

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

K. Sarmila

Research Scholar, Assistant Professor Department of Computer Science Vels University, Chennai

Research Article

Date of Submission: 10-07-2025

Date of Acceptance: 12-08-2025

Date of Publication: 19-10-2025

Abstract—In order to comply with European regulatory frameworks like the Digital Operational Resilience Act (DORA), we propose the Cyber Soldier approach and tool set, which presents a threat-led approach for evaluating the digital resilience of cybersecurity systems inside enterprises. This approach, in contrast to conventional vulnerability assessments or penetration testing, focuses on simulating the tactics, methods, and procedures (TTPs) of actual attackers in order to assess the efficacy of operational resilience mechanisms and cybersecurity measures in production systems.

In order to assess the organization's readiness for complex cyberthreats, the suggested approach combines threat information, red team scenario creation, and detection performance analysis into a single procedure.

We show how the proposed framework connects the operational practice of resilience testing with the strategic compliance obligations under DORA. We also provide some preliminary statistics about the use of the Cyber Soldier toolkit in practical settings.

Keywords—Threat intelligence, cybersecurity, and digital resilience

INTRODUCTION

Financial and critical-sector companies are required by modern regulatory frameworks like DORA [1] to evaluate their digital operational resilience via hands-on, intelligence-led testing. The European Central Bank's TIBER-EU Framework [2] defines Threat-Led Penetration Testing (TLPT), which is used to operationalize this requirement. TLPT aims to confirm how well an organization's defenses resist realistic assaults that mimic the TTPs of actual threat actors.

Although they provide process-level guidelines, TIBER-EU, DORA, and the associated Regulatory Technical Standards (RTS) [3] do not specify a consistent approach for carrying out continuous, repeatable evaluations of cybersecurity system resilience in between TLPT cycles.

Current security testing techniques, include the Penetration Testing Execution Standard (PTES) [5], PCI DSS Penetration Testing Guidance [6], OWASP Testing Guides [4], and the Finding vulnerabilities and confirming their exploitability under controlled technical settings are the main goals of the Open Source Security Testing Methodology Manual (OSSTMM) [7]. Instead of evaluating the overall resilience of cybersecurity controls and operational procedures, its main goal is to quantify the vulnerability of information systems to known vulnerabilities.

Despite being industry standards for systematic penetration testing, these approaches have a number of drawbacks when it comes to contemporary threat-led resilience assessment:

Lack of Threat information Context: Conventional approaches concentrate on vulnerabilities at the system level, but they seldom include cyber threat information (CTI) that explains how real attackers function. Usually, they don't have organized methods for connecting test activities to actual threat actors, TTPs, or ongoing attack operations.

Limited Assessment of Cybersecurity System Effectiveness: The goal of standards like OWASP WSTG, MSTG, and PCI DSS Penetration Testing Guidance is to confirm the existence of vulnerabilities or incorrect setups. They don't provide a methodology for evaluating how well defensive systems operate or how well the company can identify and react to threats in real time.

No Educational or Capability-Building Elements Testing is often seen by current approaches as a one-time audit

procedure rather than an educational or developmental endeavor. The involvement of human analysts, their decision-making during events, and their ability to learn from simulated assaults are not highlighted.

In contrast, the Cyber Soldier Project's Threat-Led Digital Resilience Assessment Methodology combines human factors, threat intelligence, and detection analytics into a single testing procedure. It places a strong emphasis on measuring the efficacy of detection, realistic enemy emulation, and ongoing education-based development.

The European Central Bank approved the TIBER-EU Framework, which outlines the Threat-Led Penetration framework.

Testing (TLPT). TIBER-EU testing is done occasionally, usually once every three years, although it is not ongoing. Organizations don't have a consistent way to track or monitor resilience gains in between TLPT cycles. By providing an ongoing, reproducible methodology for resilience assessment, the Cyber Soldier Methodology closes this gap.

I. FRAMEWORK OF THE CYBER SOLDIER METHODOLOGY

Threat-Led Penetration Testing (TLPT) is defined under the TIBER-EU Framework, which was approved by the European Central Bank. TIBER-EU testing is done occasionally, usually once every three years, although it is not ongoing. Organizations don't have a consistent way to track or monitor resilience gains in between TLPT cycles. By providing an ongoing, reproducible methodology for resilience assessment, the Cyber Soldier Methodology closes this gap. The Cyber Soldier Project offers an organized, threat-driven approach that combines the defensive (blue/purple team) and offensive (red team) viewpoints into a unified testing cycle:

Threat scenarios are executed under control in production situations.
strict use of threat intelligence to guarantee regulatory alignment and realism,
Pre-validation via interaction with Cyber Range environments
Using a defined observability matrix, detection coverage is measured.

