The American Journal of Applied Sciences
ISSN 2689-0992 | Open Access

TYPE Original Research
PAGE NO. 55-60
DOI 10.37547/tajas/Volume07Issue11-06

Check for updates

The Concept of Red Team and Blue Team Synergy as a Factor in Enhancing an Organization's Resilience to Cyberattacks

Alina Gaifulina
Manager, Cyber Fusion Center and Incident Response at MorganFranklin Consulting Prague, Czech Republic

OPEN ACCESS

SUBMITED 15 October 2025
ACCEPTED 29 October 2025
PUBLISHED 20 November 2025
VOLUME Vol.07 Issue 11 2025

CITATION
Alina Gaifulina. (2025). The Concept of Red Team and Blue Team Synergy as a Factor in Enhancing an Organization's Resilience to Cyberattacks. The American Journal of Applied Sciences, 7(11), 55–60. https://doi.org/10.37547/tajas/Volume07Issue11-06

Abstract: The article is devoted to a theoretical and applied examination of the synergetics of interaction between offensive (Red Team) and defensive (Blue Team) units in cybersecurity. The relevance of the topic is determined by the increasing complexity and frequency of cyberattacks, which necessitates abandoning fragmented, isolated defense practices in favor of integrated, proactive strategies. The scientific novelty lies in formulating a holistic model of the cyber resilience lifecycle based on continuous cooperative interaction between teams (Purple Teaming). The study revisits the classical roles and identifies the limitations of autonomous activities of the Red Team and Blue Team, examines existing options for their integration, and provides an analytical assessment of the advantages of a synergistic approach. Special emphasis is placed on designing a continuous feedback loop between offense and defense that ensures iterative improvement of protective mechanisms. The purpose of the research is to confirm that formalized coordination of offensive and defensive team actions is a decisive factor in enhancing an organization's cyber resilience. To achieve this goal, methods of analysis and synthesis of the scientific literature, comparative analysis, and conceptual modeling are applied. Sources describing both theoretical foundations and practical frameworks for implementing Purple Teaming are examined. The conclusion formulates findings on the superiority of the integrated model and offers practical recommendations for its implementation. The material is intended for information security professionals, managers, and researchers in the field of cybersecurity.

Keywords: Red Team, Blue Team, Purple Team, cybersecurity, synergy, cyber resilience, threat emulation, proactive defense, penetration testing, incident management.

Introduction

In the era of total digitalization and continuous escalation of cyber risks, a key management task is to ensure organizations' resilience to hostile influences. Nevertheless, the classical security model, which relies on the separate operation of offensive (Red Team) and defensive (Blue Team) units, demonstrates limited effectiveness: organizational isolation generates delays in data exchange, a fragmented perception of actual risks, and, as a consequence, a reduction in the overall effectiveness of protective measures.

The relevance of the study is driven by the need to shift from a reactive pattern of cyber defense to a proactive, adaptive paradigm grounded in verified threat intelligence. The decisive mechanism of such a shift is the synergy of Red Team and Blue Team within a unified concept (often referred to as Purple Team), which provides a reproducible and measurable increase in an organization's resilience to modern attacks.

The purpose of the article is to theoretically substantiate a model of synergistic interaction between Red Team and Blue Team as a critical determinant of the growth of an organization's cyber resilience. To achieve this purpose, it is proposed to analyze the classical roles, functions, and limits of effectiveness of the isolated activities of Red Team and Blue Team based on contemporary scientific literature; to study and systematize existing practices of their integration, highlighting the Purple Team concept as the most productive form of synergy; to develop and present the author's conceptual model of the Integrated Cyber Resilience Cycle, built on the continuous, iterative coupling of actions by attacking and defending teams.

The scientific novelty lies in the formation of a holistic model that is not reduced to a mechanical combination of functions, but embeds team interaction into a closed loop of continuous improvement: from tactical exercises and tests to strategic vulnerability management and the evolution of protective means, with the results fed back into the common system of knowledge and processes.

