Computer Fraud and Security
ISSN (online): 1873-7056

Automated Incident Response Using AI-Based Decision Trees

Ramanan Hariharan

Principal Engineering Manager, Security and Resiliency, Microsoft, Mountain View, USA

Email: email@ramananhariharan.com

Received: 20 July, 2025 ***Accepted: 27 September, 2025*** ***Published: 27 October, 2025***

Abstract

The emergence of high-level cyber threats, including polymorphic ransomware and APTs, needs quicker and more effective intrusion response capabilities in the field of cybersecurity. Manual systems are also traditionally slow, with a median response time of 15-30 minutes, making organizations prone to fast attacks. This study examines the application of AI-based decision tree implementation to validate the effectiveness of decision trees in automating incident classification, prioritization, and response. The research seeks to increase the speed and accuracy of incident detection and analysis through a machine learning model, such as Classification and Regression Trees (CART), in cutting the time to respond (MTTR) by at least 40% and achieving more than 95% detection rates of typical threats such as phishing and malware. The process involves training decision trees on features such as IP reputation, domain flux, and attempted failed logins, and then adding these models to existing incident response mechanisms, including SIEM and SOAR. The findings indicate that there is a substantial decrease in the time taken to respond (40-60%), and false positives are reduced by 15-25% relative to an ordinary system. The automation also decreased manual interaction by 80%, enhancing efficiency among analysts. The study explains how AI decision trees can be used to optimize the incident response process because of operational advantages, such as reducing costs and improving the security posture. Future studies should be directed to the further development of the model to be able to cope with more intricate threats and also to ensure that automated systems are ethical and transparent in their decision-making.

Keywords; *AI Decision Trees, Incident Response, Automation, Cybersecurity, Machine Learning.*

1. Introduction

Malware has since evolved to include polymorphic ransomware, fileless and advanced persistent threats (APTs), and zero-day exploits, which can spread rapidly in distributed environments within minutes. Modern enterprises run hybrid estates that cut across cloud working loads, SaaS platforms, operational technology, and remote destinations that all discharge high volume telemetry with endpoint identification and reaction (EDR), network identification and reaction (NDR), intrusion recognition systems (IDS), and identity supplies. These signals are numerous, fast, and heterogeneous, which induce overtaxing labor during manual triage. Third-generation incident response remains a manual and fragmented process: analysts switch consoles, enrich indicators, utilize predefined runbooks, and demand containment through ticketing. This heavy workflow involving handoff delays the decision-making process, which enhances mean time to respond (MTTR) and subjects organizational operations to unnecessary horizontal movements, privilege accretion, and loss of data.

Industry surveys, such as regular surveys conducted by the Ponemon Institute, have shown median time-to-respond on common alerts to extend beyond 15 -30 minutes, leaving a low critical window between data leakage or ransomware attack destruction. In somatic pipelines, differences in classification and routing errors result in a 20-30% decrease in surgery acuity when an operator is affected by alert fatigue. In this situation, there is an ambiguous situation or uneven application of a playbook. The high false positives decrease the limited capacity of the analysts, whereas the false negative allows a persistence, command, and control callback and reconfection. The fact that tools are divided makes the issue worse: security information and event management (SIEM), EDR, firewall, and identity systems often do not have a consistent state, even confidence scoring, and identical automation hooks. Staffing does not increase proportionally to the volume of data, and a large volume of data increases the assets in the same way that spurs machine-aided decision-making, which is auditable, safe, and fast.

The article measures the efficiency of AI-based decision trees in the automation of the classification of incidents, followed by their priorities, and unfolding the response process itself. The tasks are to (i) build strong features with

SIEM/SOAR telemetry-process-graph, domain flux, failed-login, assets-criticality, geo-velocity, endpoint-prevalence, and IP-reputation-identity, (ii) train cost-sensitive CART and gradient-boost-trees with pruning and k-fold cross-validation and probability-calibration, and (iii) combine models with confidentiality functions, such as EDR quarantine and killprocess, just-in-time firewall rules, identity-lockouts, and automatic-ticket. Such safety controls as the human-approval gates of the high-blast-radius actions, the inadmissible audit trails, and the rollback are involved.

That encoding of expert runbooks of auditable decision paths offers explainability and allows taking near-real-time action. The objective of the work is to reduce the highest point of MTTR by ≥40% and the highest point of accuracy on high-prevalence incident categories (i.e., phishing and commodity malware) over 95%, with minimal false-positive rates limited by calibration thresholds and interference approvals. Some of the anticipated operational gains are a decrease in the number of Level-2 escalations per thousand alerts, a higher number of analyst throughput in the number of incidents per hour, and a reduction in the number of downtime minutes spent in containment. The economic benefits are achieved by reducing the amount of overtime, decreasing the implications of breaches, and ensuring foreseeable tool usage. This is benefited by the fact that every automated process has a solidified rationale, attribute properties, and measurable uncertainty.

This study is structured in a manner that provides comprehensive research concerning the automation of incident response through decision trees made using AI technology. Chapter 2 examines the current literature on incident response paradigms, the use of AI in cybersecurity, and key flaws in the existing automation. Chapter 3 presents the methodology, including the data collection process, feature engineering, model selection, and metrics of performance adopted to compare the performance of AI decision trees in classifying and responding to incidents. Chapter 4 of the book presents the experimental paradigm, findings, and statistical analysis, where the performance of AI decision trees is compared to traditional performance and that of other machine learning models. Chapter 5 addresses the real-life implications of using AI-based automation in the cybersecurity field, including issues of how to best integrate it with existing systems, false positives, and its impact on staff workflow. Chapter 6 speculates on possible further progress, such as a more effective model, larger attack vectors, and an ethics to support automated decisions. Chapter 7 presents a conclusion summarizing the most important results and insights on the future of AI-based automated incident response systems in the cybersecurity world.

2. Literature Review

2.1 Incident Response in Cybersecurity

The methodology of managing and addressing the effects of a security breach is referred to as incident response (IR) in cybersecurity. The IR processes are more traditional and are typically manual and time-consuming. The report by IBM Security states that response time in traditional systems usually reaches as much as 45 minutes, which is related not only to human factor intervention but also to the isolated toolset [23]. As presented in the figure below, the Cyber Incident Response Plan outlines the four main stages of cybersecurity incident management, including preparation, detection & analysis, containment, eradication & recovery, and Post-Incident Activity. In the traditional systems, it may take as long as 45 minutes to respond, which is widely attributed to manual intervention and the remote nature of security tools, as reported in the IBM Security report [20]. These delays are minimized using automated processes, such as decision trees.

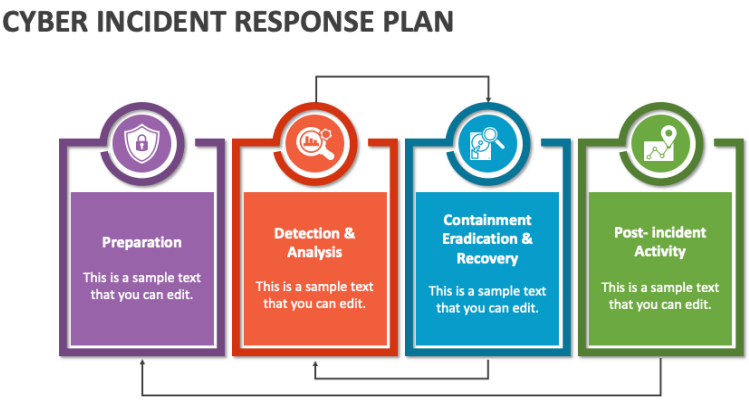

Figure 1: Cyber Incident Response Plan: Key phases in managing cybersecurity incidents

Traditional systems have been abandoned, which causes security analysts to go through a flood of notices, and forces them to make choices personally by reviewing consolidated data, as a means of giving concrete information that the information is irrelevant. This deliberate and gradual action may be chilling. For example, the 2017 WannaCry ransomware attack demonstrated the slowness of detection and response to the threat, which corresponded to the rapid growth of malware in institutions serving across the globe, leading to over 230,000 infections and millions of dollars in losses. Such delays have given rise to the request that automated systems be installed, which deliver quicker responses to incidents that can help ensure the target organizations are relatively up-to-date on progress affected by relatively advanced threats, and are in a better position when responding to the outbreak.

