INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 1, PP. 1-6
Manuscript received January 16, 2026; revised January, 2026. doi: 10.24425/ijet.2026.157878

Cyber Soldier project - A threat-led methodology for assessing the Digital Resilience of cybersecurity systems

Mariusz Stawowski, Adam Sobczyk, Mateusz Gajda, Tomasz Wojtas, Tomasz Pająk, Krzysztof Siwy, and Grzegorz Blinowski

***Abstract*—We present Cyber Soldier Methodology and tool set that introduces a threat-led methodology for assessing the digital resilience of cybersecurity systems within organizations required to comply with European regulatory frameworks such as the Digital Operational Resilience Act (DORA). Unlike traditional vulnerability assessments or penetration testing, this methodology focuses on reproducing the tactics, techniques, and procedures (TTPs) of real adversaries to evaluate the effectiveness of cybersecurity controls and operational resilience mechanisms in production environments.**

The proposed methodology integrates threat intelligence, red team scenario design, and detection performance analysis into a unified process aimed at measuring the organization's preparedness for sophisticated cyber threats.

We demonstrate how the presented framework bridges the gap between strategic compliance requirements under DORA and the operational practice of resilience testing. We also provide some initial data the application of Cyber Soldier toolset in real-world environments.

***Keywords*—cybersecurity; threat intelligence; digital resilience**

I. Introduction

MODERN regulatory frameworks such as DORA [1] mandate financial and critical-sector organizations to assess their digital operational resilience through practical, intelligence-led testing. This requirement is operationalized via Threat-Led Penetration Testing (TLPT) as defined in the European Central Bank's TIBER-EU Framework [2]. TLPT seeks to verify how effectively an organization's defenses withstand realistic cyberattacks that replicate genuine threat actors' TTPs.

While TIBER-EU, DORA and the related Regulatory Technical Standards (RTS) [3] provide process-level guidance, they do not prescribe a standardized methodology for conducting ongoing, repeatable assessments of cybersecurity system resilience between TLPT cycles.

Existing security testing methodologies - such as the OWASP Testing Guides [4], Penetration Testing Execution Standard (PTES) [5], PCI DSS Penetration Testing Guidance [6], and the Open Source Security Testing Methodology Manual (OSSTMM) [7] - focus primarily on identifying vulnerabilities and validating their exploitability under controlled technical conditions. Their principal objective is to measure the exposure of information systems to known weaknesses, rather than to assess the overall resilience of cybersecurity controls and operational processes.

While these methodologies have become industry benchmarks for structured penetration testing, they exhibit several limitations in the context of modern threat-led resilience assessment:

Absence of Threat Intelligence Context - Traditional methodologies focus on system level vulnerabilities but rarely incorporate cyber threat intelligence (CTI) describing how actual adversaries operate. They typically lack structured mechanisms to map test activities to real-world threat actors, TTPs, or current attack campaigns.

Limited Evaluation of Cybersecurity System Effectiveness - Standards such as OWASP WSTG, MSTG, and PCI DSS Penetration Testing Guidance are oriented toward verifying the presence of vulnerabilities or misconfigurations. They do not provide a framework for assessing the effectiveness of defensive systems or the organization's ability to detect and respond to attacks in real time.

No Educational or Capability-Building Component - Existing methodologies generally treat testing as a one-time audit process, not as an educational or developmental activity. They do not emphasize the role of human analysts, their decision-making during incidents, or learning from simulated attacks.

By contrast, the Threat-Led Digital Resilience Assessment Methodology introduced in the Cyber Soldier Project integrates threat intelligence, detection analytics, and human factors into a unified testing process. It emphasizes realistic adversary emulation, measurement of detection effectiveness, and continuous improvement through education.

The TIBER-EU Framework, adopted by the European Central Bank, defines the structure of Threat-Led Penetration

This work was supported by CLICO Sp. Z o.o.

