World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Integration of AI with ethical hacking tools for predictive vulnerability detection

Mullaishselvi Krishnasamy * and Mohamad Fadli bin Zolkipli

School of Computing, College of Arts and Science, University Utara Malaysia (UUM), Sintok, Kedah, Malaysia.

World Journal of Advanced Research and Reviews, 2025, 27(01), 063-074

Publication history: Received on 17 May 2025; revised on 28 June 2025; accepted on 30 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2463

Abstract

The evolving nature of cyber threats, especially zero-day exploits, demands a shift from traditional reactive security mechanisms to proactive and predictive defense strategies. This paper explores the integration of Artificial Intelligence (AI) with ethical hacking tools to enhance predictive vulnerability detection, focusing on Snort and Maltego. By embedding machine learning algorithms into these tools, their capabilities in anomaly detection and threat intelligence are significantly enhanced. This research investigates the integration of machine learning (ML) algorithms into ethical hacking tools, Snort and Maltego to strengthen their anomaly detection and threat intelligence functionalities. This study presents AI-driven framework where supervised and unsupervised learning models are embedded into Snort for packet level anomaly detection and into Maltego for enhanced threat correlation. Applying machine learning algorithms to detect and classify threats based on data from live network traffic and threat intelligence sources. Training and evaluation methods are used to improve accuracy and reduce false alarms. Although challenges like data labelling, changing patterns, and ethical issues exist, this approach greatly strengthens early threat detection and response. This research supports the advancement of intelligent cybersecurity systems capable of proactive threat mitigation.

Keywords: Artificial Intelligence; Ethical Hacking; Machine Learning; Predictive Detection; Snort; Maltego

1. Introduction

Zero-day exploits, or vulnerabilities that are exploited before developers are aware of them or have the opportunity to deploy patches, are becoming a bigger threat to cybersecurity [9, 10]. Because of their unpredictability and capacity to evade signature-based detection mechanisms, these exploits represent a significant risk of serious data breaches, system failures, and monetary loss. Proactive and anticipatory cybersecurity solutions have grown essential and urgent as threats get more complex [16]. By simulating actual attacks to find flaws in systems, ethical hacking tools are essential to proactive defense. Two of the most popular tools are Maltego, an open-source intelligence (OSINT) connection analysis tool, and Snort, an open-source intrusion detection system (IDS). Maltego is frequently used for visualizing correlations in data during reconnaissance and forensic investigations [18], whereas Snort is excellent at traffic analysis and rule-based detection of known threats [1, 8]. These technologies, however, are typically reactive in nature and have limitations when it comes to addressing new or unknown threat routes [12, 19].

To move beyond reactive defense, there is a growing need for predictive cybersecurity systems that can forecast vulnerabilities and intrusions before they occur. Predictive defense mechanisms enable organizations to strengthen their security measures and reduce incident response time [5, 13]. These systems must be capable of learning from historical data, identifying suspicious behavior, and adapting to new attack vectors without explicit programming [11]. Such capability could significantly reduce system downtime, data loss, and delay response during cyber incidents [14]. Machine learning (ML) has emerged as a transformative solution in cybersecurity analytics and threat detection. ML algorithms can recognize anomalous patterns, classify threats, and even predict the likelihood of zero-day attacks based on behavioral cues [2, 12, 14]. Integration of AI-driven models with tools like Snort and Maltego has elevated detection

* Corresponding author: Mullaishselvi Krishnasamy

accuracy, reduction in false positives, and the ability to identify emerging threats that traditional tools may overlook [3, 4, 15]. For example, AI-enhanced Snort systems have been shown to detect Distributed Denial-of-Service (DDoS) attacks in software-defined networks with improved performance [12], while Maltego has been enhanced with generative AI for penetration testing intelligence and OSINT enrichment [4, 6].

This study explores the integration of AI, specifically machine learning models with Snort and Maltego to develop a framework for predictive vulnerability detection. The objective is to anticipate zero-day exploits and enhance proactive threat intelligence. By embedding machine learning into these ethical hacking tools, the study aims to transition traditional defensive mechanisms toward a more intelligent, adaptive, and anticipatory cybersecurity posture.

1.1. Problem statement

Despite the widespread use of intrusion detection systems (IDS) and ethical hacking tools, conventional cybersecurity measures continue to struggle with addressing contemporary threats. Most detection systems depend on known threat signatures, which limits their ability to identify only those attacks that have been previously recognized [1, 8]. Consequently, they are reactive and fall short in defending against zero-day exploits, which exploit unknown or unpatched vulnerabilities [9, 10]. Identifying zero-day threats poses a challenge because their actions often resemble typical system operations. Tools-like Snort, which operate on predefined rules, find it difficult to detect these threats [1, 3]. Additionally, modern attack strategies such as encrypted traffic, polymorphic malware, and evasion techniques—further complicate real-time detection [4, 11]. While tools like Maltego assist with OSINT and threat mapping, they depend significantly on manual input and are less predictive of threats [6, 7].

The inability of present systems to anticipate or adjust to emerging threats as they materialise is a major flaw. Without regular human updates or new regulations, they are unable to predict attacks, but they are able to monitor and log them [12, 13]. Delays, missed detections, and additional effort for security teams result from this. Artificial Intelligence (AI) and machine learning (ML) must be incorporated into ethical hacking tools to solve these problems. These devices can identify anomalous activity, anticipate potential dangers, and learn from data. In order to provide real-time and predictive vulnerability detection, particularly for zero-day attacks, this article suggests integrating machine learning models into Snort and Maltego.

