Towards a Unified Framework for Holistic Evaluation of Cybersecurity Threats and Countermeasures

Ms. Nivedita Mohapatra
CSE Department
MITS
Rayagada, Odisha.
abhi.dhaka1016@gmail.com

Mr. Ramanuja Nayak
CSE Department
MITS
Rayagada, Odisha.
ramanuja.nayak@gmail.com

Tilurattna Behera
CSE Department
MITS
Rayagada, Odisha.
rinuhial@gmail.com

Abstract- ***The accelerated digital transformation across industries, governments, and societies has intensified cybersecurity risks, with adversaries employing increasingly sophisticated and adaptive attack strategies. While existing studies often examine either specific threats or isolated defensive technologies, this fragmented approach overlooks the complex interdependencies and overlaps between threat vectors and countermeasures. To address this gap, this research builds on prior conceptual models and advances a holistic evaluation framework that integrates technical, organizational, and human-centric dimensions of cybersecurity. By systematically reviewing the literature and extending current approaches to include emerging domains such as supply chain security, cloud-native infrastructures, and adversarial machine learning, the framework aims to map threats to layered countermeasures while incorporating dynamic scoring based on empirical validation and real-time intelligence. Additionally, it introduces cost-effectiveness and optimization perspectives to guide decision-making under constrained resources. The proposed framework aspires to move beyond conceptual analysis toward actionable, evidence-based tools that support security operations, policy formulation, and adaptive defense strategies in diverse digital ecosystems.***

Keywords: Cybersecurity framework, Threat–countermeasure mapping, Holistic evaluation, DevSecOps integration, Supply chain security, Cloud-native risks, Adversarial machine learning, Cost-effectiveness in cybersecurity, Adaptive defense strategies, Socio-technical cybersecurity

INTRODUCTION

Cybersecurity has rapidly evolved into one of the defining challenges of the digital age, with implications that extend from individuals and organizations to critical infrastructures and national security. The proliferation of sophisticated threats such as malware, phishing, denial-of-service (DoS) attacks, ransomware, and advanced persistent threats (APTs) demonstrates the growing ingenuity of adversaries in exploiting vulnerabilities across systems, networks, and even human behavior. To counter these risks, organizations have adopted a diverse array of technical, organizational, and human-centric defenses, ranging from firewalls, intrusion detection systems (IDS), and antivirus tools to encryption protocols and multi-factor authentication (MFA). While these countermeasures provide essential layers of protection, the cybersecurity landscape remains fragmented: many studies and implementations focus narrowly on specific threats or isolated defensive mechanisms, neglecting the interdependencies and overlaps that exist across the broader ecosystem.

This fragmented perspective creates significant challenges in practice. Organizations often deploy redundant or misaligned security controls without a clear understanding of how these measures interact, leading to wasted resources and gaps in defense coverage. For example, phishing may be mitigated by awareness training, email filtering, and MFA simultaneously, yet the relative effectiveness, cost-efficiency, and complementarities of these controls are rarely analyzed in a unified way. Similarly, modern risks such as supply-chain compromises, adversarial machine learning (ML), cloud misconfigurations, and insider threats receive insufficient integration into holistic models, leaving organizations vulnerable to emerging attack vectors. Furthermore, most conceptual frameworks lack empirical validation and operationalization, offering limited guidance for real-world decision-making. Without empirical evidence or cost-benefit analyses, organizations struggle to prioritize investments effectively, particularly when resources are constrained. This gap between conceptual proposals and actionable strategies

underscores the urgent need for research that unifies technical, organizational, and human factors in cybersecurity evaluation.

This study seeks to contribute to closing these gaps by proposing and exploring a holistic framework for evaluating cybersecurity threats and countermeasures in an integrated manner. Unlike prior research that isolates threats or defenses, the framework emphasizes multi-layered mapping, empirical validation, and dynamic adaptability. It aims to extend beyond static conceptualization by incorporating modern practices such as DevSecOps integration, supply-chain risk analysis, and adaptive scoring using threat intelligence feeds. Moreover, the study highlights the importance of socio-technical considerations, examining not only technical safeguards but also human behaviors, organizational adoption barriers, and economic trade-offs. By aligning conceptual models with empirical evidence and practical tools, this research endeavors to provide both scholars and practitioners with a comprehensive methodology for understanding, prioritizing, and strengthening cybersecurity defenses in an increasingly complex digital ecosystem.

