International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3145-3148
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0399

An Intelligent AI-Driven Vulnerability Management System for Automated Risk Assessment and Remediation

Francis Robina Swamidass [1], Abinaya M [2], Fathima Mariyam Z [3],
[1,2,3] UG Scholars, Department of Artificial Intelligence & Data Science, Saranathan College of Engineering (An Autonomous Institution), Venkateswara Nagar, Panjappur, Tiruchirappalli – 620 012, Tamil Nadu, India,
Email ID: *francisrobinaswamidass@gmail.com [1],mabinaya2502@gmail.com [2]*
mariyamfathima1111@gmail.com[3]

Abstract
The increasing complexity of modern enterprise IT environments, encompassing both cloud-based and on-premise systems, has made vulnerability management a critical challenge. Traditional approaches are often manual, reactive, and fragmented, leading to delays in detection and remediation. This paper presents an AI-driven centralized vulnerability management system that automates vulnerability detection, intelligent risk prioritization, remediation orchestration, and continuous monitoring through a unified platform. The proposed system integrates distributed scan engines, workflow automation, and an AI-based analytical module to enhance decision-making. Experimental evaluation demonstrates improved prioritization accuracy, reduced manual effort, and faster remediation cycles, thereby strengthening overall cybersecurity resilience.
Keywords: *Artificial Intelligence, Cybersecurity, Vulnerability Management, Risk Assessment, Automation*

1. Introduction
The rapid growth of digital technologies has significantly transformed organizational operations, enabling improved efficiency and scalability. However, this transformation has also increased the attack surface, exposing systems to a wide range of cyber threats. As the number of connected devices continues to grow, managing vulnerabilities efficiently has become a major concern for organizations. Traditional vulnerability management systems rely heavily on manual processes, periodic scanning, and isolated tools. These approaches often fail to provide real-time insights and effective prioritization, resulting in delayed remediation and increased risk exposure. To address these limitations, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has emerged as a promising solution. This paper proposes an intelligent AI-driven vulnerability management system that automates the entire lifecycle—from detection to remediation—while incorporating contextual risk factors such as asset criticality and exposure [3].

1.1. Problem Statement
Existing vulnerability management approaches suffer from five key limitations: periodic rather than continuous scanning, manual triage prone to human error, CVSS-only prioritisation that ignores asset criticality and business context, siloed tooling requiring manual correlation, and reactive postures that address vulnerabilities only after identification. These deficiencies result in prolonged mean time to remediate (MTTR), inconsistent stakeholder accountability, and limited real-time visibility into organisational security posture [2].

1.2.Objectives
The primary objectives of this system are:
- Automate end-to-end vulnerability detection and remediation workflows.
- Implement AI-driven, context-aware risk prioritisation beyond CVSS scoring.
- Integrate heterogeneous enterprise security tools into a unified platform.
- Deliver real-time executive reporting and stakeholder notifications.
- Shift security posture from reactive to proactive and predictive [1].

2. Literature Review
Dasgupta et al. (2020) provided a comprehensive survey of ML techniques in cybersecurity, including supervised and unsupervised approaches but did not address operational integration into end-to-end remediation workflows. Mavroeidis and Bromander (2017) identified key barriers to AI adoption in cybersecurity including model explainability and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3145-3148
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0399

data quality, predating modern orchestration tools. Elbes et al. (2024) proposed conceptual AI-driven vulnerability models but lacked practical enterprise-level implementation details. Khan et al. (2022) advanced CVSS prioritisation with contextual asset information but without real-time automation or ticketing integration. Abdulsatar et al. (2025) developed deep learning risk assessment for microservice architectures, focusing on cloud-native modelling without endpoint remediation pipelines. The present work bridges all identified gaps by delivering a complete, validated implementation combining intelligent prioritisation, orchestrated remediation, and automated stakeholder communication.

3. System Architecture

The proposed system operates through a five-layer pipeline architecture:

- Discovery Layer: Eve-NG virtual lab hosting Windows Server, Windows Desktop, Linux Server, and Cisco network nodes as scan targets.
- Detection Layer: Tenable Nessus performs credentialed authenticated scans via REST API, generating CVSS-enriched findings.
- Enrichment Layer: n8n Code nodes merge scan results with the Asset Inventory from Google Sheets, adding criticality, ownership, and internet-exposure context.
- Intelligence Layer: Anthropic Claude AI analyses enriched ticket data and generates natural-language executive summaries and remediation recommendations.
- Delivery Layer: Enriched XLSX reports and AI narratives are automatically emailed to stakeholders via Gmail without manual intervention shown in Figure 1.

