Mariana-Luminița ACHIM

RESEARCH ON OPTIMIZING THE CYBERSECURITY OF SENSITIVE DATA

Abstract: *In the context of increasing digital interconnectivity, ensuring the protection of sensitive data has become a critical priority for organizations of all sizes. Cybersecurity threats such as ransomware, phishing, and distributed denial-of-service (DDoS) attacks continue to escalate in frequency and sophistication, disproportionately affecting small and medium-sized enterprises (SMEs) with limited resources. This research addresses the need for accessible and efficient security solutions by exploring approaches that emphasize modularity, real-time detection and adaptability. The study highlights the potential of open-source and scalable frameworks to enhance cybersecurity resilience, offering a viable alternative to traditional commercial tools and emphasizing the importance of proactive defense strategies in today's threat landscape.*

Key words: *Cybersecurity, sensitive data, SMEs, Open-source tools, Virtual infrastructure, security incidents, resilience*

1. INTRODUCTION

Information that has been donned as an essential attribute for economic and technical development, the world over, in recent decades to a rapid expansion of technologies, not only in its own rights and due to its importance in sphere and the relation to all kinds of information. On the flip side, the increasingly ample access to digital networks has contributed to a growing environment for the occurrence and spread of cyber threats jeopardizing the user's confidentiality, reliability, and accessibility of information. As a result, businesses large and small are paying more attention to IT system protection and security implementations. A security attack can lead to huge financial losses, a great disruption in the system, and a big corporate image loss.

2. GENERAL TRENDS

Cyberattacks targeting sensitive data have been on the rise at a sharp pace for twenty years. In the early 2000s, incidents and situations didn’t really happen that often. Now there are thousands a year. A study done at Maryland University finds that a cyberattack takes place every 39 seconds on average. From 2000 to 2025, there has been a steady increase in cyber incident attacks. [1] Cybercrime has become an increasingly growing economic drain on the world. Cybersecurity Ventures estimates that the losses caused by cybercrime have increased from about 3 trillion US dollars in 2015 to 10 trillion US dollars per year by 2025. These are the direct effects (theft of money and data) and indirect effects like a disruption in business, recovery, fines, lawsuits, damage to corporate image, which will have a long-lasting toll on the companies. The corporate sector has been deeply affected. A prime example is that of Equifax, which suffered a breach in 2017 (impacting 147 million people) and paid out more than USD 700 million in payouts and fines. The business environment has worsened significantly as organizations are more dependent now on the digital data. [1]

Sensitive information, such as personal data, is increasingly targeted by large corporations and small businesses alike; even you. Attacks target smaller and medium sized firms due to their less protective measures and limited resources to ensure the implementation of high- performance security solutions. In 2021 thousands of data breaches occurred at organizations with fewer than 1000 people, per the Verizon report. Other research shows that 61% of small and medium sized enterprises were targeted by at least one cyberattacks in 2021 [2]. Hackers use techniques like phishing to steal confidential information like passwords or bank details and install malware (trojans, ransomware) via emails or compromised website links. Cyber attackers like to use social engineering scams to get personal information like passwords or banking details and spread malware (trojans, ransomware) via email or on an infected website. Small businesses are often disproportionately targeted by social engineering scams: employees of small businesses are roughly 3.5x more likely to be targets of this kind of scam than employees of larger organizations. The absence of adequate cybersecurity training makes them more likely to click on malicious links [2].

Hackers use SMEs to target bigger organizations: according to a Ponemon analysis 59% of organizations had a breach due to the hack of a vendor/ partner. [3]. SMEs often lack funding and cyber insurance, and thus, an attack or incident could threaten their very existence. Cyber-attack statistics show that around 60% of SMEs close within six months after the breach. One such example is the British company Travelex, a provider of financial and currency exchange services. In January 2020, the ransomware attack made it a target with the REvil group demanding USD 6 million as ransom. For a month, the company’s systems were paralyzed, affecting key partners, and Travelex filed for insolvency in August the same year, which costed 1,300 jobs. [12] Another example is the 2014 attack on Code Spaces. In this instance, a previous collaborator deleted the cloud data and backups of the company, shutting down the company in just 12 hours of the incident. Many SMEs lack a person dedicated to securing their cyber realm, and the recovery effort is also slow and costly. The cyber-attack interruption can stop businesses from doing its operations after one attack for more than 24 hours as reported by half of small businesses. Most of the time they lose data, lose operations, and pay recovery cost that can go up to tens or even hundreds of thousands. [3]

In the table 1, the percentages below are estimates and are sourced from published data at various intervals. There is no single study that provides data year by year.

