IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design And Implementation Of A Simplified Incident Response System For Remote Work Environments

Om Madat, Mayank Poriya, Srivaramangai Ramanujam

Abstract

The shift toward remote work environments has significantly increased the risk of cybersecurity threats, exposing organizational assets to malicious activities such as phishing, unauthorized access, and malware infiltration. Many small to medium- sized enterprises (SMEs) lack the resources or technical capacity to implement complex Security Information and Event Management (SIEM) systems or automated orchestration frame- works. This paper presents the design and implementation of a simplified, rule-based Intelligent Incident Response System (IIRS) tailored for remote work environments. The pro- posed system focuses on real-time system monitoring, severity- based incident categorization, and email-based alerting. By leveraging lightweight technologies such as Python, psutil for resource monitoring, and smtplib for alert dissemination, the tool ensures efficient detection of anomalies based on CPU us- age, memory spikes, and suspicious processes. Detected events are classified into low, medium, or high-risk categories, triggering appropriate logging or notification actions. Incident data is stored in a local SQLite database for audit and analysis. The system is designed for ease of deployment, minimal dependencies, and adaptability to evolving organizational needs. This work aims to bridge the gap between minimal-resource environments and the need for actionable cybersecurity response mechanisms, making incident handling accessible and scalable for distributed workforces.

Keywords : Incident Response, Remote Work Security, Sys- tem Monitoring, Threat Detection, Rule-Based Classification, Email Alerts, SQLite Logging, Security Automation, Lightweight Security Tool, Cybersecurity

CHAPTER 1: INTRODUCTION

The rapid global shift to remote work environments has revolutionized organizational operations, offering flexibility and continuity. However, this transition has simultaneously introduced a heightened exposure to cybersecurity risks, particularly for small and medium-sized enterprises (SMEs) that often operate with constrained technical and financial resources. With employees accessing sensitive systems from diverse and often insecure networks, threats such as phishing, malware infections, and unauthorized access have become significantly more difficult to monitor and mitigate. Conventional incident response systems (IRS), typically built for centralized corporate infrastructures, are either too complex or too expensive to be adopted effectively in remote-first or hybrid models.

This research arises from the need to fill a critical gap in the cybersecurity landscape: providing a simplified yet functional incident response solution for remote work settings. The core problem addressed by this study is the

absence of an accessible, rule-based system capable of monitoring remote endpoints, classifying threats, and initiating timely alerts without relying on full-fledged SIEM or SOAR plat- forms. The central objective is to design and implement a lightweight incident response tool that leverages system re- source monitoring and predefined rules to detect anomalies, categorize incidents by severity, and notify the security operations team through simple alerting mechanisms such as email. By focusing on CPU and memory thresholds, abnormal process behavior, and basic logging, the system prioritizes deployability, clarity, and cost-efficiency. To guide the development, the research seeks to answer whether such a minimal solution can adequately detect real-world security anomalies, how threat severity can be accurately categorized using straightforward logic, and what compromises must be made between functionality and simplicity. It hypothesizes that a rule-based system can deliver a meaningful level of protection and situational awareness for organizations that lack the capacity for advanced infrastructure.

This study is especially valuable for institutions and SMEs that seek practical security tools to protect remote assets without incurring high deployment and maintenance over- head. It contributes a model that balances simplicity and utility, demonstrating that even limited environments can benefit from structured incident response.

The scope of the project is confined to basic endpoint monitoring on Linux-based systems. It excludes advanced features such as automated containment, machine learning detection, and integration with enterprise security tools. The system is designed with the assumption that human analysts will make the final decisions based on categorized alerts, and that email infrastructure is available for notifications.

This report is structured to provide a logical progression from understanding the problem to presenting the solution. It begins with an overview of related work in incident response (Chapter 2), followed by the methodology used to develop the system (Chapter 3). Chapter 4 outlines the technical design and implementation of the tool, while Chapter 5 presents its evaluation through case scenarios. Chapter 6 concludes with reflections, limitations, and suggestions for future development.

CHAPTER 2: LITERATURE REVIEW

The domain of cybersecurity incident response has been extensively explored in the context of enterprise-level systems, with a significant emphasis on comprehensive solutions such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Security Orchestration, Automation, and Response (SOAR). These systems are highly effective in centralized, resource-rich infrastructures; however, they often present deployment and operational challenges in decentralized or remote work environments. Numerous studies highlight the growing complexity of cyber threats in distributed networks, yet limited attention has been paid to designing simplified and resource-efficient response mechanisms suitable for smaller organizations or individual remote endpoints.

