Le framework MITRE ATT&CK® comme outil de diagnostic de la maturité cyber d'une organisation

Thomas Des Grottes, Philippe Lépinard

30e Conférence de l'Association Information et Management

21-23 mai 2025 à Lyon

Le *framework* MITRE ATT&CK® comme outil de diagnostic de la maturité cyber d'une organisation

Thomas des Grottes, IAE Paris-Est, Université Paris-Est Créteil (UPEC)

Philippe Lépinard, Institut de Recherche en Gestion (IRG, EA 254), Université Paris-Est Créteil (UPEC)

Résumé

Cet article explore le potentiel du *framework* MITRE ATT&CK® en tant qu'outil de diagnostic de la maturité cyber des organisations. À travers une recherche-intervention menée au sein d'une banque française, nous montrons comment ce cadre offre une solution structurée et opérationnelle. Notre méthodologie combine plusieurs dispositifs de recueils de données afin de proposer une modélisation des lacunes et forces organisationnelles. Nos résultats préliminaires soulignent les atouts du *framework* pour prioriser les remédiations, soutenir les décisions stratégiques et favoriser la collaboration entre experts de la cybersécurité et décideurs.

Mots clés

Cybersécurité ; Maturité cyber ; MITRE ATT&CK® ; Recherche-intervention ; Diagnostic organisationnelle

The MITRE ATT&CK® framework as a tool for diagnosing an organisation's cyber maturity

Abstract

This article explores the potential of the MITRE ATT&CK® framework as a tool for diagnosing the cyber maturity of organisations. Through an intervention research conducted within a French bank, we show how this framework offers a structured and operational solution. Our methodology combines several data collection devices to propose a model of organisational

gaps and strengths. Our preliminary results highlight the framework's strengths in prioritising remedies, supporting strategic decisions and fostering collaboration between cybersecurity experts and decision-makers.

Keywords

Cybersecurity ; Cyber maturity ; MITRE ATT&CK® ; Intervention research ; Organisational diagnosis

Le *framework* MITRE ATT&CK® comme outil de diagnostic de la maturité cyber d'une organisation

1. Introduction

La menace numérique[1] s'impose aujourd'hui comme un enjeu stratégique majeur pour les organisations (Shin et al., 2013). La croissance exponentielle des cyberattaques, souvent couronnées de succès (Xiong & Lagerström, 2019), illustre la capacité des adversaires à exploiter les vulnérabilités humaines et techniques pour contourner les défenses existantes (Georgiadou et al., 2021). Cette réalité impose aux organisations, privées comme publiques, d'adopter une posture proactive en matière de cybersécurité. Le diagnostic de la maturité cyber constitue un défi complexe qui peut s'expliquer, entre autres, par la diversité des infrastructures informatiques, l'adoption massive des services *cloud* (Xiong et al., 2022) et l'évolution rapide des vecteurs et techniques d'attaque (Cremer et al., 2022). Dans ce contexte, il est essentiel de s'appuyer sur des outils adaptés pour modéliser les menaces et orienter les efforts d'amélioration continue. Le *framework* MITRE ATT&CK®[2], crée en 2013 par l'organisation MITRE, se distingue comme une ressource stratégique pour répondre à ces enjeux. Cette base de connaissances documente les tactiques et techniques utilisées par les adversaires, offrant une taxonomie précise et régulièrement mise à jour des comportements malveillants (Strom et al., 2018). Sa granularité, son évolution permanente et sa structure modulaire le rendent particulièrement pertinent pour des usages opérationnels variées, allant de l'émulation d'adversaires à la détection proactive (Xiong & Lagerström, 2019 ; Al-Sada et al., 2024). En parallèle, son adoption croissante dans les milieux opérationnels témoigne de son utilité comme levier stratégique pour optimiser les réponses aux incidents et améliorer les capacités (Georgiadou et al., 2021). Malgré les nombreuses applications pratiques du *framework*, la littérature scientifique s'est jusqu'à présent peu penchée sur le potentiel de ce cadre pour diagnostiquer la maturité cyber des organisations (Pirca & Lallie, 2023). En réponse à ces constats, nous formulons la question de recherche suivante : en quoi le *framework* MITRE ATT&CK® peut être un outil de diagnostic de la maturité cyber d'une organisation ? Pour répondre à cette question, nous avons débuté une recherche-intervention dans un environnement organisationnel réel, une banque française, afin d'explorer comment le cadre MITRE ATT&CK® peut être adapté pour fournir un diagnostic clair, opérationnel et accessible du niveau de maturité cyber des organisations. La première partie de l'article présente notre cadre théorique et le *framework* MITRE ATT&CK®. Dans un deuxième temps, nous détaillons notre méthodologie de recherche-intervention. Nous abordons ensuite dans une troisième étape nos résultats préliminaires. Les limites et perspectives de notre travail sont intégrées à la conclusion.