Table 1

Estimated increase in cyberattacks between the years. [11

Year	Estimated growth of cyberattacks compared to the previous year
2001	15%
2002	25%
2003	30%
2004	20%
2005	35%
2006	15%
2007	25%
2008	30%
2009	22%
2010	26%
2011	20%
2012	42%
2013	35%
2014	40%
2015	+45% (ransomware becomes popular)
2016	50%

The figures do not indicate the global total of cyberattacks but merely the number of complaints (mostly received in the USA) but nonetheless widely used as an indicator for annual trends.

The image below proportionally represents this data in percentage over the years 2000-2025 for ease of understanding the evolution of cyber-attacks. A lot of ransomware attacks like CryptoLocker, TeslaCrypt, Locky etc. happened in year 2015 and 2016 which correspond to these high figures. The increase in ransomware attacks greatly rose in 2020 due to sudden shift to remote work. After 2021, the growth rate begins to stabilize, in part due to better security but it is still high. In 2024-2025, CyberSecurity Ventures and ENISA predict a sustained high growth rate of +20% to +30% year-on-year with a special focus on IoT, cloud and supply chain.

Table 2 shows the evolution of the number of attacks/complaints every year at the FBI Internet Crime Complaint Center or more commonly referred to as IC3. It is one of the most accessible and consistent sources on cybercrime data since the year 2000. Since 2000, the money lost due to cyber-attacks has increased from tens of millions annually to billions of dollars every year. The sum of money demanded in ransom has gone from a few thousand dollars to (in years 2005-2010) to millions of dollars (after 2010). Cybersecurity Ventures forecasts total cost of cybercrimes could reach $10.5 trillion annually by 2025 which would include ransom payments in ransomware attacks. ENISA and other organizations expect that the double extortion attacks will grow in complexity, with an increase in the ransom value demanded and an increasing targeting of critical infrastructure protection [12].

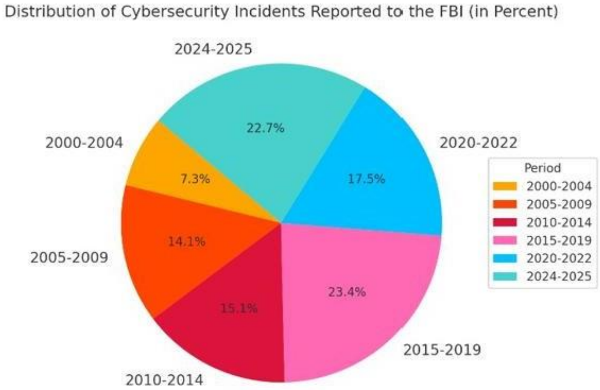

Figure 2. Distribution of cyber incidents reported to the FBI 2000-2025 [4] [5]

Table 2

Number of complaints/attacks registered with FBI [9] [10]

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
No. of complaints / reported attacks	16838	49711	75064	124509	207492	231493	207492	206884	275284	336655	303809	314246	289874	262813	269422	288012	298728	301580	351937	467361	791790	847376	800944

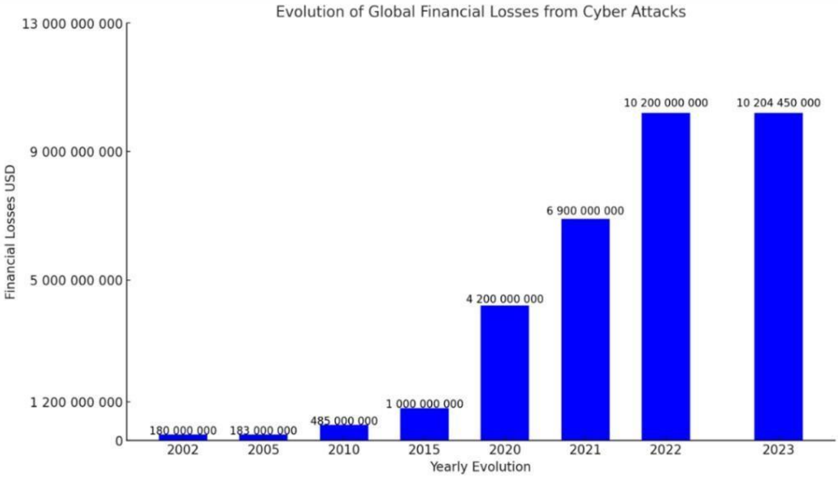

Figure 1. The evolution of financial losses following cyber-attacks between 2000-2025

3. TOP ATTACKS TARGETING SENSITIVE DATA

In order to steal sensitive data, cybercriminals use various means from destructive malware to subtle social engineering methods. From the year 2000 to 2025, one of the major types of attack that has targeted large organisations, small businesses, and individuals are as follows:

3.1 Ransomware

This malicious software encrypts the victim's data, making it impossible to access it until a ransom is paid, normally using cryptocurrency. Between 2000 and 2010, cyber-attacks only affected large businesses. They were very few in number. However, everything changed by 2015. Ransomware attacks started impacting businesses as well as individuals. [8] Cyber-attacks caused by ransomware WannaCry (May 2017) and NotPetya (June 2017) disrupted thousands of entities in more than 150 countries. WannaCry made it impossible for the UK's National Health Service to function and NotPetya which at first was seen as ransomware ended up costing over USD 10 billion in damages to companies such as Maersk, FedEx and Merck among others in over 150 countries. As time went by, ransomware groups began using a technique called "double extortion", which involved stealing data before encrypted and threatening to publish it. The number of ransomware attacks was the highest so far in 2021, as in the first six months alone, there were 304 million such attacks, which is more than the total number for 2020. But legal action and better security now have led to a 23% drop in global ransomware activity by 2022. [8]

Cyber-attacks victimized big corporations, banks, and even hospitals. However, it is the small businesses that are easy prey for the cybercriminals. As per reports of ransomware 2021, 82% of the attacks were on organizations with fewer than 1000 employees. Further, out of the total ransomware attacks, 37% were registered on micro-enterprises with less than 100 employees. The micro enterprises are mostly poorly equipped which makes recovering difficult and dear. A study by Forbes showed that in 2019, it cost an average of USD 84,000 for a small business to recover from a ransomware attack including ransom payment, restoring the system and loss of business. In 2021, the ransom mid-sized companies paid an average of USD 170,000, representing an 82% increase over the average of USD 100,000 in 2020. Even after paying the ransom, many organizations were unable to retrieve all their data, pointing to the unreliability and unpredictability of the recovery process. [11].

3.2 Phishing

This method fools users to share confidential information (such as banking details or passwords) or take unsafe actions like opening infected files. Between 2000 and 2025, phishings were one of the most common methods of security breach instigated by hackers.

According to Verizon report of 2023, 74% of all reported incidents had some kind of human involvement (either due to error, or social engineering attack). Phishing continues to be a common method in many of the cases. As phishing matured, standard phishing (generic emails with fishing links) evolved into spear phishing with tailored messages simulating genuine communication. [7] In 2023, over 709 million phishing links were attempted as reported by Kaspersky, up by over 40% from last year. Smaller businesses often get targeted by massive volumes of such attacks. Companies using no or ineffective email filters, and those that do not train staff remain vulnerable. New variations of phishing attacks (vishing through phone calls and smishing through SMS) are apparent with SMEs and their customers receiving fake banking alerts or tech support phone calls. [7] One of the well-known spear phishing attacks: The 2011 RSA breach, an employee end up activating a malware Excel document allowing attacks to steal data on their SecurID tokens, which in turn compromised many of their corporate clients. In 2016, there was an incident that caught notable attention. [10]

An email was sent by an attacker appearing like a message from the company CEO. Thus, the finance department transferred USD 47 million. This is a BEC (business email compromise) fraud, a mix of phishing with social engineering tricking the target claiming to be an executive/business partner to make payment. The FBI says BEC attacks caused losses of USD 2.9 billion in 2023. This is the most damaging cybercrime and second only to investment scams. [7].

3.3 DDos Attacks (Distributed Denial of Service)

This attacks seek to flood a server or network with excessive amounts of traffic to disrupt online services. Between 2000 to 2025 these attacks happened more and worse and this is because of a huge range of robots (botnets), such as poorly secured IoT devices. In 2016, a huge DDoS attack on DNS provider Dyn with traffic ranging from 100 to 400 Gbps crippled major sites including Twitter, Netflix and Spotify. It was caused by the Mirai botnet. In the years that followed, the frequency of such attacks hit a record high. As per NETSCOUT, there were nearly 13 million DDoS attacks throughout the globe in the year 2022. [9] This was much higher than the 9.7 million attacks that were recorded during 2021. While several of these attacks targeted huge infrastructures and corporations, small which are usually less prepared for attacks. E-commerce companies and other businesses that rely on online presence can lose significant customers and revenue for every hour that their services go offline. A DDoS attack does not take information away from your system. However, it will divert your attention while someone plays with your sensitive information. Or it will stop your services and waste your money by making you go offline. [11].

The figure below shows the most common types of cyberattacks globally and the losses they have caused.

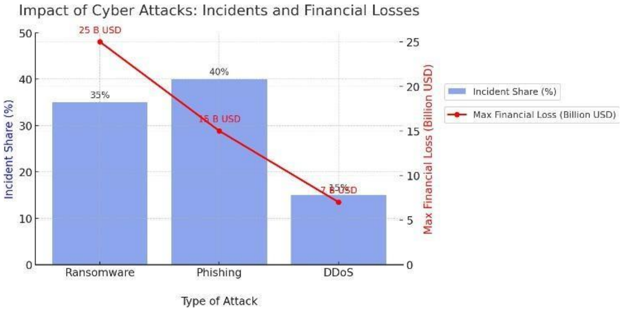

Figure 3. Impact of cyberattacks: Financial incidents and losses [6][7]

