Vers une sécurité durable des systèmes d'information : le cas de l'optimisation du *vulnerability management* au sein d'un environnement *Cloud*.

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

{prenom.nom}@dauphine.psl.eu

RÉSUMÉ. *La sécurité des systèmes d'information (SI) est cruciale pour garantir la continuité des opérations des entreprises. Elle forme l'ossature qui soutient les organisations, semblable à une structure de protection autour de leur colonne vertébrale. C'est une composante du SI qui doit être pérenne pour remplir sa fonction principale tout en prenant en compte les objectifs de responsabilité environnementale des organisations. Un aspect important mais souvent négligé de la sécurité des SI est le processus de gestion des vulnérabilités (Vulnerability Management), qui constitue un lien entre la sécurité du SI et la responsabilité environnementale. En intégrant l'aspect métier des organisations dans la gestion des vulnérabilités, on peut identifier quelles vulnérabilités sont vraiment critiques pour l'organisation concernée. Dans ce travail, nous proposons d'étendre la méthode du Système Commun de Notation des Vulnérabilités (CVSS) afin de mieux prioriser les vulnérabilités et ainsi réduire le nombre de correctifs, de scans et de déploiements qui consomment de l'énergie. Le cas d'une banque, d'un hôpital et d'un gestionnaire de sites web sont abordés afin d'illustrer l'utilisation de la méthode.*

ABSTRACT. *The security of information systems (IS) is crucial to ensuring the continuity of business operations. It is a component of the IS that must be sustainable to fulfill its primary function while considering the organizations environmental responsibility objectives. An important but often overlooked aspect of IS security is the vulnerability management process, which constitutes a link between IS security and environmental responsibility. By integrating the business aspect of organizations into vulnerability management, we can identify which vulnerabilities are truly critical for the concerned organization. In this work, we propose extending the Common Vulnerability Scoring System (CVSS) method to better prioritize vulnerabilities and thus reduce the number of patches, scans, and deployments that consume energy. The cases of a bank, a hospital, and a website manager are discussed to illustrate the use of the method.*

MOTS-CLÉS : *Sécurité des SI, Responsabilité Environnementale, Gestion des Vulnérabilités, CVSS*

KEYWORDS: *IS Security, Environmental Responsibility, Vulnerability Management, CVSS*

1 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), constitue la colonne vertébrale de l'activité immatérielle des entreprises modernes (Legrenzi, 2016). En raison de ce rôle central, il doit être sécurisé, protégé et maintenu opérationnel.

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).

Nous considérons ici le SMSI comme un pilier du SI, bien qu'il n'en couvre pas toutes les dimensions. La gestion des vulnérabilités, par exemple, reste principalement centrée sur les aspects techniques, au détriment des facteurs humains 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 systèmes d'information, leur dimension éco-responsable reste encore largement sous-explorée (Chen *et al*., 2008; Mastelic *et al*., 2014). Le concept d'organisation écologiquement durable (Starik, 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 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 cybersécurité 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 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 vitrine.

1. Nous utiliserons la traduction française : Confidentialité, Intégrité et Disponibilité.

2 Fondements théoriques de la relation complexe mais stratégique entre sécurité et durabilité écologique des SI

La relation entre les systèmes d'information (SI) et l'écologie constitue un domaine de recherche à la fois complexe et prometteur dans le cadre des enjeux de durabilité. 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. Comme le suggèrent Chen *et al*. (2008), les SI peuvent agir comme des catalyseurs de durabilité écologique, notamment grâce à des outils avancés de modélisation et de suivi de l'empreinte environnementale.

Cependant, les avantages potentiels des SI dans cette transition écologique 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 cybersécurité (Akhter, 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 cybersécurité, 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 *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 cybersécurité. 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.

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, 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 humaines et métier. Pour classifier les critères de criticité des vulnérabilités, une méthode itérative de type Delphi (Rowe, 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, Sutcliffe, 2011).

Le Système de Management de la Sécurité de l'Information (SMSI) repose sur trois composantes principales dont les interrelations sont expliquées dans la littérature par (Nyanchama, 2005) et illustrées par la figure (Fig. 1) :

– La gestion des menaces (*Threat Management*) : consiste à identifier et à définir les vecteurs et les types d'attaques susceptibles de cibler les SI.

– La gestion des vulnérabilités (*Vulnerability Management*) : vise à détecter et analyser les failles pouvant être exploitées par ces menaces à des fins malveillantes.

