SECURING THE MESSAGE: AI AS THE ANCHOR OF CONFLUENCE OF CYBERSECURITY AND MARKETING INNOVATION

Veljko Uskoković
Vesna Damnjanović
Katarina Milosavljević
Veljko Jeremić

https://doi.org/10.20867/cromar.29.18

Abstract
Purpose - This paper explores how AI-powered cybersecurity solutions shape B2B marketing strategies, foster marketing innovation, and enhance sales effectiveness, focusing specifically on VIAI's 8PO Blade solution. As AI rapidly evolves, cybersecurity providers must effectively communicate these technological advances to differentiate their offerings.
Methodology - Using a structured bibliometric-systematic literature review (B-SLR) and VOSviewer mapping, this study identifies three thematic clusters: AI's role in transforming B2B marketing processes, the intersection between cybersecurity and customer trust, and dynamic capability-driven AI adoption. Applying Dynamic Capabilities Theory (DCT), we analyse how Oktacron effectively sensed AI opportunities, seized them through strategic partnerships, and continuously transformed organisational processes.
Findings - The 8PO Blade case demonstrates the critical integration of technological innovation with compelling marketing narratives, targeted buyer personas, and practical sales tactics such as trial deployments. Findings indicate that dynamic capabilities facilitate the successful commercialisation of AI innovations, bridging technical advances and market demands.
Contribution - Practically, businesses are encouraged to leverage AI differentiators explicitly in marketing and sales activities. Strategically, our insights inform and encourage policymakers to support AI cybersecurity management to proactively protect digital assets, systems, and data from cyber threats. Future research should explore customer perceptions of AI in cybersecurity marketing and quantitatively assess these innovations' commercial impacts.

Keywords artificial intelligence, cybersecurity, B2B marketing, dynamic capabilities, marketing innovation, marketing strategy

INTRODUCTION

Given the need to manage complex, disruptive systems, it is hard to ignore that Artificial Intelligence (AI) is increasingly present in cybersecurity, with advanced tools now safeguarding organisations. Furthermore, AI-powered cybersecurity tools (e.g., threat detection systems using machine learning) tend to become key value propositions in B2B marketing strategies by bringing to the table both superior protection and efficiency.

Additionally, as cyber threats surge, companies increasingly promote AI-driven security on their platforms as a differentiator. In addition, recent studies indicate that AI-based cyber solutions improve threat prevention and response speeds (Rizvi, 2023; Onih et al., 2024). This improvement in security outcomes might translate into marketing advantages. Therefore, companies can build brand trust by demonstrating robust AI-driven defences, thereby enhancing customer confidence and sales effectiveness (Yanu Alif Fianto, 2023; Oloyede, 2024).

At the same time, AI's role also extends to marketing innovation. For instance, B2B marketers are adopting AI for personalised outreach, predictive analytics, and sales process automation (Chen et al., 2022). Interestingly, nearly 40% of all sales tasks could be automated through digital technologies like AI (Fischer et al., 2022). Therefore, a surging integration of AI into products and marketing processes draws particular attention to how AI-powered cybersecurity solutions shape B2B marketing strategies and sales performance. This intersection of topics, where cutting-edge cyber tools join with marketing and sales innovation, necessitates further examination. Ultimately, companies that effectively communicate their AI enabled security capabilities may gain competitive marketing advantages in the B2B economy (Mikalef et al., 2023; Zhan et al., 2024).

Expanding on the previous matter, it is noteworthy that there is a lack of holistic analysis of how AI-powered cybersecurity tools and tech solutions influence B2B marketing strategy. Also, it may be interesting to investigate how they drive marketing innovation and impact sales effectiveness in the end. Moreover, an examination of the confluence of cyber-related threats and B2B buyer expectations may provide additional research interest that gradually builds upon the main research idea. Gradually, grounded in this context, this study addresses two key research questions:

- RQ1: How do AI-powered cybersecurity tools influence B2B marketing positioning strategies and marketing innovation?
- RQ2: How do such tools impact B2B sales effectiveness, and in what ways can the dynamic capabilities framework explain organisations' technological, organisational, and market adaptation to these AI-driven solutions?

In order to adequately answer these questions, the study analyses 8PO Blade, an AI-powered cybersecurity tech-solution developed by VIAI and tested by Oktacron (as a client), as an in-depth case. The case is then situated within the broader literature, mapping how various AI-centric cyber tools are discussed in relation to B2B marketing strategy, innovation, and sales outcomes. Finally, the Dynamic Capabilities Theory (DCT) is applied to interpret how companies can effectively integrate and leverage these technologies. The following sections present (1) the 8PO Blade solution, (2) a review of relevant literature (using a structured literature review and bibliometric clustering), (3) an application of DCT, and (4) a discussion of theoretical and practical implications, policy linkages, future research, and conclusions.