2. Literature review

2.1. Existing AI Applications in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) have transformed cybersecurity by letting us use smart, data-driven defenses to fight against more complicated threats. There is a shift toward adaptive systems that incorporate AI because traditional rule-based systems can't always discover new or difficult dangers. ML algorithms are great at spotting intrusions, strange activity, infections, and patterns of behavior. These systems continuously learning from new data, which makes them less likely to be attacked by new types of attacks, such zero-day vulnerabilities.

Supervised learning, deep learning, and ensemble models make it much easier to find threats quickly and accurately. Random forests, decision trees, and convolutional neural networks (CNNs) are some of the technologies that have been utilized to tell the difference between safe and harmful traffic patterns in real time. One of the biggest problems with static detection systems is that they can't find threats that have not been observed before. These improvements fix that problem. Manoharan and Sarker [13] talked about how machine learning (ML) has changed cybersecurity by making it possible to find threats faster and more accurately than older ways. In the same way, Sarhan et al. [11] showed how zero-shot learning might be used to find zero-day attacks without the need for labeled instances.

2.2. Previous Integrations of ML with IDS/OSINT Tools

Integration of ML has been especially beneficial for intrusion detection systems (IDS). To increase detection rates and lower false positives, ML algorithms have been added to Snort, one of the most popular IDSs. In order to achieve greater detection accuracy, EL AERAJ and LEGHRIS [1] carried out a thorough analysis of Snort in conjunction with ML models. After integrating AI techniques with Snort for cloud environments, Sadargari and Balaji [3] reported increased accuracy and threat mitigation performance. Similarly, AbdulRaheem et al. [12] demonstrated a significant improvement in DDoS detection by applying ML-assisted detection to both Snort and Zeek in software-defined networking. Random Forest could be incorporated into IDS frameworks to improve scalability and precision, as Al-Doori and Alheeti [2] showed.

AI is also being added to open-source intelligence (OSINT) tools like Maltego. In their review, Oakley Browne et al. [6] examined the use of AI to automate OSINT tasks such as entity scoring, link analysis, and clustering. In his discussion of

Maltego's architecture, Amgai [7] raised the possibility that integrating AI could improve investigative processes. The educational and practical benefits of using AI to OSINT in professional training settings were further highlighted by Schwarz et al. [18].

2.3. Comparative Analysis of Detection Approaches

It is clear from comparing AI-enhanced models to traditional detection systems that the latter are superior at finding zero-day assaults. Signature-based detection works well for threats that are already known, but it can't be used to find new exploits. AI models, especially those trained on behaviour-based data, can find unusual things without employing threat signals that are already known. Ibraheem and Tosho [10] showed how ML can help protect against zero-day attack vulnerabilities by using performance measurements that were better than those of traditional IDS. Mohamed et al. [16] did a thorough study of ML-based zero-day exploit detection approaches and found that ensemble models and supervised learning were the best ones. Hamid et al. [8] analysed Snort and Suricata, and they concluded that both gain from ML augmentation, however Snort is still more often used in commercial contexts. On the rise, ethical hackers are using generative AI and adaptive learning models. Hilario et al. [4] looked at how generative AI could be used in penetration testing and also talked about the ethical and operational issues that come up with these technologies. Mumtaz and Javaid [5] also pushed for the use of AI along with ethical hacking to provide security testing tools that are both dynamic and predictive.

In short, the research demonstrates that more and more people agree that ethical hacking tools need to include AI and ML to create adaptive, predictive cybersecurity frameworks. Adding clever automation to tools like Snort and Maltego may turn them from passive monitoring systems into proactive defences that can block zero-day assaults before they happen.

3. Methodology

3.1. Architecture Overview of AI Integration

The proposed architecture is meant to improve ethical hacking tools like Snort (an IDS/IPS) and Maltego (an OSINT and link analysis tool) by adding machine learning features that can find vulnerabilities before they happen, especially for zero-day exploits. This integration has a number of modular parts that take care of collecting data, preparing it, making predictions with the model, and improving feedback.

3.1.1. There are six layers in the architecture

- Data Ingestion Layer combines different types of data from sources like
  - Snort can see real-time network traffic, like packet captures, NetFlow, and IDS logs.
  - Maltego's open-source intelligence feeds include WHOIS, DNS, VirusTotal, and Shodan.
  - These sources give the basic information needed for training and inference [1, 3, 7].
- Preprocessing and Feature Engineering Layer takes raw data and turns it into structured feature sets by:
  - Getting protocol-specific information for Snort, like IP entropy, payload length, and port frequency
  - Using NLP and graph analytics to parse and vectorize OSINT data for Maltego [6, 7, 20].
- The Machine Learning Inference Layer uses trained models (both supervised and unsupervised) to find problems or sort risks.
- Snort Integration Module
  - Snort's engine turns ML model outputs into alarm triggers or dynamic rules [1, 8].
  - Using anomaly scores and categorization labels to find suspicious packets in real time.
- Maltego Integration Module
  - AI-enhanced transforms check how dangerous related entities are.
  - Enriched entity relationship graphs [6, 18] show threat intelligence.
- Feedback and Model Update Layer
  - Analysts check alarms and send them back to retrain and fine-tune the algorithms.
  - Helps keep the model from drifting and makes it easier to find things over time [5, 10].

This architecture focuses on real-time predictive defense by constantly learning and adding to popular hacking and spying tools.

