PriMera Scientific Publications

Synergizing Human Expertise, Automation, and Artificial Intelligence for Vulnerability Management

Multi-method Investigation of Emerging Tensions and Scoring Methodologies

Mehdi Saadallah*, Abbas Shahim, and Svetlana Khapova

Vrije Universiteit Amsterdam, Amsterdam, Netherlands

*Corresponding Author: Mehdi Saadallah, Vrije Universiteit Amsterdam, Amsterdam, Netherlands.

Abstract

Fast-growing digital trends have driven growth in the threat landscape of cyber-attacks, pushing unprecedented burdens on organizations to manage vulnerabilities effectively. This study investigated two years of complex relationships between human expertise and technological solutions in the domain of cybersecurity vulnerability management (VM) for a leading fast-moving consumer goods (FMCG) company operating internationally in multiple countries, leveraging both on-premises and cloud infrastructure. This study introduces the tensions arising from this duality, and an innovative AI-driven scoring methodology designed to streamline the end-to-end vulnerability management process to offer a more dynamic and contextualized risk assessment that the current traditional scoring methods such as the Common Vulnerability Scoring System (CVSS) lacks. Rooted in sociotechnical systems theory (STS), actor-network theory (ANT), and resource-based view (RBV), this research bridges the gap between technological reliance and human interpretative skills, which are two dominant but often disconnected aspects of VM. This paper highlights the benefit of VM that results from a symbiotic relationship between humans and technology, emphasizing how artificial intelligence (AI) and automation can mitigate the limitations of human-centric approaches and how humans can address the technological contextual limitations, resulting in a win-win approach. The findings set the orientation for a nascent stream of academic research on the relationship between humans and AI in vulnerability management and practical applications for scoring vulnerabilities in cybersecurity.

Keywords: Vulnerability management; Artificial intelligence; Automation; Human aspects of security; technology vs human expertise; Vulnerability scoring; CVSS

Introduction

In the current digital landscape, vulnerability management (VM) has never been more critical. Organizations of all sizes and sectors are increasingly reliant on digital infrastructures, making them susceptible to various cyber threats [1, 2]. Cybersecurity [3] researchers, professionals, IT administrators, policymakers, and even end-users have a vested interest in improving and optimizing the VM process [4, 5]. Existing literature explores several aspects of VM, ranging from human-centric

approaches to technology-driven solutions. While some studies praise the virtues of automation [6], which in the context of cyber-security refers to technology performing security tasks with minimal human intervention to protect against, detect, and respond to cyber threats, and artificial intelligence (AI) [7], which pertains to machines that mimic human intelligence to perform tasks and can iteratively improve themselves based on the information they collect [8, 9], others argue for the irreplaceable value of human expertise [10]. However, there is a notable gap in the literature concerning the symbiotic relationship between these two paradigms, particularly in an end-to-end context.

Our inductive study addresses this gap by asking "How can AI and automation be effectively integrated into the end-to-end vulnerability management process to resolve the identified tensions and improve efficiency and security?". This methodology leverages the predictive capabilities of AI to forecast potential vulnerabilities and the efficiency of automation in implementing security protocols. It aims to navigate the tensions between technological reliance and human expertise by addressing the dialectic complexity and usability challenges that arise in a multi-vendor context based on the Gioia methodology [11], as shown in Figs. 1 and 2, proposing an integrated, symbiotic solution an AI-driven scoring methodology that augments and complements existing traditional systems like CVSS (Common Vulnerability Scoring System) as shown in Table. 1.

We conducted 32 interviews ranging from high-level executives such as the group chief information security officer to specialized roles such as VM lead and IT infrastructure lead working on a leading FMCG company. This study focuses not only on the current state but also on the potential future state of the VM. As the organization has recently begun automating routine cybersecurity tasks and is contemplating integrating AI for enhanced decision-making and predictive analysis, we intentionally selected a diverse sample across hierarchical levels and expertise to capture various viewpoints on both current practices and future possibilities. To explain the findings, we draw from management and organizational theories such as sociotechnical systems theory (STS), actor-network theory (ANT), and resource-based view (RBV), which describe the theoretical tensions presented in this paper.

This paper continues with a brief overview of related research and theoretical foundations. Then, after explaining our methodology, we provide an in-depth analysis of our empirical findings describing two tensions. Because our aim is to study a phenomenon through a multi-theoretical lens, each tension includes a brief theoretical background. We then explain the theoretical tensions within the VM. The study concludes by discussing the implications of our findings and suggestions for future research.

Related Research: Humans and AI in Vulnerability Management

Existing cybersecurity research often treats technological advancements, such as AI and automation, as distinct from human elements [7, 12]. This approach overlooks the complementary potential that arises from the integration of AI's predictive analytics and decision-making capabilities with the efficiency of automation in performing security measures. Studies such as those presented in Springer and IEEE Xplore advocate a holistic perspective that encompasses individual, organizational, and technological factors [12, 13]. In particular, the merging of AI's cognitive competencies with automation's capacity to execute security protocols presents a transformative potential for cybersecurity frameworks. Ethical dissonances in human-machine interactions, as discussed in the literature, underscore the necessity for an inclusive approach that synergizes AI's and automation's technical strengths with human cognitive and ethical judgments [12]. The role of AI and automation in VM is often narrowly portrayed, focusing on isolated aspects of the process rather than cohesive integration. There is a dearth of comprehensive research spanning the entire scope of VM. This includes AI's application in predictive vulnerability identification and the systematic application of remedies via automation to the increasingly complex and numerous vulnerabilities. A more encompassing view, integrating AI with strategic VM, is imperative for an overall understanding and effective implementation.