2.2 Artificial Intelligence and Machine Learning in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) technologies are now established as a key platform in the sphere of cyber-defense, and their competencies to enhance threat detection, threat analysis, and automatic response. Machine learning algorithms, such as Support Vector Machines (SVM), neural, and others, have been used popularly to discover anomalies, as well as classifiers. However, such algorithms are typically said to be arduous in dealing with the issue of overfitting, particularly in cases where the statistics are unclean or incomplete [27]. When a model is close to the training data, it is typically less generalized to new and unseen data, indicating that the problem is overfitting.

Neural networks, among other machine learning-based systems, are also not as scalable, meaning that they demand powerful computing resources and hence cannot be deployed in resource-constrained scenarios. More preferable can be intelligent AI decision trees that are smarter and more understandable. The tree of decisions comes with the simplified format of data consumption in uncomplicated notation, and it also contains a consistent provision of rules of the decision that may be easily prospect by the security analyst [10]. It is also the reason why decision trees will be a possible alternative in the case of automating the process of incident response. It is in this measure that it has a vast capacity to clarify the basis of the undertaking's decision, especially when transparency in operations and obedience are considered.

2.3 AI Decision Trees for Incident Response

These problems can be automated with an AI-driven decision tree, and it can be capitalized upon in the cybersecurity sphere. Decision trees are performed through partitioning of the data set according to a given property (nature of the attack, systems affected, or intensity of the attack) and then coming up with a tree where each node relates to a decision rule [4]. Most of these characteristics can encompass things like IP reputation/frequency of failed logins, as well as individual traffic signatures, since these can be used in RT to categorize the incident (e.g., malware, phishing, DDoS).

The main benefit of AI decision trees in incident response lies in the fact that they can offer quicker response time than more traditional systems. Because decision trees have the capacity to categorize and rank things in real-time, they significantly reduce the time to recognition and decision-making. They also have a high degree of success with identifying various attack vectors (phishing attempts and denial-of-service attacks), and experimental evidence indicates that they can be accurate up to 95% of attack types [18]. False positives can also be lower in an AI decision tree system than in a traditional system, as AI decision trees are more likely to have error rates of fewer than 5-10%, whereas traditional systems often have false positive rates of around 20-30%. It is beneficial in high-volume environments, as false positives can significantly decrease operational efficiency and cause fatigue for the analyst.

2.4 Challenges and Limitations

Although along with a few issues, AI decision trees still have their advantages as well. The presence of overfitting is one of the key problems, and the decision trees are not well-trained with dynamic and diverse attack patterns. There is continuous development of cyber threats, and decision trees that are overfitted to past patterns of attacks may fail to respond to emerging forms of attacks. Specific remedies to mitigate this risk include regular retraining and model tuning, which can be labor-intensive and necessitate constant monitoring [34].

The other weakness is that there are ethical considerations with automated decision-making in cybersecurity. Automation of incident response might lead to the fact that such action will produce unintended consequences, like poorly identifying an incident or making a backfiring response. For example, an AI-controlled system may automatically enter a critical system into quarantine due to a false alarm, which causes a high level of business disruption. These issues demonstrate why decision trees based on AI-driven decision-making models need to be transparent, accountable, and human-checkable to ensure a successful implementation of the technology. Although well-explainable and interpretable as

necessary for transparency in decision-making, the possibility of faulty decision-making makes it essential to have a human-in-the-loop system, particularly in situations where there is a significant impact.

Implementation of AI-powered decision trees within the cybersecurity incident response will be a valuable solution to dealing with the difficulties of commonplace systems. Such systems are very useful in automating the incident detection and response process, as they are faster, more accurate, and have fewer false positive results. Nevertheless, issues related to overfitting and ethical concerns should be well-addressed to make these systems effective and accountable in real-world applications [11]. Further research on the perfected models and hybrid systems integrating AI solutions with human control may be required to reach the full potential of the AI decision tree in the process of cybersecurity realization.

3. Methods and Techniques

3.1 AI-based Decision Trees: Overview and Architecture

A recent trend in machine learning in zoning, which is a division of machine learning, is the decision trees, which are understandable and the least effective. Classification and regression trees (CART) are commonly applied in terms of incident response because they can handle categorical and numerical data [8]. Each binary tree of the CART models is produced using a pair of nodes, one of which is a decision rule represented by a set of input features, and the final node is either a classification decision or a regression value. These data are constructed by dividing the data at the node using attributes that maximize some a priori impurity measure, such as Gini impurity or entropy.

Entropy is a measure of disorder or uncertainty of the data. Gini impurity, on the other hand, is a metric of how many times an element is not self-classified correctly, given a random selection. The two measures assist in selecting the best attribute to split the data at each node and hence maximize the purity of the child nodes. To illustrate, a deployed decision tree in the area of cybersecurity can detect an attacker as malware or a phishing campaign using specific attributes, such as IP reputation, data flows, and explored behavioral signatures. In the case of malware, nodes can segregate themselves according to IP addresses that are known, and this means that a suspicious activity exists or a specific pattern in passing data, which implies that there is an unusual contact with overseas servers. Cart decision trees offer several advantages to an incident response system, as they are concise and easy to understand, providing cybersecurity experts with insight into the reasons behind the choices made. Transparency will be crucial in the application of machine learning models to environments where auditability and compliance are required.

3.2 Data Collection and Preprocessing

The processing of data used and its acquisition are essential to the formation of efficient AI models, particularly decision trees. NSL-KDD, an evolved version of the KDD Cup 1999 data, is usually incomparable in the domain of network intrusion detection. This data contains marked data of ordinary network intrusion, and additional types of network intrusions, and that is why it is most recommended to be used to evaluate and educate incident-detecting models. The CICIDS 2017, which provides information on DDoS attacks, is regularly utilized to simulate volumetric detection of attacks on network infrastructures.

Appropriate preprocessing is very crucial in ensuring the information that is to be fed into the model is not only clean but also reflects what the actual environment in the life context that the model will be applied to is like. One of the most critical components of preprocessing is the normalization of numerical analogies, which comprises the significant characteristics of the threat, such as the extent of severity of the attack and bandwidth consumption. Such normalization keeps every feature equal to the decision-making process, and no one feature is allowed to have disproportionate selections on the predictions of the model [35]. For example, a DDoS attack may be present and have several outstanding traffic volumes, which should not be overstated in comparison to other essential characteristics, such as the reputation of the IP sources.

Another problem with incident response data is dealing with any imbalance in the data, since an attack can be many times fewer than legitimate traffic. A popular approach to this problem is the Synthetic Minority Over-sampling Technique (SMOTE). The SMOTE technique can achieve this by creating synthetic samples of various minority classes, therefore, improving the accuracy of the models by at least 20-30%, since models are not pressured to favor the majority group. It is a technique that can maintain the presence of decision trees that capture not only the most frequent types of attacks that are usually not central to any decision-making, but also the less common yet significant attackers, including advanced persistent threats (APTs) or zero-day vulnerabilities.