The suggested threat-led approach is intended to serve as a methodical framework for evaluating cybersecurity systems' digital resilience. It extends the concepts of threat-led penetration testing found in DORA, the TIBER-EU Framework, and the Regulatory Technical Standards (RTS) into a repeatable and quantifiable procedure appropriate for ongoing enhancement of cyber defensive capabilities.

The technique is predicated on the idea that cyclical execution of structured threat scenarios drawn from current cyber threat information (CTI) may quantify and enhance digital resilience.

A. Objectives

The framework's main goal is to provide a repeatable, threat-intelligence-driven procedure that enables businesses to: evaluate how well defensive controls are working,

- assess observability and detection coverage during the course of an assault,
- Determine procedural flaws and configuration gaps,
- train staff with realistic, engaging activities and
- assist in meeting the operational resilience testing standards set out by DORA.

B. By converting threat-led penetration testing from a recurring compliance need into an ongoing resilience management procedure, this method enables businesses to conduct internal evaluations in between official TLPT cycles.

Conceptual Structure

The four interconnected levels of the technique are as follows:

- Threat Intelligence Layer: this layer describes the contextual intelligence sources, adversary models, and TTPs that are used to generate scenarios.
- Scenario Design and Validation Layer: This layer converts threat information into organized red team scenarios and verifies them in a controlled Cyber Range setting.
- Execution and Observation Layer: gathers observability data from defensive tools and provides controlled execution of threat scenarios in production settings.
- Assessment and Learning Layer: consolidates lessons learned, fosters capacity development, and assesses detection

efficacy using the Detection and Observability Assessment Matrix.

This approach is implemented in the Cyber Soldier Project. Its modules, which translate theoretical presumptions into practical application, include Cyber Soldier Breach and Attack Simulation (BAS) [8, 9], Threat Intelligence Assistant, Cyber Range, and the Detection and Observability Assessment Matrix..

C. Principles of Methodology

The framework is based on a number of methodological tenets:

- Threat-Led Orientation: Every test activity is based on validated cyber threat data and represents actual adversary TTPs.
- Controlled Execution: To guarantee production safety, all tests are carried out morally, within authorized parameters, and with complete organizational permission.
- Detection-Centric Assessment: This kind of assessment focuses on the cybersecurity system's capacity to identify and record adversary activity, rather than only successful exploitation.
- Educational and Analytical Value: Every test advances detection engineering techniques, personnel skill development, and information transmission.
- Reproducibility and Transparency: To guarantee auditability and repeatability, every scenario is recorded, including the tools used, configuration settings, and anticipated detection events.

METHODOLOGY STAGES

The Cyber Soldier Project's threat-led digital resilience assessment methodology is divided into five steps, each of which represents a unique operational and analytical aspect of resilience testing. These phases guarantee that the evaluation stays threat-driven, regulated, quantifiable, and repeatable.

A. Stage-1 Threat Intelligence Analysis and Adversary Profiling

Finding relevant threat actors based on sectoral and geopolitical context is the first step in the evaluation. The analysis integrates:

- recent reports from suppliers of cyber threat intelligence (CTI),
- frameworks for mapping adversary TTPs, including MITRE ATT&CK [10], and
- Both commercial and open-source intelligence sources.

Known attack methods, preferred initial access routes, infrastructure utilization, and operational objectives (e.g., data theft, financial gain, disruption) are all included in each adversary profile. This guarantees that testing procedures are relevant to the organization's exposure in the actual world.

This process is automated by the Cyber Soldier Project's Threat Intelligence Assistant, which compiles MITRE ATT&CK-based data and creates structured adversary profiles that form the basis for later scenario creation.