1. BEST PRACTICE TECH-SOLUTION: VIAI 8PO BLADE

The 8PO Blade, developed by VIAI, stands as a best-practice example of an AI-powered cybersecurity tool. As an advanced Security Information and Event Management (SIEM) solution, it combines generative AI and machine learning to enhance threat detection and response capabilities. Notably, it analyses 100% of log data in real time, eliminating blind spots and reducing false positives. Additionally, the system continually learns from new data, enhancing its accuracy and adaptability to emerging threats. Consequently, these features serve as strong selling points, especially for organisations whose resources are limited in some manner. It follows naturally that automating routine tasks allows analysts to focus on strategic priorities, making high-end security accessible to a wide range of enterprises (Oktacron d.o.o., 2025).

Firstly, from a marketing perspective, Oktacron and VIAI have developed a well-coordinated strategy centred on the 8PO Blade. More to the point, a clear positioning statement brands it as a "virtual AI analyst for seamless cybersecurity". Additionally, its generative AI decoder, which produces human-readable reports, serves as a differentiator compared with competitors. Generally speaking, the marketing highlights its tailored AI models as a compelling value proposition that merges technical strength with business efficiency. Also, VIAI and Oktacron's go-to-market strategy targets specific B2B segments. Large banks, insurers, and telecoms are approached with a focus on ROI and risk reduction, appealing to Chief Information Security Officers (CISOs). Mid-sized companies are offered efficiency gains, while Managed Security Service Providers (MSSPs) are encouraged to integrate 8PO Blade into their services (Damnjanovic et al., 2025).

Secondly, although strong competitors dominate the market, 8PO Blade holds a distinctive position. For instance, Microsoft's Security Copilot offers AI-powered assistance, IBM's QRadar automates threat triage, and Darktrace's self-learning AI mimics an immune system. However, 8PO Blade's full log analysis and natural-language reports differentiate it from others. The case of 8PO Blade also provides additional sales and marketing lessons. On one hand, technical excellence must be translated into clear business benefits like speed, accuracy, and cost savings. On the other hand, the partnership between Oktacron and VIAI strengthens both credibility and client access. Additionally, their multi-channel sales approach combines direct engagement with partner networks to scale reach. Gradually, this approach enables them to leverage performance tracking, free trials, and targeted campaigns to refine their strategy further. Finally, 8PO Blade showcases how an AI-driven cybersecurity tool can be successfully positioned in the B2B market. In the following sections, an extensive contextualisation of the aforementioned will facilitate positioning of the matter in an academic framework (Damnjanovic et al., 2025).

