i-TRACING CYBERSECURITY

En partenariat avec le CESIN

LIVRE BLANC

Gestion des vulnérabilités :

Comment réduire votre exposition aux cyberattaques ?

CONTACT : infos@i-tracing.com

+33 1 70 94 69 70 - **www.i-tracing.com**

Édito

Reprendre le contrôle face à l'explosion des vulnérabilités

Jamais la gestion des vulnérabilités n'a occupé une place aussi centrale dans la résilience cyber des organisations. Dans un écosystème numérique toujours plus hybride, interconnecté et soumis à une pression réglementaire croissante, la prévention technique constitue désormais le véritable socle sur lequel reposent les capacités de défense. Si les organisations ont historiquement concentré leurs efforts sur la réaction — SOC, CERT, réponse à incident — la maturité cyber exige aujourd'hui un travail de fond, continu, souvent moins visible : maîtriser l'exposition, réduire le bruit, et assurer une remédiation efficace.

Pour mesurer la réalité opérationnelle de terrain, I-TRACING et le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) ont mené une étude d'envergure auprès de plus de **250 RSSI**. Les résultats sont sans équivoque.

À mesure que le nombre de vulnérabilités explose — dépassant les 100 CVE recensées par jour — les équipes cybersécurité se retrouvent en surrégime : **56% des répondants déclarent manquer de personnel qualifié pour absorber le flux de failles**, dont la moitié sont jugées trop critiques pour être ignorées.

Cette tension structurelle a un impact direct sur la capacité de remédiation. Comme l'explique **Laurent Besset, Directeur Général Adjoint et Cyberdéfense chez I-TRACING** :

❝ 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. ❞

L'étude révèle également un paradoxe frappant. **Alors que les attaquants exploitent une faille critique en moins de 48 heures, moins d'une entreprise sur dix parvient à corriger ces vulnérabilités en moins de 24 heures.**

Un décalage qui s'explique par la fragmentation des outils et des processus : **22% des organisations ne disposent d'aucun tableau de bord dédié**, rendant extrêmement difficile toute vision consolidée du risque.

Pour **Fabrice Bru, Président du CESIN**, cette dispersion est un obstacle majeur à l'efficacité opérationnelle :

❝ 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. ❞

C'est précisément l'ambition de ce Livre Blanc : **proposer une cartographie complète du cycle de gestion des vulnérabilités, enrichie par les retours du terrain et l'expertise d'I-TRACING**.

L'objectif est de fournir des clés pour transformer les traditionnels « tableaux de bord sapins de Noël » en instruments de pilotage fiables, d'outiller les VOC (Vulnerability Operations Centers) d'une méthodologie cohérente, et d'aider les organisations à passer d'une logique de réaction à une stratégie active de réduction du risque.

Remerciements

Nous souhaitons adresser nos sincères remerciements
aux **250 CISO et responsables cybersécurité membres du CESIN**
qui ont pris le temps de répondre à notre sondage et
ont contribué à dresser un panorama fidèle et éclairant
des pratiques VOC au sein des organisations françaises.

Nos remerciements vont également à **Julien Bui, Vincent Lefret,**
Didier Gras, Frank Van Caenegem, François Drouillot, Eric Doyen,
ainsi qu'à l'ensemble des experts ayant partagé leurs retours d'expérience.

Enfin, nous remercions chaleureusement **Fabrice Bru** et **Alain Bouillé**,
pour leur confiance de longue date et leur engagement constant
au service de la communauté cyber.

Sommaire

Introduction

Contexte actuel de la cybersécurité

La digitalisation accélérée, l'automatisation et la centralisation des services IT ont créé un environnement où les interconnexions se multiplient. Parallèlement, la cybersécurité est devenue plus accessible et mieux documentée, suscitant l'intérêt de tous les acteurs :

- Les attaquants, à la recherche de gains financiers ou des à des fins d'espionnage ;
- Les entreprises, souhaitant éviter les interruptions majeures de leur production ;
- Les éditeurs, développant des solutions de détection, surveillance et remédiation ;
- Les sociétés de conseil, accompagnant à la sensibilisation, l'intégration et l'exploitation de solutions ou services de cybersécurité.

Cette dynamique s'accompagne de défis structurels et techniques bien connus :

1. La montée des attaques ciblées ;
2. La complexité croissante des environnements hybrides ;
3. Une pression réglementaire de plus en plus forte.

Pour y répondre, les organisations renforcent progressivement leurs capacités de préparation et de réaction. SOC, CERT, investigation, intervention : ces briques opérationnelles constituent souvent les premières étapes d'une montée en maturité cyber.

Mais au-delà de la réaction, émergent les causes structurelles qui favorisent les attaques :

- Le facteur humain, adressé via la sensibilisation et la formation ;
- Les faiblesses techniques, traitées par les mises à jour, le durcissement et la maîtrise des configurations.

Ce second volet, moins visible mais essentiel, constitue le socle de résilience sur lequel reposent les capacités de détection et de réponse. C'est dans ce cadre que se positionne l'un des leviers de prévention les plus déterminants : la gestion des vulnérabilités.

Explosion des vulnérabilités (chiffres récents, CVE, etc.)

Dans l'univers des vulnérabilités, le référentiel CVE – Common Vulnerabilities & Exposures – s'impose comme l'un des standards internationaux. Chaque CVE fournit un identifiant unique, publié par un vaste écosystème de contributeurs, permettant de documenter et de partager rapidement la connaissance des failles.

L'évolution récente des chiffres est éloquente :

	2025	2024	2023	2022	2021	2020
CVE	48 448	40 077	28 961	25 059	20 161	18 375
CVE / JOUR	133	110	79	69	55	50
% DIFF. (-1 AN)	+21%	+38%	+16%	+24%	+10%	+6%
RESERVED CVE	70 729	52 316	40 051	34 553	28 506	30 680
PARTENAIRES CNA AJOUTÉS	+64	+88	+84	+56	+65	+36
PARTENAIRES CNA TOTAL	491	427	339	255	199	134

> ***“ Le niveau de vulnérabilité de l'ensemble des logiciels au niveau mondial, a atteint une situation extrêmement préoccupante. […] Les 5 critères [Avis publiés, Avis modifiés, Zero day, vulnérabilités critiques, vulnérabilités exploitées] sont en CONSTANTE AUGMENTATION, avec des records mondiaux battus chaque année.”***
>
> ■ **Didier Gras**

Le volume a littéralement explosé — dépassant désormais les 100 nouvelles CVE par jour.

Plusieurs facteurs motivent cette croissance :

1. Multiplication des technologies analysées, élargissant la surface de détection.
2. Attractivité accrue du domaine, qui attire chercheurs, éditeurs et écosystème cyber.
3. Hausse du nombre de contributeurs CNA, enrichissant la documentation.
4. Accessibilité croissante de l'information, qui simplifie la publication comme l'exploitation.

Conséquence directe : plus les vulnérabilités sont documentées, plus elles deviennent actionnables, autant pour les défenseurs que pour les attaquants.

Pourquoi la gestion des vulnérabilités est cruciale aujourd'hui

La démocratisation des connaissances, la disponibilité croissante des outils d'exploitation et la rapidité des publications ont transformé la gestion des vulnérabilités en enjeu stratégique.

Les vulnérabilités critiques sont aujourd'hui exploitées en moins de 24 heures, parfois dès la publication d'un PoC. Des campagnes automatisées ciblent systématiquement les équipements exposés, rendant le délai de réaction particulièrement court.

Dans les faits, entre la moitié et deux-tiers des compromissions initiales impliquent l'exploitation directe d'une vulnérabilité. Cette tendance est amplifiée par la hausse du nombre de zero-days, qui réduisent la marge de manœuvre des équipes défensives.

Dans ce contexte, les organisations doivent renforcer leur résilience autour de trois axes : veille adaptée à un écosystème extrêmement dynamique ; surveillance continue d'un SI en transformation permanente ; capacité opérationnelle à réagir immédiatement lorsque le risque devient concret.

La gestion des vulnérabilités n'est donc plus un simple volet technique : c'est un levier fondamental de réduction du risque cyber.

Objectif / Portée du livre blanc

La cybersécurité n'a jamais été aussi critique et paradoxalement, aussi exigeante. Chaque semaine apporte son lot de nouvelles vulnérabilités, de CVE à analyser, de correctifs à appliquer et de dépendances à vérifier. Face à ce flux continu, les équipes sécurité se heurtent souvent à deux réalités particulièrement frustrantes :

- Les tableaux de bord "sapin de Noël" : chaque vulnérabilité devient rouge clignotante. Les scans débordent de notifications critiques, et tout semble urgent. Le vrai défi n'est plus de détecter les vulnérabilités, mais de distinguer le signal du bruit.
- Le gouffre entre volume et ressources : le nombre de vulnérabilités explose, tandis que les effectifs restent humains. Les équipes jonglent entre priorisation, remédiation et reporting, avec parfois le sentiment de courir après leur propre inventaire.

Ce double défi rend indispensable une approche structurée, pragmatique et mesurable. Ce livre blanc propose une cartographie du cycle de gestion des vulnérabilités, des définitions clés aux bonnes pratiques, pour aider les organisations à faire face et à reprendre le contrôle.

1. Qu'est-ce qu'une vulnérabilité ?

> *« Comprendre pour mieux agir : entre potentiel de menace et réalité d'incident »*

Dans un contexte où la transformation numérique multiplie les interconnexions, la vitesse et la complexité deviennent des facteurs critiques de sécurité. Chaque nouvelle technologie introduit son lot d'opportunités… mais aussi de fragilités.

Pourtant, sur le terrain, un constat s'impose : les organisations peinent encore à distinguer clairement ce qu'est une vulnérabilité, une menace, un risque ou une exposition. Cette confusion conceptuelle entraîne des conséquences directes sur la capacité à agir efficacement.

Ce chapitre pose les bases. Il définit un langage commun, clarifie les concepts structurants et illustre la manière dont une vulnérabilité peut progressivement glisser vers un incident majeur si elle n'est pas maîtrisée.

1.1. Définitions (vulnérabilité, menace, risque, exposition)

DÉFINITIONS

VULNÉRABILITÉ : UNE FAIBLESSE, PAS ENCORE UN DOMMAGE

Une vulnérabilité est une faiblesse intrinsèque dans un système, une application, un équipement, un processus ou une configuration. Elle ouvre une possibilité d'exploitation, sans pour autant provoquer immédiatement un impact. Elle est un état latent, une faille qui, si elle reste ignorée, peut devenir le point d'entrée d'un incident.

« La vulnérabilité ne fait pas le dommage. Elle en crée la possibilité. »

MENACE : L'INTENTION, L'ÉVÈNEMENT OU LE MÉCANISME D'EXPLOITATION

La menace représente tout ce qui peut tenter d'exploiter une vulnérabilité. Un acteur malveillant, un outil automatisé, une organisation criminelle, mais aussi un événement accidentel ou une erreur humaine.
« Là où la vulnérabilité est une faiblesse, la menace incarne la capacité à l'utiliser. »

RISQUE : PROBABILITÉ ET IMPACT

Le risque correspond à la combinaison entre la probabilité d'exploitation et l'impact potentiel sur l'organisation en termes de pertes financières, de perturbations opérationnelles, d'atteinte à la réputation et de contraintes réglementaires et légales.

« Une même vulnérabilité peut représenter un risque faible dans une organisation…
et critique dans une autre. »

EXPOSITION : A QUEL POINT SOMMES-NOUS RÉELLEMENT CONCERNÉS ?

L'exposition mesure le degré concret de sensibilité d'une organisation face à une vulnérabilité donnée ; quelle technologie est concernée ? Est-elle exposée sur Internet ? Quelle dépendance métier repose dessus ? Est-elle massivement déployée ?

Ainsi, deux environnements partageant la même vulnérabilité n'ont pas nécessairement la même exposition, ni le même risque.

1.2. Typologies de vulnérabilités (logicielle, matérielle, configuration)

Toutes les vulnérabilités ne se valent pas, ni en origine, ni en criticité, ni en modalités de remédiation. Les classifier permet de structurer la réponse de sécurité.

LOGICIELLE	MATÉRIELLE	CONFIGURATION
VULNÉRABILITÉ : CARACTÉRISTIQUES		
Elles sont généralement recensées dans des bases publiques, corrigées par des mises à jour logicielles et peuvent passer brutalement du statut “potentiel” à “incident réel” dès qu’un exploit apparaît.	Elles représentent souvent des problèmes de conception architecturaux. Leur traitement est souvent long et complexe, nécessitant parfois un remplacement matériel ou une dépendance forte aux constructeurs.	Elles illustrent parfaitement la frontière floue entre vulnérabilité et incident, une mauvaise configuration n’est pas un incident… jusqu’au moment où quelqu’un s’en sert
VULNÉRABILITÉ : ORIGINE		
• Failles d’authentification • Injections • Élévations de privilèges • Dépassements de mémoire	• Défauts micro-architecturaux • Micrologiciels vulnérables • Faiblesses matérielles critiques	• Mauvais paramétrages • Ports inutilement exposés • Mots de passe par défaut • Droits excessifs • Absence de segmentation

1.3. Les sources NIST (CVE, CERT-FR, éditeurs) et leurs utilisateurs

La gestion des vulnérabilités s’appuie sur un réseau international d’acteurs qui détectent, analysent, qualifient et diffusent l’information. Les principales sources sont reprises ci-dessous :

SOURCES	DESCRIPTION
CVE	Base de référence mondiale attribuant un identifiant unique à chaque faille connue.
NVD	Maintenue par le NIST, elle enrichit les CVE de métriques, dont le fameux score CVSS, qui aide à prioriser.
CERT	Ils publient alertes, synthèses techniques, recommandations et indicateurs d’exploitation.
ÉDITEURS	Fournissent correctifs, bulletins et mesures temporaires de mitigation.
COMMUNAUTÉ	Chercheurs, laboratoires, sociétés spécialisées, programmes de bug bounty.

Ce modèle présente des avantages indéniables apportant une standardisation globale, une interopérabilité des outils, langage commun entre acteurs publics et privés, ainsi qu’une accélération du partage d’information.

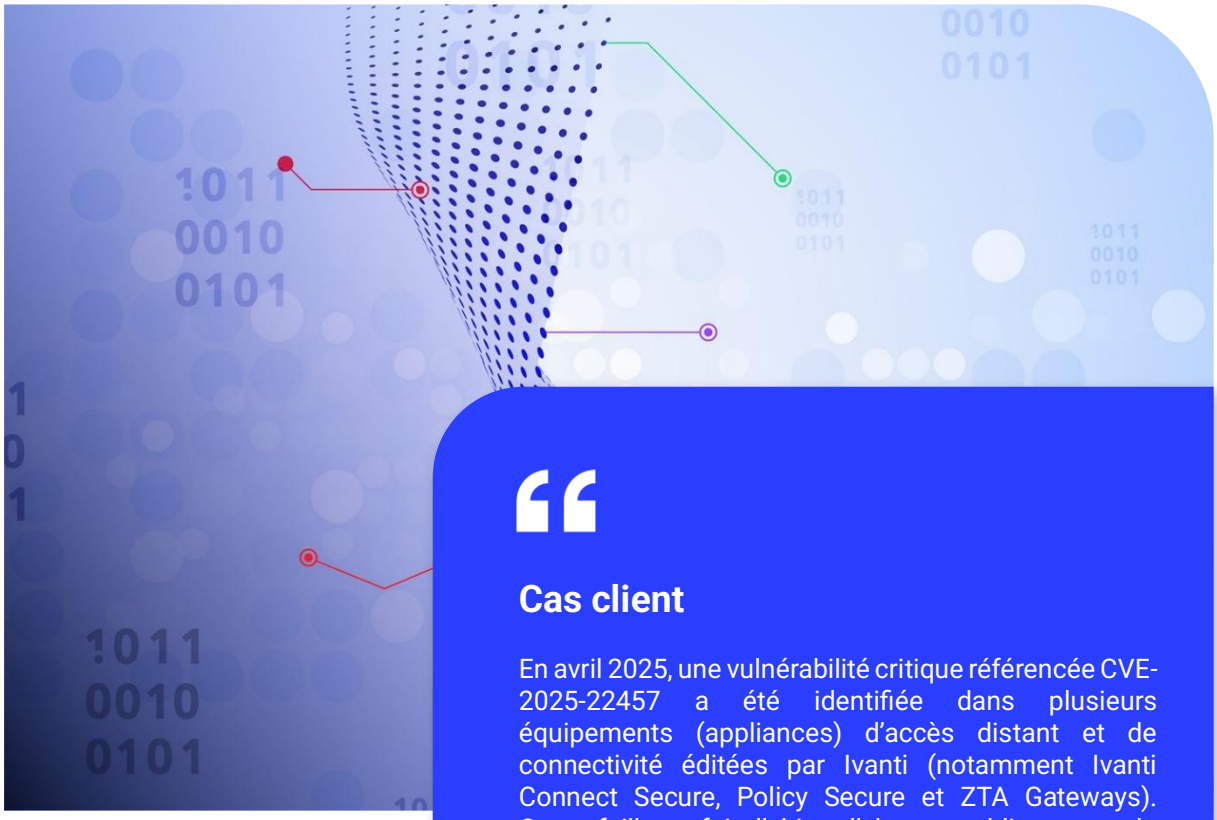
Sans relever d’un enjeu géopolitique, cette réalité pose une question de résilience de l’écosystème : la diversification des sources, le rôle croissant des CERT nationaux et régionaux, et l’émergence d’initiatives complémentaires contribuent à renforcer la robustesse du partage d’information à l’échelle internationale. Dans cette logique de diversification, des initiatives globales et régionales émergent pour renforcer la robustesse de l’écosystème global. Les projets GCVE et EUVD s’inscrive dans cette dynamique en proposant une capacité de structuration et de diffusion de l’information sur les vulnérabilités.

1.4. Exemple concret illustratif : le cas Ivanti

En avril 2025, une vulnérabilité critique référencée CVE-2025-22457 a été identifiée dans plusieurs équipements (appliances) d'accès distant et de connectivité éditées par Ivanti (notamment Ivanti Connect Secure, Policy Secure et ZTA Gateways). Cette faille a fait l'objet d'alertes publiques et de bulletins de sécurité par les CERTs* (dont le CERT-FR et d'autres agences nationales) en raison de son exploitation active observée dans la nature.

Cette vulnérabilité permet à un attaquant distant non authentifié d'atteindre une exécution de code arbitraire à distance (remote code execution – RCE) sur les systèmes vulnérables. Techniquement, elle permet un débordement de mémoire tampon basé sur la pile (stack-based buffer overflow).

PHASE VULNERABILITE : **11 février 2025**	Initialement, la faille est simplement une faiblesse dans le code exploitable en théorie. Aucune compromission n'est encore constatée.
PHASE DE MENACE ACCRUE : **Mi-mars 2025**	Dès que la preuve de concept est disponible publiquement, la menace passe de potentielle à crédible. Les équipes de sécurité doivent alors prioriser l'analyse de l'exposition.
PHASE INCIDENT : **3 avril 2025**	Avec l'exploitation active (observée par Mandiant et relayée par les CERTs), la vulnérabilité cesse d'être un simple risque théorique : elle devient un incident avéré dès qu'un système est compromis.



> **Cas client**
>
> En avril 2025, une vulnérabilité critique référencée CVE-2025-22457 a été identifiée dans plusieurs équipements (appliances) d'accès distant et de connectivité éditées par Ivanti (notamment Ivanti Connect Secure, Policy Secure et ZTA Gateways). Cette faille a fait l'objet d'alertes publiques et de bulletins de sécurité par les CERTs* (dont le CERT-FR et d'autres agences nationales) en raison de son exploitation active observée dans la nature.
>
> ■ **Ivanti**

2. Cycle de vie de la gestion des vulnérabilités

> *« De la découverte à la remédiation effective*

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS
Quel est votre procédé de suivi des vulnérabilités ?

