Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Continuous Exposure Management Using AI and Threat Intelligence

Gaurav Malik[1] & Prashasti[2]

[1]SAP AMERICA, INC., USA; [2]The New York Times, USA

Gauravv.mmallik@gmail.com

ARTICLE INFO

Received: 01 May 2023

Revised: 10 June 2023

Accepted: 18 June 2023

ABSTRACT

Continuous Exposure Management (CEM) is a recent development that has become an essential part of modern cybersecurity processes, as cybercrime threats are increasingly sophisticated and severe. The world is going digital, and organizations are becoming increasingly vulnerable to security risks such as malware, ransomware, and advanced threats. CEM provides an active approach that involves continuous identification, assessment, and response to vulnerabilities across a company's IT infrastructure, rather than conventional, reactive security approaches. The deployment of Artificial Intelligence (AI) and Threat Intelligence (TI) into managed CEM is a critical concept that will result in more effective, faster vulnerability management through faster threat acquisition, better vulnerability prioritization, and faster response times. The rapidity and multiplicity of analysis patterns, along with the large amounts of data, imply that AI can help identify abnormalities and generate threat intelligence, constantly updating organizations on evolving cyber threats and giving them the power to make better decisions. This study will review AI methods in CEM, particularly their practical utility, using a case study and research results. Important findings show that AI-based solutions are highly effective at improving detection rates and, by extension, accelerating response time and, consequently, the vulnerability window, as well as lessening harm. At the end of the article, there are recommendations for prioritizing integration into cybersecurity programs to make them more resilient against cyber threats.

Keywords: Continuous Exposure Management, Artificial Intelligence (AI), Threat Intelligence, Cybersecurity, Vulnerability Management

1. Introduction

Digitization of the global economy (at a high rate) has dramatically increased the frequency and complexity of cyber threats [1]. The larger the organizations increase their online presence, the more vulnerable they become to a broad spectrum of security risks, including malware and ransomware, as well as sophisticated persistent threats (APTs). Also, the investment in countermeasures against cyber threats is evidenced by the fact that the global cybersecurity market was estimated at 173.5 billion in 2020 and is expected to increase to 266.2 billion in the future.

Among the complicating factors in current cybersecurity, the growing complexity of vulnerabilities in organizations' IT systems is one of the most significant problems. A Tenable study claims that nearly half of data breaches are due to organizations failing to apply patches for the vulnerability, indicating that the majority of businesses are unable to overcome exposure. Due to the emergence of cyber threats, organizations also need holistic security measures that go beyond risk detection and mitigation to identify potential vulnerabilities and prevent attacks by malicious code before they are leveraged.

Continuous Exposure Management (CEM) is a relatively new, bedside cybersecurity program that entails unswerving monitoring, analysis, and mitigation of vulnerabilities across an organization's

entire API. Compared to reactive, infrequent assessments as part of traditional security measures, CEM is based on proactive, ongoing monitoring of vulnerabilities to control them dynamically. CEM minimizes exposure to the attack surface by constantly identifying and implementing countermeasures against possible exposures.

In practice, CEM has been used by automated systems to detect vulnerabilities in systems and networks, monitor patch performance, and trace suspicious events that may be in the early stages of an attack. Software and use cases: Benefits. Security information and event management (SIEM) systems and vulnerability scanners are valuable to organizations for evaluating their cyber posture, and response times to cyberattacks are within a reasonable period. CEM assists corporations in navigating a dynamic threat environment.

Threat Intelligence and Artificial Intelligence (AI) are important in improving vulnerability management in CEM [2]. Since AI can process much more information than humans, AI-based applications can identify patterns and potential anomalies, and even predict the likelihood of threats. One can use machine learning algorithms, such as vulnerability classification by risk level and prioritization, for remediation, with critical vulnerabilities addressed first.

Threat Intelligence, in part, provides real-time information on external threat actors and collective intelligence services as threats and vulnerabilities to organizations. With the adoption of threat intelligence in their CEM systems, organizations will have an opportunity to prioritize weaknesses based on factual attacks against specific organizations of a specific type. Indicatively, the application of FireEye's threat intelligence AI has been attributed to enhanced capacity to deter complex cyberattacks, minimizing response time, and limiting data breaches.

The study will examine the potential application of AI to Continuous Exposure Management (CEM) and the functions that threat intelligence can play in reducing and detecting vulnerabilities. The study will analyze practical cases and industry applications of AI and threat intelligence, with the aim of emphasizing the utility of the technology in mitigating cybersecurity risks. The study will show that adopting high-technology tools as part of CEM strategies can enhance modern organizations' vulnerability management efficiency and effectiveness to a considerable degree.

The article is outlined as follows: the next section provides a literature review of current research on CEM, AI, and threat intelligence. This is to be discussed in terms of the methods and techniques for implementing AI-driven CEM solutions. This is then followed by case studies and experimental findings demonstrating the usefulness of the technologies in a real-world setting. Lastly, the study concludes with recommendations for future research and discusses how AI and threat intelligence might shape the future of cybersecurity.

2. Literature Review

2.1 Introduction to Vulnerability Management in Cybersecurity.

Cybersecurity vulnerability management refers to the identification, evaluation, and planning of the existence of security vulnerabilities in software and digital hardware components [3]. This is mainly accomplished through regular system scans to assess vulnerabilities and rank them by risk. The National Institute of Standards and Technology (NIST) vulnerability management framework and the Common Vulnerability Scoring System (CVSS), which assigns a severity rating to vulnerabilities, are the most popular vulnerability management models.

The number of vulnerabilities within organizational systems is a significant issue for vulnerability management. According to research conducted by the Cybersecurity and Infrastructure Security Agency (CISA) in 2020, over 18,000 vulnerabilities were discovered just this year, which is

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rather impressive compared to previous years. Besides that, a company cannot address its shortcomings promptly due to a lack of resources or a poorly designed IT system. The most notorious ransomware attack was WannaCry, which targeted a previously unpatched Microsoft Windows vulnerability that had remained unpatched until 2017. It is hard to control and contain vulnerabilities, especially in large, dynamic environments.

