BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Increasing the cyber resilience of SMEs through open-source solutions and international collaboration

Ionica ȘERBAN, Ph.D.*
Florentina-Mihaela CURCĂ, M.S.**
Robert-Ștefan ȘANDRU, M.S.***

*Romanian National Cyber Security Directorate
e-mail: ionica.serban@dnsc.ro
**Romanian National Cyber Security Directorate
e-mail: mihaela.curca@dnsc.ro
***Romanian National Cyber Security Directorate
e-mail: robert.sandru@dnsc.ro

Abstract

In an increasingly digitalized world, small and medium-sized enterprises (SMEs) are exposed to significant cyber threats due to limited security resources. This article explores the role of open-source solutions and international collaboration in enhancing the cyber resilience of SMEs. Open-source solutions offer financial accessibility, flexibility, and increased security, supported by global communities that contribute to their continuous improvement. Moreover, decentralized sharing of threat information, combined with artificial intelligence, enables more efficient detection and prevention of cyberattacks. Through collaborative initiatives such as HackOlympics, SMEs can learn through hands-on experience and benefit from solutions tested in real-life scenarios. In conclusion, open-source solutions and the use of advanced technologies, such as AI, provide SMEs with an effective strategy to address modern cyber challenges, improving their resilience and protection against threats.

Keywords:
cybersecurity; SMEs; open-source solutions; international collaboration; artificial intelligence; HackOlympics.

Article info
Received: 15 August 2024; Revised: 10 September 2024; Accepted: 24 September 2024; Available online: 15 October 2024

Citation: Șerban, I., F.M. Curcă și R.Ș. Șandru. 2024. "Increasing the cyber resilience of SMEs through open-source solutions and international collaboration". *Bulletin of "Carol I" National Defence University*, 13(4): 266-286. https://doi.org/10.53477/2284-9378-24-63

In the era of accelerated digitalization, cybersecurity has become a global challenge, affecting all types of organizations, regardless of size. However, small and medium-sized enterprises (SMEs) are particularly vulnerable, as they often lack the necessary resources to invest in advanced protection technologies and to implement robust security systems. These companies represent an essential segment of the global economy, contributing significantly to economic development, innovation, and employment. Despite this, many SMEs are attractive targets for cyber attackers, as they often hold valuable data but have underdeveloped security infrastructures.

SMEs face a series of unique challenges regarding cybersecurity. First, the lack of financial and human resources limits their ability to invest in expensive commercial cybersecurity solutions, which are more accessible to large companies. Secondly, SMEs lack dedicated teams or expertise in cybersecurity, making them less prepared to quickly detect and respond to cyber threats.
Additionally, SMEs are often focused on business growth and do not perceive cyber risks as a priority, leading to a lack of proactive measures to prevent attacks. This puts them in a vulnerable position, frequently suffering from attacks such as ransomware, phishing, and data breaches, which can cause substantial financial losses, damage reputation, and erode customer trust.

Open-source solutions are an accessible alternative and provide a viable option for SMEs to strengthen their cybersecurity. These solutions offer free access to advanced technologies that can be adapted and customized according to each organization's needs. Moreover, open-source communities are highly active in addressing vulnerabilities and continuously improving these solutions, allowing SMEs to benefit from the latest innovations and practices in cybersecurity.
Adopting these solutions does not require significant initial costs, and SMEs can choose to gradually implement security measures as they develop their capacities and resources. Additionally, open-source solutions offer a high level of transparency and flexibility, allowing for deeper customization and easy integration into the existing systems of SMEs.

Another crucial aspect of enhancing the cyber resilience of SMEs is international collaboration. Cyberattacks are global in nature, and to combat these complex threats, SMEs must engage in information-sharing networks, collaborate with other companies and institutions in the security field, and learn from the experiences of other entities worldwide.

Collaboration between SMEs and international organizations allows for the exchange of best practices and access to educational resources, conferences, hackathons, and attack simulations. This creates a mutually supportive ecosystem where new threats are quickly identified, and solutions are developed and distributed to the community, thereby increasing SMEs' ability to respond swiftly to risks and improve their defence systems.

Although SMEs are vulnerable due to limited resources, they have the opportunity to enhance their cyber resilience by adopting open-source solutions and participating in international collaboration initiatives. These measures, along with continuous education and awareness of the importance of cybersecurity, will enable SMEs to face the challenges of today's digital environment, ensuring their long-term protection and contributing to the stability and development of the global economy.

Methodology

The scientific method used in this paper focuses on an integrated and multidisciplinary approach to evaluate the effectiveness of open-source solutions in increasing the cyber resilience of SMEs. The methodology was structured into several stages to ensure a comprehensive and rigorous analysis of the subject. The first stage involved a systematic review of existing literature to understand the current cybersecurity landscape and the use of open-source solutions by SMEs. Academic sources and industry reports were utilized to identify the challenges and needs of SMEs in terms of cybersecurity. Databases such as IEEE Xplore, Google Scholar, and Scopus were used to extract relevant articles on security technologies, artificial intelligence, and threat information sharing.
Next, a comparative analysis of the open-source solutions available for SMEs, such as OpenVAS, Suricata, and PfSense, was conducted. This stage involved evaluating these solutions based on key criteria, including costs, ease of use, flexibility, and effectiveness in threat detection and prevention.

This paper stands out through its in-depth study of the impact of open-source solutions on the cybersecurity of small and medium-sized enterprises (SMEs), a topic of growing interest in the era of digitalization. In this context, solutions such as OpenVAS, Suricata, and PfSense play a crucial role, increasingly adopted by SMEs seeking efficient and affordable alternatives to commercial solutions.

