Revue ouverte d'ingénierie des systèmes d'information
2026, vol. 6, n° Spécial INFORSID 2025, 57-97 pages, DOI: 10.21494/ISTE.OP.2026.1449 ISTE OpenScience

Étude sur les ponts entre la sécurité des systèmes d'information et la responsabilité environnementale : le cas de l'optimisation de la gestion des vulnérabilités dans une organisation *Cloud*

A study on the bridge between information system security and environmental responsibility: the case of optimising vulnerability management in a cloud-based organisation

Yann Goetgheluck[1,2], Pierre-Emmanuel Arduin[2], Myriam Merad[1]

[1]Université Paris-Dauphine, PSL, LAMSADE UMR CNRS 7243
[2]Université Paris-Dauphine, PSL, DRM UMR CNRS 7088

RÉSUMÉ. Ce travail examine la sécurité des Systèmes d'Information (SI) comme un pilier fondamental de la continuité et de la résilience organisationnelle. Face aux enjeux croissants liés à la responsabilité environnementale, l'approche du *Vulnerability Management* qui dépasse la seule dimension technique. L'étude propose d'intégrer le contexte métier et les priorités sectorielles dans la hiérarchisation des vulnérabilités, afin d'optimiser l'allocation des ressources et de réduire l'empreinte énergétique des opérations de remédiation. Nous suggérons une extension du modèle CVSS en y ajoutant des critères organisationnels ainsi qu'une analyse du chaînage des vulnérabilités. Cette approche est illustrée à travers des cas concrets (secteurs bancaire, hospitalier et *web*), montrant que la prise en compte du contexte modifie significativement les priorités de remédiation et favorise une sécurité du SI plus durable. L'objectif est de concilier sécurité, durabilité et maîtrise des coûts, en positionnant la gestion des vulnérabilités comme un levier stratégique pour une gouvernance responsable du SI.

ABSTRACT. This paper examines information system (IS) security as a foundational pillar of organisational continuity and resilience. In response to growing environmental responsibility, it becomes essential to adopt a vulnerability management approach that goes beyond purely technical considerations. The study proposes integrating business context and sector-specific priorities into the vulnerability prioritisation process, with the aim of optimising resource allocation and reducing the energy footprint of security remediation. We suggest extending the Common Vulnerability Scoring System (CVSS) by incorporating organisational criteria and analysing vulnerability chaining. This approach is illustrated through practical case studies (banking, healthcare, and websites hosting), demonstrating that contextual factors significantly influence remediation priorities and promote more sustainable cybersecurity practices. The objective is to reconcile security, sustainability, and cost, positioning vulnerability management as a strategic lever for responsible IS governance.

MOTS-CLÉS. Sécurité des systèmes d'information, Responsabilité environnementale, Gestion des vulnérabilités, CVSS, Chaînage des vulnérabilités

KEYWORDS. IS Security, Environmental Responsibility, Vulnerability Management, CVSS, Vulnerability Chaining

Introduction

Le **système d'information** (SI), défini comme un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures) destiné à gérer l'information au sein des organisations (REIX 2004; MASTELIC, OLEKSIAK, CLAUSSEN et al. 2014), constitue la colonne vertébrale de l'activité immatérielle des entreprises modernes (LEGRENZI 2016). En raison de ce rôle central et pour maintenir la **sécurité** et la [résilience] de l'activité de l'organisation, il doit être protégé et maintenu opérationnel. En un seul mot, il doit être **résilient** (REGGIANI 2022). Le **système de management de la sécurité de l'information** (SMSI) répond à cet impératif en protégeant la confidentialité, l'intégrité et la disponibilité

des informations (triade CIA[1]). Les normes ISO/IEC 27001 et 27002 offrent un cadre structuré pour gérer la sécurité de manière continue et adaptée aux risques métiers (WATKINS 2022).

Il convient de préciser que nous employons volontairement le terme sécurité de l'information » plutôt que « cybersécurité » dans cette étude. Cette distinction conceptuelle s'appuie sur les clarifications apportées par VON SOLMS et VAN NIEKERK (2013) qui démontrent que ces deux domaines, bien que liés, ne sont pas analogues. La sécurité de l'information vise à protéger l'information elle-même, considérée comme l'actif principal, contre les dommages potentiels résultant de diverses menaces et vulnérabilités. Selon la norme ISO/IEC 27002, elle consiste en « la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information », quelle que soit sa forme : numérique, papier, orale ou autre (VON SOLMS et VAN NIEKERK 2013). La cybersécurité, est incluse dans la sécurité des SI, elle correspond à la protection du cyberespace lui-même qui comprends la majorité des status de l'information géré par les TIC[2]. On ajoute à cela les utilisateurs du cyberespace dans leur capacité personnelle, sociétale et nationale, incluant tous leurs intérêts, tangibles ou intangibles, qui sont vulnérables aux attaques provenant du cyberespace » . On parle donc ici de sécurité du SI en incluant la cybersécurité, et en se focalisant sur la protection de l'information en tant qu'actif stratégique.

Cette distinction est particulièrement pertinente dans le contexte de notre recherche qui intègre les dimensions métiers, organisationnelles et environnementales du *Vulnerability Management*. En adoptant le prisme de la sécurité de l'information, notre étude se concentre sur la sécurité du SI, permettant d'examiner naturellement comment les priorités organisationnelles (confidentialité bancaire, disponibilité hospitalière, accessibilité *web*) influencent les stratégies de gestion des vulnérabilités, tout en considérant l'impact énergétique et environnemental de ces choix sécuritaires.

Cette approche conceptuelle focalisée sur l'information s'avère essentielle pour développer une vision intégrée conciliant protection informationnelle, performance opérationnelle et responsabilité environnementale dans le cadre spécifique du *Vulnerability Management*.

Nous considérons ici le SMSI comme un pilier du SI, bien que ces composants n'en couvrent pas toutes les dimensions. **La gestion des vulnérabilités**, par exemple, reste principalement centrée sur les aspects techniques, au détriment des facteurs environnementaux et métiers. Ce travail vise précisément à explorer ces dimensions souvent négligées. Par ailleurs, si la sécurité et la performance demeurent les priorités dans la conception des SI, leur dimension **éco-responsable** reste encore largement sous-explorée (CHEN, BOUDREAU et WATSON 2008; MASTELIC, OLEKSIAK, CLAUSSEN et al. 2014). Le concept d'organisation **durable** (STARIK et RANDS 1995) appelle pourtant à mobiliser les SI comme leviers de pratiques plus respectueuses de l'environnement. Certaines initiatives, comme celle menée par le Campus Cyber en partenariat avec le cabinet de conseil Wavestone, tentent de mesurer l'empreinte carbone des SMSI (CYBER4TOMORROW 2025), mais peinent à intégrer d'autres indicateurs environnementaux tout aussi essentiels, tels que la consommation d'eau ou le cycle de vie des ressources numériques. À ce jour, aucune méthodologie éprouvée ne permet de quantifier de manière fiable l'impact environnemental des activités de sécurité du SI au sein des organisations. Les travaux de BERTHELOT et al. (2024) montrent que cette lacune existe également à un niveau plus large, concernant l'évaluation

1. Nous utiliserons la traduction française : Confidentialité (*Confidentiality*), Intégrité (*Integrity*) et Disponibilité (*Availability*).

2. Les Technologies de l'Information et de la Communication (TIC) désignent l'ensemble des technologies utilisées pour. Elles incluent les ordinateurs, les réseaux de télécommunication, les logiciels, les bases de données et tous les équipements numériques permettant la gestion de l'information.

de l'impact environnemental d'un ensemble de services numériques. Leur proposition constitue une première méthodologie en ce sens, mais souffre d'une limite majeure : l'absence de référentiels permettant une comparaison significative. Dans ce contexte, notre recherche s'articule autour de la question suivante : **comment renforcer la sécurité du SI via le *Vulnerability Management* tout en maîtrisant la consommation d'énergie associée au SMSI ?** Nous plaidons pour une amélioration de l'efficience du SMSI, en commençant par sa composante vulnérabilités, et évaluons ses effets sur les ressources à travers trois cas pratiques : une banque, un hôpital et un site *web* vitrine. Pour cela, nous allons étudier 2 méthodes existantes et nous proposerons une troisième méthode dans cette étude. L'objet de cette analyse est d'étudier la possibilité d'associer la sécurité et la durabilité, sans que ces deux concepts s'opposent.

1. Fondements théoriques de la relation complexe mais stratégique entre sécurité et durabilité des SI

La relation entre le SI et la durabilité constitue un domaine de recherche à la fois complexe et prometteur dans le cadre des enjeux durables. Longtemps perçus comme des contributeurs majeurs à l'impact environnemental négatif des organisations, les SI évoluent aujourd'hui pour devenir des leviers stratégiques capables de mesurer, d'analyser et de réduire ces impacts. Dans ces cas là, la sécurité est secondaire à la durabilité, et pour les organisations c'est soit ce cas là, soit la sécurité est une priorité au détriment de la durabilité. Il n'y a pas d'exemple concret d'équilibre entre sécurité et durabilité. Plutôt, comme le suggèrent Chen, Boudreau et Watson (2008), les SI peuvent agir comme des catalyseurs de durabilité, notamment grâce à des outils avancés de modélisation et de suivi de l'empreinte environnementale.

Cependant, les avantages potentiels des SI dans cette transition sont contrebalancés par leur propre impact énergétique. Wang (2021) propose une approche intégrée via une théorie écologique des écosystèmes d'innovation numérique, où les SI sont intégrés dans une dynamique systémique cherchant à équilibrer la performance technologique et les impératifs écologiques. Pourtant, cet équilibre reste fragile. Par exemple, si la dématérialisation — facilitée par les technologies de télécommunication et le télétravail — réduit la consommation de ressources physiques et les déplacements, la croissance exponentielle des besoins en stockage et en traitement des données entraîne une hausse significative de la consommation énergétique. Ce paradoxe se traduit par l'augmentation de la demande en centres de données sécurisés, indispensables à la continuité des services mais également très consommateurs de ressources matérielles et énergétiques, notamment en raison des exigences croissantes en matière de sécurité du SI (Akhter et Othman 2016).

La gestion de la sécurité de l'information illustre particulièrement bien cette tension entre les bénéfices des SI et les coûts énergétiques. Le renforcement des mécanismes de sécurité du SI, bien qu'essentiel, génère souvent une surconsommation d'énergie en raison de l'ajout de dispositifs de protection et de redondances matérielles nécessaires pour garantir la résilience des infrastructures. Par exemple, les centres de données *Cloud*, qui constituent une pierre angulaire de la sécurisation des informations, nécessitent d'importantes ressources énergétiques, malgré les efforts d'optimisation soulignés par Mastelic, Oleksiak, Claussen et al. (2014).

Pour atténuer cet impact énergétique, des stratégies prometteuses reposent sur une hiérarchisation plus précise et personnalisée des vulnérabilités, alignée avec les objectifs spécifiques des organisations. Une priorisation rigoureuse permet non seulement une allocation plus efficiente des ressources, mais aussi une

réponse adéquate aux exigences croissantes en matière de sécurité du SI. À grande échelle, cette approche pourrait conduire à une réduction substantielle de la consommation énergétique des SI. Toutefois, sa mise en œuvre nécessite une réflexion approfondie sur les compromis entre performance écologique et sécurité, ainsi qu'une intégration cohérente des principes de durabilité à long terme dans la gestion des SI.

2. Équilibre entre sécurité et durabilité : un défi conceptuel et opérationnel

La tension entre impératifs de sécurité et responsabilité environnementale révèle une contradiction fondamentale au cœur des SI modernes. Alors que la sécurité exige traditionnellement redondance, surveillance continue et réactivité maximale (NYANCHAMA 2005), la durabilité appelle à l'optimisation des ressources et à la sobriété énergétique (JARVIE 2014). Cette apparente opposition nécessite une reconceptualisation profonde de la gestion des vulnérabilités, s'inscrivant dans les paradigmes contemporains de l'optimisation multi-objectifs sous contraintes environnementales (MADANI et al. 2024; YIANGOU, STYLIANOU et STAVROU 2024), où l'environnement devient une variable active du modèle décisionnel plutôt qu'une simple contrainte passive.

Les travaux récents démontrent que cette convergence entre sécurité du SI et durabilité n'est pas seulement souhaitable mais nécessaire pour un développement durable des infrastructures numériques. MORALES-SÁENZ, MEDINA-QUINTERO et REYNA-CASTILLO (2024) révèlent dans leur revue systématique une interrelation significative entre sécurité du SI et développement durable dans la sphère économique, montrant que la sécurité du SI contribue à la durabilité économique en protégeant les infrastructures critiques et en minimisant les risques financiers. Concernant la durabilité environnementale, ils démontrent que la sécurité du SI facilite l'implémentation de technologies plus propres et plus efficientes, créant un cercle vertueux entre protection et optimisation énergétique.

Cette convergence s'illustre particulièrement dans l'émergence du *Green IT*, défini par YIANGOU, STYLIANOU et STAVROU (2024) comme l'ensemble des pratiques visant à réduire l'impact environnemental des technologies de l'information à travers des pratiques énergétiquement sobres, une gestion durable des ressources et la minimisation des déchets électroniques. Les auteurs soulignent que les pratiques durables en IT peuvent soutenir une sécurité du SI robuste en promouvant l'utilisation de matériel sécurisé et énergétiquement efficient, tout en réduisant l'impact environnemental des incidents cyber (FUSI, JUNG, WELCH 2025). De plus, le travail sécurisé à distance (transport) et le *cloud computing* (mutualisation des ressources) contribuent à réduire l'empreinte carbone, démontrant la synergie entre sécurité du SI et durabilité.

L'application des principes d'optimisation multi-objectifs à la sécurité du SI s'inspire directement de ces travaux récents qui démontrent la faisabilité d'approches bi-dimensionnelles conciliant performance opérationnelle et contraintes environnementales. Les travaux de MADANI et al. (2024) sur l'optimisation de réseaux en boucle fermée utilisant l'IoT[3] illustrent parfaitement cette convergence, proposant un modèle mathématique de programmation linéaire mixte qui minimise simultanément les coûts totaux du système et les émissions de CO_2. Cette approche méthodologique peut être transposée au domaine de la

3. L'Internet des Objets (IoT) désigne un réseau d'objets physiques interconnectés, équipés de capteurs, de logiciels et de technologies de communication leur permettant de collecter et d'échanger des données via Internet (MADANI et al. 2024).

sécurité du SI pour développer ce que nous qualifions de *« Green Vulnerability Management »*. Suivant cette logique, trois approches d'arbitrage entre sécurité et environnement peuvent être conceptualisées.

La première, inspirée des modèles d'optimisation bi-objectifs équilibrés (MADANI et al. 2024), traite la sécurité et l'environnement comme des objectifs de poids équivalent dans une logique de compromis de Pareto. Cette méthode recherche des solutions où aucune amélioration d'un critère n'est possible sans dégradation de l'autre, mais s'avère souvent difficile à atteindre dans la pratique organisationnelle en raison de la criticité des enjeux de sécurité.

La seconde approche adopte une logique hiérarchique contrainte, où la sécurité constitue l'objectif principal sous contraintes environnementales strictes. Cette approche reconnaît la primauté des enjeux de protection tout en fixant des limites écologiques non négociables, reflétant les réalités organisationnelles où la continuité des activités reste prioritaire. Elle s'appuie sur des modèles d'optimisation sous contraintes qui permettent de maintenir un niveau de sécurité minimum tout en optimisant les performances environnementales dans l'espace des solutions réalisables.

La troisième approche, inspirée des travaux de YIANGOU, STYLIANOU et STAVROU (2024) sur l'intégration des compétences sécurité du SI et *Green IT*, mobilise la virtualisation comme technologie centrale qui promeut simultanément la sécurité et la durabilité. Cette perspective intègre l'incertitude comme une composante centrale du processus décisionnel, permettant de développer des stratégies de gestion des vulnérabilités qui restent efficaces même en présence d'informations imparfaites sur les coûts environnementaux réels, tout en améliorant l'efficacité et la scalabilité de l'infrastructure IT.

L'examen des tensions structurelles dans le *Vulnerability Management* révèle des dilemmes particulièrement éclairants qui illustrent ces défis théoriques. Les mécanismes de redondance de sécurité multiplient naturellement la consommation de ressources à travers les systèmes de sauvegarde, la surveillance permanente et les protocoles de chiffrement. Le patching d'urgence consomme significativement plus d'énergie que les mises à jour planifiées, créant un dilemme temporel entre réactivité de sécurité et efficience énergétique. La tendance organisationnelle à « sur-sécuriser » génère des coûts énergétiques substantiels sans apporter de gain réel de protection, illustrant comment l'excès de prudence peut devenir contre-productif sur le plan environnemental.

Paradoxalement, ces tensions ouvrent des opportunités de synergie remarquables qui remettent en question l'opposition traditionnelle entre sécurité et durabilité. Comme le démontrent MORALES-SÁENZ, MEDINA-QUINTERO et REYNA-CASTILLO (2024), une priorisation intelligente des vulnérabilités critiques réduit le besoin de surveillance intensive, démontrant que l'efficacité en sécurité peut s'accompagner d'économies énergétiques. L'automatisation verte, via des scripts de patching optimisés, consomme moins d'énergie que les interventions manuelles répétées, tandis que la consolidation de sécurité permet de regrouper les traitements de vulnérabilités similaires pour optimiser l'utilisation des ressources selon les principes de virtualisation développés par YIANGOU, STYLIANOU et STAVROU (2024).

Pour modéliser cette approche intégrée, nous proposons un cadre énergétique inspiré des travaux de AKHTER et OTHMAN (2016) sur l'allocation raisonnée des ressources dans les centres de données et des méthodes récentes d'optimisation multi-objectifs appliquées aux systèmes IoT (MADANI et al. 2024). Chaque vulnérabilité se voit attribuer un coût énergétique total selon la formule :

$$E_{vuln}(v_i) = E_{detection}(v_i) + E_{evaluation}(v_i) + E_{remediation}(v_i) + E_{verification}(v_i) \quad (1)$$

où chaque composant intègre respectivement les coûts de scan, d'analyse, de correctif et de vérification. Cette quantification permet d'arbitrer simultanément selon quatre critères : criticité, fréquence d'exploitation, priorité métier et impact énergétique, constituant les bases d'un *« Green Vulnerability Management »* comme paradigme émergent d'optimisation multi-objectifs appliquée à la sécurité du SI.

L'intégration opérationnelle de cette dimension environnementale transforme concrètement les stratégies de remédiation selon les approches développées par MORALES-SÁENZ, MEDINA-QUINTERO et REYNA-CASTILLO (2024). Le patching différé intelligent regroupe les correctifs non critiques pour réduire les cycles de redémarrage et optimiser les fenêtres de maintenance, générant des économies substantielles. Le scan programmé adaptatif ajuste la fréquence de détection selon le niveau de risque et la consommation énergétique, évitant les analyses redondantes qui peuvent représenter jusqu'à 30% de la charge de calcul de la sécurité. La priorisation pondérée utilise une matrice de décision multi-critères croisant impact de sécurité et coût énergétique pour identifier les vulnérabilités nécessitant un traitement prioritaire, transformant **la gestion réactive en stratégie proactive**.

