Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI-Driven Incident Response in Enterprise Networks: Enhancing Security and Resilience

Sunil Jorepalli[1], Vivek Bairy[2], Venkatesh Kodela[3]
[1]*Independent Researcher, San Francisco, USA*
Sunilreddyj1988@gmail.com
ORCID: 0009-0006-1911-7323
[2]*Independent Researcher, San Francisco, USA*
vbairy21@gmail.com
ORCID: 0009-0007-8787-0357
[3]*IT Lead Security Analyst, Zimmer Biomet, Warsaw, Indiana, USA*
Venkatesh.kodela@gmail.com
ORCID: 0009-0000-2194-5431

ARTICLE INFO

Received: 24 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

This study explores the role of AI-driven incident response mechanisms in enhancing the security and resilience of enterprise networks. By employing a quantitative and descriptive research design, the study analyzes the frequency and effectiveness of AI responses across various types of security incidents. Data was collected through a simulated enterprise network environment, where a total of 150 security incidents and corresponding AI response actions were recorded. The results indicate that AI significantly accelerates threat detection and mitigation, with automated threat containment and malware detection being the most common AI actions. The findings suggest that AI systems contribute to faster, more accurate incident responses, enabling organizations to effectively address security threats in real time. This research underscores the value of AI in reinforcing enterprise network defenses and reducing reliance on manual interventions.

Keywords: AI-driven incident response, enterprise networks, cybersecurity, automated threat containment, malware detection, AI security, incident response time, enterprise resilience.

1. INTRODUCTION

In the modern digital era, businesses are confronted with a growing number of cybersecurity threats that present serious risks to their networks, information, and overall operational integrity. From ransomware attacks and malware infections to phishing attacks and insider threats, organizations have to deal with a relentless stream of emerging threats that need to be detected and responded to in real-time. As the amount and sophistication of cyberattacks expand, conventional security systems, that depend heavily on human action and reactionary measures, have become steadily less effective. Such approaches often fall behind in trying to stay current with the continually evolving danger, leading to slower response times, increased vulnerability, and more potential for expensive data breaches and system downtime.

To respond to these challenges, companies are now looking increasingly towards Artificial Intelligence (AI) to bolster their incident response functions. AI technologies, especially machine learning and deep learning, are being used to automate detecting, analyzing, and responding to security incidents in real time. AI solutions are able to filter through vast amounts of network data to recognize anomalies, trends, and possible threats that might not be noticed otherwise by standard security solutions. As opposed to manual methods, AI can respond rapidly, sometimes within milliseconds, to deal with threats as they appear.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

One of the major strengths of AI-powered incident response is the potential to automate repetitive tasks that were formerly performed by human security personnel. For example, AI can identify compromised devices or malicious network traffic automatically without intervention. Automated containment of threats cuts down the response time significantly from detection to remediation, limiting the possible harm. Further, AI algorithms have the ability to learn and update continuously based on new information and adjust to the evolving patterns of attacks, such that the system continues to be effective as and when cyber threats change.

In addition, AI systems have the ability to generate real-time alerts and notifications. Upon the identification of a threat, AI is able to immediately notify security teams with the kind of rich insights and context regarding the attack nature, targeted systems, and suggested actions. Through this timely response, security personnel can leave the initial containment and mitigation activities to the AI system and dedicate their time to more strategic-level decision-making and investigation.

Another important advantage of AI-powered incident response is that it can facilitate predictive security. Through the study of past data, behavior, and network traffic, AI can predict probable vulnerabilities and risks before they occur. This predictive analysis enables organizations to be forward-looking and not just reactive, closing security loopholes before cybercriminals are able to exploit them.

AI also significantly contributes to network resilience—the capacity of a network to resist and bounce back from cyberattacks without suffering extended interruptions. By having AI systems integrated, organizations can more effectively resist attacks, for example, Distributed Denial of Service (DDoS) or data exfiltration attempts, by identifying and stopping them in real time. In addition, AI can assist in forensic examination of security breaches, gathering information to inform security teams about the extent and source of an attack. This feature is especially useful in post-incident examination since it offers detailed logs and information that can be applied to improve defenses and optimize future reactions.

Beyond improving response speed, AI also helps in scaling security efforts. Traditional manual incident response requires significant human resources, and its effectiveness can be limited by the size and complexity of the network. With AI, enterprises can scale their security operations without requiring a proportional increase in personnel. AI systems can monitor and respond to threats across large and diverse network environments, providing consistent and reliable protection around the clock.

But integration of AI in incident response is not without challenges. One of the most important concerns is the availability of quality data used to train AI algorithms. In the absence of adequate and varied data, AI systems can fail to identify threats or may generate false positives that will need to be manually verified. Additionally, although AI systems can automate much of incident response, human intervention is essential. Security analysts still need to analyze complicated incidents and offer higher-level decision-making that AI systems cannot yet match.