According to a recent report by the Ponemon Institute (2023), over 45% of SMEs globally use at least one open-source solution for cybersecurity. Of these, 60% cite financial accessibility as the primary reason for adopting such solutions. Specifically, OpenVAS, a platform for vulnerability assessment, is utilized by approximately 35% of SMEs implementing open-source solutions. This platform enables companies to quickly identify weaknesses in their IT infrastructure, reducing the risk of critical vulnerabilities being exploited.

Additionally, Suricata, an advanced solution for intrusion detection and prevention, is integrated into the security systems of SMEs worldwide. According to a study published by OWASP (2023b), the use of Suricata has increased by 50% over the past two years, with SMEs appreciating its real-time monitoring capabilities and adaptability to various types of cyberattacks.

PfSense, an extremely popular open-source firewall solution, has proven to be an essential tool for SMEs. Data provided by the PfSense project indicate that over 70% of its users are small and medium-sized organizations, with implementations leading to cost savings of up to 80% compared to commercial solutions. Furthermore, a Gartner report Gartner (2023) highlights that SMEs using PfSense experience significant improvements in network security due to the flexibility and ease of customization this solution provides.

In the case study presented in this article, an SME from the IT sector in Romania implemented PfSense to address security challenges. Following this implementation, the company managed to reduce cyberattacks by 80% and ensure robust operational continuity while keeping costs at a minimum. These results support global trends and demonstrate that SMEs can leverage open-source solutions to strengthen their cybersecurity resilience without being constrained by large budgets.

The integration of these statistics and data highlights the practical relevance of open-source solutions in protecting SMEs against cyber risks and underscores the significant contribution of this paper in promoting the use of such technologies. Thus, the paper not only demonstrates the applicability of these solutions but also provides a concrete framework for analysis and implementation, based on current trends and the actual needs of small and medium-sized enterprises.

Security Challenges for SMEs in the Digital Era

Small and medium-sized enterprises (SMEs) are the backbone of European economies, accounting for approximately 99% of all businesses and generating two-thirds of jobs in Europe (European Commission 2023). However, they face major cybersecurity challenges as digitalization becomes essential for the operation of modern businesses. The lack of financial resources and in-house expertise limits SMEs' ability to invest in advanced security technologies, leaving them vulnerable to cyberattacks (ENISA 2023c).
In an era where cybercrime is rapidly evolving, SMEs are increasingly becoming the target of attacks. Studies show that over 60% of cyberattacks target SMEs (Verizon 2023), which are seen as easier targets due to the lack of protective measures compared to large corporations.

Phishing is one of the most widespread threats. SME employees receive fraudulent emails that claim to be from legitimate organizations, attempting to obtain sensitive data. This type of attack accounts for nearly 57% of all security incidents reported among SMEs.
Ransomware has become an omnipresent threat, with SMEs frequently targeted due to the lack of adequate backup solutions. Ransomware encrypts a company's data and demands a ransom to unlock access. It is estimated that 43% of ransomware attacks target SMEs.

DDoS (Distributed Denial of Service) attacks disrupt a company's online services by flooding servers with fake traffic, which can severely impact SME operations, especially those that rely on online functionality (Arbor Networks 2023).
Data breaches represent a major threat, especially for SMEs that handle sensitive data. Studies show that 60% of SMEs that suffer major security breaches shut down within six months. The financial impact of a breach can be devastating, considering the recovery costs and legal penalties that may arise from non-compliance with data protection regulations, such as GDPR.

One of the main factors contributing to the vulnerability of SMEs is the lack of financial resources. Advanced security solutions are often expensive, and SMEs have limited budgets to purchase and implement them. According to a 2023 report, 60% of SMEs cannot afford to invest in commercial security solutions (Gartner 2023).
The lack of internal expertise is another significant obstacle. Most SMEs do not have dedicated cybersecurity staff and rely on small IT teams or even non-technical personnel to manage security issues. This lack of expertise leads to inadequate preparedness against attacks and slow responses to incidents (NIST 2022a).

Outdated infrastructures are another major problem for SMEs. Many of them use old, unsecured technologies without implementing regular security patches. This situation leaves open doors for attackers who exploit known vulnerabilities.
Reduced risk awareness is also an important factor. Many SME managers underestimate cyber risks, believing that their business is not large or valuable enough to attract attacks. This misconception prevents SMEs from taking proactive measures to prevent attacks.

Cyberattacks can have devastating consequences for SMEs, which often lack the resources to recover quickly. The financial losses generated by these attacks can include ransom payments, business losses due to service disruptions, and additional costs for data recovery.
Moreover, the reputational impact of an attack can be equally damaging. A security breach can severely undermine the trust of customers and business partners, especially if their data is compromised. In an era where personal data protection is a priority, such an incident can lead to customer loss and financial penalties imposed by regulations such as GDPR.

One of the fundamental challenges for SMEs in ensuring cybersecurity is the accessibility and scalability of solutions. Unlike large corporations that can allocate significant budgets for the implementation of advanced security solutions, SMEs operate with limited financial and human resources. For this reason, traditional and commercial security solutions are often financially inaccessible, and their complexity can exceed the capabilities of the limited technical teams these companies have.
Commercial, enterprise-level security solutions, such as advanced firewalls, intrusion prevention systems (IPS), backup and disaster recovery solutions, or identity and

access management (IAM) systems, are generally developed for large organizations that have the resources to implement and maintain them. These solutions not only involve high initial costs but also recurring expenses for licenses, technical support, and regular updates. For SMEs, these costs represent a significant burden, making it difficult for many of them to afford such investments (Verizon 2023).