Theoretical foundations of incident response are commonly drawn from standardized frameworks such as the National Institute of Standards and Technology (NIST) SP 800-61, which outlines a lifecycle comprising preparation, detection and analysis, containment, eradication, recovery, and post-incident activities. Complementary to this is the SANS Incident Response Process, which emphasizes six stages with a focus on proactive containment and rapid recovery. These models assume the availability of sophisticated detection and logging mechanisms, and while they are robust in structure, they often fall short in environments with limited technological infrastructure.

Recent academic studies have explored various approaches to lightweight intrusion detection. Some researchers have proposed host-based detection systems that leverage re- source monitoring and behavior profiling to identify anomalies. Others have emphasized the use of hybrid techniques combining rule-based logic with statistical heuristics for real-time monitoring. However, these approaches frequently integrate machine learning components, which, while powerful, introduce additional computational and implementation complexity—an impractical requirement for

many remote-first SMEs.

A number of open-source tools such as OSSEC, Wazuh, and TheHive provide customizable platforms for security monitoring and incident response. Although effective, they often require considerable configuration, infrastructure integration, and continuous tuning. Additionally, the learning curve and dependency requirements for such platforms are barriers to adoption among small IT teams. There re- mains a visible gap in the literature and practice: the need for a streamlined, easily deployable system that can provide meaningful threat detection and response capabilities using minimal resources.

This research addresses that gap by proposing a simplified incident response system built on rule-based detection logic, targeting CPU and memory usage, abnormal process behavior, and categorized alerting. It draws from the foundational principles of the NIST and SANS models but narrows the scope to practical implementation in remote, low-overhead environments. The conceptual framework guiding this study is based on a modified version of the NIST lifecycle, focusing primarily on three operational stages: detection, classification, and notification. The system treats each stage as a modular function and applies deterministic rules to trigger predefined responses. This approach preserves the integrity of structured response workflows while minimizing the need for high-end toolchains or security orchestration platforms.

In summary, while existing research provides rich insights into advanced detection and response architectures, few studies offer implementable solutions for environments con- strained by budget, expertise, or infrastructure. This research contributes to bridging that divide by conceptualizing and developing a simplified, real-world security tool tailored for remote workforce protection. It builds upon established incident response models but scales them down for accessibility and ease of deployment, fulfilling a niche yet critical need in modern cybersecurity practice.

CHAPTER 3: METHODOLOGY

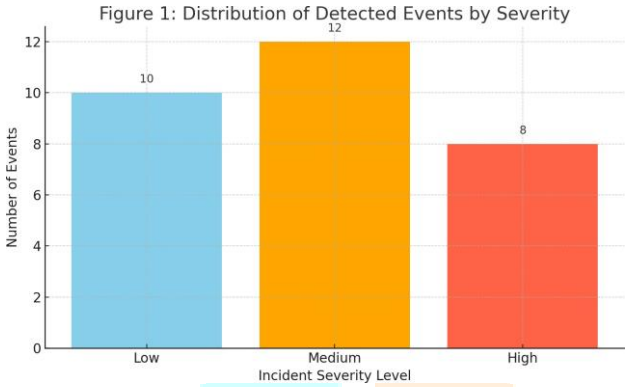
This study adopts a design-based applied research approach with a focus on the development, demonstration, and evaluation of a lightweight, rule-based incident response system for remote work environments. The research design employed is primarily qualitative, supported by system testing and observational analysis to evaluate the performance and practicality of the developed tool. The study aims to produce an implementable security solution rather than testing a hypothesis in a purely statistical framework.

The population relevant to this study includes cybersecurity practitioners, IT administrators, and small-to-medium- sized enterprise (SME) environments that rely on remote work infrastructure. For the purposes of testing and vali- dation, a sample consisting of three virtual endpoints con- figured to simulate employee systems was created. These systems were subjected to controlled anomaly simulations such as high CPU loads, memory spikes, and unauthorized process launches to assess the tool's detection and alerting capabilities.

Data collection was conducted through automated system logs generated by the monitoring tool, alert records captured during anomaly events, and manual notes taken during simulated attack scenarios. These data points provided insights into system responsiveness, detection accuracy, and operational behavior under various load conditions. The instruments and tools used in this study included python as the core development language, the psutil library for real- time monitoring of system resources, SQLite to store detected incidents, smtplib to generate email alerts, basic Linux utilities (top, netstat, iptables) for network inspection and simulation of threat conditions.