Mariusz Stawowski is with Faculty of Cybernetics, Military University of Technology, Poland and with CLICO Sp. z o.o., Kraków, Poland (e-mail: mariusz.stawowski@clico.pl, ORCID: 0009-0006-5673-6481); Adam Sobczyk, Mateusz Gajda, Tomasz Wojtas, Tomasz Pająk, Krzysztof Siwy are with CLICO Sp. z o.o. (e-mail: adam.sobaczyk@clico.pl, mateusz.gajda@clico.pl, tomasz.wojtas@clico.pl, tomasz.pajak@clico.pl, Krzysztof.siwy@clico.pl); Grzegorz Blinowski is with Institute of Computer Science, Warsaw University of Technology, Warszawa, Poland (e-mail grzegorz.blinowski@pw.edu.pl, ORCID: 0000-0002-0869-2828)

Testing (TLPT). However, TIBER-EU testing is not continuous; it is performed periodically, typically once every three years. Between TLPT cycles, organizations lack a standardized mechanism to maintain or measure resilience improvements. The Cyber Soldier Methodology fills this gap by introducing a continuous, repeatable framework for resilience assessment.

II. Framework of the Cyber Soldier Methodology

The TIBER-EU Framework, adopted by the European Central Bank, defines the structure of Threat-Led Penetration Testing (TLPT). However, TIBER-EU testing is not continuous; it is performed periodically, typically once every three years. Between TLPT cycles, organizations lack a standardized mechanism to maintain or measure resilience improvements. The Cyber Soldier Methodology fills this gap by introducing a continuous, repeatable framework for resilience assessment. Cyber Soldier Project proposes a structured, threat-led methodology that integrates both the offensive (red team) and defensive (blue/purple team) perspectives into a cohesive testing cycle:

- controlled execution of threat scenarios within production environments,
- rigorous use of threat intelligence to ensure realism and regulatory alignment,
- integration with Cyber Range environments for pre-validation,
- measurement of detection coverage via a standardized observability matrix.

The proposed threat-led methodology is designed as a systematic framework for assessing the digital resilience of cybersecurity systems. It draws upon principles defined in DORA, the TIBER-EU Framework, and the Regulatory Technical Standards (RTS) on threat-led penetration testing, while extending them into a repeatable and measurable process suitable for continuous improvement of cyber defense capabilities.

The methodology assumes that digital resilience can be quantified and improved through the cyclical execution of structured threat scenarios derived from current cyber threat intelligence (CTI).

A. Objectives

The primary objective of the framework is to create a repeatable, threat-intelligence-driven process that allows organizations to:

- measure the effectiveness of defensive controls,
- evaluate detection and observability coverage across attack phases,
- identify configuration gaps and procedural weaknesses,
- train personnel through interactive, realistic exercises, and
- support compliance with DORA's requirements for operational resilience testing.

This approach transforms threat-led penetration testing from a periodic compliance obligation into a continuous resilience management process, allowing organizations to perform internal assessments between formal TLPT cycles.

B. Conceptual Structure

The methodology is organized into four interlinked layers:

- Threat Intelligence Layer - defines adversary models, TTPs, and contextual intelligence sources that drive scenario generation.
- Scenario Design and Validation Layer - transforms threat intelligence into structured red team scenarios and validates them in a controlled Cyber Range environment.
- Execution and Observation Layer - delivers controlled execution of threat scenarios in production environments and collects observability data from defensive tools.
- Assessment and Learning Layer - evaluates detection effectiveness using the Detection and Observability Assessment Matrix, consolidates lessons learned, and supports capability improvement.

The Cyber Soldier Project serves as the implementation environment of this methodology. Its modules - Cyber Soldier Breach and Attack Simulation (BAS) [8, 9], Threat Intelligence Assistant, Cyber Range, and the Detection and Observability Assessment Matrix - correspond to the layers above, transforming theoretical assumptions into operational practice.