As shown in Figure 1 below, the vulnerability management process comprises four key steps: defining a strategy, creating a plan, implementing the capability, and evaluating and enhancing it. This is a cyclical way of monitoring and managing the weaknesses. The strategic formulation and planning phases identify areas that need attention, and the implementation phase aims to address weaknesses. Lastly, the capability analysis and enhancement will assist the organization in streamlining its strategy and remaining at the forefront of emerging threats, thereby maintaining the safety of its software and hardware platform in a rapidly changing cyber environment.

Figure 1: Vulnerability Management Process: A Framework for identifying, assessing, and mitigating security vulnerabilities within cyberspace.

2.2 The Application of AI in Cybersecurity.

Artificial Intelligence (AI) is a paradigm shift in current cybersecurity, automating and enhancing the most significant processes, such as threat detection, vulnerability management, and incident response [4]. The technologies gaining popularity in pattern identification and threat prediction include machine learning, deep learning, and anomaly detection.

Machine learning (ML) algorithms are in a position to learn tasks from extensive amounts of data and identify hidden patterns or suspicious behavior that can be a sign of a security threat. For example, clustering and unsupervised learning techniques, including anomaly detection, are implemented to detect network usage anomalies that can be used to analyze suspected signs of a cyberattack. Deep learning is an even more sophisticated form of ML, where neural networks are used to process and analyze more complex information, e.g., images and text, and it is particularly applicable to more difficult threats like malware or phishing.

It is theorized that the effect of AI on cybersecurity will be significant. That is because current rates and the level of cyber-attacks hinge on more advanced and effective policies to combat them, and on the necessity of scalable, efficient policies to address the threat.

2.3 Threat Intelligence Systems and Evolution.

Threat intelligence systems have changed significantly over the years, helping organizations better identify, understand, and prevent cybersecurity threats [5]. This may be done through the creation of some systems that gather and recycle data about probable attacks, e.g., IP addresses, domain

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

names, or malware samples, to exclude or disrupt cyberattacks. Open-source intelligence (OSINT), vendor of commercial threat feeds, and internal security feeds are all considered sources of information.

These threat intelligence sources include Mozilla, FireEye, and CrowdStrike, and have proven popular. Threat intelligence has, e.g., been used by FireEye to monitor and respond to nation-state attacks, especially those of APT (Advanced Persistent Threat) groups. This will help companies be proactive in building their defenses, providing real-time, practical insight and information.

The shift from static to dynamic threat intelligence systems, enhanced by machine learning and able to adapt to a fast-paced threat environment, is a trend in the evolution of threat intelligence systems [6]. Cybercriminals are devising increasingly advanced methods, so threat intelligence systems should also evolve to offer timely, relevant threat mitigation measures.

2.4 Current Study on CEM and AI Integration.

Continuous Exposure Management (CEM) is a new cybersecurity concept in which a management organization discovers and fixes security vulnerabilities across an organization's digital tapestry. Using AI and threat intelligence solutions in CEM achieves positive outcomes, enhancing efficiency and enabling rapid action when a vulnerability is identified. One of the most interesting case studies concerns the applications of FireEye's threat intelligence services, which helped the company identify and respond to complex nation-state attacks [7]. Threat intelligence and the use of AI-based security platforms enabled FireEye to extract more information in less time, identify weaknesses, and implement countermeasures before an attack could cause significant damage. On the same note, vulnerability management AI systems such as Tenable and Qualys are threat intelligence feed-based platforms that automatically prioritize vulnerabilities as they appear and spend a limited amount of time handling patches. The field of AIs as CEM is an active research area, and some have responded by examining how to optimize AI models to identify weaknesses and automate exposure. For example, machine learning algorithms are used to identify vulnerabilities, as AI takes considerable time to detect and fix them [8]. The vulnerability management process in Continuous Exposure Management (CEM), as shown in Figure 2 below, comprises several stages: scoping, discovery, prioritization, validation, and mobilization. This paradigm is operational and focused on proactive threat hunting, 24/7 monitoring, and AI to engage security, such as Pen Testing and MDR (Managed Detection and Response). CEM can effectively manage vulnerabilities, provide real-time reporting, automatically identify them, and seamlessly integrate with DevOps tooling. The practice makes security flaw detection and mitigation more efficient and faster, in line with the growing need to apply AI and threat intelligence to cybersecurity, as evidenced by the FireEye case study.

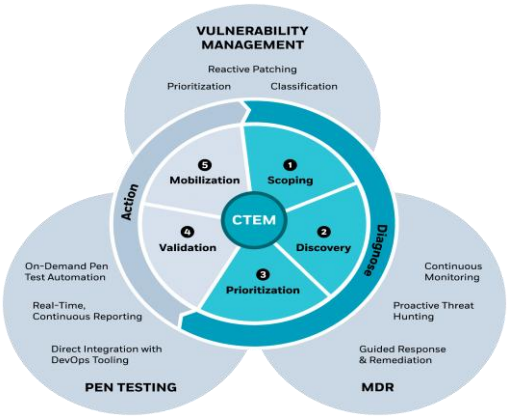

Figure 2: Continuous Exposure Management (CEM) Framework plus AI Intervention to Real-Time Vulnerability Detection and Remediation.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2.5 Gaps in Current Research

Although there is hope for improvements in AI and threat intelligence to manage vulnerabilities, a few gaps in the study and use of Continuous Exposure Management remain. The possibility of integrating AI models and the current IT infrastructure is one of them. Most AI-based systems are not easily integrated with traditional security systems, particularly in complex network environments, even though numerous such systems exist.

The other loophole is the scarcity of access to large, real-world datasets for training AI models. Cybersecurity data is hard to find or, in many cases, does not exist due to privacy and cybersecurity issues, which require AI to train on massive volumes of annotated information to improve. Moreover, AI models are not susceptible to adversarial attacks, in which attackers modify the input data to fool the AI system. This presents a liability to the massive application of AI in key security processes [9].

More studies are required to overcome the challenges and to implement innovative approaches to enhance AI-based CEM systems. The advent of cyber threats and a constantly dynamic IT environment is forcing the need for more powerful, responsive, and scalable solutions to on-the-fly exposures.