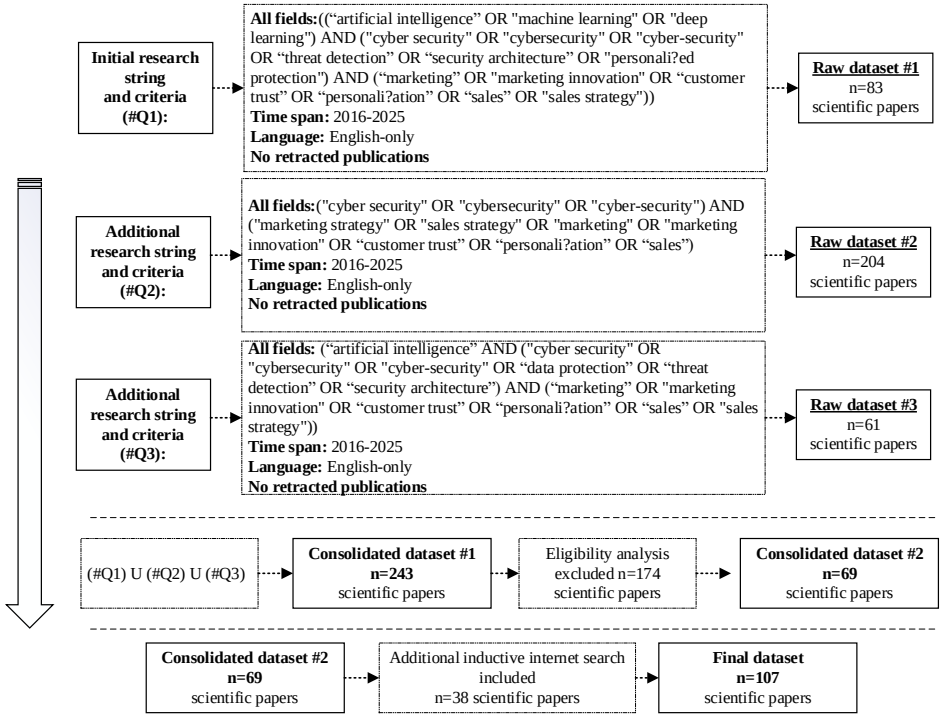
2. LITERATURE REVIEW

As noted in the introduction, research interest in AI-centred topics has surged recently. Gradually, the quantity of novel papers related to the confluence of AI and cybersecurity has followed this trend. However, there are a few papers that take this confluence into business perspective consideration. Notably, employing AI-powered tools in day-to-day B2B marketing strategies enhances customer engagement and enables data-driven decision-making (Sharma et al., 2023). Furthermore, banks tend to utilise AI for digital fraud detection, which improves user experience and general system efficiency. Therefore, AI competencies develop an impact of network effect by boosting both the domain they are attached to and also offering benefits in B2B marketing and sales (Mikalef et al., 2023). Speaking of which, AI-centred tools safeguard activities like analysing, designing and guiding customer experiences (Rustholkarhu et al., 2022). Also, they transform the B2B sales framework by enriching knowledge creation processes (Paschen, Wilson and Ferreira, 2020). However, their implementation occasionally raises socio-technical issues (Keegan et al., 2024). Accordingly, cybersecurity naturally fits well into this niche, as it fosters secure and continuous support in the communication process between the company or platform and the customer. Importantly, AI-powered cybersecurity tools like Deep Armor or Exabeam influence B2B marketing strategies by protecting against various threats (Masih, 2023), providing insights into customer behaviour. Unfortunately, due to the confluence of several distinct research areas, the body of literature regarding this topic is scarce and unstructured. Therefore, this study employs the B-SLR methodology to summarise this ambiguous confluence of topics, with the aim of scrutinising the literature from a business-oriented perspective. The underlying rationale is that too many papers examine solely technical improvements of efficacy and efficiency in safety algorithms, rather than questioning the business perspective.

Herein, an adapted B-SLR methodology is used. Although B-SLR was developed as a 10-step guide for extensive bibliometric analysis (Marzi et al., 2024), this study focuses on clustering predominant topics. Therefore, various bibliometric analyses are omitted, leaving topic clustering and a manual systematic review of selected articles as highlights. Firstly, the research idea and research questions are precisely articulated. Then it comes to database selection. Web of Science was used because it is a prominent database that indexes high-quality scientific output under rigorous selection criteria (Li et al., 2018; Birkle et al., 2020). Then, standard selection criteria narrow down the number of papers of interest. The final dataset is formed from manual eligibility checks conducted independently by all authors. Additionally, classical inductive research resulted in a cohort of papers not included in Web of Science, but because they are highly relevant, they were included in the final dataset. A detailed overview of this process is presented in Figure 1. As depicted, the final dataset comprises 107 distinct scientific papers. According to the standard bibliometric analysis procedure (van Eck and Waltman, 2010, 2017), clustering topics requires the use of functionalities of the VOSviewer software.

Precisely, the co-occurrence of keywords across selected papers underscores the complexity of examining this multidisciplinary confluence (Figure 2).

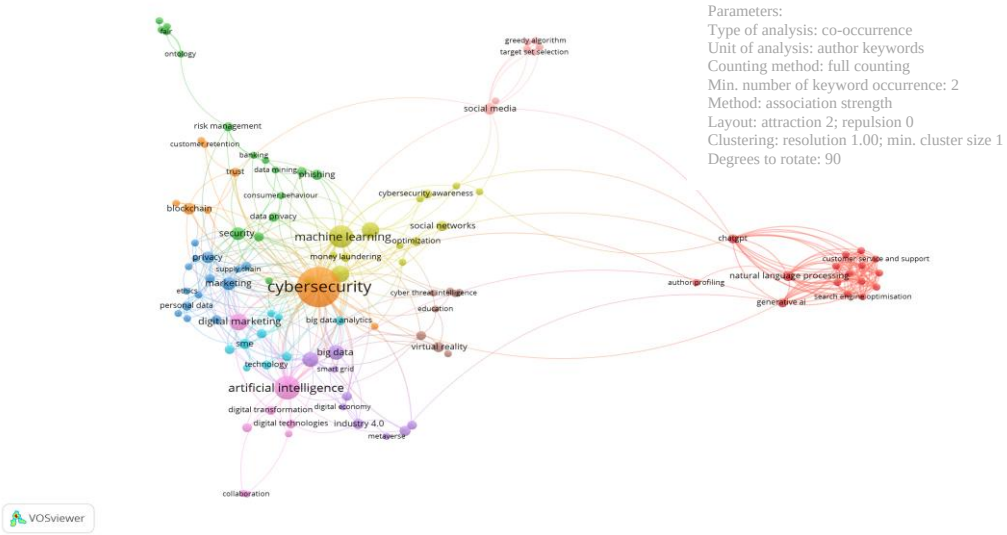
Figure 1: **Detailed overview of the data acquisition process**



Note:
Choosen scientific database: Web of Science
Data retrieved on: 10th June, 2025

Source: Authors' illustration

Figure 2: **Co-occurrence analysis of Authors' keywords in VOSviewer**



Source: Authors' illustration

Since the VOSviewer output revealed overlapping topics without forming clearly distinct clusters, a manual clustering approach was applied to ensure a more precise thematic categorisation. Manual clustering was conducted by systematically reviewing the titles, abstracts, and main findings of the identified papers and grouping them by dominant research focus. Three clusters emerged from the literature.

