Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cybersecurity: The Relationship Between Artificial Intelligence and Threat Detection

Néstor Eduardo Figueroa Cardona[1,2], Alexander Gordillo Gaitan[2]

[1]Systems Engineer, Computer Security specialist, Master's Degree in Educational Technology Management.
[2]Corporación Universitaria Minuto de Dios,
Email: Nestor.figueroa@uniminuto.edu

The symbiotic relationship between cybersecurity and artificial intelligence has led to the development of sophisticated threat detection systems. The proliferation of cybercrime and illicit access to information systems, traffic and packet analysis in computer network infrastructure, and sophisticated deep learning models such as convolutional neural networks and generative adversarial networks have collectively empowered an unprecedented ability to analyze data streams in real time and detect anomalies. Additionally, AI is employed in the identification of zero-day vulnerabilities through automated code scanning and in the expeditious response to attacks through the use of automation systems and security orchestration. However, the implementation of AI in cybersecurity presents a number of legal and ethical challenges, including the need to ensure the fairness of algorithms, the protection of private and public corporate entities, and the improvement of user data integrity. These issues require constant monitoring and the application of IDS, IPS, and SIEM technical controls in accordance with ISO 27001 regulations. The implementation of Cybersecurity-AI solutions reflects automation in repetitive tasks and offers the potential for improved and faster responses to new threats.

Keywords: Cybersecurity, Artificial Intelligence, Deep Learning, Threat Detection, Incident Response.

1. Introduction

In the field of cybersecurity, the integration of artificial intelligence (AI) with threat detection has resulted in the development of innovative systems that significantly alter the landscape of digital protection. The potential of this integration lies in the capacity of deep learning models, including convolutional neural networks and generative adversarial networks, to conduct real-time analyses of network data and identify nuances that are beyond the scope of human perception. These systems, which are imbued with unparalleled artificial intelligence, are capable of sophisticated surveillance and the detection of even the most evasive threats.

However, this novel approach to cybersecurity is not without its inherent complexities. Artificial intelligence (AI) presents a dual-edged sword, offering a novel approach to identifying zero-day vulnerabilities through automated code exploration and enabling rapid response to intrusions through task automation systems and security orchestration. This technological evolution is inextricably intertwined with significant legal and ethical challenges, including the imperative to guarantee fairness in the algorithms used and to jealously preserve user privacy in an increasingly monitored and threatened digital landscape.

The implementation of technical controls, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM), in accordance with the ISO 27001 standard, serves to establish a robust framework for information security management. These controls serve as indispensable cornerstones, facilitating a swift and automated response to cyber threats and thereby ensuring a robust defense in digital environments.

Furthermore, the incorporation of AI-based cybersecurity solutions not only enhances the automation of repetitive tasks but also markedly enhances responsiveness to the continual evolution of digital threats. This symbiotic relationship between established technical controls and AI technologies not only optimizes operational efficiency but also enhances organizations' capacity to adapt and proactively address emerging challenges in the cybersecurity landscape.

This article therefore seeks to examine the complex and pivotal relationship between cybersecurity and AI, investigating recent developments, the challenges they present, and the prospective solutions to computer security.

1. Deep Learning

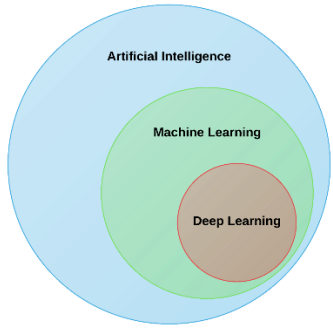

Figure 1: Euler diagram on artificial intelligence.

Deep learning has been identified as an emerging field of research in machine learning, receiving increased attention in recent years (Institute for Intelligent Systems and Experimental Teaching of Robotics et al., 2021). The implementation of deep learning techniques in the domain of cybersecurity has led to the emergence of a threat detection paradigm characterized by unprecedented complexity and sophistication. Deep learning represents a subfield of machine learning that is distinguished by its reliance on multi-layered artificial neural networks (also known as deep neural networks) for the purpose of learning

and representing complex patterns in data.

The initial successful deployment of deep learning can be attributed to Geoffrey Hinton, who introduced deep belief networks comprising a network layer and a restricted Boltzmann machine (RBM) for the initial assignment of synaptic weights. The model comprised both supervised and unsupervised learning techniques, with its primary structure comprising multiple layers of artificial neural networks. These networks were capable of learning a hierarchical representation in deep architectures. (Viteri et al., 2022)

Two key models of deep learning are the Convolutional Neural Network (CNN) and Generative Adversarial Network (GAN) models, which represent the pinnacle of this evolution. Capable of capturing feature hierarchies in high-dimensional data, convolutional neural networks (CNNs) have been demonstrated to be effective in extracting intricate patterns in network traffic flows, thereby facilitating the early detection of camouflaged threats.

