Journal of Next-Generation Research 5.0 (JNGR 5.0)

E-ISSN: 3075-2868 Website: www.jngr5.com Email: editor@jngr5.com

AI-Driven Threat Intelligence for Enterprise Cybersecurity

Ifeanyi Kingsley Kwentoa

Sheffield Hallam University, United Kingdom

Abstract

The research investigates how artificial intelligence technologies operate within enterprise cybersecurity frameworks by studying threat intelligence automation and advanced detection techniques. The research uses extensive literature analysis to show that machine learning algorithms achieve detection accuracies above 95% and deep learning approaches enhance F1-scores by up to 33% above traditional methods. Real-time data integration with behavioral analytics boosts threat identification abilities, allowing systems to detect 150,000 threats per minute and preventing 8 out of 10 attacks from causing system compromise. The current implementations primarily use centralized architectures, but distributed approaches show benefits for particular deployment situations. The research identifies essential challenges, which include privacy concerns, transparency limitations, algorithmic bias, data quality issues, and integration complexity. The research demonstrates that effective countermeasures against advanced threats require security innovations governed by comprehensive frameworks that balance technological capabilities with ethical considerations through continuous evaluation processes.

Keywords: Artificial Intelligence, Cybersecurity, Threat Intelligence, Machine Learning, Behavioral Analytics

1. Introduction

The digital environment is evolving rapidly, while enterprise cybersecurity must overcome unprecedented threats because standard detection systems cannot handle sophisticated cyberattacks. The rising complexity and velocity of contemporary threats and their elevated volume have made traditional security methods insufficient, thus demanding innovative solutions for immediate implementation [1]. Artificial intelligence technologies bring revolutionary capabilities to cybersecurity through enhanced threat detection and analysis and response features, which outperform traditional security methods.

Research data shows AI-based cybersecurity solutions deliver more than 95% accurate results across different implementation scenarios [2-4]. Security applications benefit from Random Forest machine learning algorithms and deep learning methods that deliver 33% better F1-score performance than conventional security methods [5]. These technological systems allow security systems to analyze massive threat data volumes because certain implementations identify between 150,000 network threats each minute within enterprise networks [6].

AI-powered solutions demonstrate improved operational efficiency through their capabilities beyond basic detection functions. According to research [7], the reduction of false positive and false negative rates reaches up to 40% and 43.8%, respectively, which solves a major cybersecurity operational challenge. The reduction in response times has been significant because certain implementations show a 33% decrease, and certain systems detect threats in less than 2 seconds [7, 8].

The main benefit of AI technology is that it leads organizations to adopt proactive security measures instead of reactive ones. Organizations can identify APTs early through real-time data integration and behavioral analytics, leading to the detection of eight out of ten attacks before system compromise occurs [9]. A proactive security approach becomes essential for big organizations, which face amplified security risks because of their extensive attack surface and valuable information assets.

This article examines how artificial intelligence enhances enterprise cybersecurity by automating threat intelligence processes. Drawing on recent research findings, we investigate AI models, real-time data integration architectures, and behavioral analytics methodologies, analyzing their collective impact on detection accuracy, response times, and predictive capabilities while acknowledging the ethical and operational challenges accompanying these technological advances.

2. Conceptual Framework

Enterprise cybersecurity depends on threat intelligence, which involves organized data acquisition and processing and analytical activities to identify current and future cyber threats against organizational assets. Multiple studies have defined threat intelligence as producing actionable knowledge from various data sources, which helps organizations understand threat actor capabilities, intentions, and methodologies [10, 11]. The enterprise environment holds special importance because large organizations must deal with advanced threat environments where persistent attackers use strategic methods to gain sustained access [12].

2.1 AI Technologies in Cybersecurity

2.1.1 Machine Learning Models and Applications

According to Sharma, Machine learning is the leading AI technology in cybersecurity applications because it appears in 18 out of 25 studies [1]. Multiple studies show that Random Forest algorithms deliver superior performance in various threat scenarios by achieving accuracy rates above 95% [2, 13]. Krishnan et al. [3] obtained 99.81% accuracy and a 0.001 false positive rate when implementing machine learning methods to protect cloud infrastructure. Ensemble configurations of Support Vector Machines (SVM), Decision Trees, and K-Nearest Neighbors (KNN) demonstrate substantial effectiveness according to Khan et al. [14] and Shan and Myeong [15]. Machine learning approaches provide processing abilities that surpass human capabilities because specific systems can identify between 150,000 network threats during one minute, according to Kim and Yoon [6].