B. Stage 2 - Threat Scenario Design and Validation

Adversary intelligence is converted into a technological red-team scenario in the second step. Every scenario is based on a series of attack routes, which are ordered collections of methods that mimic the actions of the chosen threat actor. During the design phase, relevant MITRE ATT&CK methodologies are mapped to attack vectors and threat scenarios. Additionally, legal and proven tools that are allowed for ethical testing are chosen and documented (e.g., netexec, nanodump[11], impacket[12]). A lawful instrument is used to carry out each stage of an assault route. According to MITRE ATT&CK, a single phase may include one or more cyberattack strategies. Techniques employed in a single stage may sometimes fall under various approaches in this matrix. The methods for carrying out the specified assault route are defined by the stages and instruments used. – see Figure 1.

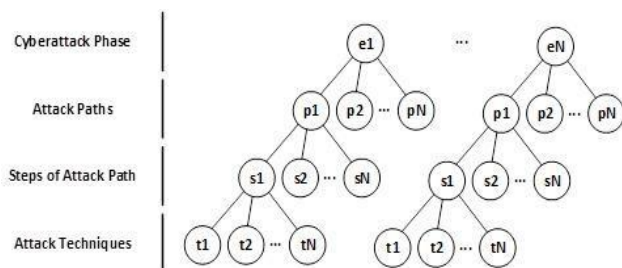


Fig. 1. Threat scenario model.

Every scenario must go through pre-validation in a Cyber Range environment that replicates standard business infrastructure (such as Windows Active Directory, databases, mail, and web servers) before being executed on production systems.

C. Stage 3 - Managed Implementation in a Production Setting

In this phase, the verified scenario is carried out under controlled circumstances inside the company's live systems. In contrast to typical vulnerability scanning, the goal is to assess how well the cybersecurity system recognizes and reacts to actual adversary action in addition to finding vulnerabilities.

The cyberattack lifecycle (e.g., reconnaissance, lateral movement, privilege escalation, and critical asset compromise) is reflected in the phased execution strategy. Through integrated defensive systems, telemetry and alarm data are gathered at every stage of the assault.

The testing team may use the "assume breach" approach, which permits the execution of all planned attack paths by granting initial access at a predetermined level, to guarantee safety and continuity. This is consistent with DORA's notion of a "leg-up" while doing TLPT exercises.

D Stage 4 - Detection and Observability Assessment

The assessment of detection and monitoring capabilities is the main emphasis of the fourth stage. The Detection and Observability Assessment Matrix, an organized framework that links attack methods with anticipated defensive reactions, is used by the Cyber Soldier Project to achieve this goal.

The Detection and Observability Assessment Matrix was created for the Cyber Soldier Project based on research done in the Cyber Range environment, where specific cybersecurity solutions were installed. These solutions are well-known on the global market and have been highlighted in Gartner Magic Quadrant reports [13, 14, 15]. The Cyber Soldier BAS program, which conducted all assault pathways, was used by specialists in certain cybersecurity solutions to conduct the study. The following cybersecurity solutions were included of the study:

- EDR & XDR (Endpoint Detection and Response & Extended Detection and Response) are systems that keep an eye on server and endpoint behavior in order to identify and address threats. XDR also integrates data from other sources (such as network, email, and cloud).

- Network Detection and Response (NDR) systems keep an eye on network traffic in order to spot threats, spot irregularities, and examine questionable network activity.

- IPS and NGFW (Intrusion Prevention System & Next-Generation Firewall) are systems that block illegal traffic and prevent intrusions; NGFW combines IPS capability with sophisticated filtering and application control techniques.

The danger scenario was broken down into stages for easier comprehension and test plan organization. The Cyber Kill Chain model [16] and strategies from the MITRE ATT&CK matrix were used to establish these stages, however they were modified to take into account the particulars of actual red team testing carried out in corporate production settings.

Analysts may find configuration gaps, tool misalignments, or inadequate telemetry integration by comparing the reported detection levels with the baseline matrix. This offers a data-driven basis for improving the detecting posture.

E. Stage 5 – Lessons Learned and Continuous Improvement

The technical and procedural discoveries are combined into practical results in the last phase. Red, blue, and purple teams evaluate the observability matrix and incident chronology results together. The goals are to:

Verify the alert logic.

- Update tools for detecting threats,

- improve incident response protocols, and
- Give repair of identified problems first priority.

This stage's educational component is just as significant. Cybersecurity professionals improve their situational awareness, analytical abilities, and knowledge with adversary tactics via interactive execution and subsequent analysis—all essential elements of a developed cyber-resilience culture.