To address these identified gaps, this study explores tensions that seamlessly integrate AI and human expertise within the strategic context of cybersecurity. This study also examines how automation can serve as the operational backbone for AI-driven decisions in the VM process. It aims to provide a holistic understanding of cybersecurity, where AI is not merely a tool but a strategic ally, working in tandem with human insight to fortify cyber defenses.

Theoretical Foundations of Vulnerability Management

Our study draws upon several theories to analyze the complexities of VM within cybersecurity. The sociotechnical systems theory [14], referred to in our study as "STS" is relevant in scenarios where human decisions intersect with technological processes in cybersecurity. It advocates that the interaction between social (human actors) and technical (technology) elements within organizations requires optimization of both aspects to enhance overall system effectiveness. The actor-network theory [15], referred to in our study as "ANT" complements the STS view by considering that both human and non-human elements, such as technology, act as influencers in a network. In our study, ANT highlights how tools like AI and automation shape practices and decision-making processes, underscoring their roles as active network participants rather than mere facilitators. The resource-based view [16], referred to as "RBV" offers another perspective in our study that focuses on leveraging organizational resources that are rare and difficult to imitate as strategic assets. Applied to our VM study, RBV unique combinations of human expertise and technological capabilities can provide competitive advantages in managing vulnerabilities.

Methods

To explore the complexities of VM in cybersecurity, this study adopts a qualitative research approach focusing on the tensions arising from the complex relationship between human expertise and advanced technological systems, such as AI and automation. This approach is instrumental in capturing the lived experiences of professionals in the field and understanding how the integration of AI and automation enhances traditional VM practices. Qualitative methods are particularly useful for understanding context, interpreting phenomena from the viewpoint of participants, and uncovering the underlying reasons and motivations for specific behaviors or trends [17, 18]. Given the exploratory nature of this study, which seeks to identify and contextualize new tensions for VM, a qualitative design is deemed most appropriate. This enables an in-depth exploration of how human decision makers interact with influence and are impacted by AI and automation technologies in the context of cybersecurity threats.

Research Context

The fast-moving consumer goods (FMCG) company under study listed on the London Stock Exchange currently employs a diverse range of tools for VM, each contributing uniquely to a robust cybersecurity posture. InsightVM is primarily used for scanning servers, Defender for endpoint is used for workstations, Claroty CTD is designated for the OT environment, and Qomplx focuses on active directory issues. The company scans for vulnerabilities across all countries and within its central IT. The scope of vulnerabilities is managed through a combination of manual, automated, and hybrid tasks, each harnessing the strengths of human oversight complemented by the consistency and efficiency of automation. Manual tasks include IP range reviews, false positive identification, inventory and classification, and continuous monitoring. Automated tasks mainly include scanning, metrics, and reporting, whereas verification and validation, prioritization, and assurance are managed as hybrid tasks that involve both human oversight and automated functionalities. The VM process is a multi-stakeholder operation involving various roles within the organization. The cybersecurity team uses automated tools for routine tasks and applies human expertise for tasks that require deeper analytical insights, such as vulnerability assessment, prioritization, and verification. Automated and hybrid tasks ensure that the bulk of operations, including scanning, metrics, and reporting, are conducted with efficiency and scale, whereas manual tasks, such as IP range reviews and false positive identification, require human judgment.

Recently, the company has been making strides in modernizing its approach to VM. In March 2022, they transitioned into an agile model using the SAFE method to tackle their backlog and prioritize tasks. They are also enhancing their configuration management database (CMDB) to automate the assignment of vulnerabilities. This shift underscores the organization's journey toward integrating AI into VM, as evidenced by the implementation of an emergency patching process to immediately address high-risk vulnerabilities, a precursor to a more AI-informed decision-making process. A high level of awareness regarding VM exists within the company. The roles are well defined, and the process is becoming increasingly formalized. Despite this, the teams are still limited by capacity limitations, leading to an extensive backlog of vulnerabilities. The lack of capacity for remediation has fostered a shared recognition of the potential benefits of automation and AI within the organization.

Data Collection Process

In 2022, the study included continuous observation [19] of the company's VM activities. This entailed participation in various internal discussions, direct oversight of the security operations environment, and real-time tracking of vulnerability resolution, yielding valuable insights into the dynamic interplay between human expertise, automation, and the future potential of AI in managing cybersecurity threats [20]. Observational data has been systematically compiled since 2022 in the form of trends, offering an invaluable long-term perspective on the evolving landscape of VM within the firm.

Several types of organizational documents were analyzed (total of 44), including automated reports generated from InsightVM, which provided crucial metrics on vulnerabilities, assets, and remediation strategies. These reports, such as "All Assets All Vulnerabilities," "All Assets," and "All Vulnerabilities," serve as instrumental resources for creating a remediation tracker that guides the organization's VM efforts and helps the authors understand the limitations of the current prioritization mechanism. In addition, other tools such as Defender for endpoint, Qomplx, and Claroty CTD offer a more rounded view of the VM landscape.

