World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Leveraging generative AI for Security: Opportunities and challenges

Yogesh Kumar Bhardwaj *

CAPELLA UNIVERSITY, USA.

World Journal of Advanced Research and Reviews, 2025, 26(02), 1536-1543

Publication history: Received on 02 April 2025; revised on 10 May 2025; accepted on 12 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1831

Abstract

This article explores the transformative role of Generative Artificial Intelligence (GenAI) in cybersecurity operations. While traditional AI systems have focused primarily on predictive and classification tasks, GenAI creates entirely new content based on patterns learned from extensive datasets, representing both significant opportunities and notable challenges for security professionals. It examines the dual nature of GenAI, highlighting how the same technologies that enable sophisticated threat actor capabilities also provide powerful defensive tools. Key security applications include automated log analysis, threat intelligence processing, biometric authentication enhancements, and predictive maintenance of security infrastructure. The article details operational benefits including reduced analyst workload, enhanced productivity, decreased cognitive fatigue, accelerated onboarding processes, and improved team collaboration. The article further analyzes implementation approaches across varying complexity levels, providing organizations with a framework to assess their GenAI security journey based on their security maturity and technical capabilities.

Keywords: Generative Artificial Intelligence; Cybersecurity Operations; Threat Detection; Security Automation; Compliance Management

1. Introduction

Generative Artificial Intelligence (GenAI) has emerged as a transformative technology across numerous sectors, including cybersecurity. The Journal of Information Security and Applications reports that the global AI cybersecurity market is experiencing unprecedented growth, projected to reach significant valuation within the next several years with a substantial compound annual growth rate [1]. Unlike traditional AI/ML systems that primarily focus on prediction and classification, GenAI creates entirely new content—text, images, code, and more—based on patterns learned from extensive datasets. This distinction represents both a significant opportunity and a notable challenge for security professionals. According to recent empirical studies, organizations implementing GenAI for security operations have reported considerable efficiency improvements in threat analysis workflows, allowing security teams to redirect substantial analyst time toward more complex security challenges [1]. The integration of these advanced AI capabilities into security frameworks has fundamentally transformed how organizations approach threat detection, vulnerability management, and incident response processes.

1.1. Traditional AI vs. Generative AI in Security

Traditional AI/ML systems have long established their value in security operations. Research published in the Journal of Student Research demonstrates that these conventional AI approaches excel at identifying class membership, applying labels to data, forecasting future performance, and powering enterprise search functionality with high detection rates for known attack patterns [2]. These systems form the backbone of conventional security operations centers, processing numerous security events per second in large enterprise environments. Traditional speech

* Corresponding author: Yogesh Kumar Bhardwaj.

recognition systems achieve low word error rates in controlled environments, while computer vision implementations for remote inspection can identify anomalies with impressive accuracy. The efficacy of these systems for anomaly detection in logs has been well-documented, with baseline performance metrics showing substantial accuracy in identifying deviations from established patterns when properly tuned to organizational environments [2].

Table 1 Traditional AI vs. Generative AI in Security [2]

Aspect	Traditional AI/ML	Generative AI
Core Function	Prediction and classification	Content creation and synthesis
Key Applications	Anomaly detection, classification, pattern recognition	Report generation, code development, natural language interfaces
Data Handling	Structured data with defined features	Multi-modal data with contextual understanding
User Interaction	Limited natural language capabilities	Advanced conversation and reasoning
Implementation	Focused on specific use cases	Ranges from simple to highly complex

Generative AI, by contrast, fundamentally transforms security operations through its creative capabilities. The Journal of Student Research documents how GenAI solutions focus on drafting comprehensive reports and summaries, reducing documentation time while simultaneously increasing the accuracy of threat assessments [2]. When deployed for supporting customer interactions via chat interfaces, these systems successfully resolve many tier-one security inquiries without human intervention. Organizations leveraging GenAI for creating visual media for security training report improvements in employee retention of security best practices and decreases in security policy violations. Voice content generation for Interactive Voice Response (IVR) systems demonstrates high intelligibility with proper security guardrails, while code generation for Security Operations (SecOps) reduces development time for security automation across implementations documented in controlled studies [2].