2.1.2 Natural Language Processing for Security Log Analysis

The primary focus of NLP applications in cybersecurity involves processing textual data, including security logs, threat reports, and source code, to detect vulnerabilities. The research by Singh et al. [16] demonstrated 95% accuracy through their NLP and deep learning approach to detect cybersecurity vulnerabilities. When using NLP to analyze Windows Event Logs for cyber intrusion detection, Steverson et al. [17] achieved near-perfect precision and recall. The techniques show exceptional value in processing unstructured data, which traditional rule-based systems cannot handle effectively, to convert large log information into valuable intelligence [18]. Implementing NLP capabilities improves threat indicator understanding through context analysis, leading to better detection accuracy and lower false positive rates [19].

2.1.3 Deep Learning Approaches

Security data with complex, high-dimensional characteristics benefits significantly from deep learning models. According to Liu and Patras, the Bi-ALSTM model achieved a 33% better F1-score than current methods for detecting large-scale network attacks [5]. The research by Kim and Yoon [6] demonstrated an F1-score of 0.998 by implementing a 1D Convolutional Neural Network (CNN) with multi-head attention networks. The ability of deep learning to detect hidden patterns in network traffic and system behavior makes it helpful in identifying sophisticated threats such as Advanced Persistent Threats (APTs), according to Eke and Petrovski [20].

2.2 Evolution from Rule-Based to AI-Driven Security Paradigms

Adopting AI-driven security methods marks a complete transformation of enterprise cybersecurity from traditional rule-based systems. AI-powered solutions analyze behavioral patterns and detect anomalies to identify unknown threats, while traditional rule-based systems depend on predefined signatures and thresholds [21]. Organizations can transition from reactive security postures to proactive threat identification through this evolution, which proves especially beneficial for detecting advanced persistent threats that avoid conventional detection mechanisms [22, 12].

Research shows that AI-based systems achieve better accuracy and operational efficiency than traditional security systems. Implementing AI technologies in industrial cyber-physical systems led to a 40% decrease in false positive rates, a 43.8% decrease in false negative rates, and a 33.3% reduction in response times, according to Ghosh et al. [7]. The enhanced capabilities resolve major weaknesses of traditional security systems because they fail to adapt to the rising complexity of contemporary cyber threats.

3. Real-Time Data Integration and Behavioral Analytics

Identifying sophisticated cyber threats in enterprise environments requires real-time data integration and behavioral analytics capabilities. These technologies enable security systems to process diverse data streams and identify anomalous patterns indicative of malicious activity, particularly Advanced Persistent Threats (APTs) that evade traditional detection mechanisms.

3.1 Data Integration Architectures

Centralized vs. Distributed Approaches

Enterprise threat detection systems clearly prefer centralized architectures because 20 out of 25 studies used centralized models instead of distributed approaches [22, 12]. The centralized architecture provides complete threat visibility through data unifying multiple sources into a single analysis platform. Security Information and Event Management (SIEM) capabilities are standard in these systems, enabling comprehensive enterprise-wide threat assessment [23].

Distributed architectures provide better scalability and resilience even though they appear less frequently. The distributed detection system developed by Dong et al. [24] used 1,130 hosts to combine lightweight client-side detection with global model derivation, producing results equivalent to state-of-the-art centralized techniques while minimizing computational overhead. The distributed detection method delivers exceptional value to organizations that operate extensive networks because it helps overcome bandwidth restrictions and organizational separation during data collection.

Data Sources and Collection Methods

Network traffic is the primary data source in 9 out of 25 studies, followed by audit logs in 6 studies [25,26]. The main data sources offer critical visibility into enterprise environment communications and activities. They consist of Domain Name System (DNS) logs, web proxy logs, Intrusion Detection System (IDS) alerts, and system-level telemetry data that monitors CPU and memory usage and registry and file system activities [27, 28].

The combination of multiple data sources creates enhanced threat detection abilities. Oprea et al. [27] studied DNS and web proxy logs from a network containing more than 100,000 hosts to detect early-stage infections with a 98.33% true detection rate. Kumar and Thing [23]used network traffic data together with audit logs and IDS alerts to achieve precise threat detection with minimal false positives in their Industrial Internet of Things (IIoT) testbed environment.

Processing Frameworks

Real-time data integration depends on graph-based processing methods which provide strong capabilities for relationship analysis and pattern detection [22,29]. The provenance tracking frameworks used in 3 studies establish event causal links to enable attack chain reconstruction and malicious activity attribution [30,31]. Real-time analysis of high-volume data flows becomes possible through stream processing frameworks. The stream-based query system developed by Gao et al. [8] processed event streams in real time to detect threats within a 2-second latency period across 150 hosts. Real-time threat response becomes essential for attack mitigation because it prevents significant damage from occurring.