Firstly, Cluster 1 is labelled as “AI in B2B Marketing and Sales Processes”. It explores the impact of AI on marketing and sales. One of the papers, Fischer et al. (2022), underline that AI automates sales tasks in a way that fosters efficiency. Another study by Ravindar et al. (2022) highlights AI's strategic role in marketing and sales through predictive analytics and personalisation. Additionally, Todorova and Antonova (2023) demonstrate AI's practical applications, enhancing marketing efficacy and customer engagement. Secondly, Cluster 2 is labelled as “Cybersecurity, Trust, and Marketing Strategy”. Studies here explore the intersection of cybersecurity, trust, and marketing. For instance, Panditharathna et al. (2024) reveal that robust cybersecurity facilitates customer trust and retention. Also, Bormane and Blaus (2024) discuss risks linked to AI-driven digital marketing, emphasising the need for robust cybersecurity to safeguard customer trust. Additionally, Asmar and Tuqan (2024) show AI’s role in digital banking security, amplifying customer confidence and brand trust. However, it is important to note that while both Cluster 1 and Cluster 2 address marketing and sales outcomes, they differ in focus. Cluster 1 explores how AI directly enhances marketing and sales

processes through automation, personalisation, and sales enablement. In contrast, Cluster 2 sheds light on how AI-powered cybersecurity indirectly supports marketing by building customer trust and confidence, thereby strengthening brand reputation and customer retention. Finally, Cluster 3 is labelled as "Organisational Adaptation and AI-Driven Capability Building". This cluster focuses on organisational innovation, particularly the integration of dynamic capabilities in adopting AI. Chen et al. (2022) propose frameworks for leveraging AI in marketing automation, underlining the need for organisational agility and strategic adaptation. Additionally, Shahzadi et al. (2025) explore how personalised and gamification-based cybersecurity solutions illustrate innovative AI use, reflecting organisational capabilities in adapting emerging technologies. Moreover, Alshaikh et al. (2025) outline frameworks for standardising cybersecurity communication, demonstrating dynamic organisational capabilities in integrating AI effectively. It should be noted that in future endeavours, researchers should employ machine learning-based models to enhance this methodology, as a recent study shows a variety of possibilities this opens up (Akagić and Kadić-Maglajlić, 2024).

Building on this matter, it is essential to address where the 8PO Blade may be positioned in the literature mentioned above. The 8PO Blade solution analysed in this study primarily aligns with Cluster 2, where (AI-powered) cybersecurity enhances customer trust, strengthens brand reputation, and supports marketing and sales through trust-building mechanisms. However, to deepen the understanding of how such solutions are developed, implemented, and sustained, it is valuable to apply the perspective of Cluster 3. By introducing DCT, this study extends the analysis to the organisational and strategic processes that enable companies to notice technological opportunities, seize them through innovation and partnerships, and continuously transform their capabilities to commercialise AI-powered cybersecurity solutions successfully.

3. APPLICATION OF DYNAMIC CAPABILITIES THEORY

Dynamic Capabilities Theory, introduced by Teece et al. (1997) and further elaborated by Teece (2007), explains how companies adapt to changing environments by developing the ability to sense, seize, and transform (reconfigure) resources. The confluence of sensing, seizing, and transforming processes enables companies to identify opportunities, mobilise resources, and reconfigure operations for adaptation in complex business settings. More to the point, sensing allows companies to identify emerging opportunities or threats. Then, seizing involves mobilising resources to capture these opportunities. Finally, transforming (reconfiguring) aligns with a tendency to continuously adjust structures, processes, and capabilities to preserve competitiveness (Teece, 2007). The rationale for employing this theoretical framework may be supported by a few studies in a similar research area that have used dynamic capabilities. For instance, Kumar et al. (2024) utilise DCT to show how organisations adapt and prosper in disruptive environments, especially in the context of AI's impact on marketing

activities. Also, Liu et al. (2024) amplify the importance of existing dynamic capabilities when adopting AI-powered solutions for business model innovation. Furthermore, Tiguint and Hossari (2020) explore AI's role in first and second-order dynamic capabilities to align with strategic objectives. To conclude, the DCT framework has already established extensive interaction with the field, enabling further scrutiny of this study's research interest.

Bringing 8PO Blade to market required both technological and organisational adaptation. Oktacron recognised that AI could cut through log noise and partnered with VIAI to build full-log models that produced human-readable reports, designing the system to learn autonomously; it also retrained staff and leveraged its existing Security Operations Centre (SOC), brand, and client relationships to integrate AI across sales, support, and monitoring. Together, the partners targeted sectors such as healthcare, banking and telecoms and defined buyer personas for CISOs and SOC managers, using multi-channel marketing and free trial deployments; continuous refinement based on client feedback and close attention to evolving regulations kept the solution aligned with market needs.

A close look at the commercialisation of VIAI's 8PO Blade, a machine-learning-driven anomaly-detection tool, through the collaboration with a managed security-services provider illustrates how these capabilities unfold in practice. Firstly, the sensing capability involves identifying market gaps and clarifying buyer personas. Early in the process, the cybersecurity provider realised that the healthcare sector represented a promising but underserved market. Public hospitals, private hospital chains, and smaller laboratories were operating with vastly different levels of digital maturity and budgetary flexibility; nonetheless, all faced increasing cyber risks and regulatory pressures. The provider therefore segmented the market based on ownership type, size, level of digitalisation (such as use of electronic health records and cloud services), financial capacity, and geographic coverage; this allowed it to prioritise institutions where proactive security solutions would have the most impact.

