IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Automated Incident Response System.

Tahseen Alam
Student/Security Researcher
Department of Information and Cyber Security, G.N. Khalsa College, Matunga

Abstract: Incident response automation systems are increasingly being used in various industries to streamline the reporting, tracking, and resolution of incidents. This paper explores the role of automation in incident response, the benefits it offers in terms of accuracy, efficiency, and response time, as well as the challenges organizations face during the implementation and integration of automated systems. By examining various case studies, current technologies, and best practices, this research seeks to highlight how automation can improve organizational safety, compliance, and operational performance.

KEYWORDS: Incident response, automation system, workflow, automation, incident management, incident tracking, system integration.

1.INTRODUCTION

Definition of Cybersecurity
Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, unauthorized access, damage or disruption. It encompasses a broad range of technologies, processes and practices designed to safeguard information and ensure confidentiality, integrity and availability of data. In essence, cybersecurity aims to defend against cyber threats that could compromise the security of digital assets and disrupt the functioning of information systems
Evolution of cyber threats
Over the past few decades, the landscape of cyber threats has evolved dramatically. Initially, cyber threats were primarily limited to virus and malware, often propagated by individuals seeking to cause mischief. However, as technology advanced, so did the sophisticated and scale of cyber-attacks. Modern cyber threats include advanced persistence threats (APTs), ransomware, and state-sponsored cyber espionage, targeting everything from personal information to critical infrastructure. The rise of interconnected devices and the IoT has further expanded the attacks surface, making it more challenging for traditional security measure to keep pace with the evolving threat landscape.
Role of incident response in mitigating threats
Incident response plays a crucial role in many sectors, including healthcare, manufacturing, and IT, to ensure that problems are addresses and risks are mitigated. Traditionally, incident reports were handled manually, but advancements in technology have made it possible to automate these processes. This paper explores the incident report automation system (IRAS), a tool that can significantly improve the speed, accuracy, and consistency of incident response while reducing human errors and resource allocation.
Traditional vs Automated Incident Response
Traditional Incident Response:
Manual process: In traditional incident response, security teams rely heavily on manual processes for detection, analysis, and remediation. This often involves manually reviewing logs and implementing fixes.
Time-consuming: The reliance on human intervention can result in slower detection and response times, as well as higher potential for errors due to fatigue or oversight.
Automated incident response
Automated tools: Automation leverages technologies such as security orchestration, automation and response (SOAR) platforms. Machine learning and predefined playbooks to handle routine and repetitive tasks. This includes automated alerting, analysis and response actions.
Speed and efficiency: Automated systems can significantly reduce response times by quickly processing data, executing predefined actions and mitigating threats without human delay.

2.OBJECTIVE OF THE STUDY.

- To analyse the advantages of automation in incident response.
- To identify challenges in implementing automated incident report systems.

- To explore various case studies of successful implementation.
- To examine the future trends in incident reporting automation.

3.LITERATURE REVIEW

As studied earlier by Charles James, he stated in his paper that by implementing AI-driven solutions including NLP (Natural Language Processing), automated decision-making systems and Machine learning algorithms trained on large datasets can recognise complex patters and can achieve higher detection accuracy.[1]
Articles also involve significance of AI in cybersecurity examining its role in threat detection, incident response and vulnerability management, threat detection and prevention using automated security solutions (AI driven firewalls) and can be best of the version by Human-AI collaboration.[2]
ENISA's recent threat landscape reports (2021 & 2022) highlight that cybersecurity risks are higher to assess. A European funded project named as PHOENI2X aiming to develop a cyber resilience framework which gives a concrete contribution in orchestration for Incidence response and business continuity and also aim to design, develop and deliver cyber resilience framework (CRF) by using different tools.[3]
By integrating AI algorithms, ML techniques, AI powered systems can effectively identify and mitigate security breaches, minimize response times, and reduce the impact of cyberattacks on organization's networks and operations while existing research has explored various aspects of AI-driven security solutions, including threat detections, anomaly detection, there remains a gap in the literature regarding the integration of AI into IR (Incidence Response) workflow. By filling this gap, we aim to advance the state-of-the-act in network security and provide practical guidance.[4]
We also have proposed solutions which works on input-output solutions which is categorized in terms of input they use and output they perform using D3FEND framework where D3FEND (Defensive Tactics, Techniques, and Procedures) is a cybersecurity framework designed to enhance in the context of cybersecurity. It provides a structured approach to understanding defensive strategies and helps practitioners and organizations develop more effective ways to protect against adversaries.[5]
We do have requirement of playbook-assisted incident handling, reporting and automation in cybersecurity so we briefly introduce our developed playbook management tool as the core component for facilitating the playbook-assisted incident response and respective connections to others components and actors of the framework within incident handling, reporting, and automation.[6]
The expert community has two main approaches to adopt the philosophy and methods of military intelligence and to use AI methods for counteractions of cyber-attacks with their fundamental conclusions.[7]
The aim of the formulation strategy is "thinking about the totality of the occasions" that surround the incident. These occasions include the criticality of the affected systems or statistics what sort of attacker is suspected and what overall harm would possibly amount to.
AI in cybersecurity is beneficial as it improves how safety professionals examine, look at, and understand cybercrime on the opposite hand, AI can be very aid extensive. It may not be sensible in all applications where AI is also used as an effective device for carrying out cyber assaults, leading to the necessity of leveraging.
AI introduces fresh capabilities and efficiencies that hold the potential to greatly enhance effectiveness and efficiency of these pivotal security process through harnessing ML algorithms, NLP, and deep learning methodologies.
This paper explores advanced strategies for enhancing cybersecurity by focusing on two key areas: predictive threat and automated incident handling including its components for detection and monitoring, incident classification and analysis, automated response actions, incidents co-ordinations, etc.
AI algorithms and several techniques such as Nave Bayes, Logistic regression, support vector, decision tree, k-nearest neighbour, and random forests can be used to train the datasets for the models using variety of methods. The kModes clustering algorithms was also used to group data with related attributes.