3.2 Behavioral Analytics Methodologies

Graph-based Analysis

Network theory within graph-based analytics enables the modeling of entity and event relationships to discover hidden attack patterns. The graph-based AI-assisted architecture of Soliman et al. [22] reached 87% balanced accuracy through its ability to correlate alerts and score incidents based on event relationships. The semantic tracking and path analysis method created by Ying et al. [29] demonstrated 25 times better performance in filtering out unnecessary edges than standard methods. The graph-based algorithm with k-nearest neighbors developed by Debatty et al. [32] analyzed HTTP traffic patterns to detect 90% of APTs in their research environment. These methods demonstrate an exceptional ability to detect hidden relationships between unrelated events, which proves essential for identifying coordinated attack campaigns.

Anomaly Detection

Anomaly detection techniques create baseline behavioral profiles to detect potential malicious activity by identifying deviations. The distributed anomaly detection system developed by Dong et al. [24] monitored 1,130 hosts to detect unusual system behavior patterns. The Strange Behavior Inspection Model created by Mohamed and Belaton [28] monitored CPU, RAM, registry, and file system activities, which resulted in a 2.7-minute detection time compared to traditional methods. Anomaly detection success relies heavily on building precise behavioral baselines. The anomaly detection ensemble developed by Ishaya et al. reached 99.95% minimum accuracy by combining static rules with machine learning algorithms, showing that hybrid approaches can effectively merge deterministic and probabilistic methodologies [33].

User and Entity Behavior Analytics (UEBA)

UEBA extends traditional anomaly detection by focusing specifically on the behavior of users and entities within enterprise environments. Marchetti et al. [25] analyzed network traffic across 10,000 hosts using multidimensional feature space analysis, effectively identifying data exfiltration attempts by tracking host movements through feature space. This approach proves particularly valuable for insider threat detection, where malicious activities originate from authorized users or compromised credentials.

3.3 Role in Identifying Advanced Persistent Threats (APTs)

The combination of real-time data integration and behavioral analytics significantly enhances APT detection capabilities. Studies report detection accuracies ranging from 84.8% to 99.95% using these approaches [34, 33]. Particularly notable is the ability to detect threats early before system compromise occurs. Cao [9] reported that their PULSAR system successfully stopped 8 out of 10 replayed attacks before a system integrity violation, demonstrating the preventive potential of advanced analytics.

The visualization capabilities enabled by these technologies also enhance security analysts' ability to understand complex attack patterns. Milajerdi et al. [26] developed HOLMES, a system capable of generating high-level scenario graphs that visualize attack campaigns as they unfold, significantly improving analyst comprehension and response effectiveness. This combination of automated detection with intuitive visualization creates powerful platforms for countering sophisticated threats in enterprise environments.

4. Automation of Threat Detection, Analysis, and Response

Automating cybersecurity processes through AI technologies has revolutionized enterprise threat management, dramatically enhancing detection capabilities while improving operational efficiency through reduced false positives and accelerated response times.

4.1 AI in Detection and Classification of Threats

The detection systems powered by artificial intelligence utilize multiple analytical methods to detect threats with remarkable precision. Multiple studies have shown that Random Forest algorithms and machine learning algorithms provide the best performance results. The research conducted by Imran et al. [2] demonstrated 99% accuracy in detecting advanced persistent threats, and Krishnan et al. [3] reached 99.81% accuracy while maintaining 0.001 false positive rates in cloud infrastructure environments. AI achieves these major performance gains over traditional rule-based systems because it can detect intricate patterns and connections in complex data sets.

AI systems demonstrate advanced classification functionality, which moves past basic threat detection to perform multi-class categorization of attack types. Khan et al. [14] used K-Nearest Neighbors with multiple boosting algorithms to reach 97% accuracy in cyber intrusion classification through their hybrid model. Random Forest and Isolation Forest algorithms used by Dorothy et al. [35] in cloud computing environments achieved 95% accuracy with 93% precision and 96% recall in threat classification. The detailed classification system allows security teams to take more specific response measures, leading to better security outcomes.

Combining natural language processing with these capabilities allows for extracting important data from unstructured information sources. Singh et al.'s [16] research showed 95% accuracy in detecting cybersecurity vulnerabilities by integrating NLP with deep learning methods. Steverson et al. [17] obtained near-perfect precision and recall through their application of NLP to Windows Event Logs for intrusion detection, which surpassed conventional analysis methods.

4.2 Performance Metrics and Effectiveness

4.2.1 Accuracy Rates and False Positive Reduction

AI-powered security solutions demonstrate their effectiveness most clearly through their high accuracy performance and ability to minimize false positives. The accuracy statistics in 16 of 21 studies showed results above 95%, while five achieved accuracy rates exceeding 99% [2-4].