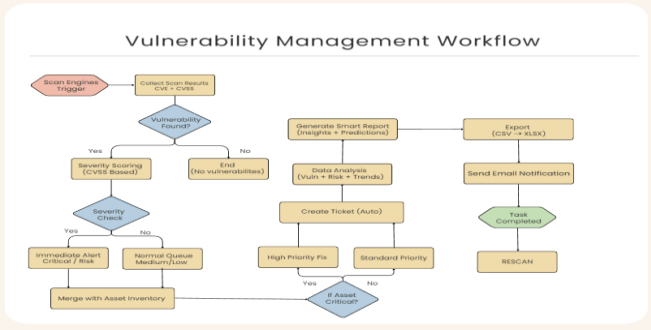

Figure 1 System Architecture

3.1.Dataset Description

The system operates on two primary datasets: vulnerability scan data and asset inventory data. The vulnerability dataset includes CVE identifiers, CVSS scores, severity levels, and affected host details obtained from scanning tools. The asset inventory dataset provides contextual attributes such as asset criticality, ownership, deployment environment, and exposure level. The integration of these datasets facilitates comprehensive and context-aware risk assessment [4].

3.2.Tools and Technologies

Tenable Nessus serves as the primary vulnerability discovery engine, scanning 279 unique plugins across four production assets and generating 1,116 open findings classified as Critical (38.7%), High (51.3%), Medium (9.3%), and Low (0.7%). n8n acts as the central orchestration hub, executing a nine-node directed acyclic workflow that ingests scan data, performs asset-inventory enrichment, runs AI analysis, converts outputs to XLSX, and delivers reports by email. The AI Analyst component uses the Claude Sonnet model with structured prompts to generate contextual, executive-quality vulnerability narratives. Gmail provides dual-mode notification: scheduled report distribution and real-time out-of-cycle critical alerts [6].

4. Methodology

The vulnerability management workflow proceeds through thirteen automated steps, triggered manually or on schedule via n8n:

- Step 1 — Initiation: The workflow is triggered via n8n's schedule or manual execution node. Steps 2–3 — Scanning and Collection: Scan engines execute authenticated vulnerability assessments across all asset groups; Tenable consolidates findings mapped to CVE identifiers with CVSS scores. Step 4 — Severity Mapping: Script 1 (Severity Mapper) normalises integer severity codes into Critical/High/Medium/Low labels and performs cross-product expansion — one row per unique asset-vulnerability pair — producing 1,401 enriched records from the current scan.
- Step 5 — Asset Enrichment: The n8n Data Merging node joins scan records with the Asset Inventory Google Sheet on IP Address, adding

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3145-3148
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0399

asset criticality, business and technical ownership, environment classification, and internet-facing status. Step 6 — Priority Scoring: Script 2 (Ticketing Engine) applies a three-dimensional composite scoring model:

- Priority Score = Sevscore + Critscore + Exposurescore : Severity contributes up to 40 points (Critical=40, High=30, Medium=20, Low=10), asset criticality contributes up to 30 points, and internet exposure contributes up to 20 points. Tickets are classified as P1 (≥80), P2 (60–79), P3 (40–59), P4 (20–39), or P5 (<20) with corresponding SLA targets of 24 hours, 72 hours, 7 days, 30 days, and best effort respectively [5].
- Steps 7–9 — AI Analysis and Reporting: The enriched ticket dataset is transmitted to the Claude API, which generates a structured executive report including: risk narrative, top critical findings with remediation steps, asset risk matrix interpretation, internet-facing asset exposure assessment, remediation priority queue with SLA context, and ownership mapping. Steps 10–13 — Report Delivery: The ticket dataset is serialised to CSV, converted to XLSX, and emailed with the AI narrative to security teams and management shown in Figure 2.

Figure 2 n8n workflow

5. Results

The system generated a total of 1,116 vulnerability findings, with 572 high, 104 medium, and 8 low severity issues, indicating that the majority of vulnerabilities fall under critical and high-risk categories. Approximately 90% of the vulnerabilities are high or critical, emphasizing the need for effective prioritization. The priority distribution shows that P1 (Immediate) vulnerabilities are minimal but critical, while P2 (High) and P3 (Medium) categories contain the majority of findings, ensuring structured remediation planning. The system successfully identified and prioritized vulnerabilities based on risk impact. Automated workflow execution enabled efficient ticket generation and reporting, reducing manual effort and improving response time. Overall, the system demonstrated effective vulnerability classification, prioritization, and automated management shown in Figure 3 and 4 .