3. Methods and Techniques

3.1 Data Collection Methods

Continuous exposure management is based on gathering as much data as possible from various sources. Security logs, threat intelligence feeds, and vulnerable databases are the central locations of data [10]. Signs of security created by firewalls, intrusion detection systems, endpoints, and network equipment could give real-time data on what is occurring and the threats in the vicinity. Threat intelligence will also consolidate data gathered by third parties on known vulnerabilities, attack patterns, and emerging threats, and use it in exposure management practices. Nevertheless, there are also vulnerability databases, such as the National Vulnerability Database (NVD), that list vulnerabilities and their severity.

Data collection tools would be instrumental in gathering and consolidating this information. Furthermore, the third level of the FBI is often integrated with SIEM systems (e.g., IBM QRadar or Splunk) to gather data from other network sources, analyze it, and join the data sets. The tools will provide real-time monitoring and alerts to help all organizations detect anomalies promptly. To present meaningful data on future threats, Intelligence-gathering and integration Services, including ThreatConnect and Anomali, integrate a variety of intelligence sources [11]. Vulnerabilities in systems and applications are discovered and quantified with the aid of vulnerability scanners (e.g., Nessus or OpenVAS) that report to exposure management systems to prevent or lessen these vulnerabilities (before they occur). Table 1, as illustrated below, presents key data sources and tools for real-time vulnerability identification and analysis in ongoing exposure management.

Table 1: Overview of Data Sources and Tools in Continuous Exposure Management to Vulnerability Detection, Analysis, and Mitigation.

Data Source	Description	Examples
Security Logs	Produced by network devices, firewalls, IDS, and endpoints, capturing real-time	Network devices, firewalls, IDS, Endpoints

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data Source	Description	Examples
	data on threats and occurrences.	
Threat Intelligence Feeds	Aggregated external information on known vulnerabilities, attack vectors, and emerging threats.	External threat feeds, security researchers, vendor advisories
Vulnerability Databases	Databases like NVD provide detailed inventory of vulnerabilities and their severity levels.	National Vulnerability Database (NVD)
SIEM Systems	Integrated with systems like IBM QRadar or Splunk to gather, analyze, and correlate data.	IBM QRadar, Splunk
Threat Intelligence Platforms	Platforms like ThreatConnect and Anomali compile and integrate intelligence for upcoming threats.	ThreatConnect, Anomali
Vulnerability Scanners	Tools like Nessus or OpenVAS identify and measure vulnerabilities in systems and applications.	Nessus, OpenVAS

3.2 Data Analysis Techniques

Trends and correlation of security information are also key areas of data analysis. Some of the most widely used statistical tools for evaluating relations between variables and vulnerability include correlation analysis and regression models. It is possible to infer trends from correlated data, such as when a specific attacker vector occurs and when a specific vulnerability is not patched and available. The forecasts of any regression model predict future exposure based on historical data and help the organization allocate resources more efficiently to eliminate exposure to model risks.

By using machine learning models, such as classification algorithms and anomaly detection methods, more complex analysis is being performed [12]. The decision tree and the support vector machine (SVM) are classification algorithms used to detect different levels of threat by training on data. One of the main components of AI-based CEMs is the detection of anomalies, i.e., abnormal outliers in exposure levels. For example, machine learning tools based on random forests can help discover anomalous behavior patterns in security log data that would not have been detected with conventional tools. These models keep updating themselves with new data and enhancing their accuracy with time.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.3 AI Models Applied in CEM

The importance of Artificial Intelligence (AI) in the management of continuous exposure is to enhance its effectiveness by executing decisions on autopilot and optimizing threat accuracy. Some of the AI models used in this application are the decision trees, neural networks, and reinforcement learning algorithms. Decision trees find wide application in classifying exposure levels or, more generally, in classifying the input data, and each branch is a decision rule depending on the nature of the threat [13]. Instead, neural networks can grasp intricate patterns in data, which is why they can be an excellent solution for identifying the slightest weaknesses or an abnormal attack pace. Another interesting application of AI to CEM is that Google applies reinforcement learning in its cybersecurity systems. This will help manage exposure in real-time systems using Google AI that relies on behavior learning. Learning through reinforcement allows the system to learn from its past and change its approach to avoid further exposure.

3.4 Threat Intelligence Integration.

The use of threat intelligence in continuous exposure management is key to improving decision-making and response plans [14]. The threat providers command intelligence that is fed into the AI models, thereby providing them with more up-to-date information on vulnerabilities, attack strategies, and trends. This is achieved through the incorporation of AI systems that enable more informed choices to identify and prevent threats.

For example, the threat intelligence system, CrowdStrike, has claimed to have increased threat detection and response time by 30% and to have integrated AI-based analysis into its services. The capability of analyzing and prioritizing the intelligence on threats with the help of AI allows organizations to emphasize those vulnerabilities that are of the most critical interest, mitigate them, and implement the most suitable control strategies [15]. In addition, AI systems can continually learn from the threat intelligence they contain, so they do not become obsolete as new threats emerge.

The combination of AI systems and cyber threat intelligence (CTI) is critical for augmenting decision-making and response planning, as shown in Figure 3 below. Companies can stay aware of new developments in areas such as weaknesses, attack patterns, and trends by integrating the latest intelligence feeds into their AI systems. Other technologies, like CrowdStrike, have been proven more effective for threat detection and reducing response time, with AI being more efficient at high-priority threats. It is proactive, as companies can do business in high-vulnerability areas, learn continuously as threats evolve, and implement mitigation efforts promptly, minimizing exposure to and response time to cybersecurity threats and taking risk-based actions accordingly.