1.2. The Dual Nature of GenAI in Security

The accessibility of GenAI tools through open-source platforms, affordable solutions, and cloud services has created a cybersecurity paradox that security professionals must navigate with increasing sophistication. Research published through ResearchGate reveals that a majority of enterprise organizations now utilize some form of GenAI in their security operations, with implementation costs decreasing significantly in recent years [3]. This democratization of advanced AI capabilities has accelerated adoption across organizations of all sizes, with medium-sized businesses showing the most dramatic increase in implementation. The research demonstrates that organizations implementing comprehensive GenAI security frameworks experienced notable reductions in mean time to detect (MTTD) significant security events and in mean time to respond (MTTR), translating to substantial cost avoidance per security incident for large enterprises [3]. However, this same technological accessibility presents significant challenges as threat actors increasingly harness these tools for malicious purposes, creating an ongoing technological arms race between defenders and attackers.

1.3. Enhanced Threat Capabilities

The empirical examination of AI-powered security systems published on ResearchGate provides extensive documentation of how GenAI enables adversaries to develop increasingly sophisticated attack methodologies [3]. The research demonstrates that GenAI-crafted phishing attempts have a higher success rate than conventional methods, with traditional detection systems flagging a much smaller percentage of these advanced attempts compared to traditional phishing emails. This dramatic reduction in detection efficacy presents significant challenges for conventional security frameworks that rely heavily on pattern matching and rule-based approaches [3].

The International Journal of Advanced Research in Computer and Communication Engineering provides comprehensive data on the development of new malware or enhancement of existing variants through GenAI assistance [4]. Their analysis documents a substantial increase in polymorphic malware variants attributed to GenAI-assisted development in recent years. These advanced malware implementations demonstrate greater resilience against signature-based detection methods and improved evasion capabilities against behavioral analysis. The research further indicates that even threat actors with limited technical expertise can leverage GenAI to develop sophisticated malware, with experimental simulations showing that individuals with basic programming knowledge could produce enterprise-grade malicious code in many test scenarios when provided with GenAI assistance [4].

Table 2 GenAI's Dual Nature in Security [4]

Domain	Threat Actor Uses	Defensive Applications
Content Generation	Sophisticated phishing, deepfakes	Enhanced detection, training simulations
Code	Polymorphic malware, exploit development	Vulnerability remediation, security automation
Data Analysis	Target identification, vulnerability discovery	Threat intelligence, anomaly detection
Decision Support	Attack planning, evasion techniques	Incident response, risk prioritization

The capability for efficient reconnaissance through rapid analysis of open-source and proprietary data represents another significant challenge documented in the research. Advanced persistent threat (APT) groups utilizing GenAI tools have demonstrated the ability to process and correlate data from numerous sources in remarkably short timeframes, a task that previously required weeks of manual effort [3]. This dramatic acceleration of the intelligence gathering phase of the attack lifecycle provides adversaries with unprecedented advantages in identifying potential targets and vulnerabilities. The research indicates that GenAI-assisted reconnaissance efforts achieve greater accuracy in identifying exploitable vulnerabilities compared to traditional methods, with many of these discoveries occurring before organizations had implemented appropriate remediation measures [3].

The ability to identify valuable targets and vulnerabilities faster than remediation measures can be implemented represents perhaps the most concerning trend identified in the research. The International Journal of Advanced Research in Computer and Communication Engineering reports that the average time from vulnerability discovery to exploitation has decreased significantly for GenAI-equipped threat actors, according to extensive research across numerous security incidents [4]. This compressed timeframe creates significant challenges for security teams, as the traditional patch management lifecycle now frequently exceeds the window of opportunity for remediation before exploitation occurs. Organizations reporting the most success in addressing this challenge have implemented automated patching solutions covering a large portion of their infrastructure, reducing mean time to remediate for critical vulnerabilities [4].