Conversely, GANs, through their capacity to generate synthetic samples that closely resemble authentic data, permit the construction of digital traps for cybercriminals. This enables the identification of anomalous behavior with unparalleled accuracy, which is an essential attribute in the detection of latent threats. GAN-based systems are capable of continuous adaptation and evolution, enabling them to remain at the forefront of evolving attack tactics.

This symbiotic relationship between deep learning and cybersecurity, exemplified by convolutional neural networks (CNNs) and generative adversarial networks (GANs), represents a pivotal shift in threat detection capabilities, redefining the manner in which digital environments are safeguarded. This technological convergence portends a future where anticipation and adaptability in cybersecurity are the norm, offering an unparalleled level of security in a world that is increasingly digitized and exposed to sophisticated threats.

2. Cybersecurity

Ballestero (2020) notes that the term "cybersecurity" has become pervasive in contemporary society, reflecting the increasing reliance on digital technologies across all facets of modern life. In addition, a number of related terms have emerged, including cybercrime, cyberterrorism, cyberattack, and cyberdefense, which collectively refer to the threats that exist with regard to information security in cyberspace.

Cybersecurity entails the implementation of intrusion detection systems, advanced firewalls, two-factor authentication, and robust password management policies, among other strategies. Furthermore, it is imperative to maintain a state of constant vigilance and to update cyber defenses in order to ensure the continued integrity of systems in an environment characterized by the constant emergence of new digital threats. Cybersecurity is the capacity to withstand, with a certain level of reliability, any action that compromises the availability, authenticity, integrity, or confidentiality of the data stored or transmitted, or of the services offered. (Ballestero, 2020)

In the digital realm, cyberattacks represent an increasingly prevalent danger. Among the most prevalent forms are SQL injection, Cross-Site Scripting (XSS), and distributed denial-of-service (DDoS) attacks. These malevolent techniques are employed by cyber actors with the objective of compromising the security of systems and applications. This is achieved by exploiting vulnerabilities in the interaction between users and servers, which can result in a

number of consequences, including database manipulation, code execution in users' browsers, or the saturation of online resources. In this context, it is of the utmost importance to gain a comprehensive understanding of each of these attacks.

3. The role of artificial intelligence in cybersecurity

The convergence of artificial intelligence (AI) and cybersecurity has emerged as a cutting-edge paradigm that demands immediate attention from governments and businesses in their efforts to enhance cyber defenses. As asserted by the Department of Computer Engineering at the University of Coimbra (2021), systems based on artificial intelligence (AI) have become a tangible reality, offering a multitude of solutions across diverse domains, including health, education, and service automation. The role that artificial intelligence, and in particular machine and deep learning, has been assuming in the field of personal and business cybersecurity is beyond question. As a result, the technological landscape is in a state of constant evolution, which is occurring concurrently with an increase in cybercrimes and cyberattacks. Innovations in this field are leading to an escalation in the complexity and intricacy of the security challenges that must be addressed (Martínez, 2020).

As Martínez (2020) notes, the primary advantage of AI in cybersecurity is its capacity to learn in real time and develop new classification criteria autonomously, without the need for human intervention. Furthermore, it is imperative to implement comprehensive monitoring of anomalous activity within the network traffic of a web portal or device, as this significantly streamlines the security process.

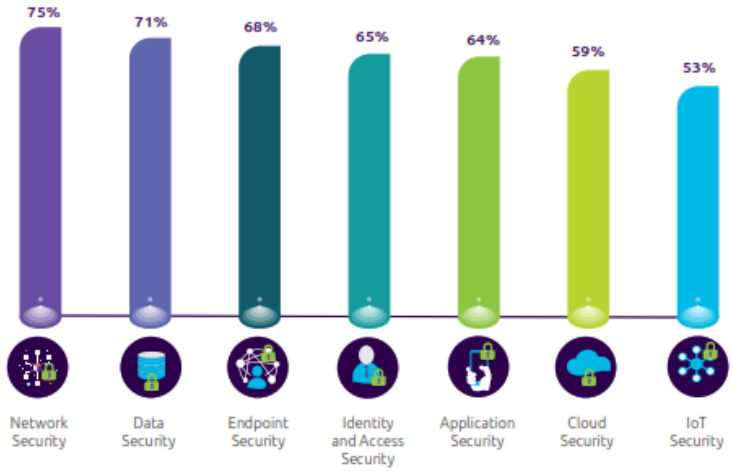

Figure 2: Executive Survey on AI in Cybersecurity (Capgemini Research Institute, n.d.)

3.1 Attack vectors: relationship between Cybersecurity and Artificial Intelligence.

In the fields of cybersecurity and computing, the term "attack vector" is used to describe the method or pathway by which a system or network is compromised or attacked. An attack vector can be defined as any means by which an attacker seeks to exploit vulnerabilities in a system or network to achieve a desired outcome. This may include the theft of information, the interruption of service, or the acquisition of unauthorized access, among other potential

actions.