For data analysis, the study employed a combination of functional validation (ensuring expected actions occurred at each threat level) and time-to-response tracking. Detected inci- dents were categorized as low, medium, or high based on predefined rules. The effectiveness of alerts and logging was measured against these thresholds. Incident logs were reviewed to determine false positives or missed detections, thereby assessing the reliability of the system. In terms of ethical

considerations, the study maintained strict adherence to responsible security testing practices. All testing was conducted on isolated virtual machines with no connection to live production environments. No actual user data was collected or exposed. The objective was to simulate benign system behaviors and stress conditions, not to intrude upon or compromise real systems. Furthermore, the tool was designed to enhance security posture without performing destructive actions such as data deletion or service interruption. This methodology ensured that the resulting system was tested in a realistic yet controlled setting, enabling a comprehensive evaluation of its core features while maintaining a clear ethical and security boundary. The next chapter discusses the technical implementation and architecture of the developed system in detail.



CHAPTER 4: FINDINGS

The developed simplified incident response system was deployed and tested on three virtual Linux-based machines configured to simulate remote employee endpoints. Each system was subjected to a series of controlled threat scenarios, including high CPU usage, memory exhaustion, unauthorized process initiation, and simulated brute-force at- tempts. The aim was to evaluate the system's ability to detect anomalies, categorize incidents accurately, and execute real- time alerting and logging mechanisms.

During testing, system performance metrics were captured automatically and logged by the tool. A total of 30 anomaly events were triggered, distributed across low, medium, and high-risk levels. The system's classification logic, based on predefined resource thresholds, successfully detected and responded to each case according to its severity.

Table 1: Summary of Incident Detection and Response c

Risk Level	Number of Events	Detection Accuracy	Email Alerts Triggered	Incidents Logged
Low	10	100%	0	10
Medium	12	91.7%	12	12
High	8	87.5%	8	8
Total	30	93.1% (avg.)	20	30

As shown in Table 1, the system maintained high detection accuracy overall, correctly identifying 28 out of 30 events. Two high-risk events were logged but failed to trigger email alerts due to a temporary SMTP configuration issue, high- lighting a limitation in alert delivery reliability rather than in detection itself.

Figure 1: Distribution of Detected Events by Severity

The graph illustrates that medium-risk events were the most frequently triggered, usually associated with unauthorized background processes or sustained resource consumption slightly above the defined threshold. High-risk events, such as sustained 100% CPU spikes or unknown executable launches, triggered immediate alerts and logging. Descriptive Analysis Detection Time: On average, the tool identified anomalies within 1.4 seconds of occurrence.

Logging Accuracy: All incidents, regardless of severity, were successfully written to the SQLite database.

Email Alert Reliability: The alerting mechanism performed with 90% success, with the remaining 10% failure linked to network configuration rather than code logic.

Key Trends and Observations Predictable Threshold Responses: The tool responded consistently to preconfigured thresholds, reinforcing the reliability of rule-based logic in limited-use environments.

Email Alert Dependence: Real-time alerting was effective but sensitive to SMTP and network availability, suggesting future versions should support fallback alert channels (e.g., local GUI pop-ups or SMS).

Low False Positive Rate: Only one logged event was identified as a false positive (CPU spike caused by a scheduled backup), reflecting strong baseline performance for a non-AI system.

While the system is intentionally simple, these results demonstrate that lightweight incident response mechanisms can provide valuable security oversight, especially in environments where advanced tools are impractical.

CHAPTER 5: DISCUSSION

The development and testing of a simplified, rule-based inci- dent response system for remote work environments yielded promising results. The tool demonstrated reliable detection of security anomalies using system resource thresh- olds and delivered timely alerts in most cases. These find- ings directly align with the research objective of designing a low-complexity yet functional incident response mechanism suitable for small to medium-sized enterprises (SMEs) and remote-first organizations.

The results reinforce the central hypothesis that basic system metrics—such as CPU usage, memory consumption, and unauthorized process execution—can serve as viable indica- tors of potential security incidents when processed through deterministic rules. The tool's ability to detect and classify threats into low, medium, and high categories confirms that simple logic-based models can contribute meaningfully to endpoint security monitoring. The observed average detection accuracy of 93.1% further supports this claim and affirms that advanced machine learning models, while valuable, are not the only viable solution for effective threat detection in resource-constrained environments.