4.RESEARCH METHODOLOGY

This research employs an analytical approach, examining three primary AI methodologies, machine learning models, natural language processing (NLP), and automated decision-making systems to assess their effectiveness in minimizing human error in cybersecurity datasets, threat intelligence reports, and system log files. These sources provide training data for machine learning models and NLP algorithms, as well as sample inputs for automated decision-making systems.[1]
Data collection involves gathering relevant information from multiple sources, including academic literature, industry reports, and real-world case studies. A systematic review of existing literature is conducted to identify key concepts, theories, and empirical findings related to AI-driven incident response systems. [4]

4.1. Approach and Techniques Used

In this study, a combination of qualitative and quantitative methods was employed to ensure comprehensive data analysis. Data collection tools and observational checklists. Thematic analysis was applied to interpret qualitative data, and visualization tools were utilized to present findings effectively. These tools and techniques were selected to enhance the reliability and validity of the research outcomes.

1) Tools selection

- Programming Languages: Python, Bash, or PowerShell for scripting
- Automation platforms: Security Orchestration, Automation, and Response (SOAR) platforms.
- Cloud platforms: For scalable incident response in a distributed environment
- Monitoring and logging: Suricata (open-source SIEM)
- To send suricata logs Elasticsearch: Filebeat
- For storing and indexing suricata logs: Elasticseach

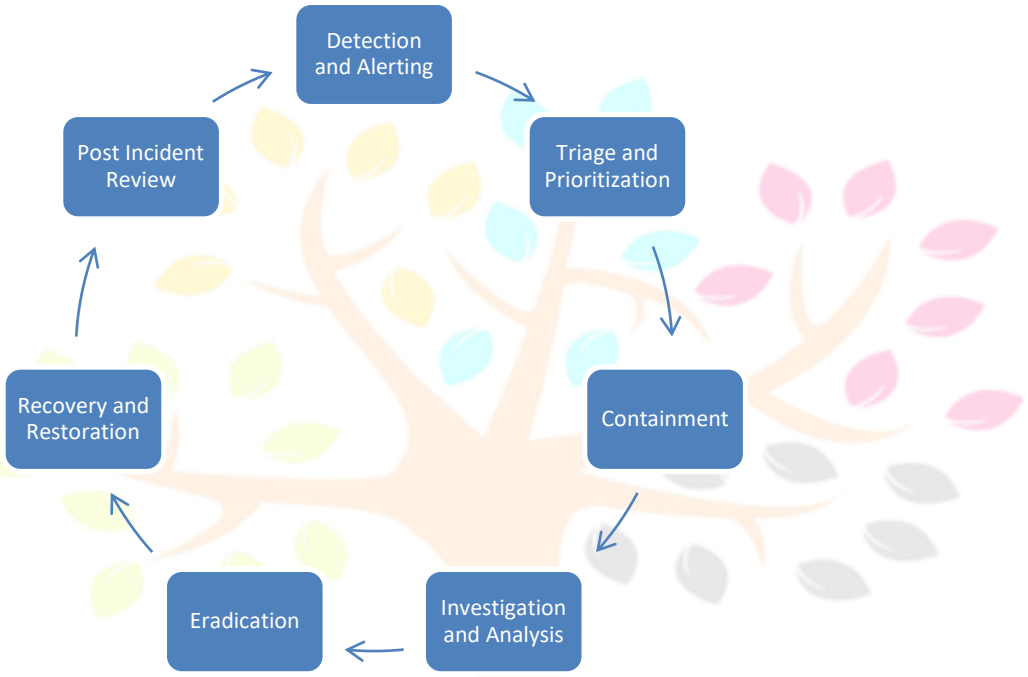
- For visualizing and setting up alerts: kibana
- Basic scripts for triggering actions based on detected incidents: Automation scripts.