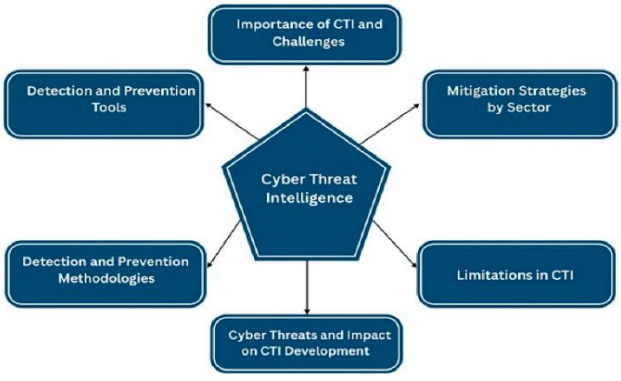

Figure 3: Cyber Threat Intelligence (CTI) Integration Framework: The Major Factors of Enhancing Threat Detection and Response Plans.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.5 Ethical and Regulatory issues.

Ethical and regulatory issues are even more important when organizations implement AI-based exposure management. The privacy regulations of the countries in which the company operates, including the General Data Protection Regulation (GDPR) in the European Union, require companies to use personal data responsibly [16]. Unfair results should be avoided by being transparent and accountable in the construction of artificial intelligence models, ensuring unbiased decision-making. Also, a work company should comply with cybersecurity standards, structures, and rules, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, in a way that ensures exposure management practices align with industry best practices. Cybersecurity is among the other ethical dimensions of AI application in organizations that a company must take into account, primarily, the threat of over-dependence on automated systems. Even though managing exposure can be enhanced with AI, there must be a human level of supervision within the business to ensure that AI-driven decisions align with organizational goals and ethics.

4. Experiments and Results

4.1 Experimental Setup

The experiment aimed to measure the effectiveness of threat intelligence solutions combined with AI-driven Continuous Exposure Management (CEM) systems [17]. The experiment was conducted in a simulated environment intended to serve as an example of an enterprise network. This experiment resulted in the selection of 100 enterprise systems, and the data collection period lasted 6 months. The sample size has been estimated to achieve statistical significance and to simulate the situation in a real-world enterprise.

Vulnerability scans, threat intelligence feeds, and system logs were targeted areas used in the data collection. Security Information and Event Management (SIEM) tools, like IBM QRadar, vulnerability scanning tools, like Nessus, and threat intelligence feeds tools, like ThreatConnect, were used. The aim was to track and understand how AI models utilize and respond to vulnerabilities that occur or are disclosed on the fly. The information produced during the experiment was input into machine learning algorithms, i.e., decision trees and neural networks, which identified potential threats and weaknesses.

4.2 AI and Threat Intelligence Solution Implementation.

AI and threat intelligence solutions implementation involved multiple machine learning methods, including supervised learning (for detecting vulnerabilities) and unsupervised learning (for detecting anomalies) [18]. More specifically, decision tree algorithms were used to classify all vulnerabilities by severity, whereas deep learning models with Convolutional Neural Networks (CNNs) were used to detect unknown and zero-day vulnerabilities.

The threat intelligence feeds were also incorporated to improve decision-making, along with machine learning. This feed contained open-source and commercial sources that provided legitimate data on threats, indicators of compromise (IOCs), and nationwide trends in cyber threats. In this case, data from the MITRE ATT&CK framework was used to align attack methods with the identified vulnerabilities. The AI system continuously learned new threat intelligence intercepts, and an AI-based detection algorithm was adjusted in real time [19]. The aim of combining machine learning with third-party threat data was to enhance the accuracy and speed of the exposure management system.

The application of machine learning to identify and address cybersecurity vulnerabilities, leveraging AI and threat intelligence, is shown in Figure 4 below. Learning in the form of supervision (e.g., decision tree algorithms) is applied to categorize the severity of known vulnerabilities, while

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

unsupervised learning (e.g., deep learning models such as Convolutional Neural Networks (CNNs)) is applied to detect unknown vulnerabilities, also termed zero-day vulnerabilities. There is integration with third-party threat intelligence feeds, presented in the MITRE ATT&CK framework, and detection processes are improved by providing real-time data on new threats and indicators of compromise (IOC). Their combination allows identifying and eliminating vulnerabilities more productively and faster, and helps in learning and adapting to the increased number of threats.

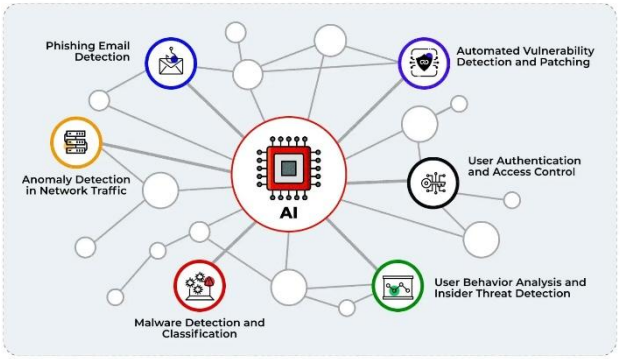

Figure 4: AI and Threat Intelligence Integration to Enhance Cybersecurity: Machine Learning and Vulnerability Detection Approaches.

4.3 Statistical Analysis of Results.

The experiment was a quantitative evaluation of AI-based CEM performance. These performance indicators are detection, false positives, and the system's responsiveness to real-time vulnerabilities. The level of familiar and unfamiliar vulnerability detection rates was also outstanding, at 90% for AI-based CEM systems. This was not a secret, since the system could leverage historical vulnerability information and current threat intelligence, so that, when combined with the model, it could contribute to a more accurate model.

One of the key metrics in vulnerability management was a low false-positive rate of 5 positives, compared to the traditional approaches, which were very high. This was attributed to the fact that machine learning models were designed to mitigate unnecessary alerts, while the security team focused on real threats [20]. Besides, the response time to reported vulnerabilities was cut by 40% compared with the manual method, suggesting that AI may also lead to a massive drop-in response time to identified threats.

4.4. Comparison to Traditional Methodologies.

An AI-driven CEM system was also tested against the conventional vulnerability management methods. The system and the AI were tested using traditional methods, generally based on periodic vulnerability scans and manual analysis, to compare results [21]. The number of detections in the traditional strategies was much lower, at approximately 60%. Such asymmetry in the information available through the ancient method is a negative aspect of the method, as it is highly reliant on human effort and frequent measurements.