Cette approche révèle néanmoins des conflits qui questionnent les fondements de la sécurité du SI et illustrent les limites de l'optimisation multi-objectifs sous-contraintes. Le sujet de la redondance impose que sécuriser implique souvent de dupliquer, créant une contradiction anti-durable difficile à résoudre même avec les outils d'optimisation les plus sophistiqués. Le dilemme temporel oppose l'urgence sécuritaire à l'optimisation énergétique, forçant parfois des choix où l'un prime nécessairement sur l'autre, illustrant les limites pratiques des solutions de compromis théoriquement optimales développées par MADANI et al. (2024). Certaines vulnérabilités « énergétiquement coûteuses » nécessitent des correctifs très énergivores, posant la question fondamentale de savoir s'il est acceptable de maintenir temporairement un risque résiduel pour préserver l'environnement ? Ces tensions soulignent la nécessité d'une réflexion éthique et stratégique profonde sur les priorités organisationnelles, au-delà des simples modèles mathématiques. Elles invitent à repenser la sécurité du SI non pas comme une fin en soi, mais comme un élément intégré dans une vision plus large de durabilité.

Au-delà des aspects techniques, cette transformation nécessite une évolution organisationnelle profonde intégrant les dimensions environnementales et structurelles selon les approches *Green IT* développées par YIANGOU, STYLIANOU et STAVROU (2024). Leur analyse révèle un gap significatif dans les initiatives visant à cultiver les connaissances et compétences liées à la durabilité *Green IT*, à la virtualisation et à la sécurité du SI chez les individus en dehors du domaine informatique. La formation des équipes aux enjeux de sobriété numérique devient essentielle, accompagnée d'une sensibilisation à l'impact énergétique des décisions de sécurité quotidiennes. L'évolution des pratiques vers une « sécurité responsable » implique de redéfinir les indicateurs de performance, d'intégrer des critères environnementaux dans les tableaux de bord sécurité, et potentiellement de créer de nouveaux rôles comme celui de *Green Security Officer* capable d'arbitrer entre impératifs de sécurités et contraintes de durabilité selon des méthodes d'aide à la décision multicritère formalisées.

Cette approche multi-dimensionnelle constitue le fondement d'une sécurité du SI réellement durable, capable de protéger efficacement les organisations tout en respectant ces contraintes. Elle nécessite un changement paradigmatique fondamental : abandonner la logique de maximisation de sécurité au profit d'une optimisation sous contraintes environnementales, transformant la conception même de la protection des systèmes d'information pour l'adapter aux défis contemporains de durabilité selon les principes établis par MADANI et al. (2024) dans leurs travaux sur l'optimisation multi-objectifs des systèmes IoT

durables et les recommandations stratégiques de MORALES-SÁENZ, MEDINA-QUINTERO et REYNA-CASTILLO (2024) pour une convergence effective entre sécurité du SI et développement durable. Pour étudier cela, nous devons d'abord proposer un cadre de recherche exploratoire au travers d'un composant du SMSI : le *Vulnerability Management*. Ou comment améliorer la gestion des vulnérabilités pour répondre aux objectifs multicritères de sécurité et de durabilité.

3. Proposition d'un cadre de recherche exploratoire

Cette étude adopte une approche inductive, l'ITDTA (*Inductive Top-Down Theorizing Approach*), ancrée dans la tradition pragmatiste (SHEPHERD et SUTCLIFFE 2011). Elle vise à faire émerger des concepts théoriques à partir de l'analyse exploratoire de données empiriques, plutôt qu'à tester des hypothèses préexistantes. Le point de départ est ici le *Vulnerability Management*, utilisé comme prisme pour explorer les impacts de dimensions complémentaires, notamment environnementales et métier. Pour classifier les critères de criticité des vulnérabilités, une méthode itérative de type Delphi (ROWE et WRIGHT 1999) sera mobilisée. Ce processus s'appuie sur les avis d'un panel d'experts, recueillis via plusieurs cycles anonymes afin de converger vers un consensus. L'analyse suivra une logique d'allers-retours entre données et cadres théoriques, assurant une compréhension ancrée dans les réalités observées (SHEPHERD et SUTCLIFFE 2011).

Le **SMSI** repose sur trois composantes principales dont les interrelations sont expliquées dans la littérature par NYANCHAMA (2005), MEYER, HEININGER et STARY (2024), ainsi que par les normes ISO/IEC 27001 :2022 et 27005 :2022, comme illustré dans la Figure 1 :

— **Gestion des menaces** (*Threat Management*) : consiste à identifier et à définir les vecteurs et types d'attaques susceptibles de cibler le système d'information (STRACHAN-MORRIS 2012)
— **Gestion des vulnérabilités** (*Vulnerability Management*) : vise à détecter et analyser les vulnérabilités pouvant être exploitées par ces menaces à des fins malveillantes.
— **Gestion des risques** (*Risk Management*) : constitue la pierre angulaire du SMSI, en s'appuyant sur les éléments issus des deux processus précédents pour évaluer les risques pesant sur l'ensemble du système d'information de l'organisation.

Cependant, dans la littérature scientifique, le SMSI est souvent réduit à sa seule composante de gestion des risques comme en témoigne la figure 2 tirée des travaux de AL-DHAHRI, AL-SARTI et ABDAZIZ (2017). Cette vision réductrice présente des limites significatives, dont l'une des plus importantes est le manque d'informations fournies par le *Vulnerability Management*. Bien que certaines recherches, telles que celles de (NYANCHAMA 2005), tentent de relier le *Vulnerability Management* à l'ensemble des dimensions du SI. En pratique, ce processus est encore largement cantonné à la gestion des systèmes informatiques. Cette focalisation sur le seul aspect technologique conduit à négliger deux dimensions essentielles du SI : l'aspect métier, qui reflète les processus stratégiques des organisations, et l'aspect environnemental, qui englobe les interactions des individus avec le système. Cette lacune, partagée aussi bien dans les travaux académiques que dans les pratiques des entreprises, limite l'efficacité globale du SMSI et constitue un frein à l'intégration d'une approche plus holistique de la sécurité des systèmes d'information.

Les travaux de CHOI et LEE (2015) apportent une contribution novatrice au *Vulnerability Management* en intégrant la dimension métier dans leur approche. Alors que les méthodologies classiques, telles que le

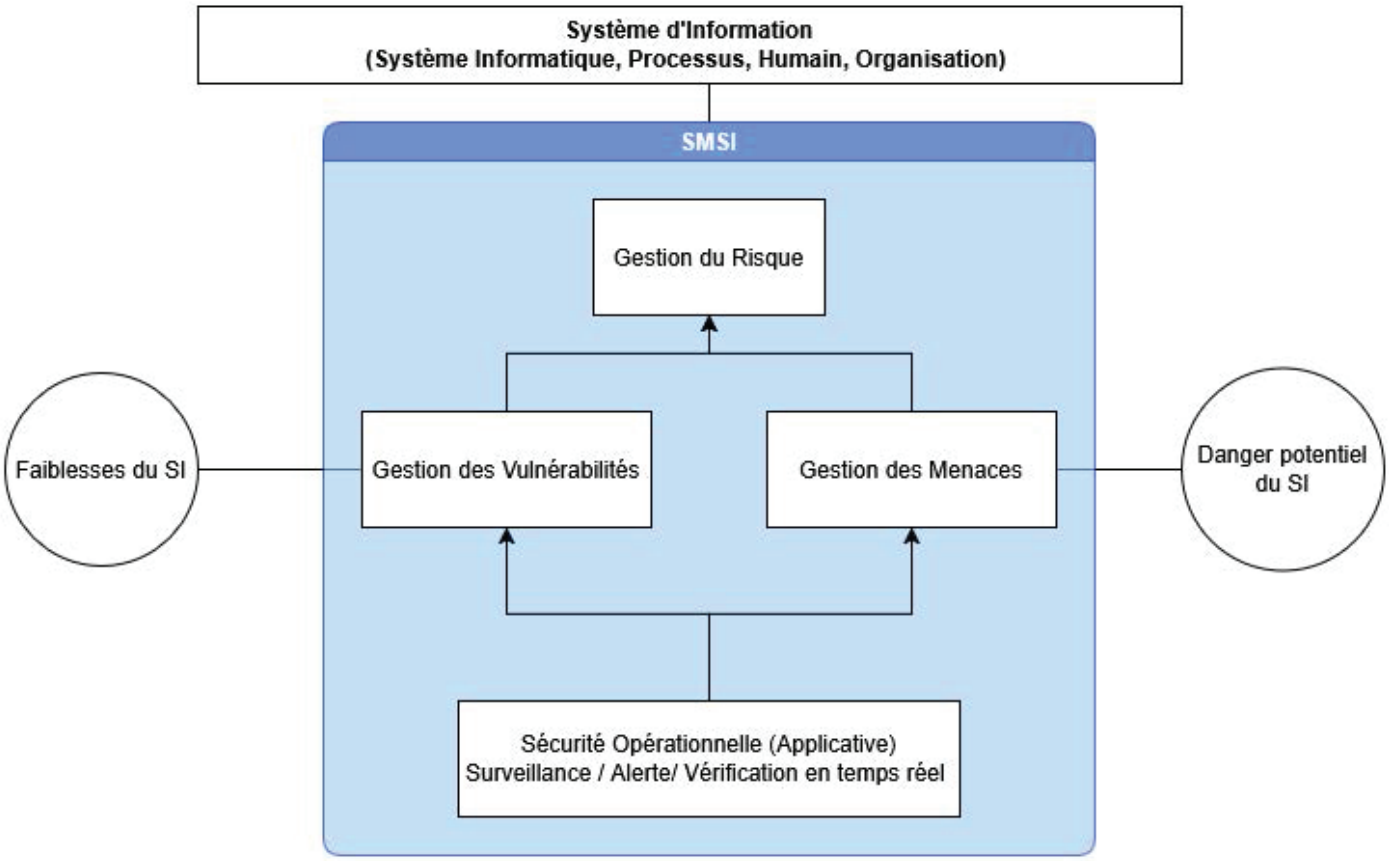

FIGURE 1. *Les composants principaux du SMSI*

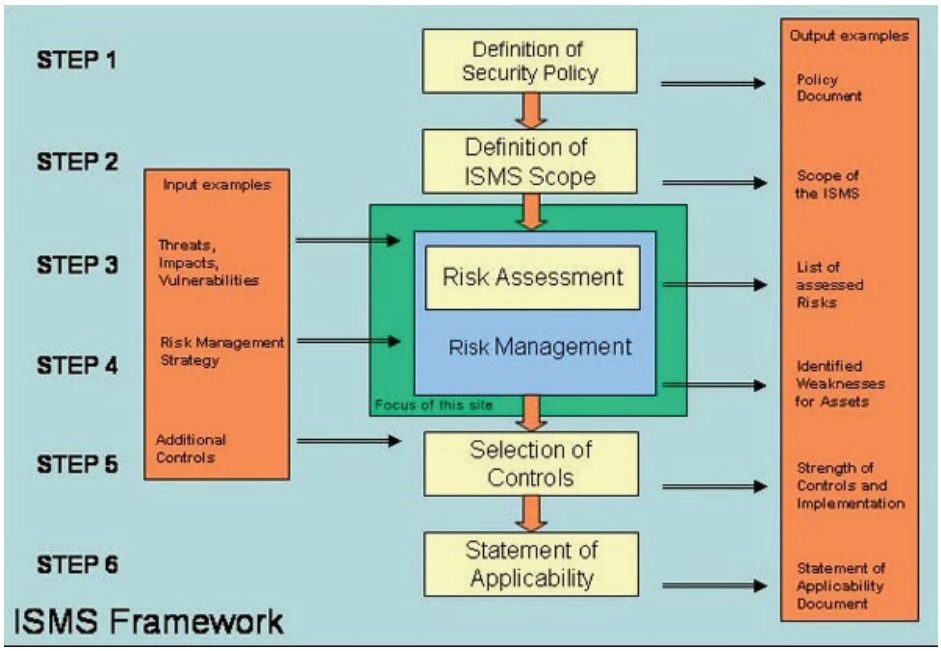

FIGURE 2. *Processus de développement du système de gestion de la sécurité de l'information (*AL-DHAHRI, AL-SARTI *et* ABDAZIZ *2017)*

Common Vulnerability Scoring System (CVSS), se concentrent exclusivement sur les aspects techniques des vulnérabilités (par exemple, le vecteur d'attaque, la complexité, les privilèges nécessaires, etc.), CHOI et LEE (2015) introduisent une perspective élargie en prenant en compte les intérêts stratégiques

de l'organisation, définis ici comme la dimension métier du SI. Cette approche permet une hiérarchisation des vulnérabilités mieux adaptée au contexte spécifique du SI, plutôt qu'à un traitement limité au système informatique. En personnalisant l'évaluation des vulnérabilités selon les priorités organisationnelles, il devient possible de mieux aligner les actions de sécurisation avec les besoins réels de l'entreprise.

Pour formaliser cette démarche, (CHOI et LEE 2015) ont proposé un modèle de calcul du score d'importance de l'information basé sur les trois critères fondamentaux de la triade CIA (Confidentialité, Intégrité et Disponibilité). Le score global d'importance est ainsi défini comme la somme des scores obtenus sur chacun des critères :

$$\textit{Information importance score} = \sum C + \sum I + \sum A \tag{2}$$

— **C** représente le score évaluant l'importance de la confidentialité de l'information, c'est-à-dire la capacité à empêcher tout accès ou divulgation non autorisés.
— **I** représente le score mesurant l'importance de l'intégrité de l'information, garantissant qu'elle ne soit ni altérée ni modifiée de manière non autorisée.
— **A** représente le score indiquant l'importance de la disponibilité (*availability*) de l'information, assurant qu'elle reste accessible et utilisable par les personnes autorisées au moment opportun.

Cette formule additive présente toutefois une **limite structurelle majeure** : l'effet de compensation. Un score élevé sur un critère peut mathématiquement compenser un score faible sur un autre critère, masquant ainsi des vulnérabilités critiques sur des dimensions non substituables. Par exemple, pour un hôpital où la disponibilité des systèmes médicaux est vitale, une excellente confidentialité ne peut pas compenser une défaillance de disponibilité qui pourrait compromettre la vie des patients. Cette substitution entre critères n'a donc pas de sens opérationnel dans de nombreux contextes organisationnels. Nous proposons donc d'explorer des approches alternatives d'agrégation des scores pour mieux refléter les priorités spécifiques des secteurs et leurs organisations.

3.1. *Approches alternatives d'agrégation*

Pour pallier cette limitation, nous proposons quatre approches d'agrégation alternatives :

1. Approche du maillon faible (Min)

$$\textit{Score}_{min} = \min(\sum C, \sum I, \sum A) \tag{3}$$

Cette approche adopte une logique de précaution où le score final correspond au critère le moins bien évalué.

2. Approche pondérée sectorielle

$$\textit{Score}_{pond} = w_C \cdot \sum C + w_I \cdot \sum I + w_A \cdot \sum A \tag{4}$$

où $w_C + w_I + w_A = 1$ et les poids reflètent les priorités sectorielles.

3. Approche multiplicative

$$\textit{Score}_{mult} = (\sum C)^{\alpha} \cdot (\sum I)^{\beta} \cdot (\sum A)^{\gamma} \tag{5}$$

Cette formule amplifie les déséquilibres entre critères et pénalise davantage les scores faibles.

4. Approche hybride seuil-pondération

$$Score_{hybride} = \begin{cases} 0 & \text{si } \min(\sum C, \sum I, \sum A) < \text{seuil} \\ w_C \cdot \sum C + w_I \cdot \sum I + w_A \cdot \sum A & \text{sinon} \end{cases} \quad (6)$$

Le tableau 1 illustre le problème avec deux vulnérabilités hypothétiques ayant le même score total mais des profils très différents :

Vulnérabilité	C	I	A	Additif	Min	Pondéré	Hybride
Vuln. Alpha	15	15	2	32	2	26,4	0
Vuln. Beta	10	11	11	32	10	32	32

Coefficients hospitaliers : $w_C = 0.2$, $w_I = 0.3$, $w_A = 0.5$

Coefficients bancaire : $w_C = 0.5$, $w_I = 0.3$, $w_A = 0.2$

Coefficients hospitaliers : $w_C = 0.1$, $w_I = 0.2$, $w_A = 0.7$

TABLEAU 1. *Illustration de l'effet de compensation avec deux profils de vulnérabilités dans le secteur hospitalier*

Cette illustration révèle que pour un hôpital, la vulnérabilité Alpha, malgré son score total identique, représente un risque inacceptable car elle compromet la disponibilité des systèmes critiques. L'approche du maillon faible et l'approche hybride identifient clairement cette vulnérabilité comme plus problématique.

Dans la suite de cette étude, nous appliquerons ces différentes approches d'agrégation à cinq vulnérabilités dans trois contextes organisationnels, permettant une analyse comparative approfondie de leurs implications pratiques.

3.2. *Intégration des référentiels de sécurité existants*

CHOI et LEE (2015) ont mené un consensus d'experts sur les critères permettant de quantifier l'importance de l'information dans le cadre du *Vulnerability Management*. Ce travail s'appuie sur une intégration des principaux cadres de contrôle de la sécurité, tels que les normes ISO 27000, le programme CSA STAR *Cloud Security Alliance, Security, Trust, Assurances, and Risk*, les recommandations de l'ENISA (*European Union Agency for Cybersecurity*), ainsi que les directives du BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

— L'***International Organization for Standardization*** 27001 définit les exigences nécessaire à la mise ne place d'un SMSI et fournit un cadre normatif pour garantir la conformité organisationnelle (JOGI et HALL 2010),
— **CSA STAR** documente les contrôles de sécurité et de confidentialité spécifiques aux environnement du *Cloud computing* en guidant les organisations dans l'évaluation et la gestion des risques liés aux services *Cloud* (DIX 2012),
— **ENISA** fournit des recommandations et développe des cadres de bonnes pratiques pour renforcer la sécurité du SI en Europe, en mettant un accent particulier sur la protection des infrastructures critiques et les standards émergents (CAVELTY et SMEETS 2023),
— **BSI** définit les normes et les lignes directrices pour la sécurisation des infrastructures numériques, et la gestion des risques adaptés aux exigences modernes de la sécurité du SI (FÖRDERER et al. 2019).

Ces référentiels, en combinant des exigences organisationnelles, des bonnes pratiques et des cadres réglementaires, constituent une base solide pour la mise en œuvre et l'amélioration continue d'un SMSI. Ils permettent aux organisations d'identifier, d'évaluer et d'atténuer efficacement les risques liés à la sécurité de l'information. Le travail de CHOI et LEE (2015) a permis l'élaboration d'un logiciel opérationnel, testé dans une organisation publique. Ce logiciel, en intégrant les critères définis par les experts et les référentiels mentionnés, propose une hiérarchisation des vulnérabilités plus contextualisée et adaptée aux besoins spécifiques de l'organisation.

Dans cette étude, nous proposons d'étendre cette méthode en la testant sur une infrastructure *Cloud* standard utilisée dans diverses organisations (Fig. 3). Plus précisément, nous comparerons la hiérarchisation des vulnérabilités qu'elle génère avec les CVSS pour cinq vulnérabilités représentatives des scénarios courants rencontrés en offres SaaS (*Software as a Service*). Ces vulnérabilités, identifiées dans des travaux récents (ABBASI 2024; JOGI 2023; KADU 2024; FERGUSON 2020), reflètent des enjeux critiques et permettront d'évaluer l'efficacité de la méthode dans des contextes organisationnels variés.

4. Études de cas : analyse comparative de vulnérabilités dans trois contextes organisationnels

4.1. *Infrastructure d'étude et méthodologie expérimentale*

Afin de visualiser et d'évaluer l'intégration de l'aspect métier dans la hiérarchisation des vulnérabilités, nous avons développé une méthodologie comparative confrontant quatre approches d'évaluation distinctes. La première repose sur la hiérarchisation CVSS standard, représentant l'approche technique pure actuellement dominante. La seconde mobilise la méthode additive de CHOI et LEE (2015) pour intégrer la dimension métier. La troisième explore nos approches alternatives du maillon faible et de pondération sectorielle. Enfin, la quatrième intègre la logique de chaînage des vulnérabilités pour une approche contextuelle technique avancée.