Advanced persistent threat detection systems achieved accuracy levels between 84.8% and 99.95% according to Ghafir et al. (34) and Ishaya et al. [33].

AI-powered systems deliver a vital benefit through false positive reduction, solving a significant issue that traditional security operations face. According to Ghosh et al. [7], implementing AI algorithms in industrial cyber-physical systems resulted in a 40% decrease in false positives and a 43.8% decrease in false negatives. Goswami et al. [36] observed that financial services implementations achieved a 5% reduction in false positive rates. The enhanced detection capabilities decrease security personnel fatigue while maintaining proper threat response to valid security incidents.

4.2.2 Processing Capabilities and Scalability

AI systems show impressive processing abilities, which are vital for detecting threats at an enterprise level. Kim and Yoon [6] built a system that processed 150,000 network threats per minute through preprocessing and classification while demonstrating machine learning scalability benefits. The system performs real-time analysis of large data streams through its processing power, which exceeds the capacity of conventional systems and human analysts. AI-driven threat detection systems have proven their scalability in various organizational environments. The approach developed by Oprea et al. [27] worked on a network containing more than 100,000 hosts while achieving a 98.33% true detection rate. Marchetti et al. [25] deployed multidimensional feature space analysis across 10,000 hosts and successfully detected data exfiltration attempts. The implementations prove that AI-powered solutions operate effectively at an enterprise scale, representing a fundamental necessity for big organizations.

4.2.3 Response Time Improvements

AI technologies speed up threat response operations, which minimizes the time attackers need to execute their plans. The research by Ghosh et al. [7] showed that industrial cyber-physical systems achieved a 33.3% decrease in their response duration. Mohamed and Belaton [28] achieved a 2.7-minute detection time for advanced persistent threats, while Gao et al. [8] used stream-based query processing to detect threats in under 2 seconds. The improved response times show exceptional value for the early identification of threats. The PULSAR system developed by Cao [9] stopped 8 out of 10 replayed attacks from succeeding before system compromise, proving the preventive capabilities of fast detection and response systems.

4.2.4 Security Orchestration and Automated Response

Security orchestration enables AI to perform automated response actions, which extends its impact beyond detection and thus enhances operational efficiency. Kumar and Thing [23] created RAPTOR, which links industrial attack stages to execute precise targeted response actions while maintaining low false positive rates. Lee et al. [37] introduced an AI-SIEM system that provides security analysts with fast cyber threat response capabilities through automated analysis and recommendation workflows. The combination of detection and response functions establishes complete security ecosystems that handle complex threats autonomously. Enterprise environments rely on orchestration to handle excessive threat volume and complexity beyond human capabilities, which enables organizations to sustain effective security postures against expanding threat environments.

5. Challenges and Ethical Considerations

While AI-driven threat intelligence offers significant advantages for enterprise cybersecurity, it also introduces substantial challenges and ethical considerations that organizations must carefully navigate when implementing these technologies.

Privacy and Data Protection

Privacy emerges as a critical concern in AI-driven security implementations [38, 39]. Effective threat detection requires extensive data collection, often including sensitive information requiring protection under various regulatory frameworks. Kakolu et al. [40] recommend data obfuscation, differential privacy, and federated learning to balance security needs with privacy requirements. The global nature of cybersecurity further complicates privacy management as protection requirements vary across jurisdictions. Organizations need comprehensive data governance frameworks addressing these variations. Osazuwa and Musa [41] warn that inadequate privacy measures can undermine system trust and expose organizations to regulatory penalties beyond direct breach impacts.

Transparency and Explainability

The "black box" nature of many AI algorithms—intense learning models—creates significant transparency challenges [42, 43]. This opacity impedes trust in system outputs and complicates incident response when analysts cannot identify the reasoning behind threat classifications. Explainable AI (XAI) approaches offer promising solutions by enabling security personnel to understand detection rationales while maintaining effectiveness. Wang et al. [42] propose integrating explainability mechanisms into security systems, while "Explainable AI in Cybersecurity" [44] highlights XAI's role in enhancing threat intelligence analysis.

Bias and Fairness

AI systems may perpetuate or amplify existing inequities through model prejudices and biased training data [45, 46]. These biases can manifest as demographic disparities in false positive rates or inconsistent protection across different organizational environments. Addressing bias requires diverse training datasets, regular fairness audits, and testing across varied populations and scenarios. Kolade et al. [46] emphasize that bias mitigation must be ongoing rather than a one-time consideration as environments evolve.

Technical Challenges

According to Khosravi and Ladani [47] and Ramuhalli et al. [48], the effectiveness of AI security depends heavily on the quality of available data. The system faces three main problems: excessive data volume, unreliable information, and inconsistent standards. Data poisoning emerges as a critical security risk because Mahlangu et al. [45] call it the "Achilles heel" of cyber threat intelligence systems. According to Simran et al. [11] and Patel et al. [49], integrating AI systems into current security infrastructure faces major integration obstacles. Financial services organizations face significant challenges because their legacy systems do not integrate well [50].