88% des organisations disent avoir un processus clair et opérationnel	dont **42%** ont un processus transverse

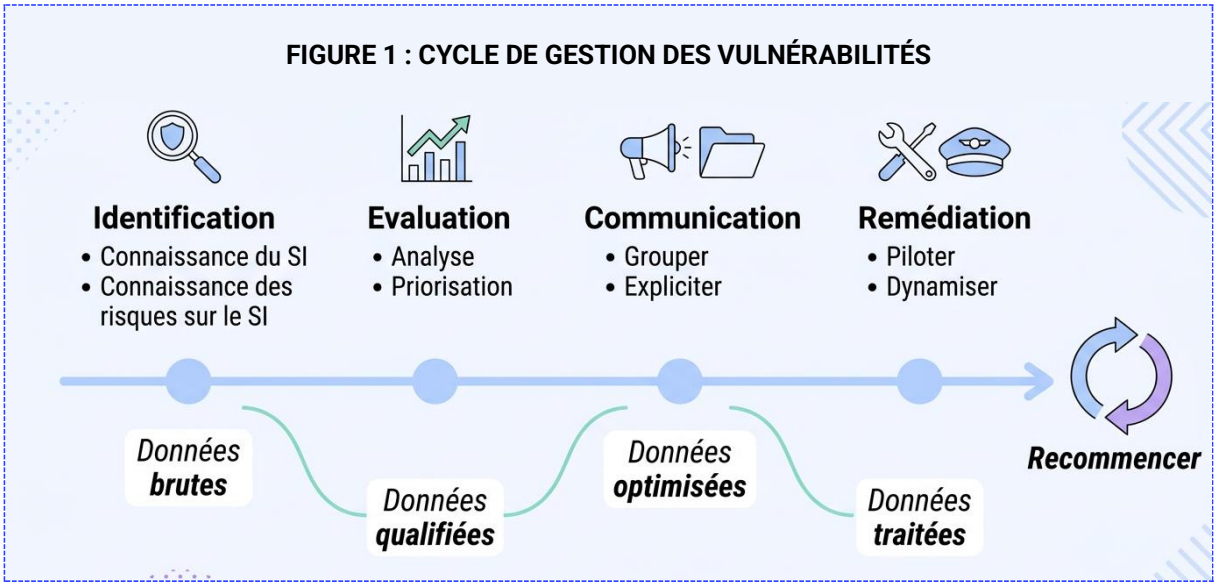
Le sujet semble dans l'ensemble pris en compte, mais les résultats du sondage du CESIN démontrent que la méthodologie ne fait pas consensus.

Le paysage des Vulnérabilités est par nature :

- En évolution constante
- Portant un risque modulé à travers le temps
- Situationnel, hautement dépendant de l'environnement et de l'industrie dans laquelle on se situe

La gestion des vulnérabilités n'est pas une activité ponctuelle, mais un processus itératif et continu. Les activités communément identifiées dans un cycle standard de traitement des vulnérabilités sont les suivantes :

FIGURE 1 : CYCLE DE GESTION DES VULNÉRABILITÉS



IDENTIFICATION

La gestion des vulnérabilités repose sur un cycle continu qui transforme des données brutes en décisions de sécurité actionnables. Elle débute par l'identification, combinant veille, scans, analyses et retours terrain pour révéler à la fois les failles techniques et leur exposition réelle.

EVALUATION

L'étape d'évaluation enrichit ensuite ces détections : criticité, menace active, contexte métier, exploitabilité — tout ce qui permet de distinguer l'urgent du bruit.

COMMUNICATION & REMEDIATION

Les phases de communication et remédiation constituent le cœur opérationnel : regrouper les vulnérabilités par actions communes, expliquer clairement le risque, piloter la correction et orchestrer patches ou mesures compensatoires lorsque les correctifs n'existent pas.

SURVEILLANCE CONTINUE

La surveillance continue vient assurer la cohérence du dispositif dans le temps, via des indicateurs de risque, d'effort et de santé, indispensables pour mesurer l'efficacité des actions et détecter les dérives.

DOCUMENTATION

Enfin, une documentation solide et une logique d'amélioration continue garantissent la stabilité du programme, sa reproductibilité et sa montée en maturité.

Retrouvez la version détaillée de ce chapitre en Annexe 1. Son contenu à vocation descriptive indique les étapes, parfois détaillées, pouvant se retrouver dans un cycle standard de gestion des Vulnérabilités.

3. Les défis courants rencontrés

> *« Ou comment consolider les prérequis »*

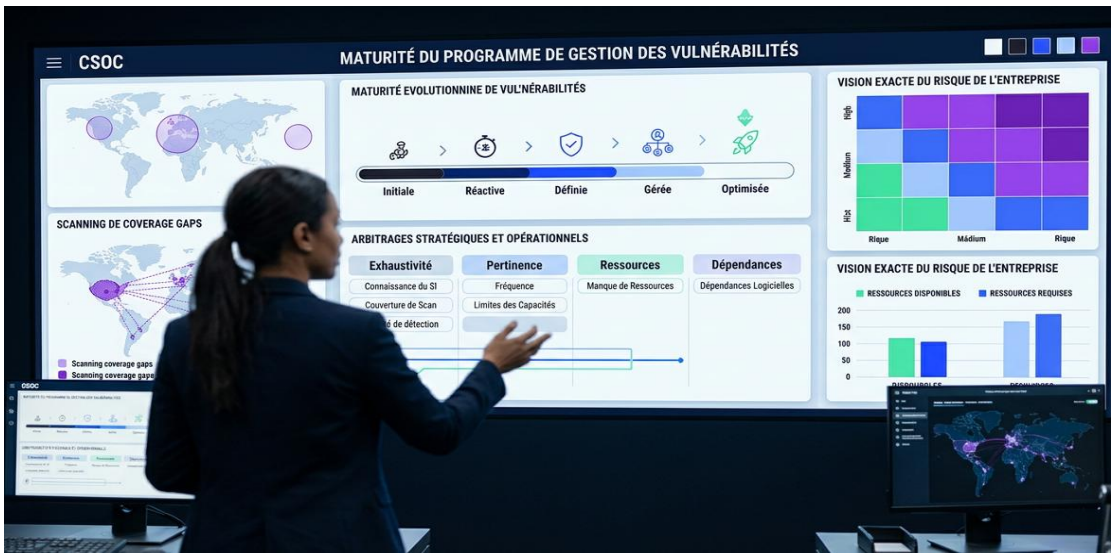
SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS

34%	22%	28%
des organisations déclarent un manque de visibilité sur les actifs	n'ont ni tableau de bord ni ITSM pour suivre la remédiation	pointent un manque de coordination avec l'IT

Ces résultats révèlent un point commun :
les bases essentielles d'un programme de gestion des vulnérabilités — visibilité, pilotage et collaboration — restent encore insuffisamment consolidées dans de nombreuses structures.

La montée en maturité d'un programme de gestion des vulnérabilités, quel que soit le point de départ, s'inscrit systématiquement au travers de choix forts. L'un des premiers objectifs réside dans l'obtention d'une vision la plus exacte possible du niveau de risque de son entreprise. Or, peu d'entreprises disposent des ressources nécessaires pour assurer une couverture parfaite, continue et appuyée sur les technologies les plus avancées.

Il faut alors faire des choix, d'ordre stratégique, financier, organisationnel ou opérationnel, sur des thématiques abordées dans ce chapitre.



3.1. Exhaustivité

La couverture parfaite est une illusion, surtout lorsqu'on ignore ce que l'on ne sait pas.

3.1.1. Connaissance de son SI

Au sein d'une entreprise, les typologies de périmètres vulnérables et exploitables sont nombreuses. Or, la majorité des entreprises n'ont pas les outils ou les ressources pour couvrir de manière exhaustive leurs environnements. Parler de taux de couverture global est une illusion tant que l'on n'a pas la capacité de répondre à quelques questions.

LES QUESTIONS A SE POSER :

1. **Est-ce que je connais l'ensemble de mes périmètres ?**
2. **Est-ce que je connais mes angles morts ?**
3. **Est-ce que ma connaissance est pérenne ?**

LA METHODE EN FONCTION DE LA REPONSE

En répondant à ces 3 questions on sait se diriger vers la méthode la plus appropriée à son niveau de maturité actuel.

➔ **Si je ne sais rien**, rassembler ce qui peut constituer un inventaire sera la première étape (en priorisant les périmètres les plus critiques, exposés, critiques pour les affaires : ce sont des éléments forts et faciles à mettre en lumière pour initier la discussion).

➔ **Si je sais, mais pas tout,** j'ai conscience de ce que je ne sais pas. La prochaine étape peut être la consolidation de sa source d'inventaire en listant les catégories d'actifs, leur source d'hébergement, et en se donnant le moyen de collecter la liste des actifs dans ces nouvelles sources. Opérationnellement, cela se traduit aussi par la création d'un processus permettant l'ajout rapide de ce qui est nouvellement connu. Je sais que je ne connais pas tout, mais dès que je connais, j'ajoute. Cela passe concrètement par l'analyse continue de couverture à différents niveaux (individuel, périmétrique, technologique, …), et par la mise en place d'actions en fonction des résultats d'analyse.

➔ **Si je connais l'ensemble de mes périmètres**, c'est déjà un grand pas. On peut être proche de se dire « Je suis exhaustif ». Mais avant cela, il est essentiel de se demander « Serais-je exhaustif dans 6 mois ?». Question anodine qui ne l'est pas tant, tant les parcs informatiques évoluent vite. On va alors souhaiter automatiser, agréger et consolider toutes sources d'information, dynamiques ou statiques, permettant la mise à jour et la mise en disponibilité d'un socle de métadonnées de base. Quasi systématiquement, ce processus devra être outillé pour être pertinent et maintenable, et presque aussi régulièrement, il ne sera pas entièrement à la main des acteurs de la cybersécurité mais plutôt opéré et maintenu par les équipes SI.

Une fois « l'exhaustif » en vue, il s'agira de mettre en place une approche résiliente pour découvrir et reconnaitre son parc, afin de rassembler les données :

- En agrégeant de multiples sources – *pour maximiser l'agrégation de la connaissance*
- De manière récurrente – *pour minimiser l'obsolescence de la donnée*
- Avec un socle de métadonnées minimal (propriétaire, criticité métier, exposition, environnement) – *pour rendre l'inventaire utile au programme de gestion des vulnérabilités*
- Et avec un sponsor métier – *pour s'assurer de la véracité des données*

3.1.2. Couverture de scan

Dans beaucoup d'organisations, les scans sont déployés par périmètre technologique — serveurs, postes, réseau — alors qu'aucun inventaire fiable ne permet d'en définir réellement l'étendue. La couverture repose alors sur des volumes estimés, compliquant le déploiement, fausse le suivi et rend le taux de couverture difficile à interpréter.

Pour un RSSI, l'enjeu n'est pas seulement de scanner, mais de disposer d'une vision exhaustive du périmètre à protéger. Les défis de la mise en place d'un taux de couverture peuvent être les suivants :

UNE BASE DE COMPARAISON INEXISTANTE

Sans revenir sur la connaissance de son SI, il s'agira à ce stade de se constituer un référentiel. À défaut d'un vrai référentiel, de mettre en œuvre des méthodes souples et qui voient large (des méthodes de découvertes, de scan réseau ou d'inventaire) sur lesquelles peut être constituée une estimation de la base de référence.

> *La CMDB existante n'étant pas exhaustive, il a fallu se baser sur les résultats des scans tout en faisant en sorte de faire évoluer la CMDB afin de pouvoir s'en servir comme référentiel. La CMDB n'étant pas gérée par le service sécurité, nous rencontrons certaines difficultés à la faire évoluer et correspondre à nos besoins.*
>
> ■ **François Drouillot**
>
> CESIN

100% DE COUVERTURE DIFFICILEMENT ATTEIGNABLE

La mouvance des SI génèrera quasi-systématiquement des actions spécifiques de correction de couverture. Il s'agira dans ce cas de vérifier que chaque maillon de la détection fonctionne :

- **OUTILLAGE :** le paramétrage de détection initial – est-ce que l'on cible bien ?
- **RÉSEAU :** le paramétrage réseau – peut-on atteindre la cible (DMZ, pare-feu, ports, etc.) ?
- **ASSET :** la disponibilité de l'asset – l'asset est-il allumé ?
- **REPORTING :** le dédoublement – ne s'agit-il pas d'un problème de visualisation plutôt que de détection ?

SPÉCIFICITÉS DE PÉRIMÈTRES TECHNOLOGIQUES

Tous les périmètres technologiques n'apportent pas le même lot de contraintes de détection. On peut faire face à des assets éphémères (conteneurs), des assets par nature indisponibles de manière intermittente (postes de travail), des assets sur lesquels le scan automatique pratique des actions spécifiques (application web) ou encore des assets à très haut besoin en disponibilité (dans le monde industriel).

Un effort particulier est à apporter sur l'adaptation de l'approche et la mise en en œuvre de méthodologie de détection adéquate au périmètre, à la technologie, à la criticité de son environnement.

Une série de questions à se poser peut-être la suivante :

- Ai-je une approche adaptée à la technologie ?
- Mon approche est-elle adaptée au risque à couvrir ?
- Ai-je l'outillage adéquat pour mettre en œuvre cette approche ?
- Ai-je l'organisation interne nécessaire pour mettre en œuvre cette approche ?

En établissant sa base au travers de ces 4 questions, on sait alors déterminer si le calcul de couverture dans son organisation peut être réalisé totalement, partiellement selon les périmètres, ou si elle est à ce stade, encore une illusion.

3.1.3. Qualité de détection

La qualité de la détection repose sur deux piliers : la capacité à identifier correctement les actifs et des politiques de scan adaptées et maintenues dans le temps. Une faiblesse sur l'un de ces axes entraîne rapidement des dérives : faux négatifs, données partielles et indicateurs peu fiables. En pratique, même un moteur de détection performant devient inutile si les scans sont mal configurés ou insuffisamment authentifiés.

SCANS AUTHENTIFIÉS : UN FACTEUR DE FIABILITÉ

Un scan authentifié apporte 5 à 20 fois plus d'informations qu'un scan non authentifié. Lorsqu'un identifiant échoue, la visibilité réelle chute et crée un faux sentiment de sécurité : les tableaux de bord paraissent propres, mais uniquement parce que le système n'a pas été inspecté en profondeur. Chaque échec d'authentification doit être traité comme un incident de couverture, car il conditionne directement la connaissance de son risque. Le maintien d'un taux d'authentification élevé est un indicateur stratégique, non un paramètre secondaire.

POLITIQUES DE SCAN : UNE APPROCHE TECHNOLOGIQUE QUASI-INDISPENSABLE

Les politiques "génériques" sont rarement efficaces : elles génèrent du bruit sur certains périmètres et manquent de profondeur sur d'autres. Une approche segmentée — par technologie (Windows, Linux, réseau, Cloud, container), par criticité (prod vs test) et par contraintes opérationnelles (fenêtres, charge, API/agent) — garantit une détection cohérente et exploitable.

Bien calibrées et régulièrement revues, ces politiques évitent les analyses superficielles, réduisent le bruit et renforcent la pertinence globale du programme de remédiation.

3.2. Véracité : assurer la pertinence de la détection

La fiabilité des détections forme le socle stratégique de tout programme de gestion des vulnérabilités mature. Une détection imprécise engendre une fatigue opérationnelle chronique tout en générant des angles morts, exposant l'organisation à des risques résiduels importants. Les équipes sécurité doivent alors évoluer en permanence entre amoncellement de faux positifs et menaces réelles non détectées.
Les sources d'imprécisions peuvent être multiples : « fraicheur » de la donnée, limites des capacités de détection, ignorance contextuelle ou encore démultiplication des informations.

3.2.1. Fréquence de détection des vulnérabilités

La fraîcheur des données est un indicateur clé : plus les scans sont récents, plus la vision du risque est juste et actionnable. Une fréquence adaptée garantit que les vulnérabilités critiques reflètent bien la réalité du SI sans perturber la production. Des données actualisées facilitent la priorisation, accélèrent la remédiation et réduisent les vérifications manuelles. Elles renforcent ainsi l'autonomie opérationnelle et l'efficacité globale du programme.

EXEMPLE DE RECOMMANDATION :

PAR TYPOLOGIE	PAR RISQUE DE L'ASSET
SERVEURS [1X/JOUR À 1X / SEMAINE]	**MAJEUR** [1X/JOUR - 3X / SEMAINE]
POSTE DE TRAVAIL [1X / SEMAINE]	**ELEVÉ** [1 À 2 X / SEMAINE]
RÉSEAU [1 À 2 X / SEMAINE]	**MOYEN & FAIBLE** [1X / SEMAINE]
APPLICATION WEB [1X / SEMAINE]	

3.2.2. Limites des capacités de détection

Maîtriser les limites techniques de ses capacités de détection est essentiel pour poser un diagnostic clair et transparent de la posture de sécurité.

Il s'agit de cartographier précisément ce que les outils, techniques et compétences disponibles permettent de détecter, et de vérifier leur adéquation au risque visé. Cela implique de trancher entre une priorité accordée à la visibilité maximale ou à la préservation de l'impact sur la production.

MAXIMISER LA PORTEÉ DE DETECTION

Connaître les capacités réelles des techniques déployées – ce qu'elles détectent, leurs domaines d'application et leurs limites intrinsèques – permet d'anticiper la gestion des risques résiduels et d'alimenter une roadmap à long terme.

Une connaissance fine de l'outillage garantit l'utilisation du bon levier au bon moment, et permet d'identifier le recours nécessaire à des alternatives lorsque les outils actuels atteignent leurs limites. Il convient d'éviter à tout prix le piège de la simple case à cocher : déployer une technique inadaptée uniquement pour prétendre qu'un périmètre est surveillé.

ARBITRAGE VISIBILITÉ VS IMPACT PRODUCTION

Activer des scans plus exhaustifs offre une détection fine des vulnérabilités, mais au prix d'une durée accrue et d'une intrusivité potentiellement perturbatrice. Les organisations doivent statuer sur des choix stratégiques :

- ➔ **Stratégie de scan :** fréquence, profondeur et planification (par exemple, scans quotidiens légers vs audits mensuels complets).
- ➔ **Actifs et réseaux ciblés :** priorisation des équipements critiques exposés face aux systèmes moins sensibles, pour limiter les interruptions de service.

Il n'y a pas d'approche parfaite, il s'agira plus d'utiliser ses moyens au plein potentiel, plutôt que de suivre un guide type.

3.2.3. Un contexte propre

Un risque réel ne peut être qualifié avec précision sans un contexte métier détaillé. L'information finale pertinente réside dans le contexte propre à chaque système ou application – système d'exploitation, applications déployées, configuration métier spécifique, environnement, utilisation, écosystème ou réglementation.
Ce niveau de granularité permet de trancher de manière fiable, et répétitive (stratégie de priorisation) entre faux positif, vulnérabilité négligeable et remédiation prioritaire, évitant ainsi les actions inutiles et optimisant l'efficacité opérationnelle de la détection des vulnérabilités.
En somme, toute approche optimisée demandera la mise à disposition d'un contexte métier précis.

3.2.4. Écart entre détection et remédiation

Un défi récurrent réside dans l'écart entre le suivi volumétrique des vulnérabilités détectées et le suivi effectif des actions de remédiation. Mesurer le volume de vulnérabilités n'équivaut pas à mesurer le volume de remédiations associées à ce même inventaire.
Se focaliser exclusivement sur la détection permet de connaître le risque unitaire encouru par chaque vulnérabilité. La priorisation de la remédiation vise, quant à elle, à optimiser les efforts de traitement.

Pour relier ces deux dimensions – établir un lien direct entre détection, risque avéré et effort de remédiation –, deux leviers s'imposent généralement :

- Un mécanisme de regroupement des vulnérabilités par action commune (par actif, technologie, correctif…).
- Un indicateur synthétique mesurant le niveau de risque couvert par ces actions groupées.

Il n'existe aucune solution miracle pour opérer cette jonction : par l'automatisation, ou la mobilisation conséquente de ressources humaines.

A noter que les éditeurs spécialisés dans le traitement des vulnérabilités intègrent nativement des fonctionnalités de groupement par action de remédiation. À l'inverse, ceux ayant un ajouté tardivement une capacité de gestion des vulnérabilités adoptent souvent une approche brute, par CVE, dépourvue de regroupement logique optimisé pour la remédiation.

3.3. Autres freins et points sensibles

3.3.1. Manque de ressources ou de coordination

Le manque de ressources qualifiées et de coordination inter-équipes est un frein majeur, où chaque phase du cycle repose sur des compétences spécialisées non toujours disponibles. En quelques points les freins courants :

- **Sous-dimensionnement :** trop de vulnérabilités, pas assez de mains pour les remédier
- **Silos organisationnels** : SSI vs IT vs Métiers ne collaborent pas
- **Priorités conflictuelles** : IT se concentre sur disponibilité, SSI sur sécurité

Ces freins nécessitent l'ajout de compétences particulières selon le point bloquant :

CATÉGORIE	PROFIL	ACTIONS
OUTILLAGE / DÉTECTION	Expert (audit, scanner, …)	Configuration, maintenance et amélioration
ANALYSE/TRIAGE/VEILLE	Expert vulnérabilité	Gère le bruit, rend la donnée qualitative et priorise
REMÉDIATION	Chef de projet / Référent	Dynamise, échange, fiabilise
COORDINATION	Chef de projet sécurité	Pilote le programme, les acteurs et prestataires. Aide à l'arbitrage entre SSI, IT, Métier
INTERCONNEXION	Expert intégration (CMDB, ITSM, CMS, …)	Créé des ponts entre les équipes IT/Métier et sécurité

3.3.2. Périmètre IT hétérogène & transversalité

La coexistence d'environnements multiples — on-premise, Cloud, IoT, workloads containers, systèmes industriels — crée une mosaïque technologique difficile à piloter de manière cohérente. Chaque périmètre possède ses propres contraintes de détection, ses outils, ses rythmes et parfois ses équipes dédiées. Sans cadre transversal, cette diversité engendre des priorités concurrentes, des injonctions multiples pour les équipes de remédiation et une perte de lisibilité globale.

