

**INOSR Scientific Research 13(1):12-20, 2026.**

**©INOSR PUBLICATIONS**

**International Network Organization for Scientific Research**

**<https://doi.org/10.59298/INOSRSR/2026/122011>**

**ISSN: 2705-1706**

**INOSRSR12200000**

## **A Cloud-Based Incident Response Platform using Machine Learning Alert Triage and Automation**

**Nwosu John Nwachukwu**

**Department of Computer Science Federal Polytechnic, Oko Anambra State, Nigeria**

**Phone Number: 08035902385**

**Email: [drnwosu2023@gmail.com](mailto:drnwosu2023@gmail.com)**

---

### **ABSTRACT**

This study developed a centralized incident response platform that records and organizes all cybersecurity incident details by automating incident detection, classifying incidents according to their types, providing real-time monitoring tools to improve visibility into incident status and their severity, and generating structured reports that support post-incident analysis, and informed decision-making by management of organizations. The methodology used is Design Science Research which involved problem identification, requirement analysis, system design using structured system analysis and design techniques, database design, and iterative software development with testing at each stage to ensure functionality, reliability, and user-friendliness. Data inputs such as incident type, severity level, affected hosts, detection time, and actions taken were captured and processed to allow for automated classification and tracking of resolution progress. The system was developed using Microsoft Visual Studio 2010 for application interface while Microsoft Access 2013 served as the database for storing and managing incident records. The platform also features dashboards and reporting tools that provide a comprehensive view of all active and past incidents, enabling organizations to assess trends, identify vulnerabilities, and maintain regulatory compliance efficiently. Testing and evaluation of the platform showed improvements in response time, accuracy of incident classification, and ease of access to incident history compared to traditional manual systems. Based on these findings, it is recommended that organizations adopt centralized and automated incident response solutions to enhance cybersecurity resilience, reduce human error, ensure faster mitigation of threats, and support effective governance and continuous improvement in security operations.

**Keywords:** Cloud-Based Incident, Machine Learning, Alert Triage and Automation

---

### **INTRODUCTION**

The growing reliance on digital technologies has significantly increased the volume of cyber incidents reported globally, necessitating more comprehensive and coordinated response mechanisms. As organizations adopt cloud-based approach for business transactions, there is an increase in various forms of cloud-based cyber attacks. As digital infrastructures expand, traditional manual response approaches have become insufficient to handle high-volume and high-velocity attacks [1]. The sophistication in the attacks has compelled organizations to adopt automated mechanisms for detecting, analyzing, and responding to security incidents. Incident Response Platforms (IRPs) have therefore emerged as essential tools that centralize incident data, streamline workflows, and support real-time decision-making. These platforms enable security teams to collect structured incident attributes, including incident type, severity level, affected assets, and timestamps, thereby enhancing response accuracy [2]. Recent studies emphasize that organizations with well-implemented IRPs experience shorter containment times and improved threat mitigation outcomes [3]. The integration of automation and analytics further strengthens an organization's ability to detect anomalies and initiate early interventions [4]. Consequently, IRPs have become indispensable components of modern cybersecurity frameworks.

In many institutions, fragmented reporting processes and inconsistent documentation hinder effective post-incident evaluation and knowledge retention [5]. IRPs address these gaps by standardizing data entry fields such as detection time, actions taken, assigned responders, and resolution summaries. This structured approach supports forensic investigations, compliance audits, and organizational learning, all of which are critical for reducing recurring security incidents [6]. Moreover, the availability of centralized dashboards

enhances situational awareness by enabling security teams to monitor incident statuses in real time [7]. The integration of threat intelligence feeds further enriches incident classification, enabling faster prioritization based on risk levels. As a result, IRPs promote efficiency, accountability, and improved organizational security governance.

In recent years, regulatory bodies and industry standards have emphasized the need for robust incident reporting systems that align with cybersecurity best practices. Organizations are now required to maintain accurate records of incident events, response actions, and closure timelines, making IRPs critical for compliance with these mandates [8]. Research highlights that platforms capable of automating documentation and generating audit-ready reports significantly reduce administrative burdens on cybersecurity teams [9]. Additionally, IRPs facilitate collaboration among incident responders by providing unified communication channels and shared access to case files. These features support multi-team coordination, which is essential during complex or large-scale cyber incidents [10]. Advanced IRPs also incorporate analytics that enable organizations to identify patterns, recurring vulnerabilities, and gaps in security controls. Through continuous monitoring and data-driven insights, organizations can strengthen resilience and adopt proactive defense strategies. Thus, IRPs play a central role in shaping modern cybersecurity readiness and operational excellence.