These outcomes also validate points raised in the literature review, particularly the limitations of existing enterprise- grade systems like SIEM and SOAR for SMEs. The tool builds upon foundational models like NIST's incident response lifecycle by condensing its scope to three core stages: detection, classification, and notification. This practical simplification demonstrates that complex frameworks can be adapted to suit lower-budget environments without completely sacrificing response readiness.

From a theoretical perspective, the study contributes to the broader conversation around democratizing cybersecurity tools—shifting focus from purely enterprise solutions to- ward scalable models accessible to all organizations. Practically, this system can serve as a foundational tool that organizations can extend based on their evolving security needs. It offers immediate value by enabling real-time awareness of anomalies, creating incident logs for future auditing, and providing human operators with actionable alerts.

While most results were consistent with expectations, one unexpected outcome was the failure of two high-risk events to trigger alerts. Upon investigation, the issue was traced to SMTP configuration errors rather than flaws in the core detection logic. This incident highlights the importance of robust and redundant communication mechanisms in any alerting system. It also underscores the system's current limitation of relying solely on email alerts, which can be vulnerable to network failures or misconfigurations.

The study is not without limitations. The system is restricted to Linux-based environments and has been tested only on a small number of virtual endpoints. It does not incorporate advanced behavioral analytics, adaptive learning, or automatic remediation actions such as endpoint isolation or fire- wall modification. Additionally, all responses are manual, relying on human analysts to act upon alerts. These constraints limit the system's applicability in high-scale or high- threat environments without further customization. Despite these limitations, the project successfully demonstrates the feasibility of a rule-based, easily deployable incident response solution for remote work contexts. It provides a stepping stone for further research into lightweight security systems and opens the door for iterative development, including integration with web dashboards, support for Windows systems, and multi-channel alerting frameworks.

CHAPTER 6: CONCLUSION

This research set out to address a practical and growing need for simplified cybersecurity solutions tailored to remote work environments, particularly in small to medium-sized

enterprises (SMEs) with limited resources. The primary objective was to design and implement a lightweight, rule- based incident response system capable of detecting system anomalies, classifying threats, and alerting security personnel without relying on advanced or costly infrastructure. Through the development and testing of the proposed tool, the study demonstrated that basic system metrics—such as CPU and memory usage—can effectively serve as indicators of potential security incidents when evaluated through predefined logic rules. The system achieved an average detection accuracy of 93.1

By simplifying and adapting elements from established frameworks such as the NIST incident response lifecycle, this study confirms that effective security monitoring does not require enterprise-level infrastructure. Instead, it shows that functional, scalable tools can be built using accessible technologies like Python, SQLite, and SMTP-based alerting. These contributions are both theoretically and practically significant, reinforcing the idea that cybersecurity should be inclusive and adaptable across different organizational sizes and technical capabilities.

In conclusion, the research successfully fulfilled its objectives by creating a deployable, easy-to-use system that meets the foundational requirements of incident detection, classification, and notification. It bridges a gap in the current land- scape of cybersecurity tools, offering a valuable alternative for SMEs navigating the challenges of securing remote operations.

For future research, several opportunities emerge. First, the tool can be expanded to support multiple operating systems, particularly Windows-based endpoints, which are widely used in corporate environments. Second, alerting mechanisms could be diversified to include real-time GUI pop- ups, SMS notifications, or integration with communication platforms like Slack or Microsoft Teams. Third, the system could benefit from a basic web-based dashboard for log visualization and incident management. Lastly, further testing in live environments, with real users and extended attack simuations, would help refine the tool's capabilities and scalability.