Sampling was performed using a stratified and purposeful sampling technique. The aim was to include participants who could provide valuable insights into VM as well as the nascent stages of automation and AI adoption within the organization [21]. The company C-levels have identified 34 members, ranging from high-level executives such as the chief information security officer to specialized roles such as VM lead and IT infrastructure lead, who would contribute to this study. We divided the population into subgroups (strata) that share similar levels of seniority within the company. We conducted judgmental interviews that allowed us to purposely select 15 subjects who were committed to our study and presented the right level of VM expertise and security operations awareness. We recruited the remaining seven sub-jects among the acquaintances of the initial interviewed subjects. This snowballing method was useful for accessing populations that were difficult to reach and were not identified in the initial sample. The duration of our study allowed us to use a hybrid sampling approach initiated by a probability method (stratification) and leverage the non-probability method (purposive and snowball) to further refine the sample and support the generalizability of the findings to the entire population. We conducted a semi-structured interview with each of the 22 participants to understand how AI, humans, and automation can enhance VM practices. We extended a second inter-view to participants who contributed more to the tensions identified.

Data Analysis Methods

For data coding and analysis, we used the Gioia methodology [11]. We summarized each interview and extracted relevant quotes using this method. None of these quotations were rephrased to avoid bias. Initial codes (first-order concepts) were inductively generated from the data, which were then grouped into second-order themes, which were further abstracted into aggregate dimensions. This iterative and inductive approach facilitated the identification of emergent themes that reflect the complex realities of integrating AI and automation with human expertise in cybersecurity practices.

Several steps were taken to ensure the reliability and validity of the findings. A triangulation of data sources [22], including interviews, observations, and document reviews, was conducted during the analysis. This allowed for a comprehensive understanding of the subject matter and reduced the risk of bias. Verbatim quotes and findings were discussed with the participants after each interview to ensure that there was no bias in the interpretation of their responses. Peer reviews and expert consultations were also conducted to validate the study findings. Finally, member checks were performed, and preliminary findings were presented for validation to a subset. Interviews provided direct insights from practitioners, highlighting their experiences and perceptions, while observations allowed us to witness the real-time application and integration of automation tools within the operational environment, providing a practical perspective that complemented the interview data. Document reviews offered a historical and policy-oriented view that helped contextualize the changes and strategic adoption of technology and agile practices in VM.

To further enhance the reliability of our findings, future methodologies should include comparative studies involving multiple organizations of different sizes. This approach will allow for a more comprehensive analysis of the interplay between human expertise and AI in VM and will help identify industry-specific factors that may affect the implementation of AI and automation.

Findings

In this section, we present our findings regarding tensions related to AI and automation in tandem with human-driven approaches toward VM. This analysis illuminates the inherent complexities, opportunities, and challenges of combining human expertise with technological solutions, setting the stage for a nuanced discussion of their practical and theoretical implications. We explore how the interplay between human decision making and AI-driven insights, augmented by automation efficiency, contributes to a robust VM framework. This interplay enhances the ability to identify, prioritize, and mitigate vulnerabilities more effectively, showcasing the complementary strengths of each component.

Our findings are presented with a strong emphasis on demonstrating how theoretical concepts are applied in real-world scenarios. We meticulously aligned our data with the theoretical frameworks, as depicted in Figs. 1 and 2, ensuring a clear demonstration of how each piece of data supports our analysis. To maintain confidentiality and provide context, we use anonymized interview identifiers. For instance, a quote from an interview might be cited as follows: "(FPA, page 1, 00:58)," which indicates the source's unique identifier, the page number of the transcript, and the exact timestamp when the statement was made. By articulating the nuanced dynamics between technology and human input, our findings highlight the critical roles that AI and automation play in enhancing decision making processes within VMs. This approach not only clarifies the operational benefits but also deepens the understanding of strategic integration points for technology within existing cybersecurity frameworks.

Addressing Challenges Across the Existing VM Process

Our research has identified several key challenges in the VM process where AI and automation can be instrumental in ensuring more accurate data handling, enhancing the speed and reliability of processes, and reducing human errors, thereby streamlining the entire VM lifecycle. Inventory and classification issues stem from an outdated configuration management database (CMDB), which is crucial for accurate asset classification " The CMDB... currently is not up to date ... information is missing." (SSO, page 2, 17:41) AI and automation can improve this by automating the data collection and updating processes, ensuring that the CMDB labels and tags (asset owner, asset type, criticality, operating system, IP address ...) remains accurate and up-to-date without manual intervention. Vulnerability assessment is hindered by inadequate tools and a lack of standardized processes, as noted by an enterprise architect: "We do not have a centralized approach or standardized official guidelines... work in progress." (PKO, page 2, 03:11). Automating vulnerability scans with AI-driven tools that adapt to new threats in real time can enhance detection capabilities and ensure consistency across assessments. In prioritization, incomplete data complicates effective threat ranking overwhelming teams: "The teams... do not have the capability or resources to address all the things that we already sent to them." (IBO, page 4, 11:22). AI can analyze vast amounts of data to dynamically prioritize vulnerabilities based on threat intelligence and business impact, thus streamlining the process and ensuring that critical issues are addressed promptly. Finally, remediation execution faces inefficiencies due to manual task management and tracking: "You need to validate... are they really remediated... this information comes from the tool that is the source of the vulnerabilities." (SSO, page 9, 59:48). Automation can streamline the execution and verification of remediation tasks by automatically updating task statuses and validating the effectiveness of patches or fixes, thus reducing manual checks and errors.

Technology Versus Human Expertise Tension

The overarching tension between technology and human expertise in the VM space relates to a debate in the literature concerning the relationship between these two elements. A long-held assumption in the literature is that asymmetric viewpoints overestimate the role of technology at the expense of human expertise or vice versa. This imbalanced approach can be understood through the lens of STS. Malatji [14] argued that technology and human systems are deeply interrelated and should be studied in a unified manner, emphasizing the need to balance social, technical, and environmental dimensions within organizational cybersecurity practices [23].