– La gestion des risque (*Risk Management*) : constitue la pierre angulaire du SMSI en utilisant les éléments issues des deux processus précédents pour évaluer les risques pesant sur l'ensemble du SI 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 (Fig. 2) tirée des travaux de Al-Dhahri *et al*. (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 humain, 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, 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 *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, Lee (2015) introduisent une perspective élargie en prenant en compte les inté-

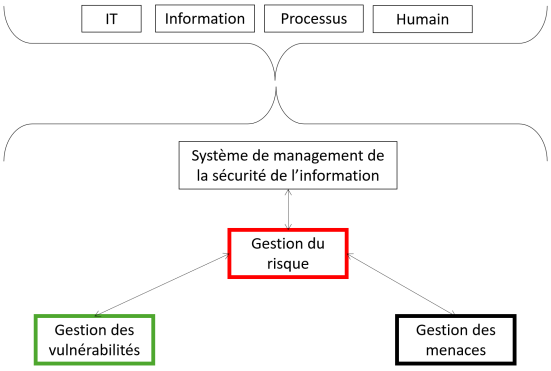

FIGURE 1. *Les composants principaux du SMSI*

rêts 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, 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 :

$$\textit{Information importance score} = \sum \mathrm{C} + \sum \mathrm{I} + \sum \mathrm{A} \tag{1}$$

– **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 méthode introduit de la flexibilité en permettant d'ajuster les pondérations des critères en fonction des spécificités de l'organisation, renforçant ainsi l'efficacité du processus de gestion des vulnérabilités. En intégrant la dimension métier, Choi et Lee démontrent qu'il est possible de dépasser les limites des approches purement

techniques, tout en offrant un cadre adaptable pour répondre aux exigences complexes des systèmes d'information modernes.

Choi, 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 27 000, 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 (Julisch, 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 cybersécurité en Europe, en mettant un accent particulier sur la protection des infrastructures critiques et les standards émergents (Cavelty, 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 cybersécurité (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, 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 privées. 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.

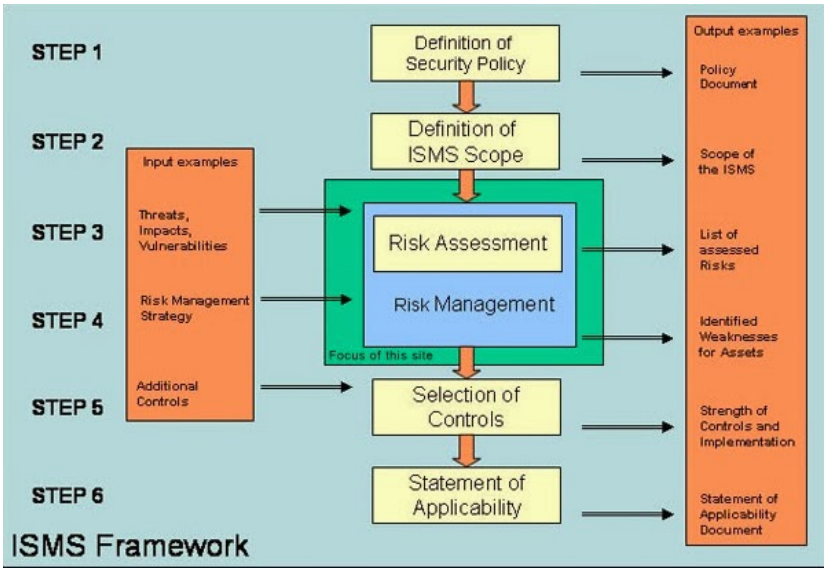

FIGURE 2. *Processus de développement du système de gestion de la sécurité de l'information (Al-Dhahri* et al*., 2017) (source : http://www.enisa.europa.eu)*

4 Études de cas : 5 vulnérabilités dans une infrastructure *cloud* de 3 organisations différentes

Afin de visualiser et d'évaluer l'intégration de l'aspect métier dans la hiérarchisation des vulnérabilités, nous avons procédé à une comparaison de deux approches . D'une part, une hiérarchisation se fondant exclusivement sur le CVSS, et d'autre part, celle dérivée de la méthode de Choi, Lee (2015). Cette comparaison vise à déterminer s'il existe des différences significatives entre les deux méthodes, et à évaluer leur pertinence respective. Nous avons employé le schéma d'une infrastructure représentative d'un environnement *Cloud* (Fig. 3) dans lequel cinq vulnérabilités informatiques ont été introduites. Cette infrastructure a ensuite été placée dans trois contextes différents : une banque, un hôpital et un site *web* vitrine. Cette approche permet d'étudier deux méthodes d'évaluation des vulnérabilités dans des environnements aux priorités variées. L'objectif est de comparer la méthode de Choi et Lee (2015) à l'approche standard du CVSS, afin d'évaluer dans quelle mesure la prise en compte du contexte métier peut influencer les priorités de gestion des vulnérabilités et améliorer la sécurité des systèmes d'information.

