CYBERSECURITY INFRASTRUCTURE AND SECURITY AUTOMATION

Alex Mathew

Department of Computer Science & Cyber Security, Bethany College, WV, USA.

ABSTRACT

AI-based security systems utilize big data and powerful machine learning algorithms to automate the security management task. The case study methodology is used to examine the effectiveness of AI-enabled security solutions. The result shows that compared with the signature-based system, AI-supported security applications are efficient, accurate, and reliable. This is because the systems are capable of reviewing and correlating large volumes of data to facilitate the detection and response to threats.

KEYWORDS

Automation, Cybersecurity, AI, Big data

1. INTRODUCTION

Cyber security threats have become sophisticated and the traditional signature-based security solutions have become quite ineffective. Advanced security solutions that utilize artificial intelligence and machine learning are required to automate information security management. Most organizations depend on their information resources to remain relevant and competitive. A security breach can thus have devastating effects on a company's operations. To enhance the security of their information assets, organizations can leverage AI and ML technologies to automate security management tasks and provide insight into security threats[1]. AI is concerned with information systems that automate complex and complicated tasks necessary for threat detection and mitigation. The systems are capable of analyzing huge volumes of data and identifying patterns that they use to make decisions. Machine learning is a core component of AI that provides computer systems with a means to learn and adapt through experience. The purpose is to examine the effectiveness of AI-based information security solutions in reducing security risks, improving efficiency and addressing common cyber security concerns.

2. THEORY OF RESEARCH

A security solution can be classified as either signature-based or AI-based. Signature-based solutions use rules developed by security experts to detect security threats. These types of security solutions have become ineffective and unreliable due to high rates of false positives[4]. Furthermore, there is usually an element of delay between threat detection and the implementation of countermeasures. The signatures must also be updated regularly to be effective in the long-term. Attackers can take advantage of the delay in releasing or installing updates to compromise the security of an information system[3]. Cybercriminals can also use sophisticated tools to design new threats or sidestep detection when signature-based security systems are used.

DOI:10.5121/acij.2019.10601

Figure one below shows the block diagram of an AI-driven information security solution. In the diagram, data from different sources such as intelligence feed, the indication of compromise, system logs, network traffic, and historical data are used to support supervised, unsupervised learning and reinforcement learning mechanisms. After learning, the system uses an identity tracker to detect rare and evolving patterns that may indicate new attacks[5]. The identity tracker comprises of behavior analytics and fuzzy logic systems. The tracker goes through various types of analyses such as reasoning, contextual and future impacts analyses[4]. The analyses allow the system to detect new and evolving threats so that appropriate deterrence responses can be taken. The system then identifies ranks and displays the key issues on a dashboard. It is important to note that the security system incorporates an automated response engine that enables it to respond to threats automatically without the intervention of an administrator.