C. Principles of Methodology

The framework is founded upon several methodological principles:

- Threat-Led Orientation - all test actions are derived from verified cyber threat intelligence and reflect real adversary TTPs.
- Controlled Execution - all tests are conducted ethically, within approved scopes, and with full organizational consent to ensure production safety.
- Detection-Centric Assessment - evaluation focuses not only on successful exploitation but primarily on the ability of the cybersecurity system to detect and log adversarial activities.
- Educational and Analytical Value - each test contributes to staff skill development, knowledge transfer, and improvement of detection engineering practices.
- Reproducibility and Transparency - every scenario is documented, including tools used, configuration parameters, and expected detection events, to ensure auditability and repeatability.

III. Methodology Stages

The threat-led digital resilience assessment methodology proposed under the Cyber Soldier Project is structured into five sequential stages, each reflecting a distinct analytical and operational dimension of resilience testing. These stages ensure that the assessment remains threat-driven, controlled, measurable, and repeatable.

A. Stage 1 - Threat Intelligence Analysis and Adversary Profiling

The assessment begins with the identification of relevant threat actors based on sectoral and geopolitical context. The analysis combines:

- current reports from cyber threat intelligence (CTI) providers,

- frameworks such as MITRE ATT&CK [10] for mapping adversary TTPs, and
- open source and commercial intelligence sources.

Each adversary profile includes known attack techniques, preferred initial access vectors, infrastructure usage, and operational goals (e.g., data theft, financial gain, disruption). This ensures that testing activities are contextually relevant to the organization's real-world exposure.

The Threat Intelligence Assistant within the Cyber Soldier Project automates this step by aggregating MITRE ATT&CK-based data and generating structured adversary profiles that serve as the foundation for subsequent scenario design.

B. Stage 2 - Threat Scenario Design and Validation

The second stage translates adversary intelligence into a technical red-team scenario. Each scenario is built around a sequence of attack paths - ordered sets of techniques emulating the behavior of the selected threat actor. The design phase includes mapping relevant MITRE ATT&CK techniques to attack paths and threat scenarios and selecting and documenting legal and validated tools permitted for ethical testing (e.g., netexec, nanodump[11], impacket[12]). Each step of an attack path is executed using a legal tool. A single step may encompass one or more cyberattack techniques as defined in MITRE ATT&CK. In some cases, techniques used in a single step may fall under different tactics within this matrix. The steps and the tools applied define the procedure for executing the given attack path – see Figure 1.

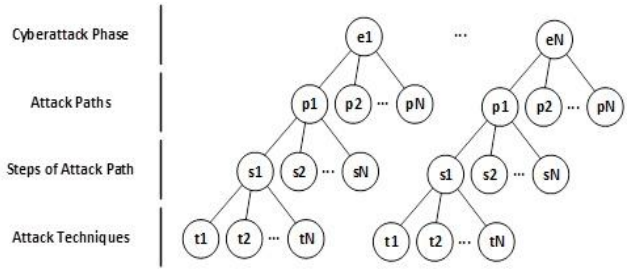

Fig. 1. Threat scenario model.

Before execution in production systems, each scenario must undergo pre-validation in a Cyber Range environment that mirrors typical enterprise infrastructure (e.g., Windows Active Directory, databases, mail and web servers).

C. Stage 3 - Controlled Execution in Production Environment

In this stage, the validated scenario is executed within the organization's live systems under controlled conditions. Unlike traditional vulnerability scanning, the objective is not only to discover weaknesses but also to evaluate how effectively the cybersecurity system detects and responds to realistic adversarial activity.

The execution follows a phased approach reflecting the cyberattack lifecycle (e.g., reconnaissance, lateral movement, privilege escalation, and critical asset compromise). Each attack phase is monitored through integrated defensive solutions to collect telemetry and alert data.

To ensure safety and continuity, the testing team may use the "assume breach" principle, in which initial access is granted at a predefined level, enabling the execution of every planned attack path. This aligns with DORA's concept of a "leg-up" during TLPT exercises.

D. Stage 4 - Detection and Observability Assessment

The fourth stage focuses on evaluation of detection and monitoring capabilities. For this purpose, the Cyber Soldier Project employs the Detection and Observability Assessment Matrix, a structured framework that correlates attack techniques with expected defensive responses.