Symmetric perspectives are a collaborative model in which AI and automation tools enhance human capabilities rather than replace them [24]. The ANT focuses on the interplay and relational dynamics between human and non-human actors (like technology). This tension illuminates how different stakeholders, technologies, and contextual factors converge to create a cohesive cybersecurity state.

For instance, Balzacq and Cavelty [15] demonstrated that the core tenants of ANT can serve as heuristics for a better understanding of the stakes of cybersecurity, how it operates, and its failures. Similarly, organizational science that focuses on the "human factor" can enrich cybersecurity initiatives, providing a richer understanding of the dynamics between technical systems and human actors [25].

We aligned this theoretical background with our empirical data to underscore the need for a symbiotic, harmonious, and integrated approach where AI and automation augment human expertise in VM. This is consistent with the RBV, which considers human and technological resources as strategic assets that provide a sustainable competitive advantage in VM for FMCG companies [26, 27].
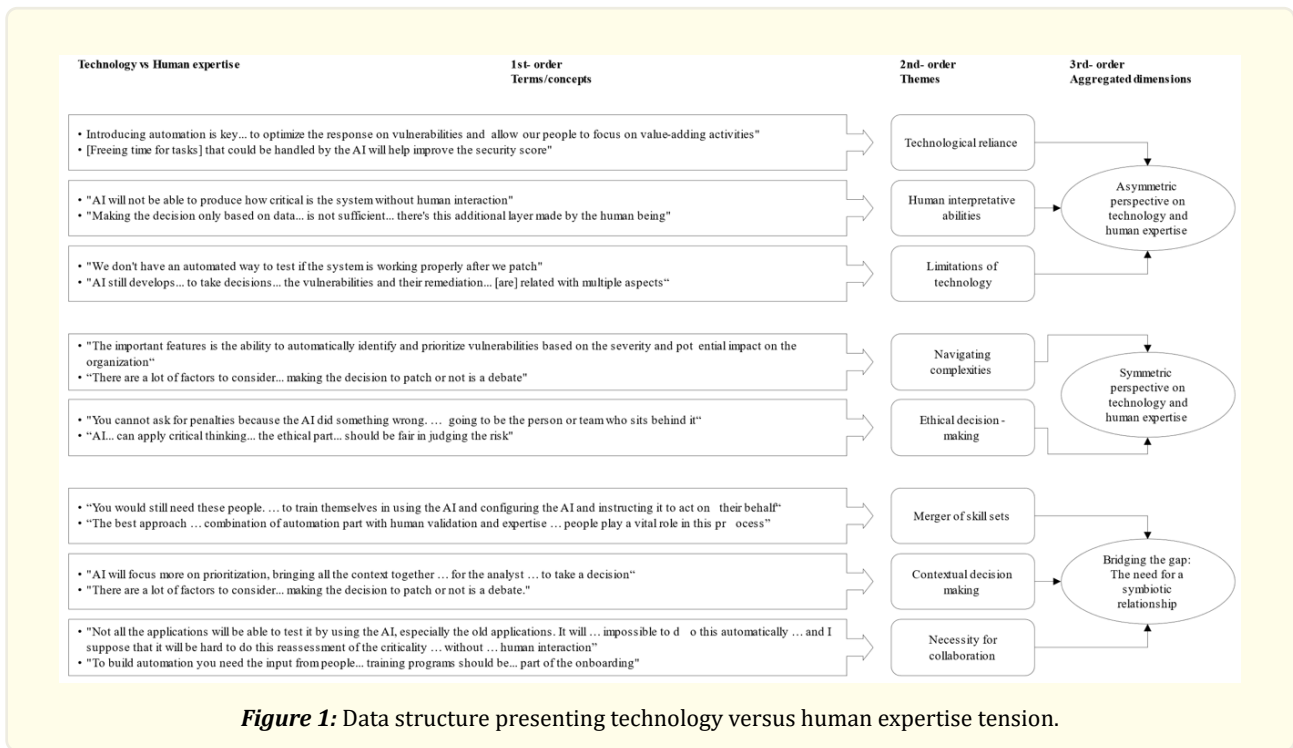

Figure 1: Data structure presenting technology versus human expertise tension.

Asymmetric Perspective on Technology and Human Expertise

Technological reliance is a prominent construct that has surfaced in the asymmetric context of VM within the FMCG company under investigation. The company's CISO underscored the importance of automation, stating, "Introducing automation is key... to optimize the response on vulnerabilities and allow our people to focus on value-adding activities." (FPA, page 1, 00:58). This illuminates the shifting paradigm in which automation has transcended from being a mere auxiliary support to a critical component for optimizing responses to vulnerabilities.

The construct of human interpretative abilities underlines an essential facet of the VM landscape in FMCG companies. It captures the ongoing tension between the capabilities of automated systems and the necessity for human expertise in various aspects of VM. The head of security platforms emphasized the need for human involvement in evaluating the criticality of system vulnerabilities "AI will not be able to produce how critical is the system without human interaction" (TST, page 5, 23:32). This highlights the limitations of technology in understanding the nuances of critical systems, thereby necessitating human interpretative skills.

The concept of "limitations of technology" exposes the constraints and challenges associated with the use of automated systems and AI in VMs. These limitations largely revolve around data accuracy, system complexities, and the inherent fallibility of automated solutions. The head of security platforms discusses a practical limitation of automated systems in the company's context, stating, "We don't have an automated way to test if the system is working properly after we patch" (TST, page 4, 16:43). This limitation points to

gaps in automation where human intervention is still necessary.