3.2. Use of Supervised/Unsupervised Learning for Pattern Recognition

3.2.1. Supervised Learning

Supervised models learn from labeled datasets that have known attack patterns in them. These models are helpful for classifying things in Snort when there is historical data to work with. Some common methods

- Random Forest and Support Vector Machines (SVM), which work well for sorting packet-level features into normal and malignant [2, 15].
- Convolutional Neural Networks (CNNs), these are helpful for finding patterns in packet sequences that change over time and space [14].
- Example of use cases, Snort uses a taught classifier to sort incoming packets in real time and Maltego improves entity scoring by using trained reputation scores and link characteristics.

3.2.2. Unsupervised Learning

Unsupervised learning is very important because there isn't much labeled data for zero-day attacks.

Methods such as

- Autoencoders with Isolation Forests which find strange behavior in a network by looking for outliers [10, 11].
- One-Class SVM only trains on "normal" data to find differences
- Example of use cases, Snort flags network traffic that has strange patterns that were not found in the training data and Maltego highlights links that look suspicious or that the analyst has never seen before.

3.2.3. Hybrid and semi-supervised learning

Hybrid and semi-supervised methods for dealing with uncertainty in the real world. Semi-supervised methods are also integrated where only partial labels are available. Ensemble models use both supervised and unsupervised predictors to make the model stronger and reduce false positives [16].

3.3. Embedding Predictive Models into Snort (for packet-level analysis)

3.3.1. Workflow Design

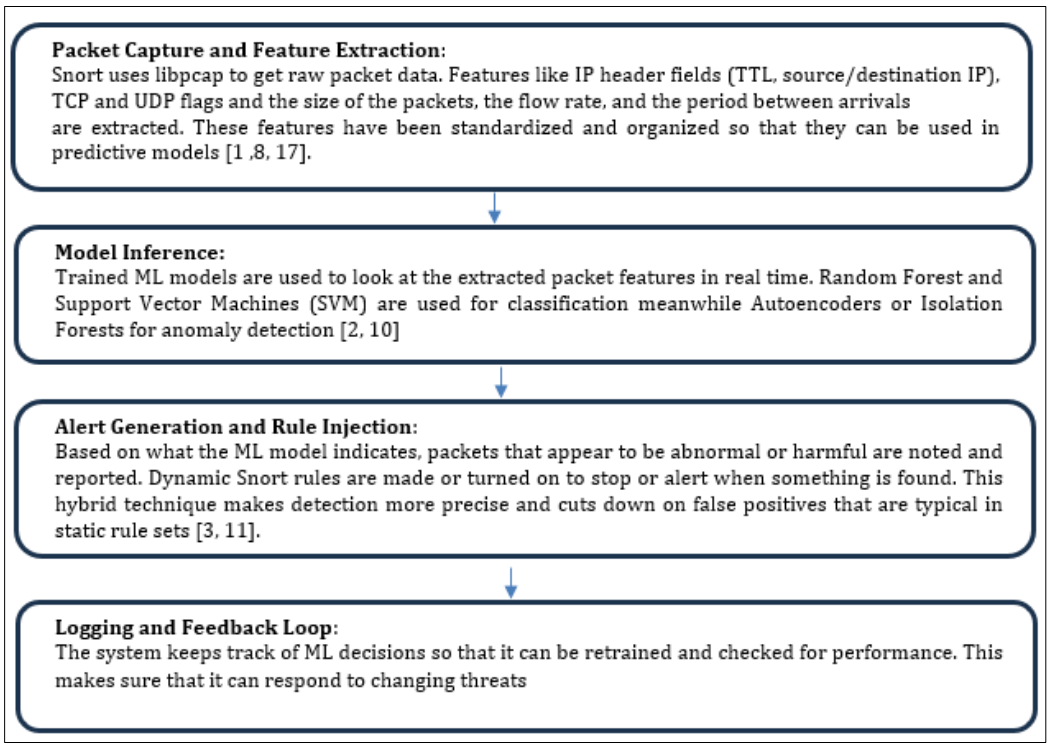


Figure 1 Workflow for packet level analysis of Snort with embedded machine learning

Snort is a signature-based intrusion detection and prevention system (IDS/IPS) that usually uses rule-based logic to find known attack signatures. This study integrates machine learning (ML) models directly into Snort's packet analysis workflow to enhance its ability to detect zero-day vulnerabilities. This embedding changes Snort from a static signature detector into a context-aware predictive engine, making it better at finding polymorphic and zero-day threats.

3.4. Integrating AI into Maltego Transforms for Threat Correlation

Maltego is a commonly used open-source intelligence (OSINT) application for mapping relationships between things like domains, IPs, email addresses, and social media accounts. By adding AI-driven transforms for threat correlation and entity risk rating, our research makes Maltego even better. This integration makes Maltego a predictive threat intelligence platform, which makes it easier to find out about threats and sketch out potential attack paths ahead of time.