Pour éviter ces dérives, la gestion des vulnérabilités doit reposer sur une stratégie unifiée, capable d'absorber les spécificités locales tout en conservant une vue d'ensemble. Cela implique de :

- Fédérer les besoins de détection sans multiplier les logiques parallèles
- Harmoniser la manière dont les résultats sont collectés, normalisés et priorisés
- Structurer un pilotage unique permettant d'arbitrer sur l'ensemble du périmètre

Cette approche offre deux avantages majeurs :

1. Elle renforce l'adaptabilité, en permettant d'ajouter de nouveaux environnements techniques ou opérationnels sans devoir reconstruire la démarche ;
2. Elle améliore la résilience, car la connaissance du risque ne dépend plus de silos locaux, mais d'un cadre partagé capable d'intégrer de nouvelles technologies ou de nouveaux modèles d'hébergement.

Dans un SI hétérogène, la transversalité n'est donc pas un luxe architectural : c'est la condition pour maintenir une détection cohérente, une remédiation pilotable, et une gouvernance capable de s'adapter aux évolutions rapides de l'organisation et de la cybersécurité.

3.3.3. Shadow IT : les programmes VOC comme capteur de visibilité externe

Une part importante des organisations reconnaît ne pas disposer d'un inventaire parfaitement exhaustif de leurs actifs numériques. Or, toute faiblesse de visibilité crée une zone d'angle mort dans la gestion des vulnérabilités. Deux questions structurantes émergent :

- Comment garantir l'inventaire complet des actifs exposés ?
- Comment maintenir cet inventaire à jour dans un système d'information en évolution permanente?

Le shadow IT ne relève pas uniquement d'un défaut de gouvernance : il est aussi la conséquence naturelle de la vitesse d'innovation, de la décentralisation des usages et de la multiplication des environnements Cloud. Il doit donc être traité comme un phénomène structurel, non comme une anomalie isolée.

Dans cette dynamique, le VOC joue un rôle stratégique de détection. Il agit comme un capteur externe du système d'information, capable d'identifier des actifs exposés que les processus internes n'ont pas encore intégrés.

Le VOC devient ainsi un producteur d'intelligence d'inventaire : il alimente en continu la connaissance du SI réel. La posture efficace consiste à faire du VOC :

- Un consommateur actif de la CMDB
- Un contributeur structurant de données de découverte
- Un mécanisme de contrôle croisé de l'inventaire officiel

3.3.4. Dépendances logicielles

Les dépendances tierces – frameworks, bibliothèques – introduisent une complexité transitive souvent invisible, exposant les applications à des vulnérabilités en cascade via la supply chain (ex. : Log4Shell CVE-2021-44228, encore téléchargée malgré des correctifs disponibles depuis plus de quatre ans).

Cette interdépendance s'amplifie avec l'essor des méthodes de développement accélérées : langages de haut niveau comme Python, montée en puissance de l'IA générative et essor du « vibe-coding » favorisant la rapidité au détriment de la maîtrise complète des dépendances. Maintenir la traçabilité dans un contexte de production rapide devient un vrai défi. Comment continuer à répondre aux besoins de production, en utilisant des outils de développement toujours plus rapides, tout en assurant une dépendance minimale et contrôlée.

Dans l'actualité, les vulnérabilités zero-day dans des composants indirects sont monnaie courante (ex. : plus de 155 millions de téléchargements vulnérables de commons-lang v2.6 en 2025) et pour autant, peu de professionnels implémentent des outils de traçabilité SBOM (Software Bill of Materials). Par ailleurs, mettre en œuvre et exploiter de tels moyen revients à ajouter une étape 'sécurité' dans la chaine de déploiement d'une application, impliquant de-facto des retards de déploiement.

Quelques pratiques recommandées :

- Assurer un monitoring continu du côté de la veille
- Générer des SBOM (Software Bill of Materials) en CI/CD (intégration et développement continus) pour inventorier exhaustivement les composants
- Intégrer des outils SCA (Software Composition Analysis) au travers de scans automatisés
- Instaurer une politique stricte de contrôle & de blocage des applications à déployer qui seraient vulnérables

4. Constats

> *« De la théorie à la pratique : à chaque organisation sa gestion des vulnérabilités »*

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS

56% des organisations expriment manquer de personnel	**51%** ont une volumétrie de vulnérabilités trop importante

Nous constatons que le manque de ressources se fait ressentir dans les entreprises de toutes tailles. La priorisation des actions n'est pas perçue comme un problème majeur, alors même que le volume de vulnérabilités à traiter est jugé trop important, et qu'il augmente avec la taille de l'entreprise. Par ailleurs, les outils et les budgets, bien que notifiés, ne constituent pas les principaux freins aux programmes de gestion des vulnérabilités.

Bien que les défis rencontrés soient souvent de nature commune, ils sont par ailleurs étroitement liés au contexte propre à chaque entreprise. Le tableau ci-dessous propose une vue schématique moyenne de différents composants selon la taille des entreprises sous le prisme de la gestion des vulnérabilités.

Les constats suivants reflètent des tendances observées sur le terrain et ne prétendent pas couvrir toutes les situations. D'autres facteurs, comme le secteur, le niveau de maturité digital ou les contraintes réglementaires, influencent fortement l'organisation et les processus.

TAILLE	ORGANISATION	ARCHITECTURE	CHARGE	ÉQUIPE SÉCURITÉ	OUTILLAGE
PME	< 3 équipes IT, découpage simple	Variable, parfois complexe	Équipes multitâches, peu de temps disponible	Petite, polyvalente (VOC, SOC, veille)	Minimal, peu automatisé
GRANDE	5-10 équipes IT, silos par technologie / géographie	Silotée, tiering model	Processus structurés, actions anticipées	Moyenne spécialisée par activité	Mature, interconnecté mais pas toujours optimisé
TRÈS GRANDE	10+ équipes IT / métier, héritages historiques	Complexe, internationale, multi-hébergement	Processus stricts, tickets, traçabilité prioritaire	Conséquente, spécialisée par activité, interlocuteur vulnérabilités	Complet, souvent redondant, besoin de rationalisation

En addition et à des fins de référence, voici ce qui pourrait être attendu par seuil de maturité à chaque étape du cycle de gestion des vulnérabilités.

DIMENSION	IMMATURE	BASIQUE	MATURE	TRÈS MATURE
IDENTIFICATION	Ad hoc	Scans réguliers	Continu et à la demande	Continue, automatisée
ÉVALUATION	Manuelle, lente	Priorisation basée CVSS	Scoring en fonction de la menace	Contextualisée, transverse, scoring intelligent
COMMUNICATION	Inexistante	Planifiée	Planifiée et proactive	Systématique ou automatisée, proactive
REMÉDIATION	Réactive	Planifiée	Planifiée et proactive	Automatisée, planifiée, proactive

4.1. Trois constats majeurs et transverses

1/
La maturité dépend davantage de la structure et de la gouvernance que de la taille

Les PME manquent souvent de formalisation et de ressources ; les grandes organisations disposent de plus de moyens mais souffrent de silos IT ou cyber.

La qualité du pilotage et la clarté des rôles importent plus que le nombre de personnes impliquées.

2/
Les capacités de détections sont moins problématiques que les capacités de remédiation

D'un côté les équipes IT n'ont pas la bande passante, les priorités opérationnelles priment (disponibilité, projets). D'un autre côté les corrections nécessitent tests, validations, fenêtres, coordination alors que les volumes sont trop élevés pour un traitement linéaire.

Résultat : l'écart entre ce qui est détecté et ce qui est corrigé ne cesse de se creuser, quelle que soit la taille de l'organisation.

3/
Les organisations les plus avancées sont celles qui travaillent de manière transverse

Les programmes vulnérabilités performants ont tous un point commun : ils ne fonctionnent pas en silos. Leur réussite repose sur :

1. Une priorisation partagée entre SSI, IT et Métiers,
2. Un langage commun autour du risque (pas autour des CVE),
3. Un pilotage régulier,
4. Une vision centralisée,
5. Un RSSI qui arbitre, IT qui corrige, Métiers qui valident.

4.2. Modèles de maturité selon les types d'organisation

	 PME	 GRANDES ENTREPRISES	 TRÈS GRANDES ENTREPRISES
FORCES	Agilité, proximité entre équipes.	Équipes spécialisées, processus établis.	Outillage complet, structure de gouvernance, équipes nombreuses.
FAIBLESSES	Manque de ressources, documentation, outillage limité.	Silos, priorités concurrentes, complexité historique.	Hétérogénéité, dette organisationnelle, inertie.
CONSÉQUENCES OPÉRATIONNELLES	Bonne réactivité, faible capacité de remédiation soutenue.	Bonne détection, priorisation inégale, remédiation freinée par la coordination.	Bons résultats mais forte dépendance aux processus et aux transitions IT/organisationnelles.

4.3. Répartition du temps dans le cycle de traitement

Une répartition cohérente du temps total nécessaire à un traitement pourrait se situer comme suit :

DÉTECTION	EVALUATION / TRIAGE	COMMUNICATION / REMÉDIATION	REPORTING
(25–30%) du temps	**(10–25%)** du temps	**(35–40%)** du temps	**(10–15%)** du temps
PHASE GÉNÉRALEMENT STABLE : **Programmation des scans, vérification des authentifications, intégration des nouvelles sources.** **Effort maîtrisé grâce à l'outillage.**	**CHARGE TRÈS VARIABLE :** Légère si la priorisation est automatisée et contextualisée ; lourde si le tri repose sur un traitement manuel des CVE. C'est souvent la première zone de saturation.	**POSTE DE CHARGE PRINCIPAL :** Explications, coordination IT, tests, fenêtres de maintenance. C'est ici que naissent retards, backlog, et écarts entre détection et correction, quelle que soit la maturité.	**PILOTAGE, KPIS, TABLEAUX DE BORD.** Fluide si intégré (ITSM/CMDB/outils VM), chronophage sinon. Indispensable pour arbitrer et démontrer la réduction du risque.

En somme, l'efficacité globale repose sur deux leviers : **optimiser l'effort d'analyse via automatisation et contextualisation (meilleure vue du risque réel)**, et **accroître la capacité de remédiation**, seule étape qui réduit réellement le risque.

> *" Le VOC doit pouvoir se raccrocher à une stratégie globale de patch management de l'entreprise et être en mesure de qualifier les remédiations à mettre en œuvre. Cela passe par une connexion permanente avec les équipes IT/métier aux équipes IT afin de pouvoir expliquer et donner du sens à ses actions."*
>
> ■ **Vincent Lefret**

4.4. Convergences & divergences entre organisations

POINTS COMMUNS OBSERVÉS PARTOUT

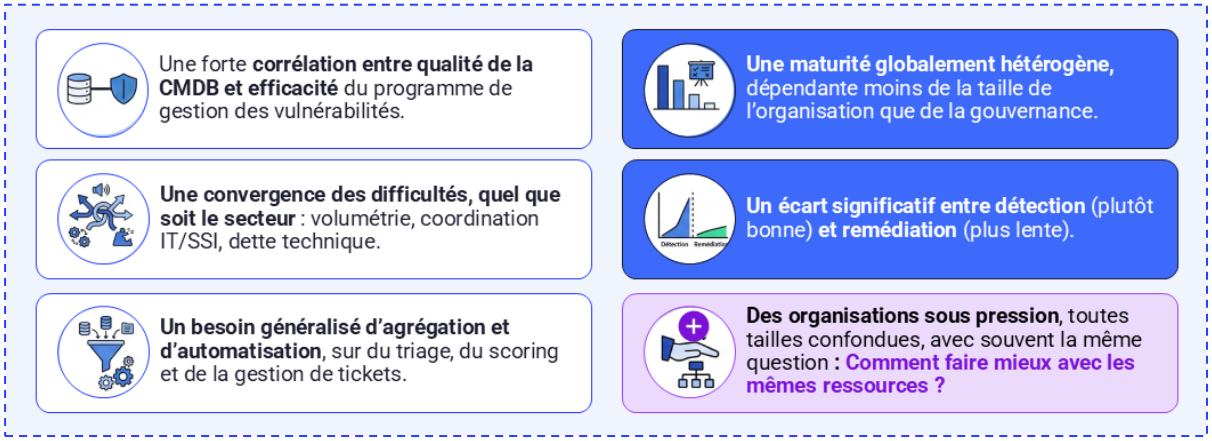
- Le backlog augmente plus vite que la capacité de traitement.
- Les vulnérabilités réellement prioritaires ne sont pas toujours celles qui mobilisent le plus de ressources.
- L'absence de visibilité sur certains périmètres est systémique.
- La remédiation reste dépendante d'équipes IT, trop souvent surchargées.

DIFFÉRENCES SIGNIFICATIVES

- Les grandes entreprises investissent plus en outillage, mais pas forcément en intégration.
- Les PME avancent plus vite sur certains sujets… jusqu'au moment où les volumes explosent.
- Les très grandes institutions sont plus matures sur la gouvernance mais peinent sur les environnements hybrides et internationaux.

4.5. En synthèse

De manière générale, les pratiques actuelles de gestion des vulnérabilités peuvent être résumées dans les tendances suivantes :



5. Bonnes pratiques pour une gestion efficace

> *« Les clés d'une démarche facilitée »*

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS

58%	12%
des organisations pointent ne pas avoir de processus de gestion des vulnérabilités transverse	parmi les 58% n'ont pas de processus formalisé du tout

Les statistiques collectées dans le cadre du sondage du CESIN mettent en lumière le besoin de structuration et de définition des fondamentaux d'une gestion des vulnérabilités réussie. Formaliser le déroulement d'un tel programme est l'une des premières étapes permettant d'adopter une approche systématique et performante.

En un tableau les points clés du chapitre :

PRATIQUE	OBJECTIF
FORMALISER LE PROCESSUS	Clarifier rôles, responsabilités et flux
PRIORISER SELON LA CRITICITÉ ET L'IMPACT MÉTIER	Optimiser l'utilisation des ressources
AUTOMATISER TOUT EN VALIDANT LES POINTS CLÉS	Réduire les angles morts sans introduire de risques
INTÉGRER CMDB / ITSM / SIEM	Éviter les silos, centraliser la connaissance, orchestrer
UTILISER LE VOC COMME CAPTEUR EXTERNE	Détecter shadow IT et actifs exposés
COMMUNIQUER RÉGULIÈREMENT	Assurer l'engagement de la direction et l'alignement des équipes IT
REVOIR ET AMÉLIORER	Cycle d'amélioration continue : s'adapter à l'évolution du SI et des menaces

5.1. Mise en place d'un processus formalisé

Commencer simple et densifier son approche progressivement reste une manière efficace de mettre en œuvre un programme efficace de gestion des vulnérabilités. Commencer simple ne veut cependant pas dire avancer tête baissée. Anticiper le futur de votre programme vous sera systématiquement bénéfique et permettra une adaptabilité et une résilience particulièrement élevées. Ces notions sont à garder en tête à chaque étape de standardisation de l'approche.

Pour tout programme structuré on pourra :

- **Avoir un cycle explicite** : identification des phases de traitement et de leurs critères de passage (voir chapitre 3)
- **Établir les responsabilités :** qui décide, agit et valide (établissement d'une matrice de responsabilité claire)
- **Documenter les procédures :** pas d'ambiguïté dans l'exécution (s'assurer que le cycle pourra être exécuté en toute circonstance)
- **Documenter les politiques :** Découverte, scan, alerting, priorisation, remédiation
- **Former les équipes :** s'assurer d'une compréhension commune, responsable et transverse à l'entreprise (Pas uniquement la SSI mais la SI aussi)
- **Gouverner le processus :** mesurer quelques points clés de la démarche pour en évaluer les effort, points bloquants et améliorations

5.2. Politiques réalistes : Priorisation et Remédiation

Les équipes GRC (Gouvernance, Risque, Compliance) sont la majorité du temps les interlocuteurs établissant les politiques de sécurité pour l'entreprise. Leur politique est bien souvent exigeante mais théorique. Elle définit une manière structurée d'appréhender un risque, avec des délais et des exigences de communication et de mise en sécurité, mais ignore très régulièrement la réalité opérationnelle.

LE DANGER :

- Avoir une politique théoriquement cohérente, opérationnellement inapplicable
- Avoir des délais de remédiation inatteignables pour la SI
- Avoir une politique trop directement liée à des scores techniques ou d'une vision sévérité (pure 'CVSS'), et trop loin de la notion de risque
- Avoir une politique ne prenant pas en compte des composantes environnementales (criticité d'actif, environnement de l'actif, exposition, exploitation d'une vulnérabilité)

LES NOTIONS À PRENDRE EN COMPTE :

1. **« Une » politique de remédiation** qui traite des exigences de la remédiation en fonction d'un risque ou d'une priorité, et non directement en fonction d'un score
2. **« N » politiques de priorisation** permettant de composer entre facteurs techniques (CVSS, EPSS, autres scores) et environnementaux (threat intelligence, criticité d'asset, exploitabilité d'une vulnérabilité) à disposition.

Cela permet d'avoir une politique unique de traitement du risque, et un ensemble de politiques de priorisation qui tirent le meilleur parti de chacun de vos outils, de vos moyens et contextes propres.

> *" Oui pour la recontextualisation/priorisation afin d'être le plus aligné possible avec notre environnement et donc la réalité terrain/IT. Plusieurs déclencheurs :*
> - *La quantité de vulnérabilités qui nous a rendu nécessaire de prioriser au maximum afin de faire traiter dans un ordre de criticité le plus précis possible.*
> - *Réduire le nombre de retours de contestation des équipes en charge des corrections, et ainsi gagner en crédibilité (avoir un maximum d'arguments contextualisés).* "
>
> ■ **François Drouillot**

5.3. Automatisation (scans, patching, alerting)

L'automatisation constitue l'un des leviers les plus puissants pour rendre un programme de gestion des vulnérabilités à la fois scalable, fiable et réactif. Automatiser ce qui peut l'être permet de concentrer les ressources humaines sur l'analyse, la priorisation et la prise de décision — là où la valeur ajoutée est maximale.
L'objectif n'est pas de remplacer le jugement humain, mais de réduire les frictions opérationnelles, supprimer les tâches répétitives et éviter les erreurs manuelles. Un processus trop dépendant de traitements manuels engendre mécaniquement des dérives : retards dans les scans, incohérences entre périmètres, pertes d'informations, difficultés à maintenir un rythme de remédiation soutenu. À l'inverse, un dispositif automatisé permet d'industrialiser la détection, la qualification et la diffusion des priorités, garantissant un cycle de gestion des vulnérabilités réellement continu.

L'automatisation doit s'envisager comme un flux global, couvrant plusieurs étapes du cycle de vie :

- Détection (scans programmés, inventaire continu, synchronisation Cloud)
- Enrichissement & classification (EPSS, KEV, criticité métier, exposition, donnée opérationnelle)
- Orchestration ITSM (création automatique de tickets, priorisation, consolidation)
- Patching & remédiation (déploiement automatisé lorsque possible, intégration à SCCM/Intune, pipelines CI/CD, ou autres outils de patch management)
- Monitoring & alerting (alertes sur dérives, non-conformités, dépassement de SLO, SLA, …)

L'automatisation ne doit pas être pensée comme un "projet IT", mais comme une démarche de maturité alignée sur les objectifs de sécurité de l'organisation. Elle nécessite un pilotage clair, une coordination étroite entre les équipes SSI, IT et DevOps, ainsi qu'une réflexion sur les cas où l'automatisation est pertinente (patchs standardisés, systèmes homogènes, endpoints) et ceux où elle doit rester limitée (applications critiques, environnements industriels, changements sensibles).

Les objectifs :

- Réduire le temps de détection et de propagation des informations critiques
- Diminuer le temps d'instruction et le bruit opérationnel
- Stabiliser les flux de remédiation et lisser la charge des équipes IT
- Améliorer la fiabilité des données et la cohérence entre les outils
- Permettre un pilotage en continu du risque

> *" Un patch management automatique et régulier, permet de traiter les vulnérabilités rapidement après leur détection, voire même par anticipation. "*
>
> ■ **François Drouillot** — CESIN

5.4. Intégration avec les outils de SIEM, ITSM, CMDB

L'intégration de la gestion des vulnérabilités avec les outils existants du SI — SIEM, ITSM, CMDB, outils Cloud, EDR, ou encore solutions de découverte réseau — est un élément structurant pour atteindre une vision cohérente, fiable et actionnable du risque. Sans cette intégration, même les meilleurs outils de scanning produisent une information partielle ou difficilement exploitable, limitant fortement la capacité de priorisation et d'automatisation.