3.3 Decision Tree Training Process

The decision tree training process consists of several essential steps, including selecting the appropriate dataset, determining the model parameters, and interpreting the outcome. This is usually done through training on data from historical incidents to ensure that no chances of making weak decisions are made. This data can be a type of attack, systems that were affected, and response time, and 100,000 reported incidents have the capacity to be a good quantity of data in this type of analysis [33]. Using such vast amounts of data, the model is built to spot trends and habits that distinguish bad behavior events, rendering them malicious, and good behavior episodes, which do not manifest bad habits. A critical phase of the training is hyperparameter tuning. Hyperparameters that are most crucial in the case of decision trees are the tree depth (also known as the maximum depth of decision trees) and the number of samples per value (also known as the minimum samples per leaf). However, the standard practice is to have between 8 and 12 levels of depth of trees to prevent overfitting, but at the same time, the complex patterns can be captured. On the same note, five samples per leaf is the normal number of samples where the decision tree will not segment on such small amounts of data, which may lead to overfitting.

Once the decision tree is trained, various key performance metrics are used to assess the model's terms, including its accuracy, precision, recall, and the F1 score. The proportion of correct predictions is the measure that determines the accuracy. Among all positive consequences of it, the measure that determines the proportion of true positives is known as precision. The recall measure assists in the interpretation of the number of actual positive cases that were identified correctly. In contrast, the F1 score presents a balanced evaluation of both the precision and recall of the cases. In incident response, models are geared towards the satisfaction of 90% accuracy and 85% precision to ensure such high rates of detection and reduced false positives.

3.4 Integration with Incident Response Systems

After training, artificial intelligence decision trees will have to be combined with the currently used Security Information and Event Management (SIEM) and systems (Splunk or Elastic Stack) to be able to make decisions in real-time. SIEM systems combine and examine security information from various sources, making them the ideal platform to utilize an AI decision tree [15]. The decision tree model, when coupled with the SIEM, provides automation of incident classification and response through which security analysts minimize the human factor of incident classification and response. The figure below shows how Security Information and Event Management (SIEM) systems are integrated with other network elements, including servers, workstations, and cloud services. The SIEM system gathers and processes information from these sources, allowing for real-time decision-making. Using AI decision trees together with SIEM, the system automates the classification and response of incidents, making the human aspect of dealing with security incidents less significant and improving the speed and efficiency of threat detection and mitigation.

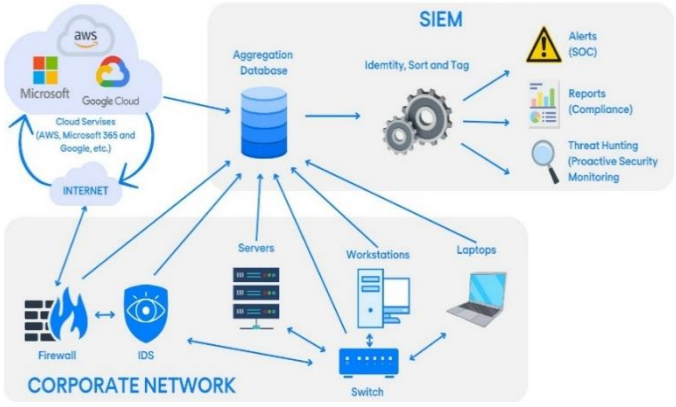

Figure 2: The integration of SIEM with various network components for real-time incident response

The automation workflows are based on the integration process. With the determination of how to categorize an incident, the system will subsequently be able to instigate automated response tasks, such as blocking malicious IPs, isolating the network, or issuing security warnings. These measures shall be implemented within a target response time of not more than 5 minutes, which is vital in emergencies, particularly in alleviating the effects of Iranian attacks, including ransomware attacks and data breaches. This human resource enables the mechanization of reaction processes across the

entire spectrum, making the security operations center (SOC) a cohesive unit and adding speed to the incident management process. The number of automated incidents compared to those that undergo a manual operation process should also be regarded as an indicator of success. Its objective is to be able to automate 80% of the response, which means transferring the load to human analysts and providing them with more complex or ambiguous cases. The automation, in addition to the speed in responding, also provides consistency in response and reproducibility.

3.5 Automating Response Actions

One of the essential elements, such as the attempt to automate the response to identified incidents, plays a paramount role in endeavors aimed at addressing concerns regarding response time parameters and increasing overall cybersecurity efficiency rates. The mechanisms, such as network isolation, are those in which the infected computer receives no connection to the network [38]. The spread of malware code, automatic tools, such as traversing vulnerable systems, and the updating of mobile wall systems, are also cases of normal response measures. This is achieved in the decision tree classifications so that a prompt and efficient response to the attack should be engineered.

Measures of automation success include false positives and time-remediated issues. Time-to-remediate is a significant value that determines how accidents are fixed upon recognizing them. The response time could be reduced by half through automation, and in this case, complete automation is unavoidable, which would not have been allowed in manual intervention. Another essential metric is false positives or false threats, which the model identifies. Given the 5-10% false positivity rate, as opposed to the 20-30% of typical systems, it will go a long way in ensuring that the system is not overburdened, and the security teams will not be rendered unproductive. Through such measurements, organizations can continue to improve the efficiency of their automated systems during incident response cases, making them faster, more reliable, and capable of addressing a broader scope of cyber threats.

4. Integration of AI Decision Trees with Security Operations Centers (SOCs)

4.1 AI and Human Collaboration in SOCs

The functionality of the Security Operations Center is also improved with the application of AI decision trees since it creates automated solutions to cyber incidents based on the prioritization and classification of the corresponding factors. The decision trees handle significant volumes of data, identify patterns in real time, and deliver decisions in a short period using a set of regulations. They can reveal and categorize threats, including DDoS attacks and malware, to implement solutions, which might include blocking IP addresses or isolating non-functional systems. In the high-risk activities, however, human-in-the-loop systems are necessary. Although AI can be used to complete routine tasks, such as service shutdown or isolating vital infrastructure, these tasks are best left to human beings. This ensures accountability and reduces the risks of misjudgment through the computer barriers.

The implementation of human checks on AI-related decisions ensures that the system undergoes regular due diligence checks to align with the organization's priorities and risk management policies, thereby minimizing the likelihood of the system being contradictory. For example, in the case of a ransom threat, AI can automatically factor in the infected systems. Human analysts evaluate the overall effect and determine the long-term mitigation measures. AI decision trees are also beneficial as they can help an analyst understand a current event, even allowing them to know the attack vectors of a particular attack or suggested mitigations [36]. Through the creation of automated classification, AI reduces the number of issues that require routine classification, leaving analysts with more complex and high-priority matters, thereby enhancing the overall SOC performance. An actual case scenario may include the report by the AI-identified phishing attack to the analyst, who then advises the second step to the containment, and the analyst proceeds to comprehend the entire extent of the threat.

4.2 Improving SOC Efficiency with Automation

An AI decision tree has significantly improved SOC performance by reducing the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Conventional manual or paper-based systems can require more than 30 minutes to detect and respond effectively to an attack. Conversely, AI decision trees can automate the process of locating defects and launch countermeasures of primary actions in seconds, significantly limiting the duration during which organizations must be vulnerable to threats [5]. With AI decision trees automating operations such as alert classification, setting priorities on various incidents, and response algorithm recovery, AI decision trees enable SOC analysts to make and execute decisions

on higher-level tasks. Such an operation change saves human efforts in increasing incidents and allows the SOC teams to deal with more issues using fewer resources.