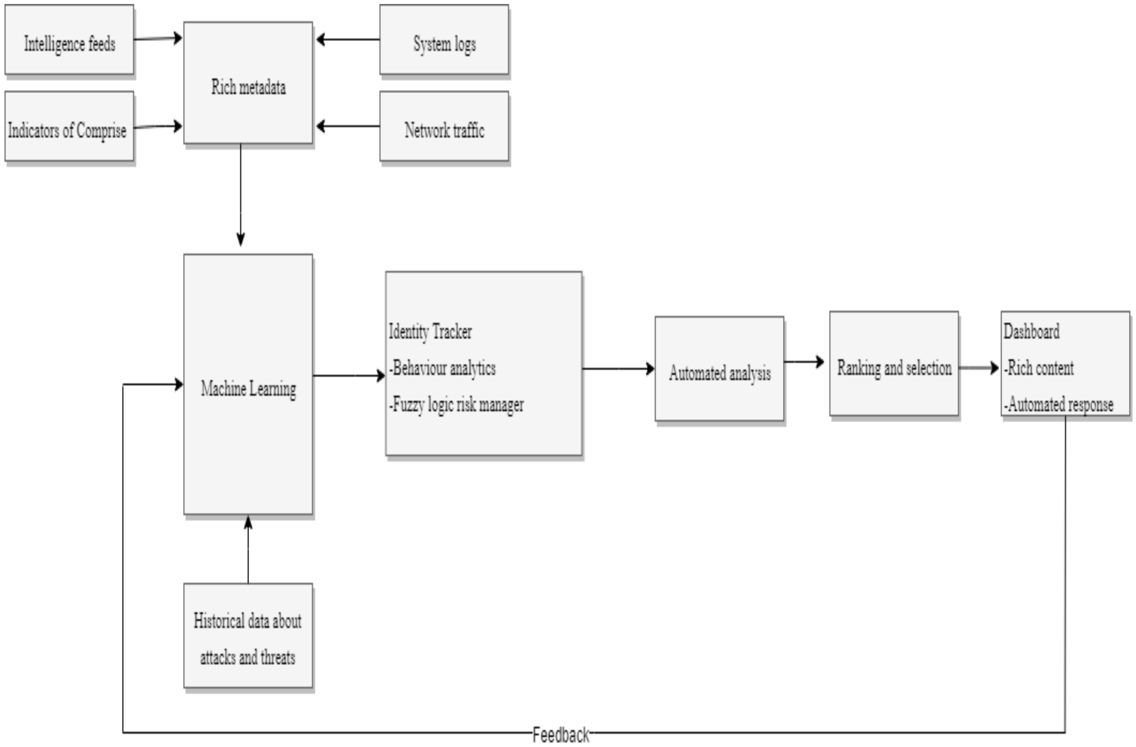


Figure 1: block diagram of an AI-driven security solution

3. PROPOSED METHODOLOGY

The case study methodology is used to examine the performance of two AI-based security solutions. The methodology involves intensive investigation or exploration of a phenomenon. The case study methodology was selected because it allows for comparison of different aspects of AI-based security systems and signature-based systems. Besides, the method allows for a comprehensive examination of the subject under investigation. It is also possible to locate deviant cases which can reveal new information about the subject being studied. The case study methodology is however associated with a high risk of biased data collection and interpretation[9]. Deep Instinct and Darktrace security solutions are used as case studies.

4. ALGORITHMS

To be effective, AI-driven security solutions use some forms of supervised, unsupervised or reinforced learning algorithms. Supervised learning algorithms are vital in situation assessment. The algorithms are used to examine past experiences, prevailing situations and future impact of identified issues[5]. The main analyses undertaken by the algorithms include reasoning, context, and risk analysis. Reasoning analysis helps the security system to understand the goal, purpose, and reason for a course of action. The context analysis is used to study the background and relationships of key security events in a computing environment[6]. Finally, risk analysis is used to examine the advantages and disadvantages of possible causes of action. The three analyses form the basis for selecting available actions in supervised algorithms. In unsupervised algorithms, the analyses are used to create new actions that are appropriate for emerging and evolving threats. In the reinforced learning algorithms, the three analyses are used to identify similar patterns.

It is noteworthy that available options are usually preloaded on AI-driven security systems. As such, supervised algorithms can make prompt responses based on the characteristics of an identified security event. In contrast, unsupervised learning algorithms learn from the data as they access it. This makes it possible to customize responses based on new information or respond to a threat dynamically[7]. Unsupervised algorithms are thus used to create new options in AI-driven security systems. Reinforcement learning algorithms are used to select the most suitable option based on the results of a cost-benefit analysis.

Various AI-driven security solutions used different types of algorithms. The algorithms can be proprietary or publicly available. For example, Deep Instinct utilizes static file analysis and threat prediction modeling to detect and eliminate threats autonomously. The application uses deep learning algorithms to learn to anticipate new attacks[7]. Its developers built a neural network in the laboratory then trained it with a large dataset of malicious codes[6]. Deep Instinct, therefore, uses predictive algorithms to determine whether an application is malicious or not. The security solution is capable of continuous learning as it comes across new data sets. When Deep Instinct accesses a suspicious application, its algorithm breaks the software into small snippets for analysis[11]. The security system operates similarly as genomic sequencing where small sequences are used to teach neural networks so that they can identify unique patterns. To support the required complex computations, Deep Instinct uses GPU clusters.