L'objectif est double :

1. Créer un référentiel commun de vérité, partagé par les équipes IT, SecOps et Métiers
2. Fluidifier le cycle de gestion, en évitant les ruptures de charge entre détection, qualification, remédiation et supervision

Une bonne intégration permet de transformer la gestion des vulnérabilités en un processus transverse et orchestré, plutôt qu'en une succession d'actions isolées.

CMDB : SOCLE DE LA PERTINENCE ET DE LA PRIORISATION

La CMDB joue un rôle central en fournissant le contexte nécessaire à la bonne priorisation des vulnérabilités : criticité métier, propriétaire, environnement, dépendances applicatives, exposition, classification des données.

Sans ce contexte, les équipes se retrouvent dans une logique “techno-centrée” où toutes les vulnérabilités semblent équivalentes. À l’inverse, une CMDB bien intégrée permet :

- De contextualiser les actifs critiques pour le métier
- D’écarter les faux positifs liés aux environnements hors périmètre
- D’associer chaque vulnérabilité à un propriétaire d’action clair
- De repérer les angles morts (actifs sans propriétaires, obsolètes, non scannés)

L’intégration doit être de préférence bidirectionnelle :

- Priorité pour la sécurité : la CMDB enrichit l’outil de détection (criticité métier, tags, périmètres)
- Optionnellement : l’outil de détection enrichit la CMDB (inventaire, OS, version, exposition)

Cette interaction permet une gouvernance plus robuste, reposant sur un référentiel unique plutôt qu’une multiplicité de listes.

ITSM : ORCHESTRER LA REMEDIATION ET SECURISER LE PASSAGE A L’ACTION

L’intégration avec l’ITSM est indispensable pour industrialiser la remédiation. Un flux maîtrisé doit permettre de :

1. Générer automatiquement les tickets pour les vulnérabilités prioritaires
2. Les assigner aux bonnes équipes, avec le bon niveau de priorité
3. Suivre le cycle de vie complet : ouverture → remédiation → preuve → fermeture
4. Appliquer les SLO/SLA en fonction du niveau de risque
5. Remonter les blocages structurels (changements refusés, dépendances non gérées, Gestion des exceptions, solutions de contournement)

Une bonne intégration ITSM permet également de détecter les dérives :

- Tickets ouverts sans action, et raisons sous-jacentes
- Retours en arrière, corrections incomplètes
- Saturation des équipes sur certains périmètres

L’ITSM devient ainsi la colonne vertébrale du pilotage opérationnel, en garantissant la traçabilité et la cohérence du processus.

(OPTION) SIEM : RELIER LES VULNERABILITES A DES SIGNAUX D’ATTAQUE

Le SIEM n’est pas directement un outil de vulnérabilités, mais il permet de contextualiser le risque réel en croisant :

- Vulnérabilités détectées
- Exploitations tentées ou réussies
- Comportements anormaux
- Exposition réseau
- Activité d’attaquants sur des failles spécifiques

Cette corrélation apporte une valeur importante :

- Confirmation du risque lorsqu’un asset vulnérable montre des signaux d’attaque
- Priorisation immédiate d’une vulnérabilité exploitée dans l’environnement
- Identification proactive des segments réseau les plus visés
- Réduction du bruit (ne pas traiter en urgence des vulnérabilités hors exposition)

À maturité, le SIEM peut aider à déclencher :

- Des alertes dynamiques en cas d’activité autour d’une vulnérabilité critique,

- Des scans dynamiques en fonction de signaux d'alerte SOC,
- Des workflows ITSM accélérés,
- Ou des mesures compensatoires (blocage d'IP, segmentation, durcissement).

En sommes, scanner les vulnérabilités ne suffit pas ; c'est en partie leur intégration au SI qui crée la valeur. Un programme mature repose sur des flux cohérents reliant la CMDB, l'ITSM et le SIEM, permettant de passer de la détection à l'action de manière fluide et gouvernée.

5.5. Collaboration entre équipes SSI, SI et Métiers

La gestion des vulnérabilités repose sur une coopération fluide entre les équipes IT, la Sécurité et les Métiers. Aucun acteur ne peut, seul, garantir la maîtrise du risque : la SSI apporte l'analyse et la priorisation, l'IT assure la remédiation, et les Métiers arbitrent l'impact et les fenêtres d'intervention. Un modèle de collaboration clair permet de réduire les frictions, d'accélérer les corrections et de stabiliser durablement le processus.

Cette collaboration réussit nécessite :

- Un RACI explicite (qui qualifie, corrige et valide),
- Des rituels réguliers (revue hebdomadaire ou mensuelle opérationnelle, comité mensuel de pilotage),
- Des critères partagés de priorisation et d'escalade,
- Un langage commun, traduisant le risque technique en risque métier,
- Une synchronisation organisationnelle, prenant en compte les contraintes des équipes IT et applicatives.

Une coopération structurée permet de réduire le temps de remédiation, de limiter les retours en arrière et d'améliorer l'acceptation des actions de sécurité. Elle conditionne aussi la qualité du reporting et la crédibilité du programme auprès de la direction.

> *“ Les remontées des pentests, bug bounties, des scanners internes/externes, […] mais également CMDB, SBOM, … ont tendance à noyer les métiers et développeurs, il est important d'avoir une vision globale simplifiée permettant d'être efficace et pragmatique. ”*
>
> ■ **Frank Van Caenegem**
>
> CESIN

5.6. Communication vers la direction (KPIs, tableaux de bord)

La communication vers la direction est un outil de décision, pas un inventaire technique.
Elle doit rendre le risque lisible, prioriser les actions et sécuriser les arbitrages essentiels. Elle permet de rendre visible l'évolution du risque cyber et d'assurer un alignement stratégique entre les équipes techniques et les objectifs de l'entreprise.

Pour être efficace, cette communication doit s'appuyer sur des tableaux de bord structurés, centrés sur quelques indicateurs clés permettant de suivre la trajectoire globale : réduction du risque, maîtrise du backlog, respect des délais de correction, couverture des actifs critiques, ou encore qualité du dispositif de détection.

Le rôle du RSSI est ici d'articuler ces indicateurs dans une logique de gouvernance : montrer les progrès, identifier les dérives, et surtout expliquer les arbitrages nécessaires (ressources, priorités, dépendances IT ou métiers).

Une lecture synthétique des données doit être proposée :

- Réalité du risque (exposition, criticité, signaux de menace),
- Capacité de traitement des équipes,
- Maturité du dispositif,
- Engagements à tenir (SLO, conformité, gouvernance interne),
- Points de blocage structurels nécessitant un appui managérial.

En appuyant et explicitant ces éléments lors d'une instance formelle (comité stratégique ou de pilotage) la direction pourra arbitrer avec une vision éclairée, allouer les ressources nécessaires, et comprendre l'impact des vulnérabilités sur les activités critiques.

Quelques exemples d'indicateurs retrouvés communément :

1/ INDICATEURS DE RISQUE

+ **Exposition des assets critiques**
+ **% de vulnérabilités KEV / exploitables non traitées**
+ **Vulnérabilités exposées à Internet par seuil de criticité ou de risque**
+ **Score de risque consolidé par BU ou application stratégique**

2/ INDICATEURS D'EFFORT (CAPACITÉ & CADENCE)

+ **Temps moyen de remédiation (MTTR) par criticité/priorité**
+ **Flux entrant vs flux remédié (et tendance de backlog)**
+ **Respect des SLO/SLA**
+ **Charge sur les équipes IT / Sécurité.**

3/ INDICATEURS DE SANTÉ DU DISPOSITIF

+ **Taux de scans authentifiés / agents actifs**
+ **Taux de couverture des actifs critiques**
+ **Angles morts détectés et évolution**
+ **Délai entre création d'un asset et premier scan**

6. OUTILLAGE : écosystème de la gestion des vulnérabilités

> *« Fluidifier la mise en action par l'intégration »*

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS
Nombre d'outils de détection de vulnérabilités

15%	85%	Dont 15%
1 OUTIL	> 2 OUTILS	> 5 OUTILS

Le sondage mené par le CESIN montre que la très grande majorité des organisations dispose d'au moins 2 outils de détection de vulnérabilité. Peu ne constitue donc leur vision du risque qu'avec une seule source. Cela souligne la place centrale de l'outillage dans la capacité à détecter des vulnérabilités.

L'écosystème des outils de gestion des vulnérabilités s'est considérablement élargi ces dernières années, au point qu'il peut être difficile pour un RSSI de distinguer les véritables leviers de valeur des simples fonctionnalités marketing.

Pourtant, quatre principes doivent guider toute réflexion sur l'outillage :

1. Les outils ne sont pas une solution en soi : ils ne font qu'accélérer et fiabiliser un processus qui doit déjà être défini
2. Chaque catégorie – scanner, patch manager, outil Cloud, EDR/XDR – ne couvre qu'une portion du cycle de gestion des vulnérabilités, et aucune plateforme n'offre une couverture exhaustive du SI à ce stade
3. Le choix de l'outillage repose donc moins sur une comparaison technique que sur la capacité à identifier ce qui correspond réellement aux périmètres, aux contraintes et à la maturité de l'organisation
4. Enfin, le marché évolue rapidement vers des approches intégrées et convergentes, combinant détection, priorisation, posture Cloud et remédiation automatisée : une tendance qui transforme la manière dont les RSSI doivent envisager la rationalisation et l'évolution de leurs outils. Pour faire écho à certains

6.1. Scanners de vulnérabilités

Pierre angulaire d'un programme de gestion des vulnérabilités, le scanner automatisé permet de traiter de grandes quantités de données, de manière répétée et systématisée.

Il constitue l'un des premiers choix structurants du programme. L'écosystème d'outils est vaste et parfois très polyvalent, ce qui peut donner l'illusion qu'une solution technique permettra de « tout couvrir ». Le principal écueil à éviter est justement de privilégier la technologie avant d'avoir clarifié l'organisation et les processus capables de traiter, prioriser et exploiter la donnée produite.

Le tableau ci-dessous offre une vue synthétique des principales familles d'outils, de leur périmètre de couverture et de l'effort de maintien ou de remédiation qu'ils impliquent généralement.

TYPE DE SCAN	COUVERTURE	EFFORT OPÉRATION	EFFORT REMÉDIATION	MATURITÉ NÉCESSAIRE
AGENT	Systèmes, configurations, services exposés	Faible	OS : Faible APPLICATION Moyen-Élevé	Faible
RÉSEAU (Network)	Systèmes et services exposés	Faible	OS : Faible APPLICATION Moyen-Élevé	Faible
WEB (DAST)	Vulnérabilités applicatives en exécution	Moyen	Moyen-Élevé	Moyenne
ASM /EASM	Exposé à internet (Domaine, Interfaces, web application…)	Faible - Moyen	Moyen	Faible
SAST (Code statique)	Dépendances, code source, patterns dangereux	Moyen-Élevé	Moyen-Élevé	Moyenne
SCA / SBOM (Software Composition Analysis)	Dépendances open-source, bibliothèques tierces, composants vulnérables, licences	Moyen	Moyen-Élevé	Moyenne
CONFIGURATION (CIS Benchmarks, Hardening)	Paramètres OS, applications mal configurées	Faible	Faible-Moyen	Faible
CLOUD (CSPM / CNAPP)	Ressources Cloud, perms excessives, secrets	Faible	Moyen	Faible
OT/IOT	Équipements spécialisés, protocoles propriétaires	Moyen-Élevé	Élevé	Élevée
CONTAINER / IMAGES REGISTRY	Images Docker, manifestes Kubernetes	Faible	Faible-Moyen	Faible - Moyenne

Opérationnellement, et avec des niveaux de maturité différents concernant la vulnérabilité, on retrouve les acteurs suivants par typologie de scan :

TYPE DE SCAN	OUTILS
AGENT	Tenable, Qualys, Cyberwatch, Rapid7, …
RÉSEAU (Network/Agentless)	Tenable, Qualys, Cyberwatch, Rapid7, …
SCAN WEB (DAST)	Tenable, Qualys, Bitsight, Invicti, Rapid7, Burp Suit
ASM / EASM	Tenable, Qualys, Bitsight, GTI, Rapid7, …
SAST (Code statique)	SonarQube, Veracode, Checkmarx, Fortify SCA, GitLab SAST, GitHub CodeQL
SCA / SBOM (Software Composition Analysis)	Qualys, Tenable, Snyk, Mend, JFrog Xray, DependencyTrack, Anchore, GitHub Dependabot
CONFIGURATION (CIS Benchmarks, Hardening)	Tenable, Qualys, Microsoft Defender Basilines, Prowler, …
CLOUD (CSPM / CNAPP)	Wiz, Orca Security, Prisma Cloud, Lacework, Microsoft Defender for Cloud, AWS Security Hub, GCP SCC, Tenable.cs, Qualys.tc
OT/IOT	Qualys, Tenable, Nozomi, Claroty, Armis, …
CONTAINER / IMAGES REGISTRY	Tenable, Qualys, Rapid7, Trivy

6.2. Gestionnaires de patchs

Bien que peu intégrés dans les processus de gestion des vulnérabilités, le patch management est le pont opérationnel entre la détection d'une vulnérabilité et sa remédiation effective. Une alerte doit se traduire en demande de remédiation structurée, puis en déploiement contrôlé de correctifs sur des périmètres hétérogènes.

Processus non trivial, il exige outils adaptés, processus stables et habitudes d'exécution (fenêtres, tests, validations). Les environnements limités à WSUS/SCCM restent Windows centrés et pas en temps réel, laissant de côté les périmètres Linux/Mac, applicatifs, middleware et Cloud ; à l'inverse, la centralisation sur un outil unifié impose une gouvernance et un cadre commun (SLA, rôles, exceptions) pour réellement passer à l'échelle.

Dans de nombreuses entreprises, le patch management est rendu complexe par une organisation en silos :

- Équipes serveurs, réseaux, postes, Cloud, BU… chacune utilisant ses propres outils
- Pratiques différentes selon les équipes, les technologies, les sites ou les prestataires
- Reporting fragmenté et visibilité incomplète
- Incohérences entre processus locaux et exigences globales
- Dépendance forte à certains acteurs, amplifiée par le turnover

Cette fragmentation empêche d'obtenir des indicateurs fiables (taux de patch, MTTR, exceptions) et rend difficile la prise de décision. Passer à un modèle unifié exige une politique globale, une standardisation des pratiques et une intégration ITSM/CMDB/EDR sous sponsoring conjoint du RSSI et de la DSI.
Le succès repose moins sur le choix d'un outil que sur la capacité à casser les silos, harmoniser les méthodes et structurer un rythme commun.

> *“ Les principales difficultés rencontrées dans les entreprises sont les priorisations dans les backlogs déjà bien chargés des équipes, c'est pourquoi un fort sponsoring interne est nécessaire ”*
>
> ■ **Vincent Lefret**

Au bout de la chaîne détection → qualification → priorisation, la remédiation reste l'effort décisif. Lorsque les périmètres sont volumineux, variés et distribués (multi-OS, Cloud, postes distants, environnements applicatifs), disposer d'une capacité de remédiation automatique, large et fiable devient un véritable défi.

C'est là que le patch management — en tant que processus (rôles, fenêtres, tests, exceptions, SLA) et en tant qu'outillage (orchestration, déploiement, vérification) — prend tout son sens. Il doit être abordé comme un complément naturel de la gestion des vulnérabilités, destiné à fiabiliser le dernier maillon :

- Capacité d'action massive et automatisée
- Rapidité de réaction
- Réduction du temps d'exposition
- Remédiation cohérente et traçable à l'échelle de l'entreprise

En conclusion, la gestion des vulnérabilités met souvent en évidence des besoins de patch management, qu'ils soient locaux ou globaux. Pour autant, cette activité ne relève ni du pilotage du programme vulnérabilités, ni des équipes sécurité : elle reste avant tout un domaine d'exécution IT. Le rôle de la sécurité est d'éclairer, orienter et prioriser, tandis que les équipes SI assurent la mise en œuvre — dans une logique de complémentarité plutôt que de transfert de responsabilités.

6.3. Solutions intégrées (XDR, EDR, VMaaS)

La tendance actuelle est clairement à l'agrégation et à l'intégration. Les grands éditeurs cherchent à couvrir un spectre de plus en plus large : les XDR et EDR ajoutent désormais de la surface d'attaque externe, de la CTI et parfois des capacités de vulnérabilités ; les CNAPP vont parfois jusqu'à intégrer des alertes proches d'un EDR, de la détection de vulnérabilités et même de la veille. Cette évolution répond à un besoin constaté sur le terrain : rationaliser, centraliser coûts et efforts, et améliorer la cohérence de la prévention et de la réaction.

Cette convergence s'accompagne aussi parfois de fausses promesses : certains outils prétendent faire du scan de vulnérabilités alors qu'ils ne listent que les packages installés ; d'autres revendiquent scanner les applications web mais se limitent à détecter les port 80/443 ouverts ; d'autres encore promettent de l'orchestration alors qu'ils n'offrent qu'un envoi automatique de rapports.

Chaque solution reste marquée par son origine et son cœur de métier : un outil issu de l'EDR, du Cloud, du DAST ou du CSPM apporte des forces mais aussi des angles morts. Rares sont les outils capables d'unifier véritablement leur modèle de données, et donc leur vision du risque. C'est pourquoi, dans des environnements denses, complexes ou très matures, une approche plus robuste consiste à s'appuyer sur un outil capable d'agréger, d'enrichir et d'orchestrer l'ensemble des sources. Cela permet d'unifier la vue, de rendre la priorisation transverse, et de simplifier des flux de sécurité parfois massifs — sans dépendre d'un seul fournisseur ni d'une seule logique d'analyse.

6.4. Comparatif rapide (prix, performance, intégration) par typologie d'acteur/éditeur

TYPOLOGIE D'ACTEURS	POSITIONNEMENT PRINCIPAL	FORCES CLÉS	LIMITES NATURELLES	INTÉGRATION / ÉCOSYSTÈME	TENDANCE DE PRIX
Scanners historiques de vulnérabilités	Détection infra/app, couverture large, scan authentifié	Maturité élevée, signatures fréquentes, reporting éprouvé	Peu de contexte métier, priorisation parfois limitée, CI/CD variable	Très bonne intégration ITSM/SIEM/EDR	+ +
Plateformes Cloud & Exposure	Analyse d'exposition Cloud, posture CSPM/CNAPP, risques contextualisés	Visibilité rapide, cartographie fine, corrélations Cloud & workload	Moins adaptés aux environnements on-prem, dépendance Cloud-first	Intégrations Cloud natives excellentes	+ + +
Plateformes intégrées "tout-en-un" (EDR/XDR + VM + CTI + posture)	Vision unifiée : détection, vulnérabilités, menace	Consolidation, réduction des angles morts, pilotage centralisé	Intégration souvent moins fluide que promis, maturité inégale selon modules	Forte mais variable selon l'éditeur	+ + + À + + + +
Solutions d'agrégation & orchestration (type Vuln.)	Normalisation, dédoublonnage, corrélation, pilotage risque, unification	Vision unifiée, flexibilité, optimisation transverse	Coût additionnel, dépendance qualité des sources, exige maturité	Excellente interopérabilité multi source	+ + À + + + +
Outils spécialisés App Sec	Analyse code, dépendances, CI/CD	Très efficaces sur leur périmètre, adaptés Dev SecOps	Très silotés, nécessitent orchestration	Intégration CI/CD forte	+ +
Solutions ASM/EASM (Surface externe)	Découverte assets exposés, analyse surface attaque	Très utile pour exposition Internet, visibilité nouvelle	Peu de remédiation native, beaucoup de bruit si mal configuré	Intégration variable	+ + +

En somme :

- Le prix augmente avec la volumétrie, la centralisation, et le niveau d'intégration réel.
- Les solutions spécialisées restent efficaces mais nécessitent un pilotage centralisé.
- Les plateformes intégrées simplifient la lecture mais leur intégration interne est parfois moins aboutie qu'annoncé.
- Les solutions d'agrégation créent de la valeur si l'organisation cherche un point de vérité unique — mais elles ajoutent un coût structurel qui doit être compensé par un gain opérationnel réel.
- Les outils Cloud-first montent en puissance, mais ne remplacent pas encore totalement les scanners traditionnels dans les environnements hybrides.

6.5. Tendances et évolutions

Il ne s'agit plus seulement d'acquérir un scanner performant, mais de définir une trajectoire d'intégration cohérente avec la maturité de l'organisation et ses ambitions de pilotage du risque. L'outillage, bien qu'un vecteur plutôt qu'une fin, reste central. Adapter son choix au regard de sa maturité et de ses cibles d'évolutions permettra d'avoir une approche durable et structurée.