The author's hypothesis is that the implementation of a formalized model of synergistic interaction between Red Team and Blue Team, based on the principles of continuous feedback and a joint analytical cycle, simultaneously increases the speed and accuracy of attack detection and optimizes the total security costs through more targeted reinforcement of protective mechanisms. Taken together, this ensures a qualitative increase in an organization's cyber resilience.

Materials and Methods

To prepare the study, an analysis and synthetic interpretation of current research on offensive and defensive cybersecurity, as well as on concepts of their integration, were conducted. The assembled corpus of sources provided a holistic view of the issue under investigation and enabled a rigorous substantiation of the proposed solutions.

Chindrus et al. (2023) describe a network defense case within a training-competition environment and demonstrate that performance metrics (reaction time, completeness of service restoration, quality of forensics) represent the readiness of an organization.

La Fleur et al. (2021), based on a series of regional and national competitions in the United States, demonstrate robust (generalizable) effects of training and functional specialization: resilience appears as an emergent property of the team system, shaped by repeated practice and proper role decomposition.

Venkata (2021) compares Red and Blue approaches through simulated attacks as a means of diagnosing resilience, emphasizing the necessity of closing the feedback loop between offensive emulation and defensive monitoring.

Mettu et al. (2025) proposes the Collaborative Cyber Defense framework for the Purple Team: joint scenario planning, telemetry sharing, formalized cycles of hypothesis validation, and alignment of the threat model with the detection/response model. The study interprets resilience as the managed capability of an organization to synchronize attack and detection models in a continuous cycle, complemented by regulations on the legality and operational safety of exercises.

Landauer et al. (2024) conduct a structured comparison of open adversary emulation tools, reducing methodological opacity in toolkit selection and strengthening the reproducibility of exercises; thus, results depend less on an accidental set of utilities and more on the deliberate coverage of TTP.

Yulianto et al. (2025) substantiate the integration of extended red-teaming exercises with MITRE ATT&CK: mapping techniques makes capability assessment

measurable (coverage-based assurance), shifting the focus from binary outcomes to a profile of detectability and latency across classes of techniques.

Steingartner et al. (2021) develop the cyber deception approach within a hybrid-threat model, demonstrating how traps and decoy artifacts, coupled with Blue Team observability and Red Team scenario design, increase the signal density of the environment, disorganize the adversary, and enhance the training effect for defenders and exercise designers.

Chen et al. (2021) demonstrate dynamic planning on graphs using a Gated Graph Neural Network; the analogy is transferred to the optimization of sensor/decoy placement and to the modeling of attack/detection paths in networks as graph processes.

Al-Okaily et al. (2021) propose a managerial model of innovation orientation; when applied to Purple-cycle initiatives, it highlights the role of moderators (risk culture, leadership, incentives) in translating exercise lessons into sustained changes in the SOC.

Schöbel et al. (2024) formulate a research agenda on conversational agents; in the context of the Blue Team this is relevant to the design of dialog assistants for the SOC and the automation of collaborative analytics in Purple cycles.

In summary, the studies are highly diverse; however, implementation cases that demonstrate a measurable improvement of MTTR/MTTD and the risk profile due to GNN/agents/managerial moderators are insufficiently explored.

As for research methods, the following were applied:

Critical analysis and synthetic processing of scientific publications to construct the theoretical foundation.

A comparative-analytical approach to contrast traditional (isolated) and synergetic approaches.

The method of conceptual modeling to develop the authors model Integrated Cycle of Cyber Resilience.

Results

A current review of scientific publications and industry practices demonstrates the key dimensions of synergy between the Red Team and the Blue Team. The traditional paradigm of separating the work of these groups reveals systemic limitations. The Red Team, which simulates an adversary, and the Blue Team, responsible for defense, have historically operated in relative isolation, resulting in a fragmented perception of threats and slower incident response. The resulting communication deficit creates blind spots in defense: the Red Team uncovers vulnerabilities that the Blue Team may misinterpret or underprioritize; simultaneously, the Blue Team expends resources on attack vectors of low relevance.