#### **Statement of problem**

Most of the available platforms are limited by API logging limitations which need to be manually enabled to stay active for many hours before auto-disabling which is inconvenient for continuous monitoring, some users find the configuration screens lacking in visual aids, making the internal setup phase slightly challenging, and setting up advanced alerts takes extra time. Alerts from various sources are reviewed manually, and actions such as containment, mitigation, and resolution are executed without full automation or standardized workflows. This approach often leads to delays, inconsistent responses, and limited visibility across the organization, making it challenging to prioritize critical incidents and ensure efficient communication among response teams.

#### **Purpose of study**

The proposed system for incident response platform will be designed to incorporate a range of features and functionalities to enhance its effectiveness and efficiency.

Some additional features that the proposed system can include:

- i. a centralized system for recording and organizing all cybersecurity incident details.
- ii. an automate incident detection, classification, and reporting processes for timely response.
- iii. a real-time monitoring tools that improve visibility into incident status and severity.
- iv. a structured reports that support compliance, post-incident analysis, and decision-making.

#### **Related works**

##### **Conceptual overview of Incident Response**

Incident response is a formalized and systematic approach to detecting, managing, and mitigating cybersecurity incidents within an organization. According to [11], It involves a life-cycle model with clearly defined phases such as preparation, detection and analysis, containment, eradication, recovery, and post-incident activities. This structured process ensures that organizations respond not only reactively but also proactively by establishing readiness before an incident occurs. [5], emphasize that incident response is not just about technical actions but also about governance, coordination, and training, integrating people, policy, and technology. The concept requires designated teams, often called Incident Response Teams (IRTs) or Computer Security Incident Response Teams (CSIRTs), whose roles and responsibilities are predefined to streamline operations. Its goal is to limit the damage of security breaches, restore normal operations, and mitigate future risks. Ultimately, incident response serves as a core pillar of an organization's cybersecurity resilience, combining administrative, technical, and procedural elements.

Central to the concept of incident response are its distinct phases, which provide a roadmap for handling security events. [8], describes the phase model starting with preparation, proceeding through identification, containment, eradication, recovery, and culminating in lessons learned. Preparation entails establishing policies, writing playbooks, and training the response team so that the organization has a proactive posture. When an anomaly or attack is detected, analysis is carried out to understand its scope, impact, and root cause. During containment, efforts focus on isolating affected systems to prevent further damage, while eradication aims to remove the threat completely. Recovery involves restoring affected assets and validating their integrity before resuming normal operations. Finally, post-incident activities involve learning from the event, updating policies, and feeding insights back into future preparedness and planning.

The organizational dimension of incident response is equally critical to its concept, as it requires combining technical capabilities with management and coordination. [12], argue that incident response maturity depends not only on technology but also on human and organizational factors, such as communication workflows, clarity of roles, and shared protocols. They propose aligning incident prioritization practices with maturity models so that the most severe incidents receive faster and more coordinated responses. The presence of a dedicated CSIRT, also underscores the need for institutional structures to manage incidents efficiently [11]. These teams are tasked with maintaining readiness, conducting drills, and ensuring effective collaboration

during crises. Further, incident response intersects with broader information security management, demanding policies that support continuous improvement. Thus, the concept extends beyond ad hoc reaction - it's about embedding incident response into the fabric of an organization's security culture.

### **Modern concepts of Incident Response Platforms**

Incident Response Platforms (IRPs) have evolved into highly integrated systems that centralize the management of security events, combining capabilities such as case handling, automation, and orchestration. [13], demonstrated in their case study that implementing a SOAR-based IRP significantly reduced response time by automating repetitive tasks like system isolation, account lockouts, and process termination. These platforms typically ingest data from diverse sources such as Security Information and Event Managements (SIEMs), vulnerability scanners, and asset inventories to build a unified incident picture and trigger appropriate playbooks [14]. By leveraging workflows, IRPs structure incident response actions through playbooks or runbooks, enabling repeatable and consistent responses across different scenarios. Automated tasks within IRPs not only eliminate routine manual interventions but empower teams to prioritize and execute actions based on severity and context. Additionally, platforms support case management, so responders can assign incidents, track status, and document the actions taken, which improves accountability and traceability. This centralized orchestration reduces miscommunications and ensures that response steps adhere to organizational policies and compliance requirements.