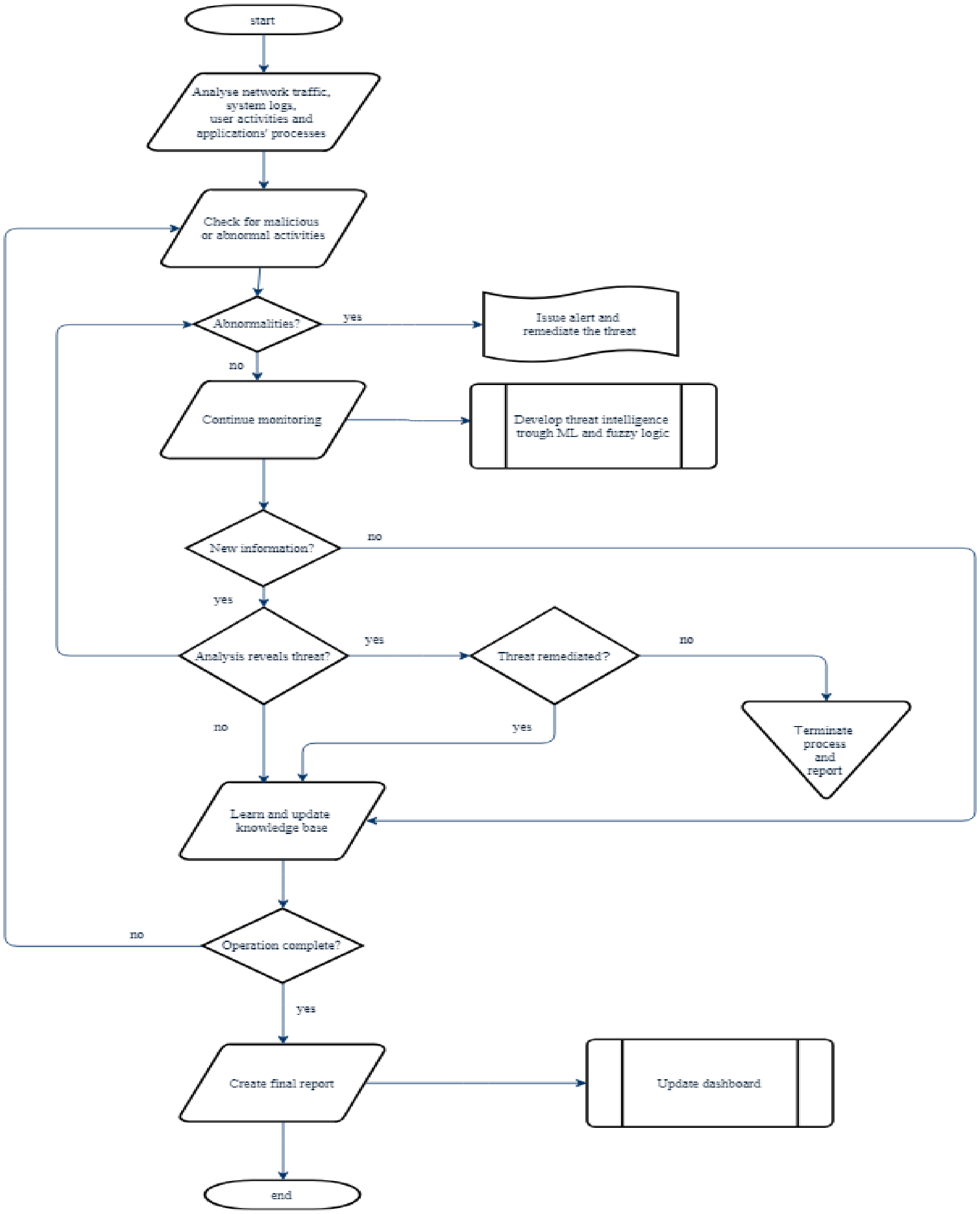

start
Analyse network traffic, system logs, user activities and applications' processes
Check for malicious or abnormal activities
Abnormalities?
yes
Issue alert and remediate the threat
no
Continue monitoring
Develop threat intelligence trough ML and fuzzy logic
New information?
no
yes
Analysis reveals threat?
yes
Threat remediated?
no
Terminate process and report
no
yes
Learn and update knowledge base
no
Operation complete?
yes
Create final report
Update dashboard
end

