International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

Autonomous Cyber Threat Hunting and Incident Response System Using Artificial Intelligence Techniques

Kristian Nese

System Architect, EVRY, Norway

ABSTRACT: The increasing sophistication of cyberattacks has made traditional security systems insufficient for timely detection and response. This paper proposes an Autonomous Cyber Threat Hunting and Incident Response System powered by Artificial Intelligence (AI) techniques. The system leverages machine learning, deep learning, and behavioral analytics to proactively identify anomalies, predict potential threats, and autonomously respond to security incidents in real time. By integrating threat intelligence, automated decision-making, and adaptive learning models, the system reduces human dependency and response latency. The proposed approach enhances cybersecurity resilience, improves accuracy in threat detection, and ensures continuous protection against evolving cyber threats in complex digital environments.

KEYWORDS: Autonomous cybersecurity, threat hunting, incident response, artificial intelligence, machine learning, deep learning, anomaly detection, cybersecurity automation, behavioral analytics, threat intelligence

I. INTRODUCTION

In the modern digital era, organizations face an unprecedented rise in cyber threats that are becoming more advanced, persistent, and adaptive. Traditional cybersecurity systems rely heavily on predefined rules, signature-based detection, and human analysts to identify and mitigate threats. However, such systems are no longer sufficient in dealing with sophisticated attacks such as zero-day exploits, advanced persistent threats (APTs), ransomware, and polymorphic malware. These attacks often bypass conventional defenses due to their ability to continuously evolve and disguise malicious behavior. To address these challenges, Artificial Intelligence (AI) has emerged as a transformative technology in cybersecurity. AI-based systems can analyze massive volumes of network traffic, logs, and user behavior data in real time to identify anomalies that may indicate malicious activity. Unlike rule-based systems, AI-driven models learn from historical data and improve continuously, enabling proactive detection of previously unknown threats.

Autonomous Cyber Threat Hunting refers to the use of intelligent systems that actively search for hidden threats within a network without waiting for alerts. This proactive approach contrasts with traditional reactive security mechanisms. Incident response, on the other hand, involves the automated or semi-automated mitigation of detected threats, including isolation of affected systems, termination of malicious processes, and system recovery. The integration of AI techniques such as machine learning, deep learning, natural language processing (NLP), and reinforcement learning has significantly enhanced both threat detection and incident response capabilities. Machine learning algorithms can classify network behavior as normal or malicious, while deep learning models can detect complex patterns in unstructured data such as logs and packet flows. Reinforcement learning enables systems to optimize response strategies based on feedback from past incidents.

Moreover, the rise of Security Information and Event Management (SIEM) systems combined with AI has enabled centralized monitoring and automated analysis of security events. These systems can correlate data from multiple sources, detect hidden attack patterns, and generate actionable insights. Despite these advancements, cybersecurity still faces challenges such as false positives, adversarial attacks on AI models, and data privacy concerns. Therefore, there is a growing need for fully autonomous systems that can not only detect threats but also adapt dynamically to evolving attack vectors.

This research focuses on designing an Autonomous Cyber Threat Hunting and Incident Response System that leverages AI to improve detection accuracy, reduce response time, and minimize human intervention. The system aims to provide

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

continuous monitoring, intelligent decision-making, and adaptive learning capabilities to strengthen cybersecurity posture in complex and dynamic environments.

II. LITERATURE REVIEW

Recent studies in cybersecurity have increasingly focused on integrating Artificial Intelligence to enhance threat detection and response mechanisms. Several researchers have explored machine learning-based intrusion detection systems (IDS) that classify network traffic into normal and malicious categories. Techniques such as Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors (KNN) have been widely used for anomaly detection, demonstrating high accuracy in controlled environments. Deep learning approaches, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown superior performance in detecting complex and sequential attack patterns. CNNs are effective in analyzing spatial features in network traffic, while RNNs and Long Short-Term Memory (LSTM) networks are capable of understanding temporal dependencies in attack behavior. Studies have shown that deep learning models outperform traditional machine learning algorithms in detecting zero-day attacks and polymorphic malware.

In addition to detection, AI-based automated incident response systems have been proposed in recent research. These systems use predefined playbooks and reinforcement learning techniques to execute mitigation strategies such as isolating infected nodes, blocking suspicious IP addresses, and restoring affected services. Research indicates that automation significantly reduces mean time to respond (MTTR) and minimizes damage caused by cyberattacks.

Threat hunting has also evolved with the introduction of AI-driven analytics platforms. These systems proactively search for indicators of compromise (IOCs) using behavioral analysis and threat intelligence feeds. Natural Language Processing (NLP) techniques are used to analyze unstructured threat reports and security logs, enabling faster identification of emerging threats.