Symmetric Perspective on Technology and Human Expertise

The "symmetric perspective on technology and human expertise," incorporates a balanced view of the roles that both technology and humans play in VM. The theme of "navigating complexities" encapsulates the multitude of challenges and decision making processes that organizations face in VM. Complexity emerges not only from technological architecture but also from the involvement of human expertise in interpretation, judgment, and decision making. As one analyst mentioned, "The important feature is the ability to automatically identify and prioritize vulnerabilities based on the severity and potential impact on the organization" (SNA, page 8, 30:52). This statement highlights the importance of technology in prioritizing activities but leaves room for human expertise to interpret the potential impact, which may involve business, operational, or even psychological considerations.

Ethical decision making serves as a cornerstone in the complex VM landscape. This theme explores the moral and ethical considerations involved in the application of automation and AI tools in the cybersecurity domain. The network & communication services ART (agile-release train) lead highlights accountability "You cannot ask for penalties because the AI did something wrong. ... going to be the person or team who sits behind it" (TDO, page 7, 38:19). This home drives the point that, at the end of the day, ethical accountability rests with humans, not machines.

### Bridging the Gap: the Need for a Symbiotic Relationship

This construct offers a holistic view of the symbiotic relationship between human expertise and technological solutions, such as AI and automation, in the context of VM. The "merger of skill sets" theme centers on the union of human skills and technological capacities, particularly in the context of automation and AI within cybersecurity. The network & communication services ART leader indicated that AI does not replace humans but changes the work saying "You would still need these people. ... to train themselves in using the AI and configuring the AI and instructing it to act on their behalf" (TDO, page 9, 47:31). This signifies that the integration of technology requires a new set of skills for human experts.

The theme of contextual decision making revolves around the combination of AI capabilities and human expertise to make context-sensitive decisions in VMs. The CISO discusses AI's role in decision making stating "AI will focus more on prioritization, bringing all the context together ... for the analyst ... to take a decision" (FPA, page 9, 34:57). This suggests that AI can aggregate contextual data to support analysts in making more informed decisions.

The theme of "necessity for collaboration" delves into the importance of collective effort among various stakeholders, such as internal teams, vendors, or automated systems, in the effective management of vulnerabilities. The head of security platforms shares "Not all the applications will be able to test it by using the AI, especially the old applications. It will ... impossible to do this automatically ... and I suppose that it will be hard to do this reassessment of the criticality ... without ... human interaction" (TST, page 5, 23:32). This highlights that automation and AI would not be able to tackle all the use cases and that different teams and vendors each play a unique role, emphasizing the need for effective coordination among them.

Dialectic Usability and Complexity in Multi-Vendor VM Ecosystems

The second tension revolves around the challenges that organizations face in navigating the intricacies of complexity, usability, multi-vendor environments, and accelerating technological advancements. STS offers insights into managing complexity through structured approaches, and ANT underscores the centrality of usability and user experience, particularly when interacting with AI and automated systems. The RBV view theory underscores the value of effectively leveraging internal resources. Collectively, these theories deepen our understanding of navigating the fast-evolving technological landscape in VM, especially when AI and automation play pivotal roles.

Figure 2: Data structure presenting the dialectic of usability and complexity in multi-vendor VM ecosystem tension.
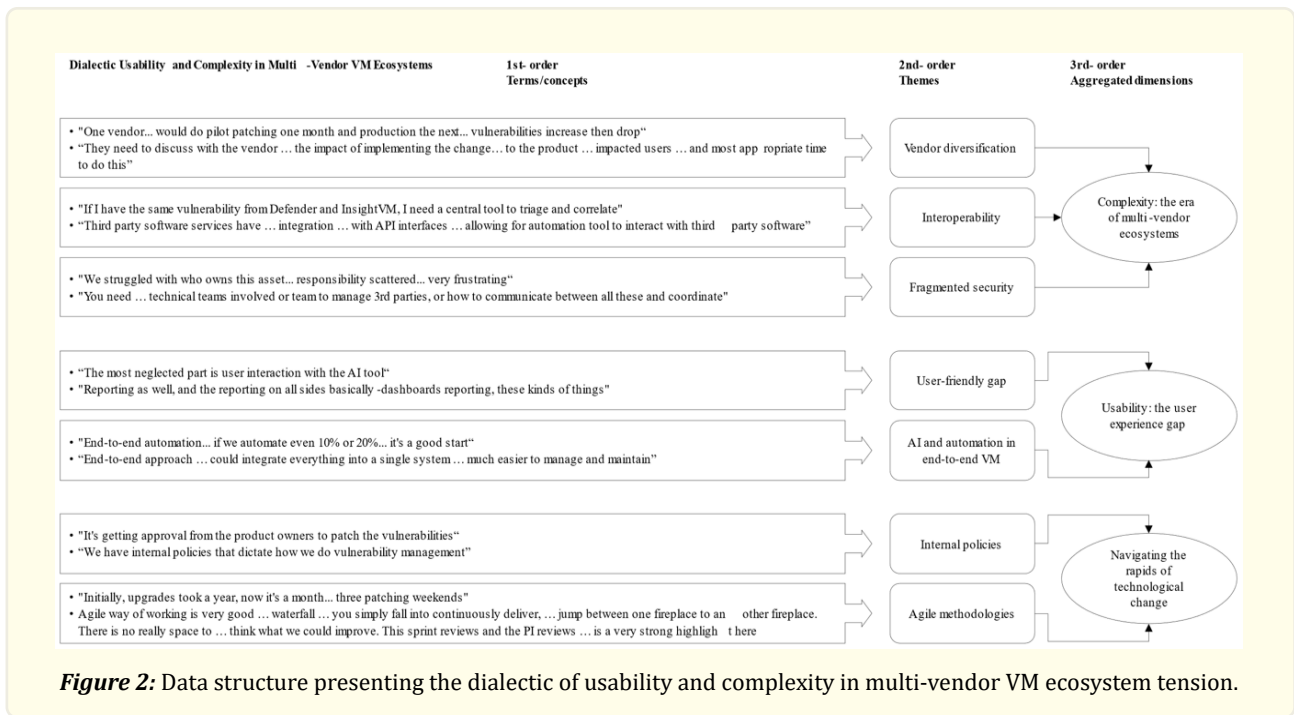
Complexity: The Era of Multi-Vendor Ecosystems