Scalability issues involve three main areas, which include computational resource requirements, data volume handling, and threat adaptation capabilities [21, 51]. The distributed system architecture proposed by Dong et al. [24] enables lightweight detection on client devices through centralized coordination.

6. Case Studies of AI-Driven Threat Intelligence

AI-driven threat intelligence implementations across various industries demonstrate significant security benefits while highlighting implementation considerations. In financial services, Labu and Ahammed [52] documented a Random Forest implementation achieving 83.94% accuracy in threat detection while addressing regulatory compliance requirements. Similarly, Goswami et al. [36] reported accuracy improvements from 68.33% to 85.91% with false positive reduction to 5% through integrated machine learning approaches. These financial implementations benefited particularly from behavioral analytics that established baseline transaction patterns to identify anomalous activities. Industrial control systems showed impressive results, with Ghosh et al. [7] achieving 98.2% accuracy alongside substantial improvements in false positive reduction 40%, false negative reduction (43.8%), and response time (33.3%) using RNNs and K-means clustering. Eke and Petrovski [20] achieved 86.36% detection accuracy through multi-stage network traffic analysis in a laboratory-scale implementation.

Cloud infrastructure security implementations demonstrated exceptional performance, with Krishnan et al. [3] achieving 99.81% accuracy and detection rates with minimal false positives (0.001) in OpenStack environments. Farzaan et al. [53] reported 90% accuracy for network traffic classification and 96% for malware analysis using Random Forest and Isolation Forest algorithms. Large enterprise implementations by Oprea et al. [27] achieved a 98.33% detection rate across 100,000 hosts using belief propagation graph theory, while Marchetti et al. [25] effectively identified data exfiltration across 10,000 hosts through multidimensional feature analysis. Successful implementations consistently incorporate multi-layered detection approaches, human-AI collaboration frameworks, continuous model retraining, graduated alerting mechanisms, and integration with existing security infrastructure. The most effective implementations balance technological capabilities with practical operational considerations to achieve meaningful risk reduction.

7. Future Outlook

The advancement of AI-driven threat intelligence continues rapidly because new emerging technologies will reshape enterprise cybersecurity practices. Large Language Models (LLMs) demonstrate substantial growth through Bokkena [54], showing predictive threat intelligence accuracy reaching 95% levels. Security data processing and actionable recommendations generation remain the strongest aspects of these models when working with unstructured security data. The combination of adaptive generative AI models and Generative Adversarial Networks (GANs) provides enhanced behavioral analysis capabilities, anomaly detection abilities, and synthetic dataset generation for training needs [21].

Organizations need XAI frameworks as essential because they must maintain detection performance and transparency standards. Wang et al. [42] demonstrated why accountable AI-assisted networks matter, and "Explainable AI in Cybersecurity" [44] showed that XAI contributes to threat intelligence analysis. However, these methods serve dual purposes for sustaining stakeholder trust alongside regulatory compliance. A significant change occurs when organizations abandon their traditional reactive security approach and adopt proactive security measures. Modern systems now integrate predictive threat intelligence features that use early warning signs and context-based risk variables to forecast potential attacks [46, 35]. Sindiramutty [55] defines autonomous threat hunting as a future threat intelligence paradigm because it proactively searches for compromise indicators instead of relying on alerts.

Threat actors shift their focus toward attacking AI systems because defensive measures have reached higher effectiveness levels. According to Mahlangu et al. [45], data poisoning is the fundamental weakness in cyber threat intelligence systems. The "Red AI" frameworks developed by Simran et al. [11] demonstrate how AI systems can serve beneficial and harmful purposes, so organizations must persistently improve their defensive measures against AI system attacks from adversaries. AI-driven threat intelligence adoption by organizations demands full ethical frameworks that handle privacy issues alongside bias prevention while requiring strong data governance and deployment of explainable AI systems and human oversight alongside continuous monitoring investments and security team collaboration with data scientists. Successful implementation demands comprehensive approaches covering technological, operational, and ethical domains instead of limited technical deployments.

8. Conclusion

AI-driven threat intelligence has revolutionized enterprise cybersecurity by providing advanced threat detection and response capabilities. Machine learning algorithms achieve detection accuracy rates higher than 95%, and certain implementations demonstrate detection rates exceeding 99% [2-4]. The F1-score performance of deep learning approaches is up to 33% higher than traditional methods [5] while providing operational advantages through threat detection at 150,000 per minute, 33.3% faster response times, and 40% fewer false positives [7, 6].

