JCST Journal of Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7546475

AI – POWERED CYBER THREAT INTELLIGENCE SHARING PLATFORM (CYBERTIP) FOR GHANA: A COMPREHENSIVE SOLUTION FOR SECURITY DATA MANAGEMENT AND REPORTING.

Paul K. Arhin Jnr[1*]

[1*]Faculty Member, Department of Computer Science and I.T, University of Cape Coast, Ghana

***Corresponding Author:** Paul K. Arhin Jnr

*Faculty Member, Department of Computer Science and I.T, University of Cape Coast, Ghana

Abstract

The rapid growth of cyber threats in this period has made the collaborative sharing of cyber threat intelligence essential to protecting national digital landscapes. Like many other nations, Ghana must contend with the difficulty of defending its data assets and vital infrastructure against a wide range of cyber threats. This research presents a novel methodology for the creation of a Cyber Threat Intelligence Sharing Platform (CyberTIP), designed for Ghana in response to this situation of growing threat.

The methodology aims to provide a centralized platform that promotes proactive cooperation between public and private sectors as well as key infrastructure sectors. Through the process of gathering, combining, standardizing, and automated examination of cyber threat information from many sources, this platform aims to provide a comprehensive view of the local threat landscape. The automated system is enhanced by human analysis, which provides context awareness and knowledge. Real-time threat identification, sharing, and incident response coordination are facilitated by this technique. This will help researchers get timely information on the state of cybersecurity in the country.

This platform is positioned to improve Ghana's overall cybersecurity readiness with a clear framework for exchanging threat intelligence. The platform enables enterprises to effectively respond to new threats while safeguarding sensitive data and vital systems by offering pertinent, industry-specific threat intelligence. The approach encourages cooperation with foreign partners, improving response skills and understanding of global threats.

The anticipated results of this study include an enhanced cybersecurity posture for Ghana, which includes better incident response, less impact from cyber threats, and increased situational awareness. Furthermore, the creation of the Cyber Threat Intelligence Sharing Platform paves the way for an international, proactive, and cooperative approach to cybersecurity. This methodology protects Ghana's digital future in an increasingly linked world by doing more than just evaluating the country's cybersecurity environment. It also provides the country with a proactive and cooperative cyber defense strategy.

Keywords: Cybersecurity, cyber threat, CyberTIP

1. Introduction

Like many underdeveloped countries, Ghana has realized how important it is to have a well-functioning infrastructure for reporting cybersecurity problems. The internet has become a double-edged sword providing individuals and organizations with opportunities, and at the same time, posing as an information security risk [1]. In Ghana, internet penetration has increased exponentially from 2.31 million in 2012 to 17 million users in 2022 which represents 53% of the country's population [2]. Ghana has recently been the target of several cyberattacks, including the defacement of several official websites by online criminals. These attacks damage Ghana's online reputation and point to gaps in the security of our cyberspace and infrastructure [3]. Ghana recorded a loss of GHc 49.5 million in the first nine months of 2023 due to cyber fraud. Most of these went unreported and even if reported, poor response time or no response at all [3]. The vulnerability of the country to cyber-based threats and attacks are largely due to the increasing prevalence of broadband connectivity resulting in security awareness challenges [4]. Unfortunately, most of the agencies in the country to control these crimes lack the technical knowledge needed to tackle the problem (5).

Most of these attacks on private and public institutions in Ghana happen because they are not security conscious thereby making them susceptible to attacks (6).

By enabling people and organizations to exchange information about cybersecurity incidents they have experienced, a dedicated reporting system may be established, promoting a culture of alertness and cooperation in the face of cyber threats [7].

Major platforms for online reporting of cyber threats in Ghana

Figure 1 shows the major forms of reporting cyberattacks in Ghana.