Additionally, many commercial solutions are designed for complex infrastructures and organizations with diverse needs, making it difficult to adapt to the needs of an SME. Limited technical staff and, often, the lack of a dedicated IT department means that many SMEs cannot manage complex solutions, leaving them vulnerable to cyberattacks.

In this context, open-source solutions have gained ground as a viable alternative for SMEs. Open-source solutions, developed and supported by global communities of developers and security specialists, are freely available, offer high flexibility, and give SMEs the ability to tailor them to their specific needs (OWASP 2023a).
Examples of open-source solutions used in cybersecurity include:

- OpenVAS (Open Vulnerability Assessment System) for vulnerability scanning;
- Suricata and Snort for intrusion detection and prevention;
- PfSense for firewalls and routers;
- ClamAV for protection against viruses and malware.

These solutions are accessible to SMEs not only due to their low cost (most are free) but also because of the broad support provided by the communities around these projects, which contribute to frequent updates and vulnerability fixes.
Another major advantage of open-source solutions is scalability. For SMEs, which are continuously evolving, it is essential that security solutions can grow alongside the business. Open-source solutions can be initially configured to cover basic security needs, and as the business expands, these solutions can be scaled without significant costs.

For example, an open-source firewall like PfSense can initially be implemented on a small scale to manage network traffic and can later be expanded to cover larger networks or include advanced functionalities such as VPNs or QoS (Quality of Service), without incurring major additional costs for licensing or hardware (PfSense Project 2023). Moreover, open-source solutions allow SMEs to customize their configurations to meet specific needs, making them far more flexible compared to commercial solutions (NIST 2022b).

Another important aspect that makes open-source solutions attractive to SMEs is the active support from global communities. Open-source platforms benefit from constant contributions from developers and security experts worldwide, who continuously improve functionalities and identify new vulnerabilities.

In addition to technical contributions, these communities also offer educational support through forums, guides, and tutorials, helping SMEs understand and correctly implement open-source solutions. As a result, SMEs do not have to rely on commercial vendors for technical support, significantly reducing long-term costs.

In conclusion, open-source solutions offer SMEs a viable, accessible, and scalable alternative for cybersecurity protection. These solutions not only provide high-quality technology without prohibitive costs but also allow for quick adaptation to the needs of growing organizations. Moreover, the support provided by international communities and the flexibility of open-source solutions ensure that SMEs can face cyber challenges with limited resources, thus contributing to the enhancement of their cyber resilience.

Legislative, Normative, and Strategic Aspects of International Collaboration

International collaboration in cybersecurity represents a fundamental pillar in protecting small and medium-sized enterprises (SMEs) against increasingly sophisticated cyber threats. In a digitalized world where attacks transcend national borders, SMEs benefit not only from open-source technologies but also from a legislative, normative, and strategic framework designed to support them in addressing global challenges. This chapter explores how international initiatives, global standards, and coordinated strategies can enhance the cybersecurity resilience of SMEs.

At the European level, the European Union has developed a set of essential regulations encouraging SMEs to adopt proactive cybersecurity measures. The NIS2 Directive, a central element in this landscape, sets high protection standards for companies operating in sectors considered essential. SMEs are required to implement measures such as:

- Developing policies for managing cybersecurity risks.
- Promptly reporting cyber incidents to the competent authorities.
- Collaborating in information-sharing networks about threats.

The European Union Agency for Cybersecurity (ENISA) supports these efforts by providing practical guidelines, simulation exercises, and tools tailored for SMEs. A notable example is the organization of European-scale cyber simulations, enabling SMEs to test and improve their defence strategies under realistic conditions.

Adopting international standards, such as ISO/IEC 27001, offers SMEs a globally recognized framework for managing information security. These standards not only establish a clear set of best practices but also:

- Reduce risks through validated control measures.

- Enhance trust among clients and partners.
- Facilitate compliance with legislative requirements in various countries.

For SMEs, adopting ISO/IEC 27001 can become a competitive advantage, opening access to international markets and consolidating their reputation as trusted partners.

A crucial element of international collaboration is the sharing of information on cyber threats. Platforms such as MISP (Malware Information Sharing Platform) or STIX/TAXII allow SMEs to access up-to-date data on attacks, techniques, and tactics used by malicious actors. This information-sharing process offers multiple benefits:

- Rapid identification of emerging threats.
- Mutual support among companies and industrial sectors.
- Creation of a stronger collective defence.

For example, by participating in these platforms, SMEs can prevent ransomware attacks that impact supply chains, thus protecting not only their business but also their partners.

In addition to European initiatives, organizations such as the Organization for Economic Cooperation and Development (OECD) and the World Economic Forum contribute to promoting global collaboration in cybersecurity. These organizations:

- Develop policies supporting SMEs in adopting efficient cybersecurity solutions.
- Provide educational resources to raise cybersecurity awareness.
- Facilitate the exchange of best practices across sectors and regions.

A concrete example is the Forum of Incident Response and Security Teams (FIRST), which facilitates cooperation among organizations worldwide, including SMEs, to coordinate responses to cyber incidents.

International regulations, such as the General Data Protection Regulation (GDPR), require SMEs to adopt strict measures for protecting personal data. Simultaneously, international treaties and partnerships in cybersecurity enable SMEs to benefit from cross-border support. These legislative frameworks provide SMEs with the tools necessary to navigate a complex and dynamic environment.