The nature and complexity of attack vectors can vary considerably. Some illustrative examples of attack vectors include:

A. Phishing: Phishing attacks involve using fake emails, instant messages, or other communication methods to trick users into revealing sensitive information, such as passwords or credit card information.

- AI-Enhanced Social Engineering Phishing: Attackers could use AI to analyze social media profiles, past emails, and other publicly available information about potential targets. This could allow them to personalize phishing messages in a much more effective way, using specific information to make emails appear more authentic and convincing.

- AI Phishing Content Generation: Attackers could use natural language generation algorithms to create phishing emails that are almost indistinguishable from legitimate emails. These algorithms could be trained on large datasets of authentic emails to accurately mimic the tone, style, and format of genuine communications.

- AI-Targeted Phishing: AI could be used to identify and segment specific targets for phishing attacks, analyzing large amounts of data to find people with specific roles in organizations or with demographic characteristics that make them more likely to fall victim to phishing. This could allow attackers to send highly personalized phishing messages targeted to specific individuals.

3.2 Cross-Site Scripting (XSS)

As posited by Weamie (2022), cross-site scripting (XSS) vulnerabilities exploit the fact that web applications execute scripts in users' browsers. If a user manipulates a dynamically generated script, it can result in the compromise of an online page. An XSS attack can be initiated on any susceptible website written in any programming language (Weamie, 2022).

XSS attacks are typically characterized by the injection of malicious code, predominantly in JavaScript. However, as previously stated, any programming language is vulnerable to this type of attack. Additionally, there are multiple methods through which an XSS can be executed:

1) Reflected XSS: Malicious code is injected into an HTTP request, usually through a URL or web form. The server receives the request and returns a response that includes the injected code, which runs in the user's browser.

2) Stored XSS: Malicious code is stored on the web server and delivered to users when they access a specific page. Typically, data entry areas, such as comments on a forum or blog posts, are used to inject the malicious code.

3) DOM-based XSS: Malicious code modifies the DOM (Document Object Model) in the user's browser. The attacker usually exploits the way the web page processes data and performs unexpected or harmful actions on the user interface.

4) XSS by Mutation XSS: This type focuses on the manipulation of objects, e.g., JavaScript through the mutation of properties and methods. Attackers can exploit

vulnerabilities in the web application that allow JavaScript objects to be modified at runtime, which can lead to unexpected or harmful behavior.

3.3 DDOS

A distributed denial-of-service (DDoS) attack is a malicious attempt to flood a target, such as a server, with an overwhelming volume of network traffic. This traffic is usually generated through a network of compromised systems, which are known as "bots" or "zombies." The goal of this attack is to overload the victim's processing power and bandwidth, thereby causing an interruption to its services. This interruption renders the services inaccessible to legitimate users and causes a significant or complete degradation of the online functionality of the victim. A DDoS attack is a type of network attack that results in the victim server's resources being taken over, leading to system outages or error messages (Lee et al., 2020).

A distributed denial-of-service (DDoS) attack is initiated from a multitude of interconnected devices by introducing traffic with falsified source IP addresses into the targeted host, thereby impeding legitimate user access (Lee et al., 2020). When these attacks are orchestrated using AI techniques, they can become even more sophisticated and challenging to mitigate. Artificial intelligence can be employed at various stages of a DDoS attack, including target identification and the generation of malicious traffic.

Methodology

The increasing prevalence of cybercrime and the advancement of attack vectors have underscored the necessity for the implementation of robust security measures within organizational frameworks. The ISO 27001:2022 standard underscores the critical role of cybercrime mitigation through the implementation of essential technical controls. Among these, Intrusion Detection Systems (IDS) merit particular attention, as they facilitate the early detection of malicious activities on the network, thereby generating alerts that can be acted upon with minimal delay. Furthermore, Intrusion Prevention Systems (IPS) supplement this functionality by proactively blocking malicious traffic, thereby reinforcing network security and reducing susceptibility to potential attacks.

Moreover, Security Information and Event Management (SIEM) provides a comprehensive view of information security by correlating and analyzing data from diverse sources. This solution enables the identification of anomalous patterns and trends, thereby facilitating an efficacious response to security incidents. The implementation of these technical controls in accordance with the ISO 27001:2013 standard serves to enhance organizations' capacity to safeguard their vital information assets and to mitigate a multitude of cyber threats.