3.4.1. Workflow Design

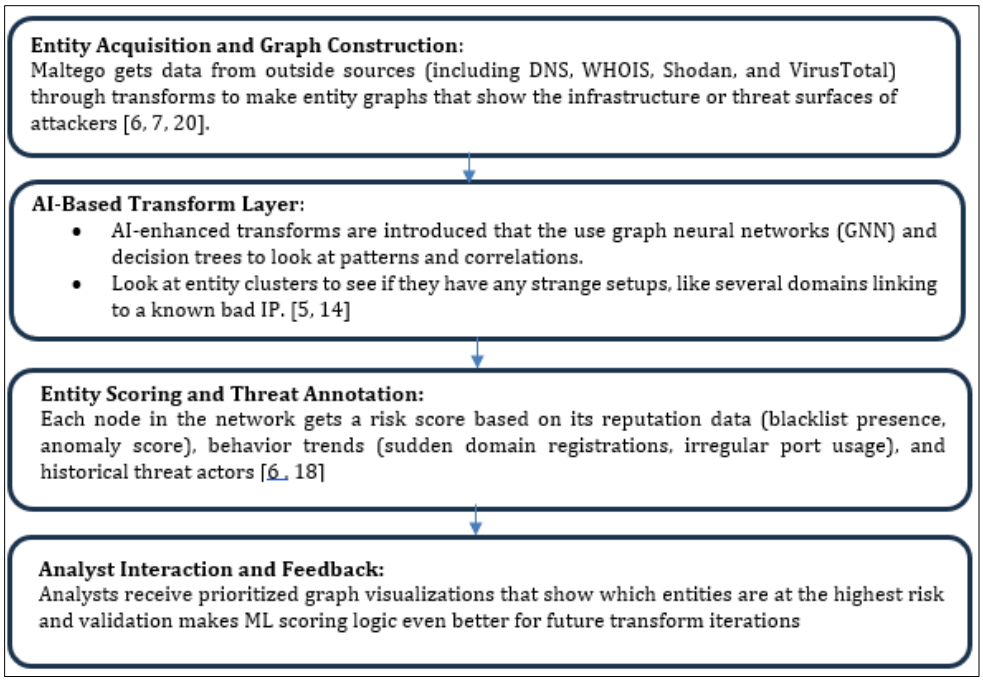


Figure 2 AI driven Maltego predictive threat intelligence workflow

3.5. Data Sources: Network Traffic and Threat Feeds

Reliable and varied data sources are crucial for the proper training and inference of machine learning models in cybersecurity systems. This research employs two primary data inputs network traffic and threat intelligence feeds to create a comprehensive dataset for the integration of Snort and Maltego.

3.5.1. Network Traffic Data for Snort-Enabled Detection

Snort records unprocessed packet-level traffic, which is the basis for deriving features that signify malicious or abnormal behavior. These encompass:

- IP, TCP, and UDP headers (source and destination IP addresses, flags, and ports)
- Payload length and protocol metadata
- Traffic flow characteristics (packet counts, bytes transmitted, inter-arrival intervals)

The datasets utilized in this research comprise

- CICIDS 2017 and UNSW-NB15: Supply annotated network attack data for model training [2, 15]
- Real-time data acquisition utilizing Snort within a regulated testbed environment

The preprocessing procedures encompass normalization, timestamp alignment, and sliding window framing to maintain temporal patterns [1,11].

3.5.2. Threat Intelligence and OSINT Feeds for Maltego

Maltego transformations depend on both organized and unstructured OSINT sources, including

- WHOIS and DNS information for domain reputation and resolution mapping
- Utilizing Shodan and Censys for the enumeration of service exposure
- VirusTotal, AbuseIPDB, and AlienVault OTX for recognized harmful indications
- Classification of tactics, techniques, and procedures (TTP) in MITRE ATTandCK

These feeds are dynamically queried and associated with Maltego entities, generating enhanced graphs for adversary analysis. Unstructured data (e.g., security blog entries, reports) are analyzed using NLP to produce contextually enriched threat profiles [6, 7, 20]. The merge of real-time network data and curated OSINT feeds facilitates both reactive and anticipatory threat identification.

3.6. Model Selection: Algorithms for Classification and Anomaly Detection

Both classification and anomaly detection methods are assessed to guarantee strong performance across various data types and attack categories.

3.6.1. Classification Algorithms (Supervised Learning)

These algorithms are trained on annotated datasets to recognize established assault classifications:

- Random Forest (RF): Highly interpretable and efficient for high-dimensional datasets [2]
- Support Vector Machines (SVM) excel in both binary and multiclass classification tasks.
- Convolutional Neural Networks (CNN): Proficient in identifying temporal-spatial traffic patterns [14]
- Logistic Regression and Decision Trees: Employed for preliminary benchmarking

Models are trained on historical traffic and OSINT-annotated entity interactions. Feature selection is refined through recursive feature elimination and grid search.

3.6.2. Anomaly Detection Algorithms (Unsupervised Learning)

Due to the unpredictability of zero-day attacks, anomaly detection methods are crucial:

- Isolation Forest: Identifies outliers by isolating anomalies via recursive partitioning.
- Autoencoders: Neural networks designed to reconstruct input; elevated reconstruction error signifies an anomaly. [10, 11]
- One-Class SVM: Trained exclusively on "normal" data; deviations are identified as anomalies.

These approaches are especially beneficial in contexts characterized by imperfect labeling or dynamic threats. They are utilized for both packet data (in Snort) and entity relationships (in Maltego).

3.6.3. Evaluation Metrics and Selection Criteria

Model performance is assessed using

- Precision, Recall, F1-Score: For classification equilibrium
- Area Under the Receiver Operating Characteristic Curve (AUC-ROC): Pertaining to binary classifiers
- False Positive Rate (FPR): Essential for Intrusion Detection Systems to mitigate alert fatigue.

The ultimate model selection is predicated on attaining the optimal balance of accuracy, latency, and scalability in practical settings [15, 16].

