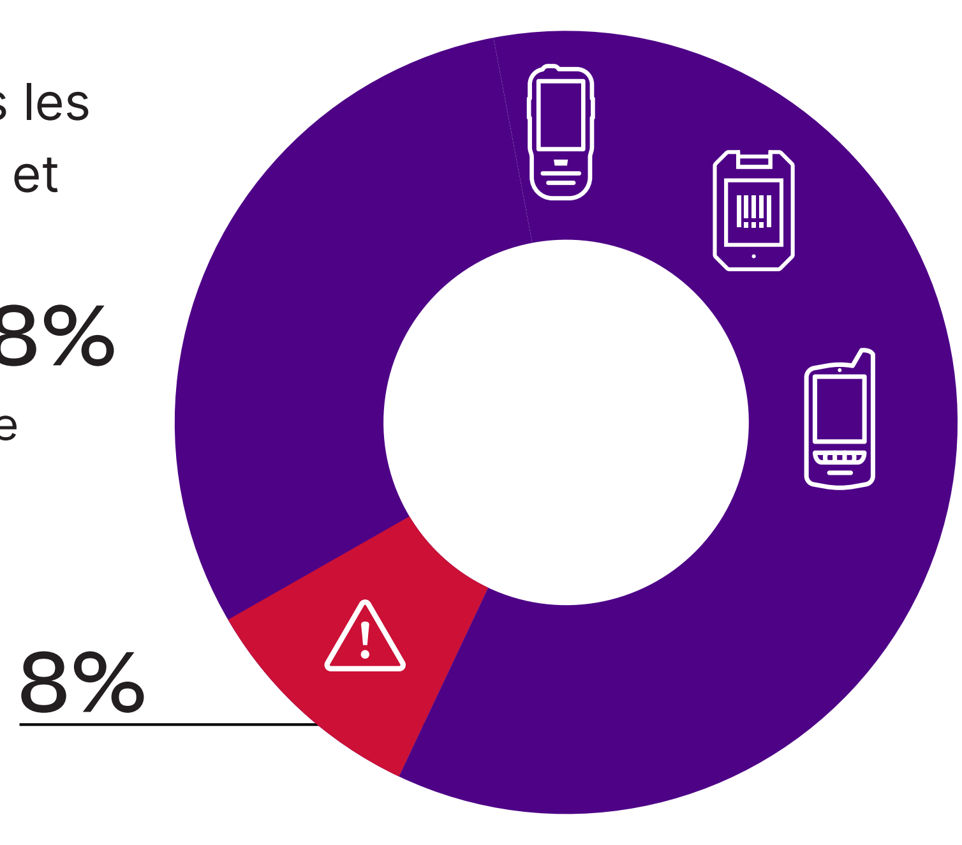
Checklist : 5 points critiques à vérifier concernant la gestion des vulnérabilités

1 Vos angles morts de vulnérabilités

Vous ne pouvez pas protéger et corriger ce que vous ne voyez pas... ou que vous ignorez devoir rechercher.

1 collaborateur sur 3 dans les entreprises Fortune 1000 utilise des applis SaaS basées dans le Cloud non approuvées.[i]

3 des scanners de vulnérabilités les plus populaires (Nessus, Qualys et Nexpose), même combinés, **manquent près de 8%** des vulnérabilités de ransomware connues.[ii]