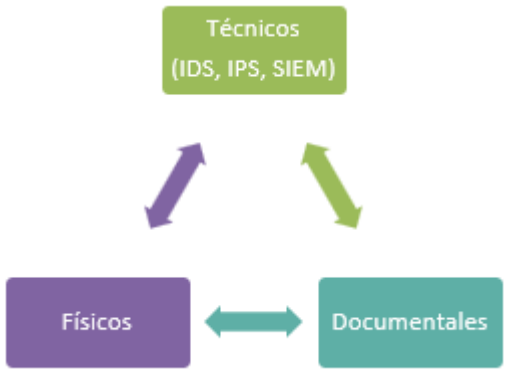

Figure 3: Controls to mitigate vulnerabilities and cyberattacks, ISO 27001 (ISO 27001)

The implementation of artificial intelligence (AI) helps mitigate the problem of false positives in intrusion detection, automate manual processes in incident detection and computer security.

Phase 1: Cybersecurity (AI) Tools

- Snort: Snort is a free, open-source intrusion detection (IDS) and intrusion prevention (IPS) system. It works by analyzing network traffic for patterns that match predefined rules, which indicate malicious or suspicious activity. The integration of artificial intelligence (AI) into Snort emerges as a solution to overcome these limitations, enabling more accurate traffic analysis, emerging threat detection, task automation, and false positive reduction.

- Meerkat: It is an open-source, high-performance intrusion detection (IDS) and intrusion prevention (IPS) system, real-time intrusion detection and prevention, network traffic analysis, and suspicious pattern search. By integrating AI with Suricata, it is possible to develop automatic threat response systems. For example, Meerkata can be configured to take immediate action to block or mitigate a threat as soon as it is detected, without human intervention, speeding up response to security incidents.

- Fortinet Fortiguard AI: Uses artificial intelligence techniques to improve the detection, response, and mitigation of cyber threats. By integrating AI into its security platform, FortiGuard AI helps organizations protect networks, data, and assets against a wide range of ever-evolving threats.

FortiGuard AI reduces false positives and improves detection accuracy when analyzing large volumes of security data. This allows security teams to focus on real threats and respond more effectively to incidents.

- IBM Security QRadar: A suite of security products designed to help organizations detect, investigate and respond to cyber threats. It focuses on Security Information and Event Management (SIEM), which means it collects and analyzes data from various security sources in your network to identify potential security incidents, integrates with threat intelligence feeds to stay up-to-date on the latest cyber threats and vulnerabilities.

QRadar can collect logs and events from firewalls, intrusion detection systems, endpoints, and other security tools. It then analyzes this data to identify patterns and potential security

incidents.

- Microsoft Azure Sentinel: Microsoft Azure Sentinel is a cloud-native Information Security and Event Management (SIEM) platform offered as part of Microsoft Azure. It is designed to help organizations detect, investigate, and respond to cybersecurity threats.

Think of Azure Sentinel as a security command center that unifies security information from different sources to give you a holistic view of your environment, AI-powered security analytics capabilities and machine learning help identify emerging and sophisticated threats. It uses artificial security intelligence (IS) and machine learning (ML) to detect threats in real-time and prioritize alerts.

- Amazon Guardduty: A cloud-based threat detection service offered by Amazon Web Services (AWS). It is designed to help organizations continuously monitor their AWS accounts and workloads for malicious activity and threat indications. It uses security intelligence and machine learning to identify anomalous patterns and activity that could indicate a threat. You can scan Amazon Elastic Block Store (EBS) volumes attached to EC2 instances or container workloads for malware, worms, cryptominers, and other potential threats.

Nombre	Protocolos	Tipo de IA
Snort	IP, TCP, UDP, ICMP, HTTP, FTP, DNS, SMB, SNMP, Telnet, POP3, IMAP, SMTP, NFS, RPC, IPX, AppleTalk, etc.	No implementa IA directamente, pero se integra con herramientas de Machine Learning para análisis de tráfico y generación de reglas.
Suricata	IP, TCP, UDP, ICMP, HTTP, FTP, DNS, SMB, SNMP, Telnet, POP3, IMAP, SMTP, NFS, RPC, IPX, AppleTalk, GRE, IPv6, SCTP, DHCP, Radius, Kerberos, etc.	No implementa IA directamente, pero se integra con herramientas de Machine Learning para análisis de tráfico y clasificación de anomalías.
IBM Security QRadar	IP, TCP, UDP, ICMP, HTTP, FTP, DNS, SMB, SNMP, Telnet, POP3, IMAP, SMTP, NFS, RPC, IPX, AppleTalk, GRE, IPv6, SCTP, DHCP, Radius, Kerberos, NetFlow, JFlow, sFlow, CEF,syslog, etc.	Machine Learning para detección de anomalías, análisis de comportamiento de usuarios, correlación de eventos y respuesta a incidentes.

Figure 4: Distribution of Snort, Meerkat, and IBM QRadar protocols (own source)

Phase 2: Laboratory

The following network diagram illustrates the configuration requirements for establishing a secure network environment, with the objective of enhancing the overall network security. The objective of this project is to implement the Snort and Meerkata tools on key devices, including switches and the internet provider's router. The central processing unit (CPU) will host the firewall, rules, and configuration for the protection of the network and its services on the server, including applications and databases. In order to achieve this objective, two network cards will be utilized in the CPU: a WAN network card and a LAN network card.