3.7. AI-Enhanced Workflow in Snort and Maltego

To optimize the operational efficiency of predictive vulnerability detection, the design integrates AI-enhanced workflow within both Snort and Maltego. This workflow enhances threat identification, correlation, and alert creation via automation and intelligent processing.

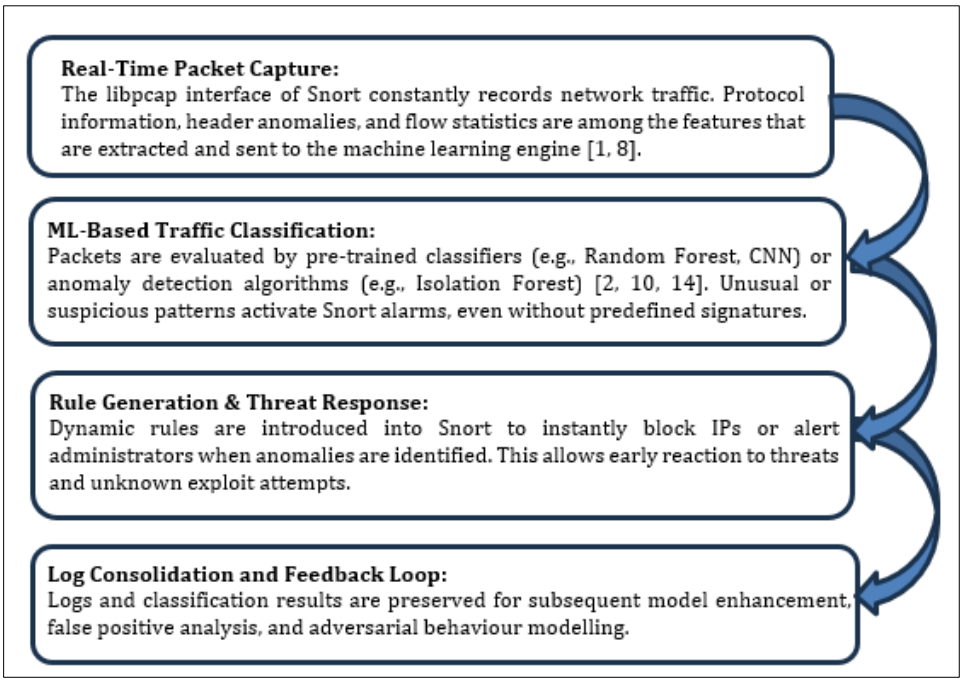


Figure 3 Snort: Intelligent Intrusion Detection Workflow

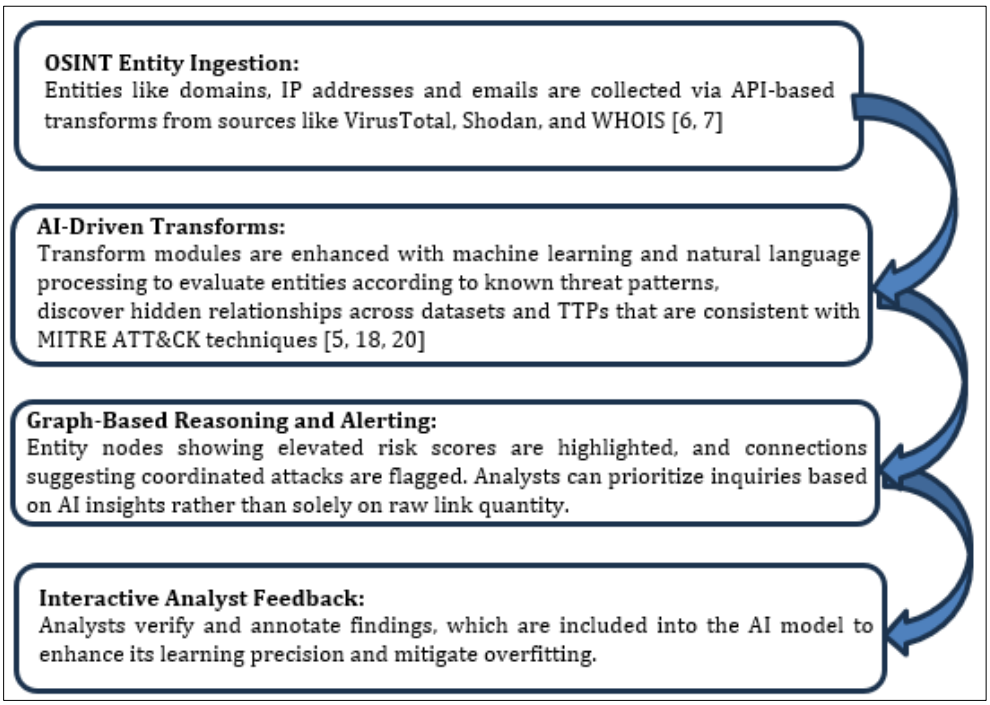


Figure 4 Maltego: AI-Powered Threat Correlation Workflow

3.8. Training and Evaluation Strategies

Reliable and understandable outputs depend on comprehensive training, validation, and testing processes that enable effective model creation.

3.8.1. Dataset Preparation

Labeled Traffic Datasets such as CICIDS 2017, NSL-KDD, and UNSW-NB15 were utilized for Snort-based classifier training [2, 15] and OSINT Datasets which is a manually curated Maltego graphs and threat intelligence feeds from AbuseIPDB, AlienVault OTX, and domain reputation services. Features scaling and normalization; noise and superfluous attribute removal; sliding time frames for temporal correlation. Data preprocessing includes the features scaling and normalization, noise and redundant attributes removal and sliding time windows for temporal correlation.

