

AI-Generated Cybersecurity Threat Intelligence Reports.

Dr.AmjadKhan, HemanthGowdaKS

AssociateProfessorDepartmentofMasterofComputerApplications,BIET,Davangere-577004.

amjadkhan.biet@gmail.com,Davangere,Karnataka,India

P.G.Student,DepartmentofMasterofComputerApplications,BIET,Davangere-577004.

hemanthgowdaks0207@gmail.com,Davangere,Karnataka,India

ABSTRACT:

In today's digital environment, the number, speed, and level of advanced cybersecurity threats have increased exponentially, making manual threat intelligence gathering and analysis practices increasingly obsolete. Presently, Security Operations Center (SOC)s and threat analysts are faced with an influx of data from various sources such as vulnerability listings (CVEs), blogger/security vendors' blogs, social media channels, dark web communities, and RSS feeds. Due to the enormous amount of unstructured data, there is a substantial bottleneck that often leads to missing or delayed analysis of critical intelligence, thus hindering an attack from being thwarted.

Moving beyond the limitations of conventional web-scraping tools, this research introduces a generative AI framework designed to decode the nuanced context of emerging cyber threats. By autonomously mapping observed adversarial behaviors against the **MITRE ATT&CK** framework, the system bridges the gap between raw data and actionable intelligence. The first goal of the research would be to achieve substantial reduction in the Mean Time to Analyze, offering high-fidelity instant information to the security leaders. One of the key aspects of the current research is the ability to use two reporting engines – one creating high-level strategic reports and another offering detailed technical information about IoC's.

The two-way approach makes sure that SOC professionals and C-level executives stay in sync with each other.

All in all, what is achieved here helps move towards proactive measures against threats that are fueled by advanced AI systems.

Keywords: Automated multi-source data, context-aware natural language processing, intelligent severity scoring & prioritization, automatic mapping to MITRE ATT&CK Framework.

I INTRODUCTION

The present-day digital environment poses a myriad of cyber threats like malware, phishing attacks, ransomware attacks, and network intrusions. Analysts must track these threats in real-time and provide comprehensive intelligence on the nature of the threat, its consequences, and methods for mitigating the threat. This is done by manually analyzing threats and preparing comprehensive reports. This process is cumbersome, tedious, and labor-intensive, necessitating an automated system for threat analysis and report generation.

AI-Generated Cybersecurity Threat Intelligence Reports is an application based on the web used for automating cybersecurity analysis reports generation with the use of Artificial Intelligence. The input from the user would be either the threat name or its description, and the application connects to the AI (based on Google's Gemini) model to generate a report on the threat.

This includes information on threat details, severity of the problem, impact, IOC's, and prevention methods. The tool provides visualizations of risk measurement using charts for better comprehension.

This project will minimize the effort and save time for cybersecurity experts to tackle potential threats. Rather than creating a local machine learning algorithm, the application utilizes advanced cloud-based AI tools, which makes it easy to use and scalable. The frontend has been created with React and TypeScript technologies, and the backend processing involves an AI API service.

II LITERATUREREVIEW

The latest studies have demonstrated that the cyber environment produces enormous volumes of threat information, which cannot be effectively analyzed manually by human experts. AI solutions have been extensively used in threat intelligence systems to automate detection, analysis, and response processes in order to improve the effectiveness of threat identification compared to traditional approaches. In addition, researchers emphasize that artificial intelligence increases the ability of security professionals to detect, respond to, and predict cyber threats. It enables them to foresee attacks rather than only responding to them.

The advent of Large Language Models (LLMs), which includes the contemporary generative AI models, has prompted cybersecurity experts to explore automated report generation and intelligent analysis techniques.

Researches recommend the introduction of an AI-powered.

cyber threat intelligence pipeline in which the task of identifying vulnerabilities, detecting attacks, and assessing risks can be fully or partially automated through AI.

These systems provide help to professionals in making decisions by producing preliminary analyses and suggestions, thus saving time and effort.

Nevertheless, studies also indicate that AI tools are intended for assistance but not for replacing humans in the decision-making process.

Even though AI tools offer the advantages of automation and scalability, there is always a need for manual intervention for validation purposes and decision-making processes. In recent times, AI-powered solutions have been created using a combination of automation and human intervention for the purpose of creating cybersecurity frameworks.

III EXISTINGSYSTEM

The existing flow requires analysts to manually digest chunks of unstructured text and filter out all of the “fluff” that can be found in marketing content or other distractions. Technicians must then manually identify indicators such as IP addresses or cryptographic hashes, which they subsequently enter manually into their systems.

Also, there is the additional problem of having to communicate findings: while it is important to explain technical details in business terms to executives, it is extremely difficult to perform this task.

IV PROPOSEDSYSTEM

The Proposed AI Threat Intelligence System aims to revolutionize the entire process of intelligence gathering by adding an Artificial Intelligence layer in between the source of information and the human analysts. The architecture of the proposed solution works in cloud/on-premise servers and runs all day long 24/7. The system never stops its activity after humans leave their offices.

The proposed system architecture will be modular. An Ingestion Module provides the senses for the system. Scrapers and API connectors come together to provide the capability of monitoring hundreds of sources all at one time. A processing module is the brain that utilizes the LLM integration. The model is preconfigured with prompt engineering techniques meant to extract the needed intelligence fields: Threat Actor, Victim, Attack Vector, Malware Type, and Remediation Strategy.

Crucially, the proposed system will incorporate a Validation and Deduplication Layer. Whereas the current system does not, the proposed solution identifies when multiple sources are talking about the same incident. It consolidates these sources into one complete "Master Incident" record, referencing all sources but providing one consistent narrative.