Meanwhile, conversations with information-technology directors and managers revealed a common persona: mid-career professionals responsible for data integrity who were constrained by limited budgets, understaffed teams, and complex procurement rules. These insights highlighted that many organisations were still reactive in their security posture and unaware of the benefits of AI-enabled monitoring. By combining market segmentation with buyer persona development, the provider sensed both the opportunity for 8PO Blade and the need to position the solution not only as a technological innovation but also as a strategic investment that safeguards patient trust and operational continuity.

Secondly, the seizing capability involves designing a marketing mix around 8PO Blade. Once the opportunity was clear, the company mobilised a multi-faceted marketing strategy. A distinctive brand identity signalled reliability and professionalism; the service portfolio clearly communicated that the provider offered more than a single tool by

showcasing a 24/7 Security Operations Centre, penetration testing and vulnerability assessment, and highlighting the integration of Zero Trust principles. Building upon previous statements, educational content was crafted for different audiences; white papers, webinars, and conference presentations used concrete examples to illustrate how cyberattacks can disrupt healthcare delivery and how proactive monitoring mitigates such risks. Furthermore, a free risk-assessment programme allowed prospective clients to obtain a detailed snapshot of their cyber posture; the resulting reports prioritised remediation actions and demonstrated the added value of AI-based anomaly detection.

Consequently, the sales team could move beyond generic promises and discuss specific vulnerabilities and cost–benefit scenarios, making it easier for decision-makers to justify investment. Also, messages were tailored for various stakeholder groups. Hospital executives were reminded that data security is inseparable from patient safety. IT administrators were offered technical workshops on continuous monitoring. Clinicians received user-friendly materials emphasising good "cyber hygiene". The public was reassured that secure handling of personal data builds trust. Such customised communication illustrates marketing innovation in practice. More to the point, collaboration with VIAI allowed the provider to integrate advanced machine-learning capabilities into its offering; 8PO Blade uses pattern-recognition techniques to identify unusual network behaviour, enabling threats to be blocked before significant damage occurs. By working with an AI specialist, the provider seized the opportunity to differentiate itself in a crowded market and to align product features with the needs identified during the sensing phase. LinkedIn campaigns, direct emails and participation in industry events further personalised outreach, cultivating relationships that are essential in B2B contexts.

Thirdly, the transforming element is identified through learning, refining, and scaling. Speaking of which, the final stage involves adapting continuously based on feedback and environmental change. The provider invested in staff training so that sales and support teams could interpret AI-generated alerts and articulate their relevance to clients; such organisational learning ensured that the technology translated into actionable insights. Additionally, pilot projects in both public and private hospitals generated lessons that informed iterative refinements to the AI models. For instance, algorithms were adjusted to reduce false positives and improve dashboard clarity. Regulatory developments, like the European Union's NIS 2 directive, were closely monitored. Marketing messages were updated to emphasise compliance benefits and to reassure clients that adopting 8PO Blade would help meet audit requirements. When a major public insurer required enhanced database monitoring, the provider complemented its AI tool with additional data-security technologies and adjusted its service bundle accordingly. Overall, these transformation activities reinforced customer trust and ensured that the offering remained aligned with evolving threat landscapes and legal frameworks. Taken together, the sensing, seizing and transforming activities show how dynamic capabilities manifest in the commercialisation of AI-powered cybersecurity solutions. A market-driven

approach, grounded in segmentation, buyer persona definition, and educational outreach, enabled the provider to position 8PO Blade effectively and foster marketing innovation and sales effectiveness in a specialised B2B environment.

4. DISCUSSION

Success in commercialising AI-powered cybersecurity depends on more than technical excellence. Moreover, companies should blend dynamic capabilities with strategic marketing and sales routines. By segmenting the market and building buyer personas, educating stakeholders about the value of proactive security, offering free risk assessments and pilots, and tailoring messages to different decision-makers, providers can build trust and accelerate adoption. Collaboration with AI specialists to develop advanced tools like 8PO Blade, coupled with continuous training, algorithm refinement, and regulatory vigilance, ensures that offerings remain relevant. Finally, integrating these elements, education, experiential proof, partnerships, and adaptability, allows organisations to turn cutting-edge technology into compelling value propositions for customers and regulators. Overall, by integrating DCT with emerging insights from academic literature, several important theoretical extensions are proposed and summarised in Table 1.

Table 1*:* **Overview of theoretical contribution areas**

Contribution area	Key insights	Reference
Extension of DCT	The study demonstrates how sensing (identifying AI opportunities in cybersecurity log analysis), seizing (mobilising partnerships, expertise, and resource investments), and transforming (adapting organisational structures, continuous learning and model retraining) explain the development and commercialisation of AI-powered cybersecurity solutions in dynamic B2B contexts. This expands DCT into complex AI-driven industries.	Teece (1997; 2007)
Integration of cybersecurity trust into B2B marketing theory	The study builds on existing research by showing that AI-powered cybersecurity is not only a technological solution but also directly enhances trust, reduces perceived risk, and becomes a key factor in B2B buyers' evaluation of vendor credibility. Trust becomes central to value propositions in high-stakes sectors like healthcare, finance, telecom, and MSSPs.	Panditharathna et al. (2024); Bormane & Blaus (2024); Asmar & Tuqan (2024)
Bridging AI marketing and AI cybersecurity literature	This paper connects two previously separate literatures: AI for sales/marketing automation and AI for cybersecurity defence. It shows how companies can synchronise AI-driven security features with sales enablement narratives to create powerful B2B market positioning.	Fischer et al. (2022); Ravindar et al. (2022)
Conceptualising AI-enabled trust as a customer value driver	This study positions cybersecurity performance itself as part of market differentiation. Instead of simply communicating technical specifications, companies leverage AI cybersecurity transparency (e.g., real-time reporting, compliance, human-readable analytics) to influence buying decisions, reduce adoption anxiety, and enable long-term B2B relationships.	Chen et al. (2021); Shahzadi et al. (2025); Alshaikh et al. (2025)