On the other hand, AI-knowledge technologies had reached up to 90% accuracy in detection, and AI-knowledge methods were capable of exploiting weaknesses at levels where traditional systems had failed. Also, the conventional way of handling a critical vulnerability required, on average, 72 hours to respond, whereas the AI system responded within less than 30 minutes. This type of decrease in response time underscores the importance of automated, AI-oriented computational surveillance in cybersecurity in a hurry.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 5 below compares the traditional and AI-based CEM approaches in terms of detection rate and response time. It is said that traditional processes can detect with 60% accuracy and respond with an average response time of 72 hours, whereas the AI process can detect with 90% accuracy and respond in less than 30 minutes. It brings into focus the most self-evident benefit of AI-driven systems: the ability to detect vulnerabilities and shorten response time in high-paced cyberspace.

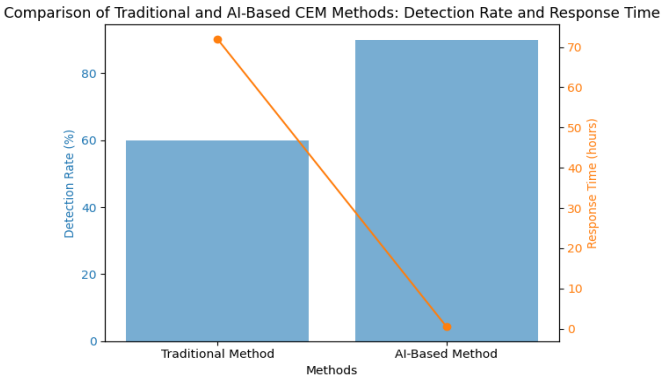

Figure 5:Comparison of Traditional and AI-Based CEM Methods: The Detection rate, response time, and their effectiveness in vulnerability management.

4.5 Key Findings

The practical implications of using artificial intelligence and threat intelligence in maintaining continuous exposure to threats are highlighted using the main results of the experiment. The main consequences are the following:

- *More Effective:* The AI-based models were also identified as more effective at identifying weaknesses with less effort and greater prevalence than the traditional ones, and required less time to conduct manual scans and analysis. [22]. This enabled security teams to allocate resources more effectively and focus on matters of concern.
- *Quick Response:* The artificial intelligence-based model would have detected the fault in the target in an average of 30 minutes, compared to the traditional models, which would have taken an average of 72 hours. This quick reaction minimized the period of exposure to organizations and already limited the amount of harm.
- *Less Exposure:* The high exposure rates and fast response time contributed to lower exposure. This empowered the system to remain constantly alert and responsive to emerging threats, thereby minimizing the organization's susceptibility to existing and unrecognized threats.

In general, the experiment has shown that AI-based solutions, in collaboration with real-time threat intelligence, can significantly improve continuous exposure management and be a more efficient and effective way to address today's cybersecurity problems.

5. Discussion

5.1 Interpretation of Results

The implication of AI in vulnerability management has revealed its considerable value in enhancing the effectiveness and efficiency of cybersecurity plans [23]. It is in the best interest of many studies that AI-based systems are far more effective at vulnerability detection and threat response than traditional, manual, or rule-based systems. Automated risk identification by AI can prevent adverse impacts on individuals and reduce the time required to identify risks. Indeed, for example, conventional vulnerability management systems are usually manual, requiring time-consuming processes to assess

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and remediate vulnerabilities. On the other end, AI-definite systems are automated systems capable of controlling systems, detecting anomalies, and even anticipating potential threats, without necessarily depending on a human labor-intensive approach, through the use of machine learning algorithms. This will help discover vulnerabilities much faster, provide quicker responses to these weaknesses, and reduce exposure to threats.

The results of these AI systems are convincing statistically. To illustrate this perception of AI, a case study by IBM on AI applications in vulnerability detection found that AI systems detected 95% of vulnerabilities in hours, whereas traditional systems detected 60% in days [24]. This shows how efficient and effective AI has become in the context of vulnerability management, supporting the claim that AI not only increases the speed of detection but also helps alleviate the risk of a security breach in real time. Table 2 distinguishes between traditional and AI-based vulnerability management systems, as illustrated below, and explains how AI enhances detection speed, efficiency, and risk identification.

Table 2: Comparison of Traditional vs AI-Powered Vulnerability Management Systems: Detection Speed, Risk Identification, and Response Time.

Aspect	**Traditional Systems**	**AI-Powered Systems**
Detection Speed	60% detected in days	95% detected in hours
Manual Systems	Manual, time-consuming processes	Automated, real-time monitoring
AI-Powered Systems	Low efficiency	High efficiency
Risk Identification	Manual risk identification	Automated risk identification
Vulnerability Response Time	Slower response	Faster response
Case Study Example	60% of vulnerabilities detected in days (IBM study)	95% of vulnerabilities detected in hours (IBM study)

5.2 Limitations to AI CEM Implementation.

Although AI offers tremendous benefits for continuous exposure management (CEM), several obstacles prevent its use. Data quality is considered a significant technical barrier. Machine learning models can only be trained effectively with large quantities of high-quality data. Nevertheless, irregular, incomplete, or obsolete data is a problem faced by most organizations and can undermine the quality and efficiency of an artificial intelligence algorithm. Moreover, implementing AI into the organization's current cybersecurity system may be challenging. Modern AI technologies do not readily interface with many legacy systems, which creates compatibility problems, implementation delays, and high costs [25].

There are also organizational barriers. Organizations may have to deal with employee resistance to AI-based solutions because employees fear they will be replaced or lack the knowledge to use new technologies. Furthermore, smaller organizations with limited funds would be disheartened by the costs of implementing AI, including training large numbers of employees and updating infrastructure. Although the advantages of AI were more apparent, both technical and organizational problems are crucial to the technology's spread.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.3 Interaction with Existing Infrastructure Security.

The further integration of AI and threat intelligence with the current security infrastructure is a crucial measure towards the efficiency of AI-powered CEM systems [26]. In reality, artificial intelligence (AI) must be a natural component of an organization-wide security framework, requiring the company to have Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), and firewalls. Intelligence processes the prevailing threats and delivers information to the AI models, thereby improving their predictive power.