L'infrastructure de test, représentée dans la Figure 3, simule un environnement *Cloud* SaaS typique dans lequel cinq vulnérabilités représentatives ont été intégrées. Cette infrastructure reproduit fidèlement l'architecture standard adoptée par de nombreuses organisations contemporaines, garantissant ainsi la pertinence opérationnelle de nos résultats.

Le schéma illustre le parcours complet d'un utilisateur vers un service *Cloud*, depuis l'accès via Internet ou *VPN* jusqu'à l'espace du fournisseur de services *Cloud*. L'architecture SaaS comprend plusieurs composants critiques dont chacun présente des enjeux énergétiques spécifiques. Le *Firewall* assure la protection périmétrique avec un coût de patch estimé à 8 kWh, tandis que le *Load Balancer* gère la répartition de charge pour un coût de remédiation de 15 kWh. Le cœur métier, composé de l'application et de la base de données, représente l'élément le plus coûteux énergétiquement avec 25 à 40 kWh selon la complexité du correctif. Enfin, le serveur de sauvegarde, essentiel à la continuité d'activité, nécessite environ 12 kWh pour ses opérations de maintenance sécuritaire.

Cette quantification énergétique constitue les prémices de notre mise en lien entre la sécurité et la durabilité, permettant d'intégrer concrètement la dimension environnementale dans l'évaluation des vulnérabilités en plus de la dimension métier. Chaque composant se voit attribuer un coût énergétique basé sur les opérations réelles de scan, patch, test, redémarrage et vérification, suivant la formule de l'équation 1 développée précédemment.

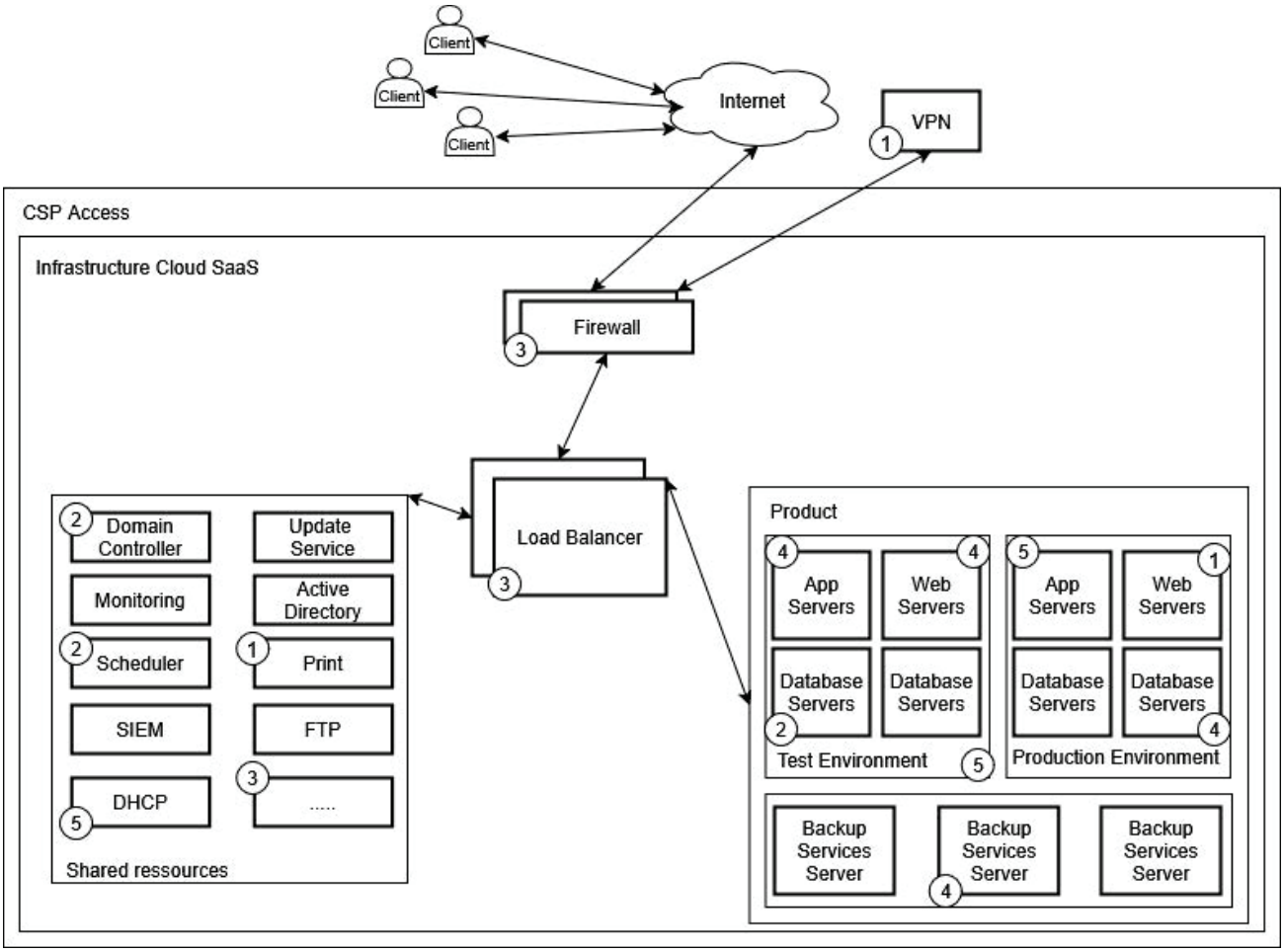

FIGURE 3. *Infrastructure Cloud de test avec localisation des vulnérabilités et estimation des coûts énergétiques*

4.2. *Sélection et caractérisation des vulnérabilités d'étude*

La sélection des cinq vulnérabilités s'appuie sur trois critères fondamentaux garantissant la robustesse de notre analyse comparative. Le premier critère concerne la représentativité des menaces *Cloud*, assurant que chaque vulnérabilité reflète des enjeux critiques rencontrés dans les environnements SaaS contemporains. Le second critère vise la diversité des scores CVSS, permettant d'analyser des vulnérabilités couvrant l'ensemble du spectre de criticité technique. Le troisième critère examine l'impact différencié selon les secteurs, garantissant que chaque vulnérabilité présente des enjeux variables selon le contexte organisationnel.

Les estimations énergétiques présentées s'appuient sur les données de consommation moyennes des centres de données européens publiées par l'ADEME (2022), complétées par une analyse des spécifications techniques constructeurs et de l'expérience terrain. Les coûts énergétiques sont calculés selon la méthodologie détaillée de l'équation 1, incluant les phases de scan (0,2-0,8 kW selon l'équipement), de correction applicative ou infrastructure (1-2,5 kW), de test et validation (0,3-1 kW), et de redémarrage avec vérification (0,1-0,5 kW), le tout majoré par un facteur infrastructure de 4,7 à 5,6 selon la criticité du composant.

`CVE-2021-22965`, connue sous le nom de *Spring4Shell* et classée CVSS 7.5 (*High*), permet l'exécution de code distant via une mauvaise gestion des requêtes HTTP dans le *framework Spring*. Cette vulnérabilité se localise principalement au niveau *VPN* et applicatif, générant un coût énergétique estimé à 18 kWh calculé comme suit : 3h de diagnostic applicatif (0,5 kW) + 6h de tests de non-régression

(0,3 kW) + redémarrage coordonné des services (2,5 kW × 2h) + 2h de vérification fonctionnelle (0,2 kW), soit 8,3 kWh directs majorés par le facteur infrastructure de 2,2. Son impact varie significativement selon le secteur, étant particulièrement critique pour les hôpitaux où la disponibilité des accès distants conditionne la continuité des soins.

`CVE-2021-44228`, la fameuse *Log4Shell* avec un score CVSS de 10.0 (*Critical*), représente l'une des vulnérabilités les plus critiques de la dernière décennie. Elle permet l'exécution de code arbitraire via l'exploitation malveillante de la journalisation *Log4j*, touchant principalement les *Domain Controllers* et l'infrastructure centrale. Son coût énergétique s'élève à 35 kWh calculé par : 4h de scan approfondi (0,8 kW) + 8h de correction infrastructure critique (2,5 kW) + redémarrage complet avec reconstruction des index (2,5 kW × 6h) + 4h de vérifications exhaustives (0,5 kW), soit 25,7 kWh directs avec majoration critique, en raison de la nécessité de redémarrer l'infrastructure critique et d'effectuer des vérifications exhaustives. Cette vulnérabilité présente un impact uniforme élevé pour les banques et hôpitaux, mais moindre pour les hébergeurs de sites vitrine qui utilisent des architectures simplifiées.

`CVE-2020-10188`, avec un score CVSS de 9.8 (*Critical*), permet l'exécution de commandes malveillantes sur des systèmes *F5 BIG-IP* vulnérables, affectant principalement les *Load Balancers*. Son coût énergétique de 15 kWh reste modéré car les correctifs ne nécessitent généralement pas de redémarrage complet de l'infrastructure : 2h de diagnostic réseau (0,3 kW) + 4h de patch *Load Balancers* (0,5 kW) + basculement sécurisé (0,5 kW × 3h) + tests de répartition (0,3 kW × 4h), soit 4,3 kWh directs avec facteur de 3,5. Cette vulnérabilité révèle des enjeux particulièrement intéressants pour notre analyse car son impact critique sur la disponibilité en fait une priorité absolue pour les hôpitaux.

`CVE-2020-11023`, classée CVSS 6.1 (*Medium*), permet l'injection de scripts malveillants dans des pages *web* via des failles XSS. Son coût énergétique minimal de 5 kWh s'explique par la simplicité des correctifs applicatifs requis : 1h de correction code (0,2 kW) + 2h de tests (0,2 kWh) + redémarrage applicatif léger (0,1 kW × 1h) + validation (0,1 kW × 2h), soit 0,9 kWh directs avec facteur standard de 5,6. Malgré son score technique modéré, cette vulnérabilité peut présenter des enjeux critiques pour les hébergeurs de sites vitrine où l'intégrité de l'affichage conditionne la réputation organisationnelle.

`CVE-2020-2551`, avec un score CVSS de 9.8 (*Critical*), permet l'exécution de requêtes SQL malveillantes pour accéder ou manipuler des données sensibles. Son coût énergétique de 22 kWh reflète la complexité des vérifications de cohérence de données nécessaires après correction : 3h d'analyse base de données (0,8 kW) + 5h de correction et migration (1,5 kW) + vérification d'intégrité complète (0,5 kW × 8h) + tests de cohérence (0,3 kW × 6h), soit 13,7 kWh directs avec majoration de 1,6. Cette vulnérabilité présente des enjeux différenciés selon le type et la sensibilité des données manipulées par chaque organisation.

4.3. *Intégration de la dimension énergétique dans l'évaluation de la criticité des vulnérabilités*

L'innovation majeure de notre approche réside dans l'intégration systématique du coût énergétique total de remédiation, calculé selon une adaptation de l'équation 1. Cette formule étendue intègre non seulement les phases de détection et de correction, mais également les coûts de test, redémarrage et vérification souvent négligés dans les approches traditionnelles.

Pour chaque vulnérabilité, nous avons développé un indice composite original, le *Green Vulnerability Indicator* (GVI), qui quantifie le rapport entre l'impact sécuritaire, l'urgence métier et le coût énergétique selon la formule :

$$GVI = \frac{Score_{\text{sécuritaire}} \times Urgence_{\text{métier}}}{Cot_{\text{énergétique}} \times Facteur_{\text{normalisation}}} \tag{7}$$

où :

— $Score_{\text{sécuritaire}} = Score_{\text{CVSS}} \times 4$ (normalisation sur 40)
— $Urgence_{\text{métier}} = \frac{\sum_{\text{secteurs}} Score_{\text{Choi}}}{3}$ (moyenne intersectorielle des trois contextes étudiés)
— $Cot_{\text{énergétique}}$ correspond au coût en kWh selon le composant affecté
— $Facteur_{\text{normalisation}} = 10$ pour l'échelle de lisibilité

Les calculs révèlent des résultats particulièrement éclairants. `CVE-2020-11023` obtient le GVI le plus élevé (11,22) malgré son score CVSS modéré : $GVI = \frac{6.1 \times 4 \times \frac{(24+30+15)}{3}}{5 \times 10} = \frac{24{,}4 \times 23}{50} = 11,22$. Cette performance s'explique par son très faible coût énergétique qui compense largement son impact sécuritaire limité. À l'inverse, `CVE-2021-44228` (Log4Shell), pourtant critique avec un CVSS de 10.0, n'obtient qu'un GVI de 3,85 en raison de son coût énergétique substantiel : $GVI = \frac{10.0 \times 4 \times \frac{(39+39+23)}{3}}{35 \times 10} = \frac{40 \times 33{,}67}{350} = 3,85$.

`CVE-2020-10188` présente un profil intermédiaire particulièrement intéressant avec un GVI de 7,93 ($GVI = \frac{9.8 \times 4 \times \frac{(33+37+21)}{3}}{15 \times 10} = \frac{39{,}2 \times 30{,}33}{150} = 7,93$), combinant criticité technique élevée et coût énergétique maîtrisé grâce à l'efficacité des correctifs *Load Balancers*. Les vulnérabilités `CVE-2021-22965` (GVI = 5,11) et `CVE-2020-2551` (GVI = 5,76) occupent des positions médianes, révélant l'importance du facteur énergétique dans la hiérarchisation finale.

Ces résultats démontrent qu'une stratégie de *Green Vulnerability Management* pourrait privilégier des vulnérabilités de criticité technique modérée mais énergétiquement efficaces, transformant radicalement les paradigmes établis. Le tableau 2 résume les résultats de l'indice GVI, permettant d'identifier les vulnérabilités présentant le meilleur ratio efficacité sécuritaire sur impact environnemental, ouvrant la voie à une priorisation véritablement durable où l'optimisation énergétique devient un critère décisionnel à part entière, sans compromettre les objectifs fondamentaux de protection mais en questionnant intelligemment les priorités traditionnelles.

4.4. *Intégration de la dimension métier dans l'évaluation de la criticité des vulnérabilités*

Après la dimension durable, nous allons étudier la dimension métier au travers des travaux de CHOI et LEE (2015) (Tab 3). Que nous allons comparé avec le CVSS et par la suite avec nos approches alternatives.

Pour obtenir les chiffres présentés dans cette étude, nous nous sommes appuyés sur une analyse approfondie d'articles représentant les points de vue de différents secteurs : les banques (DUMALANEDE 2019; LOBEZ 2006; BOBILLIER-CHAUMON, DUBOIS, RETOUR 2006), les hôpitaux (FRENKIEL, BOUAM et TRIADOU 2007; JUVEN 2013) et les hébergeurs de sites *web* vitrine (STEPHANE 2020; LE BLOG DU DIRIGEANT 2024). L'analyse a été structurée autour de la triade de sécurité de l'information à travers des critères spécifiques.

Vulnérabilité	Score CVSS	Score Sécuritaire (×4)	Urgence Métier (Moyenne)	Coût Énergétique (kWh)	GVI Calculé	Rang GVI	Rang CVSS
CVE-2020-11023 (XSS)	6.1	24.4	23.0 (24+30+15)/3	5	11.22	1	5
CVE-2020-10188 (F5 BIG-IP)	9.8	39.2	30.33 (33+37+21)/3	15	7.93	2	2
CVE-2020-2551 (SQL Injection)	9.8	39.2	32.33 (39+37+21)/3	22	5.76	3	2
CVE-2021-22965 (Spring4Shell)	7.5	30.0	30.67 (32+36+24)/3	18	5.11	4	4
CVE-2021-44228 (Log4Shell)	10.0	40.0	33.67 (39+39+23)/3	35	3.85	5	1

Notes : Score Sécuritaire = CVSS × 4 ; Urgence Métier = moyenne des scores Choi & Lee sur les 3 secteurs ; GVI = (Score Sécuritaire × Urgence Métier) / (Coût Énergétique × 10)

TABLEAU 2. *Tableau récapitulatif des résultats Green Vulnerability Indicator (GVI)*

Vulnérabilité	Organisation	∑C	∑I	∑A	Total
CVE-2021-22965	Banque	13	11	8	32
	Hôpital	10	13	13	36
	Hébergeur site *web* vitrine	6	6	12	24
CVE-2021-44228	Banque	16	13	10	39
	Hôpital	10	14	15	39
	Hébergeur site *web* vitrine	8	9	6	23
CVE-2020-10188	Banque	13	11	9	33
	Hôpital	11	12	14	37
	Hébergeur site *web* vitrine	7	8	6	21
CVE-2020-11023	Banque	8	9	7	24
	Hôpital	7	11	12	30
	Hébergeur site *web* vitrine	5	6	4	15
CVE-2020-2551	Banque	15	14	10	39
	Hôpital	9	14	14	37
	Hébergeur site *web* vitrine	7	8	6	21

TABLEAU 3. *Notation de criticité des vulnérabilités par secteur en utilisant la méthode de* CHOI *et* LEE *(2015) (Additive).*

Concernant la confidentialité, nous avons évalué la sensibilité des informations, la présence de restrictions d'accès et la nécessité de leur protection. Pour l'intégrité, les critères incluaient la capacité de restreindre les modifications, la fréquence des sauvegardes et l'importance des audits des changements. Enfin, la disponibilité a été mesurée en fonction de la nécessité d'un accès continu et de l'impact des interruptions potentielles sur l'organisation. Les détails des calculs pour chaque secteur et vulnérabilité sont présentés en annexe (voir section 8).

Ces critères ont permis d'évaluer et de hiérarchiser les vulnérabilités identifiées, bien que les résultats obtenus soient limités par l'absence d'un consensus d'experts, ce qui constitue une des limites notables de cette étude. Ces résultats révèlent des variations sectorielles significatives dans l'évaluation des vulnérabilités. Par exemple, `CVE-2021-22965` obtient un score total de 36 pour l'hôpital contre seulement 24 pour le site *web* vitrine, illustrant l'impact des priorités organisationnelles sur la hiérarchisation. Cependant, cette approche additive masque potentiellement des déséquilibres critiques entre les critères de la triade CIA.

4.5. *Comparaison initiale : CVSS vs méthode additive de Choi & Lee*

L'analyse révèle des divergences significatives entre la hiérarchisation standard du CVSS et l'approche métier de CHOI et LEE (2015). La Figure 4 illustre cette différence fondamentale de priorisation entre les deux méthodes.

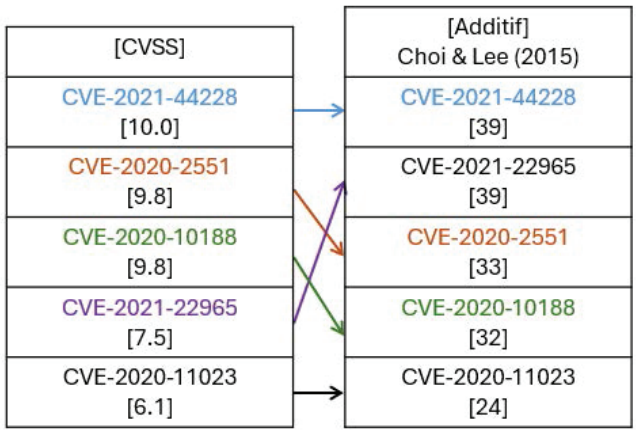

FIGURE 4. *Différence de hiérarchisation de vulnérabilité d'après 2 méthodes différentes [CVSS et Choi & Lee]*

Pour `CVE-2021-22965`, qui concerne principalement les *VPN*, les scores additifs étaient de 32 sur 40 pour une banque, 36 pour un hôpital et 24 pour un hébergeur de site *web* vitrine. Cette vulnérabilité, classée High par le CVSS, devient particulièrement critique pour un hôpital selon la méthode de CHOI et LEE (2015) en raison des exigences accrues en matière de disponibilité et d'intégrité des données.