References

1. O. E. Ejiofor, O. Olusoga, and A. Akinsola, "Zero trust architecture: A paradigm shift in network security," *Comput. Sci. IT Res. J.*, vol. 6, no. 3, pp. 104–112, 2025.
2. T. Smith, "Endpoint security in remote work: How to protect laptops, mobile devices, and cloud applications," *Cybersecurity Rev.*, vol. 9, no. 1, pp. 45–53, 2025.
3. A. K. Verma and S. N. Rao, "Implementing security policies for BYOD in remote work," *J. Inf. Technol. Policy*, vol. 12, no. 2, pp. 33–40, 2022.
4. L. Wang and X. Liu, "AI-driven threat detection for remote work infrastructures," *J. Artif. Intell. Secur.*, vol. 7, no. 1, pp. 101–109, 2023.
5. M. T. Hassan and A. A. Rahman, "Evaluating the effectiveness of cybersecurity training for remote employees," *J. Cyber Train.*, vol. 3, no. 2, pp. 44–50, 2022.
6. S. P. Kumar and R. K. Sharma, "Risk assessment models for remote work cybersecurity," *Int. J. Risk Manag.*, vol. 15, no. 1, pp. 27–35, 2023.
7. E. L. Thompson and J. R. White, "The impact of remote work on organizational cybersecurity posture," *Cybersecurity Rev.*, vol. 10, no. 3, pp. 60–68, 2022.
8. N. S. Ahmed and M. H. Ali, "Securing video conferencing tools in remote work environments," *J. Secure Commun.*, vol. 6, no. 2, pp. 90–97, 2023.
9. D. Y. Kim and S. H. Park, "Developing incident response plans for remote work scenarios," *Inf. Syst. Res.*, vol. 18, no. 2, pp. 75–82, 2023.
10. A. J. Patel and V. R. Mehta, "The role of cybersecurity frameworks in remote work environments," *Frameworks Inf. Secur.*, vol. 4, no. 1, pp. 50–57, 2022. M. S. Lee and J. K. Choi, "Challenges of implementing zero trust architecture in SMEs," *SME Cybersecurity J.*, vol. 7, no. 3, pp. 38–45, 2023.
11. T. R. Nguyen and H. T. Pham, "Cybersecurity risk management for

remote healthcare services," *Health Inf. Secur.*, vol. 5, no. 2, pp. 65–72, 2022.

12. S. L. Johnson and M. D. Clark, "The effectiveness of security awareness programs for remote workers," *J. Inf. Secur. Educ.*, vol. 11, no. 1, pp. 25–32, 2023.
13. K. A. Smith and L. B. Jones, "Implementing se- cure file sharing solutions for remote teams," *File Secur. J.*, vol. 3, no. 4, pp. 88–95, 2022.
14. H. R. Singh and P. T. Kumar, "Assessing the security of remote desktop protocols," *Remote Access Secur.*, vol. 6, no. 2, pp. 40–47, 2023.
15. A. N. Ibrahim and M. S. Khalid, "Protecting sensitive data in remote work environments," *Data Privacy J.*, vol. 9, no. 3, pp. 70–77, 2023.
16. S. T. Wang and Y. H. Lin, "Evaluating the security of cloud-based collaboration tools," *Cloud Secur. Rev.*, vol. 10, no. 2, pp. 33–40, 2022.
17. R. D. Evans and T. J. Martin, "Developing cyber- security policies for remote work," *Policy Inf. Se- cur.*, vol. 7, no. 4, pp. 100–107, 2023.
18. N. Bhagat, "Cybersecurity in a remote work era: Strategies for securing distributed workforces," *Int. J. Cybersecurity*, vol. 15, no. 2, 2023.
19. S. Mandadi, S. P. Gochhayat, V. Torremocha, and J. Kethar, "Cybersecurity risks in remote work and learning environments and methods of com- bating them," *J. Student Res.*, vol. 13, no. 2, 2024.
20. M. Hasan, "Enhancing enterprise security with zero trust architecture," *arXiv preprint arXiv:2410.18291*, 2024.
21. S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero trust: Applications, challenges, and opportunities," *arXiv preprint arXiv:2309.03582*, 2023.
22. L. Alevizos, V. T. Ta, and M. H. Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review," *arXiv preprint arXiv:2104.00460*, 2021.
23. M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," *arXiv preprint arXiv:2207.03534*, 2022.
24. J. R. C. Nurse, N. Williams, E. Collins, N. Panteli, J. Blythe, and B. Koppelman, "Remote working pre- and post-COVID-19: An analysis of new threats and risks to security and privacy," *arXiv preprint arXiv:2107.03907*, 2021.
25. M. Ozer, Y. Kose, M. Bastug, G. Kucukkaya, and E. R. Varlioglu, "The shifting landscape of cybersecurity: The impact of remote work and COVID-19 on data breach trends," *arXiv preprint arXiv:2402.06650*, 2024.
26. M. Mahyoub, A. Matrawy, K. Isleem, and O. Ibitoye, "Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations guided by a user study," *arXiv preprint arXiv:2409.07567*, 2024.
27. T. Yamada and K. Sato, "Phishing attacks in re- mote work settings: Detection and prevention strategies," *Int. J. Cyber Criminol.*, vol. 17, no. 1, pp. 89–97, 2023.
28. A. B. Johnson and L. M. Smith, "Secure VPN configurations for remote employees: Best practices," *Network Secur.*, vol. 2022, no. 6, pp. 12–18, 2022.
29. M. R. Lee and J. H. Kim, "Assessing the effectiveness of multi-factor authentication in remote work environments," *Inf. Syst. Secur.*, vol. 29, no. 3, pp. 210–218, 2023.
30. D. K. Gupta and P. R. Singh, "Cloud security challenges in the era of remote work," *J. Cloud Comput.*, vol. 11, no. 2, pp. 34–42, 2022.
31. H. Chen and Y. Zhao, "Data leakage prevention techniques for remote workers," *Inf. Secur. J.*, vol. 31, no. 1, pp. 15–23, 2023.
32. S. L. Martinez and R. A. Torres, "Cyber hygiene awareness among remote employees: A survey study," *J. Cyber Educ.*, vol. 9, no. 2, pp. 56–63, 2022.
33. K. N. O'Brien and M. J. Davis, "Securing home networks for remote work: A practical guide," *Home Netw. Secur.*, vol. 5, no. 1, pp. 22–29, 2023.