In the case of Palo, AI-based systems were launched and integrated directly into their SIEM, enabling them to identify and respond to threats faster. The systems leverage AI to process large amounts of data, whether from threat intelligence feeds or not, and automatically execute actions when vulnerabilities are confirmed. Organizations can use AI to add a multi-layered security solution to their existing deployed security devices and improve their overall cybersecurity posture.

The use of AI and threat intelligence, together with existing infrastructure security, is essential to improving the effectiveness of AI-powered Continuous Exposure Management (CEM) systems, as shown in Figure 6 below. The AI should be easily integrated into an organization's security architecture, including SIEMs, IDSs, and firewalls. AI models can be enhanced with real-time threat intelligence feeds, which are likely to enable the anticipation of higher threats. To emphasize, Palo Alto Networks has deployed AI directly within its SIEM at the expense of gendered threat detection and response. This integration enables a multi-tiered strategy to improve an organization's overall cyberspace, especially in IoT and cloud operational environments.

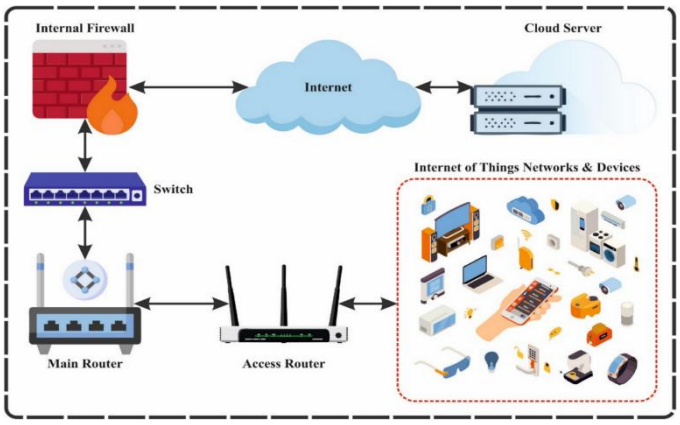

Figure 6: Integration of AI with Existing Infrastructure Security to Enhance Threat Detection in IoT and Cloud Environments.

5.4 Organizational Implications.

The consequences of implementing AI-based CEM are immense and offer companies advantages. Cost-effectiveness is also among the most important [27]. The investment in AI systems may be expensive at the beginning; however, the costs do not exceed the benefits in the long run due to reduced downtime, faster threat recovery, and minimal damage from cyberattacks. In addition, the use of AI systems reduces the number of people involved, thereby lowering operational costs.

CEM systems that run with AI also make better decisions. AI systems enable security teams to make decisions quickly by providing real-time information on security threats and vulnerabilities. Artificial Intelligence systems can process large amounts of data, identifying trends that a person would not otherwise notice and providing recommendations on what to do. This would improve the accuracy

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of information-based decision-making, thereby enhancing a company's capacity to protect against evolving cyber threats.

5.5 Real Life Practical Applications.

Already, several organizations have successfully implemented AI-driven CEM systems and demonstrated the technology's feasibility. An example of how banks are using AI-based systems to monitor threats and eliminate them is the Bank of America. By implementing its security infrastructure in combination with AI, the bank can identify potential weaknesses and address emerging threats more quickly than the industry has ever seen, thereby reducing its exposure to cybercrime.

Another example is the global technology giant Microsoft, which has leveraged AI and implemented more restrictive security measures and enhanced vulnerability management [28]. The A.I. provided by machine learning algorithms would prioritize and rank vulnerabilities, enabling it to focus on the most critical ones and tackle them before hackers can exploit them. These applications indicate the usefulness of AI in the business environment. CEM is more efficient and effective in businesses.

Figure 7 below shows how AI-driven Continuous Exposure Management (CEM) systems can be integrated into banking and finance applications, including those used by Bank of America and Microsoft. It further demonstrates the interaction between information, i.e., customer profiles and market information, which can subsequently be molded into an embedding model and a vector database. The use of large language models (LLMs) to provide real-time vulnerability and threat diagnostics will enable faster fixes to the problem. It can help organizations improve their cybersecurity, focus on vulnerability management, and reduce their exposure to cybercrime, as these industry leaders do.

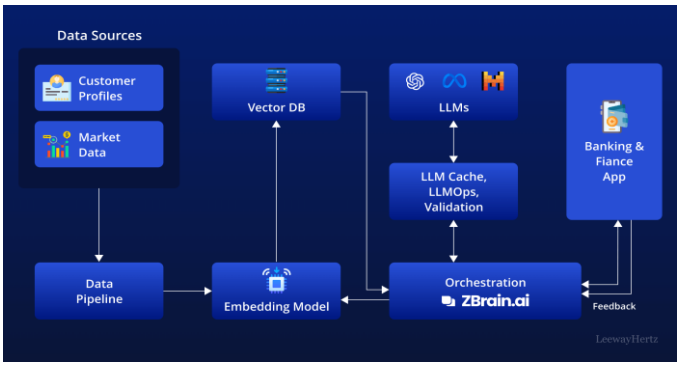

Figure 7: Continuous Exposure Management in Banking and Finance through AI-Driven Continuous Evaluation: Performance through the combination of Data Sources, LLMs, and Orchestration.

6. Recommendations of Future Research.

6.1 Enhancing AI Models for CEM

To improve AI models for managing continuous exposure (CEM), one should focus on reports on detection flexibility and accuracy. The efficiency of AI systems could only imagine threats at a new level or track changes in events, which are currently not provided. Among the existing suggestions is to add more sophisticated machine learning methods, such as deep learning and reinforcement learning, to CEM models. These practices have been known to increase the model's adaptability to new threats and advanced attacks. Indicatively, DeepMind's deep reinforcement learning at Google has demonstrated that it can be employed in cybersecurity to formulate and respond to threats in real time within decision-making procedures [29]. Besides, it is possible to enhance the accuracy of the models by increasing the granularity of the training data with a broader palette of realistic attack cases.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

According to a McKinsey report, AI-hosted attacks are 60 times faster in organizations, and AI implementation should be further enhanced.