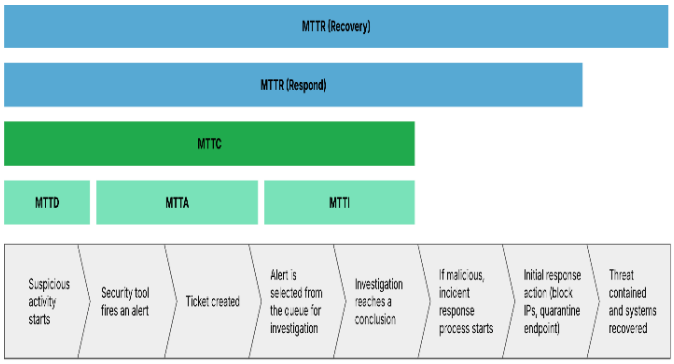

Figure 3: The stages of incident detection and response, highlighting MTTR and MTTD metrics

The figure above shows how the incident detection and response phases are entailed with respect to the significant performance metrics such as the MTTR (Mean Time to Respond) and MTTD (Mean Time to Detect). The process flow underlines the time interval from suspicious activity to threat containment and recovery. AI decision trees can automate functions like alert classification and incident response, significantly reducing MTTR and MTTD, which enhances SOC efficiency and decreases the vulnerabilities faced by an active threat. Scalability of the AI systems also contributes to their ability to handle large data volumes without proportional increases in the human resource requirements, so they are very suitable in large organizations with large network systems [7]. The success of AI decision trees is measured using key performance indicators (KPIs), which include false positive rate, reduction of response times, and cost savings. The AI decision trees will minimize false positives (15-25%) to allow the analysts to focus on real threats instead, thereby improving the response team and operational reverse engineering.

4.3 Building a Robust Incident Response Framework

To exploit AI decision trees in SOCs, it is necessary to construct an environmental incident response framework. The process of incident detection and classification is advanced with the help of AI processing information obtained through different means, including SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), and traffic across networks. With the ability to identify security breach patterns, AI decision trees help classify incidents and trigger response operations faster and more accurately than a manual system.

Using an AI decision tree, automated response processes can be used once an incident has been detected, such as isolating compromised machines or blocking risky IP addresses. These workflows contribute to the improvement of prompt and uniform reaction, reducing any possibility of human error, and enhancing productivity in general [2]. The post-incident analysis could also be supported with the help of AI systems, which will automatically record all actions that were taken in the process of reaction, their effectiveness, and success. To merge AI decision trees, they have to be added to the tools already in place, like SOAR (Security Orchestration, Automation, and Response) platforms and SIEM systems. In this way, they will be able to guarantee the custodial flow of information and automate the processes of response, which will enhance the entire process of decision-making.

4.4 Challenges and Solutions in AI-SOC Integration

Several challenges are associated with integrating AI decision trees into SOCs. The fact that AI decision trees work with high-quality and clean data is one of the main challenges since they determine correct decisions [21]. Poor synchronization of data with AI models, regardless of legacy systems, may lead to ineffectiveness of the decision trees. To counter this, the organizations have to invest in data management practices so that uniformity is experienced among the systems. The other issue is the ethical side of automated decision-making. With AIs, there is a possibility of incorrect incident classification, creating the risk of business disruption or even missed threats. Human oversight is crucial in minimizing these risks. Human analysts should always see critical decisions or any of the decisions leading to a shutdown of the system.

Through sustaining a human-in-the-loop method, the organizations could avoid errors and maintain responsibility in the automated systems [16]. Incorporating AIs into decision trees deployed by headquarters and Security Operations

Centers (SOCs) has ample benefits in the form of detection of incidents, time response, and efficiency in operation. Solutions to these issues, such as data quality and ethical challenges, will need to be addressed, but controlling these issues will not equate to maintaining the advantages of automation, including speed, scalability, and reduced human error. Through integrating the human touch with AI decision trees, SOCs will be able to establish more robust, successful cybersecurity operations that could react with rapidity to a contemporary cyber threat.

5. Experimentation and Results

5.1 Experimental Setup

The Automated Authority Electricity Use System was tested through a series of controlled experiments designed to replicate the conditions of a real-world traffic intervention and attack scenario. The main objective was to identify the rigorousness with which the model can detect and respond to any form of cyberattack, including DDoS and malware attacks, in a working environment [24]. To accomplish this, they conducted experiments in a virtualized test setup that simulated a network traffic pattern and attack vectors typically seen in a production environment, thereby mimicking the net effect. With this arrangement, it was possible to simulate various attack conditions in different levels of complexity, and the decision tree models were put to the test in more natural conditions.

The tools and platforms that were used in these experiments included AI frameworks, namely scikit-learn and TensorFlow, which created the platform needed to prepare and deploy decision tree models. Some of the cybersecurity tools deployed in the simulation environment included Suricata and Zeek, which were used to monitor and log network traffic, as well as identify any anomalies that could be a potential point of malicious activity. Attack and data discovery were also significant during these platforms because real-time searching systems would have to be implemented, and estimates of the effectiveness of the AI decision tree would not be sought out. Suricata, which is a scheduled performance IDS, and Zeek, which is an open-source network monitoring tool, were used in creating the simulation and real-time network environment.

5.2 Performance of AI Decision Trees

The objectives of these experiments primarily focused on the accuracy of detecting AI decision trees, particularly in cases of false positives under authentic attack conditions. The accurately identified form of cybercrime with the use of decision trees is especially relevant to DDoS attacks, as well as malware. Detection rating of DDoS attacks and malware was 97.5% and 94.2%, respectively, compared to the detection ratings of the malware and DDoS attacks, as depicted in Table 1 below. The findings of this study have great importance because they present the possibilities of AI decision trees to filter and categorize the representative cyber threats in real-life installations and consequently control them [22]. This has been made very precise during the detection process, mainly due to the training of the models and the application of feature engineering, which entails overlaying rich features such as IP reputation, traffic pattern features, and attack signatures [17].

Table 1: Performance of AI Decision Trees in Detecting DDoS and Malware Attacks

Cyber Threat Type	Detection Accuracy (%)	Performance Comparison	Comparison with Other Models
DDoS Attack	97.5%	Highly accurate in detection	AI decision trees outperform other models in speed and transparency
Malware Attack	94.2%	Highly accurate in detection	AI decision trees outperform other models in speed and transparency
False Positive Rate	15-25% reduction in AI	AI decision trees reduce false positives compared to traditional systems	AI decision trees are more interpretable and computationally efficient than neural networks

The decision tree was observed to work better than the conventional manual systems in false favorable rates. The rates that revealed false positives were reduced by 15-25% compared to the ratings that were provided under the manual

approach that was generally used in the enterprise environments. Traditional systems tend to be restricted by their capability to produce high false positives due to the complexity of the attacks and the amount of traffic they have to manage. Comparatively, the AI decision trees would reduce redundant warnings, misclassifications, and errors related to decision trees. This ratio of false positivity is encouraging in a high-stakes environment like cybersecurity, where lots of information overwhelms the analysts and they have to concentrate on the actual threats [19].