En trois catégories voilà ce qui ressort :

LES APPROCHES CLASSIQUES : FIABLES, EPROUVEES, INCONTOURNABLES

Les scanners historiques (agents, réseaux, config) et les outils de patch management constituent une base solide pour n'importe quel programme. Ils sont stables, documentés, bien intégrés à l'écosystème cyber/IT et permettent d'assurer une couverture minimale et prévisible. Pour les organisations cherchant avant tout la robustesse opérationnelle, ces outils restent un socle indispensable, même si leur capacité à contextualiser le risque est parfois limitée.

LES SOLUTIONS EN PLEINE DYNAMIQUE : CLOUD-FIRST, POSTURE & INTEGRATION ETENDUE

Les plateformes Cloud (CSPM, CNAPP), les solutions ASM/EASM et les suites intégrées XDR/VMaaS gagnent en importance. Elles répondent à un besoin croissant de vision transverse, de contextualisation automatique et de consolidation des signaux techniques. Cette approche attire pour sa promesse de simplification et de rationalisation, mais elle demande un minimum de structuration interne (CMDB fiable, processus de remédiation cadrés) pour produire une réelle valeur. Ces outils ont le vent en poupe, mais leur efficacité dépend de la capacité de l'organisation à exploiter une donnée plus riche et plus volatile.

LES APPROCHES AVANCEES : AGREGATION, ORCHESTRATION ET PILOTAGE UNIFIE DU RISQUE

Les solutions d'orchestration/agrégation représentent l'étape supérieure : elles unifient des sources hétérogènes, éliminent les doublons, construisent une vision globale du risque et soutiennent une priorisation transverse. Elles ne détectent pas, elles structurent. Leur adoption n'a de sens que pour une organisation disposant déjà d'outils multiples, d'un volume conséquent de données sécurité et d'une gouvernance IT/Sécu suffisamment alignée pour absorber une couche supplémentaire. Elles offrent une puissance considérable, mais nécessitent une maturité supérieure pour être réellement utiles, tant en termes de qualité de données, d'intégration que de discipline opérationnelle.

En d'autres termes : la valeur ne vient pas de la nature de l'outil, mais de sa place dans une architecture cohérente. Les organisations qui réussiront à orchestrer cet ensemble plutôt qu'à accumuler des briques isolées disposeront d'un véritable avantage en matière de pilotage du risque et d'efficacité opérationnelle.

7. Tendances et évolutions

> *« L'avenir de la gestion des vulnérabilités »*

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS
Prévisions d'évolutions de la gestion des vulnérabilités dans les 3 prochaines années

46%	49%	42%
Automatisation accrue de la remédiation	Amélioration de la détection ou priorisation via l'IA	Pression règlementaire croissante

Au travers du sondage mené par le CESIN, les RSSI se montrent globalement optimistes, misant sur une meilleure priorisation (IA) et une remédiation plus rapide (automatisation). Une part notable anticipe néanmoins un renforcement des contraintes réglementaires (NIS2, DORA, SOC2…), signe d'un environnement où les exigences de conformité deviennent un levier structurant du pilotage du risque.

Anticiper, c'est donner au programme de gestion des vulnérabilités la souplesse nécessaire pour durer. En adoptant une approche modulaire et transversale, les organisations peuvent intégrer les évolutions technologiques, réglementaires ou opérationnelles comme autant d'opportunités d'amélioration plutôt que comme des ruptures. Les sections suivantes prolongent cette idée en montrant comment transformer une pression croissante en moteur d'innovation et de maturité.

7.1. Vulnérabilité dans tous ses environnements : Cloud, OT/IoT, Code, Audits

La sécurité évolue désormais dans un écosystème où chaque environnement – Cloud, OT/IoT, code applicatif, infrastructures traditionnelles, audits externes – génère son propre flux d'alertes et d'indicateurs de risque. Les organisations ont gagné en visibilité, mais au prix d'une fragmentation toujours plus marquée : technologies différentes, équipes spécialisées, rythmes de déploiement hétérogènes, et sources de détection qui ne se parlent pas spontanément.

Cette multiplication des canaux crée un paradoxe. Plus l'entreprise cherche à affiner sa compréhension du risque, plus elle disperse sa capacité d'analyse.
La question devient alors stratégique :

Comment conserver la pertinence d'approches expertes mais silotées, tout en construisant une vision de risque unifiée, exploitable, et pilotable à l'échelle de l'organisation ?

La tendance du marché esquisse aujourd'hui deux grandes voies, encore imparfaites mais porteuses de possibilités nouvelles :

LES PLATEFORMES INTEGRÉES & POLYVALENTES

Les éditeurs poussent désormais des plateformes couvrant plusieurs domaines de la cybersécurité — vulnérabilités, SOC/EDR/XDR, CTI, analyse d'exposition. Leur promesse est attractive : rationaliser les coûts, centraliser les données et rapprocher la détection du pilotage du risque. Ces approches améliorent clairement l'intégration et réduisent certains angles morts en offrant une lecture plus transversale. Mais leurs limites persistent : l'intégration est souvent moins fluide qu'annoncé, chaque module conservant ses propres contraintes et niveaux de maturité. Les parcours de données restent hétérogènes, et certaines briques fonctionnent encore en silos. Ces plateformes ouvrent la voie à une convergence utile, mais les RSSI doivent les aborder avec discernement : elles progressent, sans constituer encore une solution totalement aboutie.

LES SOLUTIONS D'AGRÉGATION

Certaines solutions se spécialisent dans la normalisation, l'enrichissement et l'orchestration des données issues de multiples sources de détection : elles ne détectent pas, elles centralisent et orchestrent. Elles consolident les résultats, éliminent les doublons, unifient la visibilité et apportent le contexte nécessaire pour piloter la remédiation de manière transverse. Leur force réside dans la flexibilité : l'organisation peut conserver ses outils experts tout en bénéficiant d'un point de vérité unique. Cette surcouche représente un coût supplémentaire, qui ne se justifie que si elle permet réellement de gagner en efficacité opérationnelle — donc en ressources mobilisées — ou d'augmenter la sécurité par une meilleure réactivité et une réduction tangible du risque. Son intérêt dépend fortement de la qualité des données, de la richesse des intégrations et de la maturité des équipes à exploiter cette couche d'orchestration.

7.2. IA & automatisation dans la cybersécurité

L'IA s'impose progressivement comme un accélérateur dans la gestion des vulnérabilités, en aidant à réduire le bruit, à structurer l'information et à améliorer la réactivité. Mais son apport reste très variable selon les usages.

Aujourd'hui, trois axes se dégagent clairement :

- **Ce que l'IA maîtrise déjà :** la synthèse de données massives issues des outils existants (scans, CTI, logs), permettant de dédoublonner, classifier et résumer efficacement l'information. Approche assez intéressante pour le traitement de l'information issue de détection de vulnérabilités.
- **Ce qu'elle commence à bien faire :** relier différents signaux (vulnérabilités, menaces, exposition, métiers) pour faire émerger des risques pertinents et en fournir une explication compréhensible.
- **Ce pour quoi elle n'est pas encore prête :** prédire de manière fiable l'exploitation future d'un actif ou d'une vulnérabilité au niveau d'une détection précise. En somme, elle a beaucoup de mal à interpréter des données sur des critères très techniques et ne peut à ce stade qu'effleurer la surface des possibilités.

En bref, l'IA peut déjà amplifier la maîtrise et accélérer les décisions, mais son potentiel prédictif reste encore limité — et doit être, pour le moment, uniquement utilisée avec discernement et de façon modulaire pour soulager les tâches sans valeur ajoutée, et amplifier les recherches humaines.

Cette analyse prend une approche fonctionnelle et ignore totalement d'autres aspects essentiel sous-jacents : la gestion de l'information, des performances, et des couts associés. Par ailleurs, la vitesse d'amélioration des capacités « IA » incite à rester lucide quant au statut dépeint précédemment tant les possibilités d'action des « IA » évoluent et se fiabilisent vite.

7.3. Règlementation

La pression réglementaire (NIS2, RGPD, DORA, Cyber Resilience Act…) fait évoluer la gestion des vulnérabilités vers un cadre structuré, auditable et démontrable, où la réactivité, la traçabilité et la maîtrise du risque deviennent des obligations autant que des bonnes pratiques. Certains secteurs — finance, assurance, opérateurs critiques, industrie — ont une longueur d'avance, car leurs modèles exigent depuis longtemps des niveaux élevés de conformité et d'évaluation continue. La tendance est désormais à la généralisation de ces standards au reste du marché.

L'Europe avance dans la même direction : harmonisation des pratiques, standardisation des preuves, exigences renforcées pour les chaînes d'approvisionnement, et convergence entre sécurité, résilience opérationnelle et gouvernance technologique. Cette dynamique n'est plus seulement européenne : la Corée en exemple a, en 2024, renforcé ses exigences nationales avec une stratégie cyber recentrée sur la résilience, la coordination inter-agences et des obligations étendues pour les organisations publiques et privées — preuve que la conformité devient un mouvement global, pas régional.

Parallèlement, les certifications deviennent un critère de sélection commerciale : ISO 27001/27701, SOC 2 ou TISAX dans l'industrie, parfois complétées par des exigences non strictement cyber, comme des engagements RSE ou environnementaux. La conformité n'est plus seulement un impératif réglementaire: elle devient un avantage compétitif, structurant des relations client-fournisseur et légitimant les investissements dans un programme vulnérabilités fiable, traçable et mature.

7.4. L'importance croissante de la gouvernance IT

La gestion des vulnérabilités s'inscrit désormais au cœur de la gouvernance IT, car elle influence directement la continuité d'activité, la maîtrise du risque et la capacité d'une organisation à se conformer à des exigences toujours plus strictes. L'époque où l'IT, la sécurité et les métiers fonctionnaient en parallèle touche progressivement à sa fin : la tendance est à une gouvernance unifiée, capable de gérer les interdépendances entre assets, solutions SaaS, Cloud, systèmes métiers, OT et supply chain.

Plusieurs mouvements convergent : d'abord, la nécessité d'une cartographie fiable et continue (CMDB dynamique, ASM/EASM, inventaires Cloud automatisés) pour disposer d'une réalité technique exploitable ; ensuite, la mise en place de processus transverses où les décisions de remédiation, de dérogation ou d'arbitrage ne relèvent plus d'une seule équipe, mais d'un pilotage intégré associant IT, sécurité et métiers. Enfin, l'essor d'indicateurs de gouvernance — exposition réelle, backlog, temps d'amélioration, maturité des processus — impose une vision consolidée pour orienter les investissements et priorités.

À cela s'ajoute une évolution culturelle : la montée du "security as a product", où chaque équipe applicative devient responsable de la sécurité de son périmètre, et où les équipes centrales agissent en soutien, en pilotage et en contrôle. Cette approche, déjà adoptée dans le Cloud et le DevOps, tend à se généraliser.

En somme, la gouvernance IT n'est plus une structure administrative : elle devient un levier de résilience, un cadre d'arbitrage, et un outil d'alignement entre les enjeux opérationnels, réglementaires et sécuritaires. Les organisations qui réussiront cette convergence bénéficieront d'une gestion du risque plus fluide, plus cohérente, et plus durable.

Conclusion

La gestion des vulnérabilités n'est pas un exercice de détection, mais un levier de pilotage du risque. Ce livre blanc montre une réalité commune à toutes les organisations: le volume d'alertes augmente, les environnements se diversifient, et les moyens — humains comme techniques — ne suivent pas toujours la cadence.

Pour rester maîtres de leur exposition, les RSSI doivent donc structurer un modèle qui dépasse les outils et dépasse la seule technique : un modèle où gouvernance, visibilité et priorisation deviennent les véritables multiplicateurs d'efficacité.

➔ Résumé des points clés

DÉMARRER SIMPLEMENT
OUTIL : Peu d'outils de détection, typologie de vulnérabilité 'simple'
POLITIQUE : Concevoir des politiques réalistes
PROCESSUS : Un processus opérationnel complet
ONBOARDING : Sensibilisez vos équipes IT, rien ne peut se faire sans eux
AUTOMATISER & PRÉVOIR LA SUITE
VISIBILITÉ : Outiller le suivi et la vision des risques
AUTOMATISER : Minimiser les traitements récurrents à la main
ANTICIPER : Rendre agile & transverse l'approche
INTERCONNECTER : les écosystèmes (ITSM, CMDB, SIEM, CTI)
DESSINER UNE STRATÉGIE MOYEN/LONG TERME
PLANIFIER : Prendre le temps de monter en maturité: tout n'est pas traitable tout de suite
OPTIMISER : Optimiser vos ressources et vos compétences
DYNAMISER : Assurer un suivi systématique et un support au traitement

➔ Importance d'une démarche proactive

Les vulnérabilités évoluent plus vite que les capacités opérationnelles. Pour monter en maturité, attendre la prochaine alerte critique ou la prochaine intrusion ne suffit plus. Il faut :

ANTICIPER	→	STRUCTURER	→	ORCHESTRER
• Disposer d'une veille ciblée • Comprendre son exposition réelle • Détecter tôt		• Un processus clair • Des rôles définis • Une priorisation alignée avec les enjeux métier		• Automatiser ce qui peut l'être • Intégrer avec la CMDB et l'ITSM • Piloter les actions plutôt que les subir.

Cette posture proactive transforme la gestion des vulnérabilités en mécanisme de résilience continue, capable d'absorber la croissance volumétrique, l'évolution réglementaire et l'hybridation des environnements (Cloud, OT, code, workloads éphémères…)

Le RSSI au centre de la stratégie, il devient l'architecte de ce pilotage.

Non pas comme propriétaire unique de la remédiation — rôle qui appartient à l'IT — mais comme chef d'orchestre d'une mécanique collective impliquant SI, Métiers, gouvernance et direction.
Son rôle évolue vers :

- Définir le cadre et les priorités,
- Créer une vision unifiée du risque,
- Donner du sens et du contexte aux équipes techniques,
- S'assurer que le programme fonctionne même en cas d'absence, de crise ou de changement d'outillage.

Ce n'est pas qu'un sujet technique : c'est un sujet de gouvernance et de pilotage.

➔ Maintenant : Par où commencer ?

Comprenez votre situation actuelle afin de prévoir votre évolution. Tout le monde ne part pas avec les mêmes contraintes, le même historique, ni les mêmes capacités. Chaque approche se ressemble, sans pour autant être la même.

1. **(30-60j) Auditez votre maturité**
2. **(15j) Prévoyez votre évolution**
3. **(45-90j) Déployez de manière ciblée**
4. **(En continue) Sensibilisez les parties prenantes**
5. **(En continue) Optimisez votre chaine de remédiation**

Annexes

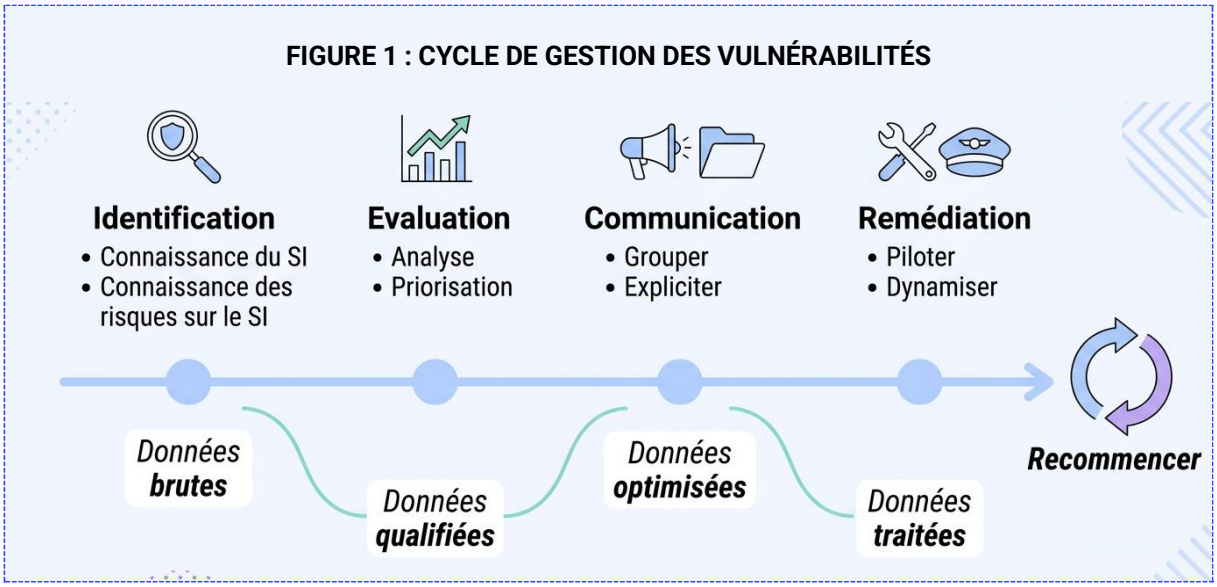
8. ANNEXE 1 : Cycle de vie de la gestion des vulnérabilités

Le paysage des Vulnérabilités est par nature :

- **En évolution constante**
- **Portant un risque modulé à travers le temps**
- **Situationnel, hautement dépendant de l'environnement et de l'industrie dans laquelle on se situe**

La gestion des vulnérabilités n'est pas une activité ponctuelle, mais un processus itératif et continu. Les activités communément identifiées dans un cycle standard de traitement des vulnérabilités sont les suivantes :

FIGURE 1 : CYCLE DE GESTION DES VULNÉRABILITÉS



8.1. Identification

Toute démarche de gestion des vulnérabilités repose sur l'information. Identifier, cartographier et différencier les écarts, vulnérabilités et risques au sein du système d'information exige l'agrégation systématique de données techniques – tant via des flux de renseignements continus que par des cycles de détection spécifiquement structurés.

8.1.1. Veille de sécurité

La veille de sécurité constitue la porte d'entrée en amont de la gestion des vulnérabilités, mais son rôle n'est pas exclusif en la matière. Elle permet d'anticiper l'apparition de nouvelles failles, de surveiller les menaces émergentes, et de détecter rapidement les vulnérabilités qui pourraient affecter le SI de l'organisation. Contrairement aux scans, qui détectent ce qui est présent, la veille détecte ce qui pourrait devenir critique, parfois avant même que des signatures ou des plugins de détection soient publiés.

Une veille structurée doit combiner plusieurs sources :

- Flux officiels : CERT-FR, CISA, ANSSI, éditeurs logiciels, bulletins de sécurité Microsoft/Adobe/Oracle…
- Sources techniques internationales : CVE, NVD, KEV (Known Exploited Vulnerabilities), EPSS (Exploit Prediction Scoring System).
- Menace active : exploitation observée dans la nature, disponibilité d'exploits publics, vulnérabilités dans des produits fortement utilisés par l'organisation.
- Veille contextualisée interne : technologies internes, Cloud provider, composants applicatifs, middlewares spécifiques, versions obsolètes.

Un exemple de veille avec une approche par le risque serait la suivante :

TIER	CATÉGORIE	SOURCE	FRÉQUENCE DE TRAITEMENT TYPE
1	Alertes & Bulletin critiques	Advisory & Alerte CERT FR ANSSI Advisory Editor clés	1X / JOUR
2	Bulletins	Advisory Editeurs autres CISA KEV NVD	2X/ SEMAINE
3	Autres réseaux	Ils publient alertes, synthèses techniques, recommandations et indicateurs d'exploitation.	1X/ SEMAINE

Attention cependant :

- À ne pas vouloir traiter trop d'informations. Les flux sont nombreux et verbeux et peuvent engendrer de la fatigue ;
- Les catégories d'information ne sont pas systématiquement pertinentes et doivent souvent être filtrées automatiquement puis manuellement avant diffusion plus large.

Opérationnellement, une veille réussie permettra de déclencher des actions immédiates (scans ciblés, vérifications manuelles, mesures compensatoire), et apporter une rapidité d'action (remédiation, contournement, mitigation) pour aligner les efforts avec la réalité des menaces.

Elle enrichit par ailleurs les méthodes de priorisation en intégrant les tendances d'exploitation observées, complétant ainsi les scores techniques classiques par une intelligence contextuelle et prospective.

8.1.2. Scans de vulnérabilité

Les scans automatisés constituent le pilier opérationnel de l'identification. Contrairement à la veille pour laquelle le traitement d'information sera fréquemment manuel et théorique, les scans vérifient directement votre SI réel pour trouver d'éventuelles vulnérabilités présentes. Leur finalité : fournir une vision fiable, régulière et exploitable de l'état de sécurité des actifs. Trois facteurs conditionnent leur valeur : profondeur, couverture, cadence.