Behavioral analytics at an advanced level detects ongoing threats by stopping 8 out of 10 potential attacks before they result in compromise [9]. Large-scale deployments benefit from distributed approaches, but centralized architectures remain dominant under specific constraints [24]. Graph-based analysis and provenance tracking demonstrate superior capabilities to detect relationships between unrelated events [22, 26]. The recent technological progress creates major ethical and operational issues that need balanced strategies to handle privacy concerns, transparency needs, and bias prevention. Enterprise cybersecurity will thrive in the future by maintaining a balance between technological advancement and ethical conduct through comprehensive security frameworks that unite innovative solutions with governance mechanisms to combat advanced threats.

References

[1] Sharma SK. AI-enhanced cyber threat detection and response systems. Shodh Sagar J Artif Intell Mach Learn. 2024;1(2):43–8. doi:10.36676/ssjaiml.v1.i2.14.

[2] Imran M, Siddiqui HUR, Raza A, Raza MA, Rustam F, Ashraf I. A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. Comput Secur. 2023;134:103445. doi:10.1016/j.cose.2023.103445.

[3] Krishnan P, Jain K, Aldweesh A, et al. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. J Cloud Comput. 2023;12:26. doi:10.1186/s13677-023-00406-w.

[4] Arora S, Khare P, Gupta S. AI-driven DDoS mitigation at the edge: leveraging machine learning for real-time threat detection and response. In: 2024 International Conference on Data Science and Network Security (ICDSNS); 2024; Tiptur, India. p. 1–7. doi:10.1109/ICDSNS62112.2024.10690930.

[5] Liu H, Patras P. NetSentry: a deep learning approach to detecting incipient large-scale network attacks. Comput Commun. 2022;191:119–32. doi:10.1016/j.comcom.2022.04.020.

[6] Kim H, Yoon Y. An ensemble of text convolutional neural networks and multi-head attention layers for classifying threats in network packets. Electronics. 2023;12(20):4253. doi:10.3390/electronics12204253.

[7] Ghosh AK, Bhupathi HP, Bhagyalakshmi L, Poddar H, Gandhi T, Jain J. Enhancing the security of industrial cyber-physical systems using AI algorithms. In: Proceedings of the International Conference on Intelligent Systems and Advanced Applications. 2024. p. 1–6. doi:10.1007/s42979-024-03540-7.

[8] Gao P, Xiao X, Li D, Li Z, Jee K, Wu Z, et al. SAQL: a stream-based query system for real-time abnormal system behavior detection. In: Proceedings of the 27th USENIX Security Symposium. 2018. p. 639–56.
[9] Cao PM. On preempting advanced persistent threats using probabilistic graphical models. arXiv Prepr. 2019. doi:10.48550/arXiv.1908.01509.
[10] Uzoka A, Cadet E, Ojukwu PU. Applying artificial intelligence in cybersecurity to enhance threat detection, response, and risk management. Comput Sci IT Res J. 2024;5(10):2511–38. doi:10.51594/csitrj.v5i10.1677.
[11] Simran, Kumar S, Hans A. The AI Shield and Red AI Framework: machine learning solutions for cyber threat intelligence (CTI). In: 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS); 2024; Gurugram, India. p. 1–6. doi:10.1109/ISCS61804.2024.10581195.
[12] Zimba A, Chen H, Wang Z, Chishimba M. Modeling and detection of the multi-stages of advanced persistent threats attacks based on semi-supervised learning and complex networks characteristics. Future Gener Comput Syst. 2020;106:501–17. doi:10.1016/j.future.2020.01.032.
[13] Maasaoui Z, Bekri A, Merzouki M, Battou A, Abane A, Lbath A. Design and implementation of an automated network traffic analysis system using Elastic Stack. In: 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA); 2024; Giza, Egypt. Available from: https://doi.org/10.1109/AICCSA59173.2023.10479347. Accessed 2025 May 5.
[14] Khan TA, Abbas S, Senapati B, Anand MR, Ghafoor MI, Pradhan S, et al. Multi-source cyber intrusion detection using ensemble machine learning. J Comput Sci. 2025;15(1):1–10
[15] Shan A, Myeong S. Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. Sensors. 2024;24(15):4888. doi:10.3390/s24154888.
[16] Singh K, Grover SS, Kumar RK. Cyber security vulnerability detection using natural language processing. In: 2022 IEEE World AI IoT Congress (AIIoT); 2022; Seattle, WA, USA. p. 174–8. doi:10.1109/AIIoT54504.2022.9817336.
[17] Steverson K, Carlin C, Mullin J, Ahiskali M. Cyber intrusion detection using natural language processing on Windows event logs. In: 2021 International Conference on Military Communication and Information Systems (ICMCIS); 2021; The Hague, Netherlands. p. 1–7. doi:10.1109/ICMCIS52405.2021.9486307.
[18] Komaragiri V, Edward A. AI-driven vulnerability management and automated threat mitigation. Int J Sci Res Manag. 2022;10:980–98. doi:10.18535/ijsrm/v10i10.ec05.
[19] Viradia V, Muthukrishnan H, Yadav D. Insider threats in healthcare application: harnessing AI to mitigate the risks. Int J Glob Innov Solutions. 2024. Available from: https://api.semanticscholar.org/CorpusID:275129379.
[20] Eke H, Petrovski AV. Advanced persistent threats detection based on deep learning approach. Ind Cyber-Phys Syst. 2023;5(2):112–27.