[1] « *Terme générique utilisé pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude* » (ANSSI, 2024, p.18).
[2] Site Internet du MITRE ATT&CK® : https://attack.mitre.org/

2. Cadre théorique et *framework* MITRE ATT&CK®

2.1. Cadre théorique

Notre projet de recherche s'intéresse à deux concepts théoriques que nous allons relier : le diagnostic organisationnel et la maturité cyber. Cette dernière est définie comme la « *capacité à adopter les meilleurs pratiques, se conformer aux normes, gérer de façon proactive son profil de risque (niveau de préparation humain, organisationnel et technique), apprendre et se remettre d'une attaque* » (Farjaudon & Gardès, 2024, p.69). Le diagnostic organisationnel est, quant-a-lui, le « *processus d'évaluation de l'état actuel (Lewin, 1964) d'une organisation (unité administrative, équipe, climat de travail, etc.), qui utilise des modèles conceptuels et des méthodes spécifiques en vue de soutenir cette organisation dans la résolution d'une situation identifiée comme étant appelée à changer* » (Charrette & Bouchard, 2020, p.16). Dans la continuité de ces définitions, nous proposons d'étudier comment la maturité cyber peut s'intégrer dans un diagnostic organisationnel afin de mieux cerner l'état de préparation et de résilience d'une organisation face aux risques numériques. Or, diagnostiquer la maturité cyber implique de considérer la cybersécurité non plus seulement comme un enjeu strictement technique, mais aussi comme une ressource stratégique. Si la cybersécurité était historiquement perçue comme un domaine réservé aux spécialistes techniques, elle s'érige aujourd'hui en levier stratégique, dans la mesure où la plupart des activités et process organisationnels dépendent du maintien d'un environnement numérique fiable et sécurisé. Notre idée est alors de proposer un diagnostic organisationnel centré sur la maturité cyber ; le tout grâce au *framework* MITRE ATT&CK®.

2.2. Le *framework* MITRE ATT&CK®

MITRE ATT&CK® (*Adversarial Tactics, Techniques, and Common Knowledge*) se présente comme une base de connaissances structurée documentant les comportements des adversaires à travers une taxonomie précise des tactiques et techniques utilisées tout au long du cycle de vie d'une cyberattaque. MITRE est une organisation américaine à but non lucratif, financée par le gouvernement fédéral des États-Unis et spécialisée dans la recherche et le développement dans des domaines stratégiques tels que la cybersécurité, la défense et la santé publique. Développé à partir de 2013, MITRE ATT&CK® trouve son origine dans le projet *Fort Meade Experiment* (FMX) visant à améliorer la détection post-compromission[3] en étudiant les comportements adverses dans des environnements simulés. Initialement centré sur les systèmes Microsoft Windows, qui constituaient une cible privilégiée en raison de leur prédominance dans les environnements professionnels (Blair, 2023), MITRE ATT&CK® s'est progressivement élargi pour intégrer d'autres plateformes (Linux, macOS), les environnements mobiles (Android, iOS) et les infrastructures critiques industriels (Strom et al., 2018 ; Al-Sada et al., 2024). Depuis sa création, MITRE ATT&CK® est mis à jour semestriellement, intégrant de nouvelles données issues de contributions publiques et d'analyses d'incidents réels. Cette capacité à s'adapter à l'évolution constante des menaces renforce son utilité opérationnelle et stratégique (Georgiadou et al., 2021 ; Al-Sada et al., 2024 ; Xiong et al., 2022).

