© September 2024 | IJIRT | Volume 11 Issue 4 | ISSN: 2349-6002

A Review on Revolutionizing Security by Combining Signature-based and AI-powered Antivirus Protection Techniques

Zahra Jabeen[1], Khushboo Mishra[2], and Binay Kumar Mishra[3]
[1]*Research Scholar, Veer Kunwar Singh University, Ara, Bihar, India*
[2]*Research Scholar, Veer Kunwar Singh University, Ara, Bihar, India*
[3]*Professor, Veer Kunwar Singh University, Ara, Bihar, India*

Abstract*—Since the level of complexity is rising continuously, a multi-layered approach has always been needed in the current hour to combat an ever-evolving landscape of cyber threats. Traditional antivirus products work solely on a single technology and although they employ diverse types of techniques to detect malware, the speed of such detection algorithms may adversely impact the performance of the antivirus products. Advanced antivirus programs like a combination of signature-based and AI-based detection methods play a crucial part in the line of defense. Certain limitations to Signature-based detection have been pointed out in the paper and the possible strategies in which an amalgamation with Artificial Intelligence could be done is also proposed. This paper will collectively cover various aspects of signature-based and AI-powered detection methods for different types of cyber-attacks, providing useful insights for developing new innovative techniques that will enhance cyber-security measures. We aim to have a brief analysis of the existing techniques of these two working together. In addition, a review has been presented on existing methods and algorithms that are used by signature-based antiviruses and AI-powered tools that dynamically minimize the time and improve the accuracy of virus detection. Finally, we present the current research challenges of using signature-based algorithms and the future scope for investigating cybercrime activities.

***Index Terms*—Cyber-security, Signature, Artificial Intelligence, Antivirus, Threat.**

I. INTRODUCTION

A signature refers to a unique pattern or a byte sequence present in network traffic or inside a file or a series of instructions often symbolized as a fingerprint or DNA sample referring solely to that particular pattern. Apart from a few similar characteristics, each malware type's signature is its own. Signature-based detections create appropriate signatures for each file and compare them with previously detected signatures. This continuous comparison takes place until a match is found and if detected, the particular file is labelled a threat and gets blocked automatically. Hence a signature may also be identified as an IDS rule or a threat signature typically designed by researchers or network defenders who work on identifying and analyzing malicious activity to extract indicators of compromise (IOCs). It allows IDSs to quickly identify malicious behavior transiting the network by searching for a list of known indicators [1].

Multi-cloud environments have opened numerous ways to infiltrate organizations and extract data more frequently than ever before. Signature-based detection isn't capable of finding new attacks without the help of pre-recorded patterns, AI-driven detection is required for that purpose. Using only signature-based detection methods doesn't help detect patterns or indicators of threats that are unknown. As a result, a conjunction of signature-based detections with tools providing context into network behavior is used by security professionals. Signature-based detection methods can work efficiently with techniques like statistical filtering and composite autoencoders. A combination with machine learning algorithms that use signatures or randomized signatures as feature extractors for anomaly detection can also be put into practice for fast and efficient virus detection. In the context of completing financial transactions, signature-based detection can be used with motion detection components to authenticate the identity of the user based on detected motion patterns.

II. LITERATURE REVIEW

Signature-based detection can only reveal what is known; thus, they are just one part of the equation

that cannot protect us from the unseen. Therefore we are required to add AI that thinks like an attacker. One such example is Vectra NDR, which combines signature-based and AI-based detection of real-time behavior. It provides complete visibility and context on both known and unknown attacker methods.

The amalgamation of Signature-based detection techniques and AI-driven detection can offer the following listed benefits-

A. *Coverage*- The consolidated attack telemetry, gives complete visibility across all high-value attack surfaces like network, public cloud, identity, and critical SaaS applications like M365.
B. *Clarity*- AI-driven detection combined with signature-based IOC context to expose all malicious behavior. By correlating and validating threat signals for accuracy, you know what's malicious — so you can focus on real attacks.
C. *Control*- AI Platform helps security team officials accelerate the transition to AI-driven threat detection and response, without sacrificing investments already made in signatures.

III. METHODOLOGY

Signature-based detection is one of the most direct and well-established methods for identifying malicious activity. It examines network traffic, compares it to known signatures, and generates an alert when a match is made. Various approaches can be employed to detect malware using signature-based techniques. One of the methods involved is using machine learning algorithms to extract characteristics from portable runnable files' headers and determine if they are malicious. Few applications combine signatures for known threats with AI-driven behavior-based detection for unknown threats in a single solution, and this solution provides complete coverage, clarity, and control for end-to-end protection against hybrid and multi-cloud attacks [2].

This model will deliver a continuous cycle of attack intelligence based on security research, global and local learning models, deep learning, and neural networks. Global learning involves a full-time group of cyber-security experts and threat researchers who continually analyze attack tools, malware, techniques, and procedures to identify new and shifting trends in the threat landscape. This work will inform the data science models used by Attack Signal Intelligence including supervised machine learning. It is also used to analyze a very large volume of attacking traffic and will distill it down to the key characteristics that make malicious traffic unique. Local learning is aimed at identifying what is normal and abnormal in an enterprise's network for revealing attack patterns using key techniques like unsupervised machine learning and anomaly detection. This amalgamation uses unsupervised machine learning models to gather information about a specific customer environment, with no direct oversight by a data scientist. Rather than concentrating on finding out to report anomalies, they look for indicators of important phases of any attack technique, including signs that an attacker is exploring the network, evaluating hosts for attack, and using stolen credentials. AI-driven prioritization engine will combine thousands of events and network traits into a single detection that uses techniques such as event correlation and host scoring. AI correlates all detection events to specific hosts that show signs of threat behaviors to automatically record every detection and host in terms of the severity of threat and certainty using the threat certainty index. Hence, each event is tracked time to time and after every phase of the cyber-attack, special focus on entities are put, that may be of strategic value to any attacker.