As we can see from figure 3, ransomware remains one of the most expensive forms of attacks as threat groups now often use “double extortion” methods (exfiltration + encryption) along with the data encryption. Also, DDoS don't always result in hard money losses (unlike ransomware), they disrupt the service and costs of remediating such issues are very high, affecting reputation and operations of the company negatively. Due to the rise in the number and the intensity of attacks, the market is increasingly requiring faster and more effective threat detection to reduce response time, solutions tested in controlled environments to evaluate how infrastructures respond to real-world attack vectors, simulation and validation methodologies to create realistic attack scenarios (cyber range) and identify weaknesses and open-source and easily customizable solutions as many companies (especially SMEs) lack large budgets for commercial solutions.

4. PROPOSED SOLUTION

As shown in the arguments in prior paragraphs and official reports, SMEs are at a much greater risk of being attacked and having sensitive data compromised, as they have much lower budgets to invest in complex security infrastructures and services, as found in larger corporations. Larger companies do have suitable budgets, which allows them to outsource their infrastructure and service security. Although it is a dependable, expert, and easy method, it is also quite costly.

Most smaller companies have little money, few people and no proper equipment. They can, therefore, defend their own internal infrastructure against malicious attacks and the theft of confidential information. And they can do this without external service providers. With a limited budget SMEs can build their own vulnerability assessment environment to get SOC in future for monitoring security incidents happening live against their systems.

An optimal price-quality-performance ratio is ensured through the implementation of standardized, easy-to-manage security measures that do not involve very high costs. In addition, its modular design enables customization and scalability, allowing businesses to expand their protection as they grow ensuring robust protection of sensitive data without breaking the bank.

This solution helps reduce cyber risks significantly along with high efficiency and a return on security investments, irrespective of organization size.

5. IMPLEMENTATION STAGES OF THE PROPOSED SOLUTION

1. Defining the Research Framework and Building a Virtual Infrastructure Composed of Virtual Machines Running Multiple Operating Systems (Windows, Linux).

Practical steps to follow:

a. Determine which types of sensitive dataare targeted by which malware.

b. Select the specifications for the virtual infrastructure window VMs.

c. The selected software tools Metasploit, Caldera, Elasticsearch and Suricata should be documented and justified.

d. Use VMware Workstation or open-source virtualization technology VirtualBox to create the infrastructure.

e. Set up virtual machines that act like real-world networks.

f. Keep documents that show how you set up the infrastructure

2. Performing Multiple Types of Attack Simulations Using Metasploit or Caldera.

We simulate attacks in this infrastructure and we target sensitive data attacks based on different sectors. These simulations will be diverse in post-compromise impact, including ones that are detected and prevented by incident detection-and- response, as well as a persistence simulation.

Practical steps to follow:

a. Set up and utilize Metasploit or Caldera tools for attack simulation.

b. Develop a collection of attack situations covering various threat types.

- Take out sensitive files from computer.
- Gaining privilege such as elevated access
- Repeated access (use of back doors)
- The lateral movement means to spread through the network.

c. Run the attacks as per the planned scenarios.

d. Keep an eye on attacks that affect sensitive data and the infrastructure.

3. Integrating the Created Infrastructure with Elasticsearch (Open-Source) to Monitor and Investigate Triggered Alerts During Simulated Attacks.

Practical steps to follow:

a. Set up Elasticsearch and connect it to the test layout.

b. Create a setup to visualize all alerts and incidents

c. See how the attacks affect traffic patterns.

d. Set up Beats and Elasticsearch monitoring agents in the built infrastructure to send logs to Elasticsearch.

4. Using Suricata or Snort to Create Optimized Detection Rules for the Simulated Attacks, Enabling Real-Time Detection from the Initial Malicious Attempts.

Practical steps to follow:

a. Create detection rules for the different types of simulated attacks.

b. Check and fine-tune the rules for a minimal number of false positives.

c. Assess the rule's efficacy through post-attack analysis and optimize them to cover multiple attack scenarios.

5. Evaluation and Validation of Results.

Practical steps to follow:

a. Look at results and compare with the published industry standards.

b. Record gaps in infrastructure and identified restrictions.

c. Provide suggestions for bridging the gaps.

6. ADVANTAGES OF THE PROPOSED SOLUTION

The solution put forward is very accessible and low-cost since it uses open-source tools like Metasploit, Caldera and Elasticsearch. Thus students, researchers and especially SMEs with limited budgets can run it without assembling large management teams. In addition, replication is also simple: the documentation allows academic institutions to reproduce the environment for cybersecurity courses and laboratories, educators are free to customize it according to different skill levels, and SMEs can roll it out in a phased manner even without a highly qualified IT staff by customizing ready to use scenarios and tuning the detection rules so that their personnel obtain practical experience in incident detection and response. The system can adjust and grow without issues. Companies can start with a small setup, then increase capabilities as their data volumes and budgets allow. Since you can use Elasticsearch to accommodate logs and monitoring data for companies of any size, you don't need to migrate to a different SIEM. Plus, you can update attack-detection rules all the time to cover new threats. In conclusion, the solution builds resilience for SMEs and academic institutions by quickly detecting and responding to attacks, as these targets often do not have authentication measures in place and store sensitive personal and financial information. Users can run attack simulations in-house, avoiding the external services costs.