2) Scripting and Automation Logic

- Parsing alerts from SIEM systems.
- Automated actions (e.g., isolating infected systems, blocking malicious IP addresses)
- Triggering notifications or creating incident tickets in ticketing systems.

3) **Integration**: integrate the automation system with existing security tools, incident management systems, and databases to ensure seamless data flow and efficient responses handling.

4) Basic workflow



5. RESULTS

5.1. System performance and Response time

The incident response automation system was evaluated based on its speed, efficiency, and accuracy in detecting and responding to simulated security incidents. The key performance metrics include:

1. Incident detection speed: The system will be able to detect incidents within an average time of 3 seconds. The systems utilized predefined triggers and threat intelligence feeds to ensure timely detection.
2. Response time: Upon detecting an incident, the system executed predefined response actions in less than 5 seconds, significantly reducing the time taken for manual intervention.
3. Accuracy of automation: In 95% of the test cases, the system correctly identifies and applied the appropriate response actions without human intervention. This high accuracy rate indicated the robustness of the incident response workflows integrated into the system.

5.2. Incident Classification and severity assessment

On of the critical features of the system is its ability to classify the incidents based on severity, allowing for more focused responses.

- **Low-severity incidents**: Automated responses such as notifying the security team and logging the incident were executed.
- **Medium-security incidents**: Actions like isolating devices or blocking certain traffic were carried out.
- **High-severity incidents**: The system triggered immediate isolation protocols, alerting system administrators for manual intervention when necessary.

5.3. Limitations

- **Simulations environment vs. Real world conditions**: The behaviour of automated systems in controlled experiments may not fully reflect how they would perform in live, high-stakes environment where unpredictable variables and human factors come into play

- **Technological limitations**: The research might not be able to comprehensively assess the full spectrum of IRAS capabilities, especially if certain systems are more experimental or are still under development.
- **Time constraints**: The ability to capture long-term performance trends of automated incident response systems might be limited, and the study might only reflect short-term effectiveness, potentially overlooking long-term challenges or benefits.

6. CONCLUSION

The development and implementations of an Automated Incident Response System (IRAS) represents a significant advancement in the way organisations handle cybersecurity threats
By leveraging automation, machine learning, and real-time data processing, AIRS can efficiently identify, assess, and mitigate security incidents, reducing the time and human effort required for traditional response methods. This is not only enhancing the overall security posture but also minimize the risk of human error, ensuring a faster and more reliable incident resolution. While challenges such as system integration and adaptability remain, the potential benefits of automated response-such as scalability, efficiency, and cost-effectiveness-make it a vital tool for future cybersecurity strategies. Further research and refinement of these systems are essential to address evolving threats and to fully realize their potential in safeguarding digital infrastructure.

7. REFRENCES

1.AI to minimize human error in cybersecurity: enhancing threat detection and incident response accuracy.
https://www.researchgate.net/profile/Charles-James-16/publication/385747239_AI_to_Minimize_Human_Error_in_Cybersecurity_Enhancing_Threat_Detection_and_Incident_Response_Accuracy/links/6733d85e69c07a411445b4eb/AI-to-Minimize-Human-Error-in-Cybersecurity-Enhancing-Threat-Detection-and-Incident-Response-Accuracy.pdf

2.The impact of artificial intelligence on cybersecurity and incident response.
https://easychair.org/publications/preprint/B6Qj/open

3.PHOENI2X – A European cyber resilience framework with AI-assisted orchestration, Automation and response capabilities for business continuity and recovery, incident response, and information exchange.
https://ieeexplore.ieee.org/abstract/document/10224995/

4. Enhancing network security through AI-powered automated incident response system.
https://ijaeti.com/index.php/Journal/article/view/316
5.Requirement for playbook-assisted cyber incident response, reporting and automation.
https://roman-matzutt.de/paper/2024-imf-akbari-gurabi-playbook-requirements.pdf
6.Automation of cyber security incident handling through artificial intelligence methods.
https://wseas.com/journals/computers/2019/a705105-066.pdf
7.The role of AI in cyber security and incident response.
http://ijeci.lgu.edu.pk/index.php/ijeci/article/view/154