In the Cyber Soldier Project, the Detection and Observability Assessment Matrix was developed based on research conducted in the Cyber Range environment, where selected cybersecurity solutions were installed - solutions recognizable on the international market and featured in Gartner Magic Quadrant reports [13, 14, 15]. The research was carried out by experts specializing in specific cybersecurity solutions using the Cyber Soldier BAS application, which executed all attack paths. The cybersecurity solutions included in the study were:

- EDR & XDR (Endpoint Detection and Response & Extended Detection and Response) - systems monitoring activity on endpoints and servers to detect and respond to threats, with XDR additionally integrating data from multiple sources (e.g., network, email, cloud),
- NDR (Network Detection and Response) - systems monitoring network traffic to identify threats, detect anomalies, and analyze suspicious network activities,
- IPS & NGFW (Intrusion Prevention System & Next-Generation Firewall) - systems preventing intrusions and blocking unauthorized traffic, with NGFW combining IPS functionality with advanced filtering and application control mechanisms.

For better understanding and structuring of the test plan, the threat scenario was divided into phases. To define these phases, the Cyber Kill Chain model [16] and tactics from the MITRE ATT&CK matrix were applied, though adapted to the specifics of real-world red team tests conducted in organizational production environments.

By comparing the observed detection levels with the baseline matrix, analysts can identify configuration gaps, misalignments between tools, or insufficient telemetry integration. This provides a data-driven foundation for strengthening the detection posture.

E. Stage 5 – Lessons Learned and Continuous Improvement

The final stage consolidates the technical and procedural findings into actionable outcomes. Results from the observability matrix and incident timelines are reviewed jointly by red, blue, and purple teams. The objectives are to:

- validate alert logic,
- update threat-detection tools,
- refine procedures for incident response, and
- prioritize remediation of identified weaknesses.

The educational dimension of this stage is equally important. Through interactive execution and subsequent analysis, cybersecurity personnel enhance their situational awareness, analytical skills, and familiarity with adversary tactics - key components of a mature cyber-resilience culture.

IV. SUPPORTING IMPLEMENTATION TOOLS

Although the proposed threat-led methodology is designed to be tool-agnostic, its implementation within the Cyber Soldier Project provides a concrete technological foundation for conducting, automating, and analyzing threat-led digital resilience assessments. The supporting tools ensure methodological consistency, repeatability, and safe testing in both simulated and production environments. Figure 2 presents the overall system architecture linking each component with its corresponding stage in the methodology.

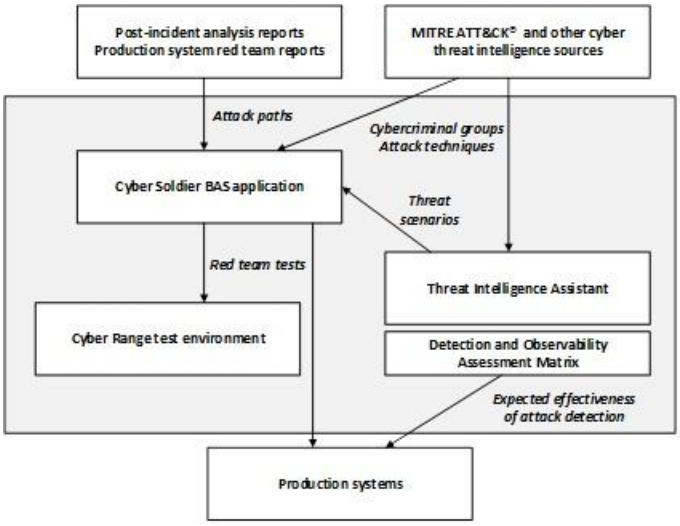

Fig. 2. Architecture of the Cyber Soldier implementation of the threat-led methodology – linking tools to specific stages of the process.

A. Cyber Soldier BAS – Breach and Attack Simulation Platform

The Cyber Soldier BAS (Breach and Attack Simulation) platform implements the Execution and Observation Layer of the methodology. It enables structured and interactive execution of attack paths corresponding to the selected threat scenario.