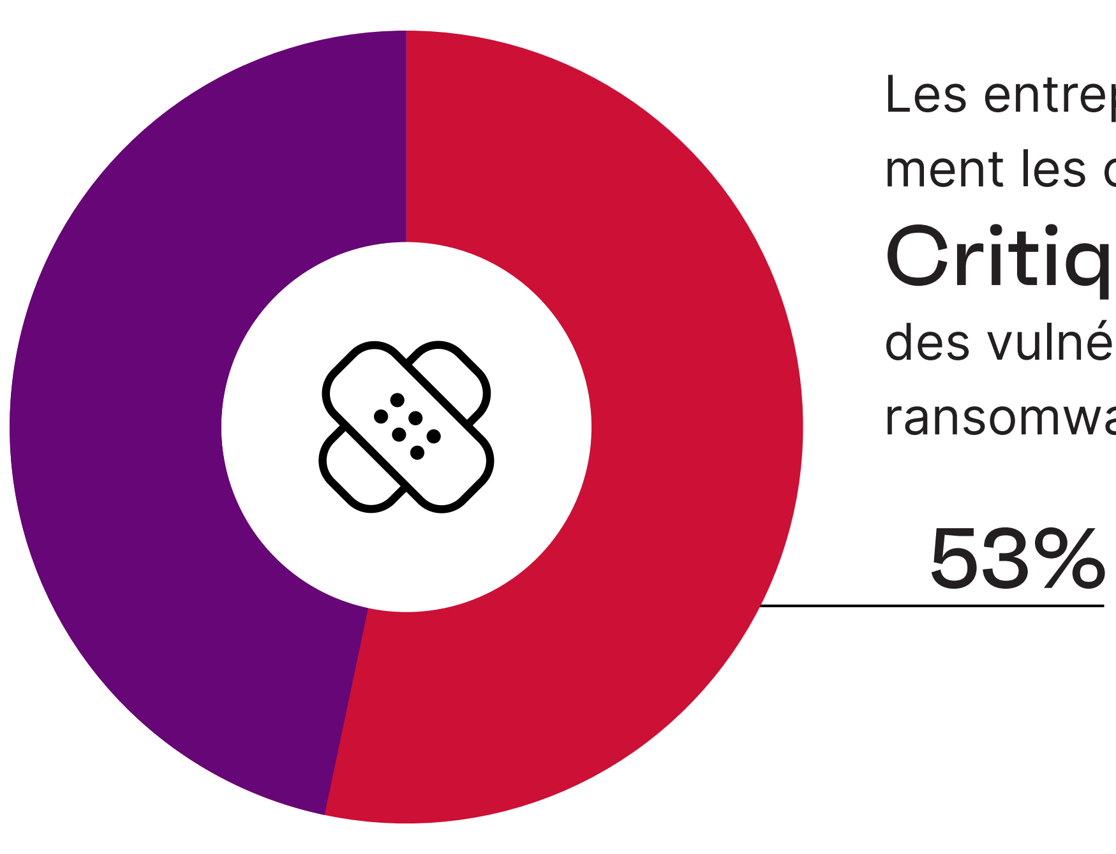
2 Manque de bande passante d'équipe

Imaginez que vous essayiez d'appliquer un correctif à chacun des risques ou vulnérabilités qui existent... ou juste, de passer manuellement en revue les vulnérabilités les plus pertinentes pour votre entreprise et votre environnement.

⚠	⚠⚠	⚠⚠⚠
Plus de 236 000 CVE (Vulnérabilités et faiblesses communes) au total	**Plus de 29 000** CVE militarisées	**Plus de 9 600** CVE dotées de capacités d'exécution de code à distance (RCE) et d'escalade des privilèges (PE)