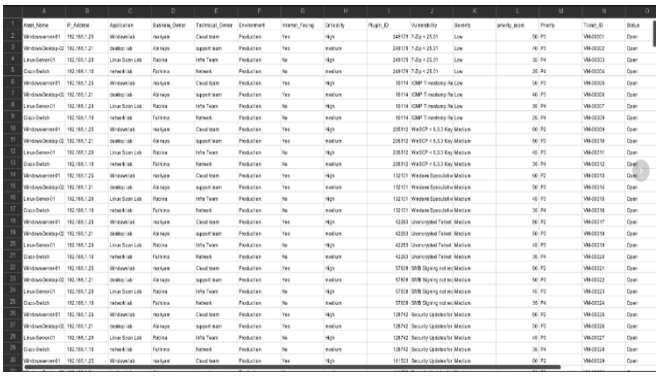

Figure 3 Final Output Dataset

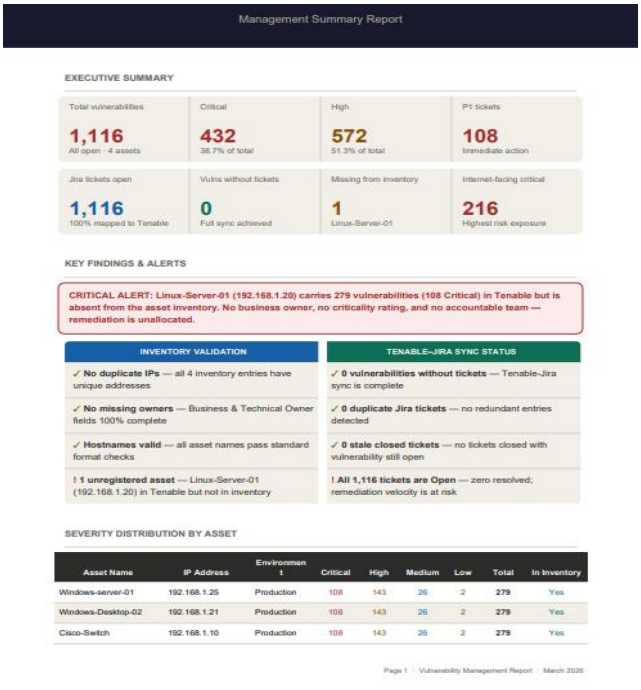

Figure 4 Output Report

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3145-3148
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0399

6. Discussion

The three-dimensional priority scoring model demonstrated superior asset-contextual accuracy compared to CVSS-only approaches. A Medium-severity vulnerability on Windows-Server-01 (High criticality, internet-facing) received a P2 classification (score: 60) while an identical finding on the internal Cisco Switch received P4 (score: 25), correctly reflecting the differential organisational risk. The AI-generated executive summaries provided actionable, contextually specific remediation guidance rather than generic patch recommendations, scaling effectively across the 1,116-finding dataset.

The system reduced the number of manual workflow steps from an estimated 47 steps in a traditional process to 2 steps (trigger and review), with total pipeline execution completing in under 4 minutes per scan cycle. Real-time alerting via Gmail ensured that Critical and P1 findings on high-value assets triggered immediate out-of-cycle notifications, addressing the SLA accountability gap identified in the literature.

Conclusion

The proposed AI-driven vulnerability management system effectively automates the entire lifecycle of vulnerability detection, prioritization, and remediation. The results demonstrate a significant reduction in manual effort through automated scanning, ticketing, and reporting processes. Additionally, the system provides unified enterprise visibility by integrating multiple components into a single workflow, enabling better governance and faster decision-making. By incorporating a multi-dimensional priority model and AI-based analysis, the system improves the accuracy of risk assessment and ensures timely remediation of critical vulnerabilities. Overall, the solution enhances operational efficiency, scalability, and proactive cybersecurity management.

Acknowledgement

The authors express their sincere gratitude to Ms. A Sridevi , Assistant Professor, Department of Artificial Intelligence and Data Science, Saranathan College of Engineering, for her invaluable guidance, encouragement, and continuous support throughout the project. The authors also extend their appreciation to the Department of Artificial Intelligence and Data Science, Saranathan College of Engineering (Autonomous), Tiruchirappalli, Tamil Nadu, for providing the necessary infrastructure and a conducive academic environment to carry out this research successfully.

References

[1]. Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine Learning in Cybersecurity: A Comprehensive Survey. Journal of Defense Modeling and Simulation.

[2]. Mavroeidis, V., & Bromander, S. (2017). Artificial Intelligence for Cybersecurity: Opportunities and Challenges. IEEE Security & Privacy.

[3]. Elbes, M., Hendawi, S., AlZubi, S., & Kanan, T. (2024). Unleashing the Full Potential of AI and ML in Cybersecurity Vulnerability Management.

[4]. Khan, N., Alghamdi, A., & Basit, S. (2022). A Risk-Based Vulnerability Management Model Using Artificial Intelligence.

[5]. Abdulsatar, M., Ahmad, H., Goel, D., & Ullah, F. (2025). Towards Deep Learning Enabled Cybersecurity Risk Assessment for Microservice Architectures. Cluster Computing.

[6]. Miraheri, S. L., Mowahhed, N., & Shahbazian, R. (2026). Cybersecurity in the Age of Generative AI: A Systematic Taxonomy of AI-Powered Vulnerability Assessment and Risk Management. Future Generation Computer Systems.