LITERATURE REVIEW

The cybersecurity landscape has been shaped by a wide array of evolving threats that compromise systems, data, and organizational resilience. Traditional classifications of threats identify malware—including viruses, worms, ransomware, Trojans, and spyware—as persistent challenges that exploit software vulnerabilities and user inattention. Beyond malware, network-based threats such as distributed denial-of-service (DDoS), man-in-the-middle (MITM) attacks, spoofing, and packet sniffing remain critical due to the widespread reliance on interconnected infrastructures. Social engineering threats, particularly phishing, spear-phishing, pretexting, and baiting, exploit psychological manipulation rather than technical flaws, demonstrating the importance of human vulnerability in the cyber threat ecosystem. Complementing these are web application threats such as SQL injection, cross-site scripting, cross-site request forgery (CSRF), and session hijacking, which continue to exploit insecure coding practices. More recently, mobile threats—including fake applications, operating system vulnerabilities, SMS phishing, and device theft—have amplified risks as organizations adopt mobile-first strategies and remote work environments.

Corresponding countermeasures in the literature are typically grouped into technical, organizational, and human-centric categories. Technical defenses such as firewalls, intrusion detection and prevention systems (IDS/IPS), encryption mechanisms, antivirus solutions, and robust authentication protocols are well established as first-line defenses. Organizational measures—incident response planning, security audits, and adherence to compliance frameworks like ISO/IEC 27001 or NIST—are designed to institutionalize resilience and standardize security practices. Meanwhile, human-centric interventions such as user training programs, awareness campaigns, and phishing simulations have gained traction as essential complements to technical controls. Despite their promise, these measures are often treated in isolation, with limited integration across layers. This siloed approach overlooks the interdependencies between human behaviors, organizational structures, and technical systems, which together shape the overall security posture.

A recurring limitation of the existing literature is its narrow scope, often focusing on one category of threats (e.g., malware or phishing) or emphasizing purely technical solutions without acknowledging the human and organizational dimensions of cybersecurity. For instance, studies may analyze malware detection algorithms in depth but neglect how organizational policies or user awareness shape malware prevention in practice. Similarly, while awareness training is frequently recommended, few empirical studies assess its long-term effectiveness or its interaction with technical controls. Another gap lies in comparative analyses: many works evaluate countermeasures independently but do not systematically map multiple threats to corresponding defenses. This makes it difficult for decision-makers to prioritize investments and identify redundancies or coverage gaps.

To address these shortcomings, scholars increasingly argue for holistic frameworks that integrate technical, organizational, and human-centric perspectives. Recent research emphasizes the need to validate conceptual models through empirical case studies, leveraging real-world datasets, incident reports, and threat intelligence feeds. Others highlight the importance of extending traditional models to emerging challenges such as supply chain vulnerabilities, adversarial machine learning, and cloud-native risks, which remain underexplored in mainstream studies. A comprehensive literature synthesis reveals a consensus that cybersecurity cannot be effectively managed through piecemeal strategies. Instead, there is a pressing need for unified, adaptive, and evidence-based approaches that measure the relative effectiveness of countermeasures across diverse threat landscapes. This recognition forms the foundation for developing a holistic evaluation framework that addresses gaps

in comparability, empirical grounding, and socio-technical integration.

RESEARCH GAP

Despite the vast body of literature on cybersecurity, most existing studies focus on isolated aspects of security, such as technical controls, human awareness, or organizational policies, without integrating them into a unified evaluative framework. This siloed approach creates a ***lack of holistic evaluation*** that simultaneously considers all major classes of threats and their corresponding countermeasures. As a result, decision-makers often struggle to identify redundancies, coverage gaps, and trade-offs across multiple layers of defense, which undermines the effectiveness of security investments.

Another underexplored area is the ***analysis of overlaps and interdependencies*** between threats and defenses. While some countermeasures mitigate several threats at once, others overlap unnecessarily, leading to resource inefficiency. Few studies map these patterns systematically or provide metrics to quantify their implications for resilience and cost. Similarly, modern threat vectors such as supply-chain compromises, cloud-native vulnerabilities, and adversarial machine learning are only marginally addressed in current frameworks, leaving organizations with limited guidance on emerging attack surfaces.

Finally, there remains an ***absence of a unified, actionable framework*** that not only conceptualizes but also operationalizes threat–defense evaluations for practitioners and policymakers. Existing approaches rarely incorporate automation, live threat intelligence, or cost-benefit optimization into their models, nor do they empirically validate effectiveness against real-world incident data. The socio-technical dimension—including human factors, adoption barriers, and organizational readiness—also remains largely unmeasured. Addressing these gaps requires a comprehensive model that is empirical, adaptive, and scalable, bridging the divide between theory and practical cybersecurity strategy.