SUPPORTING IMPLEMENTATION TOOLS

The Cyber Soldier Project's implementation of the suggested threat-led approach, despite its tool-agnostic design, offers a tangible technical basis for carrying out, automating, and evaluating threat-led digital resilience assessments. In both simulated and real-world settings, the auxiliary tools provide methodological consistency, reproducibility, and safe testing. The entire system design, which connects each component to its matching step in the technique, is shown in Figure 2.

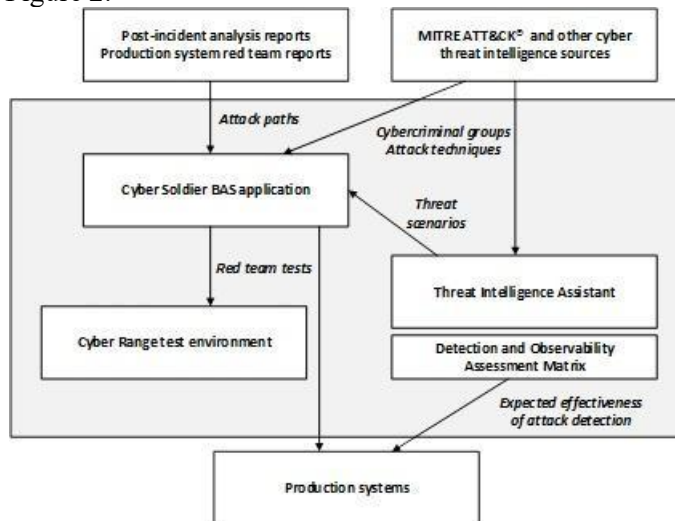


Fig. 2. Architecture of the Cyber Soldier implementation of the threat-led methodology – linking tools to specific stages of the process.

A. Cyber Soldier BAS – Breach and Attack Simulation Platform

- A. The Breach and Attack Simulation Platform, or Cyber Soldier BAS
- The methodology's Execution and Observation Layer is implemented by the Cyber Soldier BAS (Breach and Attack Simulation) platform. It makes it possible for attack pathways that match the chosen threat scenario to be executed in an organized and interactive manner.
- Important traits consist of:
 - Educational interactivity: users may practice attack pathways step-by-step while receiving contextual TTP explanations, which improves their comprehension of adversary behavior.
 - Dual-mode testing allows for safe validation prior to real-world deployment since the platform can function in both the Cyber Range and production settings.
- The legal tooling ecosystem ensures transparency and repeatability by integrating commercial and open-source technologies used in ethical red teaming.

B. Threat Intelligence Assistant – Automated Scenario Generation

By automatically creating customized red team scenarios, the Threat Intelligence Assistant module helps Stages 1 (Threat Intelligence Analysis) and 2 (Scenario Design). Key features include of:

- Using threat information sources to pick adversaries [17, 18, 19, 20],
- Technique mapping: determining the actor's MITRE ATT&CK methods,
- Scenario composition: choosing Cyber Soldier BAS-validated assault routes that correspond with those methods
- Phase alignment: grouping the chosen routes according to the stages of a cyberattack.

This module greatly increases the speed and accuracy of threat scenario production while preserving methodological integrity by automating tasks that have historically required human analysis by red team planners.

C. Cyber Range – Controlled Validation Environment

Without posing an operational danger, the Cyber Range enables researchers and defenders to assess the effect and detectability of attack strategies. Additionally, it serves as a realistic laboratory for purple team cooperation and DORA-aligned resilience validation, providing a basis for training and competence development. The Cyber Range includes:

- Windows Active Directory domains with both standard and incorrect setups,
- web, mail, and database servers,
- integrated defensive technologies, including SIEM, IPS/NGFW, EDR/XDR, and NDR
- Cloud or hybrid environment simulation is optional.

D. Detection and Observability Assessment Matrix

A key analytical tool in the technique, the Detection and Observability Assessment Matrix is mostly used in Stages 4 (Detection and Observability Assessment) and 5 (Lessons Learned).

This matrix provides a uniform framework for assessing the performance of various cybersecurity technologies throughout different stages of an assault. It evaluates detection coverage and observability levels using both qualitative and quantitative metrics.