Modern IRPs increasingly embed artificial intelligence and machine learning to enhance detection, decision-making, and automation. [15], explored how AI-driven incident response systems in cloud environments can analyze large volumes of data in real time, predict threat trajectories, and initiate automated remediation quicker than humanly possible. Similarly, [16], illustrated how integrating AI into cybersecurity defense mechanisms helps detect behavioral anomalies, forecast risks, and adapt response workflows dynamically. These AI-powered platforms not only accelerate Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) but also reduce false positives through continuous learning. The proactive nature of such systems allows security teams to move from reactive firefighting to predictive threat mitigation. Furthermore, advanced IRPs use natural language processing (NLP) to translate human-written incident playbooks into machine-executable formats, thereby improving interoperability and reducing playbook development effort. The synergy of AI and automation in IRPs makes them capable of handling complex, high-volume environments with limited human oversight. In turn, this significantly strengthens an organization's operational resilience.

Another critical evolution in IRPs is their ability to integrate memory forensics and volatile data analysis to uncover sophisticated threats that elude traditional detection. [17], introduced SPECTRE, a hybrid system that includes a module for analyzing volatile memory snapshots and detecting advanced malicious activities such as living-off-the-land malware. By emulating suspicious process behavior and correlating anomalies with threat intelligence, SPECTRE enhances the forensic depth of IRPs. This modular design can feed enriched findings back into the IRP, triggering adaptive response workflows informed by memory-based evidence. The capacity to handle such low-level forensic artifacts enables security teams to detect in-memory attacks, credential theft, and stealthy persistence techniques more effectively. Moreover, SPECTRE's compatibility with existing DFIR (Digital Forensics and Incident Response) tools demonstrates how IRPs can be extended without discarding legacy investments. Such hybrid systems exemplify the shift from purely log-based detection to richer, context-aware investigation capabilities. This trend underscores how IRPs are bridging the gap between real-time response and deep forensic analysis.

### **Incident Detection and Reporting Mechanisms**

Incident detection mechanisms have undergone significant transformation with the introduction of artificial intelligence (AI) and machine learning (ML), enabling more accurate identification of anomalous activities that may signal a security breach. According to a recent review, ML-based systems now analyze network logs, user behavior, and system telemetry to detect threats that traditional signature-based tools often miss [5]. These systems can classify events in real time, distinguishing benign anomalies from malicious actions, thus reducing the noise of false positives and alert fatigue. For instance, unsupervised learning models can identify novel threat patterns without needing prior labeled data, making them highly adaptive to emerging attack vectors. Moreover, ensemble ML techniques combining decision trees, clustering, and statistical methods improve detection rates while maintaining computational efficiency [18]. Hybrid frameworks also leverage feature selection to reduce dimensionality, enabling lightweight but high-performance threat detection even in resource-constrained environments. As a result, modern detection mechanisms are not only more sensitive and intelligent but also more scalable and resilient.

Beyond pure detection, incident reporting mechanisms are becoming more standardized and structured to facilitate clearer communication and coordination during and after security events. [19], introduced an Agnostic Incident Reporting (AIR) framework tailored to operational technology (OT) environments, defining a set of 25 essential data fields that cover context, chronology, impact, and response. This structured reporting format helps capture the complete picture of an incident, from technical causes to managerial decisions, enabling consistent communication across stakeholders. Standardized incident reporting frameworks foster interoperability between different systems and organizations, making it easier to share actionable insights and

lessons learned. They also provide a reliable foundation for post-incident analysis, regulatory compliance, and automation of follow-up tasks. Frameworks like AIR reduce ambiguity and ensure that no critical information is omitted during the pressure of responding to a crisis. By harmonizing how incidents are reported, organizations can better coordinate cross-functional response teams, including IT, legal, and executive management. Such mechanisms enhance situational awareness and support continuous improvement of cybersecurity processes.

### **Automation and Workflow Management in Cybersecurity**

Automation and workflow management within cybersecurity refer to the systematic use of computer-driven processes to execute tasks that would otherwise require manual effort, thereby improving efficiency, consistency, and speed. In the context of security operations, automation helps streamline repetitive tasks such as alert triage, log aggregation, and incident ticket creation, enabling analysts to focus on more complex issues. According to [20], the integration of artificial intelligence (AI) into Security Orchestration, Automation, and Response (SOAR) systems can significantly enhance the responsiveness and resilience of Security Operations Centers (SOCs). They argue that AI-powered SOAR platforms can not only reduce human error but also improve situational understanding by analyzing threat data more precisely. The management of workflows through orchestration ensures that response sequences from detection to containment and recovery are executed in a repeatable and auditable manner. This level of structure allows security teams to codify response procedures into playbooks, reducing reliance on ad hoc decision-making. As a result, organizations can standardize incident response processes and enforce policy compliance more effectively.