Le schéma illustre le parcours d'un client vers un service *Cloud*. L'accès se fait via Internet ou un VPN, menant à l'espace du fournisseur de services *Cloud* (*Cloud Service Provider*, CSP).On y trouve une infrastructure SaaS (*Software As A Service*) composée de plusieurs éléments : un *Firewall* pour filtrer les accès non autorisés, un

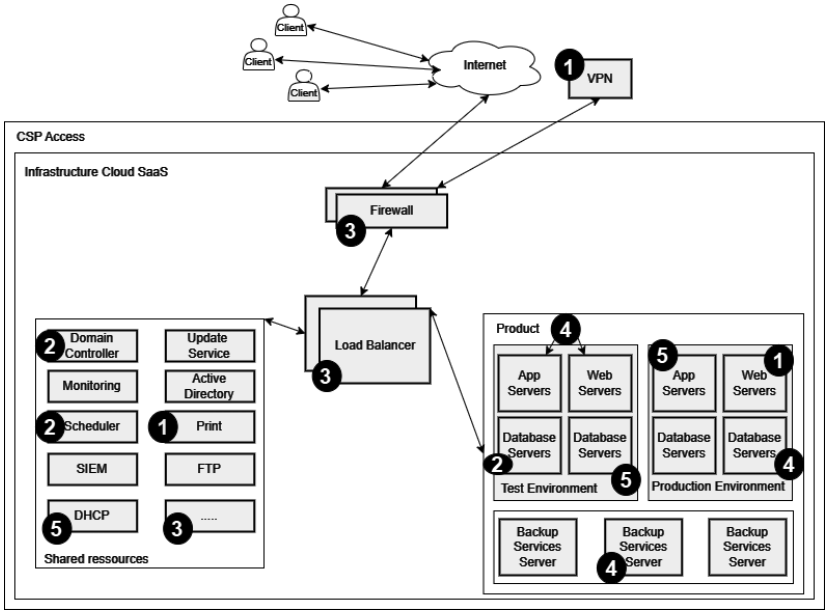

FIGURE 3. *Exemple d'une infrastructure Cloud avec des vulnérabilités détectées*

Load Balancer pour répartir la charge entre les ressources mutualisées, et le produit final qui intègre l'application, un serveur de base de données pour stocker les informations, et un serveur de sauvegarde en cas de panne ou de cyberattaque. Enfin, la zone des ressources partagées regroupe les outils nécessaires à la gestion et à l'optimisation du service.

Pour accéder aux services proposés, l'utilisateur doit franchir plusieurs niveaux de protection et de gestion des accès. La première ligne de défense est le *firewall*, élément fondamental de la sécurité réseau, qui filtre les connexions aux différentes adresses IP et empêche tout accès non autorisé. Une fois cette vérification effectuée, le *LoadBalancer* intervient pour rediriger l'utilisateur vers la ressource cible, qu'il s'agisse d'un serveur *web* ou d'une application spécifique.

Cet écosystème repose sur une orchestration de multiples ressources ayant chacune un rôle précis dans la gestion et l'exploitation des services. Les administrateurs s'appuient sur ces ressources afin de garantir la continuité, la disponibilité et la sécurité des services, conformément aux exigences organisationnelles (Nyanchama, 2005; Akhter, Othman, 2016; Choi, Lee, 2015; Albaroodi, Anbar, 2024).

Dans ce contexte et à partir de cet exemple (Fig. 3), nous avons intégré plusieurs vulnérabilités informatiques. Ces vulnérabilités permettent d'analyser leur positionnement et leur interaction avec les différentes composantes de l'infrastructure *Cloud*,

tout en testant différentes méthodologies de hiérarchisation de la criticité, notamment le CVSS et la méthode de Choi, Lee (2015). Cette approche met en évidence l'impact des vulnérabilités sur les infrastructures modernes et souligne la nécessité d'une gestion des risques adaptée.