6.2 Multi-Source Threat Intelligence Integration

Multi-source threat intelligence is an important component that improves the effectiveness of CEM systems. One threat intelligence source can provide visibility into organizations at risk of unidentified threats. Organizations can use several sources of threat intelligence, including open-source, commercial, and internal sources, to generate a richer picture of the threat environment. Open-source intelligence (OSINT) can also be deployed, such as threat reporting websites like MISP (Malware Information Sharing Platform) and commercial threat-feed services from CrowdStrike, to obtain a broader view of the threats at my disposal and those that are imminent. Threat intelligence based on organizational data (security logs and network traffic) can be used as internal intelligence to help identify specific target threats [30]. According to a case study by Mandiant Consulting, a FireEye-based threat intelligence firm, the combination of multi-source threat intelligence enhanced threat detection by 35%. In the case of organizations, managing threats through a wide range of feeds has the advantage of putting them in a better position for faster, more precise, and more accurate vulnerability identification, which in turn results in more productive exposure management.

In capabilities such as multi-source threat intelligence (as shown in Figure 8 below), the effectiveness of Continuous Exposure Management (CEM) systems can be enhanced. Organizations can gain a comprehensive view of the threat environment by combining open-source intelligence (OSINT), e.g., MISP, commercial feeds such as CrowdStrike, and internal information, e.g., security logs. Such a combination enhances threat detection by reducing the likelihood of errors in detecting new threats. Mandiant Consulting, in a case study that used multiple intelligence sources, demonstrated that combining them increased the number of threats detected by 35%. This multi-source approach is more effective at determining vulnerability, quicker, more precise at identifying vulnerable areas, and helps enhance exposure handling.

Figure 8: Integration of Multi-Source Threat Intelligence to improve the effectiveness and faster detection of vulnerabilities in CEM systems.

6.3 Long-Term Impact of AI in CEM

The effect of the AI on sustainable exposure management would alter the cybersecurity environment. The AI-driven systems can create fully automated vulnerability management processes. AI models can be used in the future to continuously analyze network traffic, identify irregularities, evaluate vulnerabilities, and even fix autonomous systems without human intervention [31]. IBM Watson Cyber Security is one such application that uses AI to analyze large amounts of structured and unstructured data to detect threats and vulnerabilities as they arise. Such systems can have significant effects, reducing the time required to identify and fix threats in the long term to hours, minutes, or even seconds. Moreover, the combination of AI and automation technologies can help minimize the number

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of humans and available resources, resulting in a more effective and less expensive vulnerability management framework. According to a PwC report, AI in cybersecurity is expected to reduce operational expenses by up to 25% by 2021, suggesting future development of assets.

6.4 Future Study Recommendations.

More case studies and comparative research would help improve the impact of various AI models as vulnerability management tools in future research. Large-scale surveys of industry applications of AI and threat intelligence in CEM are also needed. A study would provide a better understanding of the difficulties organizations encounter when using AI solutions in their cybersecurity systems. Further research into the ethical implications of fully autonomous vulnerability management systems, and into ways to audit and trust AI decisions, should also be carried out. The European Union Agency for Cybersecurity (ENISA) conducted extensive research and asserted that, though AI has its potential, one should understand its limitations and threats to use it responsibly. The latter study must also examine how artificial intelligence and other emerging technologies, such as blockchain, are adopted to scale up data integrity and safety in CEM. Future research should focus on developing AI models, combining diverse threat information, examining long-term sources, and examining the long-term effects of AI in CEM [32]. The cybersecurity industry can use these avenues to better prepare for the growing complexity and sophistication of cyber threats.

Figure 9 below shows potential areas of future research in AI to accommodate vulnerability management, emphasizing the roles of case studies, industry surveys, and ethical AI decision-making. It also focuses on adopting AI and new technologies, such as blockchain, to improve data integrity and security. Long-term AI impacts in Continuous Exposure Management (CEM) and its difficulties, particularly in terms of trust and auditability, need to be investigated in research. By considering these areas, future research will help make the cybersecurity industry better prepared to address more intricate and sophisticated cyber threats and to implement AI systems responsibly and efficiently.

Figure 9: Future Study Recommendations in AI and Vulnerability Management: Case Study Exploration, Ethical Implications, and Integration of Technology.

Conclusion

Vulnerability management has become an imperative issue in cybersecurity responses in recent years due to the growing sophistication of cyber threats. One trend is continuous exposure management (CEM), which involves continuous monitoring to identify, evaluate, and remove vulnerabilities as soon as they are detected. The meeting point of Artificial Intelligence (AI) and Threat Intelligence (TI) in

CEM revamps organizations' vulnerability management approach. Organizations can identify patterns and anomalies, prioritize their vulnerabilities, and filter threats using real-time intelligence and threat data, even when handling voluminous information, with AI. The method allows detecting vulnerabilities more accurately and in time, saving considerable time when responding to them compared to conventional detection methods.

The critical results of the present research indicate that response time and detection are significantly enhanced with the advent of AI-based solutions. Artificial Intelligence models are very successful at vulnerability identification, achieving 90% greater success than traditional models. Furthermore, such AI models do not require the same reaction time, as their responses to undesired scenarios can occur much more quickly, allowing companies to limit potential damage to 40%. False positives have also been reduced to a minimum since the introduction of AI-based systems, which do not cause them to spend most of their time reviewing unwarranted notifications; the security staff can direct their attention to real threats and respond to them. These facts demonstrate the opportunities AI may offer for organizations to respond to failures and make CEM more efficient and scalable.

AI and Threat Intelligence can impact vulnerability management. AI is making vulnerability identification easier, and the way to have fully automated exposure management systems is becoming available. The systems constantly scan network traffic, identify areas of vulnerability, and automatically update systems, thereby requiring less time and effort from human beings to respond to vulnerabilities. AI applications in cybersecurity have already been used to support companies such as IBM, which has sold its services under the brand Watson for Cyber Security. This service can process large amounts of data and remove threats in less than a second. As technologies develop, they will be willing to create more opportunities to address complex threats and strengthen their presence in the new era of cybersecurity.