7. COMPARATIVE ANALYSIS BETWEEN OPEN SOURCE PROPOSED SOLUTION AND EXISTING SOLUTIONS

To comprehensively evaluate the effectiveness of the proposed open-source cybersecurity solution, it is essential to compare it against existing industry-standard alternatives such as commercial SIEM platforms, managed security service providers (MSSPs), and endpoint detection and response (EDR/XDR) tools. This comparative analysis highlights critical evaluation criteria including: cost, technical complexity, scalability, detection and response capabilities, and overall suitability for small and medium-sized enterprises (SMEs). By contrasting these solutions, the study aims to objectively position the proposed approach within the broader cybersecurity landscape and demonstrate its practical viability.

7.1 Cost

Costs related to technology, especially software, play a major role in promoting the open source approach. An open source stack built on virtual machines that run Metasploit, the ELK stack and Suricata has no licensing fees, with each component being free and open source, costs arise only from the hardware, a multi-core CPU, 16–32 GB of RAM and SSD storage, and from the staff time needed to deploy and run it. Thus it is attractive to SMEs with very limited cybersecurity budgets. Provides zero recurring licence costs but requires in-house upkeep and know-how. Commercial SIEM platforms are those developed by external vendors. Examples include Splunk or QRadar. They usually charge a hefty upfront and on-going fee which scales with the log volume or ingestion rate. This pricing, along with the additional cost of infrastructure, vendor support and skilled resources, usually takes them out of bounds for smaller firms. When you use a managed security service provider, you pay them on a subscription basis. Usually, these rates can range between $3,000 to $30,000 per month, based on the bundle of services. Since the managed security service provider operates on a large scale, it is cheaper than deploying your security operation centre or SOC internally. Plus, managed security services spare the SME the hardware or software expense. Popular endpoint-centric EDR tools like CrowdStrike, Microsoft Defender or SentinelOne charge a predictable per-endpoint fee (roughly $60 to $185 per device per year). This per-endpoint fee is financially attractive to companies because they do not require on-premises infrastructure and costs scale neatly with the size of the company.

7.2 Technical Complexity and Expertise

The complexity of the integration as well as the expertise of the teams involved require moderate-to-high effort. Teams must integrate the parts, tune the detections, and have security and systems-administration skills. The teams rely mostly on the community to help them with any problems. Commercial SIEMs are difficult to use and need constant tuning and maintenance by experts or specialist knowledge. Using an MSSP places little technical burden on the client. The MSSP operates tooling and detection logic. The SME then communicates with analysts and implements recommended remediation. EDR/XDR products are low to moderate complexity: deployment is usually a light agent, detection is largely automated in the vendor's cloud console, and even a small IT or security team can ultimately administer them.

7.3 Scalability

An open-source stack can scale flexibly, but only with manual intervention such as adding virtual machines and expansion of storage, and the necessary adjustment of log pipelines. As such, scaling consumes additional technical effort. Commercial SIEMs are built for corporate growth but scaling them brings new costs and operational complexity. MSSPs use capacity so easily for the client, because the provider adds capacity behind the scenes as the org expands. EDR/XDR platforms that are built cloud natively scale effortlessly with the endpoints, and adding or removing devices from that environment is easy.

7.4 Detection and Response Capabilities

The open-source combo shines for signature-based network detection. This combo has limited behavioural analytics, and has no in-built automated response. So, incident handling is manual. A commercial application of SIEM allows for investigation of visibility and correlation detection most often coupled with SOAR tooling for a response action that's partially automated. Most MSSPs offer experts to monitor systems all day every day, with police-style powers to take active measures. Modern EDR/XDR suites currently utilizes behavioral and machine-learning techniques that deliver high-fidelity detection, support real-time automated containment and investigation and, when extended to XDR, provide coverage against attacks on multiple vectors beyond just the endpoint.

7.5 Suitability for SMEs

An open source solution is good for any small or medium enterprise with very tight budgets but reasonable technical knowledge and prefer to use it, learn and control it on their own. All commercial products probably don't fit small businesses because of price and complexity. But a mid-sized organisation with a compliance mandate, dedicated staff and budget might. MSSPs are the best choice for SMEs that lack in-house talent due to having outsourced the complexity in the process, remaining scalable and professional. EDR/XDR systems are perfect for SMEs since they have quick deployment, easy running, enterprise-grade endpoint protection at a predictable cost and require minimum training.