4.1 Des vulnérabilités représentatives

Pour cette étude, cinq vulnérabilités ont été sélectionnées pour représenter un éventail large de menaces pouvant affecter l'infrastructure *Cloud*, indépendamment de l'organisation concernée (Rotlevi, 2025; Smith, 2023; owasp.org, 2024).

1. `CVE-2021-22965` (Spring4Shell) - **CVSS 7.5** (*High*) : Permet l'exécution de code à distance via une mauvaise gestion des requêtes HTTP dans le *framework* Spring.

2. `CVE-2021-44228` (Log4Shell) - **CVSS 10** (*Critical*) : Permet l'exécution de code arbitraire via l'exploitation malveillante de la journalisation dans Log4j.

3. `CVE-2020-10188` - **CVSS 9.8** (*Critical*) : Permet l'exécution de commandes malveillantes sur des systèmes F5 BIG-IP vulnérables.

4. `CVE-2020-11023` - **CVSS 6.1** (*Medium*) : Permet l'injection de scripts malveillants (XSS) dans des pages *web*.

5. `CVE-2020-2551` - **CVSS 9.8** (*Critical*) : Permet l'exécution de requêtes SQL malveillantes pour accéder ou manipuler des données sensibles.

En se basant uniquement sur le score CVSS, qui reflète une hiérarchisation standard sans prise en compte du contexte organisationnel, les vulnérabilités se classent, quelle que soit l'organisation, comme suit *Forum of Incident Response and Security Teams* (FIRST, 2023) :

1. **CVSS 10** (*Critical*) : (2) `CVE-2021-44228`
2. **CVSS 9.8** (*Critical*) : (3) `CVE-2020-10188`
3. **CVSS 9.8** (*Critical*) : (5) `CVE-2020-2551`
4. **CVSS 7.5** (*High*) : (1) `CVE-2021-22965`
5. **CVSS 6.1** (*Medium*) : (4) `CVE-2020-11023`

Ainsi, selon cette hiérarchisation, la vulnérabilité (2) – Log4Shell – serait considérée comme la plus prioritaire, car elle est jugée critique, tandis que la vulnérabilité (4) – une faille XSS – serait reléguée au dernier rang, en raison de son score relativement faible. Cette classification repose uniquement sur des critères techniques définis par le CVSS, sans prendre en compte le contexte d'exploitation ou l'impact métier.

Cependant, en intégrant l'aspect métier d'une organisation, comme une banque, un hôpital ou un gestionnaire de sites *web* vitrine, l'ordre de priorité peut être radicalement modifié. Par exemple, une vulnérabilité impactant fortement la disponibilité pourrait être prioritaire pour un hôpital, tandis qu'une faille compromettant la confidentialité serait plus préoccupante pour une banque.

Afin d'évaluer ces différences d'impact, nous avons intégré ces cinq vulnérabilités dans l'infrastructure *Cloud* étudiée précédemment, en conservant les numéros attribués à chaque vulnérabilité avant leur hiérarchisation (voir Fig. 3). Cette approche permet de démontrer l'importance d'adapter les stratégies de remédiation aux contextes organisationnels spécifiques et de ne pas se baser uniquement sur les scores CVSS.

4.2 Scores de vulnérabilité et discussions

D'après les travaux de Choi, Lee (2015) et en appliquant la formule présentée dans la section 3, adaptée aux spécificités des organisations et aux priorités variables attribuées à l'importance de l'information dans chaque secteur (voir Annexe. 5), nous avons établi le tableau récapitulatif des résultats (Tab. 1) :

TABLEAU 1. *Notation de criticité des vulnérabilités par secteur en utilisant la méthode de Choi, Lee (2015).*

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

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, Vilanova, 2006; Bobillier-Chaumon *et al*., 2006), les hôpitaux (Frenkiel *et al*., 2007; Juven, 2013) et les sites *web* vitrine (Stephane, 2020; Dirigeant, 2024). L'analyse a été structurée autour de la triade de sécurité de l'information – *Confidentialité, Intégrité et Disponibilité* – à travers des critères spécifiques.

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.

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. Les scores obtenus reflètent néanmoins des tendances significatives. Pour la vulnérabilité (1), qui concerne principalement les *VPN*, les scores étaient de 32 sur 40 pour une banque, 36 pour un hôpital et 24 pour un site *web* vitrine. Cette vulnérabilité, qui pourrait permettre une exécution de code à distance compromettant l'ensemble de l'infrastructure, est particulièrement critique pour un hôpital en raison des exigences accrues en matière de disponibilité et d'intégrité des données.