- Network Diagram

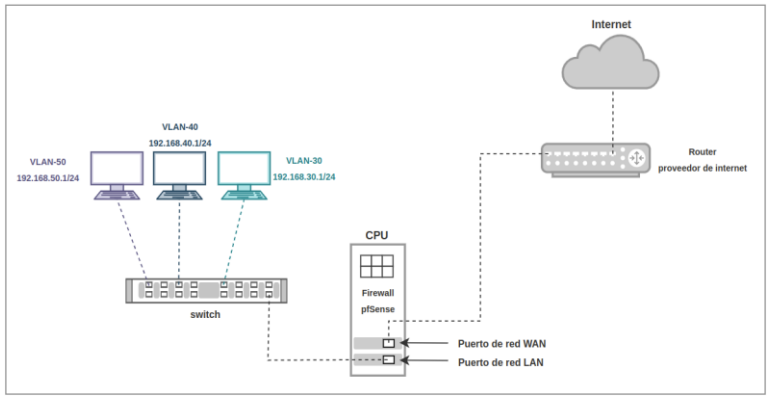

Figure 5: Network diagram for configuring Snort and Meerkat in a secure network environment. Source: Own elaboration

- Installing IDS/IPS: Snort and Meerkat were downloaded and installed from the official website or using your operating system's package manager.

- Rule Configuration: The rules archive has been configured to mitigate DOS attacks, brute force, unusual traffic analysis, port scanning, and finally Cross-Site Scripting (XSS).

- Configuring the Network Interfaces: To assign the IP address (192.168.1.254) with subnet mask (24) to the LAN network interface, we repeated the same steps that were performed to assign the IP to the WAN interface.

Phase 3: Deploy tools

- Operating Mode Configuration: IDS/IPS has been configured to operate in IDS (intrusion detection) mode.

- Notification and Alert Configuration: The security policies that the IDS will apply have been defined as: blocking malicious traffic, security alerts, XSS, brute force attack, DOS attack, DDOS, port scanning alerts.

Proceeded to configure

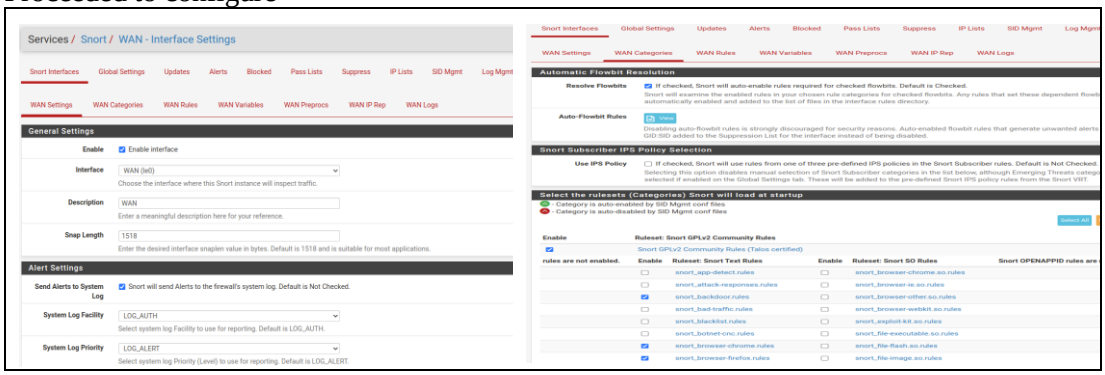

Figure 6: Deployment of Snort and Meerkat tools (own source)

- Notification and Alert Settings: The IDS/IPS will notify and alert about detected security events to email and real-time event logs and notifications through management interfaces.

- Testing and Adjustments: Extensive testing was conducted to verify the effectiveness and accuracy of the IDS/IPS, the configuration was well reviewed for intrusion detection performance and accuracy, based on the attack vectors named above.

- Implementation in Production: Once all the implementation and configuration were completed, the necessary tests were carried out, verifying the implementation of the IDS/IPS in production.

Phase 4: Identification of attack vectors

Table 1 Attack vector identification in Snort and Meerkata

Snort	Meerkat
Port Scanning Detection	Port Scanning Detection
DOS Attack	DOS Attack
Unusual traffic analysis	Unusual traffic analysis
Brute Force Attack	Brute Force Attack
Cross-Site Scripting (XSS)	Cross-Site Scripting (XSS)

Note: In the configuration of the laboratory services, these attack vectors were raised, to check the efficiency of the Snort and Meerkat tools, source: own.

A series of systematic tests were conducted in a laboratory setting to evaluate the effectiveness of the Snort and Meerkat tools in detecting intruders. The aforementioned tests are based on the various attack vectors delineated in Annex Table 1, which encompass a comprehensive array of prevalent threats.