3.8.2. Model Training and Tuning

Multiple models are trained with K-fold cross-valuation (K=5/10) to prevent overfitting and optimization of parameters by using Grid Search and Random Search. Feature importance analysis is one of the model to identify key predictive indicators. In anomaly detection method, only "normal" traffic is used for training, while anomalies are evaluated during testing [11, 16].

3.8.3. Performance Metrics

Following metrics are used to assess the model effectiveness:

- Accuracy: General accuracy of prediction
- Detection Latency: Assess real-time feasibility
- Precision and Recall: False positives and false negatives assessment
- F1-Score: Balance precision and recall
- AUC-ROC Curve: Measure classification confidence over threshold variation

3.8.4. Continuous Learning and Model Drift Handling

In order to adapt to the emerging threats, retraining model was introduced. Drift detection triggers automatic retraining pipelines [10, 16]. Periodic ingestion of new attack patterns is necessary for continuous learning and improvement. Analyst will perform review on false positive and will reintegrate the reviewed false positives for label correction.

4. Challenges and Limitations

Regardless of the potential of AI-enhanced ethical hacking tools, the integration of machine learning models into Snort and Maltego gives several challenges and limitations which required to be carefully addressed and asses. Following as the common challenges and limitations:

4.1. Data Quality and Labelling Issues

Supervised machine learning models are significant sensitivity to the quality, consistency, and completeness of training data. In the context of cybersecurity, numerous significant challenges are emerging and the most significant problem is the presence of noisy and imbalanced datasets where it predominant by benign traffic and infrequent occurrences of malicious behaviors. This discrepancy frequently causes models to prioritize predictions of "normal" behavior, thereby impairing their capacity to identify zero-day attacks [2, 14].

Another challenge resides in the ambiguity of the ground truth. Precisely classifying security data is inherently challenging due to human errors, evolving threat definitions, and insufficient contextual information from raw traffic or open-source intelligence (OSINT), complicating the compilation of reliable labels for supervised learning [10, 15]. In addition, the absence of standardization in OSINT sources is particularly problematic for tools such as Maltego, which heavily rely on publicly available intelligence. Variations in data formatting, reliability of sources, and update intervals lead to discrepancies in entity relationships and risk assessments [6, 7].

The study applies semi-supervised learning techniques and data augmentation methodologies to tackle these difficulties. The study applies semi-supervised learning techniques and data augmentation methodologies to tackle these difficulties. Nevertheless, more improvements are required to establish collaborative and automated labelling frameworks that might strengthen model robustness and reliability.

4.2. Model Drift and Maintenance

Due to the evolving nature of cyber threats, there is chances of model drift because Artificial Intelligence models are prone to performance degradation over time. This results from the statistical features of input data shifting. The

development of new tactics, strategies, and procedures (TTPs) as attackers always change their approaches to avoid detection, therefore reducing the efficacy of formerly trained models [5, 11].

Furthermore, changes in network usage patterns such that resulting from remote work regulations or the implementation of new applications may cause valid traffic to be misclassified as malicious when the model not regularly retrained. Software patches, new device additions, or OSINT API modifications might also bring unanticipated features or behaviors which is not expected in the initial model. The proposed architecture combines version-controlled model repositories, drift detection mechanisms for tracking statistical variance in input distributions, and periodic retraining pipelines to help rollback and auditing procedures [10, 16] in order to minimize these risks. In spite of these steps, the computational complexity and deployment restrictions in operational situations make real-time adaptive learning difficult to apply.

4.3. Ethical and Legal Considerations

Integrating Artificial Intelligence with ethical hacking tools raises questions with regard to important ethical and legal aspects that transcends technical restrictions. Privacy incursion is a big problem since programs like Maltego, which mines open-source intelligence (OSINT), could process sensitive or personal information and Snort, which does deep packet inspection, even if it is legally accessible data. This raise concern on privacy and data protection, therefore challenging the limits of ethical cybersecurity practices [4, 20].

There is another major issue in AI model which is discrimination and bias. Machine learning models be trained on biassed datasets and it could lead to inaccurate labelling of traffic or objects as malicious. Mislabeling could result in false allegations and reputational damage in geopolitical or socio-political areas [13, 14].

Moreover, when tools are used across countries, it is necessary to ensure compliance to cybersecurity rules and standards. The most essential is the compliance to laws including the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR), and Malaysia's Personal Data Protection Act (PDPA). Ethical hacking operations must be clearly approved to prevent breaking anti-hacking rules [5, 9]. Incorporating model explainability, privacy-preserving AI methods such data minimization and federated learning, and enforcing rigors access control policies together with thorough audit on logs of AI-driven choices helps to reduce these threats.

5. Use case scenarios

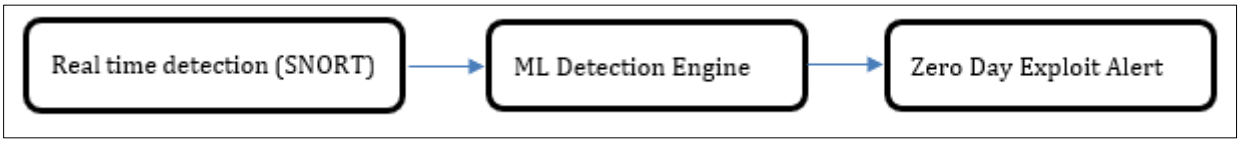
By improving Snort and Maltego's predictive and analytical powers, the suggested AI-integrated architecture is interpreted to address practical security issues. Below three illustrated use cases show how the technology can be used practically in dynamic threat settings.