[3] « *Post-compromise (intrusion) detection of cyber adversaries is an important capability for network defenders as adversaries continue to evolve methods for compromising systems and evading common defenses* » (MITRE, 2017, p.ii).

2.2.1. Structure et composantes fondamentales

Le *framework* MITRE ATT&CK® est structuré en une matrice multidimensionnelle qui s'articule autour de trois concepts : les tactiques, les techniques et les atténuations.

- Les tactiques représentent les objectifs stratégiques ou fonctionnels d'un adversaire dans une phase donnée d'une attaque (Strom et al., 2018 ; Pirca & Lallie, 2023).
- Les techniques décrivent les méthodes utilisées par les adversaires pour atteindre leurs objectifs tactiques. Les sous-techniques, apportent une granularité supplémentaire en détaillant les variations ou implémentations spécifiques d'une technique (Strom et al., 2018).
- Les atténuations regroupent les stratégies pour réduire ou prévenir l'impact des techniques adverses. Cependant, certaines techniques restent difficiles à atténuer (Xiong et al., 2022 ; Shin et al., 2023).

2.2.2. Utilisations et applications pratiques

Le *framework* MITRE ATT&CK® est largement utilisé dans des contextes variés pour renforcer la défense contre les cyberattaques et améliorer les capacités de détection. Il sert notamment de guide pour l'émulation d'adversaires et les exercices de *red teaming*[4] en fournissant une taxonomie détaillée des comportements malveillants. Cela permet aux équipes de sécurité de simuler des scénarios réalistes, d'évaluer l'efficacité des défenses organisationnelles et d'identifier les failles potentielles (Georgiadou et al., 2021). De plus, MITRE ATT&CK® contribue au développement des capacités de détection en reliant les techniques adverses aux sources de données disponibles. Par exemple, l'analyse des journaux d'événements ou des flux réseau peut être directement alignée avec des techniques documentées pour mieux détecter les activités suspectes et réagir de manière proactive (Strom et al., 2018). Grâce à sa structuration détaillée, le cadre joue un rôle clé dans l'amélioration continue des systèmes de défense et l'adaptation aux menaces évolutives.

3. Méthodologie de la recherche

L'objectif de cette recherche est d'explorer le potentiel du *framework* MITRE ATT&CK® comme outil de diagnostic de la maturité cyber des organisations. Notre méthodologie repose sur une recherche-action de type recherche-intervention, définie comme une démarche visant à « *comprendre en profondeur le fonctionnement du système, aider à définir des trajectoires possibles d'évolution, aider à en choisir une, [mais aussi à] la réaliser, à en évaluer le résultat* » (Allard-Poesi & Perret, 2003, p.95). Cette définition met en lumière la finalité pratique de la recherche qui vise à transformer la réalité organisationnelle tout en produisant des connaissances scientifiques (Allard-Poesi & Perret, 2004). Cette forme de recherche-action met l'accent sur une interaction étroite avec les acteurs organisationnels pour produire des résultats pragmatiques tout en contribuant à la compréhension scientifique du phénomène étudié. La recherche-intervention intègre une dynamique de co-construction des connaissances dans laquelle le chercheur joue un rôle actif dans le processus d'observation et d'analyse, tout en

[4] « *Dans le cadre de la cybersécurité, le red teaming est « a disciplined and systematic approach that adopts offensive strategies to bolster defensive capabilities » (McLaughlin, 2023, p.18). Il est donc destiné à tester les défenses cyber des organisations dans un cadre contractuel (et donc légal)* » (Lépinard & Yasonthiram, 2024, p.5).