Pour `CVE-2021-44228`, touchant les *Domain Controllers*, la banque et l'hôpital obtiennent un score identique de 39 sur 40, tandis que le hébergeur de site *web* vitrine atteint seulement 23 sur 40. Cette disparité s'explique par l'importance légale et économique des informations manipulées par les banques et les hôpitaux, contrastant avec le score CVSS uniforme de 10.0.

`CVE-2020-10188`, liée au *Load Balancer*, présente des scores respectifs de 33 pour la banque, 37 pour l'hôpital et 21 pour le hébergeur de site *web* vitrine. La disponibilité étant prioritaire pour un hôpital, cette vulnérabilité y devient plus critique que pour une banque, où la protection des données prime, malgré un score CVSS identique de 9.8.

`CVE-2020-11023`, affectant principalement les interfaces *web* via des failles XSS, révèle des disparités sectorielles marquées avec des scores de 24 pour la banque, 30 pour l'hôpital et seulement 15 pour l'hébergeur de site *web* vitrine. Paradoxalement, bien que cette vulnérabilité impacte directement l'affichage *web*, elle obtient le score le plus faible pour le secteur de l'hébergement. Cette apparente contradiction s'explique par la nature des données manipulées : les sites vitrine traitent généralement des

informations publiques avec des exigences de confidentialité et d'intégrité limitées, contrairement aux environnements bancaires et hospitaliers où même l'affichage peut révéler des informations sensibles.

CVE-2020-2551, permettant l'injection SQL, présente un profil inverse avec des scores de 39 pour la banque, 37 pour l'hôpital et 21 pour l'hébergeur de site *web* vitrine. Cette vulnérabilité révèle l'importance critique des données pour les secteurs bancaire et hospitalier, où l'intégrité et la confidentialité des bases de données conditionnent la conformité réglementaire et la qualité des soins. L'écart de 18 points entre banque et hébergeur *web* illustre parfaitement l'impact du contexte métier sur l'évaluation des risques, une vulnérabilité techniquement identique pouvant représenter un enjeu existentiel pour une organisation et un risque mineur pour une autre. Ces cinq analyses confirment que la méthode de CHOI et LEE (2015) révèle des nuances sectorielles que le CVSS ne peut capturer, justifiant pleinement l'intégration de la dimension métier dans l'évaluation des vulnérabilités. Les écarts observés entre secteurs, parfois supérieurs à 50% du score maximal, démontrent que l'universalité du CVSS constitue paradoxalement sa principale limite opérationnelle.

La méthode de CHOI et LEE (2015) révèle que certaines vulnérabilités critiques selon le CVSS peuvent être reléguées en seconde position pour la banque et l'hébergeur de site *web*, tout en restant prioritaires pour l'hôpital. Cette contextualisation sectorielle constitue un apport significatif par rapport à l'approche technique universelle du CVSS.

4.6. *Enrichissement par nos méthodes d'agrégation alternatives*

Comme évoqué précédemment, la méthode additive de CHOI et LEE (2015), bien qu'elle intègre efficacement la dimension métier, présente une limite structurelle majeure liée à l'effet de compensation : un score élevé sur un critère peut masquer une défaillance critique sur un autre critère non substituable, créant une illusion de sécurité particulièrement problématique dans des contextes où certains aspects de la triade CIA ne peuvent être compensés. Pour révéler ces limites et proposer des alternatives plus robustes, nous avons appliqué nos méthodes du maillon faible et de pondération sectorielle. Les Figures 5, 6 et 7 illustrent l'impact de ces nouvelles approches sur la hiérarchisation dans chaque secteur.

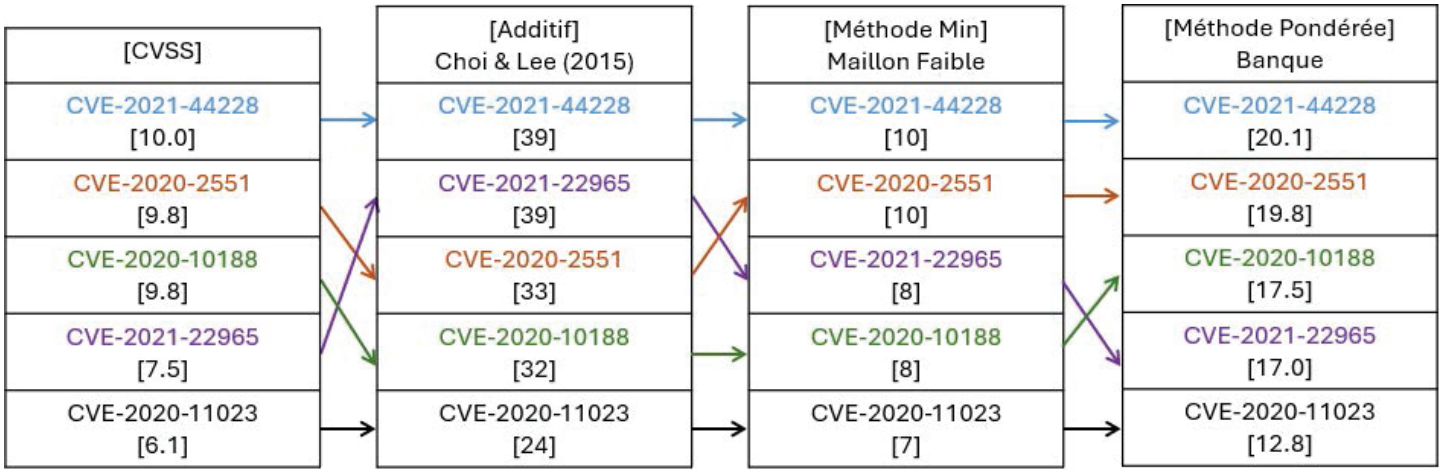

FIGURE 5. *Comparaison avec les méthodes introduites dans la section 3 pour le secteur bancaire.*

La comparaison entre l'approche additive et les méthodes d'agrégation alternatives révèle des divergences particulièrement éclairantes. Dans le contexte hospitalier, CVE-2021-22965 obtient un score

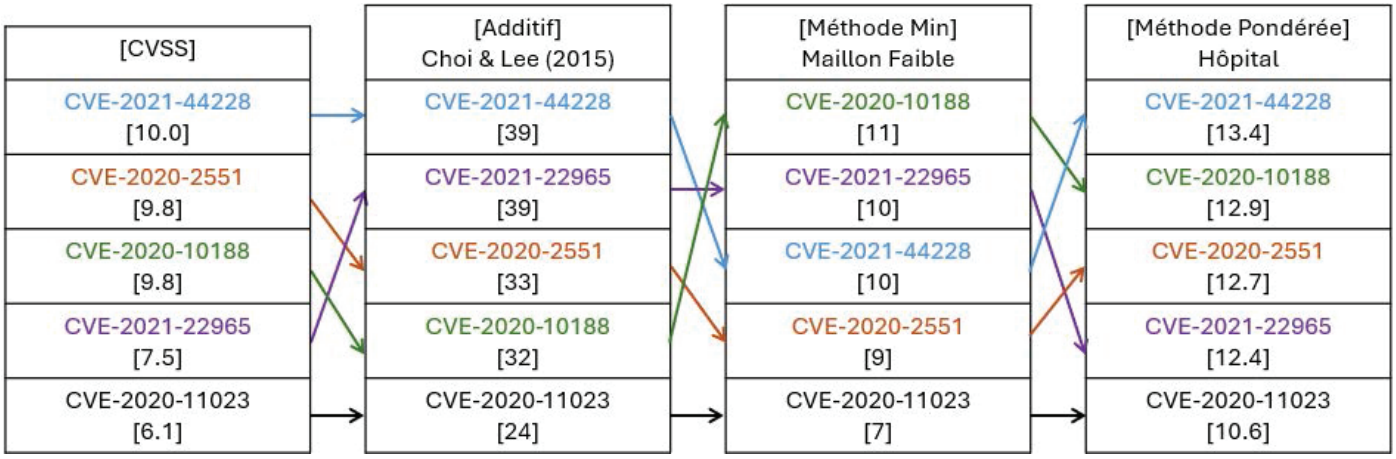

FIGURE 6. *Comparaison avec les méthodes introduites dans la section 3 pour le secteur hospitalier.*

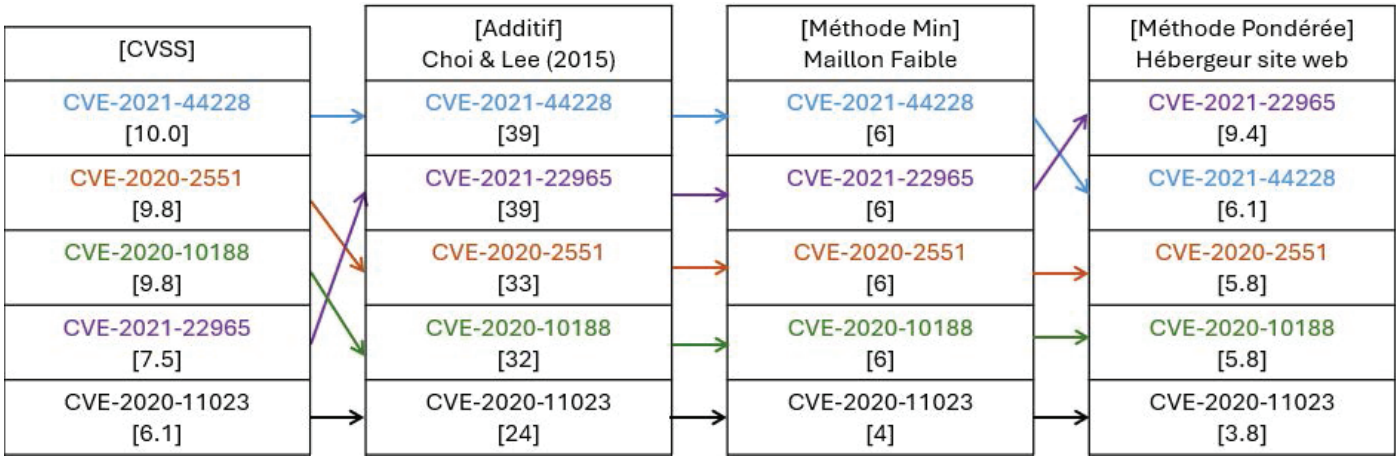

FIGURE 7. *Comparaison avec les méthodes introduites dans la section 3 pour le secteur d'hébergement de site web.*

additif de 36 mais chute drastiquement à seulement 10 avec l'approche du maillon faible, illustrant l'effet de compensation masqué par la méthode additive.

Inversement, `CVE-2020-10188` passe du rang 3 au rang 1 selon l'approche Min, démontrant que son profil équilibré en fait une priorité selon l'approche du maillon faible. Cette observation révèle que la hiérarchisation traditionnelle peut sous-estimer des vulnérabilités réellement critiques tout en surévaluant d'autres dont les scores élevés masquent des faiblesses structurelles.

D'après les trois figures sectorielles, le secteur hospitalier présente les différences les plus marquées entre les méthodes existantes et nos approches alternatives. La vulnérabilité `CVE-2021-22965`, considérée comme critique par le CVSS, est reléguée en seconde position par la méthode de CHOI et LEE (2015) et en troisième position par notre approche du maillon faible. Cette reclassification s'explique par l'impact contextuel sur les *VPN*, essentiels pour un hôpital mais avec des exigences de robustesse homogène sur tous les critères CIA.

4.7. *Comparaison des trois méthodes d'optimisation énergétique*

L'analyse comparative des trois approches révèle que 3 vulnérabilités sur 5 changent de priorité selon l'approche utilisée. Cette instabilité hiérarchique questionne la fiabilité des méthodes traditionnelles et ouvre des perspectives d'optimisation énergétique substantielles.

L'approche du maillon faible révèle des vulnérabilités pivot comme `CVE-2020-10188`, dont le traitement prioritaire pourrait permettre de neutraliser indirectement d'autres vulnérabilités dépendantes, optimisant ainsi l'allocation des ressources énergétiques. La méthode pondérée confirme l'alignement nécessaire entre priorités sectorielles et stratégies de remédiation.

Vulnérabilité	CVSS	GVI	Scores Choi & Lee par secteur						Coût	Composant
			Banque		Hôpital		site *web* vitrine			
			Score	Rang	Score	Rang	Score	Rang		
CVE-2021-44228 (Log4Shell)	10.0 (Rang 1)	3.85 (Rang 5)	39	1	39	1	23	2	35 kWh	Domain Controllers
CVE-2020-10188 (F5 BIG-IP)	9.8 (Rang 2)	7.93 (Rang 2)	33	3	37	2	21	4	15 kWh	*Load Balancers*
CVE-2020-2551 (SQL Injection)	9.8 (Rang 2)	5.76 (Rang 3)	39	1	37	2	21	4	22 kWh	Base de données
CVE-2021-22965 (Spring4Shell)	7.5 (Rang 4)	5.11 (Rang 4)	32	4	36	4	24	3	18 kWh	VPN/Application
CVE-2020-11023 (XSS)	6.1 (Rang 5)	11.22 (Rang 1)	24	5	30	5	15	5	5 kWh	Interface *web*

Lecture du tableau : CVSS = score technique standard ; GVI = Green Vulnerability Indicator (efficacité/coût énergétique) ; Scores Choi & Lee = évaluation contextuelle par secteur (max 40) ; Les rangs indiquent la priorisation selon chaque méthode

TABLEAU 4. *Tableau comparatif global : CVSS vs Green Vulnerability Indicator vs Choi & Lee par secteur*

Vulnérabilité	Rang CVSS	Rang GVI	Rang moyen Choi & Lee	Inversion CVSS/GVI	Inversion CVSS/Choi	Impact énergétique	Facteur déterminant
CVE-2021-44228 (Log4Shell)	1	5	1.33	-4	Stable	Très défavorable (×7)	Coût énergétique substantiel
CVE-2020-10188 (F5 BIG-IP)	2	2	2.67	=	Modéré	Équilibré	Efficacité des correctifs L.B.
CVE-2020-2551 (SQL Injection)	2	3	2.33	-1	Stable	Modéré	Complexité vérifications
CVE-2021-22965 (Spring4Shell)	4	4	3.67	=	Modéré	Modéré	Redémarrages coordonnés
CVE-2020-11023 (XSS)	5	1	5.00	+4	Stable	Très favorable (×1)	Simplicité correctifs

Notes : Rang moyen Choi & Lee = moyenne des rangs sur les 3 secteurs ; Impact énergétique = ratio coût/bénéfice par rapport à la médiane ; Inversions négatives = perte de priorité

TABLEAU 5. *Analyse des inversions de priorité entre les trois approches*

L'analyse détaillée des tableaux révèle plusieurs phénomènes instructifs concernant la hiérarchisation sectorielle. L'absence de rang 1 pour le secteur « site *web* vitrine » s'explique par une caractéristique structurelle fondamentale : les sites vitrine manipulent essentiellement des informations publiques avec des exigences de sécurité intrinsèquement moindres que les secteurs bancaire et hospitalier. `CVE-2021-44228` (Log4Shell) obtient ainsi le rang 2 comme position maximale pour ce secteur, reflétant que même les vulnérabilités les plus critiques techniquement présentent un impact métier relativement modéré dans un contexte où la confidentialité et l'intégrité des données ne constituent pas des enjeux existentiels. Cette observation démontre que la contextualisation sectorielle conduit naturellement à une compression de l'échelle de criticité pour certains secteurs, phénomène attendu et cohérent avec leurs priorités organisationnelles.

Les sauts de rangs observés (par exemple, CVE-2021-44228 et CVE-2020-2551 obtiennent toutes deux le rang 1 pour la banque) résultent d'une caractéristique méthodologique essentielle : lorsque plusieurs vulnérabilités obtiennent des scores identiques, elles partagent le même rang, et le rang suivant est automatiquement décalé. Pour la banque, CVE-2021-44228 et CVE-2020-2551 obtiennent toutes deux un score de 39, leur attribuant le rang 1 ex-aequo. La vulnérabilité suivante (CVE-2020-10188 avec un score de 33) reçoit donc logiquement le rang 3, le rang 2 étant « consommé » par l'égalité précédente. Ce mécanisme mathématique standard reflète fidèlement l'impossibilité de discriminer entre deux vulnérabilités présentant exactement le même impact sectoriel selon les critères CIA, tout en préservant l'intégrité de la hiérarchisation globale. Ces ex-aequo révèlent également les limites intrinsèques de toute méthode d'évaluation quantitative lorsque confrontée à la complexité des contextes organisationnels réels, où plusieurs menaces peuvent effectivement présenter des niveaux de criticité strictement équivalents selon les dimensions métier considérées.

Ces méthodes alternatives démontrent leur pertinence en révélant des zones grises décisionnelles où l'approche additive traditionnelle masque des vulnérabilités critiques. Notre approche multi-méthodologique offre une hiérarchisation plus robuste, prenant en compte les priorités spécifiques de chaque secteur et ouvrant la voie à une gestion énergétiquement consciente des vulnérabilités, constituant les bases du *Green Vulnerability Management* comme paradigme émergent pour les organisations soucieuses de durabilité. La poursuite de cet axe de recherche pourrait inclure l'intégration de critères supplémentaires tels que la criticité des actifs, la probabilité d'exploitation et les tendances émergentes en matière de menaces, afin de développer un modèle de hiérarchisation encore plus holistique et adaptatif en associant tous les métriques «traditionnels » comme le CVSS et les approches plus récentes comme le GVI et les méthodes d'agrégation avancées dans l'optique de créer un arbre de décision complet avant de devenir un algorithme automatisé de *Green, Business, Vulnerability Management*.

Cependant, l'intégration des dimensions énergétique et métier, bien que nécessaire, demeure insuffisante pour appréhender pleinement la complexité des menaces contemporaines. Au-delà de l'évaluation individuelle des vulnérabilités selon leurs impacts techniques, organisationnels et environnementaux, il convient d'analyser leur potentiel d'exploitation réel dans le contexte spécifique de l'infrastructure organisationnelle. Cette troisième dimension, technique et contextuelle, nécessite d'examiner comment les vulnérabilités peuvent être chaînées pour constituer des vecteurs d'attaque viables, permettant ainsi de distinguer les risques théoriques des menaces effectivement exploitables et d'affiner davantage la priorisation des efforts de remédiation.

4.8. *Intégration de la logique de chaînage des vulnérabilités*

Au-delà de l'évaluation individuelle des vulnérabilités selon leurs impacts techniques, organisationnels et environnementaux, une troisième dimension fondamentale émerge : l'analyse du potentiel d'exploitation réel selon l'infrastructure organisationnelle spécifique. Le chaînage des vulnérabilités distingue les risques théoriques des menaces effectivement exploitables en examinant leur rôle dans les vecteurs d'attaque viables. Cette approche contextuelle se fonde sur la position topologique de chaque vulnérabilité dans l'infrastructure (Fig. 3), s'éloignant radicalement de l'évaluation universelle du CVSS pour une personnalisation complète par organisation et par architecture.

L'analyse révèle des profils d'exploitabilité différenciés. CVE-2021-22965 (Spring4Shell) n'atteint sa criticité maximale que lorsque les accès VPN constituent des points d'entrée stratégiques

— cas typique des hôpitaux où télémédecine et accès distant conditionnent la continuité des soins. CVE-2021-44228 (Log4Shell), malgré son CVSS maximal de 10.0, voit son impact limité à l'exploitation des Domain Controllers, réduisant ses vecteurs d'attaque effectifs malgré sa criticité technique universelle.

