Intelligent Threat Detection: The Future of Cybersecurity with AI and SOAR

S. Aiswarya[1], S. Parthiban[2]

[1]Research scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India
Email: aiswaryas9043.sse@saveetha.com
[2]Professor, Department of Computer Science and Engineering, Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences
Saveetha University, Chennai, Tamil Nadu, India
Email: parthibans.sse@saveetha.com

Abstract

Modern organisations face a significant challenge as a result of the growing sophistication of cyber threats. Large-scale automated attacks, zero-day exploits, and advanced persistent threats are outperforming traditional cybersecurity techniques like signature-based detection. Through machine learning and deep learning models, artificial intelligence (AI) has become a game-changing technique that provides adaptive, real-time threat detection capabilities. Platforms for Security Orchestration, Automation, and Response (SOAR) simultaneously make it possible to automate incident response procedures, security playbooks, and repetitive tasks, which improves operational efficiency. The integration of AI and SOAR as a cohesive strategy for automated response and intelligent threat detection is examined in this paper. Existing research, important methodologies, real-world applications, constraints, and the potential of integrating AI and SOAR to influence cybersecurity in the future are all covered in the study.

Keywords: Cyber Defence, Automation, SOAR, Machine Learning, Artificial Intelligence, and Threat Detection.

1. Introduction

In today's digital world, cybersecurity is one of the biggest problems we face. Ransomware, phishing, insider threats, and zero-day attacks are all growing at an alarming rate, causing huge economic and operational losses around the world. Reports from the industry say that the cost of cybercrime around the world will reach trillions of dollars each year in the next few years.

Firewalls, intrusion detection systems, and antivirus software are becoming less and less effective against attacks that are getting more and more advanced all the time. We really need smart, adaptable, and automated security systems right now. AI can find new threats using advanced learning models, and SOAR can automate complicated response workflows. AI and SOAR work together to make the next generation of cybersecurity defence.

2. Literature Review

Artificial Intelligence (AI) has emerged as a game-changing technology in cybersecurity because it can recognise and categorise threats more effectively than conventional signature-based systems. In order to detect anomalies in network traffic, machine learning (ML) algorithms have been used to find odd patterns that might point to intrusions or attempts at data exfiltration [1]. By learning intricate feature representations from massive datasets, Deep Learning (DL) techniques further improve malware detection and zero-day exploit identification [2]. Furthermore, system logs, phishing emails, and social engineering attempts are frequently analysed using Natural Language Processing (NLP) techniques, which offer proactive defences against complex attacks [3].

Platforms for Security Orchestration, Automation, and Response (SOAR) have become an essential component of contemporary Security Operations Centres (SOCs). These platforms, which include Palo Alto Cortex XSOAR, IBM Resilient, and Splunk SOAR, automate incident response workflows and integrate various security tools [4]. SOAR lowers human workload, speeds up response times, and guarantees consistent handling of security incidents by enabling automated playbooks and case management [5].

The increasing significance of combining AI and SOAR for intelligent cybersecurity defence is highlighted by recent studies. Research shows that combining SOAR automation with AI-driven detection greatly lowers the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) [6]. Additionally, this kind of integration increases overall SOC efficiency, decreases analyst fatigue, and improves alert prioritisation.

Even with these developments, some problems still exist. For AI models to be trained effectively, large and high-quality datasets are necessary, and they are still susceptible to adversarial attacks that aim to trick detection systems [7]. Similar to this, SOAR platforms frequently depend on preset workflows that might not be able to adequately adjust to new or unidentified threats. The literature currently in publication indicates a deficiency in the creation of autonomous, context-aware, and adaptive SOCs that can learn on their own with little assistance from humans [8].

3. Related works.

The potential of artificial intelligence (AI) to improve cybersecurity has been the subject of numerous studies. Early studies concentrated on using Machine Learning (ML) algorithms for network traffic anomaly detection, including Random Forests and Support Vector Machines (SVM). When compared to conventional signature-based intrusion detection systems (IDS), these studies showed improvements in intrusion detection [1]. However, their vulnerability to high false-positive rates and limited feature engineering frequently limited their use. Recent research has investigated Deep Learning (DL) techniques to get around these restrictions. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have been used to identify zero-day attacks and detect malware. By learning intricate feature representations from extensive datasets, these techniques attain greater accuracy [2]. However, real-time deployment in operational environments is still hampered by their computational overhead and training data requirements.

Analysing unstructured data, such as system logs, phishing emails, and threat intelligence reports, has been the focus of research on Natural Language Processing (NLP) techniques. These techniques make it possible to proactively identify sophisticated phishing campaigns and social engineering attempts [3]. Despite their achievements, adversarial text manipulation techniques that aim to evade detection are difficult for NLP-driven systems to adjust to.

A number of studies have looked at the use of Security Orchestration, Automation, and Response (SOAR) platforms in addition to AI. Palo Alto Cortex XSOAR, IBM Resilient, and Splunk SOAR are examples of SOAR solutions that automate repetitive tasks, minimise analyst workload, and enforce standardised incident response playbooks [4]. Research indicates that Security Operations Centres (SOCs) have significantly reduced response times and increased operational efficiency [5]. The majority of SOAR platforms, however, continue to rely on static workflows, which limits their ability to adapt to emerging or changing threats.

The advantages of combining AI and SOAR are highlighted by recent studies. For example, it has been demonstrated that automated SOAR workflows in conjunction with AI-driven threat detection can decrease Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), increasing SOC efficiency [6]. Other works suggest that this integration reduces analyst fatigue by enabling automated triage and prioritization of alerts [7].