Key characteristics include:

- Educational interactivity - users can execute step-by-step attack paths with contextual explanations of TTPs, reinforcing understanding of adversary behavior.
- Dual-mode testing - the platform can operate in both the Cyber Range and production environments, allowing safe validation before real-world deployment.
- Legal tooling ecosystem - integrates open-source and commercial tools used in ethical red teaming, ensuring transparency and reproducibility.

B. Threat Intelligence Assistant – Automated Scenario Generation

The Threat Intelligence Assistant module supports Stage 1 (Threat Intelligence Analysis) and Stage 2 (Scenario Design) by automatically generating tailored red team scenarios. Main functionalities include:

- Adversary selection based on threat intelligence sources [17, 18, 19, 20],
- Technique mapping - identifying MITRE ATT&CK techniques used by that actor,
- Scenario composition - selecting validated attack paths from Cyber Soldier BAS that match those techniques,
- Phase alignment - arranging the selected paths into cyberattack phases.

This module automates what traditionally requires manual analysis by red team planners, significantly improving the speed and precision of threat scenario creation while maintaining methodological consistency.

C. Cyber Range – Controlled Validation Environment

The Cyber Range allows researchers and defenders to evaluate the impact and detectability of attack techniques without operational risk. It also provides a foundation for training and capability development, serving as a practical laboratory for purple team collaboration and DORA-aligned resilience validation. The Cyber Range consists of:

- Windows Active Directory domains with typical configurations and misconfigurations,
- database, mail, and web servers,
- integrated defensive technologies such as EDR/XDR, NDR, IPS/NGFW, and SIEM solutions,
- optional simulation of hybrid or cloud environments.

D. Detection and Observability Assessment Matrix

The Detection and Observability Assessment Matrix is a cornerstone analytical tool within the methodology, used primarily in Stage 4 (Detection and Observability Assessment) and Stage 5 (Lessons Learned).

This matrix establishes a standardized method for evaluating how different cybersecurity tools perform across various attack phases. It combines both qualitative and quantitative indicators to assess detection coverage and observability levels.

Each attack phase - such as Reconnaissance, Credential Access, Privilege Escalation, or Defense Evasion - is scored based on detection logs and alert data collected during controlled testing. Table 1 in Appendix A provides a representative fragment of the matrix developed in the Cyber Soldier Project. The matrix serves multiple purposes:

- benchmarking the performance of cybersecurity tools,
- guiding configuration tuning and detection engineering,
- providing a quantifiable measure of overall digital resilience.

When applied iteratively, it enables organizations to track progress in their detection and observability maturity, transforming test results into measurable resilience indicators.

V. RESULTS AND RESEARCH FINDINGS

The Cyber Soldier Project conducted an extensive research program to validate the proposed threat-led digital resilience assessment methodology. The research focused on two key areas: (1) evaluating the detection effectiveness of commonly deployed cybersecurity systems; (2) assessing the practical applicability of the methodology in production and training environments. The research involved executing multiple threat scenarios derived from validated adversary profiles. Each scenario was implemented using the Cyber Soldier BAS platform and validated through the Cyber Range before controlled execution in selected production environments.

Empirical data collected from the tests demonstrated substantial variance in detection and observability performance across different classes of security controls. The Detection and Observability Assessment Matrix provided quantifiable insights

into which defensive technologies exhibited strengths or weaknesses during specific attack phases.

The results highlight that no single defensive technology provides complete detection coverage; digital resilience depends on the synergy of multiple integrated components.

The controlled execution of validated threat scenarios within production environments provided valuable operational insights:

- Even well-maintained systems contained latent misconfigurations (e.g., over-privileged service accounts in Active Directory, unmonitored SMB shares).
- In multiple cases, red team activities were logged but not correlated or escalated, resulting in delayed detection.
- The involvement of blue team analysts during the purple-team phase significantly improved post-test awareness and incident triage skills.

These findings confirm that organizational competence and process maturity play as critical a role in resilience as the underlying technology.