### **Challenges in Traditional Incident Response Processes**

- i. **Time delays in detection and response:** Manual analysis of logs and alerts significantly slows down the detection-to-mitigation cycle [21].
- ii. **Human error and inconsistency:** Dependence on human judgment leads to inconsistent responses and potential oversight under pressure [22].
- iii. **Alert fatigue:** High volumes of security alerts overwhelm analysts, reducing their ability to prioritize and act on genuine threats [23].
- iv. **Poor coordination and communication:** Siloed teams and fragmented communication channels delay decision-making and coordination during incidents [24].
- v. **Resource constraints:** Insufficient staffing, especially skilled incident responders, hampers the ability to respond effectively [25].
- vi. **Compliance and audit challenges:** Manual reporting often fails to produce reliable, time-stamped logs, complicating regulatory compliance and post-incident review [26].

### **Benefits of Centralized Incident Management Systems**

- i. **Improved visibility and transparency:** A centralized system consolidates all incident data into one platform, enabling security teams to monitor incident status, severity, and progression in real time [27].
- ii. **Enhanced collaboration and communication:** With shared access to incident data and workflows, different teams (e.g., IT, security, operations) coordinate more effectively and avoid silos [27].
- iii. **Faster response times:** Standardized workflows and automated routing within a centralized system help prioritize and address critical incidents quickly [27].
- iv. **Accountability and auditability:** All actions, updates, and decisions are logged centrally, providing a clear audit trail for post-incident review and compliance purposes [27].
- v. **Consistency in policy enforcement and compliance:** Centralized management allows unified application of security policies across environments and simplified compliance reporting [28].

### **Methodology**

This study adopted design science research approach to understand current incident response procedures and identify areas of improvements. Callgoose was used as a tool to collect data from cloud-based platforms and aggregate the data collected with analysis based on Mean Time to Detection (MTTD) and Mean Time to Remediation (MTTR) as performance metrics. The new system was developed Python and the database is MySQL. The development involves the use of unique identifiers that includes Serial Number and Incident ID, administrative information like the Admin IPAddress, and descriptive details including Incident Type and Incident Description, Severity Level, Reported By and affected system details (Affected Host and Affected IPAddress). Other additional inputs includes Status, Assigned To, Actions Taken, Resolution Summary, Closure Date, and Detection Date and Time were added to provide contextual and temporal information, allowing the system to track incident progress, response effectiveness, and closure timelines. Random supervised learning algorithm was used to handle imbalanced datasets and provide features that were important for alert prioritization. To analyze the system comprehensively, there was systematic examination of all incident-related data captured by the system. The analysis ensures that data is complete, accurate, and structured, forming the basis for prioritization, reporting, and decision-making within the incident management process.

### **Findings**

After the implementation of the new system, the following were observed:

1. The new system achieved 85% accuracy, prioritizing critical alerts effectively.
2. There is reduced Mean Time Detection (MTTD), by 40% and Mean Time to Remediation (MTTTR) by 30%
3. There was anomaly detection of 90% unusual patterns which improved incident response.
4. There was effective alert triage and noise reduction as the machine learning-driven triage can filter out massive daily alert volumes - often reducing over 1,000 daily alerts to just a handful of actionable incidents. Automated systems have been shown to reduce the volume of alerts requiring human review by nearly 90% while doubling the accuracy of escalated alerts.
5. There was enhanced detection accuracy as system excel at identifying zero-day exploits and subtle anomalies that traditional signature-based systems miss by establishing baselines.
6. There was automated containment and remediation as the platforms can instantly isolate compromised endpoints, block malicious IPs, or revoke credentials, significantly limiting a threat's impact before a human analyst intervenes.

