Grandes méthodologies de priorisation des vulnérabilités techniques en cybersécurité

Franck Jeannot

Montréal, Canada, Mai 2025, AB833, v1.0

Abstract

Face à l'explosion du nombre de vulnérabilités et aux ressources limitées pour les corriger, il est devenu indispensable de les prioriser efficacement.

Cet article propose une synthèse des cinq grandes familles de méthodologies de priorisation identifiées dans [1] : (1) les approches basées sur les graphes, qui modélisent les dépendances et chemins d'attaque pour cibler les points critiques ; (2) les méthodes d'apprentissage automatique, qui exploitent des modèles prédictifs entraînés sur des données historiques et contextuelles ; (3) l'optimisation multi-objectifs, qui formule la priorisation comme un problème équilibrant plusieurs critères (risque, coût, disponibilité) ; (4) les systèmes à base de règles, offrant simplicité et explicabilité via des règles expertes ; et (5) les approches statistiques, qui valident empiriquement la pertinence des métriques et intègrent l'incertitude. Après présentation de chaque méthode (principe, exemples, limites), un tableau comparatif synthétise leurs forces et faiblesses. Nous concluons que l'hybridation de ces approches, combinant leurs atouts respectifs, est la voie la plus prometteuse pour une priorisation robuste et opérationnelle.

Keywords: Vulnérabilités informatiques, Priorisation des vulnérabilités, Approches basées sur les graphes, Apprentissage automatique, Optimisation multi-objectifs, Systèmes experts, Méthodes statistiques, MITRE ATT&CK

1. Introduction

Dans un monde toujours plus interconnecté, la surface d'attaque s'élargit avec l'explosion du nombre de failles découvertes chaque année. On compte désormais des dizaines de milliers de nouvelles vulnérabilités divulguées annuellement, ce qui dépasse largement les capacités de correction manuelle complète [2]. Face à cette surcharge, il est nécessaire de concentrer les efforts de remédiation sur les vulnérabil-

ités les plus critiques. La priorisation des vulnérabilités est ainsi devenue un enjeu clé de la gestion des risques en cybersécurité.

La méthode la plus répandue pour évaluer la sévérité intrinsèque d'une faille est le Common Vulnerability Scoring System (*CVSS*), qui attribue un score numérique sur 10 basé sur des caractéristiques techniques de la vulnérabilité. Cependant, CVSS présente des limites notables : c'est un score statique qui ne reflète pas le contexte spécifique d'une organisation ou d'un système donné (valeur des actifs touchés, exposition réelle, etc.), et il ne tient pas compte de l'exploitabilité effective ou des menaces en cours d'évolution.

Pour pallier ces insuffisances, de nombreux travaux de recherche ont proposé des méthodes complémentaires pour améliorer la priorisation. Ces approches peuvent être regroupées en cinq grandes catégories [1] :

- **Méthodes basées sur les graphes** (*graph-based*) : modélisation du système et des vulnérabilités sous forme de graphes (graphes d'attaque, réseaux de dépendances, etc.).
- **Méthodes d'apprentissage automatique** (*machine learning*) : utilisation de modèles d'IA entraînés sur des données pour prédire le risque ou la criticité des failles.
- **Optimisation multi-objectifs** (*multi-objective optimization*) : formulation de la priorisation comme un problème d'optimisation mathématique tenant compte de plusieurs critères simultanément.
- **Méthodes à base de règles** (*rule-based*) : application de règles prédéfinies (seuils, if/then) souvent issues de l'expertise humaine ou de standards pour classer les vulnérabilités.
- **Méthodes statistiques** (*statistical*) : approches fondées sur l'analyse statistique de données empiriques concernant les vulnérabilités et les incidents.

Dans les sections suivantes, nous passons en revue chacune de ces catégories de méthodologies de priorisation des vulnérabilités. Pour chaque catégorie, nous en décrivons le fonctionnement général, nous donnons un exemple issu de la littérature ainsi que les avantages et limitations identifiés. Un tableau synthétique (Table 1) compare ensuite ces approches. Enfin, nous concluons en discutant des perspectives et défis ouverts dans ce domaine.