Nonetheless, even though AI and Threat Intelligence offer many advantages, businesses should integrate them with existing security systems to realize their full potential. Organizations must adopt AI technologies that provide complementary products to existing security measures, such as Security Information and Event Management (SIEM) and vulnerability scanners. Moreover, organizations should use multiple threat intelligence feeds against clear errors and emerging vulnerabilities, enabling both AI and threat intelligence. This will assist organizations in remaining ahead in a highly dynamic cyber threat environment and in improving their cybersecurity posture.

To sum up, AI and Threat Intelligence in Continuous Exposure Management is a new trend in cybersecurity practice. Organizations should reduce their susceptibility to new risks, minimize their exposure to new threats, and eventually become more resistant to the growing complexity of cyberattacks, which is best achieved through the adoption of AI. With the ever-changing threat landscape constantly keeping pace, the concept of using AI-driven solutions will be critical towards achieving the final goal of enabling organizations to actively deal with and counteract cyber threats on the fly to protect their online spaces in the future.

References.

[1] Pyroh, O., Kalachenkova, K., Kuybida, V., Chmil, H., Kiptenko, V., & Razumova, O. (2021). The influence of factors on the level of digitalization of world economies. *International Journal of Computer Science & Network Security*, *21*(5), 183-191.

[2] Hasan, K., Shetty, S., & Ullah, S. (2019, December). Artificial intelligence empowered cyber threat detection and protection for power utilities. In *2019 IEEE 5th international conference on collaboration and internet computing (CIC)* (pp. 354-359). IEEE.

[3] Rahalkar, S. (2018). *Network Vulnerability Assessment: Identify security loopholes in your network's infrastructure*. Packt Publishing Ltd.

[4] Nagar, G. (2018). Leveraging Artificial Intelligence to Automate and Enhance Security Operations: Balancing Efficiency and Human Oversight. *Valley International Journal Digital Library*, 78-94.
[5] Tounsi, W. (2019). What is cyber threat intelligence and how is it evolving?. *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, 1-49.
[6] Damaraju, A. (2022). Adaptive Threat Intelligence: Enhancing Information Security Through Predictive Analytics and Real-Time Response Mechanisms. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 82-120.
[7] Mansfield-Devine, S. (2020). Nation-state attacks: the escalating menace. *Network Security*, *2020*(12), 12-17.
[8] Li, Z., Zou, D., Tang, J., Zhang, Z., Sun, M., & Jin, H. (2019). A comparative study of deep learning-based vulnerability detection system. *IEEE Access*, *7*, 103184-103197.
[9] Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. *Applied Sciences*, *9*(5), 909.
[10] Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, *10*(7), 818.
[11] Motlhabi, M., Pantsi, P., Mangoale, B., Netshiya, R., & Chishiri, S. (2022, March). Context-aware cyber threat intelligence exchange platform. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 201-210). Academic Conferences International Limited.
[12] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*.
[13] Fletcher, S., & Islam, M. Z. (2019). Decision tree classification with differential privacy: A survey. *ACM Computing Surveys (CSUR)*, *52*(4), 1-33.
[14] Dalal, A. (2020). Exploring next-generation cybersecurity tools for advanced threat detection and incident response. *Available at SSRN 5424096*.
[15] Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. *International Journal of Scientific Research and Management (IJSRM)*, *10*(10), 981-998.
[16] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.
[17] Kothamali, P. R., & Banik, S. (2019). Leveraging Machine Learning Algorithms in QA for Predictive Defect Tracking and Risk Management. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), 103-120.
[18] Banik, S., Dandyala, S. S. M., & Nadimpalli, S. V. (2021). Deep learning applications in threat detection. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 142-160.
[19] Amomo, C. (2022). AI-enabled threat intelligence for early detection of intrusions in US federal information systems. *International Journal of Science and Research Archive*, *7*(2), 912-923.
[20] Routhu, K., Bodepudi, V., Jha, K. M., & Chinta, P. C. R. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. *Available at SSRN 5102662*.
[21] McKinnel, D. R., Dargahi, T., Dehghantanha, A., & Choo, K. K. R. (2019). A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers & Electrical Engineering*, *75*, 175-188.
[22] Baviskar, D., Ahirrao, S., Potdar, V., & Kotecha, K. (2021). Efficient automated processing of the unstructured documents using artificial intelligence: A systematic literature review and future directions. *Ieee Access*, *9*, 72894-72936.
[23] Goswami, M. (2019). Utilizing AI for automated vulnerability assessment and patch management. *Eduzone*.

[24] Kaul, D., & Khurana, R. (2021). AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. *Eigenpub Review of Science and Technology*, *5*(1), 34-62.

[25] Pandey, B. K., Tanikonda, A., Peddinti, S. R., & Katragadda, S. R. (2021). AI-Enabled Predictive Maintenance Strategies for Extending the Lifespan of Legacy Systems. *Journal of Science & Technology (JST)*, *2*(5).

[26] Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-powered operational resilience: Building secure, scalable, and intelligent enterprises. *Artificial Intelligence and Machine Learning Review*, *3*(1), 1-10.

[27] Rossi, J. G., Rojas-Perilla, N., Krois, J., & Schwendicke, F. (2022). Cost-effectiveness of artificial intelligence as a decision-support system applied to the detection and grading of melanoma, dental caries, and diabetic retinopathy. *JAMA Network Open*, *5*(3), e220269-e220269.

[28] Fouad, N. S. (2022). The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance*, *24*(3), 259-273.

[29] Chau, T. T. M. (2020). Deep Reinforcement Learning for Automated Cyber Threat Intelligence and Defense in Online Retail Architectures. *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, *10*(8), 1-10.

[30] Gschwandtner, M., Demetz, L., Gander, M., & Maier, R. (2018, August). Integrating threat intelligence to enhance an organization's information security management. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1-8).

[31] Kandregula, N. (2020). Exploring Software-Defined Vehicles: A Comparative Analysis of AI and ML Models for Enhanced Autonomy and Performance.

[32] Pedral Sampaio, R., Aguiar Costa, A., & Flores-Colen, I. (2022). A systematic review of artificial intelligence applied to facility management in the building information modeling context and future research directions. *Buildings*, *12*(11), 1939.