelle nécessaire pour rétablir un alignement entre détection, priorisation et capacité effective de remédiation.

I-TRACING et le CESIN publient conjointement le Livre Blanc "Gestion des vulnérabilités : Comment réduire votre exposition aux cyberattaques"
Pour consulter le Livre Blanc, cliquez ici