Source: Authors' illustration

Beyond theoretical implications, the findings offer actionable guidance for managers seeking to develop and market AI-powered cybersecurity solutions effectively. Key managerial recommendations are synthesised in Table 2, covering strategic, operational, and commercial dimensions critical for successful implementation.

Table 2: **Overview of managerial implications**

Managerial Domain	**Managerial Guideline**
Value Communication	A cybersecurity manager who uses AI-driven tools should translate complex AI-powered technical features (log coverage, continuous learning, anomaly detection) into clear customer value narratives highlighting operational efficiency, improved regulatory compliance as business outcomes and also show how security investments protect business continuity and reduce risk.
Cross-Functional Collaboration	Companies need to ensure tight coordination between technical developers, marketing strategists, sales teams, customer support, and legal/regulatory teams to ensure consistent messaging, successful deployments, and alignment across customer touchpoints.
Customer Segmentation	Segment buyer personas in detail, addressing specific priorities of CISOs (compliance, auditability), SOC managers (operational workload, detection precision), and MSSPs (service scalability, client reporting features). Tailor messaging accordingly.
Sales Tactics	Offer trial deployments and proof-of-concept pilots that allow clients to validate system performance on their real data streams, thus lowering perceived risk and building confidence in both AI and vendor reliability.
Brand Trust	Actively showcase security certifications, compliance with regulatory frameworks (e.g. EU AI Act), third-party audits, and transparency around AI decision-making processes to strengthen corporate reputation and market credibility.
Continuous Learning	Maintain dual-loop learning: continuously retrain AI models using the latest threat intelligence while simultaneously updating sales teams with client success cases, product updates, and evolving industry pain points.
Market Positioning	Position the companies not only as a technical provider but also as a thought leader, sharing anonymised AI-generated threat insights, publishing security reports, building relevant security policy, and participating in industry forums to build long-term authority.
AI cybersecurity platform strategy	An AI-powered platform strategy that performs or assists in cybersecurity management tasks is crucial for decision-makers to gain a competitive advantage and proactively protect companies from cyber threats.

Source: Authors' illustration

To summarise for managers, success with AI-powered B2B solutions requires more than building robust technology. It entails packaging the tech into a compelling story,

delivering actual proof of value, maintaining trust, and keeping the organisation nimble to adjust strategy. Companies that achieve this can attain both innovation leadership and market success, leveraging technological capabilities to drive business performance. Given the complexity and richness of the information in the case of the 8PO Blade, it is possible to derive a few policy-related insights. More to the point, these are policy implications for facilitating the effective development and diffusion of AI-powered cybersecurity solutions. While technological innovation remains primarily driven by companies, regulatory and institutional environments play a crucial role in enabling or constraining their commercialisation pathways. Therefore, policymakers should actively promote intersectoral collaboration between technology vendors, cybersecurity companies, and industry clients, so that AI adoption might proliferate within trusted and secure governance frameworks. Additionally, transparent clarity of regulations becomes particularly salient as AI-driven decision-making introduces issues concerning accountability, transparency, and explainability. It is also noteworthy that public institutions could enhance trust by supporting independent third-party audits and transparent standards for AI model validation. That would facilitate the mitigation of concerns regarding AI opacity and bias. Moreover, workforce capacity remains a critical enabler. Therefore, governments should invest not only in developing technical AI competencies but also in fostering multidisciplinary expertise that bridges cybersecurity, marketing, sales, and regulatory compliance. Gradually, such an endeavour would support the full integration of AI-powered cybersecurity solutions into business practice.

CONCLUSION

In general, this study examined how AI-powered cybersecurity solutions influence B2B marketing, sales, and organisational adaptation. One of the best-practice solutions, 8PO Blade, was used as an illustrative case study. Regarding the previously formed research questions, a concise recapitulation is as follows. RQ1 has been answered by showing that AI-powered cybersecurity solutions not only strengthen technical protection but also serve as strategic marketing assets by enhancing customer trust, lowering perceived adoption risks, and differentiating offerings in competitive B2B markets. Also, RQ2 has been answered through the application of DCT, revealing how organisations successfully commercialise AI cybersecurity by sensing emerging opportunities, seizing them through strategic partnerships, and transforming internal processes to sustain long-term competitive advantage. However, the study's findings are subject to certain limitations. The analysis is based on English-language publications, a focused sample derived from the B-SLR approach, and a single-case examination, which may restrict broader generalisation. Future studies may build on these insights by applying comparative multi-case designs across industries, exploring sectoral differences, conducting experiments to test how AI-driven security messaging influences trust and purchase intentions, and surveying practitioners to capture their perspectives on the convergence of cybersecurity and marketing innovation. Such diverse methodological approaches

would provide empirical depth and help generalize the findings beyond the single case explored in this study.