2. Méthodes basées sur les graphes (Graph-based)

Les méthodes basées sur les graphes modélisent le système et ses vulnérabilités sous forme de nœuds reliés par des liens représentant des relations (dépendances entre composants, chemins d'attaque potentiels, co-occurrences, etc.). L'analyse de ces structures graphiques – telles que les graphes d'attaque, les arbres d'attaque ou les réseaux bayésiens – permet d'identifier les vulnérabilités dont l'exploitation pourrait avoir le plus grand impact en cascade sur l'ensemble du système. Par exemple, Li *et al.* [3] construisent un *arbre d'attaque* où chaque nœud feuille représente une vulnérabilité, notée avec un score CVSS, afin d'évaluer le risque global pesant sur un système industriel. De son côté, Chatzipoulidis *et al.* [4] exploitent un *graphe de dépendances* pour repérer les failles dont la compromission pourrait entraîner des défaillances majeures dans une infrastructure. Les approches par les graphes mettent ainsi en évidence les effets de propagation et les points névralgiques d'un réseau du point de vue de la sécurité.

L'utilisation des graphes pour la priorisation présente l'avantage de contextualiser chaque vulnérabilité dans son environnement : on évalue une faille non pas isolément mais en tenant compte de son rôle dans d'éventuels scénarios d'attaque multi-étapes. En revanche, ces méthodes requièrent une modélisation précise de l'architecture du système et de ses interdépendances, ce qui peut s'avérer complexe et coûteux pour des réseaux de grande taille. L'analyse des graphes (calcul des chemins d'attaque les plus critiques, évaluation probabiliste des scénarios, etc.) est également coûteuse en ressources calculatoires lorsque le graphe comporte de très nombreux nœuds. De plus, ces modèles sont généralement statiques et doivent être mis à jour manuellement pour refléter toute modification de la configuration du système, faute de quoi leurs résultats perdent en exactitude.

3. Méthodes d'apprentissage automatique (Machine Learning)

Cette catégorie regroupe les approches qui s'appuient sur l'intelligence artificielle, et plus spécifiquement l'apprentissage automatique, pour automatiser et améliorer l'estimation du risque des vulnérabilités. L'idée générale est d'entraîner des modèles sur des données historiques (vulnérabilités passées, incidents connus, caractéristiques extraites de descriptions, etc.) afin de prédire la criticité ou la probabilité d'exploitation de nouvelles failles.

Par exemple, certaines études appliquent le *traitement automatique du langage naturel* aux descriptions textuelles des CVE pour en extraire des caractéristiques significatives, puis estimer un score de sévérité amélioré ou un niveau de risque

associé [5]. D'autres travaux s'appuient sur des données empiriques d'attaques observées pour entraîner des classifieurs ou des modèles de régression capables de prédire quelles vulnérabilités sont les plus susceptibles d'être exploitées. C'est le cas du système EPSS (*Exploit Prediction Scoring System*), qui combine des informations sur les failles et sur leur historique d'exploitation afin de fournir un score probabiliste indiquant la chance qu'une vulnérabilité soit exploitée dans le futur [6]. Par ailleurs, certaines approches innovantes intègrent des signaux issus des réseaux sociaux ou du *dark web* (p. ex. analyse de discussions sur Twitter, de ventes d'exploits sur des forums clandestins) au sein de modèles prédictifs, afin de détecter précocement l'intérêt des attaquants pour une vulnérabilité donnée.