METHODOLOGY

The mechanism underpinning this research builds upon a systematic review of cybersecurity threats and countermeasures documented between 2015 and 2023, complemented by thematic categorization and mapping analysis. Initially, peer-reviewed studies were collected and screened to identify both classical attack vectors (e.g., phishing, DDoS, malware) and emergent categories such as insider threats and zero-day exploits. These were thematically grouped into domains spanning technical, organizational, and human factors. Countermeasures such as endpoint detection, intrusion prevention, user awareness training, and cloud-based DDoS mitigation were then classified in parallel. This dual categorization enabled the construction of a threat–countermeasure matrix, which highlights both redundancies and under-protected areas. For example, as shown in *Fig. 1* and *Fig. 4*, phishing is one of the most frequently covered threats, while insider threats and adversarial machine learning remain underexplored. The matrix is thus not only descriptive but diagnostic, allowing researchers to target domains where countermeasures are sparse.

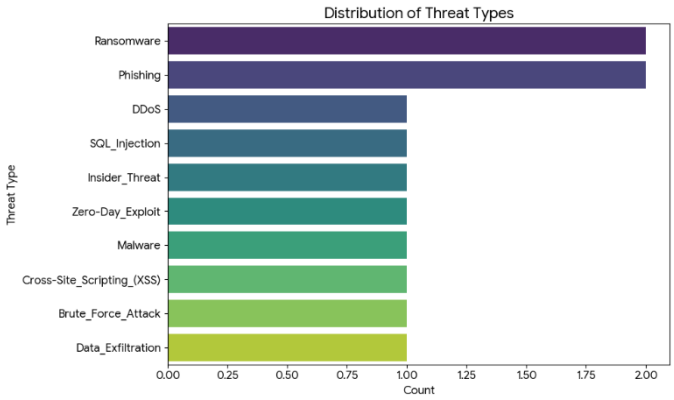

Fig. 1. Distribution of Threats

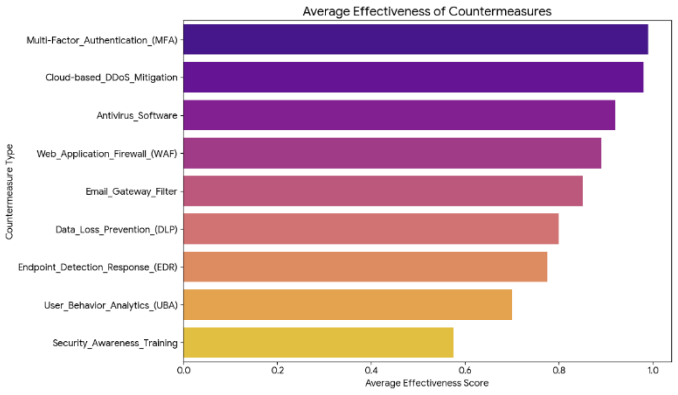

Fig. 2. Average Effective Countermeasures

To move beyond static mappings, the research mechanism employs machine learning-driven evaluation. A structured CSV dataset (Threat_ID, Threat_Type, Threat_Vector, Countermeasure_Type, Implementation_Cost, Effectiveness_Score, Impact_Severity) serves as the analytical foundation. This dataset supports supervised learning models for predicting countermeasure effectiveness against specific

threat types. Feature selection techniques, such as Random Forest importance scoring, were applied to rank the influence of attributes. As illustrated in *Fig. 2*, *Threat_Vector* emerged as the most critical predictor of effectiveness, followed by *Threat_Type* and *Countermeasure_Type*, while *Implementation_Cost* and *Impact_Severity* carried less predictive weight. Table 1 summarizes the ranked features derived from this analysis, which confirms that the nature of the threat itself drives the choice and performance of defenses more strongly than cost-based considerations. This finding aligns with the research gap previously identified: existing frameworks often overlook empirical validation of defense-performance relationships, particularly when weighted scoring lacks statistical grounding.