Pour la vulnérabilité (2), touchant les *Domain Controllers*, la banque et l'hôpital obtiennent un score de 39 sur 40, tandis que le site *web* vitrine atteint 23 sur 40. Cette disparité s'explique par l'importance légale et économique des informations manipulées par les banques et les hôpitaux. Pour la vulnérabilité (3), liée au *LoadBalancer*, les scores sont respectivement de 33 pour la banque, 37 pour l'hôpital et 21 pour le site *web* vitrine. La disponibilité étant prioritaire pour un hôpital, cette vulnérabilité y est plus critique que pour une banque, où la protection des données est prioritaire.

La vulnérabilité (4), avec des scores de 24 pour la banque, 30 pour l'hôpital et 15 pour le site *web* vitrine, présente un impact limité en raison de son périmètre restreint. Enfin, pour la vulnérabilité (5), les scores sont de 39 pour la banque, 37 pour l'hôpital et 21 pour le site *web* vitrine, reflétant l'importance stratégique de ces vulnérabilités malgré leur faible exploitabilité.

L'analyse révèle des hiérarchisations différentes selon la méthode utilisée. Avec la méthode de Choi, Lee (2015), certaines vulnérabilités critiques selon le CVSS, comme la vulnérabilité (1), sont reléguées en seconde position pour la banque et le site *web* vitrine, tout en restant prioritaires pour l'hôpital. Les vulnérabilités (3) et (5) présentent également des différences de classement, mais leurs scores restent globalement cohérents entre les deux approches. Cela souligne que les deux méthodes, bien qu'indépendantes, sont complémentaires. Le CVSS, orienté vers l'aspect technique, et la méthode de Choi, Lee (2015), centrée sur les priorités métier, apportent des perspectives distinctes qui enrichissent la compréhension et la gestion des vulnérabilités.

Toutefois, ces approches présentent des limites. En examinant les interactions entre vulnérabilités, il apparaît que certaines d'entre elles, comme la vulnérabilité (1), sont critiques uniquement dans des contextes spécifiques (par exemple, le *VPN*). De même, la vulnérabilité (2) n'impacte une organisation qu'à travers les *Domain Controllers*, et la vulnérabilité (3) devient critique parce qu'elle affecte le *LoadBalancer*. Les vulnérabilités (4) et (5) ont un impact limité en raison de leur faible exploitabilité. Cette contextualisation montre que la hiérarchisation doit prendre en compte les interdépendances et le chaînage des vulnérabilités. Si cela est gérable dans des infrastructures de taille modeste, cela devient rapidement impraticable pour des organisations com-

plexes avec plusieurs milliers de serveurs et des infrastructures variées. L'utilisation d'une méthode industrialisée devient alors obligatoire.

Ainsi, bien que la vulnérabilité (3) représente un danger critique en raison de son impact sur des éléments essentiels de l'infrastructure *Cloud*, elle n'arrive qu'en seconde position avec le CVSS et en quatrième position selon la méthode de Choi, Lee (2015). Ce cas illustre l'influence de l'impact métier sur la priorisation des vulnérabilités et met en lumière les limites des méthodes existantes, qui ne considèrent qu'un aspect du *SI* : le CVSS se concentre sur les aspects techniques, tandis que la méthode de Choi, Lee (2015) privilégie l'importance métier et la valeur de l'information. Ces observations renforcent l'idée qu'un *SMSI* intégré et adapté, prenant en compte la globalité du *SI*, est nécessaire pour une gestion durable et efficace des vulnérabilités.

Trois approches distinctes apparaissent : la méthode standard basée sur les CVSS, une méthode personnalisée vue chez Chois et Lee (2015), et une autre qui exploite le chaînage des vulnérabilités, toutes montrant des différences de priorisation dans ce cas pratique, comme le montre la Fig. 4. Des lacunes persistent donc dans le développement d'une méthode complète et adaptable. Il est nécessaire d'identifier ces lacunes avec précision et de trouver un moyen de les combler.

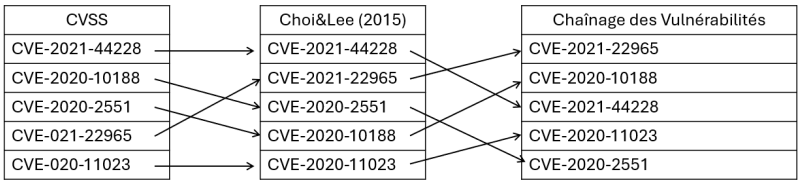

FIGURE 4. *Différence de hiérarchisation de vulnérabilité d'après 3 méthodes différentes*

En prenant en compte le chaînage des vulnérabilités, certaines failles critiques peuvent devenir totalement inexploitables, ne posant alors aucun danger pour les activités de l'organisation. Il ne s'agit donc pas d'ignorer des vulnérabilités sous prétexte d'économiser de l'énergie, mais plutôt de déterminer précisément si une vulnérabilité représente réellement un risque pour l'organisation et d'agir en conséquence.