PROFONDEUR DE SCAN

La profondeur de scan est d'abord un choix d'authentification. Sans authentification (ou agent), la couverture "voit large" mais reste superficielle ; avec authentification, le programme devient actionnable. La précision de la descriptions (versions, packages, …) augmente la fiabilité et la richesse des signaux générés. On évolue d'une vue classique non-authentifié (correspond à la surface d'exposition d'un asset) en se dirigeant vers une vue plus exhaustive de l'état de risque d'un asset.

COUVERTURE DE SCAN

La diversité de nature des actifs appelle directement à l'utilisation de politiques de scan différenciées. Il est peu conseillé d'adresser de la même manière des serveurs de production critiques, des environnements Cloud dynamiques, des postes de travail, des appliances réseau, des environnements sensibles (OT, OT-like, ICS) ou encore des ressources éphémères (containers, workloads auto-scalés). Adapter la politique à la nature et la sensibilité de vos actifs permettra d'avoir une approche optimisée. L'équilibre entre précision et impact sera le maître mot. Des scans trop agressifs ou mal programmés peuvent perturber certains systèmes, alors qu'un paramétrage trop restrictif limite la détection.

Il faudra alors préférer :

- Une segmentation des profils de scan par OS et par fonction, (parfois inutile selon votre outillage, parfois essentiel)
- Une révision périodique des politiques (plugins, configurations ou options avancées)
- Lors de modifications, des tests préalables sur périmètre pilote

CADENCE DE SCAN

La fréquence des scans est un paramètre stratégique. Dans des environnements modernes, la détection ponctuelle (mensuelle/quadrimestrielle) ne permet plus d'identifier les vulnérabilités suffisamment tôt. Une organisation mature adopte un modèle multi-cadencé :

- Serveurs critiques : hebdomadaire ou bi-hebdo
- Postes de travail : hebdomadaire / bimensuel selon capacité
- Cloud & workloads éphémères : découverte et scan en continu
- Exposition Internet : surveillance permanente (external attack surface management)

Ce rythme harmonisé évite les effets "pics de vulnérabilités" et stabilise la charge de remédiation.
En prenant un exemple de modèle multi-cadencé basé sur une approche par le risque, on pourrait choisir les activités suivantes :

TIER	CATÉGORIE DE L'ASSET	EXEMPLES	FRÉQUENCE DE SCAN TYPE
1	**Critique**	Crown Jewels ou Critiques pour l'activité de l'entreprise Surface exposée	1X / JOUR
2	**High**	Production Assets structurant pour l'entreprise	2X/ SEMAINE
3	**Medium**	Assets en lien avec la production Assets dont l'indisponibilité serait problématique mais pas majeure	1X/ SEMAINE
4	**Low**	Le reste des assets	1X/ MOIS

8.1.3. Autres sources : Pentest, bug bounty, CSPM, …

Au-delà des scans classiques, la détection des vulnérabilités s'appuie sur un ensemble de sources complémentaires, permettant d'obtenir une vision plus riche et plus réaliste de la surface d'attaque. Ces sources apportent une profondeur ou un angle que les scanners automatiques ne peuvent pas toujours couvrir, et renforcent la capacité de l'organisation à détecter des failles complexes, contextuelles ou difficiles à automatiser. On peut noter plusieurs catégories :

PENTEST	BUG BOUNTY	CSPM / CWPP / CIEM / ...
• Analyse Humaine, ciblée et réaliste. • Révèle des failles applicatives / logiques, des chaines de vulnérabilités, et des scénrios d'attques réalistes. • Souvent détachés de l'activité de gestion des vulnérabilités, ils peuvent faire l'objet des mêmes mécaniques de traitement et de suivi.	• Détection en continu sur les périmètres exposés, orientée créativité humaine. • Révèle des failles non-standard, des vulnérabilités applicatives complexes, des défauts difficilement automatisables. • Idéal pour les périmètres exposés Internet.	• Visibilité Cloud en continue, configuration, identités et vulnérabilités propre au Cloud. • Révèle les permissions à risque, les ressources exposées, les images, workloads ou autres composants non conformes.

SCA / SAST / DEVSECOPS	AUDITS, SOC, EDR, RETOURS TERRAIN
• Analyse dans le code et les dépendances. Tôt dans la chaine de développement. • Révèle les bibliothèques et dépendances utilisées (SCA), les logiciels et middleware embarqués (SBOM), les écart dans du code (SAST/DAST). • Détection précise et anticipée, réduisant sur le long terme le coût et la charge de correction.	• Détection diverses. • Révèle des tentatives d'exploitation et consolide des constats de conformité ou des reours opérationnels (IT,Applicatid,support, ...). • Aide à détecter les failles invisibles aux outils classiques.

8.2. Évaluation

L'évaluation des données brutes transforme un volume initial et souvent trop verbeux en une priorisation intelligente basée sur un risque « réel » et une capacité de remédiation. C'est ici que se prépare, se groupe, se simplifie la mise en marche de la remédiation. On compose avec score, menace & risque afin d'obtenir une mécanique d'évaluation systématique et optimisée au service de la remédiation.

CRITICITÉ **X** **MENACE** **X** **RISQUE**

8.2.1. Criticité (CVSS, impact métier)

Le score CVSS constitue l'entrée standard de tout programme de gestion des vulnérabilités, offrant une vue initiale sur l'exploitabilité et l'impact théorique via son vecteur (AV, AC, PR, UI, C/I/A, Scope). Bien que perçu aujourd'hui comme rudimentaire, il priorise efficacement l'impact métier potentiel – confidentialité, intégrité, disponibilité.

Limites pratiques majeures :

- Environnemental Score théoriquement prévu, mais quasi-absent en production (complexité, maintenance lourde)
- Contexte métier ignoré : Pas de prise en compte native de l'exposition réelle, criticité business ou configurations spécifiques
- Adoption limitée : <10% des organisations exploitent les vecteurs affinés, faute de données CMDB fiables, d'expertise, et de capacité d'utilisation systématique de la donnée

RÉSULTAT : Une criticité brute, rarement un risque contextualisé. Le CVSS pose les bases, mais exige un enrichissement (EPSS, contexte asset) pour devenir actionnable.

8.2.2. Priorisation (risques vs ressources)

Sans méthodologie formalisée, les équipes font face à un flux ingérable de signaux : tout devient urgent, rien ne l'est plus vraiment. La clé est de passer d'une liste brute de CVE à un cadre de décision structuré, aligné sur la réalité métier et la capacité de traitement.

Le score CVSS apporte une criticité théorique, mais doit être complété par deux dimensions essentielles :

- **Le risque métier**, dépendant de l'industrie, de la criticité applicative, du type d'asset et de l'exposition réseau (une vulnérabilité critique sur un ERP de production n'a pas le même impact que sur un serveur de test isolé)
- **La menace active**, visible via des indicateurs tels que CISA KEV, EPSS, la présence d'exploits publics ou l'activité d'attaquants

Une approche simple mais structurée (ex. : Priorité = Criticité × Risque asset x Menace attaque) permet d'automatiser 80 % du tri et de concentrer l'analyse humaine sur les cas ambigus, tout en offrant une vision centralisée du risque réel et en rendant les SLA/SLO de remédiation plus cohérents.

Par ailleurs, la priorisation doit aussi tenir compte de la capacité réelle de traitement : charge actuelle des équipes, cycles de patching, contraintes applicatives et disponibilités des fenêtres de maintenance. La segmentation en catégories d'action (P1 urgentes exposées, P2 critiques non exposées, P3 importantes planifiées, backlog d'hygiène) permet d'éviter « l'effet liste infinie » et de structurer un plan atteignable.

Enfin, la priorisation vise à fiabiliser l'évaluation, allouer les efforts en fonction du risque effectif, et améliorer l'efficacité opérationnelle en réduisant le MTTR et le bruit, tout en permettant au RSSI d'arbitrer les cas complexes, de cadrer les acceptations du risque et de maintenir un cadre homogène entre sécurité, IT et métiers.

OBJECTIF : passer d'une priorisation générique à un cadre pragmatique qui combine gravité, menace, exposition, valeur métier et capacité opérationnelle, afin de transformer un volume de signaux bruts en plan d'action crédible et soutenable.

8.2.3. Vérification

La phase de vérification transforme les signaux priorisés en données exploitables, éliminant une partie des faux positifs avant remédiation. Sans cette étape, les équipes opérationnelles s'enlisent dans un flux de tâches non pertinentes.

L'enjeu est triple :

- Consolidation : éliminer les erreurs de détection et les doublons, stabiliser le signal.
- Affinage : ajuster la priorisation au plus près de la réalité (exposition, criticité, impact).
- Réalisme : valider le risque effectif et non théorique, afin de calibrer correctement l'effort de remédiation.

Deux approches existent, chacune adaptée à la maturité et à la répartition des responsabilités entre équipes sécurité et opérationnelles. Schématiquement, voilà ce à quoi l'on peut s'attendre :

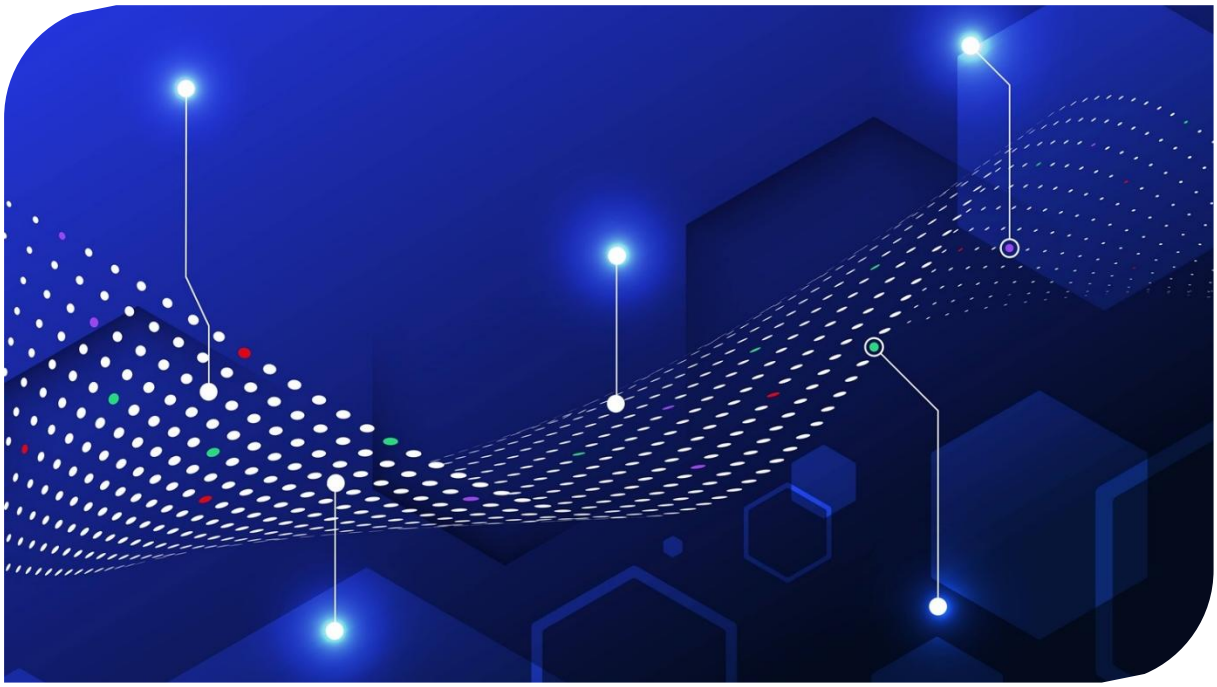
Vérification Minimaliste des équipes sécurités

- Qualité des données : limitée, niveau de confiance faible.
- Charge Métier / Opérationnelle : 40% alloué à de l'effort de vérification / 60% à la remédiation
- Impacts :
  - Court terme : Gain de temps immédiat
  - Long terme : Perte d'adhérence opérationnelle
- Risque majeur : saturation des équipes IT / opérationnelles, perception négative du programme, remédiation qui dérive dans le temps.

Vérification Structurée des équipes sécurités

- Qualité des données : élevée, confiance accrue dans le signal.
- Charge Métier / Opérationnelle : 5% alloué à l'effort de vérification / 95% à la remédiation
- Impacts :
  - Court terme : Mise en place plus longue, charge cyber accrue
  - Long terme : meilleur constance et fluidité dans la remédiation
- Risque majeur : Double charge si la qualité de la vérification n'est pas correctement assurée par l'équipe cyber

En somme, ajouter une étape de vérification à son cycle de gestion des vulnérabilités coutera du temps d'analyse mais permettra de fiabiliser le processus, de réduire le bruit et de gagner en crédibilité à travers de la constance et de la précision.



8.3. Communication et Remédiation

8.3.1. Expliciter les risques & actions de remédiations

La communication vers les propriétaires de systèmes n'est pas une simple notification, c'est un processus structuré pour maximiser compréhension et urgence. Il s'agit de donner toutes les clés pour minimiser l'effort de compréhension et de planification, et maximiser l'action immédiate. Il faut donc que le message soit :

- Clair, compréhensible sur 2 niveaux : synthèse managériale et technique
- Démontrable : Avec une preuve
- Actionnable : Avec des instructions
- Contextualisé/Priorisé : Rappelant le niveau d'urgence

EXEMPLE DE STRUCTURE DU RAPPORT DE VULNÉRABILITÉ

IDENTIFIANT UNIQUE

- **CVE-ID** (ex : CVE-2024-1234)
- *(Optionnel)* **Référence interne** (ex : VUL-2024-001-PROD-APP-01)
- *(Optionnel)* Lien vers une base centralisée de suivi

RÉSUMÉ EXÉCUTIF (1 PARAGRAPHE)

- **Quoi :** type de vulnérabilité en langage simple
- **Où :** système affecté, version
- **Quand :** deadline de remédiation
- **Qui :** propriétaire responsable

DESCRIPTION TECHNIQUE

- **Explication du défaut** (compréhensible par tout le monde)
- *(Optionnel)* **Conditions d'exploitation** (préalables)
- *(Optionnel)* **POC** (Proof of Concept) si applicable

(OPTIONNEL) IMPACT CONTEXTUALISÉ

- **Exemple :** "Une configuration erronée expose des secrets AWS. Risque d'accès Cloud à l'infrastructure"

OPTIONS DE REMÉDIATION

- **Recommandation claire :** Option X est optimale selon contexte Y
- *(Optionnel)* Une explication directe des options à disposition
  - Option A : Patch disponible, version recommandée, lien téléchargement
  - Option B : Contournement temporaire (ex : désactiver fonctionnalité)
  - Option C : Isolation réseau (ex : accès restreint à liste blanche)
  - Option D : Retrait système (si vraiment inutilisable)

DEADLINE / SLA

- **Temps de traitement attendu**

CONTACTS ET ESCALADE

- Contacts à disposition pour poser des questions techniques
- Contacts / process pour placer une demande d'exception (Faux positif, exception traitement, remédiation non applicable, …)
- Point de contact CISO pour les blocages majeurs

RÉFÉRENCES EXTERNES

- *(Optionnel)* Lien vers les ressources connues (e.g. NVD)
- *(Optionnel)* Avis officiel éditeur
- *(Optionnel)* Articles analyse (si pertinents)
- *(Optionnel)* Lien vers la source de détection

8.3.2. Piloter la remédiation

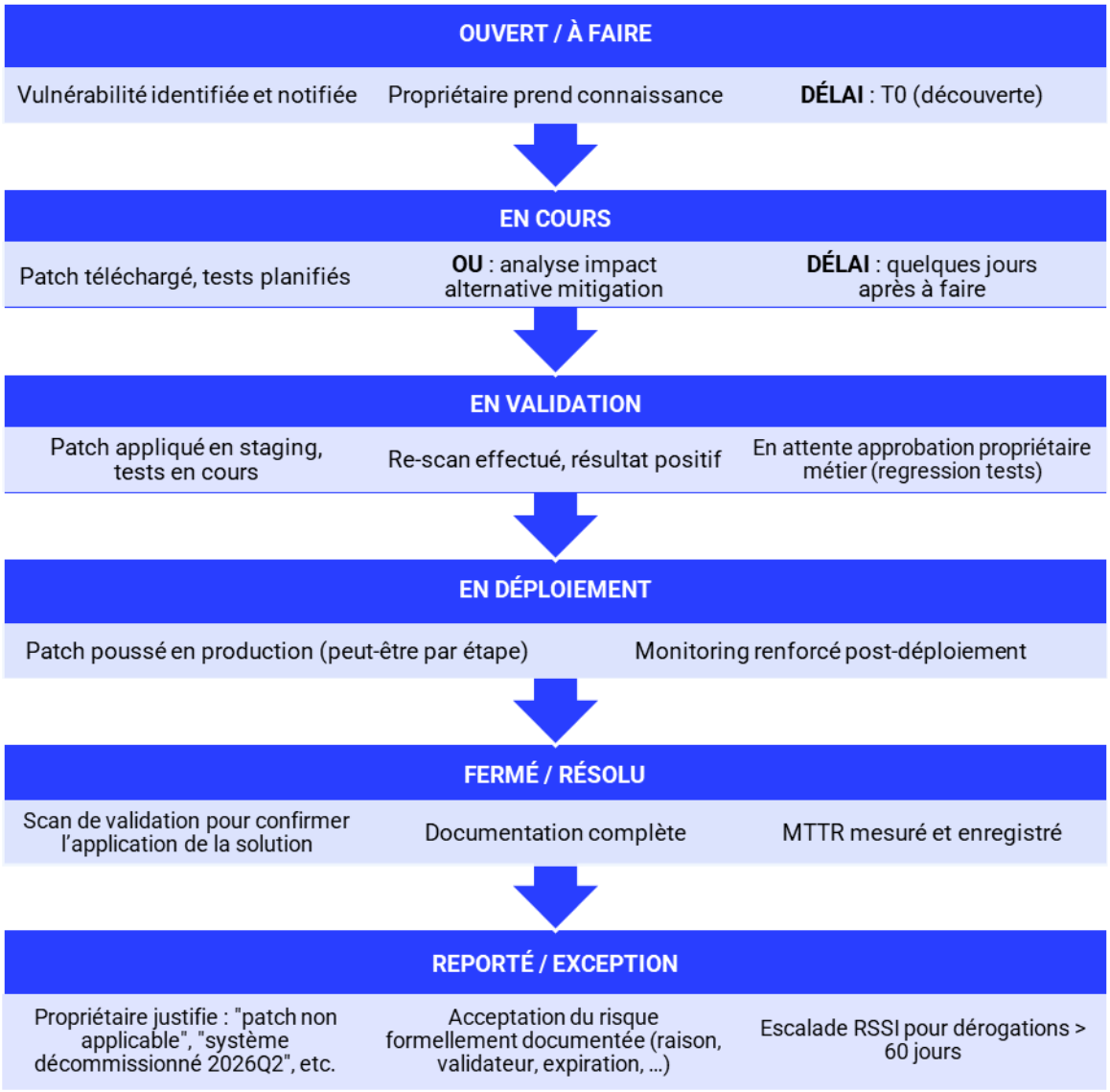
Le pilotage transforme les bonnes intentions en **actions concrètes et mesurables**. Il permet de s'assurer que les demandes de réduction du risque ne restent pas bloquées ou ignorées.

Il est de 2 ordres :

- Technique : S'assurer que les rapports, actions, campagnes sont suivies correctement
- Humain : S'assurer de l'engagement dans la dynamique et les efforts de remédiation

TECHNIQUE

Comme tout suivi d'action on peut prendre en exemple de statut classiques (et en cycle simple) :



HUMAIN

A toute échelle d'entreprise, et quel que soit le processus et le nombre de contrôle implémentés, est nécessaire la mise en place de suivis plus directs, plus humains.