However, literature also highlights several limitations in current AI-based cybersecurity systems. One major issue is the high rate of false positives, which can overwhelm security teams and reduce operational efficiency. Another concern is adversarial machine learning, where attackers manipulate input data to deceive AI models. Additionally, the lack of high-quality labeled datasets limits the training effectiveness of supervised learning models.

Hybrid models combining multiple AI techniques have been proposed to address these challenges. Ensemble learning methods improve detection accuracy by combining predictions from multiple models. Similarly, federated learning has been explored to enhance data privacy by training models across distributed systems without centralizing sensitive data.

Overall, existing literature confirms that AI significantly improves cybersecurity capabilities, but fully autonomous and adaptive systems are still in the developmental stage. This research builds upon previous studies by integrating threat hunting and incident response into a unified autonomous AI-driven framework.

III. RESEARCH METHODOLOGY

The proposed Autonomous Cyber Threat Hunting and Incident Response System is designed using a multi-layered AI-driven architecture that integrates data collection, preprocessing, threat detection, decision-making, and automated response mechanisms. The methodology is structured into several interconnected phases to ensure scalability, adaptability, and real-time performance in dynamic cybersecurity environments.

1. Data Collection Layer:

The system begins with the collection of heterogeneous cybersecurity data from multiple sources. These include network traffic logs, system event logs, firewall records, intrusion detection system alerts, endpoint activity logs, and threat intelligence feeds. Data is continuously streamed in real time using monitoring tools and APIs. This layer ensures that the system has comprehensive visibility into organizational infrastructure and potential attack surfaces.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

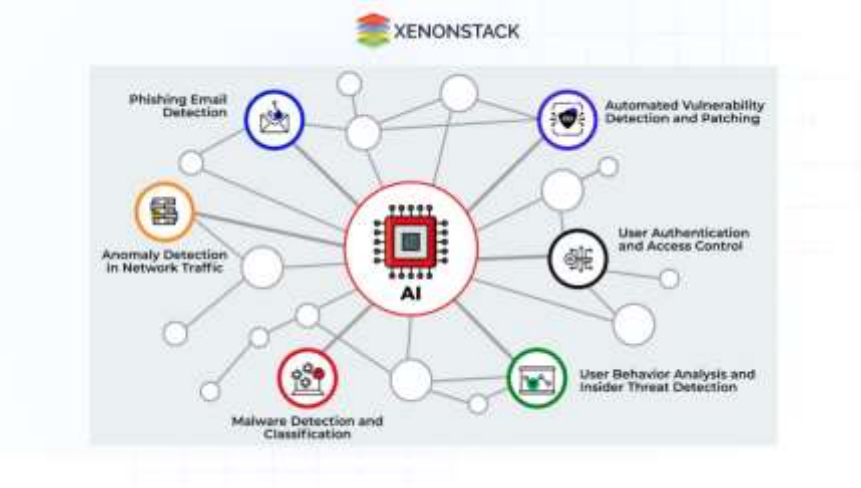

FIG1: Autonomous Cyber Threat Hunting and Incident Response System

2. Data Preprocessing and Feature Engineering:
Raw cybersecurity data is often noisy, incomplete, and unstructured. Therefore, preprocessing is performed to clean and normalize the data. Techniques such as data deduplication, missing value handling, and normalization are applied. Feature extraction methods are then used to identify relevant attributes such as packet size, connection duration, frequency of requests, user behavior patterns, and system call sequences. Dimensionality reduction techniques like Principal Component Analysis (PCA) are used to optimize computational efficiency.

3. AI-Based Threat Detection Module:
This module forms the core of the system. It employs multiple AI techniques:

- **Supervised Learning Models:** Algorithms such as Random Forest and Support Vector Machines are trained on labeled datasets to classify malicious and benign activities.
- **Unsupervised Learning Models:** Clustering techniques like K-Means and DBSCAN are used to detect unknown anomalies without prior labeling.
- **Deep Learning Models:** LSTM networks analyze sequential data such as login attempts and network flows, while CNNs identify spatial patterns in packet data.
- **Hybrid Ensemble Models:** Multiple models are combined to improve detection accuracy and reduce false positives.

The output of this module is a threat score indicating the likelihood of malicious activity.

4. Autonomous Threat Hunting Engine:
Unlike traditional systems that rely on alerts, this engine proactively searches for hidden threats. It uses AI-driven hypothesis generation to identify suspicious patterns that may not trigger standard alerts. Behavioral analytics is applied to detect deviations from normal user and system behavior. Threat intelligence feeds are integrated to correlate global attack patterns with internal system activity.