Detection logs and alert data gathered during controlled testing are used to grade each attack phase, including Reconnaissance, Credential Access, Privilege Escalation, and Defense Evasion. A sample of the matrix created for the Cyber Soldier Project is shown in Table 1 of Appendix A. The matrix has many uses:

- evaluating cybersecurity technologies' performance,
- directing detection engineering and configuration adjustment,
- offering a measurable indicator of total digital resilience.

When used repeatedly, it turns test findings into quantifiable resilience indicators, allowing companies to monitor advancements in their detection and observability maturity.

II. RESULTS AND RESEARCH FINDINGS

To verify the suggested threat-led digital resilience assessment methodology, the Cyber Soldier Project carried out a comprehensive study program. The study concentrated on two main areas: (1) measuring the detection efficacy of widely used cybersecurity systems; and (2) evaluating the methodology's practical usability in training and production settings. Several threat scenarios based on verified adversary profiles were carried out as part of the study. The Cyber Soldier BAS platform was used to implement each scenario, and the Cyber Range was used to test it before it was carefully carried out in specific production scenarios.

Significant differences in detection and observability performance across several types of security mechanisms were shown by empirical data gathered from the testing. Quantifiable insights were obtained via the Detection and Observability Assessment Matrix.

Certain defensive technology showed advantages or disadvantages throughout particular stages of the assault.

The findings demonstrate that digital resilience requires on the cooperation of many linked components; no single defensive technique can provide full detection coverage.

Important operational insights were obtained from the controlled execution of verified threat scenarios in production environments:

- Latent misconfigurations, including as unmonitored SMB shares and over-privileged service accounts in Active Directory, were present in even well-maintained systems.
- In some instances, red team actions were recorded but neither connected nor escalated, which caused discovery to be delayed.
- Post-test awareness and issue triage abilities were much enhanced by the participation of blue team analysts during the purple-team phase.

These results demonstrate that organizational skill and process maturity are just as important to resilience as the underlying technology.

III. DISCUSSION AND CONCLUSION

By the end of 2025, the Cyber Soldier BAS toolkit was in use in over 20 production settings in a variety of businesses, mostly in the critical infrastructure and financial sectors. Additionally, it has been used in incident response training exercises with more than 400 participants, mostly in Eastern European nations including Poland, Bulgaria, Romania, and others. A threat-led, detection-centric approach offers a more accurate and quantifiable evaluation of cybersecurity system resilience than static vulnerability scanning or conventional red team exercises alone, according to the gathered

study data.

A. Contribution to Regulatory Practice

Organizations must do intelligence-based red team tests at least every three years in accordance with DORA and TIBER-EU. DORA's RTS does not, however, specify how resilience should be tested and maintained in between official TLPT cycles. By providing a framework for ongoing evaluation, the suggested technique closes this gap and enables companies to:

Use validated scenarios to undertake internal threat-led assessments.

Compare detection coverage with a typical matrix.

Prepare for official TLPT encounters in a methodical manner.

By converting DORA's concept of digital operational resilience into repeatable, data-driven testing procedures, the approach operationalizes it.

B. Educational and Capability-Building Impact

The methodology's instructional value is one of its main results. Analysts and engineers are directly exposed to the logic of actual enemy activities via the integration of the Cyber Soldier BAS platform and the Threat Intelligence Assistant. The Detection and Observability Matrix provide instant feedback on the efficacy of detection, while the Cyber Range offers a secure setting for practice. This establishes a cycle of learning that constantly improves organizational preparedness and technical proficiency, changing the testing procedure into a methodical system for developing competency.

C. Limitations

Environmental limits are the main source of limitations:

- The accuracy of the approach is dependent on the caliber and timeliness of the threat information that is already accessible,
- For smaller universities, the resources needed for realistic Cyber Range simulations could be substantial.

Notwithstanding these limitations, the approach offers a flexible, scalable model appropriate for companies with different stages of development.

D. Conclusions

Threat-led digital resilience assessment is a crucial advancement in how businesses analyze and improve their cybersecurity posture, as the Cyber Soldier Project shows. The suggested approach combines detection analysis, Cyber Range validation, ethical red teaming, and threat intelligence into a logical framework that is in line with TIBER-EU and DORA. With its auxiliary tools, the method provides:

- a methodical procedure for carrying out repeatable and realistic resilience testing,
- a quantitative detection matrix that makes it possible to measure quantifiable improvements, and
- A way to help cybersecurity teams become more competent. By including threat information, adversary emulation, detection analysis, and human learning, the technique goes beyond vulnerability-centric testing paradigms. It allows for ongoing, evidence-based assessment of digital resilience, which enhances regulatory TLPT exercises.