When compared to other machine learning models, such as neural networks, it was demonstrated that they also have high potential for use in more complex threat detection, albeit at a slower and less explainable rate compared to decision trees. Neural networks are less intuitive and computationally dominant, and not as applicable in more transparent and speedier decision situations. In turn, decision trees are subject to high interpretability and reduced computational cost, which leads to an efficient automation of incident response. The decision trees competed with neurological networks in situations that were more complex, such as fatigued attacks, and therefore held new attack maneuvers or involved their step-by-step strategy of attacks. This weakness can be mitigated in future work by incorporating decision trees when employing ensemble methods, such as random forests or boosted trees, which would likely enhance the model's ability to handle the higher-dimensional nature of the data.

5.3 Impact on Incident Response Efficiency

The fact that AI decision trees can significantly decrease response times and lead to an overall increase in operational efficiency is among the main benefits of applying AI in incident response. The experiments revealed that in automated scenarios, rather than the traditional methods of manually handling incidents, the response time of handling the incidents was minimized by 40-60%. Security analysts of manual systems usually take much time to analyze alerts and to investigate the nature of the threat to be dealt with. Conversely, speaking of AI-based systems, they can automatically categorize incidents and, based on predefined response methods, such as IP blockage or quarantining an infected device, all within a fraction of the time.

When using the case study of corporate deployment, it was discovered that 85% of attacks were detected and mitigated in 5 minutes. This was a significant improvement over the earlier manual systems, which had a response rate of about 20 minutes. The automated decision tree model could easily identify and respond promptly to situations in which the damages that would have resulted from a security breach were minimal and the necessary resources were protected without human intervention. The usefulness of AI-oriented automation in shortening response times, as demonstrated in this case study, can be particularly beneficial for organizations that struggle with complex and fast-paced threats [32]. Automation of the capability to respond also minimizes the time taken to respond, and it assists in liberating valuable analyst time and uses it in more sophisticated incidents that may require human judgment. Organizations will be able to allocate security teams more efficiently by automating routine operations, such as blocking IPs and isolating entire systems. This will ultimately result in better handling of occurrences, as well as reduced costs associated with carrying out these activities.

5.4 Real-World Application Results

To further authenticate the output of AI decision trees, the results of real-life applications were gathered at a financial institute where the model was implemented within the premises of cybersecurity operations. The accumulated cost of minor alerts and major computer attacks resulted in a high rate of accidents within the institution daily. The model of the AI decision tree dealt with over 2000 incidents daily, where it was successful in identifying and taking action on threats 92% of the time. The false positive threshold applied by the deployment control of the financial institution was set at seven, which is significantly lower than the standard threshold of 20-30% typically used with conventional systems. This is an exceedingly high level of efficiency when it comes to such a reduction in false positives. It minimizes the false alarms, which will distract the analyst and force them to manage the real threats [3]. The time-to-detection was also reduced by half, and the model was significantly quicker than the human analysts in incident detection. This time saved is of extreme importance in preventing the potential danger of attacks, especially when it comes to fast-moving threats, such as ransomware and denial-of-service attacks.

Table 2: Performance Metrics of AI Decision Trees in Real-World Cybersecurity Applications

Metric	Result	Impact
Number of Incidents Handled Daily	2000+ incidents	High volume of daily incidents successfully managed
Detection Success Rate	92%	High success rate in threat detection
False Positive Rate	7% (lower than 20-30% standard)	Significant reduction in false positives
Time-to-Detection Improvement	Halved compared to manual methods	Faster detection leads to quicker mitigation
Automation Success Rate	80%	AI automation alleviates analyst workload and enhances efficiency

The researchers had obtained a success rate of 80 percent automation of the incidents the AI represented, and this corresponds to the fact that the AI was successful in the automation process. The high level of automation may help such organizations automate the incident response process to reduce the pressure on security analysts and make the response process unified and efficient. According to the test and outcome, the AI decision tree was beneficial in providing automated solutions to incidents regarding cybersecurity. It was a response that was convenient and effective. It was conducted over a short time due to the decision trees that revealed a high level of detection, reduced false positives, and easy control of incidents. The further results of the real-life scenario test on one of the financial institutions also contribute to the contextual benefits of an AI decision tree since the information was significantly more accurate in reporting an incident, eliminating it, and influencing it most beneficially. The monitoring opportunities provided by the constant creation and introduction of AI decision trees have the potential to transform the incident response process, especially in environments where a significant cyber threat is present on a large scale.

6. Discussion

6.1 Evaluation of AI Decision Trees for Incident Response

The use of AI-based decision trees is an active development of cybersecurity incident response automation. They have been proven to be efficient in the context of the traffic blasts, which need a high volume and a high speed of attacks, and mostly whenever an attack happens, as in the case of DDoS (Distributed Denial of Service) attacks [29]. AI decision trees are fast and have one of the greatest strengths in their speed and scale. For example, with a high-incidence attack, where the aim is to send 1000 DDoS requests every second, the AI-supported system concludes this timeframe, significantly less than more traditional techniques, which would require analyst involvement in every decision, thereby extending the reaction time. Using AI decision trees, responses to attacks may be made automated in seconds, which contributes significantly to the overall efficiency of incident response.

The figure below demonstrates a range of AI-based cybersecurity solutions that can be used to improve the efficiency of incident response. The significant elements include phishing email detection, network traffic anomaly detection, and malware detection. Responding to high-speed cyberattacks, including DDoS attacks, through the integration of AI decision trees is fast, automatic, and quick to analyze and mitigate the threats without human intervention. This automation saves a lot of time in reaction, and the overall response to the incident boosts the efficiency of the response to cybersecurity.

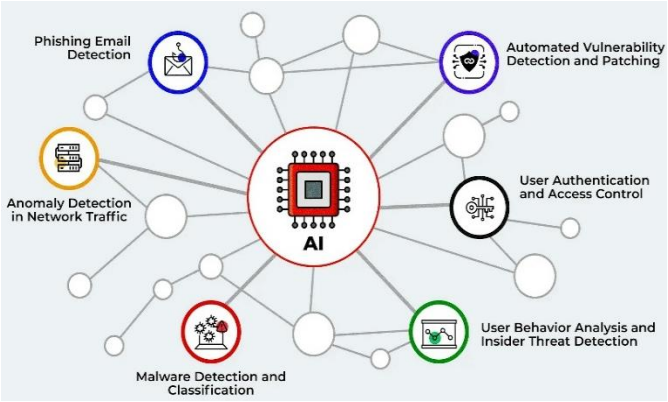

Figure 4: AI-powered solutions for real-time threat detection and incident response automation

AI decision trees are highly accurate and precise, and therefore play a crucial role in the process of threat detection and mitigation. A detection accuracy of over 95% will enable AI decision trees to accurately identify and prevent any incidents that may cause serious breaches. Such high precision also ensures that security teams are not overwhelmed with irrelevant alerts, allowing them to focus more effectively on real threats. Artificial intelligence decision trees are also beneficial in the long run because they can be easily retrained to respond to new threats using updated datasets. Such properties present advantages, such as the security staff obtaining a valuable tool to automate the initial violation, ensuring a significant reduction without compromising quality and accuracy [6].

6.2 Comparison with Traditional Methods

Purchasing the contrast between the AI-driven system of responding to the incidents and their alternative, carried out by people, is radical. The standard range of response times as recommended by conventional rules is 20-30 minutes because, under the conventional interpretation, analysts have to detect, sort, and respond to alerts manually. Such a slow pace places organizations at a prolonged risk in the tug of war of a security incident, specifically with a zero-day attack, such as ransomware or a zero-day exploit. The response times are reduced by 40 to 60% due to AI-related systems, and the threat prevention may happen just seconds away [31]. This rate is quite crucial, particularly when it takes a single second to travel one mile, particularly in one of the financial institutions or other big companies. The speedy containment of a cyberattack will prevent any news of the attack whatsoever.