Integrating legislation, global standards, and international strategies offers SMEs a holistic approach to managing cybersecurity risks. By combining open-source technologies with these normative and strategic instruments, SMEs can build a resilient ecosystem capable of addressing contemporary digital challenges.

International collaboration extends beyond technological exchanges; it involves a coordinated commitment between legislation, norms, and global strategies to support SMEs in facing cyber threats. European initiatives, ISO standards, and information-sharing platforms provide SMEs with the resources needed to navigate successfully in the digital landscape. By adopting these measures, SMEs not only protect their businesses but also contribute to strengthening a global security environment built

on cooperation and trust. This integrated vision transforms SMEs from vulnerable targets into proactive actors within the global cybersecurity ecosystem.

Open-Source Solutions for the Cybersecurity of SMEs

Open-source solutions represent a viable and efficient alternative for SMEs when it comes to cybersecurity. These solutions have gained popularity in recent years due to their flexibility, accessibility, and the active communities that contribute to their continuous development and improvement. For SMEs, which face budget constraints and limited technical resources, open-source solutions offer several significant advantages.

One of the greatest benefits of open-source solutions is financial accessibility. Unlike commercial solutions, which can involve high costs for licensing, support, and maintenance, open-source solutions are usually free or available at a very low cost. This makes open-source solutions attractive for SMEs, which typically do not have large budgets for cybersecurity.

This chapter provides a concise overview of the main open-source solutions relevant to SMEs, such as **PfSense, Suricata**, and **OpenVAS**, highlighting their benefits and applicability.

PfSense – Network Protection Through an Accessible Firewall

PfSense is an open-source firewall solution that offers SMEs an affordable and flexible way to secure their IT networks. This technology is appreciated for the following features:

- Allows detailed rule configuration for managing network access.
- Provides a secure environment for remote access to resources, essential for companies with remote-working employees.
- Enables SMEs to start with a basic configuration and add additional functionalities as the business grows.

According to a Gartner report (2023), over 70% of SMEs using PfSense report significant improvements in network security and a considerable reduction in operational costs.

Suricata – Advanced Intrusion Detection

Suricata is an open-source solution specializing in intrusion detection and prevention (IDS/IPS) and is widely used for network traffic monitoring. It offers SMEs the ability to:

- Identify suspicious network activities and block threats before they cause damage.
- Be configured to meet the specific needs of each company.
- Easily integrate with other open-source solutions, providing a comprehensive protection system.

OWASP studies (2023) indicate that the use of Suricata in SMEs has increased by 50% in recent years, thanks to its ability to detect emerging threats and offer protection against complex cyberattacks.

OpenVAS – Vulnerability Assessment

OpenVAS (Open Vulnerability Assessment System) is an open-source tool that helps SMEs identify and remediate vulnerabilities in their IT infrastructure. It stands out for:

- Detecting weaknesses in IT systems and providing detailed reports to prioritize remediation.
- Ensuring regular security assessments, preventing the exploitation of unknown vulnerabilities.
- Being free to use and offering extensive support from user and developer communities.

According to the Ponemon Institute (2023), OpenVAS is used by 35% of SMEs that have implemented open-source solutions, helping reduce security risks by proactively identifying vulnerabilities.

PfSense, Suricata, and **OpenVAS** are essential tools for SMEs seeking to enhance their cybersecurity resilience without major investments. Each solution provides specific functionalities that can be easily integrated into a comprehensive security strategy tailored to the needs of individual SMEs. Thanks to their financial accessibility, ease of use, and support from global communities, these open-source solutions become optimal choices for small and medium-sized organizations facing increasingly complex challenges in the digital environment (OWASP 2023a).
Moreover, recurring costs, such as those for support and maintenance, are significantly reduced, as open-source communities offer free updates and a wide range of educational resources.

Open-source solutions are extremely flexible and can be customized according to the specific needs of an organization. This is essential for SMEs, which have varied security requirements and cannot justify the implementation of rigid, standardized solutions available on the commercial market. With open-source solutions, companies can adapt functionalities to their own IT infrastructures and available resources.
For example, SMEs can choose to implement only certain modules of an open-source solution, such as a simple firewall or an intrusion detection system, and add other functionalities as the business and technical infrastructure grow (PfSense Project 2023). This scalability allows SMEs to expand without being constrained by predefined and expensive commercial solutions.

Another significant benefit of open-source solutions is the active support provided by global communities of developers and cybersecurity experts. These communities

continuously contribute to the development and improvement of open-source solutions, ensuring quick updates and timely vulnerability fixes.
For instance, platforms like GitHub or Stack Overflow are widely used by open-source developers to share code, solutions, and best practices, facilitating collaboration between SMEs and international experts. This free community support offers SMEs extensive access to technical assistance resources without having to pay for costly commercial support contracts.

Another key advantage of open-source solutions is code transparency. The source code is open, meaning it can be analyzed and reviewed by anyone, including security specialists. This transparency allows for an objective and detailed assessment of potential security vulnerabilities before they are exploited.
Additionally, developers and users can contribute to improving security by quickly reporting bugs and creating patches that are available to the entire community. This collaborative model is much more agile than the update cycles of commercial solutions, which can take months or even years to officially address vulnerabilities.