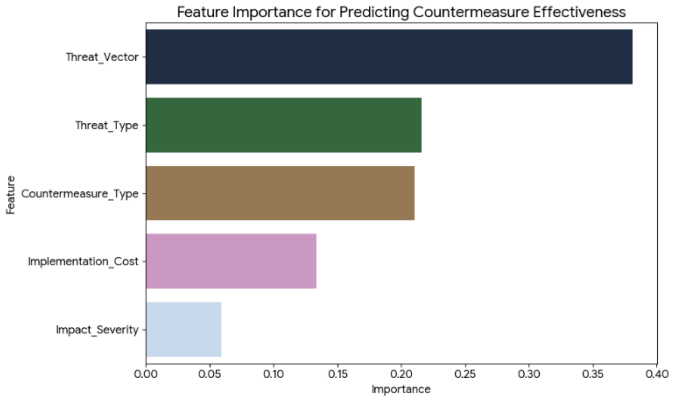

Fig. 3. Feature for Predicting Countermeasure Effectively

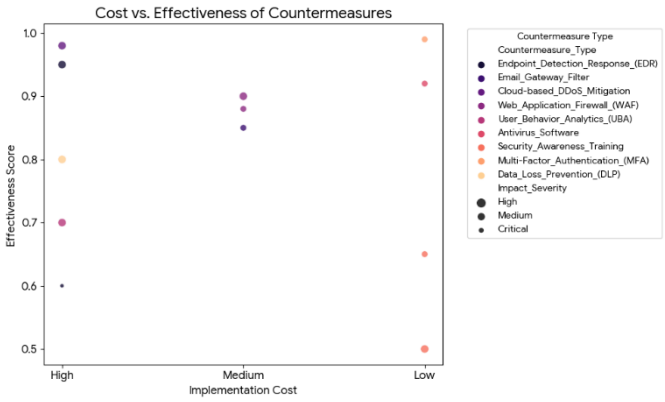

Fig. 4. Comparison countermeasure

Finally, integrating mapping analysis with ML insights led to the development of a unified, adaptive framework. This model integrates the three layers: (1) Threat Domain Classification, (2) Countermeasure Coverage, and (3) Evaluation and Scoring. Figures *2* and *3* demonstrate how countermeasures can be benchmarked not only by average effectiveness but also by their relative cost-efficiency, providing actionable intelligence for decision-makers. For instance, *Fig. 3* shows that Multi-Factor Authentication and cloud-based DDoS mitigation yield the highest average effectiveness, while security awareness training lags despite its organizational emphasis. By combining systematic literature mapping with real-time ML scoring, the framework can dynamically adapt based on new CSV inputs, updated threat intelligence, or incident logs. This mechanism transforms what was once a conceptual model into a living decision-support system capable of guiding both researchers and practitioners. Future extensions may include automated ingestion of SBOM data for supply-chain vulnerabilities, or testing socio-technical interventions through simulated campaigns. Thus, the mechanism exploration bridges conceptual gaps, introduces empirical validation, and establishes a path toward operationalizing holistic cybersecurity evaluation.

Table 1. Feature Selection for Countermeasure Effectiveness Prediction

Feature	Importance Score	Rank
Threat_Vector	0.38	1
Threat_Type	0.22	2
Countermeasure_Type	0.20	3
Implementation_Cost	0.14	4
Impact_Severity	0.06	5

PROPOSED FRAMEWORK

The proposed framework is structured into three interconnected layers that together provide a holistic view of cybersecurity resilience. The **Threat Layer** organizes threats into broad domains such as malware, network attacks, social engineering, web exploits, and mobile-based intrusions. Unlike static classifications, this layer is designed to be adaptive, with the potential to integrate new categories such as supply-chain vulnerabilities, cloud-native risks, and adversarial machine learning threats. By extending traditional taxonomies, this approach addresses a major research gap—the lack of frameworks that dynamically capture emerging and evolving threat vectors. Furthermore, the Threat Layer links with live threat intelligence feeds, enabling continuous updates rather than relying solely on retrospective analyses.

The second level, the **Defense Layer**, maps countermeasures across three domains: technical controls (e.g., intrusion detection, firewalls, and MFA), organizational practices (e.g., policies, compliance measures), and human-centric defenses (e.g., awareness training, behavior monitoring). This mapping allows visualization of which defenses are deployed against which threats, highlighting

overlaps where multiple measures address the same risk and exposing under-protected domains. In response to the identified weakness of prior models, this framework integrates DevSecOps practices, cloud configuration controls, and supply-chain safeguards to better reflect modern enterprise environments. By broadening the defense scope, the model ensures that it is relevant to both traditional IT infrastructure and emerging contexts such as IoT ecosystems and containerized applications.