Les approches par apprentissage automatique offrent l'avantage de pouvoir gérer de vastes volumes de données hétérogènes et de mettre au jour des patterns complexes indicateurs de risque, que des méthodes manuelles ou basées sur des règles ne pourraient déceler. Elles sont également évolutives : en réentraînant régulièrement les modèles avec de nouvelles données, on peut théoriquement adapter la priorisation à l'évolution des menaces. En contrepartie, ces techniques présentent des inconvénients. Leur efficacité dépend fortement de la qualité et de la représentativité des données d'entraînement : des données incomplètes ou biaisées peuvent conduire à des prédictions erronées. De plus, les modèles de machine learning sont souvent des boîtes noires dont les décisions manquent de transparence et peuvent être difficiles à justifier auprès des responsables sécurité. Enfin, ces modèles doivent être mis à jour en continu pour rester efficaces, ce qui implique un effort de maintenance non négligeable et les rend potentiellement vulnérables aux changements drastiques du paysage des menaces.

4. Optimisation multi-objectifs (Multi-Objective Optimization)

Les méthodes d'optimisation multi-objectifs abordent la priorisation des vulnérabilités comme un problème d'optimisation sous contraintes multiples. Plutôt que d'utiliser un unique critère (par exemple le score de sévérité) pour classer les failles, on considère simultanément plusieurs objectifs à atteindre, tels que : minimiser le risque global d'attaque, minimiser le coût ou l'effort de correction des vulnérabilités, limiter l'impact des mises à jour sur la disponibilité des services, respecter des contraintes de conformité réglementaire, etc. Le problème se prête alors à des techniques d'optimisation mathématique (par exemple la programmation linéaire à objectifs multiples, ou des heuristiques telles que les algorithmes génétiques) afin de trouver le meilleur compromis.

Par exemple, (Farris *et al.*, 2018) [7] ont développé l'outil *VULCON* qui modélise la sélection des correctifs de sécurité comme un problème multi-objectifs. Leur

approche utilise une recherche heuristique pour identifier un ensemble de solutions optimales (au sens de Pareto) offrant différents équilibres entre réduction du risque et coûts (en termes de ressources de patch ou d'indisponibilité induite). Dans un autre contexte, Yadav *et al.* [8] ont proposé *SmartPatch*, un cadre de priorisation des correctifs pour les systèmes industriels SCADA : il calcule pour chaque vulnérabilité un *score d'impact résiduel* qui tient compte de la diminution de risque après application d'un patch, afin d'orienter la sélection des correctifs à déployer en priorité. Certaines approches récentes font appel à des algorithmes évolutionnaires pour améliorer le classement des vulnérabilités tout en satisfaisant des contraintes complexes (p. ex. contraintes de dépendances entre correctifs, fenêtres de maintenance limitées) [9].

L'avantage des méthodes d'optimisation multi-objectifs est de fournir un cadre rationnel pour équilibrer des critères potentiellement contradictoires dans la prise de décision. Elles permettent d'explorer automatiquement un large espace de solutions et d'identifier des choix optimaux selon différentes perspectives (p. ex. favoriser la sécurité maximale vs. minimiser l'effort de patch). En contrepartie, ces techniques peuvent être difficiles à mettre en œuvre à grande échelle : la complexité combinatoire du problème de priorisation multi-critères peut exploser avec le nombre de vulnérabilités et de contraintes à considérer, rendant la résolution exacte impraticable (d'où le recours à des heuristiques). De plus, ces méthodes requièrent de définir et de paramétrer quantitativement chaque objectif (par exemple assigner des poids relatifs aux critères de risque, coût, disponibilité, etc.), ce qui peut introduire une subjectivité ou du moins nécessiter une expertise pour calibrer correctement le modèle. Enfin, les solutions proposées, bien qu'optimales mathématiquement, doivent encore être interprétées et validées par les décideurs : il peut y avoir un écart entre la solution théorique recommandée et ce qui est réalisable ou acceptable opérationnellement.

5. Méthodes à base de règles (Rule-based)

Les approches à base de règles, incluant les systèmes experts, reposent sur un ensemble de règles déterministes définies à l'avance pour évaluer la criticité des vulnérabilités. Ces règles s'appuient généralement sur des seuils ou des conditions combinant des métriques connues. Par exemple, une règle simple pourrait stipuler qu'« une vulnérabilité est critique si son score CVSS dépasse 8,0 et qu'elle est exposée sur un service accessible depuis Internet ». De telles règles peuvent être élaborées manuellement par des experts ou dérivées de guides de bonnes pratiques.