Ils peuvent prendre plusieurs formes :

- Au niveau des interlocuteurs :
  - + Par équipe métier
  - + Par région du monde
  - + Par pôle
  - + Par entité
- Au niveau de la fréquence :
  - + Au déclanchement
  - + A la semaine
  - + Au mois
  - + Au trimestre

L'objet est d'apprendre du terrain et d'itérer sur les capacités en place, afin de faciliter et fiabiliser la montée en maturité de la chaine de remédiation. Cela permet souvent le partage de points bloquants :

- Sujet sous-jacent
- Problème de charge
- Incompréhensions
- Données inexploitables
- Délais opérationnels
- Prestataires externes
- Pas le bon interlocuteur

Sur le long terme, le pilotage deviendra une nécessité. Il permettra d'identifier les blocages, et d'en systématiser leur résolution. Avec quelques exemples :

Blocages courants

- "Patch indisponible" → coordonner avec éditeur
- "Régression connue" → étudier contournement ou attendre version suivante
- "Ressources insuffisantes" → escalade pour déblocage prioritaire
- "Système en retrait" → accélérer retirement

Process d'escalade

- T+10 jours : alerte propriétaire de remédiation ("Rappel de deadline : dans 20 jours")
- T+25 jours : escalade manager propriétaire de remédiation
- T+30 jours (dépassement) : escalade RSSI + équipe gestion des risques

Revue des risques mensuelle

- Revue toutes vulnérabilités en retard
- Décision : accélérer remédiation ou documenter l'acceptation / la modulation du risque
- Présence : RSSI, responsable VOC, propriétaires systèmes critiques

8.3.3. Patch management

Une très grosse partie des vulnérabilités embarquées dans les processus de gestion des vulnérabilités est souvent à traiter via des mécaniques « classiques » de gestion de version de vos OS ou applications. Il s'agit d'une manière simpliste de juste « mettre à jour ». Pour de très nombreuses typologies, ces mises à jour sont automatisables via des outils connus et accessibles. WSUS / SCCM pour Windows, Ansible, des outils de patch management dédiés, …

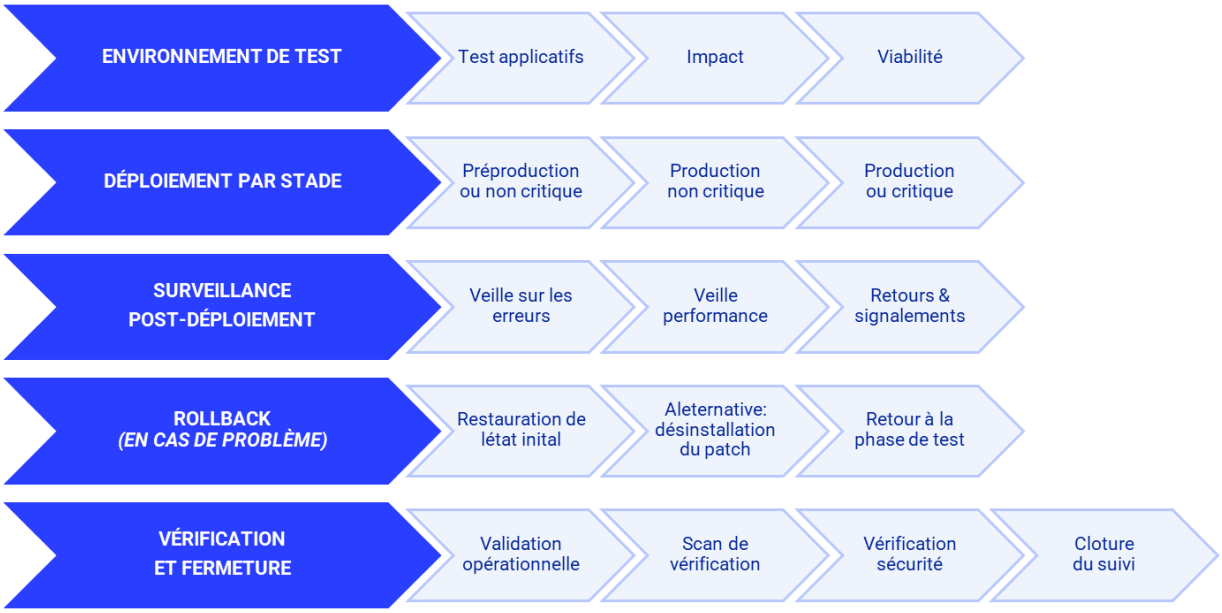
A ce stade, deux points majeurs sont à mettre en lumière pour une efficacité accrue :

- En dehors du programme de gestion des vulnérabilités, avoir des capacités de mise à jour récurrentes ou automatisées
- Intégrer ces capacités dans la mécanique de gestion des vulnérabilités :
    + Identifier ce qui sera traité par une mécanique déjà en place vs pas cadré
    + Identifier les typologies et périmètres qui pourraient faire l'objet d'un ajout dans une capacité de mise à jour existante
    + Identifier ce qui nécessiterait la création d'une capacité nouvelle de mise à jour
    + Identifier ce qui nécessiterait une intervention manuelle ou trop ponctuelle

La compréhension et l'intégration d'un programme de gestion des patchs dans celui de gestion des vulnérabilités apportera des points de progression majeurs :

- Un risque induit minimisé par une action fiable et peu couteuse en ressource
- Une rapidité de réaction élevée puisqu'automatisée ou tout du moins outillée
- Une allocation des ressources sur les situations le nécessitant vraiment, là où seuls les discernements humains, la prise de contexte, et l'ajustement technique peuvent faire la différence

Schématiquement, les cycles de gestions des patchs ressemblent aux points suivants :



8.3.4. Mitigation alternative

Un programme de gestion des vulnérabilités doit pouvoir gérer les exceptions de traitement et avoir la capacité d'indiquer et diriger l'application des mesures de remédiation alternatives. Les déclencheurs peuvent être multiples :

- Solution non-applicable :
    + Raison de disponibilité de l'infrastructure
    + Raison de compatibilité
    + Raison d'interopérabilité
    + Ressources nécessaires (financières, humaines, techniques)
- Solution indisponible
    + Pas de solution connue
    + Pas de patch publié

La direction à emprunter et alors la même que celle qui dirige le programme au complet : minimiser le risque.

On cherche alors dans l'ordre :

- A appliquer une résolution alternative (et permanentes)
  - + Patch en mémoire
  - + Patch fourni par un acteur tier
  - + Modification manuelle
- A implémenter des mesures compensatoires (et temporaire)
  - + Isolement réseau
  - + Désactivation de fonctionnalités
  - + Détection comportementale
  - + Contrôles additionnels
  - + Planification de remplacement

MITIGATION	EFFORT	EFFICACITÉ	COÛT	DURÉE MAX ACCEPTABLE
Isolation réseau	Bas	Haute	Très bas	6-12 mois
Désactiver la fonctionnalité	Très bas	Variable	Variable	Permanent
Détection comportementale	Moyen	Moyenne	Moyen	6 mois
Controls additionnels	Haut	Variable	Haut	3-12 mois
Remplacement du système	Très haut	Très haute	Très haut	6-24 mois

8.4. Surveillance continue

Quel que soit le niveau de maturité atteint, tout programme vise à identifier un risque et à le réduire. Ce processus, long, continu et dynamique, ne peut reposer uniquement sur la bonne volonté pour garantir une constance sur plusieurs années. À des fins de veille, d'alerte et de contrôle, des indicateurs clés doivent être instaurés. Ils permettent de vérifier que le périmètre du programme correspond aux attentes, que la dynamique de détection est opérationnelle, que le risque est identifié et partagé, et que sa réduction contribue activement à diminuer le niveau global de risque.
Les indicateurs proposés dans les sections suivantes constituent des bases adaptables par segment, selon l'organisation interne de chaque entreprise. Ils servent à démontrer et expliquer le bon fonctionnement d'un programme de gestion des vulnérabilités, à justifier son retour sur investissement et à assurer son efficacité dans la réduction proactive des risques.
Quel que soit les typologies d'indicateur il est primordial de respecter les principes suivants :

- Peu d'indicateurs qualitatifs valent mieux que beaucoup d'indicateurs superficiels
- Les indicateurs sont assez rarement implémentables en totalité dans vos outils de détection
- Les indicateurs sont des outils de gouvernance, les tendances valent souvent plus que la valeur brute de la donnée

8.4.1. Indicateurs de risque

Les indicateurs de risque permettent d'évaluer l'exposition réelle de l'organisation face aux vulnérabilités. Ils combinent gravité, exploitabilité, criticité métier et visibilité du périmètre. Le tableau suivant présente des exemples d'indicateurs essentiels à suivre pour prioriser efficacement et détecter les dérives.

NOM	RECO.	MATURITÉ REQUISE	DIFFICULTÉ DE MISE EN PLACE	DIFFICULTÉ DE MAINTIEN
# Vulnérabilités par sévérité	Obligatoire	Faible	Faible	Faible
# Vulnérabilités par risque	Recommandé	Moyen	Moyen	Faible
# Vulnérabilités par Priorité de remédiation	Fortement recommandé	Moyenne-Élevée	Moyen	Faible
# Vulnérabilité exploitée dans la nature concernant son SI	Fortement recommandé	Faible	Moyen	Moyen
# Vulnérabilité exploitée dans la nature dans son industrie	Recommandé	Moyenne	Élevé	Moyen
# Actifs de bordure (exposées à internet) ou critiques	Obligatoire	Faible	Faible	Faible
# Vulnérabilités sur assets critiques & de bordure	Obligatoire	Faible	Faible	Faible
Moyenne de vulnérabilité par actif, par criticité / priorité / risque	Recommandée	Moyenne	Moyenne	Faible

8.4.2. Indicateurs d'effort

Les indicateurs d'efforts seront difficiles à faire comparer par rapport à ses pairs, pour des raisons de confidentialité tout simplement, ou pour des raisons d'incomparabilité : pas les mêmes outils, pas les mêmes process, pas les mêmes découpages opérationnels, pas la même maturité. Il sera alors plus important de connaitre sa propre progression et suivant les tendances plutôt qu'en cherchant à tout pris un comparatif immédiat.

INDICATEUR	RECOMMANDATION	MATURITÉ REQUISE	DIFFICULTÉ DE MISE EN PLACE	DIFFICULTÉ DE MAINTIEN
Réactivité (Time to action)	Recommandé	Faible	Moyenne	Faible
Temps moyen de remédiation	Obligatoire	Faible	Faible	Faible
Demande d'exception rejetées	Recommandé	Faible	Faible	Faible
% de complétion des remédiation	Obligatoire	Moyenne	Moyenne	Faible
% Exceptions documentées & validées	Obligatoire	Faible	Moyenne	Faible
# Ajustement de campagne après communication	Moyenne	Moyen	Moyenne	Faible
% D'automatisation	Moyenne	Moyen	Faible	Moyenne
Jalon d'évolution continue atteints	Obligatoire	Faible	Moyenne	Faible
Temps consacré (Equipe sécurité)	Obligatoire	Faible	Faible	Faible
Temps consacré (Equipes opérationnelles)	Recommandé	Elevée	Moyenne	Moyenne
Ressources techniques allouées (Sécurité)	Obligatoire	Moyen	Faible	Faible
Ressources techniques allouées (Opérationnel)	Recommandé	Moyen	Elevé	Moyenne

8.4.3. Indicateurs de santé

Les indicateurs de santé permettent d'évaluer la qualité et la fiabilité du programme de gestion des vulnérabilités. Ils mesurent non pas l'effort fourni, mais la solidité du processus : couverture, justesse des détections, cohérence des analyses, fluidité de la communication et stabilité du service. Ils aident à identifier les angles morts et à garantir que le dispositif fonctionne de manière régulière et fiable.

CATÉGORIE	INDICATEUR	RECO.	MATURITÉ REQUISE	DIFFICULTÉ DE MISE EN PLACE	DIFFICULTÉ DE MAINTIEN
Détection	% Couverture (scanné vs inventorié)	Obligatoire	Faible	Élevée	Faible
Détection	% D'authentification	Obligatoire	Faible	Faible	Faible
Détection	% Succès scan	Obligatoire	Faible	Faible	Faible
Analyse	% Faux positifs	Moyenne	Moyenne	Moyenne	Faible
Analyse	% Doublons détection	Moyenne	Moyenne	Moyenne	Moyenne
Communication	% De tickets renvoyés pour clarification (incompréhension)	Moyenne	Recommandé	Moyenne	Moyen
Suivi	% De détection en remédiation	Recommandé	Moyenne	Moyenne	Faible
Veille	% Information convertie en action	Moyenne	Élevée	Élevée	Moyenne
Divers	# Nouveaux assets identifiés par le programme	Recommandé	Faible	Faible	Faible
Divers	# D'assets mis à jour dans la CMDB / référentiel	Recommandé	Faible	Élevée	Moyenne

8.4.4. Reporting

Le reporting constitue la synthèse de l'ensemble des indicateurs pour fournir une vision claire et actionnable à chaque niveau de l'organisation. Il doit être adapté à l'audience : granularité détaillée pour les équipes opérationnelles, vue synthétique pour le management, orientation risque et arbitrage pour la direction.
Les rapports doivent être adaptés à chaque audience, et être lisible sur différents niveaux :

- Tactique : opérationnel, granulaire, orienté actions immédiates
  - Cartographie des vulnérabilités par système, par application, par BU, par exposition
  - Rapport de remédiation
  - Action à court terme
  - Ecart et remarques
- Stratégique : synthétique, orienté risque, décision et arbitrage
  - Tendances & Directions
  - Points bloquants
  - Amélioration continue

Un reporting efficace s'appuie sur des représentations visuelles simples, des commentaires interprétatifs et une comparaison dans le temps pour suivre les tendances. Il doit mettre en évidence les priorités du moment, les zones de dérive, les succès obtenus et les arbitrages nécessaires. Le but n'est pas de produire un tableau de bord exhaustif, mais un outil permettant à chacun de savoir quoi faire, où agir, et pourquoi cela compte.

Exemples de livrables :

- Tableau de bord mensuel centralisé (risque, effort, santé)
- Cartographie des vulnérabilités par application, par BU, par exposition
- Alertes automatisées sur dépassement de SLO ou apparition de vulnérabilités KEV
- Synthèse trimestrielle pour COMEX ou Direction des Risques

8.5. Documentation et amélioration continue

IMPORTANCE DE LA DOCUMENTATION

Un processus bien documenté offre trois bénéfices critiques :

- **Scalabilité opérationnelle** : nouveau personnel formé rapidement, absence sans perte de continuité, source de vérité unique
- **Conformité et audit** : preuves documentées de chaque décision, traçabilité complète, évidence des remédiations
- **Consistance** : même procédure appliquée par tous, pas de variation entre équipes, équité des SLA

ÉLEMENTS A DOCUMENTER

Neuf domaines critiques doivent être couverts :

- **Processus général** : diagramme des 5 phases, responsabilités, SLAs, escalade
- **Politiques de scan :** technologies utilisées, périmètres, fréquences, gestion des credentials
- **Politiques de priorisation** : matrice CVSS vs impact métier, formule de scoring, logigramme
- **Politiques de remédiation** : SLA par sévérité, seuil escalade, options de correction
- **Rôles et responsabilités** : matrice RACI (RSSI, responsable Sécurité, analystes, propriétaires des systèmes et applications)
- **Workflows techniques** : intégrations ITSM, CMDB, SIEM, patch management
- **Template de communication :** rapports vulnérabilité, notifications, formulaire d'exception
- **KPI et reporting :** définitions, fréquences, limites, dashboards
- **Glossaire et standards :** terminologie partagée, scores techniques (CVSS, EPSS, …) expliqués, définitions sévérité, priorité

AMELIORATION CONTINUE (EXEMPLE AVEC PDCA) ET GESTION DES CHANGEMENTS

Cycle PDCA :

- **PLAN** (Mensuel) : identifier problème (ex : "MTTR applications 60j, cible 30j"), hypothèse amélioration, baseline, pilot test
- **DO** (1-3 mois) : implémenter, documenter, monitorer, collecter feedback
- **CHECK** (Trimestre) : analyser résultats, quantifier gains, identifier écarts, leçons apprises
- **ACT** (Trimestre) : décision (poursuivre/ajuster/arrêter), scale-up si succès, documenter mise à jour

Exemples d'améliorations typiques : automatisation scans & augmentation de la fréquence (semaine → 24/7), intégration SIEM, automatisation de patch, notifications, déduplication de vulnérabilités,

Message clé : La documentation et l'amélioration continue transforment un processus ad-hoc en système durable. Sans documentation, chaque départ d'équipe perd la connaissance. Sans boucle d'amélioration continue, le processus stagne. Ces deux éléments créent la fondation pour une maturité croissante et une efficacité durable. Tout n'est pas implémentable tout de suite. Meilleure est la qualité du socle de base et plus il anticipe la suite, moins les efforts seront importants sur le long terme. La nécessité d'anticipation est particulièrement essentielle pour les organisations tentaculaires / très matures / avec un programme.

9. ANNEXE 2 : Sondage

Le sondage a été réalisé en partenariat avec le CESIN dont les membres volontaires, principalement composés de RSSI, ont bien voulu accorder du temps au sujet présent : LA GESTION DES VULNÉRABILITÉS.

MERCI au CESIN pour le soutien et l'organisation
MERCI à ses membres pour la participation à cette enquête

Les sections suivantes reflètent une synthèse des résultats consolidés sur l'ensemble des réponses récoltées. Ne sont comptabilisées dans les statistiques à suivre que les réponses ayant dépassées les premières questions de cadrage.

9.1. Profils & segmentation des répondants

RÔLE	NOMBRE	POURCENTAGE
RSSI	143	73%
Adjoint RSSI	15	8%
Responsable IT sécurité	11	6%
Autre	10	5%
Directeur / responsable Cybersécurité	10	5%
DSI	8	5%

Le questionnaire a été introduit auprès des membres du CESIN. Les réponses apportées l'ont été par une sélection de profils aux responsabilités variées.
On relève que la très grosse majorité des répondants ont des rôles ayant la responsabilité de choisir la direction stratégique d'un programme de cybersécurité.

RÔLE	NOMBRE	POURCENTAGE
Industrie	47	24%
Services / ESN	32	16%
Banque / Assurance	28	14%
Secteur public	25	13%
Autre	22	11%
Santé / Médico-social	11	6%
Retail	10	5%
Énergie	6	3%
Commerce/Distribution	6	3%
Logistique/Transport	6	3%
BTP	2	1%
Télécommunication	2	1%

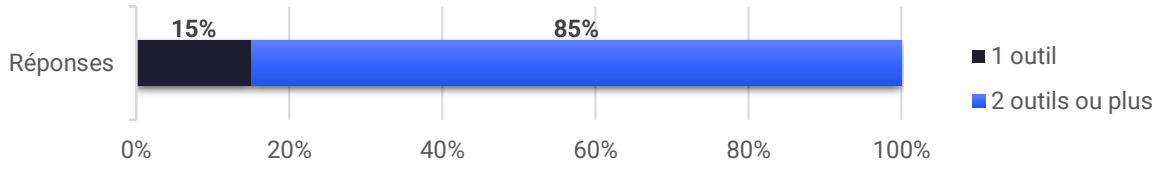
Les domaines représentés par les entreprises associées sont assez diversifiés. L'industrie mène en volume (47) avec une forte portion des entreprises représentées qui se situent dans le secteur tertiaire:

- **Tertiaire : 72,1% (142)**
- **Secondaire : 24,9% (49)**
- **Primaire : 3% (6)**

9.2. Moyens à disposition

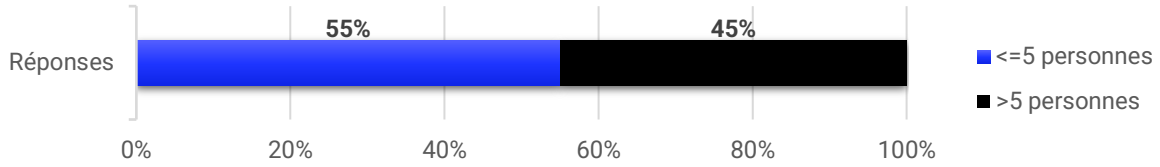
L'enquête a pu montrer une disparité d'équipement et de moyen à disposition pour mener à bien leur programme de gestion des vulnérabilités.

Outils de détection de vulnérabilité à disposition



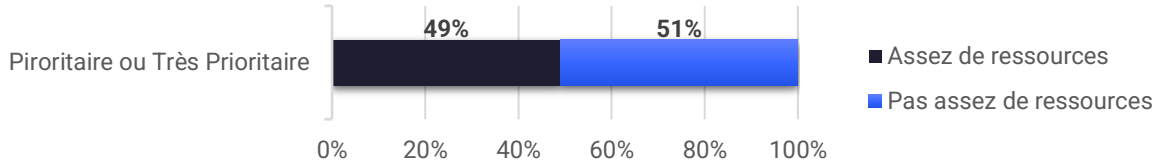
On remarque dans un premier temps que la très grande majorité des organisations ont au moins 2 outils à disposition. Peu ne constitue donc leur vision du risque avec une seule source.

Taille de l'équipe de cybersécurité



On constate dans un deuxième temps qu'une portion significative des entreprises répondantes possède une équipe de cybersécurité conséquente avec plus de 45% ayant au moins 5 personnes (dont parfois plus de 20).