#### Discussion

The implementation of a cloud-based incident response platform using machine learning alert triage and automation yielded promising results. The findings indicate that machine learning models effectively prioritize critical alerts reducing incident response times. The system was able to handle imbalanced datasets and high dimensional data. The automation virtually reduces Mean Time to Detect (MTTD) and significantly reduces Mean Time to Respond (MTTR) by continuously monitoring vast telemetry data that would overwhelm human analysts. Unlike manual processes, the new automated platform provide comprehensive alert coverage, ensuring every signal is evaluated against standardized playbooks regardless of alert volume or cloud complexity. There is an adaptive resilience as the system facilitate continuous improvement by learning from historical incident data, which allows the platform to predict emerging threat patterns and refine detection accuracy over time. By offloading routine triage, security teams can transition from repetitive tasks to strategic threat hunting and high-level decision-making, thereby reducing staff burnout and improving overall job satisfaction.

#### Conclusion

This research demonstrates the effectiveness of a cloud-based incident response platform leveraging machine learning for alert triage and automation. By prioritizing critical alerts and automating response workflows, the platform reduced Mean Time to Detection (MTTD) by 40% and Mean Time to Remediation (MTTR) by 30%. The findings highlight the importance of data quality, real-time processing and model interpretability for successful implementation. The integration of a cloud-based incident response platform with machine learning (ML) alert triage and automation marks a paradigm shift from reactive to proactive cybersecurity. By leveraging machine learning, organizations can reduce manual investigation time and lower false positive rates. This shift addresses the critical challenges of alert fatigue and the human speed bottleneck, ensuring that high-stakes threats are prioritized and mitigated in seconds.

#### References

1. Aminu, M., & Zhang, L. (2022). Automation-driven incident response in modern enterprises. *International Journal of Information Security Research*, 10(3), 118–130.
2. Oladimeji, A., & Khan, R. (2023). Centralized platforms for organizational cyber incident management. *African Journal of Information Systems*, 8(2), 55–70.
3. Williams L. *From Reaction to Recovery: An Examination of Cybersecurity Incident Response* (Master's thesis, University of Missouri-Columbia).
4. Chen, Y., & Udoh, P. (2024). Machine learning applications in automated incident response systems. *Computing and Security Review*, 9(2), 75–89.
5. Okoro, C., & Mensah, J. (2023). Challenges in cybersecurity documentation and knowledge preservation. *Information Systems Review*, 11(1), 33–47.
6. Rahman A, Sultana S, Lima RJ. Strategic Framework for Enterprise Cybersecurity Management: Integrating Intelligent Anomaly Detection for Proactive Threat Mitigation. *Journal of Computer Science and Technology Studies*. 2026 Feb 15;8(4):58-70.
7. Adeyemi, T., & Choi, S. (2024). Enhancing situational awareness through integrated incident dashboards. *Journal of Cybersecurity Management*, 12(1), 44–57.
8. Ezekiel, K., & Morgan, D. (2023). Regulatory compliance and digital incident reporting frameworks. *Journal of Digital Policy and Governance*, 15(4), 210–225.
9. Ogenyi FC, Ugwu CN, Ugwu OP. Securing the future: AI-driven cybersecurity in the age of autonomous IoT. *Frontiers in the Internet of Things*. 2025 Sep 4;4:1658273.
10. Singh IP, Ahmad MM, Sani BS. CYBERSECURITY IN AGRICULTURE: SAFEGUARDING SMART FARMS.
11. Ojo, C., Osoko, E. A., Okolo, J. N., & Jaji, M. (2024). Incident response: A structured model from detection to containment and recovery. *World Journal of Advanced Research and Reviews*, 24(1), 1401–1407.