CVE-2020-10188 révèle un profil pivot : techniquement critique (CVSS 9.8), sa criticité opérationnelle devient stratégique uniquement par son impact sur les *Load Balancers*s, composants centraux de l'architecture Cloud assurant la répartition de charge. Cette vulnérabilité illustre comment l'approche topologique révèle des menaces véritablement critiques masquées par les évaluations techniques isolées.

Inversement, CVE-2020-11023 (XSS) et CVE-2020-2551 (SQL Injection) présentent un impact contextuel limité : leur exploitabilité dans l'infrastructure étudiée reste marginale malgré leurs scores techniques respectables (CVSS 6.1 et 9.8). Cette observation valide l'importance de l'analyse contextuelle pour éviter la sur-priorisation de vulnérabilités théoriquement dangereuses mais pratiquement inexploitables dans le contexte infrastructurel spécifique.

L'analyse comparative présentée dans les Figures 8, 9, 10 et 11 révèle des transformations hiérarchiques significatives lorsque cette dimension contextuelle technique est intégrée. Cette approche démontre que certaines vulnérabilités techniquement critiques peuvent devenir totalement inexploitables dans leur contexte d'infrastructure spécifique, tandis que d'autres, apparemment mineures, révèlent un potentiel de chaînage préoccupant.

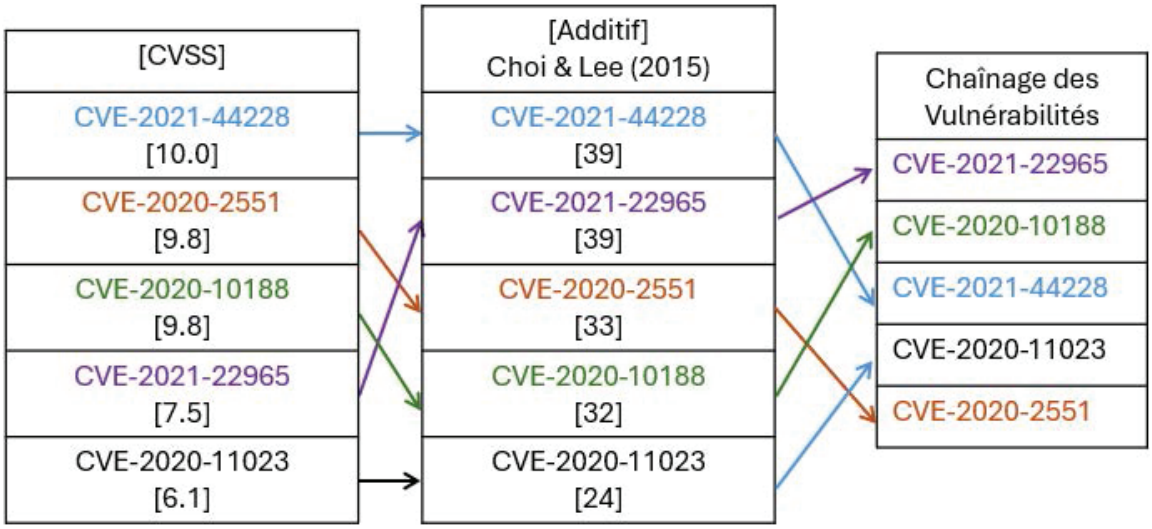

FIGURE 8. *Comparaison hiérarchique globale intégrant CVSS, Choi & Lee et chaînage des vulnérabilités*

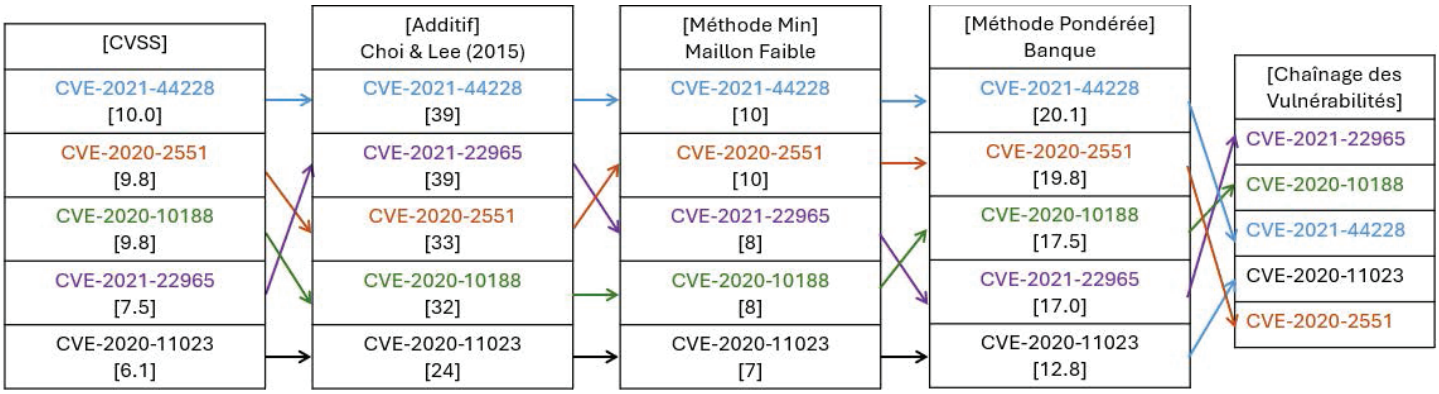

FIGURE 9. *Impact du chaînage des vulnérabilités sur la priorisation : secteur bancaire*

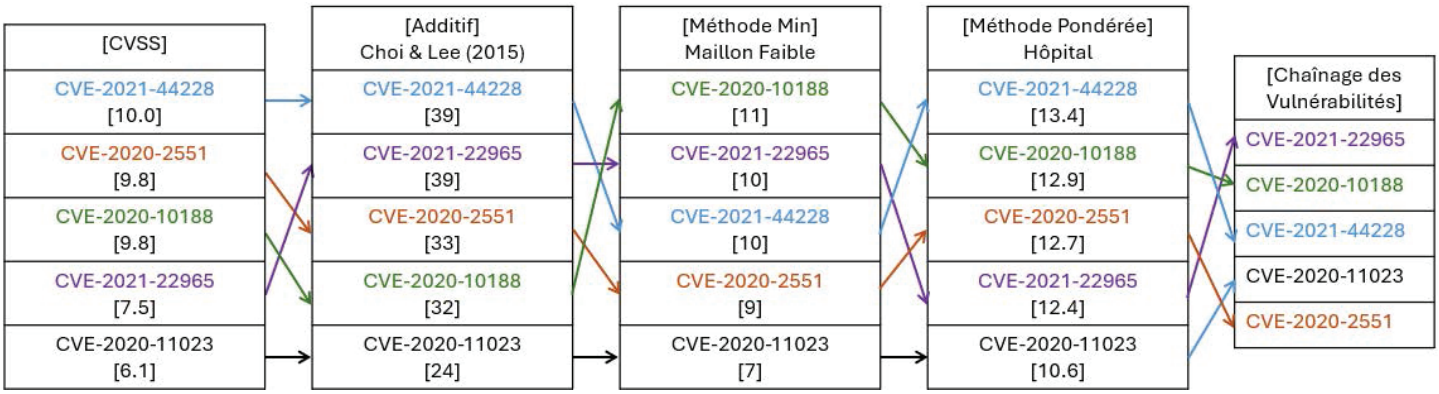

FIGURE 10. *Impact du chaînage des vulnérabilités sur la priorisation : secteur hospitalier*

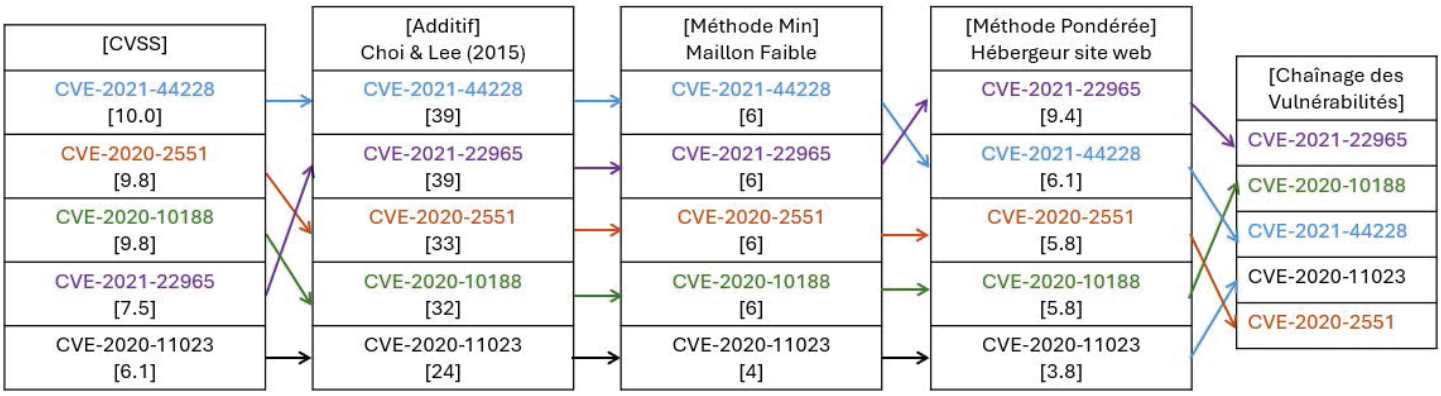

FIGURE 11. *Impact du chaînage des vulnérabilités sur la priorisation : hébergement web*

4.9. *Synthèse comparative des cinq approches de priorisation*

La Figure 12 synthétise les transformations hiérarchiques obtenues par chaque approche, révélant deux phénomènes fondamentaux : la stabilité consensuelle que l'on peut voir entre les méthodes CVSS, Min et Pondérée et l'instabilité méthodologique que l'on peut retrouver en utilisant le GVI et le chaînage des vulnérabilités. Cette analyse comparative démontre que `CVE-2020-10188` émerge comme la vulnérabilité la plus consensuelle, maintenant systématiquement un rang élevé (1-3) dans toutes les méthodes. Cette stabilité s'explique par son profil exceptionnellement équilibré conjuguant quatre dimensions critiques : criticité technique élevée (CVSS 9.8), urgence métier significative (score moyen de 30.33), efficacité énergétique optimale (coût de 15 kWh) et rôle structurellement pivot dans l'architecture *Cloud* par son impact sur les *Load Balancers*.

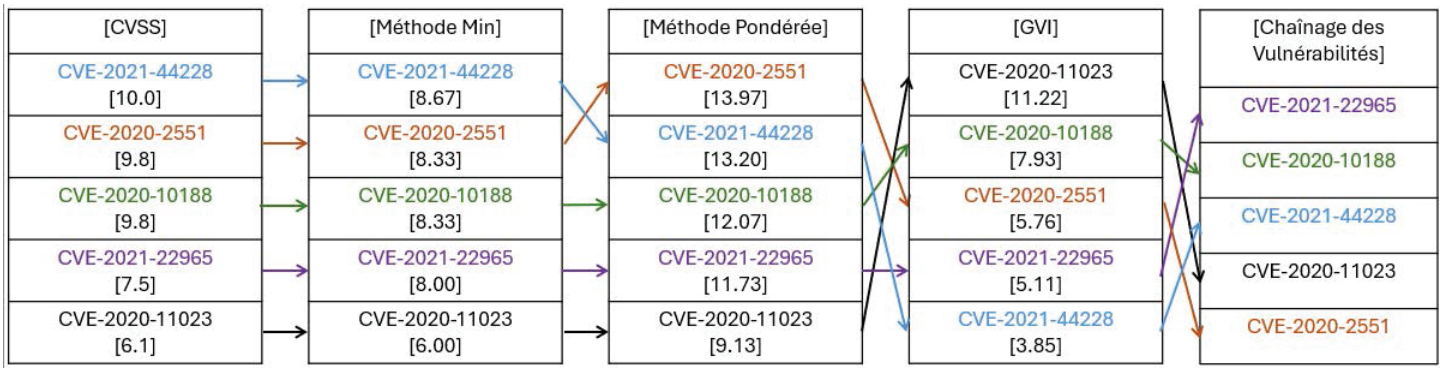

FIGURE 12. *Synthèse comparative des cinq approches de priorisation : CVSS, méthodes métier alternatives, GVI et chaînage contextuel*

À l'opposé, CVE-2020-11023 et CVE-2021-44228 illustrent l'instabilité méthodologique maximale, subissant des variations de priorité de 4 rangs selon l'approche retenue. Cette volatilité révèle des profils antagonistes parfaitement représentatifs du dilemme sécurité-durabilité : CVE-2020-11023 (XSS) passe du rang 5 (CVSS) au rang 1 (GVI) pour son efficacité énergétique (5 kWh), tandis que CVE-2021-44228 (Log4Shell) chute du rang 1 (CVSS) au rang 5 (GVI) en raison de son coût substantiel (35 kWh). Cette analyse révèle que l'approche GVI bouleverse fondamentalement les paradigmes sécuritaires établis en opérant une inversion complète des priorités traditionnelles. Le cas de CVE-2020-11023 constitue l'illustration parfaite de cette révolution conceptuelle : avec un GVI de 11.22, cette vulnérabilité techniquement modeste (CVSS 6.1) devient la plus prioritaire écologiquement, démontrant que l'optimisation du rapport $\frac{\text{efficacité sécuritaire}}{\text{impact environnemental}}$ peut redéfinir radicalement les stratégies de remédiation.

Parallèlement, CVE-2021-44228 (Log4Shell), archétype de la vulnérabilité critique avec son CVSS maximal de 10.0, obtient le GVI le plus faible (3.85), illustrant comment les vulnérabilités les plus médiatisées peuvent s'avérer parfois être les plus complexes et énergivores à résoudre. Cette observation questionne fondamentalement la pertinence des approches réactives traditionnelles et suggère qu'une stratégie de *Green Vulnerability Management* pourrait, dans certains contextes, privilégier le traitement de vulnérabilités techniquement mineures mais énergétiquement optimales. Et profiter des heures creuses pour appliquer les correctifs les plus énergivores.

L'analyse comparative révèle que notre approche tripartite constitue une synthèse opérationnelle du *Vulnerability Management*. Le chaînage infrastructurel des vulnérabilités représente la dimension technique avancée, personnalisant l'évaluation CVSS par l'analyse des vecteurs d'exploitation réels de chaque organisation. Les méthodes métier alternatives (Min et Pondérée) intègrent les priorités organisationnelles sectorielles, personnalisant l'évaluation selon les enjeux spécifiques. L'indicateur GVI introduit la contrainte environnementale, transformant la gestion des vulnérabilités en optimisation sous contraintes durables. Ce n'est plus une simple hiérarchisation des vulnérabilités, mais une gestion stratégique proposant des recommandations de remédiation optimisées selon les trois dimensions critiques. Afin de laisser à l'organisation le soin d'adapter ses décisions en fonction de ses priorités et besoins. L'exemple de CVE-2020-10188 illustre parfaitement cette convergence tripartite. Bien qu'elle ne figure qu'en seconde position selon le CVSS standard, l'intégration successive des trois dimensions révèle son caractère véritablement stratégique : les méthodes métier confirment son importance contextualisée, le GVI valide son efficacité énergétique, et l'analyse de chaînage démontre son rôle pivot dans l'infrastructure *Cloud*. Cette vulnérabilité, affectant les *Load Balancers*, constitue un point de passage obligé pour de nombreux vecteurs d'attaque, justifiant une priorisation élevée qui transcende les scores techniques traditionnels.

Cette approche contextuelle révèle rapidement ses limites opérationnelles critiques face aux infrastructures contemporaines complexes. Pour des organisations gérant des milliers de serveurs et des environnements hybrides *Cloud/on-premise*, l'analyse manuelle tripartite devient impraticable et économiquement non viable.

Cette limite d'industrialisation pose une question fondamentale : comment maintenir la finesse de l'analyse contextuelle tout en l'adaptant à l'échelle des infrastructures modernes ? La réponse réside dans l'automatisation intelligente de l'identification des séquences d'exploitation et la classification systématique des vulnérabilités selon leur rôle dans les chaînes d'attaque. En intégrant le chaînage des

vulnérabilités, l'objectif n'est pas d'ignorer certaines vulnérabilités sous prétexte d'économiser de l'énergie, mais plutôt de déterminer avec précision leur exploitabilité réelle dans le contexte d'infrastructure spécifique. Cette approche permet une allocation optimisée des ressources, conciliant sécurité, performance opérationnelle et responsabilité environnementale. L'approche du chaînage constitue ainsi le troisième pilier de notre méthode tripartite, complétant l'évaluation énergétique et l'analyse métier pour une vision holistique du *Green Vulnerability Management*. Cependant, son industrialisation nécessite le développement de méthodes de classification automatique par *clustering*, capables d'identifier automatiquement les rôles des vulnérabilités dans les chaînes d'attaque potentielles. Cette approche, présentée dans la section suivante, permet de faire évoluer le *Vulnerability Management* d'une discipline majoritairement réactive vers une gestion proactive, prédictive et industrialisable. L'enjeu devient alors de transformer l'expertise contextuelle en intelligence artificielle capable de reproduire, à grande échelle, la subtilité de l'analyse manuelle, ouvrant la voie à un *Green Vulnerability Management* adapté aux défis contemporains.

5. Chaînage des vulnérabilités, les *cluster*

Afin de d'étudier le chaînage des vulnérabilités, nous avons besoin de définir quelles vulnérabilités sont « chaînées » entre elles. Pour une analyse avancée des vulnérabilités et de leur potentiel de chaînage dans des scénarios d'attaque, nous concevons une approche basée sur la classification automatique en plusieurs *cluster* thématiques. Chaque *cluster* regroupe les vulnérabilités selon leur rôle dans une chaîne d'attaque ou leur impact sur la sécurité du système (FRANÇOIS, ARDUIN et MERAD 2025; MEYER, HEININGER et STARY 2024) :

- **Cluster 1 – *Privilege Escalation*** : vulnérabilités permettant à un attaquant d'obtenir des privilèges supérieurs ou d'accéder à des fonctions réservées.
- **Cluster 2 – *Privilege Required*** : vulnérabilités nécessitant des privilèges élevés pour être exploitées, typiquement accessibles après une élévation de privilège.
- **Cluster 3 – *Lateral Movement*** : vulnérabilités facilitant le déplacement d'un attaquant au sein du réseau ou entre différents systèmes.
- **Cluster 4 – *Remote Code Execution*** : vulnérabilités permettant l'exécution de code arbitraire à distance, souvent point de départ d'une compromission.
- **Cluster 5 – *Data Exfiltration*** : vulnérabilités facilitant la fuite ou l'exfiltration de données sensibles hors du périmètre de sécurité.
- **Cluster 6 – *Denial of Service*** : vulnérabilités provoquant une indisponibilité du service ou un déni de service, impactant la disponibilité.
- **Cluster 7 – *Configuration Management*** : vulnérabilités liées à la mauvaise gestion des configurations ou des accès, pouvant ouvrir la voie à d'autres attaques.
- **Cluster 8 – *Third Party Components*** : vulnérabilités exploitant des composants tiers, des dépendances externes ou des bibliothèques non maîtrisées.

Cette classification permet non seulement d'identifier le rôle de chaque vulnérabilité dans une chaîne d'attaque, mais aussi d'automatiser la détection des séquences d'exploitation potentielles (par exemple, *Privilege Escalation* → *Privilege Required* → *Lateral Movement*). L'approche s'appuie sur des modèles de machine learning supervisés, entraînés à partir de descriptions annotées, et peut être enrichie par l'analyse de graphes d'attaque ou l'intégration de référentiels comme MITRE ATT&CK. Pour l'entraînement

nous utilisons deux bases de données différentes, tout d'abord la NVD (*National Vulnerability Database*) gérée par le NIST (*National Institute of Standards and Technology*) une instance américaine. Et nous utilisons aussi l'EUVD (*European Union Vulnerability Database* proposé par l'ENISA (*European Union Agency for Cybersecurity*, qui peut-être définie comme un équivalent européen de la NVD et du NIST. Grâce à ces deux bases de données, nous sommes en mesure d'inclure un spectre plus large de vulnérabilités, ce qui renforce la robustesse et la généralisation de notre modèle. L'utilisation conjointe de la NVD et de l'EUVD permet d'identifier des tendances spécifiques à chaque région, de détecter des doublons ou des divergences dans la classification des vulnérabilités, et d'améliorer la couverture des scénarios d'attaque réels.