intervenant pour améliorer les pratiques organisationnelles. Dans ce contexte, le choix de la recherche-intervention s'explique par le besoin de développer une solution adaptée aux réalités opérationnelles tout en apportant une contribution théorique. Ainsi, l'intégration du *framework* MITRE ATT&CK® dans l'environnement organisationnel repose sur une démarche participative visant à expérimenter et ajuster le cadre en fonction des retours des acteurs impliqués. L'articulation de nos travaux suit les quatre phases de la recherche-intervention permettant de s'assurer de l'actionnabilité des connaissances produites (Allard-Poési & Perret, 2003) : construction de l'objet, élaboration d'un modèle théorique matérialisé sous la forme d'un outil (le diagnostic organisationnel de la maturité cyber de l'organisation étudiée), le mise en application (test) de l'outil et évolution de ce dernier selon les retours des participants et l'élaboration des connaissances.

3.1. Participants

Notre recherche est conduite au sein d'une banque française comptant 594 collaborateurs, parmi lesquels 150 travaillent à la direction des services informatiques (DSI) et trois au sein de l'équipe sécurité des systèmes d'information (SSI), rattachée à la direction risques et conformité. Le groupe de participants inclut seize acteurs clés, sélectionnés pour leurs rôles dans la gestion et la sécurisation des systèmes d'information (SI) de l'organisation. Il se compose du responsable de la SSI, de cinq membres du service sécurité, de trois membres du service infrastructure et réseau, un membre du service pilotage et projets stratégiques, ainsi que six membres du service exploitation décentralisée et support. La diversité des profils des participants a permis de collecter des perspectives variées, essentielles pour une analyse complète et nuancée (Roy & Prévost, 2013). Par ailleurs, le rôle de chercheur-praticien en alternance au sein de l'entreprise d'un des auteurs a facilité une observation participante et une collecte de données directes et indirectes, enrichissant ainsi le corpus d'analyse.

3.2. Méthodes et procédure

3.2.1. Préparation et adaptation des outils

Le *framework* MITRE ATT&CK®, spécifiquement dans sa section "*Enterprise*", a été sélectionné comme référentiel analytique. Ce module couvre les comportements adverses liés aux réseaux informatiques d'entreprise et au *cloud* (Georgiadou et al., 2021) et propose un ensemble de 44 mesures d'atténuation comprenant des configurations, outils ou processus destinées à réduire l'efficacité des techniques adverses. Par exemple, l'atténuation M1057 « *Data Loss Prevention* » recommande : « *Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data* »[5]. Afin de garantir l'adoption interne de cette méthodologie par les acteurs de l'entreprise, une traduction en français a été réalisée en amont. Cette adaptation linguistique vise à réduire les barrières sémantiques susceptibles d'impacter l'engagement et l'appropriation des participants. Chaque mesure d'atténuation a ensuite été associée à un barème de notation inspiré du *Capability Maturity Model Integration* (CMMI)[6], un modèle reconnu pour sa capacité à structurer et évaluer des processus organisationnels selon

[5] Selon MITRE ATT&CK® : https://attack.mitre.org/mitigations/M1057/ (Consulté le 06 janvier 2025).
[6] Site Internet du CMMI *Institute* : https://cmmiinstitute.com/cmmi/intro.

des niveaux de maturité bien définis. Ce cadre repose sur une approche progressive visant à classifier les pratiques organisationnelles selon leur degré de formalisation, d'efficacité et de performance. L'illustration de ce modèle est présentée en annexe A. Pour cette recherche, le modèle CMMI a été ajusté pour évaluer quatre niveaux de maturité : Faible, Limité, Intermédiaire et Avancé. Ce choix de simplification repose sur la nécessité d'harmoniser le diagnostic avec d'autres référentiels tel que le *Cybersecurity Framework* du *National Institute of Standards and Technology* (NIST) qui adopte également une échelle à quatre niveaux. Les définitions des niveaux de maturité sont les suivantes : 1. Faible : Aucune stratégie ou outil en place. 2. Limité : Défenses en place mais partiellement appliquées ou peu efficaces. 3. Intermédiaire : Défenses définies, appliquées et opérationnelles. 4. Avancé : Défenses optimisées, automatisées et régulièrement auditées. La figure 1 illustre l'application de cette méthode d'évaluation à travers l'atténuation M1057.