The essence of the synergistic approach lies in the need to shift from a logic of opposition to a model of collaboration. This transforms into a Purple Team, which can exist as a formally established unit or as a virtual coordination linkage. An important mechanism of synergy is a continuous feedback loop in which Red Team actions are jointly analyzed with the Blue Team to accelerate the improvement of detection and response processes. This mode enables near real-time adaptation: rapid retuning of SIEM use cases, refinement of correlation rules, adjustment of EDR signals, and other control mechanisms (Chindrus et al., 2023; Steingartner et al., 2021).

The effectiveness of synergy is closely aligned with the principles of threat-informed defense. Instead of generalized pentests, the Red Team reproduces tactics, techniques, and procedures (TTPs) of specific adversaries relevant to the industry and organizational context. These TTPs are generally mapped to the attack matrix and serve as the methodological framework for joint exercises. For the Blue Team this creates an opportunity to test and tune defenses against realistic rather than hypothetical scenarios. As highlighted by leading cybersecurity news, including The Hacker News, attacks are becoming increasingly targeted, which elevates the critical importance of emulating specific APT groups.

Assessing the success of such an integrated approach requires a well-considered set of metrics. Effectiveness is measured not only by the number of identified vulnerabilities but also by time to detection, time to response, and the increased coverage of techniques from the attack matrix by monitoring and protection tools. Unlike a static Red Team report that captures the state at the time of testing, joint exercises generate a dynamic data array that makes it possible to track the trajectory of increasing cyber resilience over time (Chen et al., 2021; Yulianto et al., 2025).

A key challenge is the cultural transformation from a competitiveness mindset to a partnership model (Purple Teaming). This requires explicit executive sponsorship, the development of shared goals and KPIs for both teams, and the institutionalization of regular forms of interaction (weekly syncs, joint workshops).

Taken together, the presented analysis confirms that the synergy of the Red Team and the Blue Team is an evolutionary shift in cybersecurity practices. It moves the practice from episodic assessments to continuous, data-driven improvement of the defensive perimeter based on realistic scenarios and close cooperation among domain specialists.

Discussion

The conducted analysis leads to the requirement to create a holistic, formally specified model that systematizes and makes reproducible the synergistic interaction of the teams. Common approaches still interpret Purple Teaming as an episodic practice or as a set of informal coordinations. Meanwhile, for real gains in efficiency and the strengthening of cyber resilience, it must function as a continuous process embedded in the organization's end-to-end information security strategy.

Drawing on the materials studied, a conceptual model of an integrated cyber resilience cycle is formulated. The model defines an iterative loop in which the output of each step becomes the input of the next, forming a self-learning and self-improving defense system.

In contrast to the traditional linear scheme, where the Red Team is limited to delivering a report to the Blue Team, the proposed cycle is closed and operates as a continuous feedback loop (Fig. 1).