12. Gulay A, Maglaras L. Alignment of cybersecurity incident prioritisation with incident response management maturity capabilities. arXiv preprint arXiv:2410.02259. 2024 Oct 3.
13. TEITLER K, KUZNETCOV A. Incident Response Automation Through IRP Implementation. ISACA Journal. 2023 Sep 1(5).
14. Nanda AS. Technology advantage in finance: Revolutionizing the rise of IT-enabled financial services in the digital age. International Journal of Computer Science and Information Technology Research. 2025 Feb 14;6(1):62-71.
15. Chunawala, H., & Chunawala, P. (2025). The role of artificial intelligence in automating incident response in cloud-based cybersecurity. *Journal of Operating Systems Development & Trends*, 12(01), 15–24.
16. Gautam, P. (2025). The integration of AI technologies in automating cyber defense mechanisms for cloud services. *Journal of Operating Systems Development & Trends*, 12(01), 1–14.
17. Syed AT, Ghanem MC, Benkhelifa E, Abro FI. SPECTRE: A Hybrid System for an Adaptive and Optimised Cyber Threats Detection, Response and Investigation in Volatile Memory. arXiv preprint arXiv:2501.03898. 2025 Jan 7.
18. Alhousseini MM, Feizi-Derakhshi MR. Benchmarking ChatGPT and DeepSeek in April 2025: A Novel Dual Perspective Sentiment Analysis Using Lexicon-Based and Deep Learning Approaches. arXiv preprint arXiv:2509.19346. 2025 Sep 16.
19. Vidal N, Moradpoor N, Maglaras L. Everyone Needs AIR: An Agnostic Incident Reporting Framework for Cybersecurity in Operational Technology. arXiv preprint arXiv:2510.20858. 2025 Oct 22.
20. Gustina, V. A., & Ananda, A. (2024). Artificial intelligence for security orchestration, automation and response: A scope overview. *Jurnal Komputer Terapan*, 10(1), 45–58.
21. Ndubuisi, A. F. (2025). *Cybersecurity incident response and crisis management in the United States*. *International Journal of Computer Applications Technology and Research*, 14(1), 79–92.
22. Prasad, N. (2025). A survey of cyber threat attribution: Challenges, techniques, and opportunities. *Digital Investigation*, 25(1), 101435.
23. Suhail S, Iqbal M, McLaughlin K, Lee B, Imtiaz B. A Framework for Applying Digital Twins to Support Incident Response. In *European Symposium on Research in Computer Security 2024* Sep 16 (pp. 474-493). Cham: Springer Nature Switzerland.
24. Loumachi, F. Y. (2025). Advancing cyber incident timeline analysis through scalable big-data approaches. *Computers*, 14(2), 67.
25. Aldabjan, A. (2024). Cybersecurity incident response readiness: A study of organizational practices. *Proceedings of the 18th International Conference on Enterprise Information Systems*, 4(1), 245–255.
26. Vassiliadis P, Stienon E, Windel F, Wessel MJ, Beanato E, Hummel FC. Safety, tolerability and blinding efficiency of non-invasive deep transcranial temporal interference stimulation: first experience from more than 250 sessions. *Journal of Neural Engineering*. 2024 Apr 1;21(2):024001.
27. Bianchini C, Bargioni S, di San Girolamo CC. Wikidata and SBN: An Assessment of Two Years of Work (2023–2025). *JLIS. it*. 2026 Jan 15;17(1):73-96.
28. Gomez, A., & Lee, J. (2025). *Centralized security control: How unified tools simplify policy management across multi-cloud platforms*. ResearchGate.

**Table 1: Field Name, Data type and Description**

<b>Field Name</b>	<b>Data Type</b>	<b>Description</b>
Serial Number	Integer	Unique ID for each incident (Primary Key).
IncidentID	Integer	Unique ID for each incident.
Admin IPAddress	Text	Admin IP address of the system.
Incident Type	Text	Type/category of the incident (e.g., Malware, Phishing, Trafficking, Data Breach).
Incident Description	Text	Brief explanation of what happened.
Severity Level	Text	Level of seriousness (Low, Medium, High, Critical).
Reported By	Text	Person or system that reported the incident.
Affected Host	Text	Name of affected device or location.
Affected IPAddress	Text	IP address of the affected system.
Status	Text	Current state (Open, Investigating, Resolved, Closed).
Assigned To	Text	Responder or team handling the incident.
Actions Taken	Text	Steps taken to address the incident.
Resolution Summary	Text	Summary of final resolution.
Closure Date	Date/Time	When the incident was closed.
Detection Date Time	Date/Time	When the incident was first detected.

### APPENDIX I

#### LOGIN



#### MAIN PORTAL



#### INCIDENT RESPONSE PLATFORMPAGE

INCIDENT\_RESPONSE\_PLATFORM\_RECORD

**INCIDENT RESPONSE PLATFORM SYSTEM**

ENTER THE INCIDENT ID NUMBER:  SEARCH 1 of 5

S/N	INCIDENT_ID	ADMIN_IPADDRE:	INCIDENT_TYPE	INCIDENT_DESCF	SEVERITY_LEVEL	REPORTED_BY
1	IRP/1/0001	10.129.180.61	DATA BREACH	DATA BREACH I...	MEDIUM	UDEH CHUKWU
2	IRP/1/0002					
3	IRP/1/0003					
4	IRP/1/0004					
5	IRP/1/0005					

**CITE AS: Nwosu John Nwachukwu (2026). A Cloud-Based Incident Response Platform using Machine Learning Alert Triage and Automation. INOSR Scientific Research 13(1):12-20. <https://doi.org/10.59298/INOSRSR/2026/122011>**