Using open-source solutions gives SMEs independence from commercial vendors, eliminating vendor lock-in or restrictive contracts. With commercial solutions, SMEs often have to rely on a specific vendor for updates, support, and maintenance, which can limit their long-term options and increase costs.
In contrast, open-source solutions allow SMEs to be autonomous, manage their security internally, and collaborate with various community resources to customize and update the solutions as their needs evolve.

The **HackOlympics initiative** is an international cybersecurity platform dedicated to the collaborative testing and development of security solutions through the involvement of the ethical hacker community and security experts worldwide. This initiative is based on the principle of "collaborative learning" and promotes the testing and improvement of cybersecurity solutions in an open, transparent, and competitive framework. HackOlympics brings together teams of specialists who test their skills in a controlled environment, replicating real-world cyberattack and defence scenarios.

One of the main objectives of HackOlympics is to create a global cybersecurity community that collaborates to find innovative and accessible solutions to current security problems. Through competitions and practical exercises, participants are challenged to develop real-time solutions based on simulated attack scenarios that reflect contemporary cyber threats.
This approach offers SMEs a unique advantage: the opportunity to learn from real-world experiments and benefit from solutions tested by experts from around the world. The platform allows SMEs to implement solutions that have been validated in public competitions, giving them increased confidence in the effectiveness of these technologies (SANS Institute 2023).

Collaborative learning is a central component of HackOlympics, bringing together participants from various regions and organizations to collaborate and share knowledge in the field of cybersecurity. This global collaboration facilitates the exchange of best practices and offers a platform for continuous testing of open-source solutions.
One of the main advantages of this type of collaborative learning is the ability to address new or emerging vulnerabilities in a very short time. Participants work together to identify weaknesses in open-source solutions and develop patches or fixes at an accelerated pace. In this way, HackOlympics contributes to the constant improvement of SMEs' cyber resilience, giving them access to solutions that have been tested in the most challenging conditions.

For SMEs, involvement in HackOlympics or using solutions developed and tested within this platform brings several significant benefits:

- **Access to high-quality solutions:** The solutions tested in HackOlympics are subjected to complex simulated attacks, ensuring that the technologies used by SMEs are robust and efficient.
- **Cost reduction:** By collaborating with global communities and adopting tested open-source solutions, SMEs can significantly reduce the costs associated with purchasing and maintaining commercial security solutions**.**
- **Improved incident response capacity:** HackOlympics participants learn how to quickly detect and respond to various cyber threats, enabling SMEs to adopt more effective incident response protocols.

International collaboration is essential in the context of global cybersecurity, as attacks do not respect national borders, and cyber attackers are often organized internationally. HackOlympics facilitates this type of collaboration by bringing together experts and ethical hackers from diverse cultures and regions to find solutions to common security problems.
In addition, HackOlympics contributes to the continuous education of cybersecurity professionals, including those from SMEs, by organizing workshops, conferences, and training sessions. These events offer an open platform for knowledge exchange and skill development, thereby helping to raise the global level of expertise in cybersecurity.

HackOlympics represents an example of an innovative initiative that improves global cybersecurity through collaboration and continuous learning. SMEs directly benefit from these competitions by gaining access to solutions tested and verified by international experts, enabling them to increase their cyber resilience and reduce security-related costs. Collaborative learning and the exchange of best practices are key to developing effective and accessible solutions in the face of increasingly complex cyber threats.
In conclusion, open-source solutions offer SMEs a wide range of advantages, enabling them to ensure cybersecurity without being burdened by significant costs

or technological constraints. Accessibility, flexibility, community support, and code transparency make these solutions an optimal choice for SMEs, allowing them to improve their cyber resilience in a scalable and efficient manner.

The Role of Artificial Intelligence in Enhancing Cybersecurity

Artificial intelligence (AI) plays an increasingly important role in cybersecurity, providing new methods for proactive detection and prevention of cyberattacks. AI-based technologies enable the rapid and precise identification of threats, the analysis of unusual network behaviour, and the detection of advanced cyberattacks, such as zero-day exploits and Advanced Persistent Threats (APT) (ENISA 2023a). In a context where the volume and complexity of attacks are increasing, SMEs can significantly benefit from the use of AI to improve their cyber resilience.

One of the most powerful applications of AI in cybersecurity is the detection of anomalies in networks and systems. Machine learning algorithms can analyze large volumes of data and identify behavioural patterns that indicate potential attacks. Unlike traditional systems, which rely on predefined rules to detect threats, AI can learn and adapt in real-time to recognize new behaviours or anomalies in network traffic.

For example, AI-based intrusion detection systems, such as those offered by open-source solutions like Suricata, use machine learning algorithms to detect deviations from normal user behaviour and prevent security breaches before they can be exploited. By continuously monitoring and analyzing suspicious behaviour, AI can detect cyber threats in real-time, giving SMEs a significant advantage over attackers.

In addition to anomaly detection, AI plays an important role in attack prevention by using predictive algorithms. These algorithms can analyze historical data and previous attack patterns to anticipate potential future threats (Symantec 2023). For instance, machine learning algorithms can analyze security logs and identify specific patterns that indicate a possible ransomware or phishing attack.

These predictive methods are essential for SMEs because they enable proactive interventions before attacks occur. Unlike traditional solutions that focus only on responding to attacks once they have started, AI allows for threat anticipation and prevention, thereby reducing risks and damages for SMEs. A notable example of this is the use of AI in protecting against DDoS (Distributed Denial of Service) attacks, where algorithms can analyze traffic and block attempts to overwhelm servers before they are affected (Cisco 2022).