5.1. Predicting Zero-Day Exploits in Real-Time Traffic (Snort)

Snort as traditional intrusion detection systems (IDS) mostly rely on stationary signatures, hence the capacity to identify zero-day or unknown attacks is limited. In this use case:

- Use of historical traffic data to train machine learning models to detect intricate behavioral patterns such packet sequence anomalies, protocol abuse, or time-based anomalies.
- Autoencoders and Isolation Forest algorithm deployed to detect variations from known "normal" traffic behavior
- AI-enhanced Snort system generates real-time alarms when a zero-day exploit shows unknown traffic characteristics even in the lack of pre-existing rule definitions [2, 10, 11].

Before conventional tools would identify them, this predictive capability helps companies to spot and react to new attack routes.



Adapted from references [2], [10] and [11]

Figure 5 Flow of predictive zero-day exploits in Real-Time Traffic

5.2. Early Identification of Threats via Maltego Graphs

Maltego is widely used for mapping relationships between digital entities. With Artificial Intelligence, this mechanism evolves into a predictive threat intelligence platform:

- AI-enhanced transformations utilizing OSINT feeds and prior threat patterns to assess risk level of domains, IP addresses, and email accounts [6, 7].
- Graph neural networks (GNNs) models are applied to address peculiar or suspicious entity clusters (e.g., multiple known-bad IPs associated with single domain).
- Maltego visually marks high-risk networks for immediate analyst investigation to faciliate early identification of malicious infrastructure or coordinated activities.

This use case enhances the accuracy of threat hunting, ease analysts to prioritize their focus on entities that associated with malicious behavior.

Adapted from references [6] and [7]

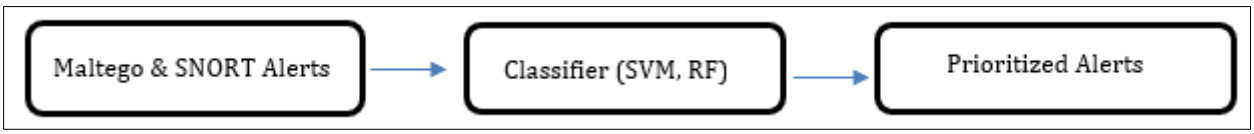
Figure 6 Early detection of threats via Maltego graph flow

5.3. AI-Driven Alert Prioritization

To address alert fatigue that is often suffered by Security operations centers (SOCs) as analysts are overwhelmed due to high volumes of less critical notification:

- AI models classify alerts according to entity patterns, context, behavior, and threat level.
- Likelihood of true positives versus false positives asses by supervised classifiers which trained on historical incident data [2, 14].
- Ranking alerts in real-time to ensure that high-risk or high-confidence anomalies ranked at the top of analyst dashboards.

This method reduces the risk of missed critical alerts due to noise from non-malicious events and improves incident response time.



Adapted from references [12] and [14]

Figure 7 Alert prioritization flow

6. Conclusion

The integration of Artificial Intelligence into ethical hacking tools such as Maltego and Snort has illustrated the substantial potential in enhancing the accuracy, effectiveness, and intelligence of cybersecurity operations. The paper provides an integrated architecture of Artificial Intelligence into two extensively used ethical hacking tools like Snort and Maltego to enable predictive vulnerability detection. Embedding supervised and unsupervised learning models inside the data processing pipelines of various technologies significantly enhances capacities for real-time packet level zero-day exploit detection using Snort, graph-based risk prioritising with OSINT (Maltego) and threat correlation. The automated alert prioritization helps to maximise analyst workflows and lower false positives. The suggested integration push cybersecurity defences from a reactive to a proactive and intelligent response system posture. The system demonstrates strong potential for application in high-risk, real-time environments via continuous feedback loops, model retraining, and adaptive rule generation where threat evolution is constant.

The long-term vision for Artificial Intelligence in cybersecurity extends beyond simple integration with existing tools. Future developments most likely involve federated and transfer learning to support distributed, privacy-preserving model development among different organizations and threat environment. The other technique which is Explainable AI (XAI) to improve trust and interpretability of decisions like high level security operations. Self-learning threat intelligence systems that autonomously adapt to emerging attack path without depending on manual rule modification or update. Besides, autonomous security agent can detect, classify, and mitigate threats in real time with less human intervention. As cyber-attack surfaces increase in complexity and cyber threats evolve in sophistication, integrating AI into ethical hacking frameworks will be crucial for developing durable, scalable, and adaptable defence systems.

Compliance with ethical standards

Acknowledgments

The authors would like to thank all members of the School of Computing who are involved in this study. This study was conducted as part of the Hacking and Penetration Testing Project. Authors extend their appreciation for all the resources and feedback during the investigation of this topic. This paperwork was supported by Universiti Utara Malaysia.

Disclosure of conflict of interest

The authors declare no conflict of interest.