Figure 2: AI-Driven security system processes

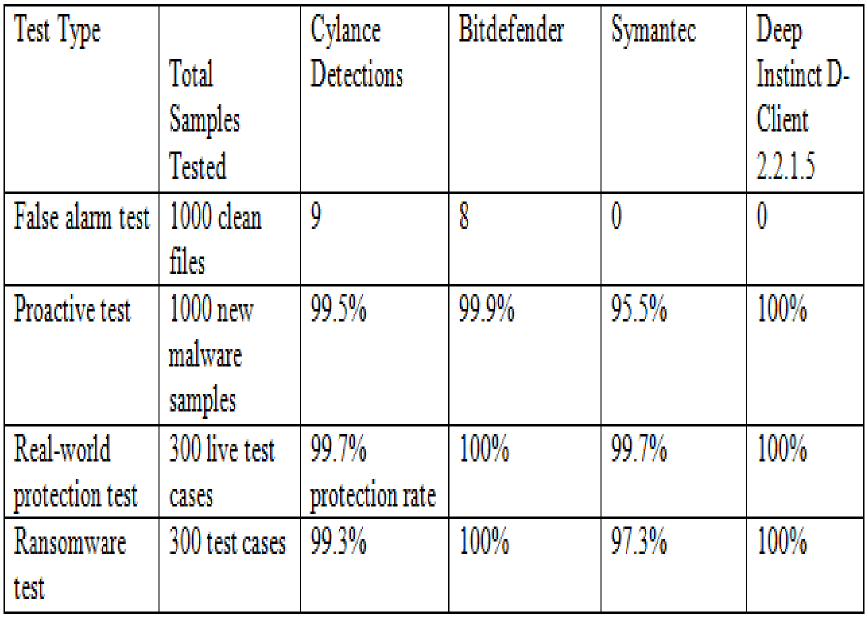
Figure two above shows a flow chart depicting common processes used by AI-drive security system. The flow chart begins with the analysis of data from various sources. The collected data is then checked for malicious applications or activities. If something abnormal is identified, the system issues an alert and remediates the issue. Afterward, it continues monitoring new information to detect threats and learn. When a security operation is complete, the system creates a final report and updates its real-time dashboard.

5. Results Analysis

Table one below shows the result of tests performed by a third party security company called AV-Comparatives on popular AI-driven endpoint security solutions. The goal of the tests was to gauge the automatic prevention and detection capabilities of some popular AI-driven cyber security solutions. Proactive, real-world protection and ransomware tests were conducted 11. During the real-world protection testing that was based on 300 live test cases such as malicious URL and email vector, Deep Instinct and Bitdefender were capable of offering 100% protection rate. Cylance and Symantec both recorded a 99.7% protection rate during real-world testing.

The proactive testing framework was used to gauge the ability of security solutions to detect unknown and evolving threats. The products' definitions were frozen before the test. 1000 new and verified malware samples were tested against each of the applications. The results show that Deep Instinct returned 100% protection rate while Bitdefender recorded a 99.9% protection rate. On the other hand, Cylance and Symantec registered 99.5% and 95.5% protection rates respectively.

The ransomware test gauged the effectiveness of the security systems at detecting and blocking ransomware. A sample consisting of a variety of new ransomware was used. Bitdefender and Deep Instinct each recorded 100% protection rate. Cylance and Symantec recorded 99.3% and 97.3% protection rates respectively during the test. The false alarm test was conducted to verify that the applications do not block legitimate applications. Out of 1000 clean files, Deep Instinct and Symantec did not issue any false alarm. Bitdefender issued 8 false alarms while Cylance issued 9.



