IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADVANCED THREAT INTELLIGENCE THROUGH THE IMPLEMENTATION OF EXPLAINABLE AI(XAI)

Mr. AnilKumar B, Rizaal.P.M, Adithya.R, Algin M Shabu, Deepu.A

Assistant Professor, Student, Student, Student, Student
Dept. of Computer Science
Yuvakshetra Institute of Management Studies, Palakkad, India

Abstract: The field of cybersecurity is always changing because threat actors are developing more advanced methods. As a result, incorporating artificial intelligence (AI) has become essential for strengthening defenses. However, effective threat mitigation measures are hampered by the typical AI models' "black-box" character, which makes it difficult to understand their decision-making processes. This abstract explores the necessity of using Explainable AI (XAI) to threat intelligence advancement, clarifying its importance, approaches, difficulties, and potential applications. Explainable AI's deployment represents a shift in perspective, in threat intelligence advancement, empowering stakeholders to effectively and confidently traverse the intricate cybersecurity landscape. XAI enables cyber security experts to decipher the complexities of AI-driven insights and create focused response plans that mitigate emerging threats by promoting openness, trust, and interpretability. The use of XAI is anticipated to be crucial in creating threat intelligence going ahead protecting digital assets, and strengthening defenses against evolving cyberthreats as the cybersecurity landscape advances.

Index Terms **- Advanced Threat Intelligence, Explainable AI (XAI), Cybersecurity, Artificial Intelligence (AI)**

I. INTRODUCTION

Across the field of cybersecurity, threat intelligence is crucial for identifying and mitigating online threats. But it can be difficult understanding how typical AI models make decisions because of their opacity. The answer is provided by Explainable Artificial Intelligence (XAI), which gives interpretability and transparency. The goal of this article is to improve adaptation strategies and decision-making by investigating the incorporation of XAI into threat intelligence. We demonstrate how XAI has the ability to completely transform cybersecurity practices through the analysis of current approaches, case studies, and potential outcomes. XAI gives enterprises the ability to confidently and precisely handle the constantly changing threat landscape by bridging the gap between advanced analytics and human comprehension.

II. EXISTING TECHNOLOGIES

The modern technologies in threat intelligence are burgeoning and a variety of tools and techniques are becoming essential for building strong cyber defenses. Amid the variety of technology instruments used by threat intelligence there is Artificial Intelligence (AI) which plays a significant role in security teams' multi-tasking. AI allows them to monitor and analyze constant streams of log data and incoming data packets to pick up on the patterns that warn of possible threats. AI-linked solutions as IBM's QRadar package (threat intelligence and automation) are designed to make the security analysts faster and more exact while responding to cyber-attacks. These deliveries (solutions) in the form of cloud-based services (AWS and others) mean a simple deployment across different platforms and integration with the logs of public cloud and SaaS.

AI, which includes Generative Pre-trained Transformers (GPT-4), LLMs, and other machine learning models, is a widely applied tool in cyber threat intelligence to perform different jobs. The job duties of an analyst involve summarization, identification of IOCs, TTPs extraction, predictive intelligence, alerts/report generation, threat detection generation, and malware analysis. AI-based Natural Language Processing (NLP) models effectively and quickly process a variety of threat information into compact summaries. They aid cybersecurity analysts in comprehending threat information and scrutinizing them, and thus turn the data into actionable intelligence. In addition, AI systems typically spontaneously extract Indicators of Compromise (IOCs) from unstructured information sources such as social media or deep web portals and, consequently, help in discovering potential hazards more quickly and effectively.

III. XAI IN CYBER ARENA

Explainable AI is a technology that can detect the threat among all the noise in the cyber threat intelligence. AI algorithms composed of such vast dataset analysis, including traffic networks data, logs, including endpoint telemetry, determine unusual behavior and security incidents. In comparison to conventional approaches, which often issue false positives or miss small indications of compromise, XAI models are chosen as the option, since they explain their decisions in details, and thus security analysts will spend more time on investigating alerts they prioritize according to model results.

Take for instance the XAI algorithms able to identify activities related to advanced persistent threats (APTs) or insider attacks by doing user behavior analysis and network consistency checks. The analysts not only get the detectable threat explanations, but also have the general idea of the threat in which they can notice and reduce risk.