Une illustration de cette approche est donnée par Kurniawan *et al.*, qui présentent un système automatisé pour quantifier le niveau de risque lié à des attaques par injection (SQLi) et inclusion de scripts (XSS). Leur méthode s'appuie sur les vecteurs

CVSS des vulnérabilités identifiées dans un système, ajustés à l'aide d'informations contextuelles collectées en temps réel (telles que l'adresse IP source de l'attaque, le niveau de privilège de l'attaquant et la proximité réseau de la cible). Le système calcule un score de risque pour chaque alerte en appliquant des règles prédéfinies aux métriques CVSS enrichies par ces données d'attaque. Dissanayaka *et al.* [10] adoptent une approche apparentée dans un environnement industriel : ils ajustent dynamiquement certaines sous-métriques de CVSS (comme le vecteur d'attaque ou la complexité d'attaque) en fonction de la topologie du réseau industriel et des mécanismes de défense déployés, afin de générer un score de vulnérabilité plus pertinent pour l'organisme considéré.

Les systèmes basés sur des règles présentent l'avantage d'être relativement simples à comprendre et à déployer. Ils s'intègrent bien avec les outils existants (par exemple, en complétant les scores CVSS standard par des règles métier spécifiques) et fournissent des résultats déterministes et explicables (chaque décision peut être justifiée par l'application d'une règle explicite). Néanmoins, leur principal inconvénient réside dans leur rigidité. Étant fondés sur des connaissances a priori figées, ils peuvent passer à côté de situations non prévues par les règles. Leur maintenance demande une mise à jour régulière des règles à mesure que de nouvelles menaces apparaissent ou que le système évolue, sans quoi leur pertinence décroît. Par ailleurs, multiplier les règles pour couvrir davantage de cas particuliers peut conduire à un système complexe, difficile à maintenir et à valider exhaustivement (risque de conflits ou d'incohérences entre règles).

6. Méthodes statistiques (Statistical)

Sous l'appellation de méthodes statistiques, on regroupe les approches qui appliquent des techniques d'analyse de données et de statistique pour prioriser les vulnérabilités. Plutôt que de proposer de nouveaux modèles de risque, ces travaux cherchent souvent à évaluer objectivement l'efficacité des métriques existantes ou à dériver des priorités à partir de données empiriques. Par exemple, Angelelli *et al.* [11] introduisent un cadre statistique s'appuyant sur une *régression par quintiles* (mid-quantile regression) pour établir un classement des vulnérabilités. Ils proposent également une mesure d'accord de classement visant à vérifier la stabilité du classement obtenu même lorsque certaines informations d'entrée sont manquantes ou incomplètes. De son côté, Holm *et al.* [12] examinent plusieurs métriques de sécurité au niveau système (comme des variantes agrégées de scores CVSS, des indicateurs de lien le plus faible ou le temps d'exposition des failles non corrigées) et mesurent empiriquement leur corrélation avec le *temps de compromission* d'un système lors

de tests d'intrusion. Leur étude, fondée sur des données d'attaques réelles en laboratoire, permet d'identifier quelles mesures sont réellement prédictives du risque et dans quelle mesure.

Un avantage des approches statistiques est qu'elles reposent sur une analyse factuelle des données : elles permettent de valider (ou d'infirmer) la pertinence de certaines métriques utilisées pour la priorisation, et d'apporter des ajustements fondés sur des observations mesurées. Elles offrent également un moyen d'intégrer la notion d'incertitude dans l'évaluation du risque, par exemple en fournissant des intervalles de confiance ou des probabilités plutôt que des scores fixes. Cependant, ces méthodes ont leurs limites. Elles exigent la disponibilité de données historiques riches et de qualité (par exemple des enregistrements d'attaques réussies, des bases de données d'incidents, etc.), ce qui n'est pas toujours réalisable en pratique ou peut introduire un biais (toutes les failles ne sont pas déclarées publiquement, certains secteurs sont sous-représentés dans les jeux de données, etc.). En outre, les résultats issus d'analyses statistiques peuvent être difficiles à interpréter directement pour orienter la décision : une corrélation ou une mesure de tendance donne une indication globale, mais il peut être délicat de traduire cela en actions concrètes de priorisation sans une expertise supplémentaire. Enfin, comme toute approche basée sur les données passées, les modèles statistiques peuvent perdre de leur validité si le contexte des menaces évolue (phénomène du changement de distribution ou *concept drift*).