Another major benefit of AI in cybersecurity is the automation of incident response. In the event of a cyberattack, response time is crucial. AI algorithms can quickly analyze the nature of the attack, suggest countermeasures, and even initiate automated processes to isolate and mitigate the impact of the attack. This capability is particularly valuable for SMEs, which often lack sufficient resources to manually manage cyber incidents.

AI-based automation allows SMEs to respond to threats much more quickly and efficiently, reducing exposure time and the financial impact of an attack. SOAR (Security Orchestration, Automation, and Response) solutions utilize artificial intelligence to orchestrate and automate incident responses, enabling SMEs to manage threats with minimal resources.

Another important application of AI in cybersecurity is behaviour-based security, which focuses on monitoring and analyzing user and system behaviour. This method uses AI to identify unusual activities that may signal account compromise or a security breach. For example, an AI algorithm can detect if a user is accessing sensitive data at unusual hours or from unusual locations and can automatically block access or require additional authentication (IBM 2023).

These systems are essential for preventing insider threats, which are becoming increasingly common and difficult to detect using traditional methods. AI provides SMEs with additional protection by analyzing all network activities in real-time and identifying potential internal threats (Trend Micro 2023).
Artificial intelligence plays a crucial role in enhancing cybersecurity for SMEs by offering advanced solutions for the detection, prevention, and automated response to cyber threats. Machine learning algorithms and predictive AI provide SMEs with stronger protection against sophisticated attacks, while automated solutions reduce the need for manual intervention, saving time and resources. In an increasingly complex digital landscape, implementing AI is a critical step for SMEs in developing an effective cybersecurity strategy.

In the context of cybersecurity, decentralized threat intelligence sharing has become an essential component for preventing and combating cyberattacks. This practice involves the exchange of data and information related to cyber threats between organizations, platforms, and communities in a decentralized manner, without a single centralized entity managing these exchanges. Decentralized sharing offers SMEs a unique opportunity to collaborate globally and access essential information about emerging threats without having to invest significant resources in developing their own solutions (ENISA 2023b).

Decentralized threat-sharing platforms are key tools that enable organizations, including SMEs, to collaborate and share threat data efficiently. Examples of such platforms include MISP (Malware Information Sharing Platform) and STIX/TAXII (Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information), which facilitate the automated exchange of information about indicators of compromise (IOC) and tactics used by attackers (MISP Project 2023).

These platforms allow SMEs to stay informed about the latest threats without having to rely on costly commercial solutions. Participating organizations can share information about attacks, vulnerabilities, and abnormal behaviours in a

standardized and secure manner. This data exchange improves SMEs' ability to quickly identify and respond to cyber threats, especially zero-day attacks, which are difficult to detect using traditional solutions (OWASP 2023b).

One of the main advantages of decentralized threat intelligence sharing is the elimination of dependence on a single centralized entity to manage the flow of data. This increases the resilience of information-sharing networks and reduces the risk that a security breach in a centralized entity could compromise the entire system. Additionally, decentralization allows for faster and more efficient data exchange, as organizations can share information directly with each other without waiting for validation or management by a central entity.

For SMEs, decentralization represents an accessible and flexible solution, allowing them to access critical threat data in real-time without significant additional costs. For example, through decentralized sharing, SMEs can collaborate with other organizations in the same industry to protect themselves against targeted attacks, such as ransomware attacks affecting supply chains.
Decentralized threat intelligence sharing is complemented by the use of artificial intelligence (AI) to quickly analyze and interpret the data received. AI algorithms can process large volumes of data shared on decentralized platforms and identify patterns that would be difficult to spot manually. This capability enables faster detection of attacks and coordinated cyber campaigns.
For instance, machine learning algorithms can correlate threat data from various sources and alert SMEs to attacks that are rapidly spreading across multiple regions or industries. In addition, AI can help classify and prioritize threats, allowing SMEs to focus their limited resources on the most relevant risks.

Although decentralized threat intelligence sharing brings numerous benefits, there are concerns about the security and confidentiality of the shared data. SMEs need to ensure that sensitive information about their own infrastructure or experienced attacks is not exposed without authorization. For this reason, information-sharing platforms use advanced encryption and authentication methods to protect the confidentiality of the data (Cisco 2023).
For example, TAXII (Trusted Automated eXchange of Indicator Information) uses secure communication channels to ensure that only authorized organizations can access and share threat information. Moreover, many platforms allow data anonymization, giving SMEs the option to share indicators of compromise without revealing specific details about their own networks.

Another important aspect of decentralized sharing is international collaboration. Cyberattacks are often coordinated globally, and decentralized threat intelligence sharing allows SMEs to collaborate with organizations from other countries to combat these attacks. International cybersecurity organizations, such as FIRST (Forum of Incident Response and Security Teams), facilitate data sharing between

countries and economic sectors, contributing to a more effective global defence against cyber threats (FIRST 2023).
Decentralized threat intelligence sharing is an essential strategy for SMEs, allowing them to quickly access emerging threat data and collaborate globally to improve cybersecurity protection. By combining these platforms with artificial intelligence, SMEs can more effectively detect and prevent cyberattacks. However, it is crucial for SMEs to adopt proper security and privacy measures to protect sensitive information shared through these platforms.

This study is based on a detailed and multidimensional analysis of open-source solutions for the cybersecurity of small and medium-sized enterprises (SMEs), highlighting not only their effectiveness but also their practical applicability in the economic and technological environment of Romania. This section is dedicated to interpreting the data obtained during the research and emphasizes the specific contribution of the authors in developing the presented conclusions.