Limites, conclusions et perspectives

Les méthodes existantes, telles que le *CVSS*, qui s'impose comme un standard de référence pour évaluer la criticité des vulnérabilités, et la méthode de Choi, Lee (2015), qui intègre les dimensions métiers, constituent des bases solides pour la gestion des vulnérabilités. Toutefois, ces approches présentent des limites importantes lorsqu'elles sont appliquées à de grandes organisations aux structures complexes et diversifiées. Le *CVSS* se concentre exclusivement sur les aspects techniques des vulnérabilités, négligeant les spécificités métiers des organisations. Inversement, la méthode de Choi, Lee (2015), bien qu'innovante sur le plan métier, omet souvent les contraintes techniques qui restent essentielles dans les environnements hautement technologiques.

Ce travail de recherche qui se poursuit vise à combiner ces trois perspectives en développant une méthode personnalisée de *Vulnerability Management*. Capable d'intégrer de manière équilibrée les dimensions métier et technique propres à chaque organisation tout en prenant en compte le chaînage des vulnérabilités. L'objectif est de fournir une approche optimisée de la hiérarchisation des vulnérabilités, réduisant ainsi les besoins en remédiation et contribuant à une forme de sobriété numérique dans le domaine de la sécurité des *SI*.

Dans cette optique, nous prévoyons de mobiliser la méthode *Delphi* pour affiner notre démarche. En impliquant un panel d'experts issus de divers secteurs, nous chercherons à établir un véritable consensus sur les critères essentiels à considérer, notamment l'importance de l'information et les priorités spécifiques des parties prenantes. Cette approche permettra de concevoir un cadre plus robuste et adaptable pour répondre aux besoins variés des entreprises. Un travail pour trouver ou déterminer une métrique propre à l'empreinte écologique de la sécurité des systèmes d'information est prévu afin de pouvoir évaluer la pertinence de ces travaux. L'ambition à long terme est de proposer une solution personnalisable, complète, durable et efficiente pour la gestion des vulnérabilités en entreprise. Cette méthode cherche également à transformer la perception du SMSI, souvent considérée comme un centre de coûts, en un véritable investissement stratégique. Une gestion efficiente des vulnérabilités peut en effet améliorer non seulement la résilience des organisations face aux menaces, mais également leur image de marque et leur engagement en faveur d'une sobriété numérique durable. En intégrant des considérations économiques et environnementales, cette approche vise à concilier efficacité opérationnelle, viabilité économique et durabilité écologique.

Bibliographie

Abbasi S. (2024, 11). *Qualys TRU Uncovers Five Local Privilege Escalation Vulnerabilities in needrestart | Qualys Security Blog.* Consulté sur https://blog.qualys.com/vulnerabilities-threat-research/2024/11/19/qualys-tru-uncovers-five-local-privilege-escalation-vulnerabilities-in-needrestart

Akhter N., Othman M. (2016). Energy aware resource allocation of cloud data center: review and open issues. *Cluster Computing*, vol. 19, n° 3, p. 1163–1182.

Albaroodi H., Anbar M. (2024). *Journal of Applied Data Sciences*, vol. 6, n° 1, p. 155–177. Consulté sur https://bright-journal.org/Journal/index.php/JADS/article/view/324

Al-Dhahri S., Al-Sarti M., Abdaziz A. (2017). Information security management system. *International Journal of Computer Applications*, vol. 158, p. 29-33.

Berthelot A., Caron E., Laage R. de, Lefèvre L., Nicolas A. (2024). *Fine-grained methodology to assess environmental impact of a set of digital services.* Consulté sur https://hal.science/hal-04928998 (working paper or preprint)

Bobillier-Chaumon M.-E., Dubois M., Retour D. (2006). *L'acceptation des nouvelles technologies d'information : le cas des systèmes d'information en milieu bancaire.* Consulté sur

https://shs.hal.science/halshs-01562077v1

Cavelty M. D., Smeets M. (2023). Regulatory cybersecurity governance in the making: the formation of enisa and its struggle for epistemic authority. *Journal of European Public Policy*, vol. 30, nº 7, p. 1330–1352. Consulté sur https://doi.org/10.1080/13501763.2023.2173274

Chen A. J., Boudreau M.-C., Watson R. T. (2008). Information systems and ecological sustainability. *Journal of Systems and Information Technology*, vol. 10, nº 3, p. 186–201.