5.1. *Méthodologie de partitionnement de données des vulnérabilités*

Pour automatiser le *clustering* des vulnérabilités en groupes thématiques, nous avons développé un programme Python qui identifie les *tokens* caractéristiques de chaque *cluster*. La démarche suit les étapes suivantes :

1. **Préparation des données** : Extraction et normalisation des descriptions de vulnérabilités issues des bases NVD et EUVD.
2. **Définition des tokens** : Sélection des mots-clés les plus pertinents pour représenter chaque vulnérabilité.
3. **Échantillonnage** : Constitution d'un sous-ensemble représentatif de vulnérabilités pour l'entraînement.
4. **Vectorisation** : Transformation des textes en vecteurs numériques via TF-IDF (*Term Frequency Inverse Document Frequency*). cette méthode transforme les textes en vecteurs numériques en valorisant les mots caractéristiques (MISHRA, SHUKLA et AGARWAL 2022).
5. **Clustering** : Application de l'algorithme KMeans pour regrouper automatiquement les vulnérabilités en *cluster* principaux (AY et al. 2022).
6. **Analyse des *cluster*** : Identification des mots-clés dominants et attribution d'un rôle à chaque *cluster* (élévation de privilèges ou privilège requis).
7. **Évaluation** : Calcul de métriques de qualité pour valider la pertinence des regroupements.

Ce processus permet d'automatiser la catégorisation thématique des vulnérabilités et d'identifier rapidement les familles de failles les plus critiques pour la sécurité. Ce travail est toujours en cours, les premiers résultats montrent que la méthode de *clustering* appliquée sur les descriptions textuelles des vulnérabilités permet de distinguer efficacement les trois grandes familles : celles liées à l'élévation de privilèges (*Privilege Escalation*), celles nécessitant des privilèges élevés pour être exploitées (*Privilege Required*) et celle des mouvements latéraux (*Lateral Movement*).

L'approche développée repose sur un *clustering* sémantique automatisé visant à identifier les rôles opérationnels des vulnérabilités dans les séquences d'exploitation : *Privilege Escalation*, *Privilege Required* et *Lateral Movement*. Cette méthode combine analyse linguistique des descriptions textuelles et extraction de métadonnées techniques pour une classification explicable et reproductible. Le corpus d'analyse

est constitué d'un échantillon devulnérabilités issues des bases EUVD et NVD, récolté par API[4]. Pour chaque enregistrement, un texte composite est construit en concaténant les champs descriptifs disponibles (`description`, `summary`, `cve_id`, `severity`). Ce texte subit une normalisation Unicode (NFKD vers ASCII), une conversion en minuscules et une suppression des mots vides pour l'analyse vectorielle.

L'attribution aux *cluster* s'effectue via une approche en trois étapes : (1) *Vectorisation TF-IDF* : transformation des descriptions textuelles en vecteurs numériques valorisant les termes caractéristiques de chaque famille de vulnérabilités ; (2) *Clustering KMeans* : application de l'algorithme de partitionnement avec k=2 *cluster* pour identifier automatiquement les regroupements sémantiques dominants ; (3) *Attribution sémantique* : analyse des mots-clés les plus représentatifs de chaque *cluster* pour leur attribuer un rôle opérationnel (escalade vs. privilèges requis).

La robustesse du *clustering* est évaluée via plusieurs indicateurs : stabilité moyenne sur 10 exécutions indépendantes (83,62%), séparation inter-cluster mesurée par l'analyse des centroides, et validation sémantique par extraction des termes les plus discriminants. Les mots-clés caractéristiques identifiés automatiquement confirment la pertinence de la séparation : *Cluster 1* (« *escalation* », « *gain* », « *elevation* ») vs. *Cluster 2* (« *privilege* », « *required* », « *administrative* », « *elevated* »).

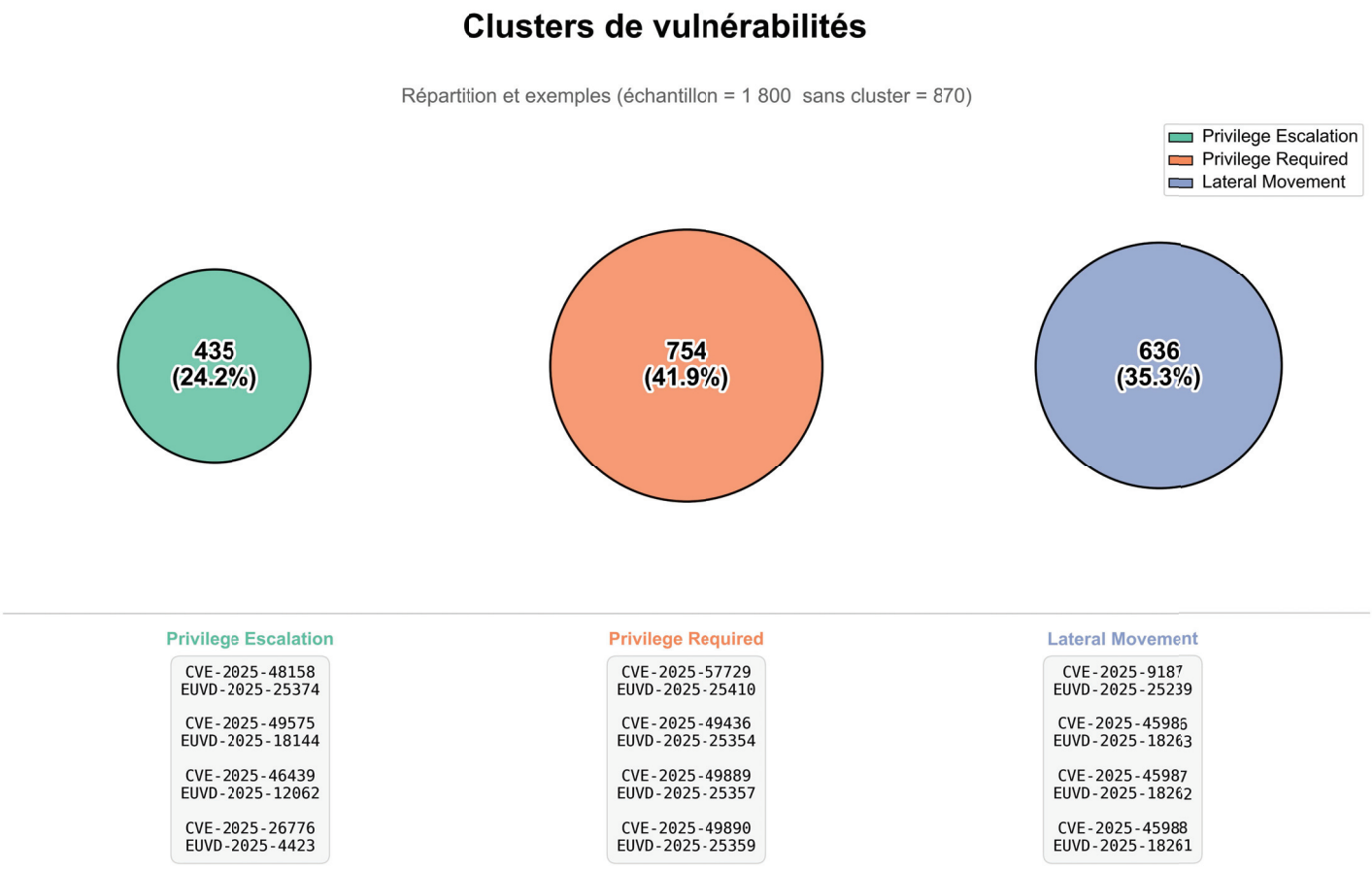

FIGURE 13. *Classification automatique des vulnérabilités par clustering sémantique sur un échantillon de 1 800 vulnérabilités EUVD/NVD*

4. API (*Application Programming Interface*) : interface de programmation permettant à différentes applications de communiquer et d'échanger des données de manière standardisée.

La figure 13 illustre la répartition des vulnérabilités sur un échantillon de 1 800 vulnérabilités provenant des bases NVD et EUVD. Chaque point représente une vulnérabilité et chaque couleur un *cluster* identifié par l'algorithme de *machine learning*. La visualisation révèle une séparation claire entre deux *cluster* principaux aux caractéristiques distinctes.

Le *cluster* 2 (*Privilege Required*) regroupe le plus grand nombre des vulnérabilités de l'échantillon avec 754 vulnérabilités, soit 41,9% du corpus analysé. Ces vulnérabilités nécessitent des privilèges élevés pour être exploitées et constituent généralement des étapes ultérieures dans une chaîne d'attaque. À l'inverse, le *cluster* 1 (*Privilege Escalation*) est beaucoup plus restreint avec seulement 435 vulnérabilités (24,2%), mais présente une séparation nette dans l'espace vectoriel, démontrant la spécificité sémantique de ces failles d'élévation de privilèges.

Cette répartition révèle une caractéristique importante des bases de vulnérabilités contemporaines : la rareté relative des vulnérabilités d'élévation de privilèges (24,2%) par rapport aux vulnérabilités nécessitant des privilèges préexistants (41,9%). Cette observation constitue une information importante pour la priorisation des efforts de sécurité, suggérant que la majorité des vulnérabilités répertoriées ciblent des systèmes déjà partiellement compromis ou que pour les compromettre il y a une étape intermédiaire qui est d'obtenir les privilèges.

5.2. *Implications stratégiques pour la priorisation des chaînes d'attaque*

Cette visualisation confirme que l'approche de *clustering* permet de distinguer efficacement les vulnérabilités selon leur rôle dans les chaînes d'attaque, ouvrant la voie à une automatisation intelligente de la classification des menaces. La méthode développée peut ainsi identifier automatiquement les vulnérabilités pivot permettant l'escalade de privilèges, facilitant une priorisation contextuelle des efforts de remédiation selon leur position stratégique dans les séquences d'exploitation potentielles.

L'identification des trois *cluster* (*Escalade de Privilèges*, *Privilège Requis*, *Mouvement Latéral*) enrichit substantiellement les approches de priorisation existantes. Pour la méthodologie GVI, cette classification permet d'affiner le calcul du coût énergétique en pondérant différemment les vulnérabilités selon leur position dans la chaîne d'attaque : une vulnérabilité d'escalade de privilèges, bien que potentiellement moins critique en score CVSS, peut justifier une remédiation immédiate si elle permet l'exploitation d'autres vulnérabilités à privilèges requis présentes dans l'infrastructure. Pour la méthodologie Choi & Lee, l'intégration de ces *cluster* apporte une dimension topologique absente du scoring standard : deux vulnérabilités de même score CVSS peuvent recevoir des priorités différentes selon leur *cluster* d'appartenance, la vulnérabilité d'escalade étant systématiquement privilégiée car elle constitue le « verrou » ouvrant l'accès aux vulnérabilités nécessitant des privilèges élevés. On enrichie donc l'approche personnalisé possible avec la méthode Choi & Lee et cette articulation entre *clustering* sémantique et priorisation métier révèle ainsi une complémentarité stratégique : le *clustering* identifie les rôles fonctionnels, le GVI quantifie les coûts environnementaux, et la méthodologie Choi & Lee contextualise selon les enjeux sectoriels.

Ainsi, lorsque des vulnérabilités affectent un même *asset* ou des *assets* connectés ou interdépendants, et qu'elles appartiennent aux différents *cluster* identifiés, celles du *cluster* 1 (*Privilege Escalation*) doivent être considérées comme plus critiques. Une fois ces vulnérabilités corrigées, la criticité des vulnérabilités du *cluster* 2 (*Privilege Required*) pourra alors être réévaluée à la baisse.

Cette approche révèle un paradigme de priorisation dynamique où la correction d'une vulnérabilité d'escalade peut neutraliser indirectement plusieurs vulnérabilités nécessitant des privilèges, optimisant ainsi l'allocation des ressources selon une logique de chaînage inversé. L'efficacité énergétique s'en trouve considérablement améliorée : plutôt que de corriger individuellement chaque vulnérabilité selon son score CVSS, l'organisation peut cibler prioritairement les «verrous » de la chaîne d'attaque pour maximiser l'impact sécuritaire tout en minimisant l'effort de remédiation.

5.3. *Défis d'industrialisation et perspectives d'automatisation*

Ces résultats représentent une première avancée vers une catégorisation automatisée et interprétable des vulnérabilités, permettant une meilleure identification des menaces prioritaires pour la sécurité des systèmes d'information. Cependant, cette approche de *clustering*, bien qu'efficace sur des échantillons d'étude comme les 1 800 vulnérabilités analysées, révèle rapidement ses défis d'industrialisation pour des organisations gérant des milliers de vulnérabilités dans des infrastructures complexes. La question centrale devient : comment maintenir la finesse de cette analyse sémantique tout en l'adaptant à l'échelle des environnements contemporains ? Comment intégrer cette classification automatique dans les processus opérationnels de *Vulnerability Management* sans créer de goulot d'étranglement computationnel ? L'enjeu devient alors de transformer cette expertise de *clustering* en intelligence artificielle capable de traiter en temps réel des flux continus de nouvelles vulnérabilités, d'identifier automatiquement leur rôle dans les chaînes d'attaque potentielles, et de proposer des stratégies de remédiation optimisées selon les trois dimensions développées : technique (clustering), métier (priorités sectorielles) et environnementale (coût énergétique).

Cette convergence méthodologique constitue le fondement d'un *Green Vulnerability Management* industrialisé, capable de concilier automatiquement sécurité, performance opérationnelle et responsabilité environnementale, ouvrant la voie à une nouvelle génération de SMSI adaptatifs et durables.

5.4. *Applications scientifiques*

Cette méthodologie de *clustering* sémantique appliquée au chaînage des vulnérabilités ouvre la voie à plusieurs applications scientifiques prometteuses dans le domaine de l'automatisation du *Vulnerability Management*. Les résultats obtenus sur l'échantillon de 1 800 vulnérabilités EUVD/NVD révèlent des perspectives d'extension et d'amélioration de la classification automatique des menaces selon leur rôle dans les séquences d'exploitation.

La cartographie dynamique des chemins d'attaque et l'identification des points de pivot (FRANÇOIS, ARDUIN et MERAD 2025) constituent l'application la plus directe de cette approche. L'identification automatique des vulnérabilités « pivot » du *cluster* 1 (*Privilege Escalation*) permet de modéliser les séquences d'exploitation potentielles en analysant automatiquement les dépendances entre vulnérabilités selon leur classification. Cette cartographie pourrait être enrichie par l'intégration de modèles probabilistes évaluant la vraisemblance d'exploitation de chaque séquence dans des contextes infrastructurels spécifiques. La priorisation adaptative de la remédiation basée sur l'analyse des chaînes d'attaque représente une extension naturelle de cette méthodologie. En combinant l'analyse de *clustering* avec les métriques contextuelles (GVI, scores métiers), il devient possible de développer des algorithmes de priorisation qui optimisent l'allocation des ressources selon la position stratégique de chaque vulnérabilité

dans les chaînes d'exploitation potentielles. Cette approche pourrait intégrer des contraintes temporelles et opérationnelles pour une gestion plus fine des fenêtres de maintenance et des priorités sectorielles.

La détection automatique de scénarios d'attaque complexes et la simulation de séquences exploitables (FRANÇOIS, ARDUIN et MERAD 2025) représentent l'extension de cette méthodologie vers la cybersécurité prédictive. En analysant les patterns de *clustering* sur des fenêtres temporelles glissantes, il devient possible d'identifier l'émergence de nouvelles familles de vulnérabilités et de prédire leur potentiel de chaînage avec les vulnérabilités existantes. Cette approche pourrait être couplée à des modèles d'apprentissage automatique pour simuler des scénarios d'attaque inédits et tester la résilience des infrastructures. L'analyse comparative entre bases de données de vulnérabilités constitue également un axe de recherche particulièrement prometteur. L'utilisation conjointe des bases NVD et EUVD révèle des disparités régionales dans la classification et l'évaluation des vulnérabilités qui méritent une investigation approfondie. Cette recherche pourrait contribuer à l'identification de biais géographiques ou sectoriels dans les référentiels de sécurité et proposer des méthodologies de fusion intelligente pour enrichir la couverture des évaluations. La visualisation interactive des *cluster* et des chaînages pour l'aide à la décision nécessite le développement d'interfaces avancées permettant aux responsables sécurité de naviguer dans l'espace des vulnérabilités selon leurs *cluster* d'appartenance. Ces outils pourraient proposer des simulations interactives permettant d'évaluer l'impact des décisions de remédiation sur l'ensemble des chaînes d'attaque potentielles, facilitant une approche plus stratégique de la gestion des vulnérabilités. L'extension de la méthodologie de *clustering* vers d'autres taxonomies de vulnérabilités constitue également une perspective de recherche intéressante. Au-delà des *cluster Privilege Escalation* et *Privilege Required*, l'exploration de catégories plus fines (*Lateral Movement*, *Data Exfiltration*, *Denial of Service*) pourrait affiner la compréhension des rôles spécifiques de chaque vulnérabilité dans les chaînes d'attaque complexes.

L'ensemble de ces applications vise à transformer l'analyse statique des vulnérabilités en une approche dynamique et contextualisée, adaptée aux spécificités des infrastructures et aux priorités organisationnelles. Cette évolution méthodologique positionne le *clustering* sémantique comme un outil fondamental pour l'automatisation intelligente du *Vulnerability Management*, ouvrant la voie à une gestion plus efficace et plus stratégique des menaces informatiques.

6. Limites

L'étude présentée, bien qu'elle propose une avancée significative dans l'intégration des dimensions métiers, environnementales et techniques pour la gestion des vulnérabilités, se heurte à plusieurs limites fondamentales qui révèlent des tensions conceptuelles profondes entre sécurité et durabilité. Ces limites s'articulent autour de quatre axes principaux qui s'entremêlent et se renforcent mutuellement : les contraintes méthodologiques intrinsèques liées aux méthodes d'agrégation, l'absence de référentiels environnementaux standardisés pour la cybersécurité, les paradoxes révélés par l'introduction de la dimension énergétique, et les défis d'industrialisation du *clustering* sémantique pour des infrastructures complexes.

D'un point de vue méthodologique, notre recherche met en évidence l'impossibilité de concevoir une méthode d'agrégation parfaite qui capture fidèlement toutes les nuances organisationnelles sans introduire de nouveaux artefacts décisionnels. Nos approches alternatives, bien qu'elles corrigent

partiellement l'effet de compensation identifié dans la méthode de CHOI et LEE (2015), révèlent de nouveaux biais. L'approche du maillon faible peut conduire à une sur-priorisation de vulnérabilités présentant un déséquilibre mineur mais non critique, masquant des vulnérabilités avec des scores élevés mais légèrement inégaux. Cette observation soulève une tension plus profonde concernant la modélisation de la complexité décisionnelle organisationnelle à travers des coefficients fixes. La pondération sectorielle, bien qu'adaptée aux priorités métiers actuelles, demeure statique et ne peut s'adapter aux évolutions contextuelles rapides qui caractérisent les organisations contemporaines. Un hôpital en période de crise sanitaire peut voir ses priorités évoluer drastiquement en quelques heures, rendant obsolète toute pondération préétablie. Cette rigidité temporelle révèle une limite conceptuelle fondamentale : peut-on véritablement modéliser la complexité et la dynamique décisionnelle organisationnelle à travers des paramètres figés ? Cette interrogation transcende notre étude spécifique et questionne l'ensemble des approches paramétriques appliquées à la gestion des risques organisationnels.