It also proposes a Feedback Loop: the quality of the reports generated through AI can be rated by analysts. Based on this feedback, the model is fine-tuned further with each passing day, so the system becomes more attuned to the specific needs and tone of the organization. The final output is not a mere text file but a dynamic dashboard and automated e-mail alerts routing certain intelligence to the proper teams, such as patch management teams receiving the vulnerability reports and network teams receiving IP blocklists.

Advantages of Proposed System

1. Much-Reduced MTTR:

The system provides near real-time intelligence by the automating the collection and synthesis phases. It is that

What would take an analyst four hours to compile can now be generated in seconds, enabling defenders to block threats well before they will have fully infiltrated the network.

2. 24/7 Continuous Monitoring:

Software does not sleep. The proposed system is one

that is continually monitoring worldwide threat feeds so that any threats that may occur in other time zones are ready for processing by the time the analyst arrives for work or send out immediate emergency notifications if critical.

3. Standardization of Reporting

The system ensures that each and every report that goes out is in the same format and style. This makes it convenient for the management to analyze the information and program the reports to be saved.

4. Cost Efficiency and Resource Optimization:

Even if there is some cost involved initially in terms of development, the gains are huge in the end. The network removes the need for human analysis to worry about data aggregation processes and enables them to focus on more important tasks and those that require human ingenuity. The network can manage 10, 100, or even 10,000 sources to collect the data. The network can manage a very large number of sources. The network can handle an increase in the volume of data in case of global cyber threats (such as the Log4j crisis).

5. Enhanced Accuracy and Contextualization:

By comparing different sources of information, the system lowers the risk of false positives. What the model provides that the scripts don't is the explanation of why a specific vulnerability is considered harmful based on its previous history of being exploited and not the CVSS score only.

SYSTEMARCHITECTURE

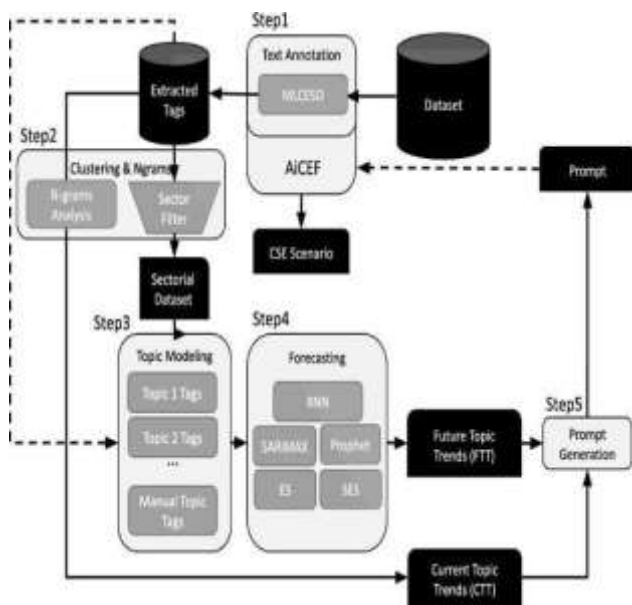


Figure:showsthatarchitecture diagram

V EXPERIMENTALRESULTS

To evaluate the working of the system, different cyber threat examples such as phishing attacks, ransomware, SQL injection, and DDoS attacks were entered as input. A comprehensive threat intelligence report is prepared for every input, covering the description of the attack, the level of severity, its impact on the computer system, warning signs, and preventive measures. The generated reports were relevant and reflected the provided threat, hence being understandable even to people without expertise in cybersecurity.

The time used to produce a report was quite minimal since the analysis process relies on an artificial intelligence model hosted in the cloud environment. Normally, the feedback was generated in a matter of seconds, depending on the speed of the internet connection. The visual graph displayed accurate results reflecting the level of risk involved in the attack. This way, it became easy to determine whether the threat was low, medium, or high in risk.



VI CONCLUSION

It is evident that the AI-Generated Cybersecurity Threat Intelligence Reports initiative stands for a major step forward in terms of cybersecurity technology. This world where there is an increasing imbalance on the attacker side, because of the high number of attacks and hence low availability of human intelligence to handle them, has found an effective solution in this project.

By successfully merging sophisticated Large Language Models with strong web scraping and automation tools, the project resolves the key problem of "Information Overload." This project has clearly proven that AI can not only help in the process of acquiring data but can actually do high-level cognitive tasks such as Summarization, Mapping to Context, and Severity Assignment with overall high accuracy.

The execution of this technology enables the Security Operations Centers to refocus. Rather than devoting hours to manually documenting information and consuming countless blog posts, they can now simply rely on the system to provide them with the most pertinent information, so they can dedicate themselves to decision-making and incident response. The feasibility study has established that this technology has cost feasibility and technological feasibility, and the testing phase has confirmed reliability. Ultimately, this project enables organizations to transition from a reactive approach to predictive, which will shake the very foundations of the pernicious cyber threats of the future.

VII REFERENCES

1. MITRE Corporation. (2023). *MITRE ATT&CK®: Design and Philosophy*. The MITRE Corporation.
2. NIST. (2023). *Cybersecurity Framework 2.0*. National Institute of Standards and Technology, U.S. Department of Commerce.

3. OpenAI. (2023). *GPT-4 Technical Report*. OpenAI Research.

4. Recorded Future. (2022). *The Machine Learning Approach to Threat Intelligence*. Recorded Future Whitepapers.

SANS Institute. (2022). *Automating the SOC: A guide to practical implementation*. SANS Reading Room