[21] Vemuri N, Thaneeru N, Tatikonda VM. Adaptive generative AI for dynamic cybersecurity threat detection in enterprises. Int J Sci Res Arch. 2024;11(1):2259–65. doi:10.30574/ijsra.2024.11.1.0313.

[22] Soliman HM, Sovilj D, Salmon G, Rao M, Mayya N. RANK: AI-assisted end-to-end architecture for detecting persistent attacks in enterprise networks. IEEE Trans Depend Secure Comput. 2023;20(5):3581–94. doi:10.48550/arXiv.2101.02573.

[23] Kumar A, Thing V. RAPTOR: advanced persistent threat detection in industrial IoT via attack stage correlation. In: Proceedings of the Conference on Privacy, Security and Trust. 2023. p. 1–6. doi:10.48550/arXiv.2301.11524.

[24] Dong F, Wang L, Nie X, Shao F, Wang H, Li D, et al. DISTDET: a cost-effective distributed cyber threat detection system. In: Proceedings of the 32nd USENIX Security Symposium. 2023. p. 4521–38.

[25] Marchetti M, Pierazzi F, Colajanni M, Guido A. Analysis of high volumes of network traffic for advanced persistent threat detection. Comput Netw. 2016;109(Pt 2):127–41. doi:10.1016/j.comnet.2016.05.018.

[26] Milajerdi SM, Gjomemo R, Eshete B, Sekar R, Venkatakrishnan V. HOLMES: real-time APT detection through correlation of suspicious information flows. In: Proceedings of the IEEE Symposium on Security and Privacy. 2018. p. 1–18. doi:10.48550/arXiv.1810.01594.

[27] Oprea A, Li Z, Yen T, Chin S, Alrwais SA. Detection of early-stage enterprise infection by mining large-scale log data. In: Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. 2014. p. 1–10. doi:10.48550/arXiv.1411.5005.

[28] Mohamed N, Belaton B. SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. IEEE Access. 2021;9:42919–32. doi:10.1109/ACCESS.2021.3066289.

[29] Ying J, Zhu T, Cheng W, Yuan Q, Ma M, Xiong C-L, et al. SPARSE: semantic tracking and path analysis for attack investigation in real-time. arXiv Prepr. 2024. doi:10.48550/arXiv.2405.02629.

[30] Irshad H, Ciocarlie G, Gehani A, Yegneswaran V, Lee KH, Patel JM, et al. TRACE: enterprise-wide provenance tracking for real-time APT detection. IEEE Trans Inf Forensics Secur. 2021;16:4363–76. doi:10.1109/TIFS.2021.3098977.

[31]Milajerdi SM. Threat detection using information flow analysis on kernel audit logs. In: Proceedings of the International Conference on Cyber Security and Protection of Digital Services. 2020. p. 1–8.

[32] Debatty T, Mees W, Gilon T. Graph-based APT detection. In: Proceedings of the International Conference on Military Communications and Information Systems. 2018. p. 1–8.

[33] Ishaya AO, Aminat A, Hashim B, Adekunle AA. Improved detection of advanced persistent threats using an anomaly detection ensemble approach. Int J Comput Sci Inf Secur. 2021;19(6):1–7.

[34] Ghafir I, Hammoudeh M, Přenosil V, Han L, Hegarty R, Rabie KM, et al. Detection of advanced persistent threat using machine-learning correlation analysis. Future Gener Comput Syst. 2018;79:1–10.

[35] Dorothy AB, Madhavidevi B, Nachiappan B, Manikandan G, Patjoshi PK, Sindhuja M. AI-driven threat intelligence in cloud computing: detecting and responding to cyber attacks. In: 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS). 2024. p. 1–6. Available from: https://api.semanticscholar.org/CorpusID:273590592.

[36] Goswami S, Mondal S, Halder R, Nayak J, Sil A. Exploring the impact of artificial intelligence integration on cybersecurity. J Ind Intell. 2024;6(2):45–58.