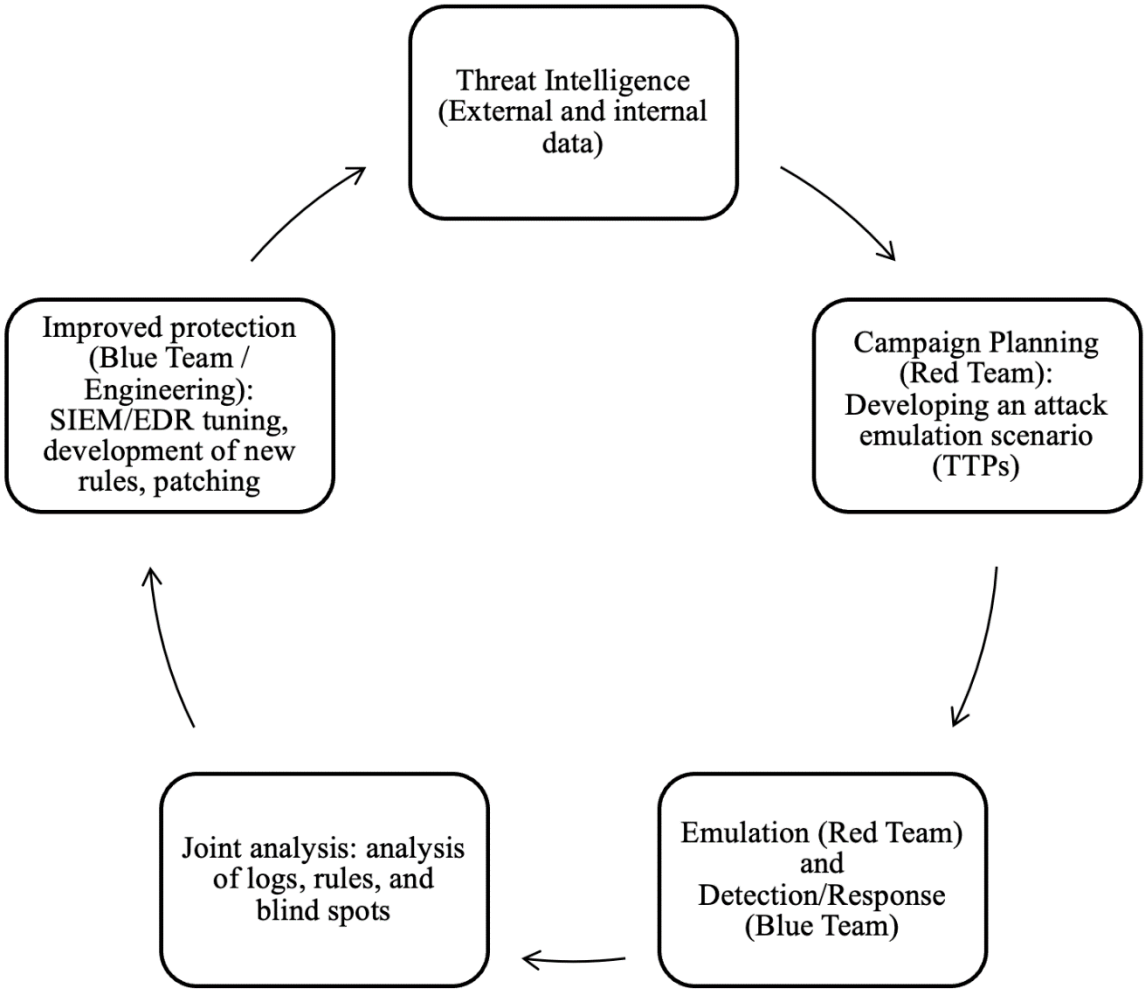

Fig.1. The author's model of the "Integrated cycle of cyber resilience" (Mettu et al., 2025; Venkata, 2021; La Fleur et al., 2021)

The conceptual scheme of the Integrated Cyber Resilience Cycle depicted in Figure 1 is structured as a sequence of interrelated, methodologically grounded stages, each of which functionally feeds the next and thereby ensures the integrity and reproducibility of the process.

The optimal form for presenting the advantages of this cyclical approach is their representation in comparative Table 1.

Table 1. Comparison of approaches to organizing cyber defense (Venkata, 2021; La Fleur et al., 2021)

Parameter	Traditional (isolated) approach	Integrated (synergistic) approach
Feedback speed	Low (weeks, months)	High (hours, days)
Realism of exercises	Medium (generic tests)	High (emulation of relevant TTPs)
Effectiveness of improvements	Low (changes based on a report)	High (targeted tuning based on joint analysis)
Personnel development	Isolated, within one's function	Comprehensive, mutual learning of offensive and defensive techniques
ATT&CK technique coverage	Fragmentary, random	Systematic, measurable
Total cost	High (due to inefficient use of resources)	Optimized (resources allocated to eliminating real gaps)

The practical implementation of the proposed model presupposes the prior operationalization of objectives through formalized and unambiguously interpretable performance indicators (KPI) (Table 2).