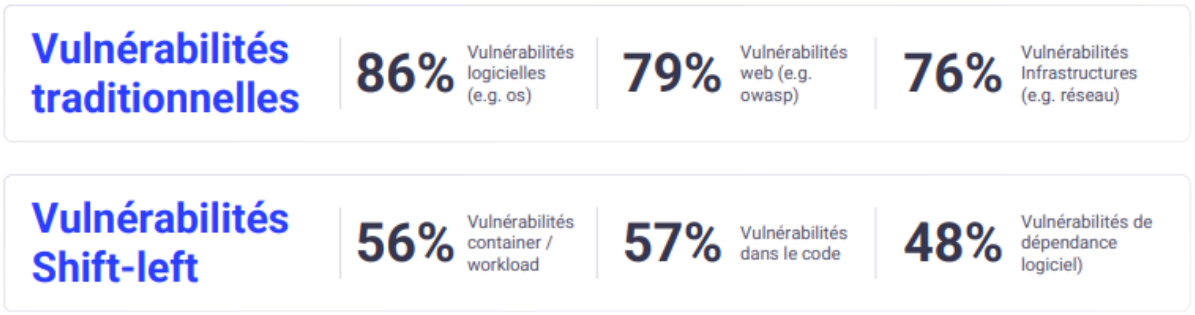
Priorité du programme au regard des ressources à disposition



La moitié des organisations percevant la gestion des vulnérabilités comme prioritaire dit ne pas avoir les ressources ou le budget nécessaire afin de mener à bien cette mission.

9.3. Opérations

9.3.1. Typologie de détection & types de traitements



Typologies de vulnérabilités non-traitées

	RÉPONDANTS	LOGICIELLES (OS, MIDDLEWARE, APPS)	WEB (OWASP)	CONTAINERS / WORKLOADS CLOUD	RÉSEAU / INFRASTRUCTURE
Total Non Traité	**197**	**14,21%**	**20,81%**	**44,16%**	**23,86%**
Total Traité	**197**	**85,79%**	**79,19%**	**55,84%**	**76,14%**

	RÉPONDANTS	CONFIGURATIONS (CIS BENCHMARKS, ETC.)	CODE	DÉPENDANCES (SBOM / OPEN SOURCE)
Total Non Traité	**197**	**45,69%**	**42,64%**	**51,27%**
Total Traité	**197**	**54,31%**	**57,36%**	**48,73%**

Détail des typologies de vulnérabilités non traitées par secteur

SECTEUR	RÉPONDANTS	LOGICIELLES (OS, MIDDLEWARE, APPS)	WEB (OWASP)	CONTAINERS / WORKLOADS CLOUD	RÉSEAU / INFRASTRUCTURE
Autre	**22**	22,73%	45,45%	50,00%	18,18%
Banque / Assurance	**28**	14,29%	10,71%	42,86%	35,71%
BTP	**2**	0,00%	0,00%	50,00%	0,00%
Commerce/Distribution	**6**	0,00%	16,67%	33,33%	33,33%
Énergie	**6**	33,33%	33,33%	50,00%	16,67%
Industrie	**47**	8,51%	21,28%	36,17%	23,40%
Logistique/Transport	**6**	0,00%	16,67%	50,00%	16,67%
Retail	**10**	0,00%	10,00%	30,00%	0,00%
Santé / Médico-social	**11**	9,09%	9,09%	54,55%	27,27%
Secteur public	**25**	28,00%	24,00%	52,00%	28,00%
Services / ESN	**32**	15,63%	18,75%	43,75%	25,00%
Télécommunication	**2**	0,00%	0,00%	100,00%	0,00%

SECTEUR	RÉPONDANTS	CONFIGURATIONS (CIS BENCHMARKS, ETC.)	CODE	DÉPENDANCES (SBOM / OPEN SOURCE)
Autre	**22**	54,55%	63,64%	40,91%
Banque / Assurance	**28**	42,86%	32,14%	53,57%
BTP	**2**	50,00%	100,00%	100,00%
Commerce/Distribution	**6**	33,33%	16,67%	50,00%
Énergie	**6**	50,00%	16,67%	66,67%
Industrie	**47**	44,68%	48,94%	55,32%
Logistique/Transport	**6**	33,33%	16,67%	50,00%
Retail	**10**	40,00%	30,00%	60,00%
Santé / Médico-social	**11**	45,45%	45,45%	45,45%
Secteur public	**25**	52,00%	52,00%	52,00%
Services / ESN	**32**	46,88%	37,50%	43,75%
Télécommunication	**2**	0,00%	0,00%	50,00%

CONCLUSION

- Intégration Dev SecOps encore insuffisante dans les programmes de gestion des vulnérabilités
- Bande passante SecOps saturée, qui freine le traitement des écarts et priorités applicatives
- Les vulnérabilités applicatives ou liées à des environnement éphémères sont plus chronophages à assimiler, prioriser, traiter à cause du fort besoin en contextualisation

9.3.2. Délais de traitement des vulnérabilités critiques

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS
Délais de traitement des vulnérabilités critiques

50%
Expriment le faire en moins de 7 jours

dont **7.6%**
en moins de 24H

CONCLUSION

Étonnant selon notre l'expérience générale :

- Oui, les PSSI tendent souvent à imposer un délai inférieur à 7 jours
- En revanche, les délais de moins de 7 jours ne sont que rarement respectés
  - En particulier lorsque les démarches VOC ne sont pas en place depuis longtemps
  - En particulier lorsque la PSSI a été définie sans alignement avec les capacités opérationnels

La question du biais se pose :

- Est-ce qu'une vulnérabilité critique est définie de la même manière pour chacun ?
- Quelle est la fréquence d'application de stratégies choisissant de moins détecter pour avoir moins de critiques / remédier plus vite ?

9.3.3. Méthodes et moyens de suivi des vulnérabilités

Les participants au sondage dévoilent en très grande majorité avoir défini un processus clair et opérationnel de gestion des vulnérabilités (88%) avec **42%** qui indiquent l'avoir conçu pour fonctionner de manière transverse.

D'un autre côté, afin de suivre la progression de la remédiation :

- **51%** Utilisent des outils de ticketing (ITSM)
- **66%** Utilisent directement leur outil de détection de vulnérabilité
- **24%** Suivent leur traitement au travers de fichier partagé type Excel
- **Plus étonnant, 22% fonctionnent sans tableau de bord ou ITSM.**

CONCLUSION

- Le sujet semble pris en compte mais la méthodologie ne fait pas consensus
- Nous constatons cette multiplicité d'approches sur le terrain, bien souvent liée à la disparité des moyens à disposition et à l'inertie technologique ou organisationnelle de certaines entreprises

9.3.4. Responsabilité finale de la gestion des vulnérabilités : La remédiation

CONCLUSION

- Les acteurs de la cybersécurité ne disposent souvent que d'une partie des leviers nécessaires pour réduire efficacement le risque lié aux vulnérabilités. Le dernier maillon de la chaîne – l'application opérationnelle des correctifs – demeure majoritairement sous la responsabilité des équipes IT opérationnelles.
- Dans ce contexte, la fonction sécurité devient de facto un catalyseur, révélant la nécessité d'une stratégie de patch management réellement transverse. Ce constat est accentué par le sponsoring croissant des outils de patch management par les équipes sécurités / RSSI qui cherchent à structurer et harmoniser cette démarche à l'échelle de l'organisation.

9.4. Stratégie

9.4.1. Modèle d'équipe Cyber & choix organisationnel

42% des répondant on choisit un modèle 100% internalisé, alors que 41% délègue tout ou une partie de leur gestion des vulnérabilités.
Par ailleurs, les entreprises ont plus tendance à faire appel à de l'aide externe lorsque leur taille croît.

SECTEUR	RÉPONDANTS	INTERNE 100%	EXTERNE 100%	DISTRIBUÉ	HYBRIDE (EXTERNE + INTERNE)
TPE (> 250 salariés)	**27**	55%	0,00%	11,11%	29,63%
ETI (entre 251 et 4999 salariés)	**91**	46,15%	7,69%	20,88%	25,27%
Grande entreprise (< 5000 salariés)	**79**	31,65%	2,53%	16,46%	49,37%
Total	**197**	**41,62%**	**5,08%**	**17,77%**	**35,53%**

Corolaire de l'externalisation, les entreprises faisant appel à un modèle hybride comptabilisent plus de personnes dans leurs équipes.

TAILLE ÉQUIPE	RÉPONDANTS	INTERNE 100%	EXTERNE 100%	DISTRIBUÉ	HYBRIDE (EXTERNE + INTERNE)
1 à 2	**59**	47,46%	6,78%	16,95%	28,81%
3 à 5	**50**	46,00%	2,00%	20,00%	32,00%
6 à 10	**33**	42,42%	9,09%	6,06%	42,42%
Entre 11 et 20	**23**	34,78%	0,00%	21,74%	43,48%
Plus de 20	**32**	28,13%	6,25%	25,00%	40,63%
Total	**197**	**41,62%**	**5,08%**	**17,77%**	**35,53%**

CONCLUSION

- Aucune industrie en particulier ne tend vers un modèle particulièrement interne ou externe.
- Les proportions restent approximativement les mêmes, à l'exception du secteur bancaire, qui tends plus sensiblement vers un modèle 100% externalisé que les autres secteurs (14,3% des répondants).
- Les entreprises ont plus tendance à faire appel à de l'aide externe lorsque leur taille croit.
- Le modèle hybride est particulièrement présent dans les tailles d'équipes cybersécurité conséquentes, 6 et +.

9.4.2. Modèle d'équipe IT pour la remédiation

SECTEUR	RÉPONDANTS	DÉCENTRALISÉ / LOCALISÉ	GLOBALISÉ/ CENTRALISÉ & CLUSTERS TECHNOLOGIQUES	GLOBALISÉ/ CENTRALISÉ ET TRANSVERSE	HYBRIDE : DÉPEND DU PÉRIMÈTRE
Autre (veuillez préciser)	**22**	18,18%	27,27%	27,27%	27,27%
Banque / Assurance	**28**	10,71%	32,14%	25,00%	32,14%
BTP	**2**	0,00%	50,00%	0,00%	50,00%
Commerce/Distribution	**6**	0,00%	50,00%	0,00%	50,00%
Énergie	**6**	16,67%	16,67%	0,00%	66,67%
Industrie	**47**	10,64%	17,02%	17,02%	55,32%
Logistique/Transport	**6**	16,67%	33,33%	16,67%	33,33%
Retail	**10**	10,00%	50,00%	20,00%	20,00%
Santé / Médico-social	**11**	0,00%	9,09%	36,36%	54,55%
Secteur public	**25**	4,00%	32,00%	36,00%	28,00%
Services / ESN	**32**	12,50%	15,63%	34,38%	37,50%
Télécommunication	**2**	0,00%	0,00%	100,00%	0,00%
Total	**197**	**10,15%**	**24,87%**	**25,38%**	**39,59%**

SECTEUR	RÉP.	DÉCENTRALISÉ / LOCALISÉ	GLOBALISÉ/ CENTRALISÉ & CLUSTERS TECHNOLOGIQUES	GLOBALISÉ/ CENTRALISÉ ET TRANSVERSE	HYBRIDE : DÉPEND DU PÉRIMÈTRE
TPE (> 250 salariés)	**27**	11,11%	14,81%	55,56%	18,52%
ETI (entre 251 et 4999 salariés)	**91**	12,09%	28,57%	25,27%	34,07%
Grande entreprise (> 5000 salariés)	**79**	7,59%	24,05%	15,19%	53,16%
Total	**197**	**10,15%**	**24,87%**	**25,38%**	**39,59%**

CONCLUSION

- Les modèles d'organisation IT entièrement centralisés ou décentralisés deviennent marginaux. La majorité des entreprises adopte désormais des structures hybrides, mieux adaptées à la complexité des environnements technologiques et à la diversité des besoins métiers.
- La tendance est particulièrement marquée dans les grandes organisations, où la gouvernance, la standardisation et la maîtrise des risques exigent davantage de centralisation. Les modèles hybrides y représentent plus de la moitié des organisations, reflétant un équilibre entre pilotage global, mutualisation des expertises et proximité opérationnelle.
- Les équipes locales conservent cependant un rôle clé : elles assurent la réactivité et l'adaptation aux contextes métier, tandis que les pôles centralisés — parfois structurés en clusters technologiques — garantissent l'alignement, l'efficience et la cohérence globale.

En résumé, l'avenir semble appartenir aux modèles capables de combiner efficacement gouvernance centralisée, compétences mutualisées et capacité d'exécution locale, pour répondre simultanément aux besoins d'agilité et de rationalisation.

9.4.3. Objectifs principaux du programme de gestion des vulnérabilités

Les objectifs sont sensiblement les mêmes en moyennes pour tout le monde :

1. Réduction de la surface d'attaque ;
2. Améliorer la posture de sécurité globale ;
3. Être en adéquation avec les diverses conformités règlementaires ou normatives ;
4. Pouvoir partager des indicateurs auprès de la direction.

On pourra cependant noter que la taille d'entreprise et le secteur peuvent aussi démontrer des priorités légèrement différentes.

- La conformité est légèrement plus mise en avant chez les ESN et sociétés de services et les Télécommunications.
- La réduction de la surface d'attaque et l'amélioration de la posture de sécurité globale prime dans l'Industrie ou les Énergies.

9.4.4. Freins principaux rencontrés

SECTEUR	RÉPONDANTS	MANQUE DE RESSOURCES HUMAINES	BUDGET INSUFFISANT	TROP GRAND VOLUME DE VULNÉRABILITÉS À TRAITER	DIFFICULTÉ À PRIORISER LES ACTIONS
TPE (> 250 salariés)	**27**	55,56%	29,63%	37,04%	29,63%
ETI (entre 251 et 4999 Salariés)	**91**	67,03%	27,47%	47,25%	35,16%
Grande entreprise (< 5000 salariés)	**79**	44,30%	16,46%	60,76%	29,11%
Total général	**197**	**56,35%**	**23,35%**	**51,27%**	**31,98%**

SECTEUR	RÉPONDANTS	MANQUE DE COORDINATION AVEC LES ÉQUIPES IT	OUTILS INSUFFISAMMENT ADAPTÉS	MANQUE DE VISIBILITÉ SUR LES ACTIFS	AUTRE (VEUILLEZ PRÉCISER)
TPE (> 250 salariés)	**27**	3,70%	14,81%	7,41%	7,41%
ETI (entre 251 et 4999 salariés)	**91**	31,87%	10,99%	30,77%	4,40%
Grande entreprise (< 5000 salariés)	**79**	31,65%	12,66%	46,84%	20,25%
Total général	**197**	**27,92%**	**12,18%**	**34,01%**	**11,17%**

SONDAGE CESIN : PANORAMA DE LA GESTION DES VULNÉRABILITÉS
Principaux freins

56%
Expriment manquer d'effectifs

51%
Volumétrie de vulnérabilité trop importante

La tendance nous pousse à plusieurs observations :

- Le manque de ressource se fait ressentir dans toute taille d'entreprise ;
- Le besoin en priorisation d'action n'est pas ressenti comme un problème majeur alors même que le volume de vulnérabilités à traiter est déclaré trop important. Celui-ci croit avec la taille des entreprises ;

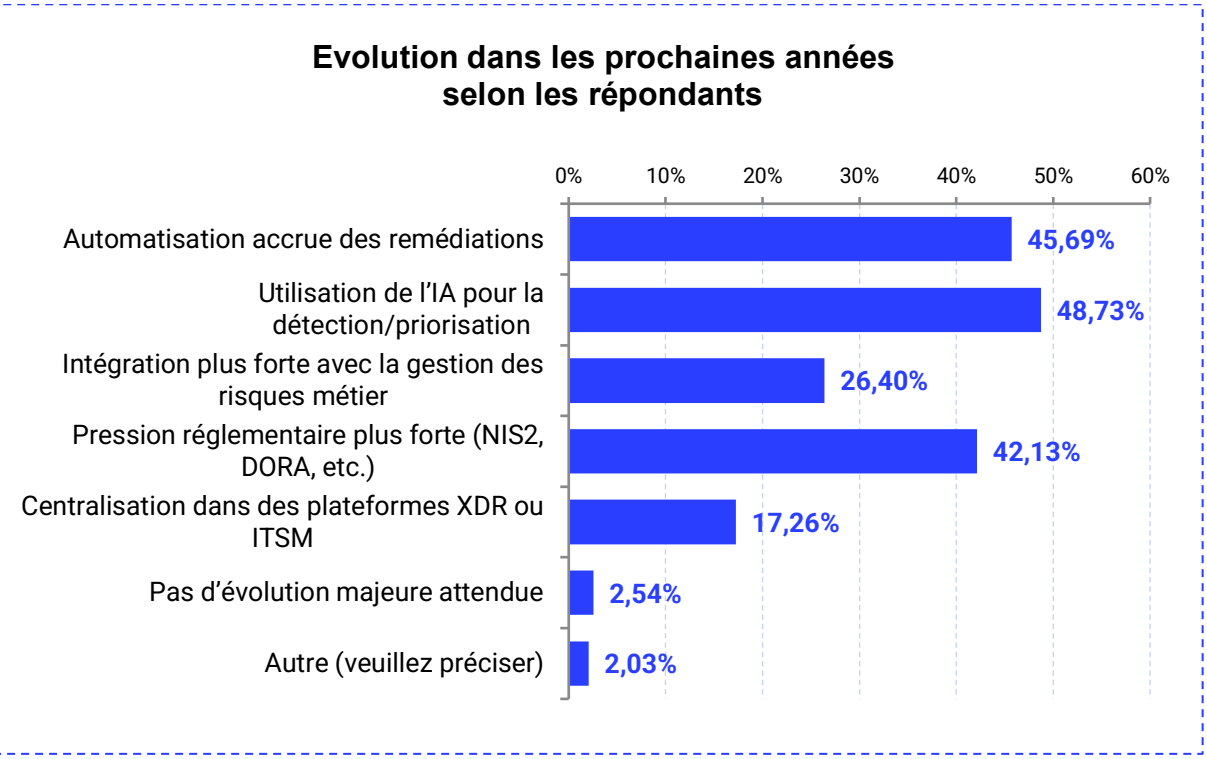
- Les outils et les budgets, bien que notifiés, ne constituent pas les principaux facteurs ralentissant les programmes de gestion des vulnérabilités.

CONCLUSION

- La masse de travail projetée est au-dessus des capacités à disposition au sein d'une entreprise ;
- Les stratégies mises en place ne prennent pas du tout ou pas suffisamment le risque réel, contextualisé ;
- L'effort est donc linéairement dispersé sur une masse à traiter importante, cela génère de la fatigue, et le sentiment de sous-effectif se fait d'autant plus ressentir ;
- La question de l'efficience arrive, et l'une des thématiques principales pour réduire la charge se pose : Comment optimiser les efforts pour réduire au mieux le risque détecté ?
  + Approche par le risque, unification de la visibilité, automatisation, sont des axes de solution.

9.5. Prévisions & évolutions futures

9.5.1. Évolutions des vulnérabilités dans les 3 prochaines années



- 46% des répondant penchent vers une automatisation accrue des remédiations.
- 49% vers une amélioration des capacités via l'utilisation de l'IA.
- Et 42% prévoient une pression grandissante des cadres réglementaires sur la gestion des vulnérabilités.

CONCLUSION

- La majorité des répondant sont optimistes et voient dans le future une amélioration des points difficiles d'une gestion des vulnérabilités efficaces :
  + Une détection et priorisation améliorée (ici par IA), avec parfois une contextualisation avancée (gestion des risques métiers) ;
  + Une remédiation plus rapide et efficiente (ici automatisée) ;

- Une part significative voit aussi leur environnement comme étant progressivement plus contraignant (cadre réglementaire croissant). Cela traduit l'inquiétude à laquelle souhaitent répondre les cadres réglementaires (NIS2, SOC2, DORA, …) et organisation (ANSSI, CESIN, INTER CERT, CERT EU, …) aux missions variées qui se constituent de plus en point de repère dans leur activité propre.

i-TRACING
CYBERSECURITY

En partenariat avec le CESIN

Gestion des vulnérabilités :

Reprenez le contrôle face à l'explosion des vulnérabilités

Face à l'explosion des menaces — plus de 100 nouvelles failles recensées par jour — la prévention technique est devenue le socle de la résilience cyber. Pourtant, les équipes sont en surrégime : l'étude menée par **I-TRACING** et le **CESIN** auprès de 250 RSSI révèle que **56 % des organisations manquent de personnel qualifié** pour absorber ce flux constant.

Le constat est sans équivoque : alors qu'une faille critique est exploitée en moins de 48h, moins d'une entreprise sur dix parvient à la corriger en 24h. Cette tension, accentuée par des outils souvent cloisonnés et une pénurie de ressources, oblige à repenser radicalement l'approche de la remédiation.

Ce Livre Blanc décrypte la réalité du terrain et vous livre les clés pour :

- Transformer vos tableaux de bord en véritables outils de pilotage.
- Structurer une méthodologie cohérente pour vos équipes (VOC).
- Passer d'une gestion subie à une stratégie active de réduction des risques.

CONTACT : infos@i-tracing.com

+33 1 70 94 69 70 - www.i-tracing.com