

# Fortifying the digital fortress: A multi-layered defense strategy with SIEM, mail gateway, and sandbox technologies

Maksim Iavich<sup>1,†</sup>, Giorgi Akhalaia<sup>1,†</sup>, Roman Odarchenko<sup>2,\*†</sup> and Ana Imnadze<sup>3,†</sup>

<sup>1</sup> Caucasus University, Paata Saakadze Str., 1, Tbilisi, 0102, Georgia

<sup>2</sup> National Aviation University, Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

<sup>3</sup> Georgia Liberty Bank, Ilia Chavchavadze Ave., 74, Tbilisi, 0162, Georgia

## Abstract

Defending organizational assets against cyber threats has become a necessity, and relying on single-layered defense mechanisms is no longer viable. This research paper emphasizes the importance of data analysis within a multi-layered security framework that integrates Security Information and Event Management (SIEM), Mail Gateway, and Sandboxing technologies. By leveraging data analysis, SIEM systems continuously monitor network activity to detect signs of compromise in real-time, analyzing vast amounts of security data to identify patterns and anomalies. Mail gateways utilize data filtering techniques to block malicious attachments and links, preventing users from inadvertently downloading harmful content. Sandboxing offers a controlled environment where potentially harmful files can be executed and analyzed, allowing for data-driven insights into their behavior before they enter the network. This comprehensive approach enhances the organization's ability to respond to cyber threats through better data collection and analysis, improving threat detection and prevention. The paper explores how these systems interact operationally, highlighting best practices for effective data integration and analysis, as well as the challenges organizations may face during implementation.

## Keywords

multi-layered security, security information management, mail gateway, sandbox technology, cyber defense, threat detection, security integration, incident response, threat prevention

## 1. Introduction

In the current digital landscape, defending organizational assets against cyber threats became a critical necessity. Single-layered defense mechanisms are inadequate to provide the level of protection required in today's complex threat environment. This research paper introduces a multi-layered security framework, with a strong emphasis on the role of data analysis in enhancing overall security effectiveness.

The objective of this study is to demonstrate how the integration of Security Information and Event Management (SIEM), Mail Gateway, and Sandboxing technologies can create a robust defense against cyber threats. By leveraging data analysis, organizations can improve their detection, prevention, and response capabilities.

SIEM systems play a pivotal role in this framework by continuously monitoring and analyzing large volumes of security data from various sources. Through the identification of patterns and anomalies, SIEM enables real-time detection of potential threats, allowing organizations to respond swiftly. Meanwhile, Mail Gateways utilize data filtering techniques to block malicious emails and attachments, reducing the risk of user exposure to harmful content. It must be mentioned that,

---

*ADP'24: International Workshop on Algorithms of Data Processing, November 5, 2024, Kyiv, Ukraine*

\* Corresponding author.

† These authors contributed equally.

✉ miavich@cu.edu.ge (M. Iavich); gakhalaia@cu.edu.ge (G. Akhalaia); odarchenko.r.s@ukr.net (R. Odarchenko); a\_imnadze@cu.edu.ge (A. Imnadze)

ORCID: 0000-0002-3109-7971 (M. Iavich); 0000-0002-4194-2681 (G. Akhalaia); 0000-0002-7130-1375 (R. Odarchenko); 0009-0003-5419-0284 (A. Imnadze)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

Sandboxing provides a controlled environment for analyzing suspicious files, enabling organizations to gain insights into potential threats before they enter the network. This multi-layered approach, driven by robust data analysis, not only enhances the organization's security posture but also complicates attackers' efforts to succeed.

This paper will discuss how these systems operate synergistically, highlight best practices for effective data integration and analysis, and discuss the challenges organizations may encounter during implementation. By focusing on a data-centric approach to multi-layered security, we aim to illustrate how innovative strategies can significantly strengthen defenses against evolving cyber threats, ultimately paving the way for a more resilient digital infrastructure.

## 2. Literature overview

The world of cybersecurity encompasses the interconnected environment where digital interactions occur, with networks, systems, and technologies working together to form a complex, vulnerable ecosystem. Experts emphasize the importance of protecting these assets from ever-evolving cyber threats, as the cybersecurity landscape continuously changes, bringing new vulnerabilities and risks to the forefront. In recent years, literature has increasingly focused on proactive security measures and groundbreaking advancements in defense strategies. Scholars underscore the significance of safeguarding critical assets, establishing a foundation for understanding the challenges involved in pioneering cyber sentinel strategies [1, 2].

A key narrative in the literature is the evolution of cyber threats from basic attacks to today's highly sophisticated threat landscape, highlighting the necessity of adapting security approaches to counter these emerging dangers effectively.

Cutting-edge innovations in cybersecurity, such as integrating threat intelligence and employing anomaly detection, have become central to this adaptive approach. The field has witnessed a paradigm shift toward proactive defense measures, with organizations actively seeking solutions to preemptively address potential cyber threats [3, 4]. However, despite notable progress in the cybersecurity field, gaps and challenges persist in current strategies. Traditional, reactive security measures often have limitations, and addressing these gaps is essential for successfully implementing innovative defense techniques. This comprehensive literature review lays the groundwork for exploring new proactive security defense methods by merging insights into the cyber threat landscape, the evolution of current defense mechanisms, proactive strategies, and the challenges of this dynamic field [5, 6].

One prominent area of focus in recent cybersecurity advancements is the integration of multiple security technologies, which has proven instrumental in strengthening defenses. Security Information and Event Management (SIEM) systems, for instance, have seen significant development [7]. Modern SIEM platforms now aggregate and analyze security data from various sources, offering enhanced data correlation, real-time monitoring, and automated responses, which improve threat detection and response capabilities. The integration of machine learning and advanced data analytics in these systems enables faster, more precise identification of threats and streamlined incident responses.

Similarly, mail gateway technologies have evolved to incorporate artificial intelligence (AI) and machine learning techniques to better manage email-borne threats like phishing, spam, and malware. These advancements have resulted in more accurate filtering and a reduction in false positives, ultimately enhancing email security. In parallel, sandbox technologies have progressed, with recent innovations enabling the isolated analysis of suspicious files to detect and understand sophisticated malware behaviors. Dynamic analysis capabilities now provide detailed insights into malicious activities, helping to prevent threats before they reach core systems.

Recent studies highlight the improvements in the effectiveness of SIEM systems through the integration of advanced analytics and machine learning, leading to refined threat detection and accelerated response times [2, 8]. Similarly, the application of machine learning in mail gateways has demonstrated higher accuracy in identifying email-borne threats, helping to mitigate potential

attacks more effectively. Sandboxing has also benefited from advancements in dynamic analysis techniques, improving the detection and understanding of novel malware and its impacts.

However, there remains a notable gap in research exploring the combined efficacy of integrating SIEM systems, mail gateways, and sandbox technologies within a comprehensive, multi-layered security strategy [9]. Most studies examine these technologies in isolation or within limited contexts, thus providing limited insight into their potential synergy. More practical research is needed to assess the challenges and benefits of deploying these technologies together in real-world environments. Understanding their combined impact could enhance cybersecurity defense frameworks by leveraging the unique strengths of each technology, thereby enabling organizations to develop a more resilient, adaptive approach to cyber threats. This exploration of multi-layered security strategies offers valuable insights into the complex and changing world of cybersecurity and the need for innovative approaches to combat the evolving threat landscape effectively.

### 3. The novelty and distinctiveness of this research

Our study presents an innovative framework that combines SIEM, mail gateways, and sandbox technologies in a manner that has not been explored in the literature extensively. The existing trend of considering these technologies as separate entities is reversed by our proposed model, which looks into their joint effect on security operations to prove the concept of how they can better mitigate emerging cyber threats that are complex. This represents a fresh perspective toward understanding and improving multilayered security strategies with insights from recent developments within each technology.

We use a multidimensional methodology incorporating empirical studies, simulations, and comparisons. This holistic approach enables us to evaluate the individual performance of every technology as well as integrated efficiency. Our research calls for contemporary advancement and empirical data to test our hypothesis that suggests improved detection of threats, faster response time to attack occurrence, and also higher level of overall security. This methodological strictness makes our study stand out against others that may only be based on theoretical models or solitary case analyses. Our study is intended to close the space between theoretical investigation and pragmatic application by offering practical advice and ideas for fusing SIEM, mail gateway, and sandbox. This research critically analyses the advantages and disadvantages of each technology as well as its use together hence providing useful guidance for security professionals and organizations looking to implement strong multi-layered security solutions. In response to such gaps in literature, this study therefore offers an evidence-based approach to addressing cyber security issues.

Our research contributes to the academic field in addition to its practical implications by expanding the understanding of how integrated security technologies can work together to improve overall security. These new methodologies and frameworks provide a basis for future studies in this area. Academics and researchers can take our findings further, for instance, this could involve looking at how emerging technologies are affecting integrated security solutions or developing advanced threat modeling techniques. Our research enhances theoretical as well as empirical knowledge on cybersecurity thus supporting the need for effective and innovative security strategies that will address dynamic cyber threats environment.

### 4. Cyber threat landscape analysis

An in-depth examination of emerging risks is necessary since hostile actors' techniques are evolving along with technology. The ensuing segments offer an all-encompassing synopsis of cyber hazards, their possible consequences, and preemptive steps toward alleviation. Considering the scope of the cyber realm, a variety of cyber-attacks exist, including [10–12]:

1. Malware Attacks is a common hazard to digital ecosystems is malware, an acronym for malicious software. Three of the most common types of malware are viruses, trojans, and ransomware, and each has unique traits. Viruses replicate and spread by attaching themselves to

host programs, while Trojans disguise themselves as legitimate software to create clandestine backdoors. Ransomware, on the other hand, encrypts files or systems, demanding a ransom for their release. It is essential to comprehend the subtleties of these hostile agents to develop defense measures that work.

2. Social Engineering Attacks. Social engineering attacks rely on manipulation to trick people or groups into revealing information granting unauthorized access or carrying out actions that could jeopardize security. Unlike cyber threats that exploit weaknesses, social engineering takes advantage of the trust, curiosity, or fear present, in human interactions to accomplish nefarious goals. Categories of Social Engineering Attacks:

- Phishing refers to attempts through email where the sender disguises themselves as a source enticing the recipient into clicking on harmful links providing login details or downloading malicious attachments.
- Spear phishing involves phishing attacks targeting individuals or organizations. These attacks often utilize information to increase their chances of success.
- Baiting involves offering something like a free software download or a USB drive labeled as a prize to trick individuals into compromising their security.
- Pretexting is when someone creates a scenario or pretext to manipulate individuals into revealing information. This is often done by pretending to be someone in a position of authority.
- Quid pro quo refers to exploiting the nature of interactions by offering a service or benefit in exchange, for sensitive information.

3. Denial of Service (DOS) and Distributed Denial of Service (DDoS) Attacks. The immense impact of DoS and DDoS attacks should not be underestimated. These attacks overload systems, networks, or websites, by flooding them with traffic leading to disruptions, in their operations. In today's interconnected world, the consequences of these disturbances are felt across industries. It is essential to understand the complexities of these attacks to develop infrastructures that can withstand the onslaught of malicious traffic.

4. Man-In-the-Middle (MitM) Attack. These attacks are a particularly dangerous type of cybersecurity threat because they take advantage of flaws in digital communication. A MitM attack, as the name suggests, occurs when an unauthorized third party secretly intercepts and may alter communication between two parties without the parties' knowledge. The confidentiality and integrity of the exchanged information may be jeopardized if this covert intermediate surreptitiously monitors, modifies, or inserts malicious stuff into the communication stream.

5. Zero-Day Exploits. Zero-day exploits are a type of cybersecurity threat that emerges from weaknesses, in software or hardware to developers or the general public. The term "zero day" indicates that attackers take advantage of these security vulnerabilities as soon as they discover them leaving no time for the targeted party to protect themselves or address the problem.

6. Insider Threats. Within the landscape of cybersecurity insider threats pose a challenge that requires a deep understanding of the human factor in the digital world. Insider threats encompass situations where individuals who have authorized access to an organization's systems exploit that privilege for purposes. These threats can arise from misconduct or unintentional actions caused by negligence creating a multifaceted security landscape. Different types of insider threats are:

- Malicious Insiders. These are individuals who intentionally seek to compromise an organizational asset. Motivations behind their actions may include profit, and revenge or they may be driven by ideologies.
- Negligent Insiders. This category includes employees who unknowingly compromise security through actions or lack of awareness regarding established protocols. Data breaches or unknowingly sharing sensitive information fall under the above-mentioned category.

- Compromised Insiders. These employees have had their credentials or access rights compromised often unknowingly becoming victims of threats.

7. Advanced Persistent Threat (APTs). Advanced Persistent Threats (APTs) are. Well-financed and organized entities carry out targeted cyber-attacks. These adversaries establish a lasting presence, within a network often going undetected for extended periods. The main goals of APTs involve gathering intelligence stealing data and infiltrating vital systems.

8. IoT Threats. The security risks associated with the Internet of Things (IoT) cover a range of vulnerabilities in how interconnected devices are designed deployed and managed.

- Insecure Hardware. IoT devices often lack built-in security controls due to computational and power limitations.
- Maintenance and Update Challenges. Difficulty in maintaining and updating devices creates security vulnerabilities. Connectivity limitations and outdated device models contribute to update challenges.
- Poor Asset Management. Nearly 48% of devices in organizations are at risk due to outdated operating systems or undetected status.
- Shadow IoT. Unsanctioned IoT devices deployed without official support create security risks. Lack of monitoring and awareness by IT teams increases the likelihood of breaches.
- Unencrypted Data Transmission. The majority of IoT device traffic is unencrypted, exposing personal and confidential data.
- IoT Botnets. Botnets target IoT devices for DDoS attacks due to weak security configurations.

These threats take advantage of weaknesses, within ecosystems, which can put data privacy, network integrity, and even physical safety, at risk. The changing nature of IoT adds to the complexity of these threats requiring analysis to develop effective countermeasures [13].

9. Cloud Security Threats. Threats to cloud security encompass a wide range of hazards related to using cloud computing services. These attacks take advantage of vulnerabilities in the cloud architecture, jeopardizing the availability, confidentiality, and integrity of data and apps housed there, from configuration errors to highly skilled cyberattacks. Categories of Cloud Security Threats:

- Data breaches occur when sensitive data stored in the cloud is accessed without authorization. This often happens due to access control misuse, weak authentication methods, or compromised credentials.
- Misconfigurations of cloud settings and permissions can unintentionally expose data creating vulnerabilities that attackers can exploit to gain entry.
- Insecure interfaces and APIs within applications are a target, for actors who seek unauthorized access. They can use these vulnerabilities to execute commands or manipulate data within the cloud environment.
- Identity and access management (IAM) practices can lead to access to cloud resources. This allows attackers to impersonate users and compromise information.
- Denial of service (DoS) attacks overload cloud services with traffic resulting in service disruptions and impacting the performance of applications hosted in the cloud.

10. Mobile Security Threats. These threats cover a range of risks that specifically target smartphones, tablets, and other portable devices. These threats take advantage of weaknesses within the mobile ecosystem compromising the privacy of users the integrity of data and overall device security. From malware attacks to insecure applications, mobile security threats require vigilance to protect the information that is processed and stored on these devices.

11. Wireless Network Attacks. Attacks on networks involve cyber threats that specifically target the vulnerabilities found in wireless communication protocols. These attacks take advantage of weaknesses in Wi-Fi networks resulting in compromised data confidentiality and integrity when

transmitted through the airwaves. From intercepting information on networks to executing exploits, it is crucial to adopt a proactive and watchful mindset to protect the integrity of wireless communication channels. Different Types of Wireless Network Attacks:

- Eavesdropping refers to the interception of communication, where attackers capture and analyze data transmitted over unsecured Wi-Fi networks. This can potentially lead to unauthorized access to sensitive information.
- Spoofing involves impersonating a Wi-Fi network to deceive devices into connecting to an access point. This can give rise to Man in the Middle (MitM) attacks and unauthorized interception of data.
- Denial of Service (DoS) Attacks aim at overloading networks with traffic disrupting normal operations and rendering the network unavailable for legitimate users.
- Cracking Wi-Fi Encryption. This type of attack exploits vulnerabilities in Wi-Fi encryption protocols such as WEP or WPA allowing access, to the network and compromising data confidentiality.
- Rogue access points are access points introduced into a network, which can serve as channels for attackers to infiltrate and compromise the security of connected devices.

## 5. Security measures

### 5.1. Traditional security measures

In today's evolving cyberspace, protecting digital assets against a vast array of cyber threats is crucial. Traditional cybersecurity measures have long served as the backbone of defense, but the rapid growth of technology and complex interconnectivity call for a re-evaluation of their effectiveness. This paper reviews foundational tools and strategies in cybersecurity to understand their relevance in our modern digital landscape.

1. Firewalls act as a security barrier between trusted and untrusted networks, filtering data packets to prevent unauthorized access and protect against cyber threats.
2. Antivirus Software scans for and isolates malicious threats like viruses and ransomware, ensuring ongoing computer security.
3. Encryption Protocols safeguard communications by encoding data, using SSL/TLS, SSH, and IPsec to protect against unauthorized access.
4. Intrusion Detection Systems (IDS) monitor network activity, detecting suspicious behaviors through either host-based or network-based monitoring.
5. Access Control Mechanisms regulate user permissions, incorporating multi-factor authentication and role-based access control to prevent unauthorized access.
6. Virtual Private Networks (VPNs) ensure secure, encrypted online communication, offering anonymity, privacy, and protection on public Wi-Fi, while also enabling remote access [14-17].

These traditional security tools remain essential but must continuously adapt to address the complex challenges in today's cybersecurity landscape.

### 5.2. Reactive approaches

In the ever-changing cybersecurity field, responding to security incidents is critical to minimize impact and restore system integrity. Reactive strategies are essential for detecting, managing, and resolving breaches.

1. Incident Detection and Response involves monitoring for unauthorized access and suspicious activities. Once detected, teams work to investigate, contain, and eliminate threats, forming the foundation of incident response frameworks.

2. Forensic Analysis and Attribution helps understand the breach's nature, extent, and the attacker's identity. Techniques like log and malware analysis are used to reconstruct events and gather insights for future prevention.
3. Remediation focuses on addressing vulnerabilities by patching, removing malware, and restoring affected systems to secure states, reducing future risks.
4. Communication with employees, customers, regulators, and the public is crucial. Transparent and timely communication helps manage reputational damage and maintains trust with stakeholders.

These reactive steps are vital in restoring security and preventing future incidents.

### 5.3. Limitations of reactive approaches

Cybersecurity is rapidly evolving, yet reactive strategies have significant limitations as they often require organizations to catch up to cyber threats.

1. Time Lag in Detection. Delays between incident occurrence and detection give attackers time to exploit vulnerabilities, hindering timely response.
2. Dependence on Past Data. Reactive methods rely on known attack patterns, limiting effectiveness against new or modified threats that evade detection.
3. Zero-Day Vulnerability. Reactive strategies struggle with zero-day exploits, where unknown vulnerabilities are exploited, highlighting the need for proactive measures.
4. Complex Remediation. Addressing incidents involves forensic analysis and corrective actions, which are time-intensive and can delay recovery.
5. Resource Strain & Alert Fatigue. Managing frequent alerts can exhaust resources, risking missed threats among false positives.
6. Lack of Root Cause Analysis. Reactive approaches focus on containment but often neglect underlying vulnerabilities, risking repeated incidents.
7. Regulatory and Reputational Risks. Delays in detection can increase breach impacts, leading to regulatory penalties and reputational damage.

These limitations underscore the need for proactive measures to reduce incident frequency and impact.

### 5.4. Proactive security defense innovations

In cybersecurity, moving beyond reactive defenses has become essential to stay ahead of threats. This shift toward proactive strategies focuses on advancements that help predict and adapt to evolving cyber risks, fostering resilience and strategic defense.

Threat Intelligence Integration. Effective security relies on integrating threat intelligence, which provides insights into emerging threats, tactics, and vulnerabilities. This foresight enables defenders to bolster defenses before attackers exploit them. Threat intelligence is categorized into three types:

1. Strategic Intelligence: Offers high-level insights on geopolitical and economic factors influencing cybersecurity, aiding long-term security planning.
2. Operational Intelligence: Provides specific information on active threats, refining security policies for current risks.
3. Tactical Intelligence: Delivers detailed data on threats, including attack patterns and malware signatures, essential for immediate incident response.

Common tools include MISP (Malware Information Sharing Platform) and OSINT tools like Shodan and Maltego. These resources empower organizations to anticipate and counteract potential cyber threats effectively.

## 6. Research results

The current state of cybersecurity architecture demands security information and event management (SIEM) systems, which provide a centralized way to gather, examine, and manage safety data. In real time, SIEM solutions collect logs as well as events from the IT environment of an organization hence monitoring potential threats that may occur. The ability of SIEM technologies to detect threats depends on their capacity for correlating enormous amounts of data to discover anomalies, patterns, and alerts for possible security incidents. One of the most prominent features of SIEM technology is its capability to connect information from different sources including network gears, and servers among others. With analysis being made through logs and events, SIEM applications can identify complex attack patterns which might be difficult if considered separately. For example, through using correlation rules and algorithms, these systems are capable of detecting indicators that present compromise; this could be IoCs or behaviors that indicate potential vulnerabilities. An enhanced form of correlational matching is available in current SIEM technology that can more accurately detect advanced persistent threats (APTs), insider attacks, and other sophisticated intrusions.

While the SIEM systems and SMG are some of the most significant aspects of a good cybersecurity infrastructure, on their own, they are still not able to be a full defense against the entire spectrum of cyber threats. Aggregating and correlating security event data, SIEM is good at it. Filtering and blocking malicious emails, SMG is good at it. However, in many cases, advanced threats bypass these defenses and would require more tools and services to integrate for effective countermeasures.

For example, open-source IP checker tools are extensively used in identifying and blocking known sources of malicious activities by IP address. These, integrated with SIEM and SMG, enhance better detection and response capability through real-time intelligence on harmful IP addresses. In this regard, threats are identified and neutralized before any entry into networks.

This would also necessitate sandboxing services that isolate suspicious files and URLs to be analyzed in a secure environment (Figure 1), thereby enabling security teams to understand the behaviors of the content without jeopardizing the network's integrity. Such sandboxing capability accomplishes the detection of zero-day exploits and other sophisticated malware that may bypass traditional defenses, such as SIEM and SMG through the leverage of sandboxing (Figure 2). Sandboxing then brings an extra layer of analysis that augments the larger threat detection of SIEM and the email filtering of SMG. The corresponding behavioral indicators are shown in Figure 3.



Check IP Reputation for 202.6.215.3	
IP Address	202.6.215.3
Proxy/VPN Detection Check	 <b>Reputation Issues Detected</b> This IP address has been detected as a proxy connection, which could be hurting your IP reputation.
IP Reputation Score	65% - Suspicious IP
Blacklist Checks	IP blacklist check passed, this IP address was not detected on popular blacklists
Country	ID 
CIDR IP Address Subnet	202.6.215.0/24

Figure 1: URL filtering.



Time	From	To	Original Subject	Verdict(s)	Action(s)
Thursday, Aug 01, 2024 06:36:48 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	[warning - attachment ...	Encrypted attachment	Deliver message normally
Thursday, Aug 01, 2024 06:36:39 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent.xlsx	Encrypted attachment	Modify the subject line
Thursday, Aug 01, 2024 06:36:39 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent.xlsx	Encrypted attachment	Modify the subject line
Thursday, Aug 01, 2024 06:09:47 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	[warning - attachment ...	Encrypted attachment	Deliver message normally
Thursday, Aug 01, 2024 06:09:47 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	[warning - attachment ...	Encrypted attachment	Deliver message normally
Thursday, Aug 01, 2024 06:09:46 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:45 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:45 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:36 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:36 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:36 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent	None	Deliver message normally
Thursday, Aug 01, 2024 06:09:36 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent.xlsx	Encrypted attachment	Modify the subject line
Thursday, Aug 01, 2024 06:09:36 AM AZT	layanan_tellex@bca.co.id	[REDACTED]	urgent.xlsx	Encrypted attachment	Modify the subject line

Figure 2: Sandboxing process.

Title	Categories	ATT&CK	Tags	Hits	Score
Document Created an Executable File	Phishing	Execution	dropper, obfuscation, phishing	4	90
A Document File Established Network Communications	Phishing	Command and Control	dropper	103	81
A PE Artifact has an Invalid Certificate Signature	Static Anomaly	Defense Evasion	artifacts, certificate, PE	1	80
Excessive Remote Process Code Injection Detected	Execution	Defense Evasion, Privilege Escalation	injection, memory, threshold	1	80
Excessive Number of DNS Queries	Domain	Command and Control	communication, dns, threshold	1	70
JavaScript Contains an Excessively Long String	Obfuscation	Defense Evasion	javascript, obfuscation	3	64
Email with Non-permitted Sender and Body Hash Error Detected	Information	Initial Access	HTTP, phishing	2	60
Outbound HTTP GET Request	Network Information	Command and Control	get, http, network	5	56
Process Modified File in a User Directory	Dynamic Anomaly	Discovery	executable, file, process	129	56
Process Uses Localhost for Network Traffic	Dynamic Anomaly	Discovery	communication, process	5	56
Executable Artifact has Misleading File Extension	Static Anomaly	Defense Evasion	PE	1	54
Office Document Requires Password	Static Anomaly	Defense Evasion	document, password	3	45
Email References Localhost in Received Message Trace	Information	Initial Access	phishing, social engineering, spam, suspicious	1	40

Figure 3: Behavioral indicators.

Hypothesis 1: Enhanced Threat Detection. It was an all-in-one solution: SIEM, mail gateways, open-source IP checker tools, and sandboxing services combined to offer threat detection capabilities well beyond the limits of a single technology. It was, in fact, the SIEM system and the SMG that provided the first alert and general information such as identification of malicious IP addresses and details of senders and recipients in practice. These tools alone could not give a deep understanding of the threat landscape. Open source tools gave more context and details that provided more information, helping in the identification of threats more accurately. For example, IP checker tools can give far more extensive history and reputation about the suspicious IPs, which was not available with only SIEM and SMG.

Hypothesis 2: Reduced Incident Response Time. Coupling sandboxing technologies with SIEM and SMG was important. It was the case that the SIEM and SMG systems flagged possible threats, but in most instances, it was the sandboxing that did an in-depth analysis of suspicious attachments, identifying them as highly critical with a score of 90. This gave detailed insight that enabled quicker decision-making and response actions. The sandboxing tool's ability to simulate a safe execution environment for the malicious payload evidenced the threat's nature and severity, instrumental in speeding up the incident response process. This multi-layered approach ensures that threats are not only detected but also quickly understood and mitigated.

## 7. Conclusions

This paper has evaluated the effectiveness of the multi-layer defense strategy using SIEM, Secure Mail Gateway, and sandbox technologies. The result reached is that while SIEM and SMG provide relevant information – identifying malicious IP addresses, sender details, and recipient information; they cannot work in isolation. Open source tools and sandboxing technology will be necessary to

provide a view of threats in minute detail to identify and analyze. Among them, the sandboxing process, especially about high-criticality malicious attachments, turned out to be crucial with the criticality score often reaching 90.

The results provide a case for a holistic approach toward threat detection and mitigation in cybersecurity. Although SIEM and SMG are strongly oriented toward supporting threat detection and response, relying solely on these technologies can result in security gaps that sophisticated threats might be able to bypass. This involves the inclusion of open-source intelligence tools and state-of-the-art sandboxing techniques. With such, an organization may better its position in detecting and responding to threats. This multi-layered approach improves threat detection accuracy while reducing incident response time, thus remaining a core element in modern cybersecurity strategies.

Additional future research shall be set out to see how these different security technologies can be integrated and how effective such an integrated setup will be across various environments. There is a need to investigate the potential for automating the integration process of SIEM, SMG, open-source tools, and sandboxing technologies in a bid to reduce the risk of human error and make operations easier. Future studies need to be orientated to the dynamics of cyber threats and how multi-layered strategies of defense can keep pace with these changes. Further research into the performance of such integrated systems in real-world scenarios would therefore be able to provide relevant insights that will contribute to the ongoing development of more robust cybersecurity solutions.

## References

- [1] M. Iavich, G. Akhalaia, S. Gnatyuk, Method of improving the security of 5G Network architecture concept for energy and other sectors of the critical infrastructure, in: A. Zaporozhets (Eds.) *Systems, Decision and Control in Energy III*, volume 399 of *Studies in Systems, Decision and Control*, Springer, Cham, 2022, pp. 237–246. doi: 10.1007/978-3-030-87675-3\_14.
- [2] Z. Hassan, Shahzeb, R. Odarchenko, S. Gnatyuk, A. Zaman, M. Shah, Detection of Distributed Denial of Service attacks using snort rules in cloud computing & remote control systems, in: *Proceedings of 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, IEEE, Kiev, Ukraine, 2018, pp. 283–288. doi: 10.1109/MSNMC.2018.8576287.
- [3] S. Gnatyuk, et al., New Secure block cipher for critical applications: Design, implementation, speed and security analysis. In: Z. Hu, S. Petoukhov, M. He (Eds.) *Advances in Artificial Systems for Medicine and Education III. AIMEE 2019*, volume 1126 of *Advances in Intelligent Systems and Computing*, Springer, Cham, 2020, pp. 93–104. doi: 10.1007/978-3-030-39162-1\_9.
- [4] V. Kharchenko, I. Chyrka, Detection of airplanes on the ground using YOLO neural network, in: *Proceedings of 17th International Conference on Mathematical Methods in Electromagnetic Theory (MMET)*, IEEE, Kyiv, Ukraine, 2018, pp. 294–297. doi: 10.1109/MMET.2018.8460392.
- [5] R. Odarchenko, A. Abakumova, O. Polihenko, S. Gnatyuk, Traffic offload improved method for 4G/5G mobile network operator, in: *Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, IEEE, Lviv-Slavske, Ukraine, 2018, pp. 1051–1054. doi: 10.1109/TCSET.2018.8336375.
- [6] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, *CEUR Workshop Proceedings 2255 (2018)* 193–204. URL: <https://ceur-ws.org/Vol-2255/paper18.pdf>.
- [7] S. Gnatyuk, Critical aviation information systems cybersecurity, in: *NATO Science for Peace and Security Series – D: Information and Communication Security, Volume 47: Meeting Security Challenges Through Data Analytics and Decision Support*, 2016, pp 308–316. doi: 10.3233/978-1-61499-716-0-308.
- [8] E. Ukhanova, Cybersecurity and cyber defence strategies of Japan, *SHS Web of Conferences 134 (2022)*. doi: 10.1051/shsconf/202213400159.

- [9] D. Galinec, D. Moznik, B. Guberina, Cybersecurity and cyber defense: national level strategic approach, *Automatika* 58(3) (2017) 273–286. doi: 10.1080/00051144.2017.1407022.
- [10] K. Baker, What is cyber threat intelligence? URL: <https://preview.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/>.
- [11] A. Bylund, Blockchain security defined. URL: <https://www.fool.com/terms/b/blockchain-security/#:~:text=Blockchains%20manage%20a%20large-scale,a%20distributed%20network%20of%20computers.>
- [12] K. Chin, The role of cybersecurity in blockchain technology. URL: <https://www.upguard.com/blog/the-role-of-cybersecurity-in-blockchain-technology#:~:text=cybersecurity%20best%20practices-,What%20is%20Blockchain%3F,transparently%2C%20and%20cost-efficiently.>
- [13] M. K. Pratt, Top 12 IoT security threats and risks to prioritize. URL: <https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize.>
- [14] L. Stanham, What is AI-powered behavioral analysis in cybersecurity. URL: <https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/>.
- [15] C. Team, The importance of blockchain security. URL: <https://www.chainalysis.com/blog/blockchain-security/>.
- [16] What Is Deception Technology? URL: <https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology.>
- [17] What Is Zero Trust Architecture? URL: <https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-architecture.>