Vendor diversification is complex and multifaceted, and it touches on challenges related to integration, risk management, and operational efficiency. It also raises important questions about how organizations can best manage a diverse array of critical multi-vendor relationships [28] securely and efficiently in an environment where AI and automation are becoming increasingly prevalent. The infrastructure team leader described the difficulty of coordinating patch schedules between different vendors "One vendor... would do pilot patching one month and production the next... vulnerabilities increase then drop" (YBE, page 5, 27:16).

Interoperability challenges are pivotal in the context of VMs as they dictate the effectiveness of integrating various automated and AI-driven security tools. These challenges are not just technical but involve human and organizational aspects, making them multifaceted issues to address [29]. The VM leader discusses the need for a central tool for vulnerability correlation "If I have the same vulnerability from De-fender and InsightVM, I need a central tool to triage and correlate" (ITZ, page 9, 26:27).

The fragmented security approach theme indicates the multifaceted nature of managing vulnerabilities in a multi-vendor setting. This complexity extends beyond technical challenges to organizational and process-related issues. The VM lead laments the dispersed responsibilities for remediation "We struggled with who owns this asset... responsibility scattered... very frustrating" (ITZ, page 6, 14:33).

Usability: The User Experience Gap

The "user-friendly gap" theme exposes the imperative need for a more intuitive, user-centric design in VM tools. These design issues not only affect user satisfaction but also hinder the effective management of vulnerabilities. The incident coordinator focuses on the neglected aspect of how users interact with AI tools "The most neglected part is user interaction with the AI tool" (MST, page 4, 11:39).

The role of AI and automation in end-to-end VM is being increasingly recognized for its potential to enhance process efficiency. The CISO emphasizes the practical benefits of automating even a small percentage of cases in VM "End-to-end automation... if we automate even 10% or 20%... it's a good start" (FPA, page 4, 10:37).

Navigating the Rapids of Technological Change

The theme of internal policies focuses on governance structures, prioritization mechanisms, and operational guidelines that steer VM within organizations. These policies serve as the backbone for decision making and execution in a landscape marked by rapid technological changes. The SOC leader discusses the challenges of obtaining approval for patching vulnerabilities: "It's getting approval from the product owners to patch the vulnerabilities" (CTZ, page 6, 30:37).

The adoption of agile methodologies has been a game changer in addressing the responsiveness and flexibility challenges in VM. The network and communication services ART leader speaks to the speed that agile methodologies have brought into the upgrade cycle: "Initially, upgrades took a year, now it's a month... three patching weekends" (TDO, page 5, 29:20).

AI and human-driven scoring in vulnerability management

"Bridging the Gap: The Need for a Symbiotic Relationship", from the third aggregate of the first tension (as delineated in figure 1) "Technology vs Human expertise", call for a balanced approach that leverages both technological solutions and human expertise [12]. In this chapter, we introduce a novel vulnerability scoring system based on four components (Table 1) that addresses AI-human expertise and the limitations of traditional vulnerability scoring methods such as the common vulnerability scoring system (CVSS), exploit prediction scoring system (EPSS), and vulnerability priority rating (VPR) [30, 31].

Components	*Sub-components*
AI-Driven Algorithms	**Exploitability Score Assessment:** The exploitability score predicts the exploitability of new threats to the FMCG environment. It leverages modern machine learning techniques, such as the risk scoring system developed by NopSec and the multi-year vulnerability data history of Cyentia and Kenna, for better informed decision making. **Impact Assessment:** Leverage business impact analysis (BIA), asset exposure, and potential attack tree to provide real-time and on-demand cybersecurity risk analysis. Solutions such as cyberwire predictive analytics calculate the likelihood of a specific cyberattack and predict the type and amount of financial losses resulting from the cyberattack. **Zero-Day Prediction:** The likelihood of a vulnerability being a zero-day vulnerability can be anticipated. Machine learning, deep learning, and natural language processing were used to evaluate anomalies in the datasets. Qualys introduced a predictive analytic engine specifically designed for zero-day and Microsoft Patch Tuesday vulnerabilities to analyze the impact of such vulnerabilities.
Human analytical input	**Contextual Understanding:** The purpose is to leverage human understanding of the attack surface within the FMCG company to assess the impact on security posture. Initiatives such as Stakeholder-Specific Vulnerability Categorization (SSVC) along with context-based vulnerability risk scoring and prioritization with the help of human inputs would enhance the effort to score higher exploitable vulnerabilities. **Business Criticality:** The purpose is to distinguish between business critical and non-critical vulnerabilities. Due to its large acquisition model, the CMDB project within the FMCG company has faced numerous challenges in building a reliable source. Once trained on methodologies such as the OWASP risk rating methodology, an analyst would rate how critical a vulnerable asset is to business operations. **Ethical Concerns:** Human experts, guided by moral principles and an awareness of societal regulation and organizational values, flag vulnerabilities that could lead to ethical concerns.