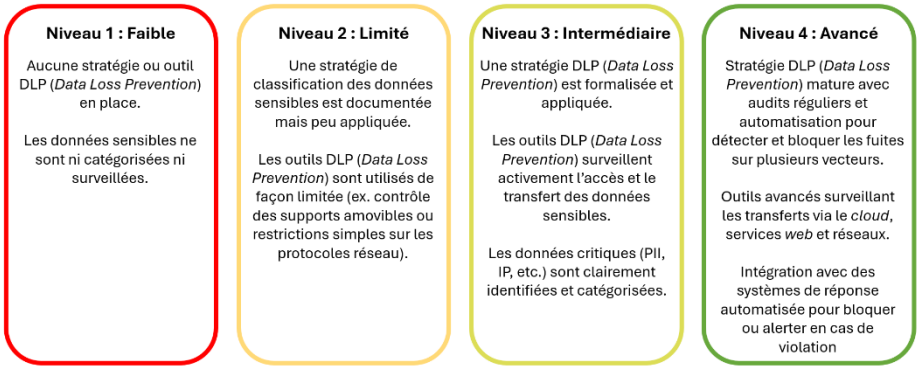

Figure 1. Exemple de notation de l'atténuation M1057.

3.2.2. Collecte des données

Les données recueillies reposent sur des approches qualitatives combinant :

- Des entretiens semi-directifs : un total de trize entretiens individuels ou en groupe a été conduits avec les membres du projet. Ces entretiens, structurés autour des atténuations MITRE ATT&CK®, visaient à collecter des informations détaillées sur les politiques, outils, et pratiques en place pour chaque mesure.
- De l'observation participante : le statut d'alternant en 2nde année d'un des auteurs a permis une immersion directe dans les processus organisationnels et une observation des pratiques opérationnelles.
- De l'analyse documentaire : les documents internes tels que les politiques de sécurité, les audits passés et les rapports d'incidents, ont été analysés afin de contextualiser et trianguler les données issues des entretiens.

3.2.3. Analyse et transposition des données

Les données qualitatives recueillies ont été analysées en suivant une méthode inductive inspirée de Mayring (2014) visant à dégager des thématiques principales. Chaque atténuation a été évaluée selon les niveaux de maturité définis et triangulée avec les données documentaires. Ce travail a permis d'obtenir une note pour les 44 mesures d'atténuation du MITRE ATT&CK® *Entreprise*. Enfin, les résultats ont été synthétisés et présentés lors de sessions de restitution aux participants pour valider leur pertinence. Le total de trize entretiens a permis d'atteindre un

niveau de saturation satisfaisant, c'est-à-dire que les nouvelles discussions n'apportaient plus d'informations significatives à la recherche. Les scores obtenus ont été transposés sur la matrice MITRE ATT&CK® pour visualiser la couverture des défenses organisationnelles. En effet chaque technique documentée dans la matrice est associée à une ou plusieurs mesures d'atténuation. Prenons l'exemple de la technique T1052 intitulée « *Exfiltration Over Physical Medium » décrite* comme suit : « *Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive.* »[7]. Cette technique peut être atténuée par les mesures d'atténuations suivantes : M1057 *« Data Loss Prevention »*[8] , M1042 *« Disable or Remove Feature or Program »*[9] et M1034 *« Limit Hardware Installation »*[10]. Pour une technique donnée, le score d'atténuation est alors calculé en faisant la moyenne des notes attribuées aux mesures associées. Cela permet d'obtenir une valeur unique, reflétant le niveau global de maturité lié à la couverture de cette technique. Cependant, certaines techniques ne disposent d'aucune atténuation documentée par MITRE ATT&CK®. Dans ces cas, les cases correspondantes de la matrice restent non évaluées.