[37] Lee J, Kim J, Kim I, Han K. Cyber threat detection based on artificial neural networks using event profiles. IEEE Access. 2019;7:165607–26. doi:10.1109/ACCESS.2019.2953095.

[38] Mbah G, Achudume N. AI-powered cybersecurity: strategic approaches to mitigate risk and safeguard data privacy. World J Adv Res Rev. 2024;24(3):310–27. doi:10.30574/wjarr.2024.24.3.3695.

[39] Alevizos L, Dekker M. Towards an AI-enhanced cyber threat intelligence processing pipeline. Electronics. 2024;13(11):2021. doi:10.3390/electronics13112021.

[40] Kakolu S, Faheem MA, Aslam M. Privacy-preserving AI for cybersecurity: balancing threat intelligence collection with user data protection. Int J Sci Res Arch. 2021;9(3):1–6.

[41] Osazuwa M, Musa M. The expanding attack surface: securing AI and machine learning systems in security operations. Int J Innov Sci Res Technol. 2024;9:8. doi:10.38124/ijisrt/IJISRT24MAY1613.

[42] Wang S, Sandeepa C, Senevirathna T, Siniarski B, Nguyen M-D, Marchal S, et al. Towards accountable and resilient AI-assisted networks: case studies and future challenges. In: Proceedings of the 2024 Joint European Conference on Networks and Communications & 6G Summit. 2024. p. 818–23.

[43] Baroni P, Cerutti F, Fogli D, Giacomin M, Gringoli F, Guida G, et al. Self-aware effective identification and response to viral cyber threats. In: Proceedings of the 13th International Conference on Cyber Conflict. 2021. p. 353–70.

[44] Singh K, Kumar M. Explainable AI in cybersecurity. Int Res J Mod Eng Technol Sci. 2024;6(5):1102–10.

[45] Mahlangu T, January S, Mashiane CT, Dlamini TM, Ngobeni SJ, Ruxwana LN. ‘Data poisoning’ – Achilles heel of cyber threat intelligence systems. In: Proceedings of the 12th International Conference on Cyber Conflict; 2019. p. 1–8.

[46] Kolade TM, Obioha-Val OA, Balogun AY, Gbadebo MO, Olaniyi OO. AI-driven open source intelligence in cyber defense: a double-edged sword for national security. Asian J Res Comput Sci. 2025;18(1):133–53. doi:10.9734/ajrcos/2025/v18i11554.
[47] Khosravi M, Ladani BT. Alerts correlation and causal analysis for APT based cyber attack detection. IEEE Access. 2020;8:162642–56. doi:10.1109/ACCESS.2020.3021499.
[48] Muhlheim MD, Ramuhalli P, Huning A, Yigitoglu AG, Saxena A. Status report on regulatory criteria applicable to the use of artificial intelligence (AI) and machine learning (ML). Oak Ridge National Laboratory; 2023 Sep. Report No.: ORNL/SPR-2023/3072. doi:10.2172/2007715.
[49] Patel B, Patel KB, Dhameliya N. Revolutionizing cybersecurity with AI: predictive threat intelligence and automated response systems. Darpan Int Res Anal. 2024;12(4):1–6. doi:10.36676/dira.v12.i4.126.
[50] Haass JC. Cyber threat intelligence and machine learning. In: Proceedings of the 2022 4th International Conference on Transdisciplinary AI (TransAI). 2022. p. 156–159. doi:10.1109/TransAI54797.2022.00033.
[51] Stency VS. Redefining cyber defense: the evolution of threat detection with artificial intelligence. Recent Trends Manag Commer. 2024;5(2):35–41. doi:10.46632/rmc/5/2/7.
[52] Labu MR, Ahammed MF. Next-generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. J Comput Sci Technol Stud. 2024;6(1):179–88. doi:10.32996/jcsts.2024.6.1.19.
[53] Farzaan MAM, Ghanem MC, El-Hajjar A, Ratnayake DN. AI-enabled system for efficient and effective cyber incident detection and response in cloud environments. arXiv [Preprint]. 2024 Apr 8. Available from: https://doi.org/10.48550/arXiv.2404.05602.
|54] Bokkena B. Enhancing IT security with LLM-powered predictive threat intelligence. In: Proceedings of the 5th International Conference on Smart Electronics and Communication (ICOSEC); 2024 Sep 21–23; Trichy, India. IEEE; 2024. p. 751–6. doi:10.1109/ICOSEC57956.2024.10345678.
[55] Sindiramutty SR. Autonomous threat hunting: a future paradigm for AI-driven threat intelligence. arXiv [Preprint]. 2023 Dec 30. Available from: https://doi.org/10.48550/arXiv.2401.00286.