7. Conclusion

La priorisation des vulnérabilités constitue un domaine de recherche dynamique, à l'interface entre la gestion des risques et des disciplines techniques variées (sécurité des systèmes, intelligence artificielle, recherche opérationnelle, etc.). Les cinq familles de méthodes passées en revue dans cet article – graphes, apprentissage automatique, optimisation multi-objectifs, règles expertes et statistique – offrent chacune des perspectives différentes et souvent complémentaires pour aborder le problème. Le tableau 1 récapitule leurs points forts et faibles respectifs.

En pratique, aucune de ces approches n'éclipse totalement les autres : chacune apporte des éléments utiles, et c'est souvent une combinaison de méthodologies qui donnera les meilleurs résultats. On observe d'ailleurs une tendance à l'hybridation des solutions, par exemple en intégrant les scores CVSS dans des modèles bayésiens ou en couplant l'analyse de graphes avec des classements assistés par l'IA, afin de tirer parti des atouts de chaque approche [1]. Malgré les progrès réalisés, plusieurs défis de recherche demeurent. Il est nécessaire de développer des métriques plus dynamiques et contextuelles, capables d'évoluer en temps réel avec l'apparition de

Méthodologie	Avantages	Inconvénients
Basée sur les graphes	- Contextualise les failles dans l'architecture globale (vue d'ensemble des dépendances) - Identifie les points critiques (chemins d'attaque, failles pivot)	- Requiert un modèle exhaustif du système - Difficulté de passage à l'échelle (grands graphes complexes) - Modèle statique à mettre à jour manuellement
Apprentissage automatique	- Exploite de grandes quantités de données (NVD, historiques d'attaques, données textuelles) - Capte des motifs complexes indicateurs de risque - S'adapte aux évolutions en réentraînant les modèles	- Dépend de données d'entraînement de qualité (bruit, biais) - Modèles souvent opaques (boîte noire) - Nécessite une maintenance continue (mise à jour du modèle)
Optimisation multi-objectifs	- Approche rigoureuse équilibrant plusieurs critères (risque, coût, etc.) - Fournit un ensemble de solutions optimales (flexibilité de choix)	- Complexité computationnelle élevée (problème NP-difficile) - Paramétrage délicat (pondération des objectifs) - Solutions optimales parfois difficiles à appliquer directement
À base de règles	- Simplicité et transparence (décisions explicables) - Implémentation facile (s'appuie sur des standards comme CVSS)	- Rigidité : couvre mal les cas non prévus - Maintenance manuelle des règles (évolution des menaces) - Multiplication des règles $\rightarrow$ risque de conflits ou complexité
Statistique	- Fondé sur des données réelles (validation empirique des métriques) - Permet d'intégrer l'incertitude (approche probabiliste)	- Nécessite de larges jeux de données historiques - Portée explicative parfois limitée (résultats globaux à interpréter) - Pertinence conditionnée par la stabilité du contexte (menaces similaires à l'historique)

Table 1: Comparaison synthétique des principales catégories de méthodologies de priorisation des vulnérabilités, avec leurs avantages et inconvénients.

nouvelles menaces. L'évolutivité des solutions est également un enjeu, compte tenu du volume sans cesse croissant de vulnérabilités à traiter. Enfin, la fiabilité et la véracité des données (par exemple issues du renseignement sur les menaces) restent un point de vigilance pour éviter d'orienter la priorisation sur de fausses alertes.