Table 3: A comparison between AI and Traditional Incident Response based on speed, accuracy, and operational Impact

Metric	Traditional (Manual)	AI Decision Trees	Change / Impact
Response time (MTTR)	20–30 minutes to detect, triage, and act	Seconds to minutes; automation triggers actions immediately; 40–60% faster	Shorter exposure window; faster containment of ransomware/zero-day activity
Classification / response error rate	20–30% analyst-driven misclassification	5–10% after rule-driven decisions	−10 to −25 percentage points; fewer missed/incorrectly handled incidents
Exposure during incident	Prolonged risk while analysts review alerts	Rapid mitigation; prevention may occur within seconds	Material reduction in dwell time and blast radius
Analyst workload	High manual triage and routing; alert fatigue	Routine tasks automated; analysts focus on complex cases	Efficiency gains and better use of expert time
Consistency of actions	Variable; depends on analyst and workload	Consistent, auditable rule paths across incidents	Higher reliability and easier governance/compliance

Incident classification and response due to human error is also experienced in the manual traditional environment at a 20-30% rate, as highlighted in Table 3 above. A human analyst, particularly one with a large number of alerts, can identify classification errors or miss apparent threats. AI decision trees, however, are also aimed at stoning the established decision rules, thereby making the decision tree minimize errors during threat identification. In practice, AI-based applications can reduce all these mistakes to 5 or 10% which will result in much more reliable solutions to the issue of ensuring that security incidents are properly noticed and addressed. This approach not only enhances the overall capability to respond to incidents but also reduces the workload of security personnel, allowing them to focus on more complex threats that require manual attention.

6.3 Challenges and Limitations

There are some challenges associated with AI decision trees, despite their use. One of the issues to be aware of, in the present case, is overfitting in general, and most typically arises in machine learning, where machine learning models are over-performing on the available training data and cannot be used in new, previously unseen attack examples. This is an even more special problem with the fast-evolving sphere of cyber threats, whereby attack vectors can emerge extremely frequently. When the decision trees are over-fitted, they will not be able to detect new threats, hence missing or sending out false negatives. To decrease the overfitting, a variety of measures can be used, such as pruning (increasing the complexity of the choice tree), cross-validation (training the model on hidden data), and ensemble models like Random Forests or Gradient Boosting. The methods combine a range of decision trees to bolster model resilience and precision, particularly in complex situations. Through these tricks, AI models can be effective in a dynamic threat environment.

The other difficulty is an ethical one, which is also linked to the cybersecurity decision-making automation. The possibility of automated misclassification in cases where an accidental or unintentional occurrence of the vice occurs is one of the potential issues [37]. This may lead to unnecessary functionality of the businesses or the inability to respond to a real attack. The fact that the human element cannot control the process of automating the decision-making process can further exacerbate these problems, as security specialists might fail to identify such falsifications of AI systems within the shortest possible time. The most significant action to be taken in response to these concerns would be the implementation of a human-centered-loop strategy, where vital choices can be examined from the perspectives of human analysts, especially when making decisions at an advanced level of risk (e.g., isolating critical infrastructure). This mixed approach will enable a scenario where, in case routine cases can be covered by automation, in case of more serious or complex cases, the human judgment will be applied. To establish accountability and deal with ethical issues, it is also essential to ensure that the process of making decisions using AI remains auditable and transparent [26].

6.4 Practical Implications

Implementation of AI-based incident response systems has several cost advantages for an organization. Incident detection and response can be automated to save up to 40% of staffing and operational costs, as it reduces the number of human resources required to handle the process. Having the capability to automate routine operations, the organization will reduce the need for analysts to manually review each incident, allowing them to be more strategic in their approach to cybersecurity. Such economic potential can provide the most value to large businesses that use the complex network infrastructure and experience high rates of security breaches.

Table 4: Key Implications and Benefits of AI Decision Trees in Incident Response

Aspect	Details	Impact on Organizations	Challenges	Long-term Impact
Cost Savings	Automates detection and response, saving up to 40% in staffing and operational costs	Cost-effective solution, especially beneficial for large businesses	Requires reduction in human labor for incident response tasks	Helps organizations reduce operational costs and scale cybersecurity efforts
Operational Efficiency	Reduces the need for manual review, allowing	Improves incident response speed and	Ensuring timely integration with existing	Increases productivity by automating routine

Aspect	Details	Impact on Organizations	Challenges	Long-term Impact
	analysts to focus on strategic tasks	accuracy, enhancing overall efficiency	systems and infrastructure	tasks and focusing on complex threats
Integration Challenges	Integration with legacy systems is time-intensive and expensive	Requires thorough planning and may be affordable only for larger organizations	Large organizations can bear the cost, but smaller organizations may struggle	Requires careful consideration of compatibility with existing systems
High Initial Investment	High initial costs for installation, training, and integration of AI systems	Initial setup can be expensive, but the long-term benefits justify the investment	Requires a significant initial outlay, but future savings make it worthwhile	Expected to become more affordable as AI systems mature
Overall Benefits	Faster response, reduced errors, and significant long-term savings in cybersecurity	AI decision trees improve detection, reduce false positives, and streamline response	Integration with legacy systems and dealing with overfitting and ethical concerns	Expected to enhance the overall security posture across industries

AI deployment as decision trees in current cybersecurity systems faces its obstacles. Integrating with legacy systems to facilitate the new systems is among the most significant challenges, as it can be both time-intensive and expensive. Most of the organizations have old security tools and workflows, and the integration of the AI-oriented systems into the existing environment necessitates thorough planning and a highly-priced new structure. In addition to this, the initial cost of installing AI systems is very high, which is compounded by the cost of data cleaning, training models, and integrating systems, which can only be afforded by larger organizations. Despite these concerns, the value of AI decision trees to incident response best justifies their initial investment, even for the majority of organizations. This combination of opportunities to reduce the needs of humans to conduct activities regularly, to shorten the response time, and accelerate the total rates of detection is why AI can be incredibly beneficial towards improving the efforts put in by cybersecurity missions. The increasing maturity and affordability of AI are expected to boost its usage across various sectors, further enhancing the security posture of companies in the international scene.

An AI decision tree is significantly better than a human-based system, as it responds faster to events, identifies better, and minimizes rare cases of error. Although issues such as overfitting and ethics have not been fully resolved, they can be addressed nowadays with the help of elaborate procedures, including pruning, cross-validation, and human oversight [12]. The implementation implications of implementing AI-based systems are significant savings in costs and a high level of efficiency in their operations, which is lucrative to organizations that are willing to boost their cybersecurity. AI must be integrated into existing infrastructures with a deep consideration of the compatibility of legacy systems and the steep initial requirements of its implementation.

7. Future Considerations and Research Recommendations

7.1 Improving Decision Tree Models

Although AI-based decision trees have shown promise for automating incident response, there are significant opportunities for improvement and further enhancement. Ensuring that the performance of decision tree models is enhanced by using ensemble techniques, like Gradient Boosting and Random Forests, is one of the strategies. These approaches use multiple decision trees to enhance the accuracy of the models, diminish overfitting, and cluster data assumptions that are more complex [14]. A more realistic and generally more stable example is Random Forests, where decision trees are constructed individually using random samples of the data and averaged together by creating many instances of the model.