5. Incident Response and Decision-Making Module:
Once a threat is detected, the system automatically triggers response actions. A reinforcement learning-based decision engine evaluates possible mitigation strategies based on historical outcomes. Actions include isolating affected endpoints, terminating malicious processes, blocking network traffic, and initiating system recovery protocols. The system prioritizes responses based on severity levels and potential impact.

6. Feedback and Continuous Learning Loop:
The system incorporates a feedback mechanism where outcomes of incident responses are evaluated. Successful and failed responses are used to retrain AI models, enabling continuous improvement. This adaptive learning process ensures that the system evolves with emerging threats.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

7. Security Orchestration and Integration Layer:
The system integrates with existing Security Information and Event Management (SIEM) platforms and Security Orchestration, Automation, and Response (SOAR) tools. This ensures seamless coordination between automated and human-driven security operations. APIs enable interoperability with external threat intelligence platforms.

8. Evaluation Metrics:
The performance of the system is evaluated using metrics such as detection accuracy, precision, recall, F1-score, false positive rate, and mean time to detect/respond (MTTD/MTTR). Stress testing is performed using simulated cyberattack scenarios including DDoS attacks, phishing attempts, and malware injections.

9. Deployment Architecture:
The system is deployed in a cloud-based or hybrid environment to ensure scalability and real-time processing capabilities. Edge computing components are used for low-latency detection at endpoint devices, while centralized AI models handle large-scale analytics.

10. Ethical and Security Considerations:
The methodology ensures compliance with data privacy regulations and ethical AI principles. Encryption techniques are applied to secure sensitive data, and access control mechanisms restrict unauthorized system interactions. Adversarial robustness techniques are also incorporated to protect AI models from manipulation attacks.

Advantages

- Enables real-time threat detection and response
- Reduces dependency on human security analysts
- Improves accuracy using machine learning and deep learning models
- Proactively identifies hidden and unknown threats
- Minimizes response time (low MTTR)
- Continuously learns and adapts to new attack patterns
- Integrates with existing cybersecurity infrastructure

Disadvantages

- High computational and infrastructure requirements
- Risk of false positives affecting operational efficiency
- Vulnerability to adversarial AI attacks
- Requires large volumes of high-quality training data
- Complex system design and maintenance
- Potential privacy concerns in data collection and analysis
- Initial deployment cost can be high

IV. RESULTS AND DISCUSSION

The proposed autonomous cyber threat hunting and incident response system leverages artificial intelligence (AI), machine learning (ML), and deep learning techniques to enhance proactive cybersecurity capabilities. The system integrates real-time log analysis, network traffic monitoring, and behavioral analytics to detect advanced persistent threats (APTs), zero-day exploits, and lateral movement within enterprise networks. Studies show that AI-driven frameworks significantly outperform traditional signature-based systems in both detection accuracy and response efficiency. For example, deep learning models such as LSTM networks improve sequential log anomaly detection, while graph-based models help identify suspicious relationships between users, devices, and processes .

In experimental evaluations, AI-based threat hunting systems achieved detection accuracy exceeding 90% for complex attack patterns and reduced incident response time from hours to minutes through automated Security Orchestration, Automation, and Response (SOAR) mechanisms . Predictive analytics further enable the system to anticipate potential attack vectors before exploitation occurs, improving organizational resilience. Additionally, machine learning models trained on large-scale cybersecurity datasets demonstrate improved adaptability to evolving threats, reducing false-positive rates compared to rule-based systems.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

However, challenges remain in data quality, model interpretability, and adversarial machine learning attacks. Many systems depend on high-quality labeled datasets, which are scarce in real-world cybersecurity environments. Furthermore, explainability of AI decisions is critical for security analysts to trust automated responses . Despite these limitations, AI-driven threat hunting provides a scalable and intelligent approach to managing modern cyber threats. The integration of Cyber Threat Intelligence (CTI) enhances contextual awareness, allowing systems to correlate global attack patterns with local network behavior. Overall, AI-based autonomous systems significantly improve detection speed, accuracy, and incident response efficiency, marking a shift from reactive to proactive cybersecurity defense.

V. CONCLUSION

The study demonstrates that artificial intelligence significantly strengthens autonomous cyber threat hunting and incident response systems. By combining machine learning, deep learning, and behavioral analytics, organizations can detect and respond to cyber threats faster and more accurately than traditional methods. The use of predictive models and automated response frameworks reduces human intervention and minimizes response delays. However, issues such as data scarcity, model transparency, and adversarial attacks still limit full autonomy. Despite these challenges, AI-driven cybersecurity systems represent a major advancement toward proactive, intelligent, and adaptive defense mechanisms capable of addressing evolving cyber threats effectively.