ACKNOWLEDGEMENT

The authors gratefully acknowledge VIAI and its partner Oktacron for providing valuable insights and comprehensive information on the development, functionalities, and strategic implementation of their 8PO Blade AI-powered cybersecurity solution. Their openness and expertise greatly contributed to the depth and practical relevance of this study.

REFERENCES

Akagić, A. and Kadić-Maglajlić, S. (2024), "How can a machine learning-based LDA model help in literature search in systematic literature review?", in *How to achieve societal impact through engaged and collaborative scholarship*, Edward Elgar Publishing, Cheltenham, pp. 190-210 https://doi.org/10.4337/9781800888531.00020

Alshaikh, O., Parkinson, S. and Khan, S. (2025), "A contextual framework to standardise the communication of machine learning cyber security characteristics", *Computer Standards & Interfaces*, Vol. 94, 104015 https://doi.org/10.1016/j.csi.2025.104015

Asmar, M. and Tuqan, A. (2024), "Integrating machine learning for sustaining cybersecurity in digital banks", *Heliyon*, Vol. 10, No. 17, e37571 https://doi.org/10.1016/j.heliyon.2024.e37571

Birkle, C., Pendlebury, D.A., Schnell, J. and Adams, J. (2020), "Web of Science as a data source for research on scientific and scholarly activity", *Quantitative Science Studies*, Vol. 1, No. 1, pp. 363-376 https://doi.org/10.1162/qss_a_00018

Bormane, S. and Blaus, E. (2024), "Artificial intelligence in the context of digital marketing communication", *Frontiers in Communication*, Vol. 9, 1411226 https://doi.org/10.3389/fcomm.2024.1411226

Chen, L., Jiang, M., Jia, F. and Liu, G. (2022), "Artificial intelligence adoption in business-to-business marketing: Toward a conceptual framework", *Journal of Business & Industrial Marketing*, Vol. 37, No. 5, pp. 1025-1044 https://doi.org/10.1108/JBIM-09-2020-0448

Damnjanovic, V.et al. (2025), *Oktacron business challenge 2027: Strategic market positioning for 8PO BLADE innovative AI cyber security solution*, Business case for Belgrade Business International Case Competition 2025 [Unpublished].

Masih, J. (2023), "Enhancing employee efficiency and performance in Industry 5.0 organizations through artificial intelligence integration", *European Economic Letters*, Vol. 13, No. 4, pp. 300-315 https://doi.org/10.52783/eel.v13i4.589

van Eck, N.J. and Waltman, L. (2010), "Software survey: VOSviewer, a computer program for bibliometric mapping", *Scientometrics*, Vol. 84, No. 2, pp. 523-538 https://doi.org/10.1007/s11192-009-0146-3

van Eck, N.J. and Waltman, L. (2017), "Citation-based clustering of publications using CitNetExplorer and VOSviewer", *Scientometrics*, Vol. 111, No. 2, pp. 1053-1070 https://doi.org/10.1007/s11192-017-2300-7

Fischer, H., Puscher, D., Schöler, L. and Zinnbauer, M. (2022), "Artificial intelligence in B2B sales: Impact on the sales process", in Ahram, T., Kalra, J. and Karwowski, W. (eds.), *Artificial intelligence and social computing: AHFE 2022 International Conference*, AHFE Open Access, Vol. 28, AHFE International, USA, pp. 1-8 https://doi.org/10.54941/ahfe1001456

Keegan, B.J., Dennehy, D. and Naudé, P. (2024), "Implementing artificial intelligence in traditional B2B marketing practices: An activity theory perspective", *Information Systems Frontiers*, Vol. 26, No. 3, pp. 1025-1039 https://doi.org/10.1007/s10796-022-10294-1

Kumar, V., Ashraf, A.R. and Nadeem, W. (2024), "AI-powered marketing: What, where, and how?", *International Journal of Information Management*, Vol. 77, 102783 https://doi.org/10.1016/j.ijinfomgt.2024.102783

Li, K., Rollins, J. and Yan, E. (2018), "Web of Science use in published research and review papers 1997-2017: A selective, dynamic, cross-domain, content-based analysis", *Scientometrics*, Vol. 115, No. 1, pp. 1-20 https://doi.org/10.1007/s11192-017-2622-5

Liu, Y., Soroka, A., Han, L., Jian, J. and Tang, M. (2024), "How AI impacts companies' dynamic capabilities", *Research-Technology Management*, Vol. 67, No. 3, pp. 64-76 https://doi.org/10.1080/08956308.2024.2324407

Marzi, G., Balzano, M., Eggers, F., Kraus, S., Menon, A. and Nason, R.S. (2024), "Guidelines for bibliometric-systematic literature reviews: 10 steps to combine analysis, synthesis and theory development", *International Journal of Management Reviews* (in press) https://doi.org/10.1111/ijmr.12381

Mikalef, P., Conboy, K. and Krogstie, J. (2023), "Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective", *Journal of Business Research*, Vol. 164, 113998 https://doi.org/10.1016/j.jbusres.2023.113998

Oktacron d.o.o. (2025), *About Oktacron company*, available at: https://oktacron.rs/ (accessed 17 February 2026).