VI. Discussion and Conclusion

As of the end of 2025, the Cyber Soldier BAS toolset had been deployed in more than 20 production environments across various organizations, primarily within the financial and critical infrastructure sectors. It has also been utilized in incident response training exercises, mainly across Eastern European countries (including Poland, Bulgaria, Romania, and others), with a total number of participants exceeding 400. The collected research data confirms that a threat-led, detection-centric methodology provides a more realistic and measurable assessment of cybersecurity system resilience than static vulnerability scanning or traditional red team exercises alone.

A. Contribution to Regulatory Practice

Under DORA and TIBER-EU, organizations are expected to conduct intelligence-based red team tests at least every three years. However, DORA's RTS do not prescribe how resilience should be maintained and measured between formal TLPT cycles. The proposed methodology fills this gap by offering a continuous assessment framework, enabling organizations to:

- conduct internal threat-led evaluations using validated scenarios,
- benchmark detection coverage against a standardized matrix, and
- prepare systematically for formal TLPT engagements.

The methodology operationalizes DORA's principle of digital operational resilience by translating it into repeatable, data-driven testing processes.

B. Educational and Capability-Building Impact

A key outcome of the methodology's application is its educational value. By integrating the Cyber Soldier BAS platform and the Threat Intelligence Assistant, analysts and engineers gain direct exposure to the logic of real-world adversary operations. The Cyber Range provides a safe environment for practice, while the Detection and Observability Matrix delivers immediate feedback on detection effectiveness. This creates a learning loop that continuously enhances both technical skills and organizational readiness - transforming the testing process into a structured competence-development mechanism.

C. Limitations

Limitations primarily relate to environmental constraints:

- The methodology's precision depends on the quality and currency of available threat intelligence,
- Resource requirements for realistic Cyber Range simulations may be significant for smaller institutions.

Despite these constraints, the methodology provides an adaptable, scalable model suitable for organizations of varying maturity levels.

D. Conclusions

The Cyber Soldier Project demonstrates that threat-led digital resilience assessment represents a vital evolution in how organizations measure and enhance their cybersecurity posture. The proposed methodology integrates threat intelligence, ethical red teaming, Cyber Range validation, and detection analysis into a coherent framework aligned with DORA and TIBER-EU. Through its supporting tools, the approach offers:

- a structured process for conducting realistic and repeatable resilience tests,
- a quantifiable detection matrix enabling measurable improvement tracking, and
- a competence-building mechanism for cybersecurity teams.

The methodology extends beyond vulnerability-centric testing paradigms by integrating threat intelligence, adversary emulation, detection analysis, and human learning. It complements regulatory TLPT exercises by enabling continuous, evidence-based evaluation of digital resilience.

Future research will extend this work toward integrating AI-assisted threat scenario generation, cloud and hybrid infrastructure testing, and OT resilience validation, ensuring that the methodology continues to evolve alongside emerging technologies and threat landscapes.

Note on Availability

The CyberSoldier.EU (https://cybersoldier.eu/) service provides the Threat Intelligence Assistant (TIA) application free of charge. TIA is a response to the cybersecurity testing requirements established for the financial sector in EU countries by DORA and TIBER-EU. TIA enables the selection of a specific cybercriminal group (the naming of groups in TIA is consistent with MITRE ATT&CK) and the generation of a detailed cybersecurity testing plan for that group, containing the cyberattack techniques used by the selected group.

Cyber Soldier BAS tools are used by the organization conducting the Cyber Soldier project (Clico) as well as by companies that have completed training in the operation of this tool. The use of Cyber Soldier BAS tools for cybersecurity testing by trained operators is free of charge.

Acknowledgements

We are very grateful to numerous testers and users of the Cyber Soldier framework and tools for their valuable input into the features of this software. The users' opinion leads to constant improvement and development of the framework and methodology.