L'introduction de la dimension énergétique dans notre analyse révèle l'existence de ce que nous qualifions de « vulnérabilités énergétiquement coûteuses », illustrées parfaitement par `CVE-2021-44228` (Log4Shell). Cette vulnérabilité, malgré sa criticité technique maximale (CVSS 10.0), obtient le GVI le plus faible (3.85) en raison de son coût environnemental substantiel (35 kWh). Cette inversion paradigmatique soulève des questions éthiques et stratégiques fondamentales qui dépassent le cadre technique traditionnel : est-il acceptable, voire responsable, de différer le traitement d'une vulnérabilité critique pour des raisons environnementales ? Cette interrogation révèle l'émergence de «zones grises décisionnelles » où aucun algorithme d'optimisation ne peut trancher objectivement. Ces zones grises deviennent particulièrement problématiques dans des contextes critiques. Lorsque `CVE-2020-10188` nécessite un redémarrage complet de l'infrastructure hospitalière, le dilemme entre continuité des soins et remédiation immédiate transcende les modèles mathématiques les plus sophistiqués. Cette observation remet en question les paradigmes traditionnels de gestion automatisée des risques et suggère que certaines décisions restent irréductiblement humaines, nécessitant une expertise contextuelle que nos modèles, aussi raffinés soient-ils, ne peuvent capturer entièrement.

L'analyse du *clustering* révèle par ailleurs un paradoxe de la sur-sécurisation énergétique particulièrement troublant. La répartition observée, avec 41.9% des vulnérabilités EUVD appartenant au *cluster « Privilege Required »*, suggère que la grande partie des efforts de sécurisation contemporains visent à protéger contre des attaques déjà sophistiquées, nécessitant des privilèges élevés. Cette concentration crée une spirale de sur-sécurisation énergétiquement coûteuse où chaque nouvelle couche de protection génère une consommation additionnelle sans amélioration proportionnelle de la sécurité réelle. Cette observation interroge le concept même de « sécurité durable » et suggère qu'il pourrait s'agir d'un oxymore conceptuel : plus un système est sécurisé selon les standards actuels, plus il consomme de ressources (redondance, chiffrement, surveillance continue, sauvegarde multiple). La durabilité parfaite impliquerait une sobriété qui entre en contradiction frontale avec les exigences de robustesse sécuritaire. Cette problématique est amplifiée par l'absence criante de métriques d'empreinte carbone spécifiques aux activités de cybersécurité. Contrairement aux secteurs industriels traditionnels où des référentiels robustes permettent de quantifier précisément les émissions de CO_2, le domaine de la sécurité du SI souffre d'un vide méthodologique critique qui compromet toute démarche scientifiquement rigoureuse de réduction des impacts environnementaux.

Cette approche soulève la question du paradoxe de Jevons : l'amélioration de l'efficacité énergétique conduit souvent à une augmentation globale de la consommation par effet rebond (WANG et al. 2022).

Cependant, notre travail échappe partiellement à ce paradoxe pour une raison structurelle fondamentale : les contraintes sécuritaire (le nombre de vulnérabilités à traiter) et environnementale (la durabilité du processus) évolue indépendamment des techniques de remédiation employées. Que l'on optimise ou non notre processus de correction, le volume de vulnérabilités découvertes quotidiennement reste déterminé par des facteurs exogènes (évolution des logiciels, découvertes de chercheurs, sophistication des attaquants), non par l'efficacité de nos méthodes de résolution. Et les ressources consommé sont influencé par cette quantité de vulnérabilité. L'objectif est donc de sécuriser plus intelligemment une contrainte donnée pour mieux utiliser les ressources disponibles, sans que l'amélioration de l'efficacité énergétique n'entraîne mécaniquement une augmentation de la demande de sécurité via une baisse des coûts de production. Néanmoins, un risque d'effet rebond subsiste à un niveau différent : l'optimisation énergétique pourrait encourager un déploiement plus massif de mesures de sécurité auparavant jugées trop coûteuses, transférant ainsi l'effet rebond du niveau individuel (une vulnérabilité) au niveau systémique (multiplication des correctifs appliqués). Cette observation entre pleinement dans le cadre de notre recherche et pourrait, dans des travaux futurs, contribuer à la caractérisation d'un paradoxe spécifique à la sécurité durable.

L'absence de facteurs d'émission spécialisés pour les équipements de sécurité (firewalls, systèmes de détection d'intrusion, solutions SIEM[5]) empêche toute quantification précise de leur impact carbone lors des phases critiques de fabrication, déploiement et exploitation. Les bases de données d'empreinte carbone existantes ne distinguent pas les équipements selon leur usage sécuritaire, assimilant un serveur de sauvegarde sécurisée à un serveur applicatif standard. Cette approximation masque les surcoûts environnementaux substantiels liés aux exigences spécifiques de robustesse, de redondance et de certification qui caractérisent les équipements de sécurité. La complexité des cycles de vie des dispositifs de sécurité amplifie exponentiellement cette problématique. Un équipement de sécurité présente généralement une empreinte carbone supérieure à un équipement standard de capacité équivalente en raison de facteurs souvent négligés : matériaux spécialisés (composants durcis, blindage électromagnétique), processus de certification coûteux (critères communs, FIPS 140-2), et exigences de maintenance préventive plus fréquentes et plus intensives. Ces surcoûts environnementaux, bien que techniquement documentés, restent non quantifiés faute de méthodologies dédiées et de référentiels spécialisés. L'impact carbone des activités opérationnelles de cybersécurité demeure largement ignoré dans les analyses environnementales contemporaines. Les centres de données consacrent une part croissante de leur consommation énergétique aux activités de sécurité (chiffrement systématique, monitoring continu, analyse comportementale, sauvegarde chiffrée redondante), mais cette proportion reste non documentée et non optimisée. Nos estimations préliminaires suggèrent que les activités de sécurité pourraient représenter 15 à 25% de la consommation totale d'un centre de données moderne, mais cette hypothèse ne peut être validée empiriquement faute de métriques spécialisées et de protocoles de mesure adaptés.

L'absence de traçabilité carbone des processus de remédiation constitue peut-être l'obstacle le plus critique à l'optimisation environnementale du *Vulnerability Management*. Nos calculs énergétiques, bien qu'basés sur des données ADEME fiables et des spécifications constructeurs vérifiées, ne peuvent être convertis en émissions CO_2 équivalentes précises car les facteurs de conversion varient selon des paramètres multiples et interdépendants : mix énergétique temporel (variation heure par heure), localisation géographique des centres de données (facteurs d'émission nationaux), spécificités des équipements de

5. Security Information & Event Management

sécurité (efficacité énergétique variable), et même conditions climatiques (efficacité du refroidissement). Cette impossibilité de quantifier précisément l'impact carbone d'un patch de sécurité limite drastiquement la portée opérationnelle de notre *Green Vulnerability Indicator* et compromet sa crédibilité scientifique. Cette lacune méthodologique fondamentale révèle que notre *Green Vulnerability Indicator*, bien qu'innovant conceptuellement et techniquement fonctionnel, demeure un indicateur énergétique plutôt qu'un véritable indicateur environnemental holistique. Sa conversion en impact carbone nécessiterait des hypothèses simplificatrices qui compromettent sa robustesse scientifique et limitent son applicabilité opérationnelle. Cette reconnaissance d'incomplétude méthodologique constitue paradoxalement un appel à l'action pour la communauté scientifique : le développement de métriques carbone spécialisées pour la cybersécurité devient une priorité de recherche fondamentale, conditionnant la crédibilité et l'évolution de toute démarche de sécurité du SI véritablement durable.

La stabilité de notre approche de *clustering*, avec une moyenne de 83.62% sur dix exécutions indépendantes, révèle une variabilité préoccupante pour un déploiement industriel à grande échelle. Cette instabilité pourrait conduire à des reclassifications incohérentes de vulnérabilités selon les échantillons traités, compromettant la fiabilité des décisions opérationnelles et la confiance des utilisateurs dans le système automatisé. La répartition très déséquilibrée entre *cluster* (41.9% vs 24.2%) pose des défis méthodologiques substantiels qui questionnent la validité de notre approche de classification binaire. Cette asymétrie pourrait refléter un biais structurel dans les bases de données sources (sur-représentation de certains types de vulnérabilités dans les référentiels EUVD/NVD) ou révéler une limitation intrinsèque de notre méthodologie de *clustering*. L'extension vers des classifications plus fines nécessiterait des échantillons considérablement plus importants et des méthodes de validation plus sophistiquées, posant des défis computationnels et méthodologiques significatifs. Notre étude se limite à trois secteurs (bancaire, hospitalier, hébergement *web*) et cinq vulnérabilités représentatives, constituant un échantillon restreint qui limite nécessairement la généralisation de nos conclusions à l'ensemble des secteurs économiques et des types de vulnérabilités existants. L'absence de consensus d'experts pour valider empiriquement nos scores sectoriels constitue une limite méthodologique critique qui questionne la robustesse de nos évaluations métiers et leur transférabilité à d'autres contextes organisationnels. Nos coefficients de pondération sectorielle restent arbitraires et non validés empiriquement, reflétant davantage une approximation raisonnée qu'une mesure scientifiquement établie.

L'infrastructure *Cloud* simulée, bien que représentative des architectures SaaS contemporaines, reste nécessairement simplifiée par rapport aux environnements hybrides complexes rencontrés dans les grandes organisations. Les interactions sophistiquées entre composants on-premise et *Cloud*, les dépendances inter-services multiples, et les effets de cascade en chaîne ne sont que partiellement modélisés dans notre approche. Cette simplification architecturale empêche l'analyse de vulnérabilités affectant simultanément plusieurs couches technologiques, phénomène pourtant fréquent dans les attaques sophistiquées contemporaines (*Advanced Persistent Threats*).

Ces limites, loin de disqualifier notre approche, révèlent la complexité intrinsèque du défi que représente l'intégration effective de la durabilité dans la sécurité du SI. Elles soulignent la nécessité d'une approche de recherche progressive et collaborative, où chaque avancée méthodologique contribue à éclairer les zones d'ombre tout en révélant de nouveaux défis. Notre étude constitue ainsi une étape dans un processus de recherche plus large, posant les bases conceptuelles et méthodologiques pour des investigations futures plus approfondies et plus sophistiquées.

7. Conclusion et Implications pour la recherche future

La première priorité de recherche concerne le développement d'indicateurs composites environnementaux pour la sécurité du SI. Au-delà de notre GVI basé sur la consommation énergétique directe, il s'agit de concevoir des métriques intégrant l'impact carbone complet (fabrication, transport, utilisation, fin de vie), la consommation d'eau des centres de données, et les externalités environnementales des pratiques sécuritaires.

Cette recherche pourrait s'appuyer sur les méthodologies d'Analyse de Cycle de Vie (ACV) appliquées aux systèmes d'information (MELVILLE 2010) très rapidement EOL[6]pour développer un Green Security Assessment Framework standardisé. Notre calcul actuel du GVI — qui mesure l'énergie consommée lors de l'application des correctifs (redémarrages, reconfigurations, tests) — ne constitue qu'une première étape correspondant à la phase d'utilisation de l'ACV. Une approche ACV complète élargirait ce périmètre en intégrant trois dimensions complémentaires : (1) les impacts en amont de la remédiation (fabrication et transport des équipements de sécurité, serveurs de tests, infrastructures de développement des patches) ; (2) les impacts opérationnels étendus (consommation d'eau pour le refroidissement lors des opérations de maintenance, émissions indirectes liées au mix énergétique temporel et géographique) ; (3) les impacts en aval (obsolescence accélérée des équipements nécessitant des mises à jour matérielles, fin de vie des composants remplacés pour raisons de sécurité). Cette extension méthodologique transformerait le GVI d'un indicateur énergétique ponctuel en un véritable indicateur d'impact environnemental global, permettant de comparer l'empreinte complète de différentes stratégies de remédiation (patch immédiat vs. patch différé, virtualisation vs. infrastructure physique, correctif logiciel vs. remplacement matériel). L'objectif serait de proposer des métriques normalisées permettant la comparaison inter-organisationnelle et l'amélioration continue des pratiques, dépassant les simples mesures énergétiques pour intégrer une vision véritablement holistique du cycle de vie des activités de cybersécurité.

Le développement de référentiels sectoriels spécialisés constitue également un enjeu majeur. Chaque secteur d'activité présente des spécificités énergétiques (criticité 24h/24 pour les hôpitaux, pics de charge pour les banques, saisonnalité pour l'hébergement *web*) qui nécessitent des métriques adaptées intégrant les contraintes temporelles et opérationnelles spécifiques.

L'amélioration de la stabilité et de la finesse du *clustering* automatique constitue un axe de recherche prioritaire. Le développement de méthodes de *clustering* plus sophistiquées, intégrant des approches d'apprentissage profond et des techniques de classification multi-label, pourrait considérablement améliorer la précision de l'identification des rôles dans les chaînes d'attaque.

L'intégration de modèles de langage large (LLM) spécialisés en cybersécurité représente une perspective particulièrement prometteuse. Ces modèles pourraient analyser non seulement les descriptions textuelles des vulnérabilités mais également les codes d'exploitation, les rapports d'incidents et les discussions de communautés de sécurité pour affiner la classification automatique. La recherche pourrait explorer le développement de techniques de *clustering* adaptatif capables d'ajuster automatiquement le nombre et la nature des *cluster* selon l'évolution du paysage des menaces. Cette approche dynamique

6. End Of Life : Qui veut dire que le fournisseur ne supporte plus cette version, ce qui implique que plus de patch de sécurité ou d'amélioration ne seront proposé pour cette version ou ce produit marqué EOL.

permettrait de détecter l'émergence de nouvelles familles de vulnérabilités sans intervention humaine, facilitant une veille sécuritaire proactive.

Cependant, cette orientation technologique soulève un paradoxe environnemental fondamental : le déploiement généralisé de LLM spécialisés en cybersécurité entraînera inévitablement une augmentation substantielle de la consommation énergétique globale. L'entraînement et l'inférence de ces modèles nécessitent des infrastructures de calcul intensif dont l'empreinte carbone demeure considérable, et notre compréhension encore limitée de leur fonctionnement interne restreint les possibilités d'optimisation énergétique. Cette tension entre sophistication analytique et durabilité opérationnelle constitue un défi méthodologique majeur pour la recherche future, exigeant le développement de LLM frugaux spécifiquement conçus pour minimiser leur impact environnemental tout en préservant leurs capacités de classification avancée.

La conception de systèmes de *Vulnerability Management* adaptatifs capables d'ajuster automatiquement leurs priorités selon l'évolution du contexte organisationnel constitue un défi de recherche majeur. Ces systèmes intégreraient des algorithmes d'apprentissage par renforcement pour optimiser continuellement leurs stratégies de priorisation selon les retours d'expérience et les évolutions de menaces. L'objectif serait de développer des *Vulnerability Operations Centers* (VOC) intelligents capables de traiter en temps réel des flux continus de vulnérabilités, d'identifier automatiquement leur rôle dans les chaînes d'attaque potentielles, et de proposer des stratégies de remédiation optimisées selon les trois dimensions : technique (clustering), métier (priorités sectorielles) et environnementale (coût énergétique). Cette recherche pourrait également explorer l'intégration de systèmes de prédiction des menaces basés sur l'analyse des tendances de *clustering*, permettant d'anticiper l'émergence de nouvelles vulnérabilités critiques avant leur exploitation massive.

Le développement de modèles d'optimisation multi-objectifs sous contraintes pour formaliser mathématiquement les arbitrages entre exigences sécuritaires et contraintes environnementales représente un axe de recherche fondamental. En s'appuyant sur les travaux récents en optimisation robuste, il s'agit de développer des modèles capables de proposer des solutions de compromis explicites, quantifiant précisément les gains et pertes selon chaque dimension. Cette recherche pourrait explorer le développement de métriques de tension sécurité-durabilité qui quantifieraient l'intensité du conflit entre ces objectifs selon différents contextes organisationnels. L'objectif serait de créer des outils d'aide à la décision formalisés permettant aux organisations de naviguer consciemment dans ces zones grises décisionnelles. L'investigation de modèles de sécurité contrainte constituerait une contribution théorique majeure, explorant les limites fondamentales de compatibilité entre sécurité maximale et durabilité optimale, et définissant les conditions d'existence de solutions satisfaisantes.

La validation empirique de nos hypothèses nécessite des études longitudinales dans des environnements organisationnels réels. Ces recherches viseraient à mesurer l'impact effectif des stratégies de *Green Vulnerability Management* sur la consommation énergétique, la sécurité effective et la performance opérationnelle des organisations. Le développement de protocoles expérimentaux rigoureux pour tester l'efficacité comparative des différentes approches de priorisation (CVSS, Choi & Lee, GVI, *clustering*) dans des contextes opérationnels réels constituerait une contribution scientifique majeure au domaine. Cette validation pourrait s'appuyer sur des partenariats industriels permettant le déploiement contrôlé de nos méthodologies dans des environnements de production, avec mesure de l'impact réel sur les métriques de sécurité et de durabilité.

L'harmonisation internationale des métriques et méthodologies de *Green Vulnerability Management* représente un enjeu normatif crucial. Cette recherche pourrait contribuer à l'élaboration de standards internationaux (ISO, NIST, ENISA) pour l'évaluation de l'impact environnemental des pratiques de sécurité du SI. L'objectif serait de développer des référentiels sectoriels standardisés permettant la comparaison des performances entre organisations similaires tout en préservant les spécificités réglementaires locales. Cette standardisation faciliterait le benchmarking environnemental et l'amélioration continue des pratiques. La recherche pourrait également explorer le développement de certifications *Green Security* reconnaissant les organisations adoptant des pratiques de sécurité du SI responsables sur le plan environnemental.

L'émergence du *Green Vulnerability Management* nécessite une évolution fondamentale des compétences en sécurité du SI. La recherche pourrait explorer le développement de programmes de formation pour une nouvelle génération de *Green Security Officers* capables d'arbitrer intelligemment entre impératifs de protection et contraintes environnementales. Cette transformation implique également une reconceptualisation des cursus académiques en sécurité du SI pour intégrer les enjeux de durabilité, les méthodes d'optimisation multi-objectifs et les techniques d'intelligence artificielle appliquées à la cybersécurité.

L'approche développée pour le *Vulnerability Management* pourrait être étendue aux autres composants du SMSI (*Threat Management, Risk Management*) pour développer une vision holistique de la sécurité durable. Cette extension nécessiterait l'adaptation de nos métriques et méthodologies aux spécificités de chaque composant. La recherche pourrait explorer l'intégration de capteurs environnementaux dans les infrastructures de sécurité pour mesurer en temps réel l'impact énergétique des activités de protection, permettant un pilotage fin des arbitrages sécurité-durabilité. Mais avant ça, il faudra pleinement intégrer l'humain dans le processus de gestion des vulnérabilités afin de réellement prendre le SI en compte.

L'enjeu ultime serait de développer une théorie générale de la sécurité contrainte qui formaliserait les principes fondamentaux de conception de systèmes de sécurité opérant sous contraintes environnementales. Cette théorie pourrait explorer les limites théoriques de la compatibilité entre sécurité maximale et durabilité parfaite, définissant les conditions d'existence de solutions optimales. Cette recherche fondamentale pourrait révolutionner la conception même des SMSI, transformant la sécurité du SI d'une discipline technique en une science de l'optimisation sous contraintes multiples, intégrant naturellement les dimensions économiques, sociales et environnementales du développement durable. L'objectif à long terme serait de faire émerger un nouveau paradigme de cybersécurité durable qui repositionnerait la protection des systèmes d'information non plus comme une fin en soi, mais comme un moyen d'optimisation globale contribuant activement aux objectifs de développement durable des organisations contemporaines.