Hybrid Components	**Initial Scoring:** The initial scoring phase involves the creation of an initial risk assessment using a weighted sum of AI-driven and human-provided scores, as described in the next section. **Final Prioritization:** Following the initial scoring, the results are subjected to a rigorous review and potential adjustment by a committee of cybersecurity experts. This committee includes individuals with diverse expertise in cybersecurity, business operations, and ethics and undertakes a thorough examination of the initial scores.
Feedback Loop	**Machine Learning Model Refinement:** Successful and missed outcomes are integrated into the core system, which enhances the detection algorithms. **Human Expert Review and Analysis:** The committee gathers regularly to review the latest threat intelligence, recent changes in the business environment, or emerging ethical issues that might not be fully captured by the initial AI– human hybrid score.

Table 1: Components of AI-human driving scoring in vulnerability management.

The mathematical equation that powers the new scoring system focuses on how AI-driven metrics and human input are combined to produce a comprehensive vulnerability score.

Vulnerability Score $(V) = \alpha \times$ (*Human Driven Score*) $+ \beta \times$ (*AI Driven Score*).

AI Driven Score = Exploitability Score $(E) +$ *Impact Assessment* $(I) +$ *ZeroDay Prediction* (Z).

Exploitability Score (E): A machine learning model trained on historical vulnerability data. The score ranges from 0 to 10.

$E = f(x_1, x_2,..., x_n)$ where f is the machine learning model and $x_1, x_2,..., x_n$ are features such as CVE details, attack vectors, and available patches.

Impact Assessment(I): uses a separate machine learning model to predict the potential impact of a successful exploit on business operations.

$I = g(y_1, y_2,..., y_m)$ where g is the machine learning model and $y_1, y_2,..., y_m$ are features such as asset criticality, data sensitivity, and network topology.

ZeroDay Prediction(Z): Employs a probabilistic model to estimate the likelihood of a vulnerability being zero-day.

$Z = h(z_1, z_2,..., z_p)$ where h is the probabilistic model and $z_1, z_2,..., z_p$ are features such as exploit maturity, vendor response time, and historical zero-day trends.

Human Driven Score = Contextual Understanding $(C) +$ *Business Criticality* $(B) +$ *Ethical Concerns* (Eth).

Contextual Understanding (C): Expert rating on a scale from 0 to 10 based on analysis of the specific business and environmental context.

Business Criticality (B): Also rated on a scale from 0 to 10, reflecting how crucial the asset is to business operations.

Ethical Concerns (Eth): Scored between 0 and 10 based on potential ethical implications, such as data privacy risks.

The final vulnerability score Vulnerability Score (V) is calculated as follows:

$$V = \alpha \times (C + B + Eth) + \beta \times (E + I + Z)$$

Here α and β are weights assigned to balance the contributions of the human analytical input and the AI-driven score.

By closely aligning this approach with the challenges and complexities identified in both tensions, we provide a scoring system that is not only robust but also adaptable to the evolving landscape of vulnerability management in the FMCG company context.

Contributions and Research Implications

The academic contributions of this study lie in its multi-theoretical approach, which fills several gaps in the existing literature on VM [2, 4, 7], especially within the context of big corporations such as FMCG companies. We have incorporated theories such as STS, ANT, and RBV to provide a nuanced perspective on the interplay between AI, automation, and human expertise. Drawing upon STS helps us understand how technological tools (such as AI and automation systems) and human elements (such as cybersecurity teams) must be aligned to optimize both security and efficiency. The implications of our findings that a balanced approach that enhances the capabilities of both humans and technology can lead to more effective VM strategies. ANT highlights how different cybersecurity tools and personnel within the organization interact as a network. The theory implies that the resolution of tensions must account for these interactions and dependencies to effectively predict and manage vulnerabilities. RBV underscores the importance of unique capabilities such as specialized cybersecurity expertise, automation, and AI, which, when combined, can differentiate the organization's approach to VM from its competitors.

We offer empirical solutions to the real-world challenges faced by companies in vulnerability management. The introduction of a human and AI-driven scoring system is a monumental step in automating and enhancing the vulnerability assessment process. This system offers a balanced, innovative, and accurate approach to vulnerability prioritization that goes beyond traditional methods such as CVSS by incorporating a range of metrics from machine learning models and human expertise.

Although this study provides valuable insights, its findings are derived from a single organizational context. This limitation raises questions about the generalizability of the results across different settings. One of the key areas for future research is the practical application and validation of the proposed AI-driven scoring system. While this study lays down the building blocks, theoretical consistency and empirical studies are needed to test its real-world effectiveness, scalability, and reliability to generalize the findings to other industries or even other FMCG companies with different operational structures, technological stacks, or corporate cultures.

Further research could also focus on the ethical implications of AI and automation in VM, a topic that was touched upon but not extensively covered in this study. As AI technologies become more advanced, understanding their ethical dimensions becomes increasingly crucial. In addition, this study highlights the complexities arising from multi-vendor ecosystems. Future research could explore this area through case studies of companies that have successfully managed to navigate these complexities. This could provide more concrete guidelines for organizations struggling with vendor diversification and interoperability issues.