Additionally, there are privacy and ethics issues related to the application of AI in security. AI applications that constantly watch network traffic and user activity might pose questions of data privacy, surveillance, and bias. There is a need for organizations to have well-defined policies and security measures in place to ensure AI is applied in an ethical manner and does not violate individuals' rights or compromise the security of the larger environment.

In spite of these issues, AI-based incident response systems have immense potential to facilitate enterprise security and resilience. The capacity to automate threat detection, enhance response times, anticipate vulnerabilities, and enhance security efforts on a large scale gives businesses a robust weapon to counter ever-more sophisticated cyber threats. As AI technologies advance, their presence in the field of cybersecurity will expand further, resulting in more intelligent, efficient, and resilient defense systems.

This study seeks to investigate the different ways in which AI can improve incident response within enterprise networks, with a focus on how AI systems enhance security, efficiency, and resilience. Through an analysis of the effectiveness of these AI tools in practical environments, this research hopes to identify their potential to revolutionize the cybersecurity scene and reduce the threats posed by emerging threats. Finally, it highlights how AI can be a game-changer for organizations looking to protect their digital assets and ensure operational continuity in the event of constantly changing cyber threats.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. LITERATURE REVIEW

Sundaramurthy et al. (2022) debated the significance of operation resilience driven by AI in today's businesses and highlighted the imperative for intelligent, scalable, and secure frameworks capable of handling mounting cybersecurity threats. Their research put into perspective the ability of AI systems to introduce adaptive and real-time threat mitigations to uncertainties in security as presented by complexities in network configurations. Organizations will be able to attain increased resilience through faster response to cyber breaches and lower downtimes if they implement AI-enabled incident response systems.

Chinta et al. (2024) examined how AI-driven Enterprise Resource Planning (ERP) systems and big data might be leveraged to enhance cybersecurity resilience. They were concerned with how AI, combined with big data analytics, facilitates real-time monitoring and automated response to threats, dramatically improving incident management and security decision-making. Their studies indicated that AI-based methods not only enhance detection but also optimize the robustness of ERP systems in actual threat situations by foretelling future threats before they turn into greater breaches.

Akinade et al. (2021) presented a conceptual framework for automating network security, suggesting a framework that incorporates AI-based technologies with multi-vendor infrastructures to enhance overall cyber resilience. Their framework underscored the manner in which AI would be able to automatically detect and react to network security threats, enabling faster containment and recovery. This was also done in a way that reduced human intervention, resulting in enhanced operational efficiency in managing cyber threats, especially in heterogeneous network system environments.

Mori (2023) highlighted the critical role of AI in enhancing threat prediction, detection, and recovery. He focused on the application of AI-powered systems in critical infrastructure environments, where the stakes of cyber incidents are particularly high. Mori's findings supported the notion that AI can offer advanced predictive capabilities, allowing organizations to proactively address potential threats and recover quickly from any disruptions. This study aligned with broader trends in AI adoption for improving cyber resilience in high-risk sectors.

Reddy and Ayyadapu (2020) investigated AI-based cloud security incident response, highlighting the increasing importance of automation in cloud security incident management. Their research indicated that AI was not only able to identify but also independently remediate security threats in the cloud ecosystem, an environment that is unique in its dynamism. The study found that AI-powered incident response automation had the potential to significantly enhance the accuracy and response time of cloud security systems, offering organizations the potential to respond to incidents with very little human intervention.

3. RESEARCH METHODOLOGY

3.1.Research Design

This study employs a quantitative, descriptive approach to examine the effect of AI-based incident response mechanisms in corporate networks. The emphasis is on investigating the frequency and efficacy of various AI responses against multiple types of security threats. Utilizing numerical data, the study exemplifies how AI improves security and resiliency.

3.2. Data Collection

Data was gathered in a simulated enterprise network setting with an AI-powered incident response platform. Within the observation timeframe, 150 AI response actions and 150 security incidents were noted. Data was automatically collected by the AI system and manually authenticated by cybersecurity experts to provide assurance of accuracy.

3.3. Sampling Technique

A purposive sampling technique was used, focusing on those incidents that specifically elicited an AI response. Excluded were manual-only interventions or incidents beyond the scope of AI actions to keep the research focus specifically on AI capabilities.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.4. Data Analysis Methods

The data gathered was processed using frequency and percentage analysis to establish the distribution of incident types and AI response actions. Comparative analysis was used to identify incident categories and the most frequently deployed AI actions. Descriptive statistics were applied to summarize and interpret the findings, offering insights into the performance trends of AI systems.

4. DATA ANALYSIS

The table shows the distribution of AI response actions in a simulated enterprise network. Automated Threat Containment was the most common action, accounting for 33.3% of responses, emphasizing AI's role in quickly isolating threats.