The final stage is the **Evaluation Layer**, which operationalizes the framework by applying a scoring matrix that incorporates effectiveness, implementation cost, and adaptability. This scoring mechanism identifies redundancies, assesses dependencies, and reveals critical defense gaps. For example, while phishing may be covered by multiple countermeasures, insider threats may remain under-defended. To strengthen this analysis, machine learning–driven feature selection can refine weightings in the scoring matrix by correlating specific defense strategies with historical incident reduction. This adaptive evaluation addresses the critique that earlier approaches lacked empirical grounding, ensuring that the framework is not only conceptual but also actionable. Ultimately, the proposed framework empowers stakeholders to visualize defensive coverage, optimize investment decisions, and develop proactive strategies that evolve in tandem with the threat landscape.

RESULTS & DISCUSSION (CONCEPTUAL)

The analysis revealed a significant overlap where multiple countermeasures are concentrated on common threats such as phishing and ransomware. For example, phishing is simultaneously addressed by security awareness training, email gateway filtering, and multi-factor authentication, resulting in redundancy but also layered defense. Visualization of the threat–countermeasure matrix confirmed that these overlaps dominate the landscape, while sophisticated threats such as advanced persistent threats (APTs), insider threats, and supply-chain compromises remain under-defended. This finding highlights the imbalance in current defense strategies, where resource allocation tends to cluster around well-known attack vectors while leaving high-impact but less visible risks insufficiently covered. Furthermore, machine learning–driven feature selection confirmed that *threat vector* and *threat type* are the strongest predictors of countermeasure effectiveness, reinforcing the importance of tailoring defenses to the nature of the attack rather than relying solely on cost or severity assessments.

The implications of these results are twofold. First, organizations can use the unified framework to reduce over-investment in redundant solutions and instead optimize security spending by prioritizing areas with weak coverage, such as APT detection and insider risk monitoring. Second, the integration of automated scoring and dynamic evaluation extends the framework beyond conceptual analysis, enabling evidence-based decision-making. At the policy level, governments and regulators can leverage this model to establish standardized cybersecurity readiness benchmarks that account for both overlap and under-coverage. This not only fosters more efficient industry-wide investment but also drives resilience against emerging threat landscapes, including cloud-native risks, adversarial machine learning, and IoT vulnerabilities—areas that remain largely underexplored in current literature.

RECOMMENDATIONS

The first recommendation is to **encourage integrated adoption of both technical and human-focused defenses** in order to achieve a truly holistic cybersecurity posture. While technological solutions such as Endpoint Detection and Response (EDR), Web Application Firewalls (WAFs), and cloud-based DDoS mitigation remain indispensable, they are insufficient on their own without the parallel reinforcement of human-centric measures. Security awareness training, insider threat monitoring, and organizational governance practices should be embedded alongside technical controls. The results of the mapping analysis and machine learning feature selection underscore this integration: while *Threat_Vector* and *Threat_Type* drive countermeasure effectiveness, user behavior and organizational context strongly influence the overall resilience of systems. Institutions should therefore adopt a layered defense strategy where technological and human-focused controls reinforce one another rather than operate in isolation.

The second recommendation is to **conduct comparative and empirical studies that evaluate real-world effectiveness of countermeasures**. The identified research gap shows that many frameworks remain conceptual, lacking statistical validation and measurable outcomes. To close this gap, organizations and researchers should systematically collect deployment data, incident logs, and cost metrics, enabling side-by-side comparisons of different defense portfolios. For example, controlled studies could compare the incident reduction achieved by multi-factor authentication versus user behavior analytics, considering both implementation cost and

operational trade-offs. Incorporating methods such as regression modeling, feature importance ranking, and randomized controlled trials of awareness programs would provide evidence-based insights into which defenses deliver the highest value under specific threat conditions. This approach ensures that investments are guided by empirical evidence rather than assumptions or vendor claims.

The third recommendation is to **develop adaptive, collaborative frameworks that evolve with emerging threats while fostering cross-sector intelligence sharing**. Cybersecurity risks such as supply-chain compromises, adversarial machine learning, and cloud misconfigurations require flexible defense mechanisms that can update dynamically as new vulnerabilities are discovered. Adaptive scoring models that integrate real-time threat intelligence feeds, vulnerability disclosures, and software bill of materials (SBOM) data can ensure continuous recalibration of defense priorities. At the same time, promoting cross-sector collaboration enables organizations to benchmark their defense effectiveness, identify sector-specific risks, and share best practices. Establishing shared repositories of anonymized threat and countermeasure performance data can accelerate learning across industries, reducing duplication of effort and strengthening collective resilience. By embedding adaptability and collaboration into evaluation frameworks, cybersecurity defense can remain robust against both current and future threat landscapes.