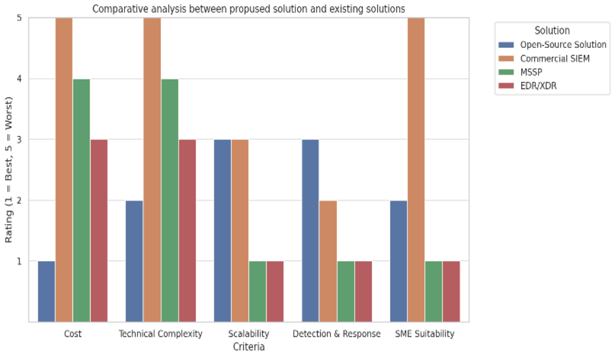

Figure 4. Comparative analysis: Proposed solutions and existing solutions

8. MINIMUM TECHNICAL REQUIREMENTS FOR BUILDING THE INFRASTRUCTURE

When creating a cyber security lab, we start off with a workstation with modern multi-core processors like Intel 12th and 13th generation or similar to run multiple virtual machines simultaneously without slowing down the system. A workstation should have at least 16 GB of RAM, but 32 GB (or more) is much better if you expect to keep around 10 VMs running at once. The more memory we have, the less the OS has to swap to disk, which is especially important if you're monitoring traffic or logs in real-time. SSDs are almost a must for storage these days: an NVMe drive delivers read/write speeds in the thousands of MB/s, compared with about 100 MB/s on a spinning hard drive. These quicker I/O speeds make a noticeable difference when VMs are constantly reading their disk images (in traffic replay, log indexing, and vulnerability scans). We should get an SSD of 500GB because anything above 1TB will give our lab room to grow.

Oracle VirtualBox is an easy and free tool for hosting our VMs on Windows, macOS and Linux. The user interface is simple enough to set up a lab whizzes by but still offers snapshots, multiple network modes (NAT, bridged, host-only), and Guest Additions for shared folders and dynamic screen sizes. It has enough functionality to serve most security-testing scenarios without the licensing costs of commercial hypervisors.

The cybersecurity lab which protects sensitive data must use the OS which is relevant for industry use. In order to enable better security testing we can use both Windows and Linux. If we are using Windows, we should use 64-bit Windows 10 Pro or Enterprise version. Windows 10 still accounts for approximately 65–70% of all deployed Windows desktops. It is compatible with a large variety of security tools and, crucially, unlike the Home editions, it contains essentials such as BitLocker for full-disk encryption. Windows 11 does add security features like TPM 2.0 requirements and VBS by default. However, many documented exploits and attack techniques still target Windows 10. Therefore, Windows 10 is the more valuable target platform.

We should choose distributions for Linux according to their intended purposes. Kali Linux is the standard in the industry for attacker or red-team VMs. It is a Debian-based distro that comes pre-loaded with more than 600 penetration-testing tools. As such, we can start testing immediately with Kali Linux. Ubuntu Server LTS is a good choice for servers and monitoring boxes due to its long-term support, good community support, robustness, and flexibility. As it is open-source, many use it and find many vulnerabilities which soon gets patched. Its scripting and automation help a lot during the incidents also.

9. LIMITATIONS OF OPEN SOURCE PROPOSED SOLUTION

While the open-source solution is a low-cost means for SMEs to tackle cybersecurity issues, it also comes with restrictions that must be considered. It is useful to categorize the limitations into technical, financial and organizational to assess its practicality and long-term viability. Overall, it shows both the strengths of the approach and the scope for the future. [17][18]

From a technical perspective, the coverage is limited mainly to signature detection (e.g. Snort), which means that unknown (zero-day) or very sophisticated attacks can escape detection. The platform can't see encrypted traffic, like HTTPS, unless further complex configuration is added. Moreover, its default rules produce a large number of false-positive alerts that must be painstakingly tuned out. Every part (the virtual machines, the ELK stack and the IDS) must be installed and configured by hand, with no vendor help; troubleshooting depends on forums or in-house expertise. [7]

Regarding the financial aspect, the "free" software hides hardware prices, because the system still needs a powerful multicore processor, 16-32 GB of RAM and solid-state storage - burdening a micro-business. Another indirect cost is the staff time . A significant build investment is required, along with constant updating of rules and regular maintenance. When a corporation lacks internal know-how, it may need to hire third-party experts. Moreover, unlike product sales, there are no service level guarantees or damage coverage with the setup deal [7].

From an organizational viewpoint, the platform only works if there's at least one mid-level IT security specialist in place tasked with running it and keeping it maintained; its value can fall quite steeply should that person leave. Due to a lack of automated tools or pre- configured playbooks, human operators must take every containment or remediation step. In addition, the business must formalize procedures to review alerts, respond to incidents, and update detection rules. [16][17]

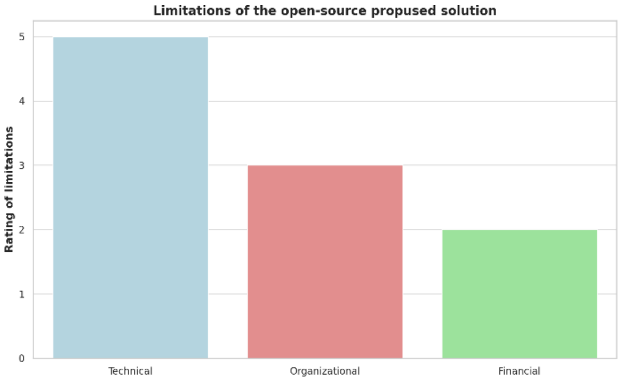

Figure 5. Limitations of open source proposed solution [17]

10. CASE STUDY: PHISHING ATTACK SIMULATION

1. Company Profile:

A financier firm with almost 200 employees managing sensitive data (financial and personal information) of their clients.

2. IT Infrastructure:

A combination network containing Windows systems (for workstations and application servers) and Linux systems (for web and monitoring servers). Initially, it depended on commercial security solutions, but limited funds have now led it to pursue an open-source option.

3. Attack Scenario

The objective of this simulation is to penetrate the systems of the company by means of a traditional phishing attack with an infected attachment. The private IP address of the target computer 192.168.1.50 belongs to the organization.

Email Used in the Simulation:

Subject: Important Notice - Service Disruption. Dear valued customer,

Your recent purchase has just had its invoice updated. To check the details and make sure the information is correct, please download your updated invoice. This update must be performed urgently to avoid any service interruption.

Download: Updated_Invoice.exe. Thank you.

Customer support team.

This email is sent in a controlled testing environment (eg, email address created especially for lab exercise) the virtual machine that simulates the victim system.

4. Simulation Objective

The aim is to check that when the user downloads the file, and runs it, the handler of Metasploit takes over the session, and the monitoring (ELK Stack) and Suricata detection rule (configured to alert the download of .exe file and MZ signature) triggers alerts.

The “msfvenom” tool is used to create a malicious executable file (payload) which opens a Meterpreter session (reverse shell) back to the attacker when run.

5. Command line:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.50 LPORT=4444 -f exe -o Updated_Invoice.exe. This command creates an executable "Updated_Invoice.exe" file. Once we run this file, it creates a reverse shell to the 192.168.1.50 IP on port 4444. The “Updated_Invoice.exe” file is created using msfvenom with a payload like windows/meterpreter/reverse_tcp so that when the file is executed the target system, a Meterpreter session is opened to your configured handler.

6. Configuring the Handler in Metasploit:

Launch “msfconsole” and configure a handler for the generated payload.

```
“msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp set
LHOST 192.168.1.50
set LPORT 4444
exploit -j”
```

A handler that listens at address 192.168.1.50:4444. As soon as the victim runs the malicious file, whomever is accessing the handler will get the Meterpreter session. Suricata can be configured with detection rules to identify suspicious activity, such as downloading a malicious file.

7. The Rule:

Alert http any -> (msg:"Potential malicious file download detected - executable file”; flow:established,to_server; fileext:"exe"; content:"MZ"; offset:0; classtype:trojan-activity; sid:100001; rev:1;)

8. Explanation for the rule

msg: The alert message which will appear on your screen.

flow: indicates that the traffic will flow from the client to the server, on a fixed connection

fileext:exe: See if the downloaded file extension contains exe. content:"MZ"; offset:0 will check the first two bytes of the file and see if they are “MZ”.

classtype: Alert category (malware)

the “sid” represents an unique member or identifier for the rule

rule: Rule review

the local rules file is where you will add this rule to Suricata, after which you will be restarting Suricata for the change to load. After Suricata finds the download of the bad file, an alert goes to Elasticsearch and is visible at Kibana. An alert of this type would appear as follows.

Alert title: Potential malicious file download detected - executable file

Timestamp: 2023-08-15T14:22:35Z

Source IP: 192.168.1.110

Destination IP: 192.168.1.50

SID: 100001

Details: Additional information can consist of URL visited, user agent and other information.

When investigating in Elasticsearch, the following flow must be followed.

a. Look through suspicious data traffic that was recorded on the private IP.
b. Analyze the malicious file
c. Erasing File from Device
d. Check if there are any other suspicious files present in the device.

e. See if there are any changes in the registry keys or the Windows Registry.
f. To demonstrate the malicious action, show a copy of the malicious file.
g. Use the local scanning solution (e.g., Windows Defender) to scan the device.