With a large number of trees, the model increases its resistance to noisy or incomplete data and is also capable of modeling the variability of cyber threats [13]. Gradient Boosting works similarly, as it is trained on serial trees with each successively correcting the mistake of the former tree, resulting in more accuracy within a complex attack-detection

environment. Such a combination of decision trees and more sophisticated ensemble techniques can be even better in simplifying attacks in the environment, particularly in one where the character of attacks changes very quickly. Studies on how to optimize the interaction between decision trees and ensemble approaches may also enhance their efficiency, as they can become even more effective in cybersecurity-related applications.

7.2 Expanding the Scope of Automation

As AI decision trees are inevitably expanded, they have the potential to develop automation for even intricate attacks. Modern decision tree models are great at identifying the most frequent forms of threats, such as DDoS or malware, but may not identify complex attacks, such as the trace of the insider threat or Advanced Persistent Threat (APT). These are some of the threats, one of which is called insider threats, which consists of the attacks within a given organization that are hard to detect, as they usually resemble the regular functioning of the organization. To this effect, APTs suggest that there exists exceedingly professional and resolute malware, which can easily bypass the usual detection methods through advanced tactics. An AI decision tree that also takes into consideration user behavior analytics and access patterns, as well as analyzes the context of each action, will be required to maximize the AI decision-making process and reduce the prominence of such attacks, allowing for other, less noticeable and harder-to-trace offenses.

The AI used in the future may involve the use of AI with Threat Intelligence Platforms (TIPs), where real-time and external intelligence on emerging threats and signs of attack are involved. The process of the decision tree would be enhanced with the inclusion of this external data in terms of making the decision, and also, recognizing new forms of attacks that would be logged, and the time response would be reduced. Such integration would mean that people will only search internal data using these incident response systems, and no need to refer to the global intelligence, in fact, to counter the sophisticated threats [30]. External threat intelligence also gains the ability to find zero-day vulnerabilities rapidly, particularly when the attacks are performed by already unfamiliar threats, which further makes the discovery and protection mechanism even faster. This would play a crucial role in enabling AI-based decision trees to handle more instances of attacks effectively.

7.3 AI Ethics and Interpretation

The explicability of the AI models and ethical AI has become one of the main issues to consider, particularly as automated decision-making is integrating AI broadly. The central issue with adopting AI in sensitive fields such as cybersecurity is that the model should be clear and understandable in its potential to reach judgments. Explainability ensures that security analysts have confidence in the decisions made by a system, which includes the logic behind those decisions. This is particularly important in high-stakes emergencies, such as the seclusion of essential systems or the interception of large volumes of network traffic.

Explainable AI (XAI), which is studied, supports the idea that it can help in making decision trees readable. By developing models that present the decision and give information on why and how decisions were reached, organizations have a higher chance of feeling confident about this type of automation process. The LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley Additive Explanations) datasets have been designated as one of the two most popular datasets able to explain machine learning models that may be implemented into AI decision trees to encourage transparency.

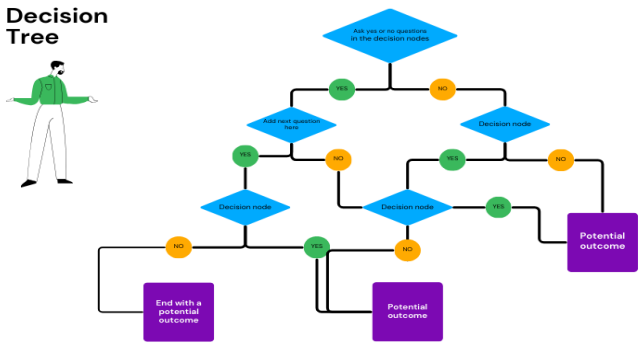

Figure 5: Decision tree model illustrating AI's explainability and decision-making process

A decision tree, as shown in Figure 5 above, illustrates how Explainable AI (XAI) facilitates the explanation of automated security decisions. Human-readable reasons can be provided with every yes/no division and outcome, allowing the analysts to gain insight into why an alert was escalated or containment was suggested. Some methods (LIME and SHAP) produce both local and global attributions, where the characteristics (IP reputation, process lineage, and process velocity) that led to each branch decision are highlighted [1]. Their embedding enhances transparency, auditability, and confidence, allowing SOC teams to confirm that they have taken the right action, optimized specific rules, and responsibly implemented AI-driven incident response at an enterprise scale.

Another priority that addresses the element of unintended consequences as an emerging dilemma is the question of ethical implications in AI decision-making. Automated systems label harmless operations as threats, thus interfering with business operations and potentially endangering the loss of crucial data. Research has indicated that these issues can be addressed by implementing relevant mitigating factors, such as continuous education, human controls, and controls over hazardous areas, as well as actions that involve feedback loops. The efficacy of AI models will become necessary, and they will be expected to be fair, transparent, and accountable, enabling this technology to gain broader usage in the sphere of cybersecurity and, in general [28].

7.4 Research Recommendations

Even though making the application of an AI decision tree to incident response is valuable as well, there are still several research and development possibilities. Research into the integration of multi-modal data, such as the gating of network traffic data and endpoint behavior, or even user activity logs, can increase the precision of detection of complex threats [25]. It is also possible to implement learning methods that enable the achievement of learning outcomes in the absence of supervision. Decision trees can track new attack patterns that do not require supervised data, helping to solve new or entirely unknown cyber threats.

The use of AI decision trees with real-time data analytics systems, such as SIEM systems and Security Orchestration Automation and Response (SOAR) systems, has the potential to enhance the speed and efficiency of response times [9]. Based on the topics of this research, the new frontier of incident response is automation enabled by AI, which will be a crucial factor in ensuring that such systems remain flexible and can learn new information to stay as efficient as possible. The moral aspects and regulations must also change in tandem with the development of AI. Fair and explainable AI model research will be a critical factor in making sure AI applied to cybersecurity is trustworthy and responsible in actual implementation situations.

8. Conclusion

The paper has confirmed the high promise of AI-assisted decision trees in making incident response much more effective in the context of cybersecurity. Decision trees are much slower and less successful in responding to incidents, with the infrastructure of autoinformatics, which checks and ranks incidents. The experiments also proved that AI-driven platforms are capable of reducing response times by up to 40 to 60%, and AID-tree is capable of identifying typical cybercrimes of 95% together with DDoS, malware, and other crimes. This offers far superior performance compared to traditional manual systems, which tend to have the disadvantages of slow response and a high false positive rate. Automating most of the processes involved in detecting and responding to incidents, AI decision trees are also used to ease the workload on security analysts, allowing them to concentrate on more advanced threats, while increasing the overall level of efficiency in handling incidents.

There was a tendency to generate AI-based decision trees that are integrated into the current security systems, including SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) platforms, which helped simplify the process of incident response and enhance the scalability of the cybersecurity processes. The performance of the activities that had been done in the real world also proved the hypothesis that AI decision trees are capable of processing a large quantity of incidents efficiently, as the reality that one of the financial institutions had managed more than 2000 incidents a day with a 92% success rate confirmed that AI decision trees in work are indeed effective in the real world. This would imply that the solutions based on AI are more receptive to threats and can block them. The practical response to the adoption of AI-powered incident response frameworks is comprehensive for modest and considerable organizations. Companies can significantly reduce the cost of operations involved in incident management by automating crucial response aspects, thereby reducing the need to incur up to 40% of staffing and operational expenses. Furthermore, automated systems might ensure faster responses to cyber threats, which will be

particularly needed to prevent data breaches and ransomware threats that would otherwise cost them crippling financial and reputational devastation.