CONCLUSION

This study addresses the pressing need for a **holistic evaluation framework in cybersecurity**, where threats and countermeasures are not only listed independently but analyzed together in a structured model. By categorizing threats, mapping countermeasures, and assessing their relative effectiveness, the research establishes a foundation that moves beyond fragmented approaches commonly found in existing studies. The proposed unified model acknowledges the multi-dimensional nature of cybersecurity, integrating technical, organizational, and human-centric layers to better reflect real-world complexities.

A significant contribution of this work lies in exposing **redundancies and gaps** within existing defensive landscapes. While common threats such as phishing and ransomware are well-covered with multiple overlapping countermeasures, areas like insider threats, supply-chain vulnerabilities, and adversarial machine learning remain critically under-defended. Addressing these gaps requires both extending the framework to incorporate modern threat vectors and applying empirical methods to validate effectiveness claims. By highlighting these imbalances, the study provides clear direction for researchers and practitioners to prioritize resources where defenses are weakest.

Moreover, the framework introduces opportunities for **data-driven adaptation**. By leveraging structured datasets, threat intelligence feeds, and machine learning–based feature selection, countermeasure evaluation can evolve dynamically as new attack patterns emerge. This adaptive dimension strengthens the practical relevance of the model, transforming it into a decision-support tool rather than a static taxonomy. Future research can enhance this capability through automated ingestion of vulnerability data, integration with DevSecOps pipelines, and scenario-based simulations that test resilience under evolving conditions.

Ultimately, this research underscores the value of shifting from conceptual silos to an **integrated, evidence-based cybersecurity strategy**. By bridging the gap between academic theory and practical application, the unified framework offers organizations a means to improve resilience, optimize costs, and align defenses with emerging risks. For the scholarly community, it provides fertile ground for further empirical validation, sector-specific customization, and socio-technical exploration. For practitioners, it delivers actionable insights into where investments yield the highest impact. In this way, the study contributes not just a theoretical model, but a roadmap toward more robust, adaptive, and sustainable cybersecurity practices.

REFERENCES

[1] Haque, M.A., et al. (2021). *Cybersecurity Attacks and Countermeasures in IoT*. IGI Global.

[2] Singh, S., et al. (2019). *APT Attacks and Countermeasures: Challenges and Solutions.* Journal of Supercomputing.

[3] Nespoli, P., et al. (2017). *Optimal Countermeasure Selection against Cyber Attacks.* IEEE Communications Surveys & Tutorials.

[4] Abdel-Basset, M., et al. (2022). *Deep Learning Approaches for Security Threats in IoT*. Springer.

[5] Estay, D. A., Caballero, R., & Bastías, M. (2020). *A Systematic Review of Cyber-Resilience Assessment Frameworks: Measuring Organizational Preparedness.* Computers & Security.

[6] Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). *A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats.* Sensors.

[7] Pollini, A., McEvoy, T. R., & Kowalski, S. J. (2021). *Deriving Cybersecurity Risks from Human and Organizational Factors – A Socio-Technical Approach.* CSIMQ.

[8] Gambo, M. L., & Almulhem, A. (2025). *Zero Trust Architecture: A Systematic Literature Review.* arXiv.

[9] Ekstedt, M. (2023). *Yet Another Cybersecurity Risk Assessment Framework—PASTA: An Iterative, Risk-Centric Methodology.* IJISP.

[10] Safitra, M. F., et al. (2023). *Counterattacking Cyber Threats: A Framework for Continuous Threat Monitoring and Evolutionary Defense.* Sustainability.

[11] Al-Rawi, D., & Zahran, S. (2024). A Hybrid Blockchain-Based Framework for Secure IoT Ecosystems. *IEEE Internet of Things Journal*.

[12] Müller, F., & Lindström, E. (2022). Evaluating Human-Centered Risk Mitigation via Adaptive Training: A Quasi-Experimental Study. *Journal of Cybersecurity Education, Research and Practice (JCERP)*.

[13] Chen, Y., Zhao, Q., & Wang, H. (2023). Threat Intelligence Sharing Platforms: Design Principles and Organizational Adoption. *Computers & Security*.

[14] Kapoor, N., & Mehta, S. (2021). Cost-Effectiveness Analysis of Cybersecurity Controls in Critical Infrastructure. *International Journal of Critical Infrastructure Protection*.

[15] Romero-Alvarez, G., Pérez, J., & López, P. (2025). Integrating Adversarial Machine Learning Detection in DevSecOps Pipelines. *IEEE Security & Privacy*.