IV. IMPROVING INCIDENT RESPONSE AND REMEDIATION EFFORTS

Furthermore, Exact AI adds defence by containing and mitigating the risk in an incident. In the case of a security incident, time is a critical factor, and fast actions, as well as prompt decision making are necessary in order to reduce the damage (we are minimizing the impact). With XAI, it becomes possible for the security personnel to trace the source of the problem, and thus, assess its impact for elaborating an efficient response plan.
XAI delivers the cursory precision with IOC and attack vectors to allow the human user to follow the attack path, identify compromised assets, and arrange the remediation tasks in terms of their importance. In addition, the simulating "what-if" scenarios, XAI models can predict the potential consequences of various response measures allowing the leaders or organizations to come up with practical and precautionary decisions.

V. ENHANCING THREAT INTELLIGENCE SHARING AND COLLABORAION

We live in an era marked by the interconnected threats, hence joint effort and data sharing among organization are now key to efficient cyber-security. Yet, sharing information about threat intelligence may be problematic as there are issues such as the fear of infringing on privacy, confidentiality, or trust. Explainable AI solutions, which are the machines that can precisely translate the instructions of human teams, are beneficial in overcoming the challenges of transparency and explainability, resulting in the collaboration and knowledge sharing across security teams.

Through information sharing cover things like explainable aspects of threat indicators, hacking techniques, and mitigation strategies, organizations can gain from the collective wisdom of security prospects around the space while building responses that are more effective against the emerging threats. The XAI-enabled threat intelligence platform is compatible with the security applications that are already in use and allows organizations to efficiently share information and develop a common and balanced response to the new and developing threats.

VI. ADDRESSING ETHICAL AND REGULATORY CONSIDERATIONS

If Big Data and AI Technologies are applied to cyber threat intelligence, these tools offer advantages to the problem, but and ethical and regulatory considerations need to be addressed as well. The role of AI algorithms in decision marking regarding cybersecurity poses a high need for transparent methods as well as accountability and fairness consideration.

Ethical AI principals, including transparency, accountability, fairness, and so on should be followed with the XAI development and operation in CTI. AI organizational frameworks must be governed by good governance standards with a bias-free atmosphere ensuring transparency and explainability of AI models, among other aspects. As an example, a regulatory demand that necessitates companies to explain certain apparent decisions affects the rights of people. This regulation includes the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

VII. PROPOSED IDEA

The evolving cyber range should have a technology that can withstand the change and advancement of both defensive and offensive side of threat intelligence. Here the idea of Explainable AI clearly paves the way for advanced defensive enhancements through the integration of advanced data models.

The integration of Explainable AI (XAI) with Security operation centre (SOC). Explainability of AI assists Security Operations Centers (SOCs) in their efficient performance during a cyber-attack in that it makes the decision-making process of the AI systems in the tools clear, interpretable and it provides users with actionable insights. Here's how XAI could assist a SOC during a cyber-attack. Here's how XAI could assist a SOC during a cyber-attack:

7.1. Improved Threat Detection:

XAI algorithms can allow user to get the complete details about why a certain act or conduct is shown as suspicious or hostile. Analysts can draw conclusions with respect to the credit, during which SOC employees will be able to evaluate the degree of the threat and decide which action should be taken first only after understanding each recommendation’s rationale individually.

7.2. Faster Incident Response:

Timing is paramount, as often, every second counts during a cyber-attack. Through XAI, analysts can get real-time explanations as to what the classification is about and whether this threat is critical or something that they have been looking at for a while and can address it immediately. The upside of the situation is that this makes it possible to figure out the consequences more promptly and less downtime.

7.3. Enhanced Situational Awareness:

AI prompts the SOC analysts to obtain richer understandings concerning the particular methods, schemes, and proposals utilized by attackers. Knowing attack routes and attack patterns allows the analysts to understand cyber threats and hence they can better anticipate the future threats, secure their networks with proactive defense techniques, and tweak their security posture accordingly.

7.4. Reduced False Positives:

One of the difficulties of security operations centers is the high volumes of events being reported by security tools causing many of them to turn out to be false positives. XAI can aid in minimizing a false alarm rate by generating better explanations concerning the alert, where the idea can be very suitable for the background and the alert can be distorted between a genuine threat and a harmless anomaly more deliberately.