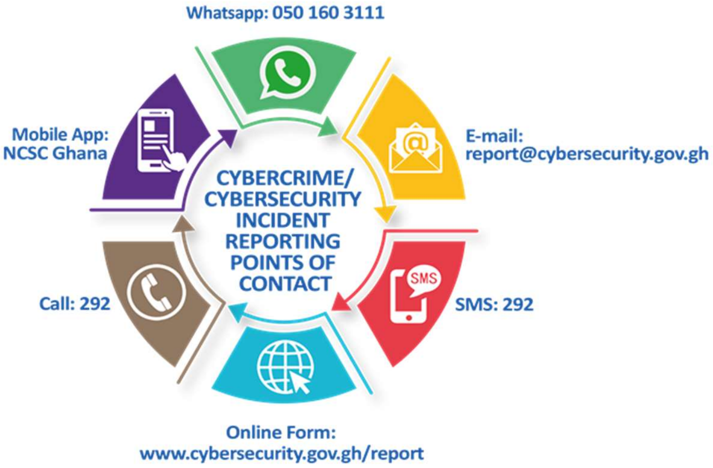
Whatsapp: 050 160 3111
E-mail: report@cybersecurity.gov.gh
SMS: 292
Online Form: www.cybersecurity.gov.gh/report
Call: 292
Mobile App: NCSC Ghana
CYBERCRIME/ CYBERSECURITY INCIDENT REPORTING POINTS OF CONTACT
SMS

Fig 1: Major forms of reporting cyberattack incidences in Ghana (www.cybersecurity.gov.gh)

The CyberTIP is a comprehensive tool or methodology developed to assist business organizations handle security-related occurrences at every level of the organization.

The CyberTIP enables employees at all levels to report security incidents quickly and easily. These reports are then funneled up to the security team, who can use them to look into and address situations more efficiently. The CyberTIP also uses AI-powered automation to help explain incidents and suggest solutions.

2. Objectives of CyberTIP

The objectives of CyberTIP are as follows:

1. To enable an efficient incident reporting platform that will streamline the process of reporting cybersecurity incidents.
2. Utilize AI to quickly identify and assess potential threats. This is done in real time. The platform is enabled to respond to identified threats, ensuring swift and precise countermeasures.
3. An intuitive and user-friendly interface that will benefit both cyber security experts and non-experts and promoting widespread adoption and usability
4. Automated response mechanisms that will be empowered by AI to enhance response times to cyber threats and mitigating potential damages effectively.

3. Key features of the CyberTIP:

1. Role-based access to system resources:

The CyberTIP supports role-based access control (RBAC), which allows organizations to grant users access to specific system resources depending on their job role and responsibilities. This helps to ensure that users can only access the information and resources they need to do their jobs, reducing the risk of unauthorized access and data breaches. For example, a security analyst may be granted access to all incident reports, while a customer service representative may only be granted access to incident reports that are related to their customers.

2. Notification framework:

The CyberTIP includes a notification framework that allows organizations to issue notifications and alerts to users based on specific activities. For example, an organization can configure the CyberTIP to send an alert to a security analyst when a new incident report is submitted, or to send a notification to a customer service representative when a customer reports a security incident.

The notification framework can also be used to send automated reports and updates to users on the status of security incidents and investigations.

3. Metric and dashboard:

The CyberTIP includes a built-in metric and dashboard that provides organizations with real-time insights into their security posture. The dashboard displays a variety of metrics, such as the number of open incidents, the typical response time to occurrences, as well as the most common attack vectors. Organizations can utilize this information to identify areas where their security posture needs improvement and to track the efficiency of their safety controls over time.

4. AI Automation:

The CyberTIP uses artificial intelligence (AI) to automate many of the tasks involved in security incident investigation and response. This includes tasks such as:

- Correlating data from different sources to identify the primary cause of an incident
- Prioritizing incidents based on their severity and impact
- Suggesting remediation plans and actions

- Generate Case reports

By automating these tasks, the CyberTIP can help security response teams to reply to incidents more speedily and effectively.

a. AI with MIRTE ATTACK integration:

The SR&RGS can be integrated with MIRTE ATTACK, a knowledge base of attack patterns and countermeasures. This integration allows CyberTIP to use AI to identify attack patterns in incident data and suggest appropriate countermeasures.

This integration can help security teams to better understand the threats they are facing and to develop more effective remediation plans.

b. AI support for case reporting:

The CyberTIP can use AI to assist security teams with case reporting. For example, the CyberTIP can automatically generate draft case reports that include a summary of the incident, the root cause, and the recommended remediation plan.