Conclusions

Navigating the VM landscape is an ongoing challenge that is made increasingly complex by the proliferation of technological solutions and the human elements that interact with them. This study serves as a pivotal step toward understanding the synergies and tensions between human expertise, AI, and automation in achieving a robust, agile, and efficient VM. By introducing an AI-human-based scoring system and examining its complexities through a multi-theoretical lens, we have laid the groundwork for a more cohesive and adaptive approach in the field.

Although the study's findings are promising, they are initially based on data from a single large company. Recognizing this limitation, it is crucial to extend this research to include more varied organizational contexts. Doing so will not only help validate and refine the tensions but also enrich our understanding of the strategic integration of AI and automation in VM across different operational landscapes.

Disclosure of Interests

The authors declare that they have no known competing interests.

References

1. Haber MJ and B Hibbert. "The Vulnerability Management Program, in Haber 2018 emphasizes the role of vulnerability and compliance management initiatives in securing critical information and demonstrating regulatory compliance". Apress (2018): 111-118.

2. Riggs H., et al. "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure". Sensors 23.8 (2023): 4060.

3. Craigen D, N Diakun-Thibault and R Purse. "Defining cybersecurity". Technology innovation management review 4.10 (2014).

4. Syed R. "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system". Information & Management 57.6 (2020): 103334.

5. Hazar D. 2020 Vulnerability Management Survey. SANS Institute (2020).

6. Ahmadi Mehri V, P Arlos and E Casalicchio. "Automated Context-Aware Vulnerability Risk Management for Patch Prioritization". Electronics 11.21 (2022): 3580.

7. Khan S and S Parkinson. "Review into State of the Art of Vulnerability Assessment using Artificial Intelligence". Springer International Publishing (2018): 3-32.

8. Hillman DJ. "Artificial Intelligence". Human Factors: The Journal of Human Factors and Ergonomics Society 27 (1985): 21-31.

9. Sadiku MNO, O Fagbohungbe and SM Musa. "Artificial Intelligence in Cyber Security". International Journal for Research in Applied Science and Engineering Technology (2020).

10. Yoon YE, S Kim and H-J Chang. "Artificial Intelligence and Echocardiography". Journal of Cardiovascular Imaging 29.3 (2021): 193-204.

11. Gioia DA, KG Corley and AL Hamilton. "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology". Organizational research methods 16.1 (2013): 15-31.

12. Pollini A., et al. "Leveraging human factors in cybersecurity: an integrated methodological approach". Cognition, Technology & Work 24.2 (2022): 371-390.

13. van der Kleij R and R Leukfeldt. "Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security". in Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington DC, USA 10. 2020. Springer (2020).

14. Malatji M, SV Solms and AL Marnewick. "Socio-technical systems cybersecurity framework". Inf. Comput. Secur 27 (2019): 233-272.

15. Balzacq T and MD Cavelty. "A theory of actor-network for cyber-security". European Journal of International Security 1.2 (2016): 176-198.

16. Fernandez de Arroyabe JC., et al. "Cybersecurity Resilience in SMEs. A Machine Learning Approach". Journal of Computer Information Systems (2023): 1-17.

17. Yoo Y and H-S Park. "Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship". Journal of Marine Science and Engineering 9 (2021): 565.

18. Crotty J and E Daniel. "Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment". Applied Computing and Informatics (2022) (ahead-of-print).

19. Balmer DF and BF Richards. "Conducting qualitative research through time: how might theory be useful in longitudinal qualitative research?". Advances in Health Sciences Education 27.1 (2022): 277-288.

20. Aguinis H, NS Hill and JR Bailey. "Best Practices in Data Collection and Preparation: Recommendations for Reviewers, Editors, and Authors". Organizational Research Methods 24.4 (2021): 678-693.

21. Young JC., et al. "A methodological guide to using and reporting on interviews in conservation science research". Methods in Ecology and Evolution 9.1 (2018): 10-19.

22. Carter N. "The use of triangulation in qualitative research". Oncol Nurs Forum (2014): 545-7.

23. Triplett WJ. "Addressing Human Factors in Cybersecurity Leadership". J. Cybersecur. Priv 2 (2022): 573-586.

24. Webb J. "687C42Rethinking the Governance of Technology in the Digital Age". The Oxford Handbook of Cyber Security, P. Cornish, Editor. Oxford University Press (2021).

25. Dalal RS., et al. "Organizational science and cybersecurity: abundant opportunities for research at the interface". Journal of Business and Psychology 37 (2021): 1-29.

26. Direction S. "Investing in cybersecurity: Gaining a competitive advantage through cybersecurity". J. bus. strat 37 (2021): 19-21.

27. Cowley J and FL Greitzer. "Organizational Impacts to Cybersecurity Expertise Development and Maintenance". Proceedings of the Human Factors and Ergonomics Society Annual Meeting 59 (2015): 1187-1191.

28. Russell MG and NV Smorodinskaya. "Leveraging complexity for ecosystemic innovation". Technological Forecasting and Social Change (2018).

29. Ishikawa E., et al. "Modeling a Cyber Defense Business Ecosystem of Ecosystems". Handbook of Research on Cyber Crime and Information Privacy (2021).

30. Walkowski M, J Oko and S Sujecki. "Vulnerability Management Models Using a Common Vulnerability Scoring System". Applied Sciences 11.18 (2021): 8735.

31. Jung B, Y Li and T Bechor. "CAVP: A context-aware vulnerability prioritization model". Computers & Security 116 (2022): 102639.