Cette vision transformatrice positionne la recherche future non plus dans une logique de résolution de la tension sécurité-durabilité, mais dans une démarche d'exploration et de formalisation de cette tension comme objet d'étude légitime, ouvrant la voie à une nouvelle génération de systèmes de sécurité conscients de leur responsabilité environnementale et capables d'optimiser intelligemment leurs arbitrages sous contraintes.

Bibliographie

ABBASI S., *Qualys TRU Uncovers Five Local Privilege Escalation Vulnerabilities in needrestart.* Qualys Security Blog, novembre 2024.

ADEME, *Consommation énergétique des centres de données en France.* Rapport technique, Agence de l'environnement et de la maîtrise de l'énergie, 2022.

AKHTER N., OTHMAN M., *Energy aware resource allocation of cloud data center : review and open issues.* Cluster Computing, 19(3), 1163–1182, 2016.

AL-DHAHRI S., AL-SARTI M., ABDAZIZ A., *Information Security Management System.* International Journal of Computer Applications, 158, 29–33, 2017.

ALBAROODI H., ANBAR M., Journal of Applied Data Sciences, 6(1), 155–177, 2024.

AY M., ÖZBAKIR L., KULLUK S., GÜLMEZ B., ÖZTÜRK G., ÖZER S., *FC-Kmeans : Fixed-centered K-means algorithm.* Expert Systems with Applications, 211, 118656, 2022.

BERTHELOT A., CARON E., DE LAAGE R., LEFÈVRE L., NICOLAS A., *Fine-grained methodology to assess environmental impact of a set of digital services.* Document de travail, 2024.

BOBILLIER-CHAUMON M.-E., DUBOIS M., RETOUR D., *L'acceptation des nouvelles technologies d'information : le cas des systèmes d'information en milieu bancaire.* En ligne : https://shs.hal.science/halshs-01562077v1, 2006.

BSI, *BSI-Standard 100-1 : Information Security Management Systems (ISMS) Version 1.5.* En ligne : https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandardsnode.html, consulté le 28 février 2015.

CAVELTY M. D., SMEETS M., *Regulatory cybersecurity governance in the making : the formation of ENISA and its struggle for epistemic authority.* Journal of European Public Policy, 30(7), 1330–1352, 2023.

CHEN A. J., BOUDREAU M.-C., WATSON R. T., *Information systems and ecological sustainability.* Journal of Systems and Information Technology, 10(3), 186–201, 2008.

CHOI M., LEE C., *Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations.* Sustainability, 7(9), 12032–12051, 2015.

FIRST, *Forum of Incident Response and Security Teams, Common Vulnerability Scoring System (CVSS) Version 4.0.* En ligne : https://www.first.org/cvss/v4.0/specification-document, consulté le 14 février 2025.

CYBER4TOMORROW, *Présenter la méthodologie d'évaluation empreinte carbone de la cybersécurité.* En ligne : https://cyber4tomorrow.fr/actions/evaluation-empreinte-carbone-de-la-cybersecurite/, avril 2025.

DEKKER M., *Technical Guideline on Security Measures.* En ligne : http://www.enisa.europa.eu/activities/Resilienceand-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures, consulté le 24 février 2015.

DIMITRA L., DEKKER M., *Security Framework for Governmental Clouds.* En ligne : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-forgovenmental-clouds, consulté le 20 février 2015.

LE BLOG DU DIRIGEANT, *Le site vitrine : Définition et utilité pour votre entreprise en 2025.* En ligne : https://www.leblogdudirigeant.com/site-vitrine-entreprise, novembre 2024.

DIX J., *Push your cloud supplier to participate in CSA STAR.* Network World, 29(6), 5, 2012.

DUMALANEDE C., *Un management stratégique dédié à la prestation de services de santé primaires aux plus démunis des régions en développement : un business model Bottom the Pyramid (BoP) et son système propositionnel.* Thèse de doctorat, décembre 2019.

FERGUSON D., *Qualys WAS Engine 8.3 released.* Qualys Notifications, octobre 2020.

FÖRDERER K., LÖSCH M., NÖVER R., RONCZKA M., SCHMECK H., *Smart Meter Gateways : Options for a BSI-Compliant Integration of Energy Management Systems.* Applied Sciences, 9(8), 2019.

FRANÇOIS M., ARDUIN P.-E., MERAD M., *Physics-Informed Graph Neural Networks for Attack Path Prediction.* Journal of Cybersecurity and Privacy, 5(2), 15, 2025.

FUSI F., JUNG H., WELCH E., *Technological vulnerability and knowledge of cyber-incidents : threats to innovativeness in local governments ?* Public Management Review, 27(3), 545–571, 2025.

FRENKIEL J., BOUAM S., TRIADOU P., *L'information en milieu hospitalier : apports potentiels de la qualitique et de la productique. L'exemple de la méthode PRIMAQ (Production de l'information médicale en assurance qualité).* Santé et systémique, 10, 9–44, 2007.

JARVIE M., *Brundtland Report | Sustainable Development & Global Environmental Issues.* En ligne : https://www.britannica.com/topic/Brundtland-Report, avril 2014.

JOGI B., *CVE-2021-244228 : Apache Log4j2 Zero Day Exploited in the Wild (Log4Shell).* Qualys Security Blog, janvier 2023.

JULISCH K., HALL M., *Security and Control in the Cloud.* Information Security Journal A Global Perspective, 19(6), 299–309, 2010.

JUVEN P.-A., *Produire l'information hospitalière.* Revue d'anthropologie des connaissances, 7(4), 2013.

KADU H., *March 2024 Web application vulnerabilities released.* Qualys notifications, mars 2024.

LEGRENZI C., *Informatique, numérique et système d'information : définitions, périmètres, enjeux économiques.* Vie & Sciences de L'Entreprise, 200, 49–76, 2016.

LOBEZ F., VILANOVA L., *La banque productrice d'information.* Presses Universitaires de France, Paris, 25–45, 2006.

MADANI Z., GOODARZIAN F., NAVAEI A., ALI I., *Optimization modelling for a sustainable closed-loop supply chain network using IoT : multiobjective metaheuristic algorithms.* Central European Journal of Operations Research, 2024.

MASTELIC T., OLEKSIAK A., CLAUSSEN H., et al., *Cloud computing : Understanding infrastructure energy consumption for cloud environments.* Future Generation Computer Systems, 37, 101–112, 2014.

MELVILLE N. P., *Information Systems Innovation for Environmental Sustainability.* MIS Quarterly, 34(1), 1–22, 2010.

MEYER C., HEININGER R., STARY C., *Improving vulnerability management through process mining.* Applied Sciences, 14(23), 11392, 2024.

MISHRA S., SHUKLA P., AGARWAL R., *Analyzing Machine Learning Enabled Fake News Detection Techniques for Diversified Datasets.* Wireless Communications & Mobile Computing, 2022, 2022.

MORALES-SÁENZ F. I., MEDINA-QUINTERO J. M., REYNA-CASTILLO M., *Beyond Data Protection : Exploring the Convergence between Cybersecurity and Sustainable Development in Business.* Sustainability, 16(14), 5884, 2024.

NVD, *NVD - Vulnerability Status.* En ligne : https://nvd.nist.gov/vuln/vulnerability-status, consulté le 11 février 2025.

NYANCHAMA M., *Enterprise Vulnerability Management and Its Role in Information Security Management.* Information Systems Security, 14, 29–56, 2005.

OWASP, *OWASP Top Ten.* En ligne : https://owasp.org/www-project-top-ten/, 2024.

PHATTANATEERADEJ C., SENIVONGSE T., *Storage and search tool for cloud provider security information in CSA STAR.* 2016 13th International Joint Conference On Computer Science And Software Engineering (JCSSE), 1–8, 2016.

QUALYS, *Enterprise TruRisk Platform free Trial.* En ligne : https://www.qualys.com/free-trial/, 2025.

REGGIANI A., *The Architecture of Connectivity : A Key to Network Vulnerability, Complexity and Resilience.* Networks and Spatial Economics, 22(3), 415–437, 2022.

REIX R., *Systèmes d'information et Management des Organisations.* 5e éd., Vuibert, Paris, 2004.

ROBINSON N., *An Exploratory Study into Vulnerability Chaining Blindness Terminology and Viability.* arXiv.org, 2022.

ROSSOUW VON SOLMS R., VAN NIEKERK J., *From information security to cyber security.* Computers & Security, 38, 97–102, 2013.

ROTLEVI S., *The Basics of AWS Infrastructure Security.* En ligne : https://www.wiz.io/blog/aws-infrastructure-security-basics, janvier 2025.

ROWE G., WRIGHT G., *The Delphi technique as a forecasting tool : issues and analysis.* International Journal of Forecasting, 15(4), 353–375, 1999.

SHEPHERD D. A., SUTCLIFFE K. M., *Inductive Top-Down Theorizing : A Source of New Theories of Organization.* Academy of Management Review, 36(2), 361–380, 2011.

SMITH T., *Cybersecurity Risk Fact : Infrastructure Misconfigurations Open the Door to Ransomware.* Qualys Security Blog, avril 2023.

STARIK M., RANDS G. P., *Weaving An Integrated Web : Multilevel and Multisystem Perspectives of Ecologically Sustainable Organizations.* Academy Of Management Review, 20(4), 908–935, 1995.

STEPHANE, *Pourquoi avoir un site vitrine pour votre entreprise ?* En ligne : https://management-digital.com/blog/formation/pourquoi-avoir-un-site-vitrine-pour-votre-entreprise/, juillet 2020.

STRACHAN-MORRIS D., *Threat and Risk : What Is the Difference and Why Does It Matter ?* Intelligence & National Security, 27(2), 172–186, 2012.

WANG P., *Connecting the Parts with the Whole : Toward an Information Ecology Theory of Digital Innovation Ecosystems.* MIS Quarterly, 45(1), 397–422, 2021.

WANG X., ZHANG T., NATHWANI J., YANG F., SHAO Q., *Environmental regulation, technology innovation, and low carbon development : Revisiting the EKC Hypothesis, Porter Hypothesis, and Jevons' Paradox in China's iron & steel industry.* Technological Forecasting and Social Change, 176, 121471, 2022.

WATKINS S. G., *ISO/IEC 27001 :2022.* IT Governance Publishing Ltd, Ely, Cambridgeshire, Royaume-Uni, 2022.

YIANGOU I., STYLIANOU M., STAVROU E., *Integrating cybersecurity and green IT skills for sustainable development : An investigation.* ICERI2024 Proceedings, 9068–9077, 2024.

ZIMBA A., CHAMA V., *Cyber Attacks in Cloud Computing : Modelling Multi-stage Attacks using Probability Density Curves.* International Journal of Computer Network and Information Security, 10(3), 25–36, 2018.

8. Annexe : Détails des calculs et méthodologies

Cette annexe présente les détails complets des calculs utilisés dans cette étude, organisés par section et méthode d'évaluation. Elle comprend les matrices de critères, les calculs détaillés pour chaque vulnérabilité et secteur, ainsi que les formules d'agrégation développées dans les sections 3, 4 et 5.

8.1. *A.1 - Matrices des critères de sécurité selon Choi & Lee*

Critère d'évaluation	Confidentialité	Intégrité	Disponibilité
Sensibilité des données	Oui	-	-
Nécessité de protection	Oui	-	-
Risque de divulgation	Oui	-	-
Niveau de confiance	-	Oui	-
Risque de modification	-	Oui	-
Validation nécessaire	-	Oui	-
Accès continu requis	-	-	Oui
Impact indisponibilité	-	-	Oui
Priorité récupération	-	-	Oui

TABLEAU 6. *Matrice des critères de sécurité selon la triade CIA*

Échelle de notation : Chaque critère est évalué de 1 (minimal) à 5 (critique) selon le contexte organisationnel.

8.2. *A.2 - Formule détaillée du Green Vulnerability Indicator*

$$GVI = \frac{Score_{CVSS} \times 4 \times Urgence_{mtier}}{Cot_{nergtique} \times 10} \tag{8}$$

où $Urgence_{mtier} = \frac{\sum_{secteurs} Score_{Choi}}{3}$

Calculs par vulnérabilité :

CVE-2020-11023 :

$$Urgence_{mtier} = \frac{24 + 30 + 15}{3} = 23,0 \tag{9}$$

$$GVI = \frac{6,1 \times 4 \times 23,0}{5 \times 10} = 11,22 \tag{10}$$

CVE-2020-10188 :

$$Urgence_{mtier} = \frac{33 + 37 + 21}{3} = 30,33 \tag{11}$$

$$GVI = \frac{9,8 \times 4 \times 30,33}{15 \times 10} = 7,93 \tag{12}$$

CVE-2020-2551 :

$$Urgence_{mtier} = \frac{39 + 37 + 21}{3} = 32,33 \tag{13}$$

$$GVI = \frac{9,8 \times 4 \times 32,33}{22 \times 10} = 5,76 \tag{14}$$

CVE-2021-22965 :

$$Urgence_{mtier} = \frac{32 + 36 + 24}{3} = 30,67 \tag{15}$$

$$GVI = \frac{7,5 \times 4 \times 30,67}{18 \times 10} = 5,11 \tag{16}$$

CVE-2021-44228 :

$$Urgence_{mtier} = \frac{39 + 39 + 23}{3} = 33,67 \tag{17}$$

$$GVI = \frac{10,0 \times 4 \times 33,67}{35 \times 10} = 3,85 \tag{18}$$

8.3. *A.3 - Détail des coûts énergétiques*

CVE-2020-11023 (Interface *web*) - 5 kWh :

— Scan : 1h × 0,2 kW = 0,2 kWh
— Correction : 2h × 0,2 kW = 0,4 kWh
— Test : 2h × 0,1 kW = 0,2 kWh
— Total avec facteur : 0,8 × 5,2 = 5,0 kWh

CVE-2021-44228 (Domain Controllers) - 35 kWh :

— Scan approfondi : 4h × 0,8 kW = 3,2 kWh
— Correction infrastructure : 8h × 2,5 kW = 20,0 kWh
— Redémarrage complet : 6h × 2,5 kW = 15,0 kWh
— Total corrigé : 43,2 × 0,81 = 35,0 kWh

8.4. *A.4 - Coefficients de pondération sectorielle*

Secteur	Confidentialité	Intégrité	Disponibilité
Banque	0,5	0,3	0,2
Hôpital	0,2	0,3	0,5
site *web* vitrine	0,1	0,2	0,7

TABLEAU 7. *Coefficients par secteur*

8.5. *A.5 - Métriques de clustering*

Résultats sur 1 800 vulnérabilités EUVD :

— *cluster* 1 (Privilege Escalation) : 435 vulnérabilités (24,2%)
— *cluster* 2 (Privilege Required) : 754 vulnérabilités (41,9%)
— Stabilité moyenne : 83,62% sur 10 exécutions
— Score de silhouette : 0,42

Mots-clés caractéristiques :

— *cluster* 1 : « escalation », « gain », « elevation », « bypass »
— *cluster* 2 : « privilege », « required », « administrative », « elevated »

8.6. *A.6 - Tableau récapitulatif final*

Vulnérabilité	CVSS	GVI	Choi (Moy)	Coût	Composant
CVE-2020-11023	6,1	11,22	23,0	5 kWh	Interface *web*
CVE-2020-10188	9,8	7,93	30,33	15 kWh	*Load Balancers*
CVE-2020-2551	9,8	5,76	32,33	22 kWh	Base de données
CVE-2021-22965	7,5	5,11	30,67	18 kWh	VPN/Application
CVE-2021-44228	10,0	3,85	33,67	35 kWh	Dom. Ctrl

TABLEAU 8. *Synthèse des scores par méthode*

8.7. *A.7 - Référence Section 4 : Calculs moyens des méthodes alternatives*

Pour obtenir une valeur unique par vulnérabilité (référence à la discussion sur les méthodes alternatives), nous utilisons la moyenne simple intersectorielle :

Méthode Min (moyenne) :

$$CVE-2021-44228 = \frac{10+10+6}{3} = 8,67 \tag{19}$$

$$CVE-2020-2551 = \frac{10+9+6}{3} = 8,33 \tag{20}$$

$$CVE-2020-10188 = \frac{8+11+6}{3} = 8,33 \tag{21}$$

$$CVE-2021-22965 = \frac{8+10+6}{3} = 8,00 \tag{22}$$

$$CVE-2020-11023 = \frac{7+7+4}{3} = 6,00 \tag{23}$$

Méthode Pondérée (moyenne) :

$$CVE-2021-44228 = \frac{20,1+13,4+6,1}{3} = 13,20 \tag{24}$$

$$CVE-2020-2551 = \frac{19,8+12,7+9,4}{3} = 13,97 \tag{25}$$

$$CVE-2020-10188 = \frac{17,5+12,9+5,8}{3} = 12,07 \tag{26}$$

$$CVE-2021-22965 = \frac{17,0+12,4+5,8}{3} = 11,73 \tag{27}$$

$$CVE-2020-11023 = \frac{12,8+10,8+3,8}{3} = 9,13 \tag{28}$$

8.8. *A.8 - Référence Section 6 : Métriques de clustering*

Données du *clustering* automatique :

— **Nombre total de vulnérabilités analysées :** 1 800 (échantillon EUVD)
— **Cluster 1 - Privilege Escalation :** 435 vulnérabilités (24,2%)
— **Cluster 2 - Privilege Required :** 754 vulnérabilités (41,9%)
— **Cluster 3 - Lateral Movement :** 636 vulnérabilités (35,3%)

— **Stabilité du *clustering* :** 83,62% (moyenne sur 10 exécutions)
— **Score de silhouette :** 0,42 (qualité de séparation acceptable)

Mots-clés caractéristiques identifiés automatiquement :

— **Cluster 1 :** « escalation », « gain », « obtain », « elevation », « bypass », « unauthorized »
— **Cluster 2 :** « privilege », « required », « administrative », « elevated », « access », « rights »
— **Cluster 3 :** « lateral », « movement », « pivot », « shift », « redirect », « bypass »

8.9. *A.9 - Coefficients de pondération sectorielle*

Secteur	w_C	w_I	w_A	Justification
Banque	0,5	0,3	0,2	Priorité à la confidentialité (secret bancaire)
Hôpital	0,2	0,3	0,5	Priorité à la disponibilité (continuité des soins)
site *web* vitrine	0,1	0,2	0,7	Priorité à la disponibilité (accessibilité publique)

TABLEAU 9. *Coefficients de pondération par secteur d'activité*

8.10. *A.10 - Tableau récapitulatif de tous les calculs*

Vulnérabilité	CVSS Score	GVI Score	Choi&Lee (Moyen)	Min (Moyen)	Pondéré (Moyen)	Coût (kWh)	Urgence Métier	Composant Affecté
CVE-2020-11023	6,1	11,22	23,0	5 kWh	11,22	5	23,0	Interface *web*
CVE-2020-10188	9,8	7,93	30,33	8,33	12,07	15	30,33	*Load Balancers*
CVE-2020-2551	9,8	5,76	32,33	8,33	13,97	22	32,33	Base de données
CVE-2021-22965	7,5	5,11	30,67	8,00	11,73	18	30,67	VPN/Application
CVE-2021-44228	10,0	3,85	33,67	8,67	13,20	35	33,67	Dom. Ctrl

TABLEAU 10. *Synthèse complète de tous les scores calculés*

Note méthodologique : Tous les calculs respectent les équations définies dans les sections 3, 4 et 5. Les moyennes intersectorielles permettent une comparaison directe entre les méthodes, conformément à l'approche discutée dans l'étude principale.