Choi M., Lee C. (2015). Information security management as a bridge in cloud systems from private to public organizations. *Sustainability*, vol. 7, nº 9, p. 12032–12051.

Cyber4Tomorrow. (2025, 4). *Présenter la méthodologie d'évaluation empreinte carbone de la cybersécurité - Cyber4Tomorrow*. Consulté sur https://cyber4tomorrow.fr/actions/evaluation-empreinte-carbone-de-la-cybersecurite/

Dirigeant L. B. du. (2024, 11). *Le site vitrine : Définition et utilité pour votre entreprise en 2025.* Consulté sur https://www.leblogdudirigeant.com/site-vitrine-entreprise

Dix J. (2012, Mar 26). Push your cloud supplier to participate in csa star. *Network World*, vol. 29, nº 6, p. 5. Consulté sur https://www.proquest.com/trade-journals/push-your-cloud-supplier-participate-csa-star/docview/1009899414/se-2 (Copyright - Copyright Network World Inc. Mar 26, 2012; Last updated - 2017-11-19)

Dumalanede C. (2019, 12). *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.* Consulté sur https://theses.hal.science/tel-03419273v1

Ferguson D. (2020, 10). *Qualys WAS Engine 8.3 released | Qualys Notifications.* Consulté sur https://notifications.qualys.com/product/2020/09/04/qualys-was-engine-8-3-released

FIRST. (2023). *Forum of incident response and security teams, common vulnerability scoring system (cvss) version 3.0.* Consulté sur https://www.first.org/cvss/v4.0/specification-document (Accessed: 2025-02-14, Also available in NVD: https://nvd.nist.gov/)

Frenkiel J., BOUAM S., Triadou P. (2007, 06). 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*, vol. 10.

Förderer K., Lösch M., Növer R., Ronczka M., Schmeck H. (2019). Smart meter gateways: Options for a bsi-compliant integration of energy management systems. *Applied Sciences*, vol. 9, nº 8. Consulté sur https://www.proquest.com/scholarly-journals/smart-meter-gateways-options-bsi-compliant/docview/2331407740/se-2

Jogi B. (2023, 1). *CVE-2021-244228: Apache Log4j2 Zero Day Exploited in the Wild (Log4Shell) | Qualys Security Blog.* Consulté sur https://blog.qualys.com/vulnerabilities-threat-research/2021/12/10/apache-log4j2-zero-day-exploited-in-the-wild-log4shell

Julisch K., Hall M. (2010, 11). Security and Control in the Cloud. *Information Security Journal A Global Perspective*, vol. 19, nº 6, p. 299–309. Consulté sur https://doi.org/10.1080/19393555.2010.514654

Juven P.-A. (2013, 1). Produire l'information hospitalière. *Revue d anthropologie des connaissances*, vol. 7, nº 4. Consulté sur https://doi.org/10.3917/rac.021.0815

Kadu H. (2024, 3). *March 2024 Web application vulnerabilities released | Qualys notifications.* Consulté sur https://notifications.qualys.com/product/2024/03/29/march-2024-web-application-vulnerabilities-released

Legrenzi C. (2016). Informatique, numérique et système d'information: définitions, périmètres, enjeux économiques. *Vie & Sciences de L'Entreprise*, nº 200, p. 49–76.

Lobez F., Vilanova L. (2006). *La banque productrice d'information*. Paris, France, Presses Universitaires de France eBooks.

Mastelic T., Oleksiak A., Claussen H. *et al*. (2014). Cloud computing: Understanding infrastructure energy consumption for cloud environments. *Future Generation Computer Systems*, vol. 37, p. 101–112.

Nyanchama M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security*, vol. 14, p. 29–56.

owasp.org. (2024). *Owasp top ten | owasp foundation.* Consulté sur https://owasp.org/www-project-top-ten/

Reix R. (2004). *Systèmes d'information et management des organisations* (5e éd.). Paris, France, Vuibert.

Rotlevi S. (2025, 1). *The Basics of AWS Infrastructure Security.* Consulté sur https://www.wiz.io/blog/aws-infrastructure-security-basics

Rowe G., Wright G. (1999). The delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, vol. 15, no 4, p. 353–375.