APPENDIX A

TABLE I
SAMPLE FRAGMENT OF THE DETECTION AND OBSERVABILITY ASSESSMENT MATRIX

Cyberattack Phase	Detection Coverage and Observability by Cybersecurity Solution [Scale: 0-5]		
	EDR & XDR	NDR	IPS & NGFW
Phase 1. Reconnaissance, Initial Access & Command and Control	2	2	2
Phase 2. Active Directory and Network Discovery	1	3	1
Phase 3. Credential Access and Lateral Movement	3	3	1
Phase 4. Exploitation of Vulnerable Web Applications	1	1	3
Phase 5. Privilege Escalation and Continued Lateral Movement	3	1	2
Phase 6. Net-NTLM Reflection and Relaying	3	4	3
Phase 7. Defense Evasion and Credential Dumping	5	2	2
Phase 8. Aggressive Exploitation	4	2	3
Phase 9. Critical Asset Compromise	3	2	1

Scale Description:

0 – No detection and no logging
1 – Minimal logs, no alerts
2 – Partial event logging, occasional alerts
3 – Good logging and alerts for selected TTPs
4 – Full logging and most alerts in this phase
5 – Full logging + immediate alerts, real-time detection

REFERENCES

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[2] European Central Bank. (2025, January). TIBER-EU framework: How to implement the European framework for threat intelligence-based ethical red teaming. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf

[3] European Banking Authority, European Securities and Markets Authority, & European Insurance and Occupational Pensions Authority. (2025, July 8). Joint draft Regulatory Technical Standards specifying elements related to threat-led penetration tests. European Banking Authority. https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-standards-specifying-elements-related-threat-led-penetration-tests

[4] OWASP Foundation. (2024). OWASP Testing Guides: Web Security Testing Guide (WSTG), Mobile Security Testing Guide (MSTG), and Firmware Security Testing Methodology. Open Worldwide Application Security Project. https://owasp.org

[5] Penetration Testing Execution Standard (PTES). (2020). The Penetration Testing Execution Standard v1.1. PTES Organization. https://www.pentest-standard.org

[6] PCI Security Standards Council. (2022). Penetration Testing Guidance: Guidance for PCI DSS Requirement 11.4. PCI SSC. https://www.pcisecuritystandards.org

[7] ISECOM – Institute for Security and Open Methodologies. (2021). Open Source Security Testing Methodology Manual (OSSTMM), Version 4.1. ISECOM. https://www.isecom.org/research

[8] Gartner, Inc. (2024, January 30). Voice of the customer for breach and attack simulation tools. Gartner Research.

[9] IBM. (2024, February 16). What are breach and attack simulations? IBM Think Blog. https://www.ibm.com/blog/what-are-breach-and-attack-simulations

[10] MITRE Corporation. (n.d.). MITRE ATT&CK®: A knowledge base of adversary tactics and techniques based on real-world observations. https://attack.mitre.org/

[11] Pierantoni, G. (2024, February 15). Dumping LSASS remotely from Linux. Medium. https://medium.com/@giuliopierantoni/dumping-lsass-remotely-from-linux

[12] Shawn. (2024, April 7). Impacket: The Swiss Army Knife of Network Security. Medium. https://medium.com/@shawn2600/impacket-the-swiss-army-knife-of-network-security-21d9abb906cd

[13] Gartner, Inc. (2025, May). Magic Quadrant™ for Endpoint Protection Platforms (EPP). Gartner, Inc.

[14] Gartner, Inc. (2025, April). Magic Quadrant™ for Network Detection and Response (NDR). Gartner, Inc.

[15] Gartner, Inc. (2025, July). Magic Quadrant™ for Hybrid Mesh Firewall. Gartner, Inc.

[16] Lockheed Martin Corporation. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains [White paper]. Lockheed Martin Corporation.

[17] MITRE Corporation. (n.d.). Groups. In MITRE ATT&CK®. https://attack.mitre.org/groups/

[18] Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity alerts & advisories. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories

[19] The DFIR Report. (n.d.). The DFIR Report. https://thedfirreport.com/

[20] The National Security Archive, & SANS and Electricity Information Sharing and Analysis Center. (2016, March 18). Analysis of the cyber attack on the Ukrainian power grid. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf