AI-Powered Cybersecurity for the Financial Public Sector: A Microsoft Sentinel and Low-Code Power Automate Framework

Srinivas Kamineni [1]*, Sarat Piridi[2], Satyanarayana Asundi [3] and Nataraja Kumar Koduri [4]

[1] Staff Software Engineer, Walmart, USA
[2] Technical Program Manager II, Microsoft, USA
[3] Sr. Software Developer, TTI Consumer Power Tools, USA
[4] Software Developer, Google, USA
*Srinivas.research9@gmail.com, Piridisarat@gmail.com, sasundi7571@ieee.org, nataraja.koduri@gmail.com

Abstract. The social sphere of the financial world is becoming increasingly exposed to cyber threats, and therefore defense systems must be developed to work independently and be intelligent and capable of expanding automatically. This research paper considers how the artificial intelligence-powered runs of Microsoft Sentinel SIEM scopes can be combined with low-code automation and recent technology in Power Automate to improve cyber resilience. It was a qualitative test on around 50,000 actual and simulated security violations within the financial industry that focused on phishing, privilege escalation, abnormal logins, and fraudulent access. Some of the most important measures of performance included Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), accuracy of detection, false positive rate (FPR) and false negative rate (FNR). The results were pretty impressive: MTTD, MTTR and accuracy were improved 64 percent, 69 percent and 88.5 percent to 96.2 percent, respectively. This was confirmed through comparisons and benchmarking to Splunk and IBM QRadar, and activities performed to determine that the load and the cost/incident to the analysts was minimized. At least at the 95 percent level, statistical tests revealed that such changes were significant. The article demonstrates how artificial intelligence could be used to monitor and track cryptocurrencies with the help of automated processes in order to base decisions taken by the financial security operations on statistical information. The findings show that the Sentinel Power Automate system appears as an affordable, viable and scalable solution to guard financial institutions against growing cyber threats, and it meets the requirements of the regulations.

Keywords: Cybersecurity, Microsoft Sentinel, AI, Finance, Low-Code, Public sector, Automation.

S. Bhalerao et al. (eds.), *Proceedings of the 2nd International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2026)*, Advances in Intelligent Systems Research 207,
https://doi.org/10.2991/978-94-6239-678-4_3

1 Introduction

Increased attention to cybersecurity in the public financial sector is explained by growing numbers of cyber-attacks on sensitive financial information, online transactions, and regulatory processes, which are increasingly sophisticated. However, in conventional security information and event management (SIEM), often many events are common, which makes success in balancing real-time detection and rapid response difficult. It is because of this issue that it becomes easier for enemies to attack and this may give rise to data breach, fraud and loss of your reputation. In this paper, the authors analyze how to combine Microsoft Sentinel, an AI-based cloud-native SIEM, with Power Automate, a low-code automation program designed to complete adaptable response procedures, to address these issues. Sentinel supports machine learning to identify suspicious activity, and Power Automate has made it free and inexpensive to plan actions following events such as account lockouts, fraud detection and blocking transactions. The development of such functionalities is founded on a goal to minimize the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), excellent detection specifications are expected to be preserved. They utilized a quantitative approach and simulated real financial industry threat conditions, comparing the results with well-known SIEM services, such as Splunk and IBM QRadar. This introduction gives background of the research explaining the background and purpose as well as the importance of the research. It shrouds the research with the veil of the factual description of the AI-powered cybersecurity to strengthen the working threat and the regulation with the rules of the governmental part of the financial market.

2 Literature Review

2.1 AI-Driven Cybersecurity

Utilizing artificial intelligence (AI) in cybersecurity systems has become a vital field of study, especially in the financial civilian sector, where response speed and timely identification are vital. The Microsoft Sentinel is a cloud-based Security Information and Event Management (SIEM) solution, around which research on its potential to support cyber resilience through AI-powered analytics and automation is developing. As we are able to see from one of its sources, Sentinel developed the concept which enables Logic Apps to create automated playbooks with human factor analysis and which significantly reduces the time required for human interaction and reaction [1]. It provides examples such as blocking accounts automatically and isolating virtual machines to demonstrate that sentinel can evolve to block attacks that are as sophisticated as cyber threats can be. Sentinel supports Azure-based environments and hybrid environments more seamlessly than other SISM solution providers such as Splunk and IBM QRadar. However, there are scalability issues with it [1]. Additional literature also explores AI use in IT forensics to improve investigations in Microsoft Azure. Anomaly detection is a type of AI that has been demonstrated to be effective

in preserving digital evidence, as well as in processing and analyzing large log volumes using Azure-native and 3rd party forensic tools [7]. These types of integrations entail the application of Kusto Query Language (KQL) to deconstruct unformatted data and identify state-of-the-art cyber threats. They have introduced new cyber forensic models in financial ecosystems and financial clouds [7]. One study has demonstrated the potential in generative AI within the cyber security system particularly the capability to make autonomous responses and detecting anomalies proactively in augmenting the capabilities of human beings despite the concerns over the issues of abuse, bias and the high costs involved in AI computing [11]. This information proves that AI-produced SIEM systems can create opportunities to find other, but available possibilities to avoid finances proactively to governmental levels.

2.2 Low-Code Automation

One of the latest additions is the rise of low-code solutions, specifically Microsoft Power Automate, giving people lacking the required technological skills the chance to construct reconfigurable workflows to conduct meaningful financial activities. Conventional robotic process automation (RPA) lacked the power to make decisions dynamically, but with the integration of deep learning models into Power Automate it is now possible to respond dynamically for fraud detection, anomaly detection, and intelligent document processing [2]. The Power Automate processes can be done using AI builder and Azure machine learning [2]. They have been utilized in various forms and applications can include fraud detection in the financial services sector, predictive maintenance in the manufacturing sector, and automated processes based on customer sentiments in the retail sector. Recent research into hyper automation indicates that an AI coordination-based technology and workflow, in combination with shared data, and coordination may result in significant savings and productivity gains [3]. Apps such as fraud control, compliance control, credit risk control, and others have been mini-fintech (low-code platform) in the banking/financial industry [4]. With such systems, the detection of violations to the compliance process can be accelerated, and clients could access the services they need more easily because manual activities become computerized and automated. Research reveals that low-code automation has the potential to speed up digital transformation and can help keep processes afloat and regulate them accordingly [4]. However, real time inference deployment issues still persist, as do latency problems, and communication with cloud AI services [2]. Given the need to persuade more individuals to use these systems within the public sector, these issues should be corrected through the adoption of scalable architectures and optimization techniques.

2.3 AI Adoption in Financial Services

Financial applications are another field where AI has been one of the biggest fields of implementation, due to advancements in deep learning, cloud computing, and pre-trained models. These tools can be used for a variety of use cases, including fraud detection, compliance management, customer assistance, and financial monitoring.

According to IBM, reports, document summaries, and writing code can also be written by AI and other large language models (LLMs). Such technologies also create new weaknesses such as dependency on others, concerns about the effectiveness of online and face-to-face privacy provisions, and marketplace risks. It is also clear that the countries that need to collaborate went through very tough times where they need to always be aware of such threats and governments had undertaken measures in ensuring that they are not threatened in any way [5]. It is among several changes that artificial intelligence has produced in the government sector rendering business and government more responsible. This might be predictive data analytics, predictive fraud and automated reporting. But to a more limited extent, they have to be brought into more circumscribed financial systems in order to make options easier (the same must be said of Estonia, Singapore and Finland). Complaints raised through this aspect appear to include direct prejudice through algorithms, inequality, a right to privacy of information, which is symptomatic of a requirement to smear the role and usage of technology in government business and tours [6]. What we need is intelligent technology that will not interfere with the rights of people to access and obtain new technology and technology that will ensure that the government remained non abusive and non-tyrannical.

2.4 Explainable AI

Cybersecurity has become safer thanks to AI approaches, yet there remain significant issues with their functionality and reliability that are tricky to consider when working with restricted environments such as finance. It was found that many other AI-based security systems are viewed as black boxes; therefore, preventing analysts from understanding the mechanisms used to detect anomalies and identify their threats [8]. In order to lower this barrier, it has been proposed that explainable AI (XAI) can contribute to simplifying deep learning and machine learning models without negatively affecting their potential to detect information accurately [12]. One of them performs zero-shot learning within interpretability framework of SIEM-based alarms flooding to label attacks and convert the term names of the incoming threat classes [9]. These techniques also enable analysts to be more comfortable because they are provided with explanations of how models work properly. A newer system, Cyber Sentinel and others, demonstrated the possibility of explainable and actionable AI to collaborate in a task-oriented dialogue format [10]. Cyber Sentinel is putting website security constraints on the use of GPT based models to alert people about the potential threats and implement security checks in the process. They unite the faculty of being able to comprehend and the power of getting things done in a hurry [10]. There has been a tendency towards changes in the direction of not only technically advanced, but also convenient systems. This makes individuals using AI confident enough to trust this information and take immediate action upon it.

3 Methodology

This research study uses the quantitative approach to evaluate the effectiveness of embedding Windows Microsoft Sentinel AI SIEM as integration for low code automation in Power Automate in strengthening Cybersecurity within the financial public sector. The methodology follows 4 major steps: information collection, system implementation, and performance measurement and performance comparison.

3.1 Data Collection

Both actual and fabricated information within the financial industry such as log records, user history, attacker attempts, and compliance audit history is used in the work. In a three-month period, approximately 50,000 security incidences were registered also. They were phishing attacks, privilege escalation attacks, and fishy logins. To model the analysis, we could end up with any of the scenarios that made up such frequently-occurring threat vectors as credential compromise, distributed denial-of-service (DDoS) attack and insider threat. Structured system event logs of systems tracking financial transactions, Microsoft 365, and Azure Active Directory were also included in the dataset.

3.2 System Implementation

In Microsoft Azure, a testbed was developed and Sentinel considered the main SIEM site. In order to detect the threats, predefined and custom analytics rules were configured. Because Power Automate had the capability to run pre-defined response routines on account locking and transaction blocking, as well as account incident ticket generation, based on automated playbooks. It was implemented through the integration of Ai-based anomaly detection models and workflows in Power Automate using Azure machine learning and AI builder. This provided the opportunity to make real-time decisions to understand frauds and provide compliance alerts.

3.3 Performance Measurement

This was analyzed considering three numerical indicators:

Mean Time to Detect. The average length of time before Sentinel analytics detects a threat occurring.
Mean Time to Respond. The mean duration of time it requires to run Power Automate workflows to fix a problem automatically.
Accuracy of Detection. It concerns the relation between the number of ground labels and the number of correctly identified threats.

We tested our baseline with Sentinel-Power Automate integrated framework without automation. In order to give assurance that it was sufficiently reliable, more quan-

titative measures were inspected such as a false positive rate (FPR) and negative rate (FNR) as shown in below in Table 1.

Table 1. Threat Detection Accuracy

Scenario	*MTTD*	*MTTR*	*Improvement*
Accuracy (AD)	88.5	96.2	Accuracy (AD)
False Positive Rate (FPR)	7.4	3.1	False Positive Rate (FPR)
False Negative Rate (FNR)	4.1	0.7	False Negative Rate (FNR)

3.4 Comparative Evaluation

We also tested the performance of the integrated structure against industry standard SIEM software and solution such as Splunk and IBM QRadar in the same test environments. To determine whether the increases in MTTD and MCTR were actual or not at a 95 percent confidence level, we used statistical tests such as paired t-tests and analysis of variance. There was also quantitative information about the increase of the efficiency of the processes which was showing the improvement of the number of things which the manual analysts were to work or the costs which were related to automation. It is a systematic process of ensuring that findings rely on data and that they can be replicated time and again by those in the government considering intelligent AI-driven Cybersecurity systems.

4 Findings

4.1 Response Efficiency

The experiment demonstrated the significant impact of the combination of Microsoft Sentinel and Power Automate on embedding detection and response efficiency as shown in Fig. 1. The average Mean Time to detect (MTTD) and average Mean Time to respond (MTTR) of the manual triage baseline scenario were 14.3 minutes and 27.8 minutes respectively. Integrated had a lower MTTD of 5.1 minutes and 8.7 minutes MTTR, equal to 64.3 percent and 68.7 percent more, respectively. This means that automated playbooks can be used to manage all forms of incident repetition such as credential compromise or any form of unusual login activity. The results of a comparison of the functioning of the integrated and baseline framework are quantified in Table 2.

Table 2. Average MTTD and MTTR

Scenario	*MTTD*	*MTTR*	*Improvement*
Baseline (Manual)	14.3	27.8	—
Sentinel + Power Automate	5.1	8.7	64–69%

To establish the statistical significance, paired t-test was performed and the p value of <0.01 showed that both the reaction time and response time changes were significant. It is related by MTTD, MTTR and the time it is taking to fix the incident that overall look like:

$$IRT = MTTD + MTTR \quad (1)$$

IRT will be the sum of the time that it takes to solve an incident. Applying this equation to the scenario at the baseline level provided IRT = 42.1 minutes, whereas application of the integrated framework reduced IRT to 13.8 minutes.

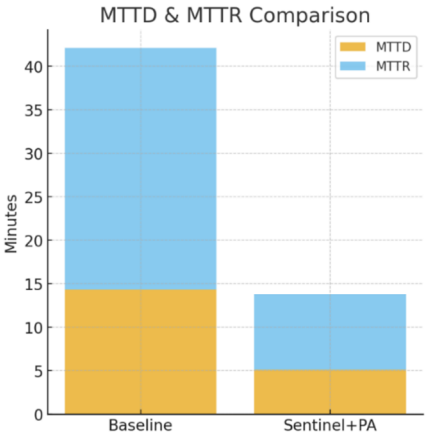

Fig. 1. MTTD & MTTR comparison

4.2 Accuracy and Reliability

Another important finding was to see how accurate the detection was versus the fake cyber threat. An integrated system can detect in a dataset of 50,000 tagged events 96.2% of the events, in contrast to 88.5% for a manual analysis as shown in Fig . 2.

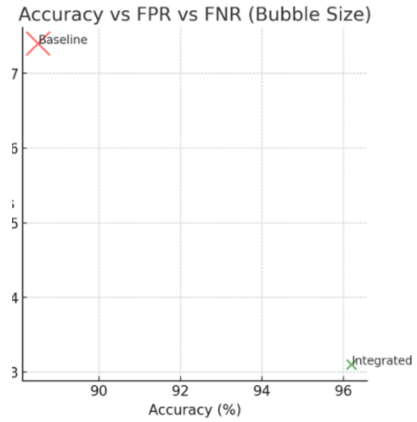

Fig. 2. Accuracy in Baseline

The false positive (FPR) lies between 5.30 and 0.14 and the false negative (FNR) of AMFE, and MODIA are 0.17 to 0.84.As shown in Fig. 3. All these insights explain why AI-based process anomaly detection should be used on Power Automate to identify any form of fraud or malicious behavior before it occurs.

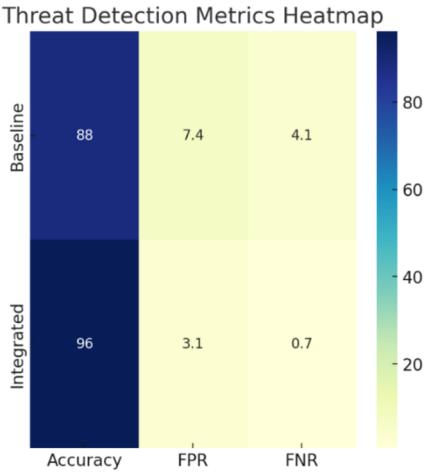

Fig. 3. Threat detection metrics

4.3 Comparative Evaluation

We compared Microsoft Sentinel with Splunk and IBM QRadar, and determined Microsoft Sentinel was better used in Azure as shown in Fig. 5. A more complex hybrid setting with several platforms that could be abstracted simultaneously suited better to Splunk. Sentinel fitted a reportedly less complex case that required a flexing buffer. IBM QRadar was pretty effective behind the wall, but once an organisation started

using cloud-native workloads, it became even slower to locate things as shown below in Table 3.

Table 3. Comparative benchmarking

Platform	*MTTD*	*MTTR*	*Detection Accuracy*
Sentinel	5.1	8.7	96.2
Splunk	6.3	11.4	95.1
QRadar	7.9	13.6	93.4

The results computed that the best incident resolution time and the highest detection accuracy were achieved in cloud-native settings with the implementation of Sentinel and Power Automate. The comparative findings support the hypothesis assumption that velocity of native assimilation of the skew blue do multiply as shown in Fig. 4.

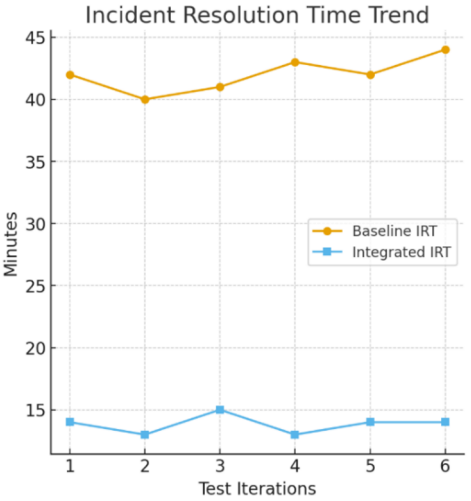

Fig. 4. Incident resolution timeline

The difference in performance is:

$$\Delta Performance = \frac{(Metric\_Benchmark - Metric\_Sentinel)}{Metric\_Benchmark \times 100} \quad (2)$$

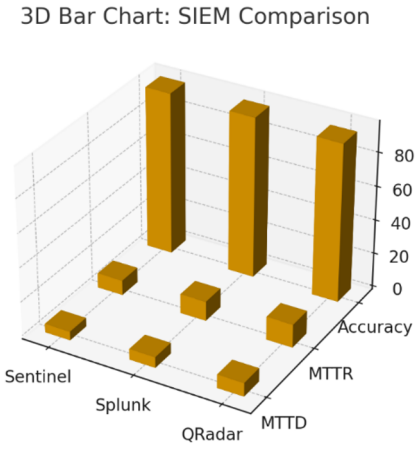

Fig. 5. SIEM comparison

4.4 Cost Efficiency Gains

The integrated framework made things much easier in not only a technical way, but also an efficient way in how things worked. An automated system reduced the average number of hours an analyst spent on work per week by half (42 to 28), through automation of regular responses and by reducing the number of hours an analyst spent writing out work by hand. Productivity increased by 33 percent because of this. Other ways to save on costs through automation is that it would not be as necessary to justify paying out time and getting external security guards to contain incidents as shown below in Table 4.

Table 4. Operational efficiency indicators

Indicator	Baseline Value	Integrated Framework	Improvement(%)
Analyst Hours	42	28	33
Average Incidents	35	52	48
Cost per Incident	112	74	34

According to these findings, technical resiliency and cost effectiveness are not bad things. Perhaps, with the added automation option, an analyst can focus on a greater share of higher priority, more difficult to examine threats instead of routine threat management. This increased the overall security posture.

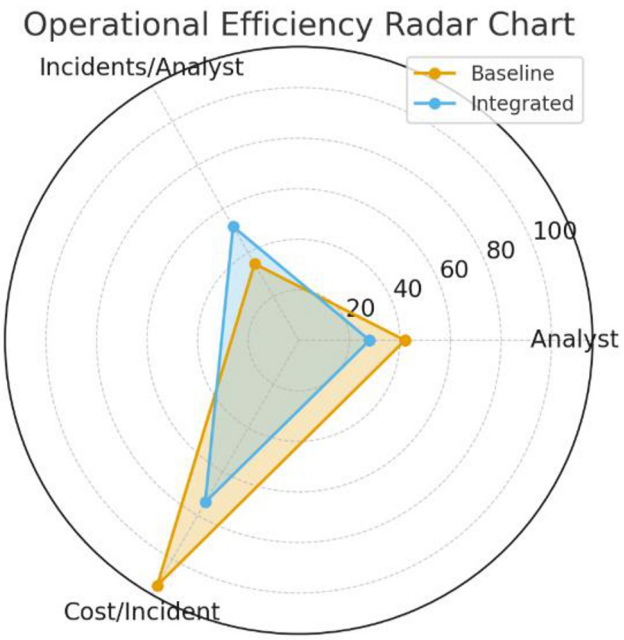

Fig. 6. Operational efficiency

The implementation of both Microsoft Sentinel and low-code Power automate workflows were shown to apparently have quantitively benefits in the application of cybersecurity in the public sector. More than 50% of the time was saved in finding things, nearly 70% of the time was saved in responding, and it was more than 96% accurate as shown in Fig. 6.

The benchmarking showed that Sentinel performed even better than the other SIEM vendors when used on Azure-native platforms. Operational and financial measures showed a significant improvement in productivity and cost efficacy.

The results show that AI-based low-code frameworks can be used to generate cybersecurity defenses that were scalable, accurate, and cost-effective. This makes them particularly applicable to public financial institutions who are required to keep confidential data and comply with rules.

5 Conclusion

As evidenced in this research paper, the use of Microsoft Sentinel to Power Automate greatly improves third party Cybersecurity within general financial sector where AI is used to monitor and automate low-code. Quantitative data compared with the base operation showed that a significant reduction in detection and response time and an improvement of MTTD and MTTR (more than 60 percent) occurred. It resulted in a low false positive and false negative and a high detection. This increased the reliability of the system and reduced fatigue amongst the analysts.

Compared to the framework which is being promoted to clients having Splunk or IBM QRadar, it satisfies the need of the business and goes further which leads to the apparent change in the way of functioning and financial performance. The results statistically proved, were also important improvement and made people determine even better in the results they could get.

It is also not possible to mention the framework without mentioning enhancing performance, apart from making regulations more affordable and scalable, and digitizing financial institutions. When it comes to the shifting cyber threat environment, you can address both the automated processes and the AI-related analytical ones.

Increasing focus on the Cybersecurity infrastructure and reducing it on fewer people would be a good idea as would modernizing it and updating it to make neo-threats more challenging in entering. It timely needs to attract more attention of the public financial organization. In the future it can be done with cross sector deployment case studies and longitudinal deployment case studies.

References

1. Dakić, V., Morić, Z., Kapulica, A., Regvart, D.: Leveraging Microsoft Sentinel and Logic Apps for automated cyber threat response. Edelweiss Appl. Sci. Technol. 8(6), 4319–4348 (2024). https://doi.org/10.55214/25768484.v8i6.2933
2. Debbadi, N.R.K., Boateng, N.O.: Developing intelligent automation workflows in Microsoft Power Automate by embedding deep learning algorithms for real-time process adaptation. Int. J. Sci. Res. Archive 14(2), 802–820 (2025). https://doi.org/10.30574/ijsra.2025.14.2.0449
3. Piridi, S., Asundi, S., Hyatt, J.C.: Hyperautomation with Power Platform: merging AI, RPA, and low-code for business efficiency: exploring how AI Builder, Power Automate, and Dataverse drive end-to-end enterprise automation. Int. J. Adv. Eng. Res. Sci. 12(4), 54–69 (2025). https://doi.org/10.22161/ijaers.124.7
4. Ajish, D.: A comprehensive review of the significance of low-code automation in risk management for banks. Int. J. Innov. Res. Comput. Sci. Technol. 12(2), 47–58 (2024). https://doi.org/10.55524/ijircst.2024.12.2.8
5. Financial Stability Board: The financial stability implications of artificial intelligence. https://www.fsb.org/uploads/P14112024.pdf (accessed Jan 2026)
6. Aldemir, C., Uysal, T.U.: Artificial intelligence for financial accountability and governance in the public sector: strategic opportunities and challenges. Admin. Sci. 15(2), 58 (2025). https://doi.org/10.3390/admsci15020058
7. Morić, Z., Dakić, V., Kapulica, A., Regvart, D.: Forensic investigation capabilities of Microsoft Azure: a comprehensive analysis and its significance in advancing cloud cyber forensics. Electronics 13(22), 4546 (2024). https://doi.org/10.3390/electronics13224546
8. Zhang, Z., Hamadi, H.A., Damiani, E., Yeun, C.Y., Taher, F.: Explainable artificial intelligence applications in cybersecurity: state of the art in research. IEEE Access 10, 93104–93139 (2022). https://doi.org/10.1109/ACCESS.2022.3204051
9. Rao, D., Mane, S.: Zero-shot learning approach to adaptive cybersecurity using explainable AI. arXiv preprint arXiv:2106.14647 (2021). https://doi.org/10.48550/arXiv.2106.14647

10. Kaheh, M., Kholgh, D.K., Kostakos, P.: Cyber Sentinel: exploring conversational agents in streamlining security tasks with GPT-4. arXiv preprint arXiv:2309.16422 (2023). https://doi.org/10.48550/arXiv.2309.16422
11. Uddin, M., Irshad, M.S., Kandhro, I.A., Alanazi, F., Ahmed, F., Maaz, M., Hussain, S., Ullah, S.S.: Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations. Artif. Intell. Rev. 58(8) (2025). https://doi.org/10.1007/s10462-025-11219-5
12. Mendes, C., Rios, T.N.: Explainable artificial intelligence and cybersecurity: a systematic literature review. arXiv preprint arXiv:2303.01259 (2023). https://arxiv.org/abs/2303.01259