References

[1] EL AERAJ, Ouafae; LEGHRIS, Cherkaoui. “Analysis of the SNORT Intrusion Detection System Using Machine Learning,” International Journal of Information Science and Technology, [S.l.], v. 8, n. 1, p. 1 - 9, may 2024. ISSN 2550-5114. https://innove.org/ijist/index.php/ijist/article/view/251

[2] M. B. Al-Doori and K. M. Ali Alheeti, "AI-Driven Features for Intrusion Detection and Prevention Using Random Forest," Journal of Cybersecurity and Information Management, vol. 16, no. 1, p. 1, 2025, doi: 10.54216/JCIM.160101

[3] Sadargari V, Balaji N. “Enhancing intrusion detection and cloud security by integrating Snort with advanced AI techniques for improved accuracy and threat mitigation”, J Inf Syst Eng Manage. 2025. https://www.jisem-journal.com

[4] Hilario E, Azam S, Sundaram J, et al. Generative AI for pentesting: the good, the bad, the ugly. Int J Inf Secur. 2024;23:2075–97. doi:10.1007/s10207-024-00835-x

[5] Mumtaz A, Javaid T. AI and Ethical Hacking Synergy: Revolutionizing Vulnerability Management. 2025 Mar 1. doi:10.13140/RG.2.2.20510.86086

[6] T. Oakley Browne, M. Abedin, and M. J. M. Chowdhury, “A systematic review on research utilising Artificial Intelligence for open-source intelligence (OSINT) applications,” La Trobe. Journal contribution, 2024. https://doi.org/10.26181/26536642.v1

[7] R. Amgai, " MALTEGO: OSINT Framework and Research Analysis," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol. 9, no. 5, May 2020. www.ijirset.com

[8] H. S. Hamid, M. J. Zaiter, and A. S. G. Behadili, “Snort versus Suricata in intrusion detection,” Iraqi Journal of Information and Communication Technology, vol. 7, no. 2, pp. 73–88, 2024, doi: 10.31987/ijict.7.2.290.

[9] I. Zengeni and M. Zolkipli, “Zero-day exploits and vulnerability management,” Borneo Int. J., vol. 7, no. 3, pp. 26–33, 2024. http://majmuah.com/journal/index.php/bij/article/view/648

[10] I. O. Ibraheem and A. U. Tosho, “Zero-day attack vulnerabilities: Mitigation using machine learning for performance evaluation,” J. Comput. Soc., vol. 5, no. 1, pp. 43–58, 2024. https://doi.org/10.17509/jcs.v5i1.70795

[11] Sarhan, M., Layeghy, S., Gallagher, M. et al, “From zero-shot machine learning to zero-day attack detection,” Int. J. Inf. Secur. 22, 947–959 (2023). https://doi.org/10.1007/s10207-023-00676-0

[12] AbdulRaheem, M., Oladipo, I.D., Imoize, A.L. et al. “Machine learning assisted snort and zeek in detecting DDoS attacks in software-defined networking,” Int. j. inf. tecnol. 16, 1627–1643 (2024). https://doi.org/10.1007/s41870-023-01469-3

[13] A. Manoharan and M. Sarker, "Revolutionizing cybersecurity: Unleashing the power of Artificial Intelligence and machine learning for next-generation threat detection," International Research Journal of Modernization in Engineering Technology and Science, vol. 4, no. 12, pp. –, Dec. 2022. doi: 10.56726/IRJMETS32644.

[14] J. N. Chukwunweike, A. Praise, and B. B. Bashirat, "Harnessing machine learning for cybersecurity: How convolutional neural networks are revolutionizing threat detection and data privacy," International Journal of Research Publication and Reviews, vol. 5, no. 8, 2024.

[15] W. Zheng, J. Gao, X. Wu, F. Liu, Y. Xun, G. Liu, and X. Chen, "The impact factors on the performance of machine learning-based vulnerability detection: A comparative study," Journal of Systems and Software, vol. 168, p. 110659, 2020.

[16] N. Mohamed, H. Taherdoost, and M. Madanchian, "Review on machine learning for zero-day exploit detection and response," in Proc. EAI 3rd Int. Conf. Smart Technol. Innov. Manage. (MTYMEX 2024), H. Taherdoost, Y. Farhaoui, S. R. Shahamiri, T. V. Le, M. Madanchian, and M. Prasad, Eds. Cham, Switzerland: Springer, 2025. doi: 10.1007/978-3-031-64957-8_13

[17] P. Sharma, P. Nand, and P. Sharma, "Intrusion detection and prevention systems using Snort," in Advances in Data Science and Management, S. Borah, S. K. Mishra, B. K. Mishra, V. E. Balas, and Z. Polkowski, Eds., Lecture Notes on Data Engineering and Communications Technologies, vol. 86. Singapore: Springer, 2022. doi: 10.1007/978-981-16-5685-9_46

[18] Klaus Schwarz, Franziska Schwarz, Reiner Creutzburg, "Conception and implementation of professional laboratory exercises in the field of open-source intelligence (OSINT)" in Proc. ISandT Int'l. Symp. on Electronic Imaging: Mobile Devices and Multimedia: Technologies, Algorithms andamp; Applications, 2020, pp 278-1 - 278-10, https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278

[19] M. Kumar and A. Bhandari, "DDoS detection in ONOS SDN controller using Snort," in ICT with Intelligent Applications, J. Choudrie, P. Mahalle, T. Perumal, and A. Joshi, Eds., Smart Innovation, Systems and Technologies, vol. 311. Singapore: Springer, 2023. doi: 10.1007/978-981-19-3571-8_17.

[20] A. Dutta and S. Kant, "An overview of cyber threat intelligence platform and role of Artificial Intelligence and machine learning," in Information Systems Security (ICISS 2020), S. Kanhere, V. T. Patil, S. Sural, and M. S. Gaur, Eds., Lecture Notes in Computer Science, vol. 12553. Cham: Springer, 2020. doi: 10.1007/978-3-030-65610-2_5.