4. Résultats préliminaires

L'outil de gestion créé doit pouvoir fournir une modélisation claire et accessible du niveau de maturité cyber de l'organisation étudiée. Pour atteindre cet objectif, les données collectées ont été transposées sur la matrice MITRE ATT&CK® *Entreprise*, permettant d'attribuer à chaque technique un score correspondant au niveau de couverture actuel. La figure 2 illustre une matrice fictive d'une organisation. Chaque case correspond à une technique spécifique, avec une coloration reflétant le niveau de maturité associé (Faible, Limité, Intermédiaire ou Avancé). Les techniques non couvertes sont représentées par des cases blanches.

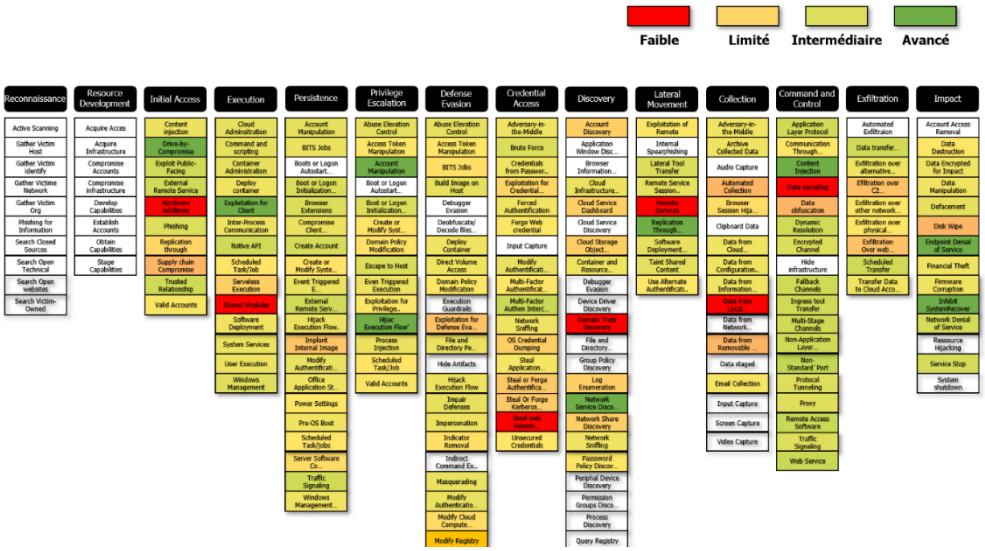

Figure 2. Matrice fictive du niveau de maturité d'une organisation[11].

[7] Selon MITRE ATT&CK® : https://attack.mitre.org/techniques/T1052/ (Consulté le 6 janvier 2025).
[8] Page Internet de la M1057 : https://attack.mitre.org/mitigations/M1057/. (Consulté le 6 janvier 2025).
[9] Page Internet de la M1042 : https://attack.mitre.org/mitigations/M1042/. (Consulté le 6 janvier 2025).
[10] Page Internet de la M1034 : https://attack.mitre.org/mitigations/M1034/. (Consulté le 6 janvier 2025).
[11] Possibilité d'annoter et d'explorer les matrices avec MITRE ATT&CK® *Navigator* à l'adresse : https://mitre-attack.github.io/attack-navigator/. (Consulté le 6 janvier 2025).