Table 1: Frequency and Percentage of AI Response Actions

AI Response Action	Frequency (Number of Actions)	Percentage (%)
Automated Threat Containment	50	33.3%
Alert Generation and Notification	30	20%
Traffic Filtering and Blocking	25	16.7%
Behavior-Based Access Restriction	20	13.3%
Automated Forensic Data Collection	15	10%
Incident Report Generation	10	6.7%

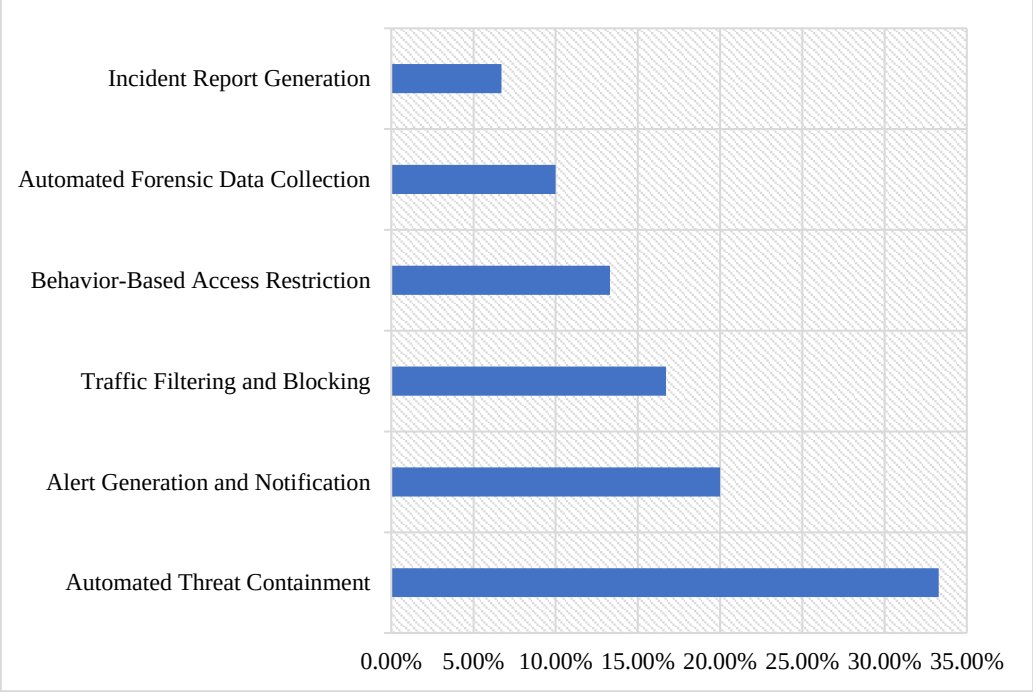

Figure 1: Percentage of AI Response Actions

Alert Generation and Notification (20%) keeps security teams informed, while Traffic Filtering and Blocking (16.7%) proactively mitigates network threats. Behavior-Based Access Restriction (13.3%) limits suspect user behavior, and Automated Forensic Data Collection (10%) assists in the collection of evidence. Finally, Incident Report Generation (6.7%) provides documentation. Generally speaking, AI's actions facilitate streamlined incident response by minimizing manual intervention and maximizing security efficiency.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2: Frequency and Percentage of AI-Driven Incident Responses

Type of Incident	Frequency (Number of Cases)	Percentage (%)
Malware Detection	40	30%
Phishing Attack	30	20%
Insider Threat (Behavioral Anomaly)	25	15%
DDoS Attack	20	12.5%
Unauthorized Access Attempt	15	10%
Data Exfiltration Attempt	15	7.5%
Other Minor Security Events	5	5%