7.5. Optimized Resource Allocation:

XAI enables a specialized operations center to focus its resources during a cyber attack and get work done quickly. Through protocols for alerts prioritization based on the criticality or the extent of probable damage, the analysts can concentrate on responding to the most substantial mishaps first and vice-versa to effectively respond to crises and prevent widespread devastation. Furthermore, the training should be tailored to equip the staff with the right skills and knowledge to perform the job accurately.

7.6. Facilitated Collaboration:

The use of XAI as part of the SOC creates a collaborative environment between security analysts that allows them to understand AI-driven security systems which are based on transparent and interpretable insights. The mutual exchange of explainable insights and threat intelligence encourages a more effective cooperation of the analysts as they can benefit from the different competencies, and even answer to collective efforts across teams and departments.

7.7. Continuous Learning and Improvement:

With XAI, SOC analysts can tackle earlier attacks using past incident data, which results in a continuous improvement in SOCs' detection and response abilities. What stares out is the way the XAI algorithms explain themselves, which enables analysts to draw conclusions, identify trends and patterns, as well as the most recurring threats, leading to refining of the detection rules, update of the threat models, and this results in improving of the overall cybersecurity posture.

VIII. CONCLUSION

Finally, it is worth mentioning that Explainable AI (XAI) plays the role of one of the most essential weapon in front of Security Operations Centers (SOCs) when it is crucial to manage new cyber threats. Through providing transparency, interpretability, and actionable security insights into the decision-making algorithms of AI driven security systems, XAI allows better detection, analysis and response to cyber attacks and thus shapes the way of security operation centers functioning.

XAI is the tool that not only provides improved adversary detection, speedy response work flow, greater situational awareness, and wiser utilization of resources, but as well it aids human security analysts in shaping the cyber defense strategy and keeping the cyber threat by stealth. In this way, it helps curtail the rate of false positives, controls collaboration better, and advances the dynamic and ongoing learning and betterment efforts within organizations.

The intensity of confrontation of the cyber threat domain will surely grow with time, which will, in turn, underline the significance of XAI in the SOC operations philosophy. XAI technologies bring an opportunity for organizations to accept them into their security workflows, which eventually will improve the resilience of the organizations, develop a powerful demonstration of the defense system, and ensure the security of the digital assets confronted by different cyber dangers in the electronic field. In the midst of a cyber warfare which is sometimes exhausting and overwhelming, Explainable AI acts as a beacon of light, trust and resilience to the world's SOCs.

IX. REFERNCES

[1] Miller, Tim. "Explanation in artificial intelligence: Insights from the social sciences." Artificial Intelligence 267 (2019): 1-38.

[2] Guidotti, Riccardo, et al. "A survey of methods for explaining black box models." ACM Computing Surveys (CSUR) 51.5 (2018): 1-42.

[3] Ribeiro, Marco Tulio, Sameer Singh, and Carlos Guestrin. "Why should I trust you?": Explaining the predictions of any classifier." Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016.

[4] Doshi-Velez, Finale, and Been Kim. "Towards a rigorous science of interpretable machine learning." arXiv preprint arXiv:1702.08608 (2017).

[5]Adadi, Amina, and Mohammed Berrada. "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)." IEEE Access 6 (2018): 52138-52160.

[6] Narayanan, Arvind, and Vitaly Shmatikov. "Robust de-anonymization of large sparse datasets." Proceedings of the 2008 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2008.

[7] Liu, Xi, et al. "Cyber threat intelligence sharing and analytics: A survey." IEEE Transactions on Emerging Topics in Computing 5.1 (2017): 94-106.

[8] Ashish M Kothekar; Sandeep Patil, Building a Next-Gen SOC with IBM QRadar: Accelerate your security operations and detect cyber threats effectively , Packt Publishing, 2023.

[9] https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity

[10] https://cyware.com/security-guides/cyber-threat-intelligence/what-is-the-role-of-ai-in-cyber-threat-intelligence-acd4

[11]https://www.wipro.com/cybersecurity/how-to-make-artificial-intelligence-core-to-your-cybersecurity-strategy

[12].https://www.darpa.mil/program/explainable-artificial-intelligence.

X. SPECIAL REFERENCE

Vaishnav C V, (Principal Cyber Security Engineer | VAPT)
Nuvepro Technologies Pvt Ltd.
Linkedin:https://www.linkedin.com/in/vaishnavucv/