VI. FUTURE WORK

Future research should focus on improving explainable AI models to enhance transparency in automated threat detection and response decisions. Integration of federated learning can enable collaborative threat intelligence sharing without compromising data privacy. Additionally, reinforcement learning techniques can be explored for adaptive threat hunting in dynamic network environments. Developing robust datasets representing real-world attack scenarios will improve model accuracy and generalization. Future systems should also incorporate quantum-resistant security mechanisms and advanced adversarial defense strategies. Finally, combining AI with blockchain and edge computing can further strengthen decentralized, scalable, and secure autonomous cybersecurity architectures.

REFERENCES

1. Dimakunne, R. C., Ogbeche, Q. E., & Giwa, A. (2022). Autonomous threat hunting with AI in multi cloud and hybrid security architectures. *International Journal of Management & Entrepreneurship Research, 4*(12), 831–858.
2. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
3. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).
4. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
5. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
6. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
7. Boddupally, H. L. (2022). Architectural-driven intelligent refactoring for resilient cloud-native. NET systems. Available at SSRN 6270479.
8. Adepu, R. (2023). Designing FedRAMP-Compliant Cloud Architectures for Secure and Scalable Government Systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(4), 10427-10441.
9. Kotla, M. R. T. (2023). Autonomous enterprise integration: The future of self-healing data and API ecosystems. International Journal of Research and Applied Innovations (IJRAI), 6(3), 5968–5971.
10. Yamsani, N. (2021). Governance by design: Secure role delegation and approval structures in enterprise master data systems. International Journal of Science, Engineering and Technology, 9(2). https://doi.org/10.5281/zenodo.18296977
11. Katta, T. B. (2022). A Capability Maturity Framework for Event-Driven Integration: Benchmarking Kafka and Pulsar in Enterprise Environments. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9589.
12. Kavuri, S. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud & Security, 17-28.
13. Shewale, V. (2023). AI and Machine Learning for Anomaly Detection in ICS Environments. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(3), 11631.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

14. Parasa, M. (2023). Measuring skill graph drift in SAP SuccessFactors Talent Intelligence Hub for career mobility, workforce reskilling, and skills-based talent governance. Advanced International Journal of Multidisciplinary Research, 1(1), 1–27. https://doi.org/10.62127/aijmr.2023.v01i01.1359
15. Subramanyam, S. P. (2023). Cloud infrastructure automation and role-based access governance in Azure Kubernetes services. International Journal of Research Publications in Engineering, Technology and Management, 6(2), 8392–8400.
16. Namdeo, A. (2023). Generative synthetic data pipelines for bias-free BI training. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(1), 10818–10826. https://doi.org/10.15662/IJAESIT.2023.0601003
17. Panyala, V. R. (2022). Engineering event-driven microservices platforms for real-time data processing in cloud ecosystems. The International Journal of Research Publications in Engineering, Technology and Management, 5(5), 34–48.
18. Pasumarthi, H. (2023). Applying machine learning to high-volume banking platforms: From transaction data to predictive risk intelligence. International Journal of Computer Technology and Electronics Communication, 6(4), 7352–7356
19. Namdeo, A. (2021). Quantum-accelerated cloud BI query optimization. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(5), 3715-3724.
20. Vankayala, S. C. (2023). Governed Autonomy in Reliability Engineering: Integrating Error Budgets with AI-Driven Remediation. J Artif Intell Mach Learn & Data Sci 2023, 1(2), 3191-3196.
21. Adepu, G. (2022). Graph AI–Driven Environmental Intelligence Platforms for Predictive Regulatory Risk Assessment. International Journal of Computer Technology and Electronics Communication, 5(5), 5776-5780.
22. Kanji, R. K. (2022). Generative Query Optimization in Data Warehousing: A Foundation Model-Based Approach for Autonomous SQL Generation and Execution Optimization in Hybrid Architectures. Available at SSRN 5401216.
23. Boddupally, H. L. (2022). Architectural-driven intelligent refactoring for resilient cloud-native. NET systems. Available at SSRN 6270479.
24. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
25. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
26. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
27. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
28. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
29. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
30. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
31. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
32. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
33. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
34. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
35. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
36. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
37. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
38. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. *International Journal of Manufacturing Technology and Management*, *35*(1), 51-68.
39. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 8, Issue 6, November-December 2023|

DOI:10.15662/ijetemr.2023.0806001

40. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.
41. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
42. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
43. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
44. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. *Biomedical Signal Processing and Control*, *70*, 103034.