Test Type	Total Samples Tested	Cylance Detections	Bitdefender	Symantec	Deep Instinct D-Client 2.2.1.5
False alarm test	1000 clean files	9	8	0	0
Proactive test	1000 new malware samples	99.5%	99.9%	95.5%	100%
Real-world protection test	300 live test cases	99.7% protection rate	100%	99.7%	100%
Ransomware test	300 test cases	99.3%	100%	97.3%	100%

Table 1: Test results for selected AI-driven systems

The results show that all the four AI-driven products are very good at detecting and blocking common threats including malicious scripts, applications, and ransomware.

The security systems are also capable of detecting and responding to unknown and evolving threats with accuracy. This is because they utilize machine learning techniques to learn about unknown threats. This is in contrast with traditional security systems that depend entirely on set rules, known signatures, behavioral analysis and prior knowledge to detect malicious applications. The AI-enabled solutions are therefore capable of recognizing emerging threats that circumvent traditional security systems. They are therefore ideal in setting up automated security in organizations. Once deployed, the security team will hardly ever need to manually configure or update the tools. The tools will run without fail and will keep updating their threat knowledge to incrementally become more effective at sealing any IT security loopholes.

6. CONCLUSION

AI-based cyber security solutions have unmatched performance when compared to signature-based tools. The AI-based systems use artificial intelligence to detect significant deviations that are then correlated to identify genuine threats with minimum floods of false positives. The security systems are also capable of monitoring, detecting and remediating threats autonomously. The examination of AI-based security solutions shows that they leverage patented machine learning technologies to improve their effectiveness. Moreover, the solutions use a mixture of approaches including behavioral analysis and signature-based threat detection. While machine learning is used to train the systems and support automation, behavioral analysis is used to combat modern-day malware. Security tools based entirely on behavioral analysis are prone to a high number of false positives. This is why AI-based tools do not solely depend on the increasingly defective conventional threat detection technologies. As advancements are made in computing, AI-based tools will become more efficient at ensuring the security of organizations without human assistance.

REFERENCES

[1] AV-Comparatives, Advanced Endpoint Protection Test, AV-Comparatives, 23 March 2018, https://www.av-comparatives.org/tests/advanced-endpoint-protection-test/

[2] IBM. “Artificial intelligence for a smarter kind of cybersecurity.” IBM, 16 August 2018, https://www.ibm.com/security/artificial-intelligence

[3] Joshi, Naveen, “Can AI Become Our New Cybersecurity Sheriff?” Forbes, Feb. 4 2019, https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#6d981a6f36a8

[4] Mandt, Ej. “Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations", Journal of Information Warfare, vol. 16, no. 1, pp. 31-48. 2017.

[5] Mitkovskiy Alexey, Ponomarev Andrey and Proletarskiy Andrey. “SIEM-Platform for Research and Educational Tasks on Processing of Security Information Events.” The International Scientific Conference eLearning and Software for Education Bucharest. Vol. 3, pp 48-56. 2019.

[6] Powell, Matt. “Artificial Intelligence: A Cybersecurity Solution or the Greatest Risk of All?” CPO Magazine, April 15, 2019, https://www.cpomagazine.com/cyber-security/artificial-intelligence-a-cybersecurity-solution-or-the-greatest-risk-of-all/

[7] Panimalar Arockia, Pai Giri and Khan Salman, Artificial intelligence techniques for cyber security. International Research Journal of Engineering and Technology, Vol. 5, no. 3. pp. 122-124. 2018.

[8] Siddiqui Zeeshan, Yadav Sonali and Husain Mohd. Application of Articicial Intelligence in fight against cyber crimes: A review. International Journal of Advanced Research in Computer Science, Vol. 9, no. 2, pp. 118-121. 2018.

[9] Starman, Adrijana. “The case study as a type of qualitative research.” Journal of contemporary educational studies vol. 1. pp.28-43. 2013.

[10] Veeramachaneni, Kalyan and Arnaldo, Ignacio. “AI2: Training a big data machine to defend.” MIT, [10] July 2016, https://people.csail.mit.edu/kalyan/AI2_Paper.pdf

[11] Vahakainu, Petri and Lehto, Martti. Artificial Intelligence in the Cyber Security Environment, Academic Conferences International Limited, Reading. 2019.

AUTHOR:

Alex Mathew Ph.D., CISSP, CEH, CHFI, ECSA, MCSE, CCNA. Security+