Each attack vector is replicated in a controlled environment, thereby emulating conditions and scenarios that might occur in the real world. The response of the Snort and Meerkat tools to each attack is monitored and evaluated:

- Detection capacity: It is analyzed if the tools correctly detect the attack and generate the corresponding alerts, categorizing into: known attack and detection of new attacks.

- Accuracy of the alerts: It is verified if the alerts generated are accurate and relevant to the attack in question, avoiding false positives or negatives.

- Response time: The time it takes for tools to detect the attack and generate the alert is measured, which is crucial for a rapid response to intrusions.

- System impact: Observes whether running the tools affects system performance or generates additional resources.

- False positives: Verify the accuracy of alerts, if there are false positives.

- Compare the effectiveness of both tools: It is possible to determine which tool offers better performance in intrusion detection, considering different types of attacks.

- Improve the security posture against AI attacks: Informed decisions can be made about the implementation of the tools in the real environment, selecting the most appropriate option for the specific needs of the organization in the event of any attack event with artificial intelligence.

- Optimize tool configuration: Snort and Meerkat's rules and parameters can be adjusted to improve their accuracy and efficiency in detecting attack vectors.

Phase 5: Results

The penetration tests were conducted using a variety of techniques, including pentesting, black-box testing, and white-box testing. These tests were implemented using a range of security tools. In two scenarios, Snort and Meerkata were deployed and configured with the respective rules to safeguard the integrity, confidentiality, and availability of the laboratory exercise information in a controlled environment. The security of these two solutions was then attacked, and the results are as follows:

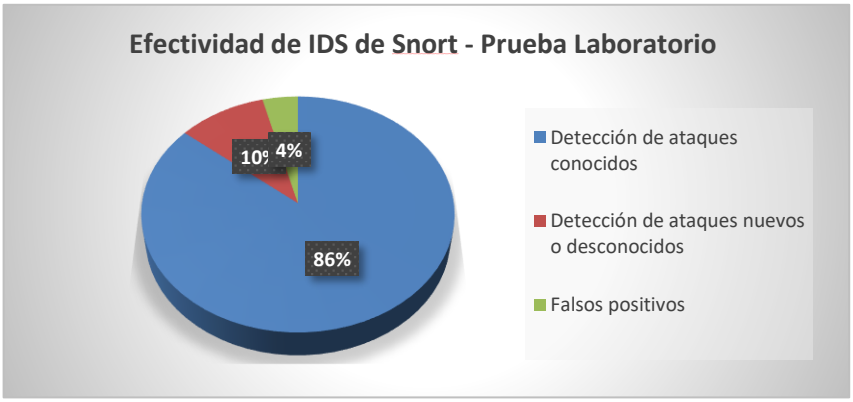

Figure 7: Snort effectiveness percentage distribution, laboratory test (own source)

Statistical analysis indicates that 86% of known and traditional attacks can be identified, with 10% of sophisticated new attacks detected with the assistance of an artificial intelligence (AI) tool. Additionally, 4% of false positives were mitigated. The Snort tool's capacity for analysis and identification is a crucial aspect of cybersecurity in organizational settings.

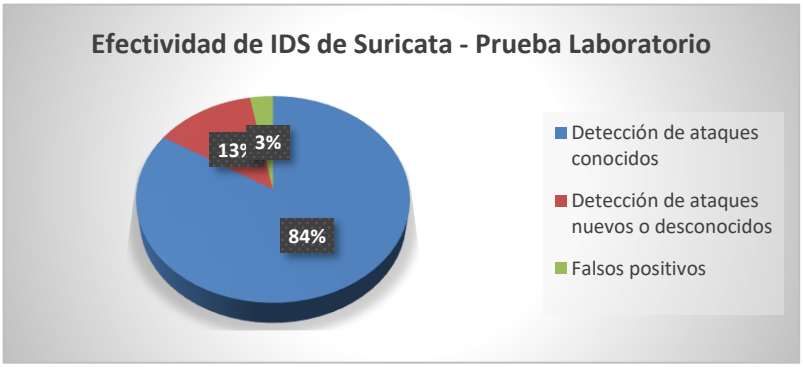

Figure 8: Percentage distribution of Meerkata effectiveness, laboratory test (own source)

Statistical analysis indicates that 84% of known and traditional attacks can be detected, while 13% of new or unknown attacks can be identified. The remaining 3% are false positives. When Suricata is compared to Snort, it is evident that Suricata is more effective in detecting new attack vectors. Additionally, it is more sophisticated in mitigating false positives and its traffic analysis and threat control model, such as IDS and IPS, are more scalable. These findings are based on laboratory tests.