En synthèse, l'état de l'art met en lumière la nécessité de combiner les approches pour aboutir à des stratégies de priorisation robustes et efficaces. En poursuivant les efforts de recherche sur l'intégration de ces méthodologies et sur l'adaptation aux nouveaux contextes (cloud, IoT, etc.), la communauté scientifique contribuera à combler le fossé entre les propositions académiques et les besoins opérationnels concrets en cybersécurité.

References

[1] Y. Jiang, N. Oo, Q. Meng, H. W. Lim, B. Sikdar, A Survey on Vulnerability Prioritization: Taxonomy, Metrics, and Research Challenges, arXiv preprint arXiv:2502.11070Cs.CR (2025). doi:10.48550/arXiv.2502.11070.
URL https://arxiv.org/abs/2502.11070

[2] E. Iannone, R. Guadagni, F. Ferrucci, A. De Lucia, F. Palomba, The secret life of software vulnerabilities: A large-scale empirical study, IEEE Transactions on Software Engineering 49 (1) (2022) 44–63. doi:10.1109/TSE.2022.3140868.

[3] S. Li, S. Wu, X. Guo, Security Risk Assessment Method for Measurement Control Systems Based on Attack Tree Model and Common Vulnerability Scoring System, in: Proc. of the 2023 Intl. Conf. on Artificial Intelligence, Systems and Network Security (AISNS), 2023, pp. 360–369. doi:10.1145/3661638.3661706.

[4] A. Chatzipoulidis, D. Michalopoulos, I. Mavridis, Information infrastructure risk prediction through platform vulnerability analysis, Journal of Systems and Software 106 (2015) 28–41. doi:10.1016/j.jss.2015.04.062.

[5] G. Aivatoglou, M. Anastasiadis, G. Spanos, A. Voulgaridis, K. Votis, D. Tzovaras, L. Angelis, A RAkEL-based methodology to estimate software vulnerability characteristics & score — an application to EU project ECHO, Multimedia Tools and Applications 81 (7) (2022) 9459–9479. doi:10.1007/s11042-021-11073-x.

[6] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, M. Roytman, Exploit Prediction Scoring System (EPSS), Digital Threats: Research and Practice 2 (3) (2021) 1–17. doi:10.1145/3436242.

[7] K. A. Farris, A. Shah, G. Cybenko, R. Ganesan, S. Jajodia, VULCON: A system for vulnerability prioritization, mitigation, and management, ACM Transactions on Privacy and Security 21 (4) (2018) 1–28. doi:10.1145/3196884.

[8] G. Yadav, P. Gauravaram, A. K. Jindal, K. Paul, SmartPatch: A patch prioritization framework, Computers in Industry 137 (2022) 103595. doi:10.1016/j.compind.2021.103595.

[9] F. Colombelli, V. Kehl Matter, B. Iochins Grisci, L. Lima, K. Heinen, M. Borges, S. José Rigo, J. L. Victória Barbosa, R. Da Rosa Righi, C. André Da Costa, et al., Multi-objective prioritization for data center vulnerability remediation,

in: Proc. of the 2022 IEEE Congress on Evolutionary Computation (CEC), 2022, pp. 1–8. doi:10.1109/CEC55065.2022.9870289.

[10] A. M. Dissanayaka, S. Mengel, L. Gittner, H. Khan, Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with MongoDB on Singularity Linux containers, in: Proc. of the 2020 4th International Conference on Compute and Data Analysis (ICCDA), 2020, pp. 58–66. doi:10.1145/3388142.3388168.

[11] M. Angelelli, S. Arima, C. Catalano, E. Ciavolino, A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence, Expert Systems with Applications 255 (2024) 124572. doi:10.1016/j.eswa.2024.124572.

[12] H. Holm, M. Ekstedt, D. Andersson, Empirical analysis of system-level vulnerability metrics through actual attacks, IEEE Transactions on Dependable and Secure Computing 9 (6) (2012) 825–837. doi:10.1109/TDSC.2012.66.