Table 2. Key Performance Indicators (KPI) for the Integrated Cyber Resilience Cycle (Landauer et al., 2024; Al-Okaily et al., 2021; Schöbel et al., 2024)

Cycle phase	Key Performance Indicator (KPI)	Measurement method
Emulation and Response	Mean Time To Detect (MTTD)	Measurement of the time lag between a Red Team action and a Blue Team alert
Emulation and Response	Mean Time To Respond (MTTR)	Measurement of the time from alert to full containment of the threat
Joint Analysis	Number of identified blind spots in monitoring	Count of Red Team actions that did not generate alerts
Defense Improvement	Percentage coverage of MITRE ATT&CK techniques	Analysis of the ATT&CK map before and after the improvement cycle
Entire Cycle	Reduction of MTTD and MTTR in subsequent iterations	Comparative analysis of KPIs across cycles (quarter over quarter)

The presented concept of the Integrated Cyber Resilience Cycle is interpreted not as a mere coordination of functions but as the formation of a new quality—self-learning defensive architecture. It shifts security practices from a static, post hoc–oriented paradigm to a dynamic and proactive one, commensurate with the current cyberthreat profile. Its implementation, grounded in clearly defined KPIs, ensures a significant increase in the organization's level of cyber resilience

Conclusion

The study achieved the stated objective: the model of synergistic interaction between the Red Team and the Blue Team has been theoretically substantiated and conceptually articulated as a determining driver for enhancing the organization's cyber resilience. To achieve this result, all research tasks were addressed sequentially.

First, a critical reflection was conducted on the classical roles and the limitations of isolated team functioning. It was demonstrated that the traditional cooperation format suffers from delayed feedback, a fragmented perception of the threat landscape, and, as a consequence, inefficient allocation of defensive resources.

Next, existing integration practices were systematized, and as a result the concept of Purple Teaming was identified as the most productive form of purposeful synergy. It was established that its foundation is a continuous feedback loop and a joint interpretation of the actions of the attacking and defending sides. Based on the conducted analysis, a conceptual construct of the integrated cyber resilience cycle is proposed. The framework transforms interaction from a mode of disparate episodes into a continuous iterative process: from threat analysis to planning and emulation, then to joint analysis of results and the sequential strengthening of defensive mechanisms. Such a cycle enables the organization to systematically and purposefully increase its ability to counter cyberattacks.

Thus, the research hypothesis received empirical and theoretical confirmation. The formalized synergistic model not only increases the speed and accuracy of attack detection (through the reduction of MTTD and MTTR) but also optimizes the security budget by prioritizing improvements based on practice-validated data. Taken together, this provides a qualitative increase in overall cyber resilience, making the organization ready to repel both known and new attack vectors that have not yet been typologized.

References

1. Chen, J., Li, K., Li, K., Yu, P. S., & Zeng, Z. (2021). Dynamic planning of bicycle stations in dockless public bicycle-sharing system using gated graph neural network. ACM Transactions on Intelligent Systems and Technology (TIST), 12(2), 1-22. https://doi.org/10.1145/3446342.
2. Mettu, B. P. R. (2025). Collaborative Cyber Defense: A Framework for Purple Team Integration in Countering Sophisticated Adversaries. Journal of Computer Science and Technology Studies, 7(5), 1013-1020. https://doi.org/10.32996/jcsts.2025.7.5.117
3. Venkata, B. (2021). Red Team vs. Blue Team: Assessing Cybersecurity Resilience Through Simulated Attacks, 8 (4), 82-87.
4. Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587
5. Al-Okaily, M., Al Natour, A. R., Shishan, F., Al-Dmour, A., Alghazzawi, R., & Alsharairi, M. (2021). Sustainable FinTech Innovation Orientation: A Moderated Model. Sustainability, 13(24), 13591. https://doi.org/10.3390/su132413591
6. Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. Cyber Security and Applications, 3, 100077. https://doi.org/10.1016/j.csa.2024.100077
7. Schöbel, S., Schmitt, A., Benner, D., Saqr, M., Janson, A., & Leimeister, J. M. (2024). Charting the evolution and future of conversational agents: A research agenda along five waves and new frontiers. Information Systems Frontiers, 26(2), 729-754.
8. La Fleur, C., Hoffman, B., Gibson, C. B., & Buchler, N. (2021). Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. Computers & Security, 104, 102229.https://doi.org/10.1016/j.cose.2021.102229.
9. Landauer, M., Mayer, K., Skopik, F., Wurzenberger, M., & Kern, M. (2024, December). Red team redemption: A structured comparison of open-source tools for adversary emulation. In 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 117-128). IEEE. https://doi.org/10.1109/TrustCom63139.2024.00043.
10. Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597. https://doi.org/10.3390/sym13040597