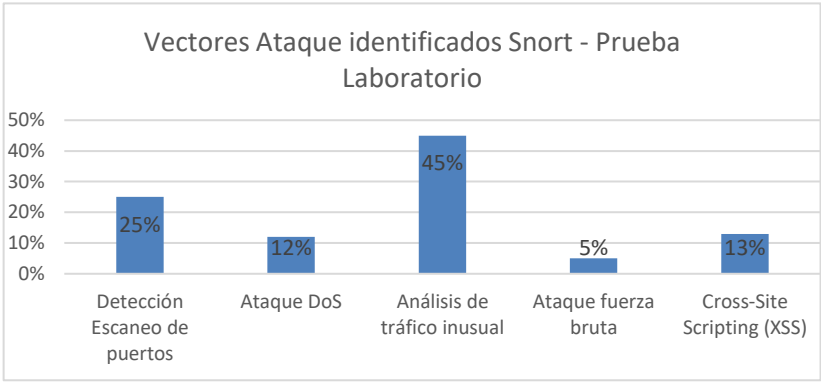

Figure 9: Percentage distribution of attack vectors identified by Snort, laboratory test (own source)

The Snort tool identified four attack vectors, accounting for 45% of the total. These included unusual traffic analysis and the deployment capacity to analyze traffic with the support and relationship with artificial intelligence. In addition, multiple attacks were made. The Snort tool identified and flagged a multitude of malicious activities, including denial-of-service (DoS) attacks, port scanning, cross-site scripting (XSS) vulnerabilities, and brute force attacks.

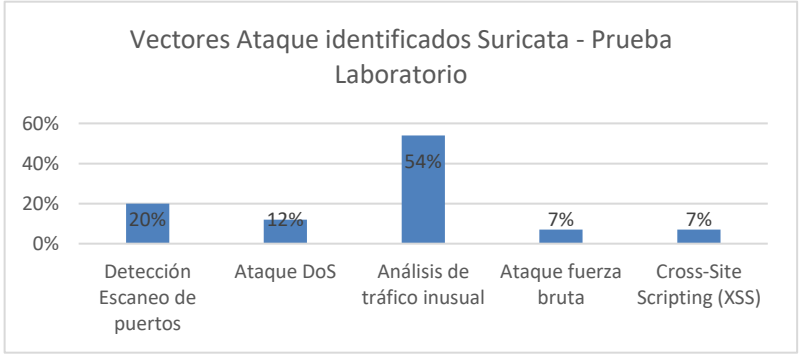

Figure 10: Percentage distribution of attack vectors identified by Smerica, laboratory test (own source)

The attack vectors identified in the tool, Unusual Traffic Analysis, have a 54% success rate. The deployment capacity to analyze traffic with the support and relationship with artificial intelligence is more efficient than that of Snort. The blocking of traffic by IP Snort has rules that mitigate DoS attacks. A good balance in port detection scanning generates relevant alerts to evaluate possible incidents.

Discussion of results Cybersecurity, the relationship between artificial intelligence and threat detection

1. Real-time threat detection: Meerkat or Snort can detect and prevent attacks in real-time, while a SIEM AI can provide a broader view of the network-wide security posture by correlating Meerkat events with other security data.

2. Advanced incident analysis: An AI SIEM can analyze events generated by Meerkat or Snort along with other security events and network logs to identify patterns and relationships that could indicate an ongoing attack or broader security breach.

3. Improved responsiveness: By integrating Seerkat or Snort with an AI SIEM, you can automate incident responses based on predefined rules and policies, allowing you to respond quickly to detected threats.

4. Log consolidation and centralized visibility: An AI SIEM can provide a centralized view of all security events and logs on the network, making it easier to monitor and manage security across the infrastructure.

5. Identify the strengths and weaknesses of each tool: Areas where each tool stands out or has limitations in intrusion detection can be determined.

6. Relationship Cybersecurity and AI in intrusion detection: They have become allies in the fight against cyber threats, especially in intrusion detection. AI is emerging as a crucial complement to traditional security tools, allowing tasks and processes to be optimized in organizations. AI has three important components: accuracy, adaptability, and automation.

Accuracy: AI can identify anomalous patterns and behaviors more accurately than traditional tools, reducing false positives and increasing efficiency.

Adaptability: AI can continuously learn and adapt to new threats, making it a flexible and effective tool against emerging threats.

Automation: AI can automate repetitive and tedious tasks, such as reviewing security records, freeing up time for security professionals to focus on more strategic tasks.

Conclusions

In conclusion, this article has provided a comprehensive examination of the pivotal nexus between cybersecurity and artificial intelligence. It has been emphasized that, in the context of the proliferation of Big Data, cybersecurity has become a critical necessity for a diverse range of entities, from relatively simple websites to prominent corporate entities such as Google. Artificial intelligence, particularly in the form of deep learning, has emerged as a crucial tool for both threat defense and intrusion detection. Convolutional neural networks (CNNs) and generative adversarial networks (GANs) have been presented as deep learning models that offer more robust answers than conventional tactics.