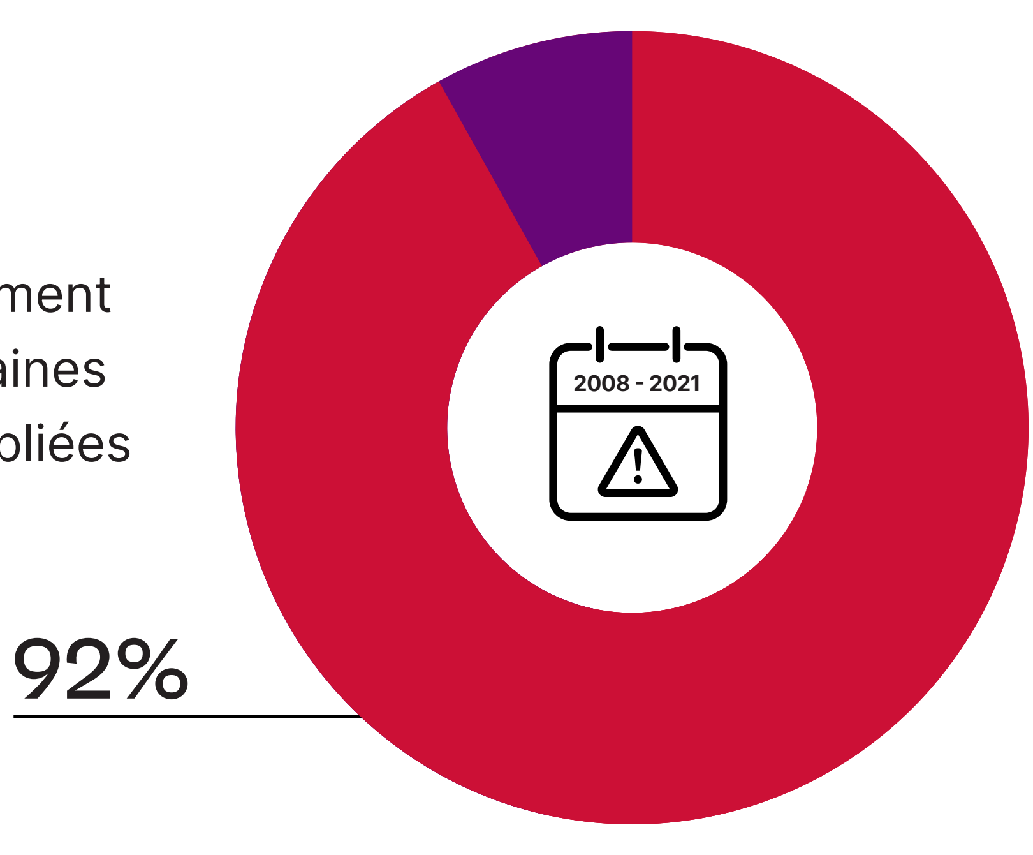
3 Exposition aux CVE moins « critiques » ou plus anciennes

Toutes les vulnérabilités ne présentent pas les mêmes risques... et il est impossible de déterminer celles qui concernent votre entreprise simplement en regardant leur âge ou leur criticité.



Les entreprises qui appliquent uniquement les correctifs des CVE marquées **Critique manquent 53%** des vulnérabilités exploitables liées aux ransomwares.[iii]

92% des vulnérabilités activement datent de plus d'un an... certaines ont même été initialement publiées en 2008 ! [iv]



4 Manque de ressources de programme et d'adoption

RBVM de base

Priorisation via les scores CVSS et scores de scanner

Faiblesses
Très dépendant de la qualité des données et de la fréquence des mises à jour de scanner

Ignore les vulnérabilités à faible score correspondant aux risques propres à l'entreprise

Forces
Existence de la gestion des vulnérabilités

RBVM intermédiaire

Priorisation d'après la probabilité d'exploitation des CVE de l'année écoulée

Faiblesses
Nécessité d'un ajustement et d'une vérification manuels constants

Ignore les vulnérabilités plus anciennes (plus d'1 an) toujours pertinentes

Forces
Priorise la remédiation au-delà du score CVSS

Met en lumière les nouveaux correctifs de vulnérabilité

RBVM avancée

Priorisation à l'aide d'une intelligence issue de plusieurs sources et contextualisation des risques d'entreprise

Faiblesses
Nécessite une suite d'outils complète pour couvrir les différentes sources de données