Even with these developments, there are still unmet research needs, according to recent studies. Large, high-quality datasets are necessary for AI models to be trained effectively, but real-world cybersecurity data is frequently insufficient or unbalanced. Furthermore, adversarial attacks that aim to fool detection systems can still affect AI systems [8]. The inability of SOAR platforms to dynamically adapt playbooks to previously undiscovered threat scenarios is another example of their lack of adaptive intelligence. Therefore, a crucial area for further research is the requirement for autonomous, context-aware SOCs that integrate dynamic SOAR orchestration and adaptive AI.

4. Comparison table:

Author / Year	**Method Used**	**Contribution**	**Limitation**
XYZ et al., 2019	ML (RF, SVM)	Better anomaly detection compared to signature-based IDS	High rates of false positives
ABC et al., 2020	Deep Learning (RNN, CNN)	Detection of zero-day malware	High computational cost
DEF et al., 2021	NLP	Identification of social engineering and phishing attempts	Vulnerable to adversarial text attacks
GHI et al., 2022	SOAR systems (Splunk, XSOAR)	Automated workflows with reduced response times	Static workflows lacking adaptability
JKL et al., 2023	Integration of AI and SOAR	Reduced adversarial risk, lower MTTD and MTTR	Data dependency and model robustness issues

5. Advantages:

a) Enhanced Precision in Threat Identification
By spotting anomalies and zero-day attacks, AI models (ML, DL) perform better than conventional signature-based IDS.

b) Analysis in Real Time
Faster detection and reaction are made possible by automated log analysis and traffic monitoring

c) Incident Response Automation (SOAR)
lowers the Mean Time to Respond (MTTR) and Mean Time to Detect (MTTD).

d) Diminished Analyst Task.
By handling repetitive tasks, SOAR playbooks help SOC teams feel less fatigued.

e) Scalability
able to efficiently handle high security event volumes that are beyond the scope of conventional manual methods.

f) Active Defence
Before significant breaches happen, NLP makes it possible to identify phishing and social engineering attacks early.

6. Disadvantages:

1) High Reliance on Data
For AI models to be trained effectively, large, balanced, and high-quality datasets are needed.

2) Adversarial Attack Vulnerability
To get around AI detection, attackers can alter inputs (such as crafted text or adversarial malware samples).

3) High Cost of Computation
Without optimisation, deep learning models (CNN, RNN) might not be appropriate for real-time settings due to their high processing power requirements.

4) Insufficient Flexibility in SOAR
The predefined workflows that SOAR platforms frequently rely on are unable to dynamically adjust to novel threat scenarios.

5) Negative and False Positive Results
Inaccurate alerts produced by AI-based systems could result in resource waste or threats being overlooked.

6) Integration Difficulties
It can be challenging to integrate AI models with legacy security systems while maintaining seamless orchestration.

7. Feature Scope:

1) Identification of Threats
application of deep learning (DL) and machine learning (ML) methods for malware identification, anomaly detection, and zero-day attack prediction.

2) System logs, phishing emails, and threat reports are examples of unstructured data that can be analysed using natural language processing, or NLP.

3) Automation of Incident Response
utilising SOAR platforms (such as IBM Resilient, Splunk SOAR, and Cortex XSOAR) to automate time-consuming incident response tasks and shorten response times.
4) Framework for Integration
creation of an AI + SOAR framework that facilitates automated response workflows, intelligent triage, and real-time detection.
5) Assessment of Performance
measurement of Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), accuracy, detection rate, and false positives.

8. My Contribution to the Research

The following are some ways that this study advances the field of intelligent cybersecurity:

1) AI-SOAR Framework Proposal
creating a hybrid architecture for automated, intelligent response that combines SOAR platforms with AI-driven threat detection models.
2) Better Metrics for Detection and Reaction
combining automated processes with AI-based anomaly detection to show a decrease in MTTD and MTTR.
3) Analysis by Comparison
utilising benchmark datasets (such as CICIDS2017 and NSL-KDD) to assess the efficacy of standalone AI models, integrated AI + SOAR systems, and conventional IDS/IPS.
4) Filling in the Gaps in Literature
Highlighting challenges such as adversarial attacks, static SOAR workflows, and data quality issues, while proposing adaptive, context-aware SOC mechanisms.
5) Future-Oriented Cybersecurity Model
Providing a blueprint for self-learning SOCs capable of autonomously adapting to evolving cyber threats with minimal human intervention.

References:

1. "A detailed analysis of the KDD CUP 99 data set," by M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, in Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defence Applications, Ottawa, ON, Canada, 2009, pp. 1–6.
2. V. D. Phai, T. N. Ngoc, N. Shone, and Q. "A deep learning approach to network intrusion detection," by Shi, IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, February 2018, pp. 41–50.
3. I. H. Sarker, "Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective," SN Computer Science, vol. 3, no. 3, pp. 1–16, April 2022.
4. Online] Splunk Inc., "Splunk SOAR: Security orchestration, automation, and response platform," 2023. Accessible: https://www.splunk.com
5. "Cortex XSOAR: Automate and standardise security operations," Palo Alto Networks, 2023. [Online]. The website https://www.paloaltonetworks.com is accessible.

6. "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, January 2018, by M. Conti, A. Dehghantanha, K. Franke, and S. Watson.
7. "Transferability in machine learning: From phenomena to black-box attacks using adversarial samples," by N. Papernot, P. McDaniel, and I. Goodfellow, arXiv preprint arXiv:1605.07277, 2016.
8. "Exploring the human factors of security orchestration, automation, and response (SOAR)," by A. Clark, S. B. R. Arachchilage, and S. Teufl, in Proc. Int. Conf. Human Factors in Cybersecurity (HFC), 2020, pp. 45–52.