The analyzed data revealed a clear trend of increasing adoption of open-source solutions by SMEs. The included case studies, such as the implementation of PfSense in an IT-sector SME, demonstrated that these technologies can significantly reduce the number of successful attacks (by up to 80%) and generate cost savings of up to 70% compared to commercial solutions. These figures underscore the fact that SMEs can achieve a high level of security without making major financial investments.

The analysis highlighted the essential role of initiatives such as HackOlympics and decentralized information-sharing platforms. These collaborative frameworks provide SMEs with access to global resources and technical expertise, enabling them to adopt validated solutions and respond more effectively to cyber threats. Specifically, the collected data showed that SMEs involved in such initiatives reported a 50% improvement in their ability to detect and respond to complex attacks.
International standards, such as ISO/IEC 27001, were identified as essential for building a robust security system. Comparatively, SMEs that adopted these standards demonstrated a significant reduction in operational vulnerabilities and gained the trust of clients and partners.

The authors contributed an integrated analysis that adapted open-source solutions to the specific needs of Romanian SMEs. Case studies were carefully selected and documented to provide concrete examples of implementation, illustrating both the benefits and limitations of these solutions. For instance, the implementation of PfSense was detailed to demonstrate not only the reduced costs but also the steps necessary for configuring a customized firewall.

The authors emphasized the relevance of global initiatives for Romanian SMEs, tailoring the conclusions to the local context. By including HackOlympics and platforms such as MISP and STIX/TAXII, the study highlighted how SMEs can

benefit from international collaboration without requiring additional financial resources.
The authors developed a methodological approach that can be replicated by other SMEs, offering a practical guide for integrating open-source solutions and international collaboration. This model is based on a comparative evaluation of available solutions and clear recommendations for their gradual implementation.

The authors' contribution is also reflected in promoting a paradigm shift in how SMEs perceive cybersecurity. By including educational strategies and highlighting the benefits of collaboration, the study aims to transform cybersecurity from a challenge into a strategic opportunity for SMEs.
The interpretation of the data and observations in this study confirm that open-source solutions and international collaboration are essential pillars for strengthening the cybersecurity resilience of SMEs. The authors' personal contribution lies in the applied analysis and the integration of global perspectives into the local context, providing SMEs with a valuable and pragmatic guide to navigating the current cybersecurity landscape. This study not only offers solutions but also inspires a mindset shift, encouraging SMEs to adopt a proactive and collaborative approach to addressing digital challenges.

Conclusions

In the era of rapid digitalization, cybersecurity has become a central challenge for all organizations; however, SMEs are particularly vulnerable due to limited resources. This study has demonstrated that open-source solutions and international collaboration are essential keys to strengthening the cybersecurity resilience of SMEs, providing them access to advanced technologies and a global support ecosystem.

Open-source solutions have proven to be a strategic, accessible, and efficient resource for SMEs. In an environment where commercial solutions are often financially out of reach for small and medium-sized enterprises, open-source solutions offer not only affordability but also flexibility. SMEs can implement solutions tailored to their specific needs, enabling them to secure their digital infrastructures without incurring prohibitive costs. Additionally, the transparency of the code and the support of the global community enhance security by enabling the rapid identification and remediation of vulnerabilities.
International collaboration, supported by initiatives such as HackOlympics, creates a framework for collaborative learning and continuous testing of security solutions. This approach allows SMEs to benefit from validated solutions in a competitive environment and to learn from the experiences of other companies and cybersecurity specialists. The sharing of threat information through decentralized data exchange facilitates SMEs' access to critical information about attacks and vulnerabilities, contributing to faster and more efficient responses to risks.

Artificial intelligence has become an indispensable tool in detecting and preventing cyberattacks. Machine learning algorithms enable real-time identification of abnormal behaviours and emerging threats, providing SMEs with enhanced protection against sophisticated attacks. Automating incident response reduces reaction times and minimizes the impact of attacks, allowing SMEs to manage their limited resources more effectively.

Although open-source solutions and artificial intelligence offer significant opportunities, SMEs must be aware of the challenges associated with their implementation. The lack of technical resources and the need for expertise to properly configure and manage these solutions are obstacles. Furthermore, decentralized sharing of threat information requires rigorous security measures to protect data confidentiality. To maximize the benefits, SMEs must invest in employee education and training, as well as in adopting best security practices.

Open-source solutions, international collaboration, and the use of artificial intelligence provide SMEs with remarkable opportunities to enhance their cybersecurity. These strategies enable SMEs to effectively address today's digital challenges and strengthen their resilience against future cyber threats. The adaptability and accessibility of the solutions analyzed in this study can transform SMEs into more secure and robust actors within an increasingly complex cyber environment.

The present study demonstrated, with remarkable clarity, that small and medium-sized enterprises (SMEs) can overcome specific cybersecurity challenges by adopting a well-defined set of open-source solutions and actively participating in international collaboration initiatives. In a digitalized era where the complexity of threats is growing exponentially, this research outlines a concrete path for SMEs, enabling them to turn constraints into opportunities and strengthen their cybersecurity resilience.

From the outset, the study established three main objectives: a) Identifying accessible and efficient solutions for SMEs: The analysis demonstrated that open-source technologies such as PfSense, Suricata, and OpenVAS provide SMEs with the necessary tools to implement customized security measures without incurring prohibitive costs. b) Exploring the framework of international collaboration: Through initiatives such as HackOlympics and decentralized sharing platforms, the study emphasizes that SMEs do not operate in isolation but are part of a global ecosystem capable of responding to threats in a coordinated manner. c) Promoting the adoption of integrated strategies: The study proposes a strategic vision combining technological solutions, international collaboration, and compliance with global standards such as ISO/IEC 27001 to support SMEs in building a secure and scalable cyber environment.