2. Proactive Security Applications for GenAI

While the threat landscape has evolved significantly with the advent of GenAI technologies, these same capabilities provide powerful tools for enhancing organizational security postures. The Journal of Information Security and Applications documents numerous successful implementations of GenAI for cyber threat detection, with leading platforms processing substantial volumes of network traffic while maintaining high accuracy in anomaly detection [1]. These systems have demonstrated the ability to recognize more zero-day attack signatures than traditional systems through advanced pattern recognition and contextual analysis capabilities. The research further indicates that GenAI-powered threat detection solutions achieve enhanced accuracy and speed, with reduced false positive rates compared to conventional rule-based approaches while simultaneously increasing true positive identification across diverse threat categories [1].

The implementation of GenAI for fraud detection represents another significant area of security enhancement documented in the Journal of Student Research [2]. Advanced GenAI systems demonstrate the capability to process vast numbers of transactions while flagging suspicious patterns with high precision, dramatically outperforming traditional rule-based approaches. The research documents a reduction in false positives when GenAI augments traditional fraud detection systems, significantly reducing the operational burden on security teams while improving detection efficacy. Organizations implementing comprehensive GenAI-based fraud detection report substantial cost savings for large financial institutions, representing a significant return on investment within the first several months of deployment [2].

The empirical examination published on ResearchGate highlights the significant advancements in biometric authentication enabled by GenAI technologies [3]. These systems achieve very low error rates for multimodal authentication implementations, representing a substantial improvement over traditional approach. GenAI-powered biometric authentication demonstrates strong resistance to presentation attacks (including deepfakes and synthetic fingerprints) in controlled testing environments, addressing one of the most significant vulnerabilities in conventional biometric implementations. The research further indicates that these enhanced systems reduce authentication time while improving accuracy compared to conventional biometric implementations, simultaneously enhancing both security and user experience [3].

The International Journal of Advanced Research in Computer and Communication Engineering documents significant advancements in predictive maintenance for security infrastructure through GenAI implementation [4]. These systems demonstrate the ability to analyze equipment sensor data from numerous sensors simultaneously, detecting potential failures with high accuracy well before critical systems would otherwise fail. Organizations implementing comprehensive predictive maintenance solutions report increased operational efficiency, reducing unplanned downtime of security systems across documented implementations. The research indicates substantial cost savings for large companies through preemptive maintenance of security infrastructure, representing a significant return on investment over traditional reactive maintenance approaches [4].

Video surveillance analysis represents one of the most dramatic transformations enabled by GenAI technologies. Research published in the Journal of Information Security and Applications documents systems capable of real-time analysis of video feeds from numerous cameras simultaneously using distributed GenAI processing architectures [1]. These systems achieve high accuracy for common security events and good accuracy for novel or unusual activities, dramatically outperforming conventional motion-based detection methods. The implementation of these advanced capabilities has resulted in improved monitoring efficiency, reducing false alarms while increasing true positive detection compared to traditional surveillance systems. Security personnel augmented with GenAI video analytics demonstrate the ability to effectively monitor many more camera feeds than unassisted operators while maintaining higher detection rates, significantly enhancing the scalability and efficacy of physical security operations [1].

3. Operational Benefits and Key Security Use Cases for Generative AI: A Detailed Analysis

3.1. Operational Benefits of GenAI in Security

The integration of Generative AI (GenAI) into security operations centers has revolutionized how teams handle security challenges. According to comprehensive research on security operations centers, the implementation of GenAI has led to a dramatic restructuring of analyst workloads, with time spent on routine tasks significantly reduced, freeing security professionals to focus on complex tasks that require human judgment and expertise [5]. This shift in workload distribution has fundamentally transformed the operational capacity of security teams, enabling them to address sophisticated threats that previously might have gone undetected due to resource constraints.