In order to ensure that the technique keeps up with new technologies and threat environments, future research will expand on this work by including AI-assisted threat scenario development, cloud and hybrid infrastructure testing, and OT resilience validation.

NOTE ON AVAILABILITY

The Threat Intelligence Assistant (TIA) application is available for free via the CyberSoldier.EU (<https://cybersoldier.eu/>) service. TIA is a reaction to the cybersecurity testing standards set by DORA and TIBER-EU for the financial industry in EU nations. TIA makes it possible to choose a particular cybercriminal group (groups in TIA are named in accordance with MITRE ATT&CK) and create a comprehensive cybersecurity testing strategy for that group that includes the cyberattack strategies used by the chosen group.

Both the company running the Cyber Soldier project (Clico) and businesses who have finished the tool's operating training employ Cyber Soldier BAS products. It is free for skilled operators to utilize Cyber Soldier BAS tools for cybersecurity testing.

[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

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 Council of December 14, 2022, which amends Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011. European Union Official Journal, L 333, 1–79. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng> [2] European Central Bank. January 2025. TIBER-EU framework: How to use the European framework for ethical red teaming based on threat information. Central Bank of Europe.
- [4] OWASP Foundation (2024). Web Security Testing Guide (WSTG), Mobile Security Testing Guide (MSTG), and Firmware Security Testing Methodology are OWASP Testing Guides. The Global Application Security Project is open. [5] Penetration Testing Execution Standard (PTES) <https://owasp.org>. (2020). The PTES Organization's Penetration Testing Execution Standard v1.1. [6] PCI Security Standards Council, <https://www.pentest-standard.org> (2022). Guidelines for Penetration Testing: PCI DSS Requirement 11.4. PCI SSC. The website: <https://www.pcisecuritystandards.org>
- [7] The Institute for Security and Open Methodologies, or ISECOM. (2021). Version 4.1 of the Open Source Security Testing Methodology Manual (OSSTMM). ISECOM. <https://www.isecom.org/research> [8] Gartner, Inc. January 30, 2024. Customer voice for tools that simulate breaches and attacks. Gartner Research.
- [9]IBM. February 16, 2024. Breach and assault simulations: what are they? IBM Think Blog. [10]MITRE Corporation. (n.d.). MITRE ATT&CK®: A knowledge base of adversary tactics and methods based on real-world observations [<https://www.ibm.com/blog/what-are-breach-and-attack-simulations>]. [11] Pierantoni, G. (2024, February 15). <https://attack.mitre.org/>. Linux remote LSASS dumping. Medium.

International Journal of Electronics and Telecommunication Systems

Volume1, Issue 04 2025

<https://medium.com/@giulio pierantoni/dumping-lsass-remotely-from-linux> [12] Shawn. April 7, 2024. Impacket: The Network Security Swiss Army Knife. Moderate. <https://medium.com/@shawn2600/impacket-the-swiss-army-knife-of-network-security-21d9abb906cd> [13] Gartner, Inc. (May 2025). Gartner, Inc. [14] Magic Quadrant™ for Endpoint Protection Platforms (EPP). Gartner, Inc. (2025, April). Network Detection and Response (NDR) Magic Quadrant™. Gartner, Inc. [15] Gartner, Inc. July 2025. For a hybrid mesh firewall, use Magic Quadrant™. Lockheed Martin Corporation [16] Gartner, Inc. (2011). Analyzing adversary campaigns and intrusion kill chains to inform intelligence-driven computer network protection [White paper]. Lockheed Martin Company.

[17] MITRE Corporation, n.d. MITRE ATT&CK® Groups: <https://attack.mitre.org/groups/> [18] Cybersecurity and Infrastructure Security Agency. (n.d.). cybersecurity advisories and warnings. Department of Homeland Security, United States. [19] <https://www.cisa.gov/news-events/cybersecurity-advisories> The DFIR Report, n.d. The National Security Archive, SANS, and the Electricity Information Sharing and Analysis Center are available at <https://thedfirreport.com/> [20]. March 18, 2016. An examination of the cyberattack on the electricity system in Ukraine.