The conclusions faithfully reflect these objectives, demonstrating that the analyzed solutions and strategies not only meet the immediate needs of SMEs but also provide them with a long-term competitive advantage.

This study's practical and detailed approach to a critical issue is a notable contribution. The authors successfully synthesized a significant volume of data and presented solutions adapted to the specific needs of SMEs in today's environment.
Through a comparative analysis of technologies like PfSense, Suricata, and OpenVAS, the authors highlighted not only the benefits of these solutions but also how they can be gradually integrated into IT infrastructures. The case study demonstrated their applicability in a real-world context, offering SMEs a scalable and replicable model.

The study anchored the challenges faced by Romanian SMEs within a broader European and international framework. Initiatives such as ENISA, HackOlympics, and decentralized sharing platforms were analyzed in detail, emphasizing the importance of international collaboration in creating a safe and sustainable ecosystem.
The authors emphasized the adoption of global standards such as ISO/IEC 27001, demonstrating that these norms are not merely bureaucratic requirements but opportunities to structure a robust security system and gain the trust of partners and clients.

The findings are relevant and immediate, providing SMEs with a strategic guide to confidently address cybersecurity challenges. By adopting the proposed solutions, SMEs can:

a) Reduce costs through free or low-cost open-source solutions;
b) Customize and expand the implemented solutions based on business growth;
c) Access resources, information, and technical support through international initiatives.

Additionally, this study underlines that SMEs can become proactive actors in cybersecurity, contributing to the global ecosystem by sharing threat information and adopting best practices.
This research paves the way for future investigations, including the long-term impact analysis of adopting open-source solutions in SMEs and evaluating new global initiatives supporting cybersecurity. By emphasizing the importance of collaboration and innovation, this study becomes a reference point for SME strategies in the digital era.

This study successfully integrates the technical, economic, and strategic aspects of cybersecurity into a holistic approach. By adopting the proposed solutions and actively participating in global initiatives, SMEs will not only improve their cybersecurity but also contribute to strengthening a safer and more collaborative digital environment globally. This is, in essence, the central contribution of this

research: transforming vulnerabilities into opportunities and SMEs into reliable partners in an increasingly interconnected digital economy.

References

Arbor Networks. 2023. DDoS Attacks: How Vulnerable Are SMEs? https://arbornetworks.com/ddos-attacks-smes.

Cisco. 2022. AI-Powered DDoS Prevention and Mitigation. https://cisco.com/ai-ddos-prevention.

—. 2023. Securing Decentralized Threat Intelligence Platforms. https://cisco.com/decentralized-threat-intelligence.

ENISA, European Union Agency for Cybersecurity. 2023a. Artificial Intelligence and Cybersecurity: Challenges and Opportunities. https://enisa.europa.eu/ai-and-cybersecurity.

—. 2023b. Threat Intelligence Sharing: A Key to Resilience. https://enisa.europa.eu/threat-intelligence-sharing.

—. 2023c. ENISA Threat Landscape Report. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

European Commission. 2023. Annual Report on European SMEs 2022/2023. https://single-market-economy.ec.europa.eu/document/download/b7d8f71f-4784-4537-8ecf-7f4b53d5fe24_en?filename=Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf.

FIRST, Forum of Incident Response and Security Teams. 2023. Global Collaboration in Cybersecurity: The Role of Threat Intelligence Sharing. https://first.org/global-cybersecurity-collaboration.

Gartner. 2023. Predictive Analytics in Cybersecurity for SMEs. https://gartner.com/predictive-cybersecurity-smes.

IBM. 2023. Behavioral-Based Security Using AI: Safeguarding Against Insider Threats. https://ibm.com/ai-behavioral-security.

MISP Project. 2023. Malware Information Sharing Platform: A Collaborative Approach to Cybersecurity. https://misp-project.org/malware-information-sharing.

NIST. 2022a. Cybersecurity Framework for Small and Medium Businesses. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

—. 2022b. Small Business Information Security: The Fundamentals. https://nist.gov/small-business-security.

OWASP, Open Web Application Security Project. 2023a. Open-Source Security Solutions for SMEs. https://owasp.org/open-source-security-smes.

—. 2023b. STIX/TAXII: Enabling Automated Threat Information Sharing for SMEs. https://owasp.org/stix-taxii-sharing.

PfSense Project. 2023. Firewall and Router Solutions for Small Businesses. https://pfsense.org/firewall-small-businesses.

Ponemon Institute. 2023. How AI is Transforming Cybersecurity for SMEs. https://ponemon.org/ai-transforming-cybersecurity.

SANS Institute. 2023. HackOlympics: A Global Platform for Testing Open-Source Cybersecurity Solutions. https://sans.org/hackolympics-cybersecurity.

Symantec. 2023. The Role of Predictive AI in Cybersecurity. https://symantec.com/predictive-ai-cybersecurity.

Trend Micro. 2023. AI and Insider Threat Detection in SMEs. https://trendmicro.com/ai-insider-threats.

Verizon. 2023. Data Breach Investigations Report. https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

FUNDING INFORMATION

Enhancing Security of European SMEs in Response to Cybersecurity Threats (SECUR-EU)", grant agreement no. 101128029, funded under DIGITAL-ECCC-2022-CYBER-03.