Beyond simple time efficiency, empirical evidence demonstrates substantial enhancements in human performance within security workflows. A detailed study documented significant improvement in analyst productivity measured by incidents handled per hour when augmented with GenAI capabilities, representing a paradigm shift in how security operations can scale to meet growing threat volumes without proportional increases in staffing [5]. This productivity boost translates directly to improved security posture as teams can process and respond to substantially more potential threats with the same human resources, creating a multiplier effect on security team effectiveness.

The psychological impact of GenAI on security professionals represents a crucial but often overlooked benefit. Longitudinal research into analyst experience found that a majority of security professionals reported reduced cognitive fatigue after GenAI implementation, with corresponding improvements in job satisfaction and decision quality [5]. This reduction in cognitive burden addresses a fundamental challenge in the cybersecurity industry—analyst burnout and fatigue that often leads to missed detections and high turnover rates. By automating the most mentally taxing aspects of security operations, GenAI preserves human cognitive resources for tasks where human judgment adds the most value.

The acceleration of onboarding processes for security personnel demonstrates another critical operational benefit in today's competitive cybersecurity talent landscape. Detailed analysis shows that onboarding time for new security analysts decreased substantially in organizations that implemented comprehensive GenAI training and assistance tools [7]. This dramatic reduction in time-to-effectiveness addresses one of the industry's most persistent challenges—the shortage of skilled cybersecurity professionals. By enabling more rapid development of effective analysts, organizations can better maintain security operations despite talent shortages and high turnover rates.

Team collaboration and coordination show remarkable improvements with GenAI implementation. Research indicates that a significant majority of security teams reported improved collaboration efficiency after implementing GenAI tools that provide consistent documentation, shared context, and centralized intelligence [7]. This enhanced coordination is particularly valuable in complex security environments where multiple teams must work in concert to address sophisticated threats. The standardization of information presentation and analysis that GenAI enables creates a shared operational picture that improves team cohesion and response effectiveness across distributed security operations.

3.2. Key Security Use Cases for GenAI

3.2.1. Automated Security Log Analysis

The sheer volume of security telemetry represents a fundamental challenge that GenAI addresses through transformative improvements in processing capacity. Technical benchmarking shows that processing capacity for log analysis increased substantially when organizations transitioned from traditional rule-based systems to GenAI-powered analysis [6]. This significant improvement in raw processing power enables comprehensive coverage of security events across even the largest enterprise environments, eliminating the sampling and prioritization that often leaves security gaps in conventional approaches.

The quality of threat detection shows even more dramatic improvements than raw processing capacity. Comparative testing documented that GenAI demonstrated higher accuracy in identifying novel threats compared to traditional machine learning methods, with particularly significant improvements in detecting zero-day exploits and sophisticated attack patterns that lack established signatures [6]. This enhanced detection capability represents a fundamental shift from reactive to proactive security, enabling organizations to identify and mitigate threats before significant damage occurs rather than simply responding to known attack patterns.

The speed of threat detection—a critical factor in limiting attack impact—shows substantial improvement with GenAI implementation. Detailed operational measurements revealed a significant reduction in mean time to detect (MTTD) security incidents when security operations were augmented with GenAI capabilities [5]. This acceleration of detection processes directly correlates with reduced attack impact, as security teams can interrupt attack progressions earlier in the kill chain, preventing attackers from achieving their objectives or establishing persistence within target environments.

The efficiency of security investigations improves dramatically with GenAI-powered natural language interfaces to security data. Research demonstrates that natural language security queries reduced search time compared to traditional query languages and user interfaces [7]. This improvement in search efficiency enables more comprehensive investigations as analysts can explore more hypotheses and examine more data within the same time constraints. The intuitive nature of natural language interaction also reduces the technical barrier to effective security investigations, enabling less specialized staff to contribute meaningfully to security operations.