Oloyede, J. (2024), "Ethical reflections on AI for cybersecurity: Building trust", *SSRN Electronic Journal* (preprint) https://doi.org/10.2139/ssrn.4733563

Onih, V.A., Sevidzem, Y.S. and Adeniji, S. (2024), "The role of AI in enhancing threat detection and response in cybersecurity infrastructures", *International Journal of Scientific and Management Research*, Vol. 7, No. 4, pp. 64-96 https://doi.org/10.37502/IJSMR.2024.7404

Panditharathna, R., Jayasuriya, N.A., Siriwardana, A. and Perera, P. (2024), "How cyber security enhances trust and commitment to customer retention: The mediating role of robotic service quality", *Big Data and Cognitive Computing*, Vol. 8, No. 11, 165 https://doi.org/10.3390/bdcc8110165

Paschen, J., Wilson, M. and Ferreira, J.J. (2020), "Collaborative intelligence: How human and artificial intelligence create value along the B2B sales funnel", *Business Horizons*, Vol. 63, No. 3, pp. 403-414 https://doi.org/10.1016/j.bushor.2020.01.003

Ravindar, M., Srinivas, K., Rao, G.S., Rao, C.S. and Sekhar, K.C. (2022), "AI: A new strategic method for marketing and sales platforms", in *Impact of artificial intelligence on organizational transformation*, Wiley, Hoboken, NJ, pp. 183-199 https://doi.org/10.1002/9781119710301.ch12

Rizvi, M. (2023), "Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention", *International Journal of Advanced Engineering Research and Science*, Vol. 10, No. 5, pp. 55-60 https://doi.org/10.22161/ijaers.105.8

Rusthollkarhu, S., Hautamäki, P., Aarikka-Stenroos, L., Olkkonen, R. and Mahlamäki, T. (2022), "Managing B2B customer journeys in digital era: Four management activities with artificial intelligence-empowered tools", *Industrial Marketing Management*, Vol. 104, pp. 241-257 https://doi.org/10.1016/j.indmarman.2022.04.014

Shahzadi, A., Iqbal, W., Anwar, T., Khattak, H.A., Dustgeer, G. and Imran, M. (2025), "Unveiling personalized and gamification-based cybersecurity risks within financial institutions", *PeerJ Computer Science*, Vol. 11, e2598 https://doi.org/10.7717/peerj-cs.2598

Sharma, K.K., Tomar, M. and Tadimarri, A. (2023), "Unlocking sales potential: How AI revolutionizes marketing strategies", *Journal of Knowledge Learning and Science Technology*, Vol. 2, No. 2, pp. 231-250 https://doi.org/10.60087/jklst.vol2.n2.p250

Teece, D.J. (2007), "Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28, No. 13, pp. 1319-1350 https://doi.org/10.1002/smj.640

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18, No. 7, pp. 509-533 https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

Tiguint, B. and Hossari, H. (2020), "Big data analytics and artificial intelligence: A meta-dynamic capability perspective", *SSRN Electronic Journal* (preprint) https://doi.org/10.2139/ssrn.3709077

Todorova, A. and Antonova, D. (2023), "Smart marketing solutions: Applications with artificial intelligence to increase the effectiveness of marketing operations", in *2023 7th International Symposium on*

Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE, pp. 1-6 https://doi.org/10.1109/ISMSIT58785.2023.10304899

Yanu Alif Fianto, A. (2023), "Artificial intelligence and novel services: Exploring opportunities in the marketing landscape", *Journal of Applied Management and Business*, Vol. 4, No. 1, pp. 49-59 https://doi.org/10.37802/jamb.v4i1.399

Zhan, Y., Tan, K.H., Chung, L., Tseng, M.L. and Lim, M. (2024), "The impact of artificial intelligence adoption for business-to-business marketing on shareholder reaction: A social actor perspective", *International Journal of Information Management*, Vol. 76, 102768 https://doi.org/10.1016/j.ijinfomgt.2024.102768

VELJKO USKOKOVIĆ, MSc, Teaching Associate
University of Belgrade – Faculty of Organizational Sciences,
Jove Ilića 154, Belgrade, Serbia
veljko.uskokovic@fon.bg.ac.rs

VESNA DAMNJANOVIĆ, PhD, Full Professor
University of Belgrade – Faculty of Organizational Sciences,
Jove Ilića 154, Belgrade, Serbia
vesna.damnjanovic@fon.bg.ac.rs

KATARINA MILOSAVLJEVIĆ, MSc, PhD candidate
University of Belgrade – Faculty of Organizational Sciences,
Jove Ilića 154, Belgrade, Serbia
km20225005@student.fon.bg.ac.rs

VELJKO JEREMIĆ, PhD, Full Professor
University of Belgrade – Faculty of Organizational Sciences,
Jove Ilića 154, Belgrade, Serbia
veljko.jeremic@fon.bg.ac.rs