It is imperative to recognize that artificial intelligence is not merely a weapon designed to attack or defend, but rather, an advanced set of programming techniques. The implementation of artificial intelligence in security systems, particularly those based on neural networks,

provides an impenetrable shield or an effective weapon against cyber threats.

The results of laboratory tests conducted with Snort and Meerkata demonstrate the pivotal role that AI plays in the detection of intruders. The capacity of AI to analyse vast quantities of data, identify patterns and continually learn makes it an invaluable asset in the fight against ever-changing cyber threats. The selection of either Snort or Meerkat will be contingent upon the particular requirements of the organization in question. Snort is a mature tool with a substantial user base, whereas Suricata is a relatively recent addition to the field with a focus on efficiency and scalability.

The incorporation of AI into intrusion detection tools confers tangible benefits for organizations, enhancing security posture with greater precision, reducing the time and resources necessary for threat detection, enabling security teams to operate more efficiently and strategically, and establishing a long-term partnership in threat detection.

Acknowledgment

I would like to express my sincerest gratitude to God and to all those who have made a significant contribution to the realisation of this scientific article. I would like to express my gratitude to the Universidad Minuto de Dios for providing me with the necessary resources to conduct this research and for their ongoing support. I am also indebted to the Faculty of Graduate Studies in Computer Security Specialization for their assistance. I would like to express my gratitude to the Academic Coordinator, the Graduate Coordinator, and the Dean for their guidance and unwavering support throughout my academic pursuits. Furthermore, I would like to express my gratitude to the Research Directorate for its invaluable guidance and counsel in the advancement of this project. Finally, I would like to express my gratitude to my family for their unwavering support and understanding throughout this process. Your words of encouragement have been a significant source of motivation. The completion of this article would not have been possible without the commitment and collaboration of all parties involved. I would like to express my sincerest gratitude.

References

1. Ballestero, F. (2020). Cybersecurity in Challenging Times: Do We Care About It or Care About It? ICE Economic Bulletin, 3122, Article 3122. https://doi.org/10.32796/bice.2020.3122.6993
2. Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. Journal of Physics: Conference Series, 1757(1), 012055. https://doi.org/10.1088/1742-6596/1757/1/012055
3. Covarrubias, L., & Zadamig, J. (2020). Las tres “C” de los Estados Contemporáneos: Ciberespacio, Ciberseguridad y Contrainteligencia. (The Three «c» of the Contemporary States: Cyberspace, Cybersecurity and Counterintelligence) (SSRN Scholarly Paper 3649221). https://doi.org/10.2139/ssrn.3649221
4. Institute for Intelligent Systems and Experimental Teaching of Robotics, Elkfury, F., Ierache, J., & Institute for Intelligent Systems and Experimental Teaching of Robotics. (2021). Classification and representation of emotions in spoken discourse in Spanish using Deep Learning. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 42, 78-92. https://doi.org/10.17013/risti.42.78-92

5. Lee, T.-H., Chang, L.-H., & Syu, C.-W. (2020). Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks. 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 1-6. https://doi.org/10.1109/ICCWorkshops49005.2020.9145085
6. Martínez, W. R. (2020). Analysis of Machine Learning techniques applied to computer cybersecurity to improve the detection of intrusions and anomalous behavior on the Web. #ashtag, 2(17), Article 17. https://doi.org/10.52143/2346139X.829
7. Portela, S. (2022). Landscape of artificial intelligence in the domain of cybersecurity. RUIDERAe: Journal of Information Units. (ISSN 2254-7177), 19, Article 19. https://revista.uclm.es/index.php/ruiderae/article/view/3082
8. Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). A review of Deep Learning applied to cybersecurity. UPSE Scientific and Technological Journal, 9(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671
9. University of Coimbra, Department of Computer Engineering, Lino, A. D. P., Sizo, A., & University of Porto, Laboratory of Artificial Intelligence and Computer Science. (2021). The integration of Computer Systems with Artificial Intelligence. RISTI - Iberian Journal of Information Systems and Technologies, 42, xi-xiv. https://doi.org/10.17013/risti.42.0
10. Viteri, J. T. M., Valero, M. I. G., Torres, A. del R. F., & Torres, N. M. C. (2022). Security against DDoS attacks in SDN environments with Artificial Intelligence. Revista de las Ciencias: Revista de Investigación e Innovación, 7(3), 105-127. https://doi.org/10.33262/rmc.v7i3.2844
11. Weamie, S. (2022). Cross-Site Scripting Attacks and Defensive Techniques: A Comprehensive Survey. International Journal of Communications, Network and System Sciences, 15, 126-148. https://doi.org/10.4236/ijcns.2022.158010
12. Zhang, X., Zhou, Y., Pei, S., Zhuge, J., & Chen, J. (2020). Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks. IEEE Access, 8, 10989-10996. https://doi.org/10.1109/ACCESS.2020.2965184
13. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2), 1029-1053. https://doi.org/10.1007/s10462-021-09976-0