3.2.2. Threat and Vulnerability Management

The analysis of threat intelligence represents a time-intensive process that benefits substantially from GenAI capabilities. Detailed time studies documented a substantial reduction in time required for threat intelligence analysis when augmented with GenAI summarization and correlation capabilities [7]. This dramatic efficiency improvement enables security teams to process and apply vastly more threat intelligence than was previously possible, enhancing their ability to anticipate and prepare for emerging threats before they materialize as attacks on the organization.

The correlation of security events across diverse data sources shows substantial improvement with GenAI implementation. Comparative analysis revealed that context-aware threat correlation improved significantly with GenAI compared to rule-based systems, enabling the identification of complex attack patterns that span multiple systems and time periods [6]. This enhanced correlation capability enables security teams to identify sophisticated attacks that deliberately operate below the threshold of detection in any single security domain, addressing a fundamental limitation of traditional security monitoring approaches.

The signal-to-noise ratio in security alerting—a persistent challenge in security operations—shows remarkable improvement with GenAI implementation. Operational measurements documented a significant reduction in false positives through GenAI-enhanced alert triage without corresponding increases in false negatives or missed detections [5]. This improvement in alert quality directly addresses one of the most significant operational challenges in security operations: alert fatigue that leads to missed detections as analysts become desensitized to constantly triggering alerts. By dramatically reducing false positives while maintaining detection sensitivity, GenAI enables security teams to focus on genuine threats without the cognitive burden of constant false alarms.

The automation of security remediation represents a particularly valuable capability that GenAI substantially enhances. Performance testing showed that automation success rates for remediation actions increased substantially when traditional automation was enhanced with GenAI capabilities [6]. This improvement in remediation reliability enables organizations to implement more comprehensive automation of security responses, reducing both the mean time to respond and the operational burden on security teams. The contextual awareness that GenAI brings to automation

decisions enables more nuanced responses that adapt to the specific circumstances of each security incident rather than applying one-size-fits-all remediation actions.

3.2.3. Deep Analysis of Security Reports

The quality of security documentation represents a critical factor in effective security operations that GenAI significantly enhances. Comparative assessment demonstrated a notable improvement in accuracy of security incident documentation when augmented with GenAI capabilities [7]. This enhancement in documentation quality improves both the immediate response to security incidents and the long-term learning process that security teams undergo as they analyze past incidents to improve future responses. By ensuring comprehensive and accurate documentation, GenAI enables more effective knowledge transfer and process improvement across security operations.

The speed of security response shows substantial improvement with GenAI implementation. Detailed operational measurements revealed that mean time to respond (MTTR) decreased significantly in organizations implementing GenAI for security analysis and response coordination [6]. This acceleration of response activities directly correlates with reduced impact from security incidents, as faster containment and remediation limit the damage that attackers can inflict and the data they can exfiltrate. The improvement in response time creates a virtuous cycle in security operations, as faster resolution of incidents frees resources to address other security challenges, further enhancing overall security effectiveness.

3.2.4. Robust Data Protection

The efficiency of compliance processes represents a critical operational concern that GenAI substantially improves. Detailed time studies showed that organizations implementing AI-powered compliance tools reduced audit preparation time significantly while simultaneously improving the comprehensiveness and accuracy of compliance documentation [8]. This efficiency gain enables more robust compliance processes without corresponding increases in operational overhead, addressing the growing regulatory burden that organizations face across multiple jurisdictions and regulatory frameworks.

The detection of compliance violations shows dramatic improvement with GenAI implementation. Comparative testing documented that regulatory violation detection improved substantially with AI monitoring compared to traditional compliance checking approaches [8]. This enhancement in violation detection enables more proactive compliance management, as organizations can identify and address potential regulatory issues before they trigger formal findings in compliance audits. The continuous nature of GenAI-powered compliance monitoring creates a dynamic compliance posture that adapts to changing regulations and organizational circumstances rather than relying on point-in-time assessments.