This case study provides a practical demonstration of how a virtual structure, attack simulations using Metasploit, tracking with Elasticsearch and detection using Suricata can contribute to the improvement of SMEs cyber-resilience. By detecting attacks early on and analyzing incidents in a coordinated manner, organizations can minimize the financial and operational repercussions of cyberattacks. The findings indicate that the SMEs could enjoy advanced protection at a low cost by adopting this solution, which represents a feasible alternative to a commercial one..

11. CONCLUSIONS

The number of cyberattacks globally has increased in recent years, and this upward trend is expected to continue in the coming years. The financial losses and consequences following a cyberattack are significant for companies and, in extreme cases, can even lead to bankruptcy. Phishing remains a primary vector for initiating security breaches, exploiting human weaknesses and lack of security training, while ransomware has become one of the costliest types of incidents, affecting both large companies and SMEs.

The results of this research show that preventive protection systems should be taken as follows: carrying out simulated attacks in a lab to check vulnerabilities and assess the defense mechanism, monitoring everything from one place and checking the logs all the time to catch problems fast and applying real-time detection and response solutions ensures prompt intervention in case of an incident to limit financial and operational damage.

The proposed solution is optimal for SMEs with limited budgets. It requires low to moderate time for implementation, low costs, and moderate technical expertise (for configuration). The solution is scalable, allowing SMEs to start with a minimal configuration and expand it as data volume and organizational resources grow. The solution cannot be implemented or tested in a test environment/infrastructure that does not meet the minimum configuration and operational requirements.

REFERENCES

[1] Stallings, W. (2020). *Network Security Essentials: Applications and Standards, in English (Network Security Essentials),* Pearson, ISBN 9780134527338, Boston

[2] Andress, J. (2021). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, in English (The Basics of Information Security),* Syngress, ISBN 9780128007440, Amsterdam.

[3] Enoka, S. (2019). *Cybersecurity for Small Networks, in English (Cybersecurity for Small Networks)*, Packt Publishing, ISBN 9781789809015, Birmingham.

[4] *https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report Accessed*: 2025-03-20

[5] *https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf Accessed:* 2025-03-20

[6] *https://industrialcyber.co/reports/fbis-internet-crime-report-2024-records-16-6-billion-in-cybercrime-losses-amid-rising-ransomware-threats/ Accessed*: 2025-03-20

[7] Meeuwisse, R. (2017). *Cybersecurity for Beginners, in English (Cybersecurity for Beginners),* Cyber Simplicity Ltd., ISBN 9781911452034, London

[8] Grimes, R.A. (2017). *Hacking the Hacker: Learn from the Experts Who Take Down Hackers, in English (Hacking the Hacker)*, Wiley, ISBN 9781119396215, Indianapolis

[9] Kim, D., Solomon, M. (2016). *Fundamentals of Information Systems Security, in English (Fundamentals of Information Systems Security),* Jones & Bartlett Learning, ISBN 9781284116458, Burlington

[10] Skoudis, E., Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, in English (Counter Hack Reloaded),* Prentice Hall, ISBN 9780131481046, Upper Saddle River

[11] Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, in English (Countdown to Zero Day),* Crown Publishing, ISBN 9780770436179, New York

[12] Verizon. (2025). *2025 Data Breach Investigations Report,* available at*: https://www.verizon.com/business/resources/Tb77/reports/2025-dbir-data-breach-investigations-report.pdf Accessed:* 2025-05-24.

[13] Handa, A., Negi, R., Venkatesan, S., Shukla, S.K. (2023). *Implementing Enterprise Cyber Security with Open-Source Software and Standard Architecture: Volume II,* River Publishers, ISBN 9788770227950, Gistrup, Denmark.

[14] Stellar Cyber. (2023). *Open XDR vs. SIEM: Choosing Cybersecurity Solutions*, available at: *https://stellarcyber.ai/open-xdr-vs-siem/ Accessed*: 2025-05-24.

[15] Seceon. (2022). *Comparing SIEM Solutions: Advanced Security Analytics Platforms*, available at: *https://seceon.com/comparing-siem-solutions-advanced-security-analytics-platforms/ Accessed*: 2025-05-24.

[16] Ishikawa, T. (2024). *Public and Private Governance of Cybersecurity: Challenges and Potential Solutions*, Cambridge University Press, ISBN 9781009374530, Cambridge

[17] Negg Blog. (2023). *Cyber security open source: advantages and limitations,* available at*: https://negg.blog/en/cyber-security-open-source-advantages-and-limitations/ Accessed*: 2025-05-24.

[18] SentinelOne . (2023). *13 Open Source Software Security Risks,* available at: *https://www.sentinelone.com/cybersecurity-101/cybersecurity/open-source-software-security-risks/ Accessed:* 2025-05-24.

Author:
Eng. Mariana-Luminița ACHIM, PhD Student,
Industrial Engineering and Robotics Doctoral School,
National University of Science and Technology
Politehnica Bucharest, E-mail:
achim.luminita@yahoo.com