A methodology could be created on five core principles of applied AI for cyber security:

1. Start with the right problem statement.
2. The right data.
3. Build an ML engineering competency.
4. Unlock ML innovation with the platform.
5. Continually validate and improve.

An analysis of over 150 models has been done covering neural networks, supervised ML, unsupervised ML, and novelty detection, 12 references for MITRE D3FEND, and a network effect made up of over 1500 customers continuously validating and improving AI detections for both existing attacker techniques and new ones discovered. Cases were found where it has been found that new attacker techniques and

developed detections before they are published in MITRE ATT&CK which means customers get continuous coverage for new attack techniques without any detection engineering work. AI-powered threat detection algorithms ensure minimal false positives and false negatives also referred as Attack Signal Intelligence and it uses AI to analyze, correlate, and triage thousands of detection events a day spanning networks, clouds, identities, and SaaS applications. Instead of delivering thousands of alerts on individual threat events, our AI platform delivers single-digit alerts per day on prioritized entities for both hosts and accounts that might be under attack.

AI answers the three basic questions that SOC analysts might need to answer when they sit in front of their monitors [3]: Is this threat real? Do I care? And how urgent is it? In other words, is it worth my time and talent?

IV. LIMITATIONS AND CHALLENGES

Challenges of many signature-based detection tools include that it will provide some alert context, which typically is restricted to a narrow alert frame, and will not provide much detail about whatever could have occurred before the alert got fired, or what other activity could have occurred simultaneously. Continuous introduction of finding new ways of exploiting vulnerabilities or producing similar variants of known threats that can elude signature-based detection methods have been happening, resulting in significant blind spots, if any solution relies exclusively on this singular method. Also, it will become challenging for network administrators to keep their signatures current. Automation tools might have updated the working process, but network administrators still need to manually update their databases.

For this reason, the most mature and comprehensive security postures combine signature-based detection and AI-based algorithms to fuse alerts. Increasingly, network detection and response platforms are fusing signature-based and AI-based approaches to create systems that provide a richer context for alerts while helping security teams ignore false alarms.

V. FUTURE SCOPE

Since the level of complexity is rising, the sheer number of Malware attacks is becoming worrisome and has become a serious threat to organizations all around the world. There is no doubt that the rate of development of malware detection technology is evolving at a phenomenal speed but so is the role of malicious actors. Hence it has become so important that researchers and cyber security professionals must utilize emerging technologies to stop malware in its agenda. Introducing new developments and trends in malware detection technology has become fundamentally important ensuring state-of-the-art malware detection methods is always a priority. Meanwhile exploring the challenges and limitations of AI and machine learning implementation in malware detection is key for its utilization in malware detection that combines the modeling of both good and bad behavior introducing a Dual-Engine Defense [4]. It can be a very powerful weapon against even the most advanced malware.

We have seen this happening already with vendor adoption and the use of LLMs to help SOC analysts reduce investigation workload and speed up investigation at times. Potentially, AI can take a step further to make the appropriate response action to stop or isolate the attack. It has been designed to focus first on delivering the most integrated and accurate attack signal by contending the most accurate attack signal, to get the most compelling application of LLMs for effective investigation and response. Phase three of the evolution of the SOC as AI for predictive defense has given an understanding of attacker behaviors i.e. Attack Signal.

VI. CONCLUSION

By integrating these methods, a comprehensive and robust approach to malware detection through signature-based techniques can be achieved [5]. As per the above article presented it is hereby concluded that the most effective approach to malware detection could be, a hybrid model that must combine the best of both protection methodologies. Hybrid methods that use a combination of signature-based and AI-based intrusion detection often cover most of the known and unknown attacks while keeping the number of false positives to a minimum.

Cyber security professionals have to be aware that combining signature-based detection with other methods helps in better protection of servers, files, and data. A hybrid approach secures all levels of company assets thus ensuring its security. It is also evident to note that the greatest possible protection can only be provided by combining the broadest and best layers of security for a defense-in-depth strategy.

REFERENCES

[1]. corelight.com-resources-glossary-signature-based-detection
[2]. vectra.ai : solutions-use-cases-signature ai driven detection
[3]. Mark Wojtasiak, Vice President of Product Marketing, May 1, 2024, Vectra : AI Security, Redefining Cyber Threat Detection with AI
[4]. Matthew G. Gaber, Mohiuddin Ahmed, Helge Janicke; Malware Detection with Artificial Intelligence: A Systematic Literature Review, December 2023, ACM Computing Surveys 56(6), DOI:10.1145/3638552
[5]. Scispace: Home /Questions /What methods go well with signature-based detection method?
[6]. Mohammed Al-Asli, Taher Ahmed Ghaleb, Taibah University, Queen's University: Review of Signature-based Techniques in Antivirus Products, 03 Apr 2019-(IEEE)-pp 1-6
[7]. Bhargav B. March 9, 2023 linkedin : The Revolution: AI & Signature-less Cyber Security