The assessment of data breach risk represents a complex analytical challenge that GenAI significantly enhances. Validation testing showed that data breach risk assessment accuracy improved markedly with GenAI analytics compared to traditional risk assessment methodologies [8]. This improvement in risk assessment enables more effective prioritization of security investments and more targeted remediation of security vulnerabilities. By providing more accurate assessments of where breaches are most likely to occur and what their potential impact might be, GenAI enables organizations to focus their limited security resources where they will deliver the greatest risk reduction.

3.2.5. Security and Compliance Chatbots

The resolution of security and compliance inquiries represents a time-intensive process that GenAI dramatically streamlines. Operational measurements showed that the vast majority of compliance queries were successfully resolved by GenAI chatbots without requiring human intervention, freeing specialized compliance and security staff to focus on more complex issues [8]. This high resolution rate enables more comprehensive coverage of security and compliance questions across the organization, ensuring that employees have ready access to the guidance they need to maintain secure operations without creating an unsustainable burden on specialized security and compliance staff.

The economic impact of GenAI in compliance operations represents a compelling return on investment. Financial analysis documented that the cost of compliance management reduced substantially over time following implementation of comprehensive GenAI compliance tools [8]. This cost reduction stems from both the direct automation of compliance tasks and the indirect benefits of more effective compliance processes that reduce the incidence and impact of compliance failures. The economic case for GenAI in compliance operations is particularly strong given the increasing financial penalties associated with compliance failures across multiple regulatory frameworks.

Table 3 Security and Compliance Applications [8]

Domain	Applications	Key Benefits
Regulatory Compliance	Policy mapping, continuous monitoring	Reduced compliance burden, proactive management
Security Documentation	Policy generation, procedure development	Standardization, faster development
Risk Assessment	Threat modeling, impact analysis	Comprehensive analysis, strategic prioritization
Incident Response	Alert triage, response orchestration	Faster response time, consistent execution

3.3. Implementation Complexity Spectrum

The implementation of GenAI for security operations spans a spectrum from relatively straightforward applications to highly complex integrations. Each point on this spectrum represents different levels of investment, technical complexity, and potential return. The most accessible implementations focus on augmenting existing security processes with GenAI capabilities, while more complex implementations involve fundamental restructuring of security operations around GenAI-centric workflows. Organizations should carefully assess their security maturity and technical capabilities when determining where to begin their GenAI implementation journey.

Basic implementations typically focus on discrete use cases with clearly defined boundaries, such as the automation of routine security documentation or the enhancement of threat intelligence analysis. These targeted implementations deliver substantial benefits with relatively modest investment and disruption, making them ideal starting points for organizations beginning their GenAI journey. The focused nature of these implementations also facilitates clear measurement of benefits and return on investment, building organizational confidence in the value of GenAI for security operations.

Table 4 GenAI Implementation Framework [8]

Phase	Key Activities	Success Metrics
Assessment	Security maturity evaluation, use case prioritization	Clear requirements, defined success criteria
Pilot	Limited scope implementation, controlled testing	Functionality validation, performance benchmarks
Deployment	Scaled implementation, workflow integration, training	Adoption metrics, efficiency improvements
Optimization	Performance tuning, use case expansion	Operational improvements, ROI achievement

Advanced implementations typically involve deeper integration of GenAI across multiple security domains and processes, creating a cohesive security fabric that leverages GenAI capabilities throughout the security lifecycle. These comprehensive implementations deliver transformative benefits but require substantial investment in technology, process redesign, and staff development. Organizations pursuing advanced implementations should plan for extended implementation timelines and ensure strong executive sponsorship to sustain the initiative through inevitable challenges and adjustments.