The trend of organizations facing a need to react to massive amounts and sophisticated types of threats would make AI decision trees a valuable instrument in detecting threats and responding to them quickly. One such example is that automated systems have been shown to avoid a DDoS attack within seconds in comparison to a traditional system, which can take minutes or even several minutes, exposing vulnerable systems to vulnerability of refraction. Automation can also be applied to routine activities like IP blocking, network isolation, and the generation of alerts so that cybersecurity teams can focus on the high-scope incidents to raise the response rate on incidents and improve the level of safety in general. The adoption of AI-based systems also paves the way to improvement that may manifest itself through the expansion of opportunities in combating cases of more complex attacks, including insider threats and Advanced Persistent Threats (APTs) that have recently become challenging to counter via the application of current methods. This integration of external threat awareness and real discrepancy statistics suggests that the expanded AI decision tree will be continuously updated to reflect new and emerging dangers and react promptly to cybersecurity-related issues.

The future of cybersecurity is the continuation of AI-based automation and decision trees to influence the accuracy, speed, and scalability of the incident response. AI decision trees will transform the process of identifying and reacting to cyber threats by organizations by providing more rapid, dependable, and scalable solutions. With minimal-to-zero false positives and the capability to automate repetitive routine actions, AI-driven systems will enable security analysts to invest more energy in addressing more advanced and previously unseen incidents more quickly.

Although they can be overfit, their ethical implications require attention, and continuous training is necessary. AI decision trees can provide a potent response tool for both manual and automated responses to incidents. The combination of human control and machine-based decision-making ensures that cybersecurity processes are both practical and responsible. In the future, AI decision trees will continue to advance, and new advanced methods, such as ensemble and explainable AI (XAI), will provide additional functionality to AI-driven systems that can identify, forestall, and prevent cyber threats. Artificial intelligence-ASDDT is one of the most significant advances to automate cybersecurity and provide the required automated tools to tackle the escalated intensities and assortment of cyber threats by improving response timeframes and minimizing expenses incurred in organization operations. The future of AI-driven systems and the automation process can be viewed with high expectations for changing incident response procedures, especially in the field of cybersecurity.

References;

[1] Abdullah, T. A. A., Zahid, M. S. M., Turki, A. F., Ali, W., Jiman, A. A., Abdulaal, M. J., ... & Attar, E. T. (2024). Sig-lime: A signal-based enhancement of lime explanation technique. *IEEE access*, *12*, 52641-52658.

[2] Adepoju, A. H., Austin-Gabriel, B. L. E. S. S. I. N. G., Eweje, A. D. E. O. L. U. W. A., & Collins, A. N. U. O. L. U. W. A. P. O. (2022). Framework for automating multi-team workflows to maximize operational efficiency and minimize redundant data handling. *IRE Journals*, *5*(9), 663-664.

[3] Alahmadi, B. A., Axon, L., & Martinovic, I. (2022). 99% false positives: A qualitative study of {SOC} analysts' perspectives on security alarms. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 2783-2800).

[4] Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *Ieee Access*, *11*, 80348-80391.

[5] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial intelligence review*, *54*(5), 3849-3886.

[6] Chavan, A., & Romanov, Y. (2023). Managing scalability and cost in microservices architecture: Balancing infinite scalability with financial constraints. *Journal of Artificial Intelligence & Cloud Computing, 5*, E102. https://doi.org/10.47363/JMHC/2023(5)E102

[7] Christa, S., Suma, V., & Mohan, U. (2022). Regression and decision tree approaches in predicting the effort in resolving incidents. *International Journal of Business Information Systems*, *39*(3), 379-399.

[8] Dhanagari, M. R. (2025). Aerospike: The key to high-performance real-time data processing. *Journal of Information Systems Engineering and Management.* https://www.jisem-journal.com/index.php/journal/article/view/8894

[9] El Emam, K., Mosquera, L., & Hoptroff, R. (2020). *Practical synthetic data generation: balancing privacy and the broad availability of data*. O'Reilly Media.

[10] Fan, W., Zhao, X., Chen, X., Su, J., Gao, J., Wang, L., ... & Li, Q. (2022). A comprehensive survey on trustworthy recommender systems. *arXiv preprint arXiv:2209.10117*.

[11] Gartley, M. E. (2024). Preregistration and Registration as a New Method for Transparency of External Validation in Artificial Intelligence and Machine Learning Applications to Address Overfitting, Underspecification, and Shortcut Learning.

[12] Goel, G., & Bhramhabhatt, R. (2024). Dual sourcing strategies. *International Journal of Science and Research Archive*, 13(2), 2155. https://doi.org/10.30574/ijsra.2024.13.2.2155

[13] Halabaku, E., & Bytyçi, E. (2024). Overfitting in Machine Learning: A Comparative Analysis of Decision Trees and Random Forests. *Intelligent Automation & Soft Computing*, *39*(6).

[14] Jangampet, V. D. (2021). The Rise of The Machines: AI-Driven SIEM User Experience for Enhanced Decision-Making. *International Journal of Computer Engineering and Technology*, *12*(3).

[15] Karwa, K. (2024). Navigating the job market: Tailored career advice for design students. *International Journal of Emerging Business*, *23*(2). https://www.ashwinanokha.com/ijeb-v23-2-2024.php

[16] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[17] Licitra, S. (2024). *Leveraging AI Techniques for Automated Security Incident Response* (Doctoral dissertation, Politecnico di Torino).

[18] Liu, H., Zhong, C., Alnusair, A., & Islam, S. R. (2021). FAIXID: A framework for enhancing AI explainability of intrusion detection results using data cleaning techniques. *Journal of network and systems management*, *29*(4), 40.

[19] Mahbooba, B., Timilsina, M., Sahal, R., & Serrano, M. (2021). Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. *Complexity*, *2021*(1), 6634811.

[20] Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing resilient cyber-physical systems: a review of state-of-the-art malware detection approaches, gaps, and future directions. *Computers*, *12*(4), 79.

[21] Mohan, R., Vajpayee, A., Gangarapu, S., & Chilukoori, V. V. R. (2024). Mitigating Complex Cyber Threats: An Integrated Multimodal Deep Learning Framework for Enhanced Security. *International Journal for Research in Applied Science and Engineering Technology*, *12*(9), 1108-1117.

[22] Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637

[23] Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

[24] Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: A survey. *Journal of Supercomputing*, *76*(7).

[25] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525-2556.

[26] Schmidt, E., Work, R., Catz, S., Horovitz, E., Chien, S., Jassy, A., ... & Moore, A. (2021). National security commission on artificial intelligence (ai).

[27] Singh, V. (2024). AI-powered assistive technologies for people with disabilities: Developing AI solutions that aid individuals with various disabilities in daily tasks. *University of California, San Diego, California, USA. IJISAE*. https://doi.org/10.9734/jerr/2025/v27i21410

[28] Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *Ieee Access*, *8*, 128440-128475.

[29] Tsamardinos, I., Charonyktakis, P., Papoutsoglou, G., Borboudakis, G., Lakiotaki, K., Zenklusen, J. C., ... & Lagani, V. (2022). Just Add Data: automated predictive modeling for knowledge discovery and feature selection. *NPJ precision oncology*, *6*(1), 38.

[30] veria Hoseini, S., Suutala, J., Partala, J., & Halunen, K. (2024). Threat modeling AI/ML with the Attack Tree. *IEEE Access*.

[31] Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P. S., ... & Gabriel, I. (2021). Ethical and social risks of harm from language models. *arXiv preprint arXiv:2112.04359*.

[32] Yu, Z., Zhu, H., Xiao, R., Song, C., Dong, J., & Li, H. (2021). Detection and defense against network isolation attacks in software-defined networks. *Transactions on Emerging Telecommunications Technologies*, *32*(5), e3895.