4.1. Avantages de la représentation matricielle

L'un des principaux avantages de cette représentation visuelle est de combler le fossé entre les experts techniques et les décideurs organisationnels. Les rapports de cybersécurité traditionnels, souvent complexes et techniques, sont difficiles à interpréter pour des profils non spécialisés, ce qui peut entraîner des réponses inadéquates ou tardives face aux menaces (Pirca & Lallie, 2023). La matrice MITRE ATT&CK®, en offrant une visualisation intuitive des faiblesses et forces du système d'information, permet de simplifier ces discussions et de soutenir des prises de décisions éclairées.

4.2. Intégration dans les processus organisationnels

L'application de cette matrice ne se limite pas à une simple évaluation descriptive. Elle a été intégrée dans plusieurs processus organisationnels clés, démontrant son potentiel pour orienter les pratiques et améliorer la posture de cybersécurité de l'organisation. Deux cas d'usage concrets ont été identifiés :

- Orientation des investissements en sécurité : les décisions relatives à l'achat de nouveaux outils ou services de cybersécurité sont désormais guidées par leur capacité à couvrir des techniques actuellement peu ou non couvertes.
- Gestion des vulnérabilités : en hiérarchisant les techniques critiques identifiées dans la matrice, les équipes ont pu prioriser les efforts de remédiation.

5. Discussion et conclusion

Le cadre MITRE ATT&CK®, conçu initialement pour documenter les comportements adverses dans le domaine cyber, s'impose désormais comme un outil stratégique dépassant son usage opérationnel. Cette étude a mis en évidence son potentiel pour mener un diagnostic organisationnel de la maturité cyber, en offrant une représentation structurée des forces et des faiblesses en cybersécurité. Sa granularité et sa modularité permettent une identification précise des lacunes défensives, tout en facilitant l'alignement entre les experts techniques et les décideurs organisationnels. Grâce à notre recherche-intervention, nous avons démontré l'adaptabilité de ce cadre à un environnement organisationnel réel. Les résultats soulignent l'utilité du *framework* pour guider les décisions stratégiques et prioriser les efforts de remédiation et d'investissement en cybersécurité.

Malgré ces résultats prometteurs, plusieurs limites ont toutefois été identifiées dans cette phase préliminaire. La première concerne le manque d'exhaustivité des vecteurs d'attaque au sein même du l'utilisation du *framework* MITRE ATT&CK®. Il est nécessaire de mettre en œuvre de manière complémentaire d'autres outils tels que *Common Attack Pattern Enumerations and Classifications* (CAPEC™)[12] ou *Common Weakness Enumeration* (CWE™)[13] qui se concentrent davantage sur les vulnérabilités spécifiques et les techniques d'exploitation (Strom et al., 2018). Cette complémentarité souligne la nécessité d'intégrer le *framework* MITRE ATT&CK® dans une approche holistique, combinant différents outils pour obtenir une vision complète des menaces et des défenses potentielles. Par ailleurs, la mise à jour semestrielle de la base de données MITRE ATT&CK®, bien qu'indispensable pour refléter les évolutions des cybermenaces, exige un effort constant de révision et d'adaptation. Cette contrainte peut

[12] Site internet du dispositif CAPEC™ : https://capec.mitre.org/.
[13] Site internet du dispositif CWE™ : https://cwe.mitre.org/.

s'avérer particulièrement lourde pour les organisations aux ressources limitées. De plus, la pondération des scores entre plusieurs atténuations associées à une même technique introduit une certaine subjectivité dans l'analyse. Cette limitation souligne l'importance de formaliser et standardiser les critères de pondération pour minimiser les biais dans l'évaluation. De plus, l'absence d'atténuations pour certaines techniques met en lumière des lacunes dans la couverture du *framework*.