Forces
Contient toutes les sources possibles de données de vulnérabilité

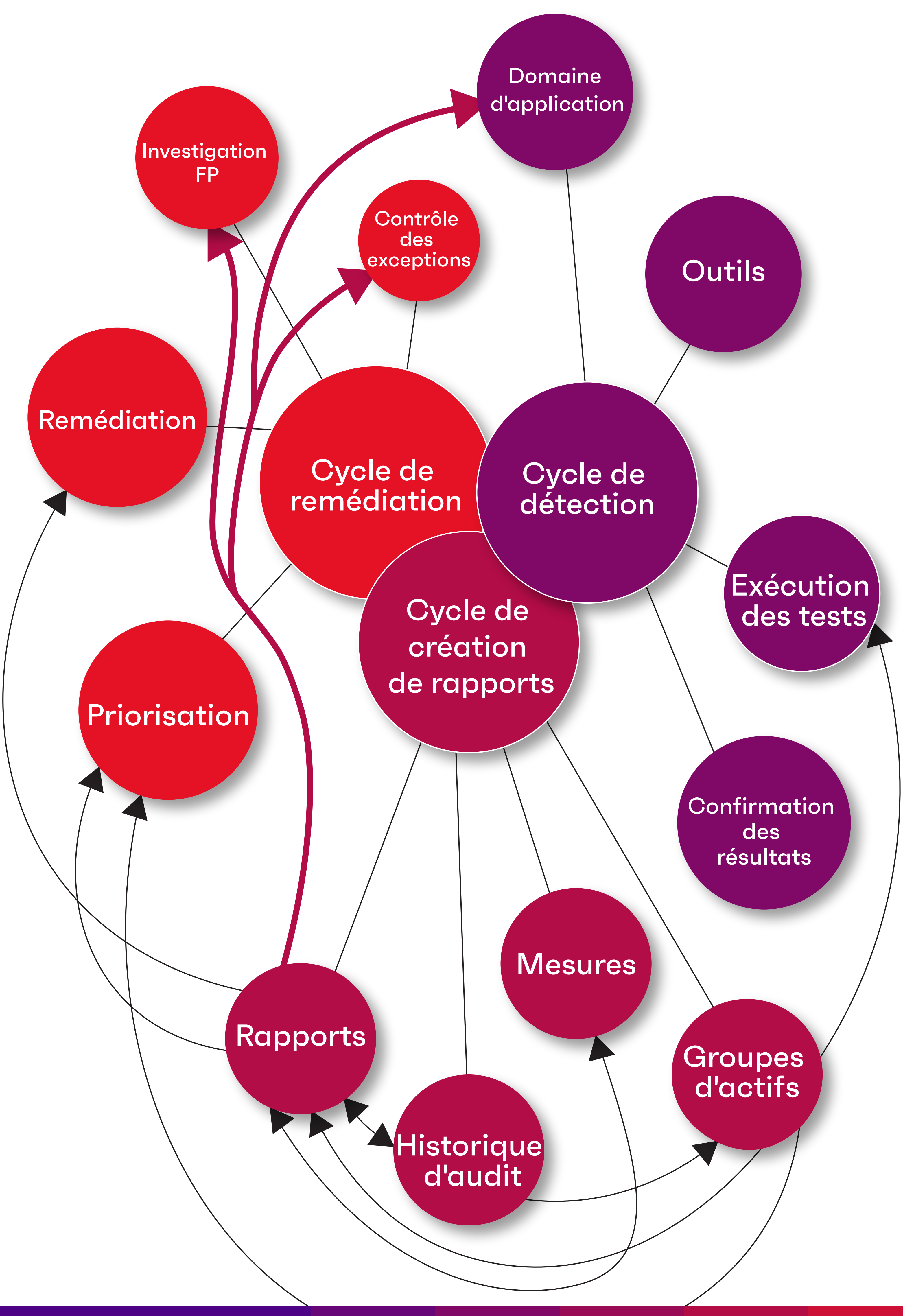
Priorisation basée sur les risques particuliers propres à l'entreprise

Évolue rapidement pour incorporer de nouveaux contextes et affiner la priorisation

5 Analyses et reporting

Les programmes de gestion des vulnérabilités efficaces peuvent créer rapidement le réseau enchevêtré de détections, de remédiations et de rapports interdépartementaux nécessaire pour s'exécuter correctement.

Sans un outil d'automatisation pour regrouper, prioriser et afficher les informations et les activités de vulnérabilités, votre programme de cybersécurité peut être noyé sous les exigences de création de rapports, avant même de commencer.[v]



Mais ce n'est pas une fatalité. Lisez le rapport « 2022 Spotlight Ransomware Report » pour connaître les dernières vulnérabilités en vogue.

Télécharger le rapport

---

i "Why shadow IT is the next looming cybersecurity threat" (The Next Web)
ii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iv Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
v OWASP Vulnerability Management Guide (OVMG) - June 1, 2020