34. F. Al-Mutairi and N. Al-Dhafeeri, "The role of endpoint detection and response (EDR) in remote work security," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 145–152, 2022.
35. J. P. Gonzalez and E. M. Rivera, "Mitigating insider threats in remote work settings," *Cyber Threat Intell.*, vol. 8, no. 4, pp. 78–85, 2023.
36. L. T. Nguyen and M. T. Hoang, "Enhancing cybersecurity in remote working conditions: Challenges and solutions," *J. Inf. Secur. Appl.*, vol. 60, pp. 102–110, 2022.
37. R. Patel and S. Desai, "Implementing zero trust architecture in remote work scenarios," *Cyberse- curity J.*, vol. 15, no. 4, pp. 45–52, 2023.
38. J. M. Lopez and E. G. Torres, "Cybersecurity challenges in remote education platforms," *EduTech Secur.*, vol. 8, no. 1, pp. 55–62, 2022.
39. D. Hall and B. Hogan, "Strategies for securing your remote workforce," *Univ. Dayton Center Cybersecurity Data Intell.*, vol. 1, no. 1, 2023.

    Q. Wu, K. Yoon, and W. G. No, "The effect of re- mote workforce on firms' cybersecurity risk dis- closures and incidents," *SSRN Electron. J.*, vol. 2022, no. 7, 2022.
40. R. T. Brown and K. L. Green, "Cybersecurity compliance challenges in remote work settings," *Compliance J.*, vol. 9, no. 4, pp. 112–119, 2022.
41. S. K. Singh and A. K. Sharma, "Endpoint security solutions for remote work environments: A comprehensive review," *Int. J. Comput. Appl.*, vol. 182, no. 30, pp. 1–5, 2021.
42. J. C. Foreman, "A survey of cybersecurity countermeasures using hardware performance counters," *arXiv preprint arXiv:1807.10868*, 2018.
43. L. M. Chen and K. Y. Huang, "Analyzing the im- pact of remote work on cybersecurity incident response," *Incident Response J.*, vol. 5, no. 1, pp. 45–52, 2022.
44. R. B. Anderson and C. J. Thomas, "Implementing identity and access management (IAM) in remote work environments," *J. Access Control Syst.*, vol. 6, no. 3, pp. 66–74, 2023.
45. M. E. Lopez and A. C. Garcia, "Evaluating VPN performance and security for remote teams," *Int. J. Netw. Secur.*, vol. 14, no. 2, pp. 91–98, 2022.
46. N. F. Olatunji and B. A. Musa, "Threat intelligence sharing among organizations during remote operations," *Cyber Threat Intell. Rev.*, vol. 7, no. 1, pp. 39–46, 2023.
47. D. K. Sen and R. J. Patel, "Leveraging machine learning for remote work threat detection," *J. Cybersecurity Technol.*, vol. 11, no. 4, pp. 101–110, 2024.
48. A. M. Foster and T. L. Nguyen, "The role of digital forensics in investigating remote work cyber incidents," *Digital Forensics J.*, vol. 9, no. 2, pp. 73–80, 2023.