Pour pallier ces limites, nous proposons plusieurs pistes de recherche futures. Nous recommandons le développement d'une méthode de pondération standardisée afin de minimiser les biais et d'améliorer la comparabilité des évaluations. En parallèle, l'identification de nouvelles stratégies pour combler les lacunes actuelles du *framework* paraît essentielle. Une extension de l'approche MITRE ATT&CK® à des contextes organisationnels variés, notamment les petites et moyennes entreprises (PME) ou les secteurs moins dotés en ressources cyber, permettrait également de tester et d'enrichir nos résultats initiaux. Enfin, la cybersécurité s'inscrit également dans une approche inter-organisationnelle. À ce titre, nous pensons qu'une démarche de diagnostic partagé (Michaux & Defélix, 2019) serait une extension importante de notre travail.

Références

Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. *IEEE Access*, 12, 1217-1234. https://doi.org/10.1109/ACCESS.2023.3344680.

Allard-Poesi, F., & Perret, V. (2003). La Recherche-Action. In Y. Giordano (Éd.), *Conduire un projet de recherche, une perspective qualitative* (p. 85-132). EMS.

Allard-Poesi, F., & Perret, V. (2004). La construction collective du problème dans la recherche-action : Difficultés, ressorts et enjeux. *Finance Contrôle Stratégie*, 2004, 7(4), 5-36. https://shs.hal.science/halshs-00536277/document.

ANSSI (2024). Cyberdico. https://urlr.me/vB4gX3.

Blair, R. (2023). *Aligning Security Operations with the MITRE ATT&CK Framework : Level up your security operations center for better security*. Packt Publishing.

Charette, L., & Bouchard, M. (2020). *Diagnostic organisationnel et analyse de besoins*. Presses de l'Université Laval.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, 47(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6.

Farjaudon, A.-L., & Gardès, N. (2024). La maturité cyber au prisme de la communication extra-financière : une analyse des entreprises du CAC 40. Revue Française de Gestion Industrielle, 38(2), 67-85. https://doi.org/10.53102/2024.38.02.1187.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, 21(9). https://doi.org/10.3390/s21093267.

Godfrey, S. (2008). Using CMMI for Improvement at GSFC. *NASA presentation*. https://ses.gsfc.nasa.gov/ses_data_2004/040601_Godfrey.ppt.

Lépinard, P., & Yasonthiram K. (2024). Osinter et red teamer Les corsaires du cyberspace. *Revue de Management et de Stratégie*. https://www.revue-rms.fr/attachment/2646864/.

Mayring, P. (2014). *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*. Klagenfurt.

Michaux, V., & Defélix, C. (2019). Conduire un diagnostic partagé en contexte inter-organisationnel : enseignements théoriques et pratiques. *Revue de gestion des ressources humaines*, 111(1), 19-34. https://doi.org/10.3917/grhu.111.0019.

MITRE (2017). *Finding Cyber Threats with ATT&CK™-Based Analytics*. The MITRE Corporation. https://apps.dtic.mil/sti/trecms/pdf/AD1107945.pdf.

Pirca, A. M., & Lallie, H. S. (2023). An empirical evaluation of the effectiveness of attack graphs and MITRE ATT&CK matrices in aiding cyberattack perception amongst decision-makers. *Computers & Security*, 130, 103254. https://doi.org/10.1016/j.cose.2023.103254.

Roy, M., & Prévost, P. (2013). La recherche-action : origines, caractéristiques et implications de son utilisation dans les sciences de la gestion. *Recherches qualitatives*, 32(2), 129–151. https://doi.org/10.7202/1084625ar.

Shin, C., Lee, I., & Choi, C. (2023). Exploiting TTP Co-Occurrence via GloVe-Based Embedding With MITRE ATT&CK Framework. *IEEE Access*, 11, 100823-100831. https://doi.org/10.1109/ACCESS.2023.3315121.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A.G., & Thomas, C. B. (2018). *Mitre Att&ck™: Design and Philosophy.* MITRE Corporation. https://urlr.me/emrGqh.

Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security*, 84, 53-69. https://doi.org/10.1016/j.cose.2019.03.010.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 21(1), 157-177. https://doi.org/10.1007/s10270-021-00898-7.

Annexe

Annexe A. *Characteristics of the Maturity levels* (Godfrey, 2008, p.6).