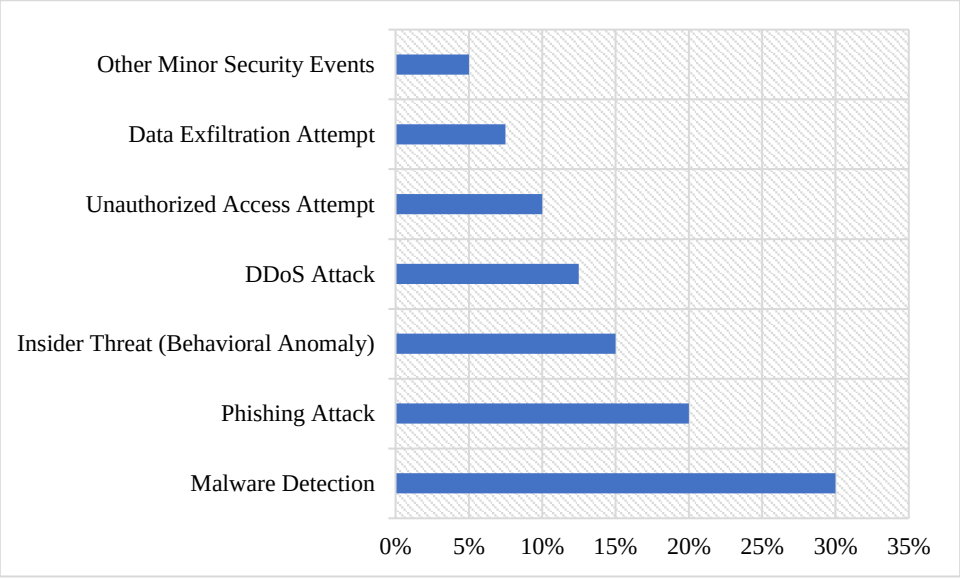

Figure 2: Percentage of AI-Driven Incident Responses

The table depicts the occurrence of various types of security incidents that were experienced in a simulated enterprise network setup. The most frequent incident was Malware Detection at 30% of the total number, due to the prevalence of malware-based attacks in network environments. Phishing Attacks stood at 20%, as was the prevalence of social engineering-based attacks on users. Insider Threats (15%) point to the threat of unauthorized or suspicious activity in the organization, while DDoS Attacks (12.5%) denote outside threats directed at overwhelming network resources. Unauthorized Access Attempts and Data Exfiltration Attempts each totaled 10% and 7.5%, respectively, with a clear concern regarding unauthorized access and possible data breaches. Finally, Other Minor Security Events (5%) were fewer in occurrence but nonetheless significant because they tend to be precursors to more severe threats. Overall, the statistics highlight the myriad of security events that AI-powered incident response systems must contend with in today's enterprise networks.

5. CONCLUSION

The study proves that AI-based incident response processes greatly increase the efficacy, speed, and precision of cybersecurity activities in enterprise networks. By comparing 150 AI response actions and 150 classifiable security incidents quantitatively, it was discovered that automated threat containment was the most commonly used AI action, with 33.3% usage out of total responses. Malware detection was the most prevalent incident type, contributing 30% towards all incidents. The statistics indicate that AI technologies not only facilitate quicker detection and threat mitigation but also enable intelligent prioritization and reporting, lightening the load for human analysts. The very high rates of automated responses, including containment and alert generation, demonstrate AI's vital role in reacting to incidents in real time. In total, the results confirm that the integration of AI in incident response platforms

strongly enhances enterprise network security and resilience, enabling organizations to address changing cyber threats proactively with greater agility and accuracy.

REFERENCES

[1] Ahmed, N., Hossain, M. E., Hossain, Z., Kabir, M. F., & Hossain, I. S. (2024). AI-Enabled System for Efficient Cyber Incident Detection and Response in Cloud Environments: Safeguarding Against Systematic Attacks. Indonesian Journal of Educational Science and Technology, 3(4), 233-248.

[2] Akinade, A. O., Adepoju, P. A., Ige, A. B., Afolabi, A. I., & Amoo, O. O. (2021). A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience. International Journal of Science and Technology Research Archive, 1(1), 39-59.

[3] Ashfin, P. (2024). AI-Driven Threat Detection and Response in Cybersecurity. Bulletin of Engineering Science and Technology, 1(2), 125-143.

[4] Chinta, P. C. R., Jha, K. M., Velaga, V., Moore, C., Routhu, K., & SADARAM, G. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. Available at SSRN 5151788.

[5] Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. International Journal for Electronic Crime Investigation, 7(2).

[6] Hussain, A. (2024). AI and Machine Learning in Action: Revolutionizing Enterprise Data Security and Cloud Infrastructure Protection.

[7] IBRAHIM, A. (2024). Innovating Security: AI-Driven Solutions for Cyber Resilience.

[8] Khalid, I., & Purdie, M. S. (2024). AI-Powered SOC Operations: Revolutionizing Cyber Security Incident Response and Management.

[9] Maharjan, P. (2023). The Role of Artificial Intelligence-Driven Big Data Analytics in Strengthening Cybersecurity Frameworks for Critical Infrastructure. Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 7(11), 12-25.

[10] Moore, C., Chinta, P. C. R., & Routhu, K. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. Available at SSRN 5130235.

[11] Mori, J. (2023). AI-Driven Cyber Resilience in Critical Infrastructure: Enhancing Threat Prediction, Detection, and Recovery. Journal of Computing and Information Technology, 3(1).

[12] Reddy, A. R. P. (2022). The Future Of Cloud Security: Ai-Powered Threat Intelligence And Response. International Neurourology Journal, 26(4), 45-52.

[13] Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.

[14] Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-Powered Operational Resilience: Building Secure, Scalable, and Intelligent Enterprises. Artificial Intelligence and Machine Learning Review, 3(1), 1-10.

[15] Tatineni, S. (2023). AI-infused threat detection and incident response in cloud security. International Journal of Science and Research (IJSR), 12(11), 998-1004.