Shepherd D. A., Sutcliffe K. M. (2011). Inductive top-down theorizing: A source of new theories of organization. *Academy of Management Review*, vol. 36, no 2, p. 361–380.

Smith T. (2023, 4). *Cybersecurity Risk Fact : Infrastructure Misconfigurations Open the Door to Ransomware | Qualys Security Blog.* Consulté sur https://blog.qualys.com/vulnerabilities-threat-research/2023/04/03/risk-fact-5-infrastructure-misconfigurations-open-the-door-to-ransomware

Starik M., Rands G. P. (1995). Weaving an integrated web: Multilevel and multisystem perspectives of ecologically sustainable organizations. *Academy Of Management Review*, vol. 20, no 4, p. 908–935.

Stephane. (2020, 7). *Pourquoi avoir un site vitrine pour votre entreprise ?* Consulté sur https://management-digital.com/blog/formation/pourquoi-avoir-un-site-vitrine-pour-votre-entreprise/

Wang P. (2021). Connecting the parts with the whole: Toward an information ecology theory of digital innovation ecosystems. *MIS Quarterly*, vol. 45, no 1, p. 397–422.

Watkins S. G. (2022). *ISO/IEC 27001:2022*. Ely, Cambridgeshire, Royaume-Uni, IT Governance Publishing Ltd. Consulté sur https://doi.org/10.2307/j.ctv30qq13d

5 Annexe

TABLEAU 2. *Matrice des critères de sécurité.*

Critère	**Confidentialité (C)**	**Intégrité (I)**	**Disponibilité (D)**
Sensibilité des données impactées	✓	-	-
Nécessité de protéger l'information	✓	-	-
Possibilité de divulgation non autorisée	✓	-	-
Niveau de confiance dans les données	-	✓	-
Risque de modification non autorisée	-	✓	-
Nécessité de validation de l'intégrité	-	✓	-
Besoin d'accès continu aux informations	-	-	✓
Impact en cas d'indisponibilité	-	-	✓
Priorité de récupération après incident	-	-	✓

Chaque vulnérabilité est ensuite analysée en fonction de ces critères.

Calculs détaillés des scores exemple avec : CVE-2021-22965 (Spring4Shell)

Banque

Confidentialité (C)	**Intégrité (I)**	**Disponibilité (D)**
Sensibilité des données impactées: 4	Niveau de confiance dans les données: 4	Besoin d'accès continu aux informations: 3
Nécessité de protéger l'information: 5	Risque de modification non autorisée: 4	Impact en cas d'indisponibilité: 3
Possibilité de divulgation non autorisée: 4	Nécessité de validation de l'intégrité: 3	Priorité de récupération après incident: 2
Score total: $C = 4 + 5 + 4 = 13$	**Score total:** $I = 4 + 4 + 3 = 11$	**Score total:** $D = 3 + 3 + 2 = 8$

Total final: $\sum C + \sum I + \sum D = 32$

Hôpital

Confidentialité (C)	**Intégrité (I)**	**Disponibilité (D)**
Sensibilité des données impactées: 3	Niveau de confiance dans les données: 5	Besoin d'accès continu aux informations: 5
Nécessité de protéger l'information: 4	Risque de modification non autorisée: 4	Impact en cas d'indisponibilité: 4
Possibilité de divulgation non autorisée: 3	Nécessité de validation de l'intégrité: 4	Priorité de récupération après incident: 4
Score total: $C = 3 + 4 + 3 = 10$	**Score total:** $I = 5 + 4 + 4 = 13$	**Score total:** $D = 5 + 4 + 4 = 13$

Total final: $\sum C + \sum I + \sum D = 36$

Site Web Vitrine

Confidentialité (C)	**Intégrité (I)**	**Disponibilité (D)**
Sensibilité des données impactées: 2	Niveau de confiance dans les données: 2	Besoin d'accès continu aux informations: 5
Nécessité de protéger l'information: 2	Risque de modification non autorisée: 2	Impact en cas d'indisponibilité: 4
Possibilité de divulgation non autorisée: 2	Nécessité de validation de l'intégrité: 2	Priorité de récupération après incident: 3
Score total: $C = 2 + 2 + 2 = 6$	**Score total:** $I = 2 + 2 + 2 = 6$	**Score total:** $D = 5 + 4 + 3 = 12$

Total final: $\sum C + \sum I + \sum D = 24$