4. Conclusion

The integration of Generative AI into security operations represents both a significant challenge and an unprecedented opportunity for organizations navigating an increasingly complex threat landscape. The empirical research documented across multiple academic sources demonstrates that while GenAI has enabled adversaries to develop more sophisticated attack methodologies, these same technologies provide security teams with powerful tools to enhance detection capabilities, improve operational efficiency, and implement proactive security measures. Organizations that successfully leverage these advanced capabilities report significant improvements across key security metrics,

including reduced detection and response times, improved accuracy in threat identification, and substantial cost savings through operational efficiencies.

The psychological benefits for security analysts should not be overlooked, as GenAI's ability to reduce cognitive burden and automate repetitive tasks directly addresses the industry-wide challenges of burnout and high turnover rates. Similarly, the acceleration of onboarding processes through GenAI-powered training tools helps organizations maintain effective security operations despite the persistent shortage of skilled cybersecurity professionals.

As organizations consider GenAI implementation, they should approach this journey strategically, beginning with clearly defined use cases that deliver immediate value while building institutional knowledge and confidence. More advanced implementations that integrate GenAI across the entire security lifecycle offer transformative potential but require substantial investment in technology, process redesign, and organizational change management.

As GenAI technologies continue to evolve at an accelerating pace, security professionals must remain at the forefront of these advancements, continuously adapting defensive strategies to address emerging threats while leveraging the transformative potential of these technologies to enhance organizational security postures. The future of cybersecurity will likely belong to organizations that most effectively balance human expertise with GenAI capabilities, creating security operations that are simultaneously more comprehensive, efficient, and resilient than traditional approaches.

References

[1] Irshaad Jada, Thembekile O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," Data and Information Management, Volume 8, Issue 2, June 2024, Available: https://www.sciencedirect.com/science/article/pii/S2543925123000372

[2] Kadhir V. Palani, et al, "Impact of AI and Generative AI in Transforming Cybersecurity," 2024, JSR, Available: https://www.jsr.org/hs/index.php/path/article/view/6710/3112

[3] Justyna Żywiołek, "EMPIRICAL EXAMINATION OF AI-POWERED DECISION SUPPORT SYSTEMS: ENSURING TRUST AND TRANSPARENCY IN INFORMATION AND KNOWLEDGE SECURITY," June 2024, Scientific Papers of Silesian University of Technology Organization and Management Series, Available: https://www.researchgate.net/publication/381552222_EMPIRICAL_EXAMINATION_OF_AI-POWERED_DECISION_SUPPORT_SYSTEMS_ENSURING_TRUST_AND_TRANSPARENCY_IN_INFORMATION_AND_KNOWLEDGE_SECURITY

[4] Jayasudha Yedalla, "AI-Generated Cyber Threats the Rise of Autonomous Hacking Systems," IJARCCE, 2024, Available: https://ijarcce.com/wp-content/uploads/2025/03/IJARCCE.2024.131263.pdf

[5] James Bono, et al, "Generative AI and Security Operations Center Productivity: Evidence from Live Operations," November 2024, Online, Available: https://www.researchgate.net/publication/385560290_Generative_AI_and_Security_Operations_Center_Productivity_Evidence_from_Live_Operations

[6] Daniel Licea, "COMPARING TRADITIONAL AI AND GENERATIVE AI IN MODERN CYBERSECURITY DEFENSE," November 2024, Online, Available: https://www.researchgate.net/publication/386346649_COMPARING_TRADITIONAL_AI_AND_GENERATIVE_AI_IN_MODERN_CYBERSECURITY_DEFENSE

[7] Narayanan Ganesh, et al, "SUSTAINABLE HORIZONS: GENERATIVE AI'S EVOLUTION IN EMPOWERING SECURITY OPERATIONS CENTERS," 2024, ijnrd, Available: https://www.ijnrd.org/papers/IJNRD2407096.pdf

[8] Adebola Folorunso, et al, "Impact of AI on cybersecurity and security compliance," November 2024, Online, GJETA, Available: https://www.researchgate.net/publication/385558741_Impact_of_AI_on_cybersecurity_and_security_compliance