This AI support can help security teams to save time and produce more comprehensive and informative case reports.

5. Information repository of incidents for research works and other productive uses (where other companies can learn for each other and applying the learnt knowledge to their own systems):

The CyberTIP can be used to create a repository of security incidents that can be used for research and other productive purposes. Organizations can also use the incident repository to learn from the experiences of other organizations and to improve their own security posture. For example, an organization can identify the most common attack vectors used against financial institutions and implement additional security controls to protect themselves from those attacks.

The CyberTIP is a powerful tool that can help business organizations of all sizes to improve their security posture and reduce the risk of security incidents. The key features of the CyberTIP, such as role-based access control, the notification framework, the metric and dashboard, AI automation, and the information repository, make it a valuable tool for security teams of all sizes.

4. Designing and Implementing a Micro-Services-Based CyberTIP with AI

To build the CyberTIP using a microservices architecture (9), The following technologies are used (as also shown in Fig. 2):

- Web UI (Frontend): React
- Backend Technologies: Python (Flask, FastApi, or Django), Java, or C++
- Storage: PostgreSQL (relational database) and MongoDB (NoSQL database)
- AI Automation System: GPT (Generative Pre-Trained Transformer) for OpenAI

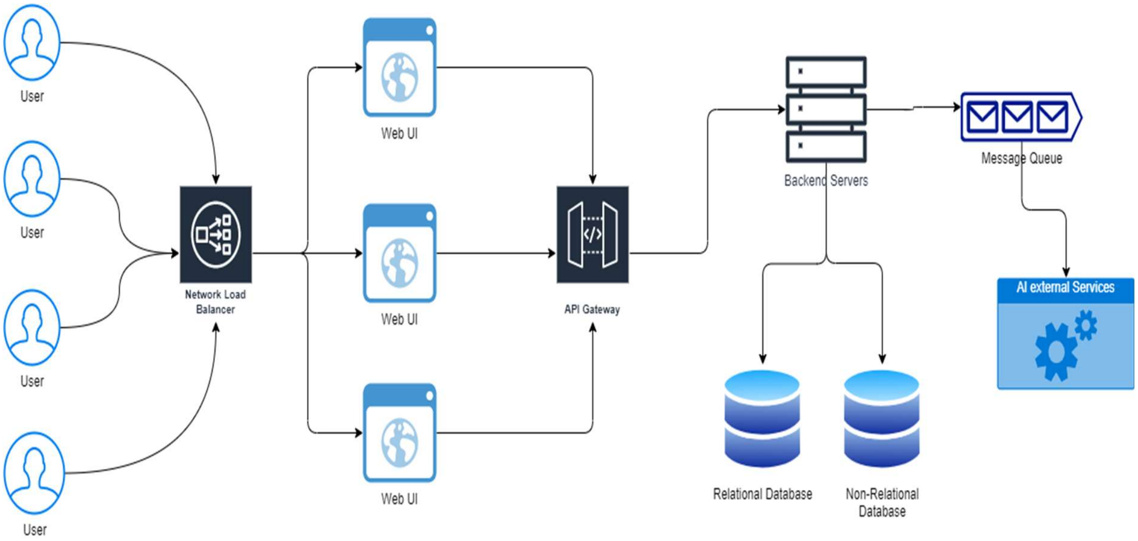

Fig 2: A Diagram showing a micro-service based CyberTIP with AI

Web UI (Frontend)

The web UI section of the Cyber Threat Intelligence Sharing Platform (CyberTIP) is responsible for providing users with a user-friendly interface for interacting with the system. This includes displaying dashboards, reports, and other relevant information, as well as allowing users to perform various tasks, such as submitting incident reports, managing users, and configuring the system. React is a popular JavaScript library for building user interfaces. It is known for its speed, flexibility, and ease of use.

Backend Technologies

The backend technologies for the Cyber Threat Intelligence Sharing Platform (CyberTIP) are responsible for processing incident reports, generating reports, and performing AI-powered automation. Python is a popular programming language for developing web applications. It is known for its simplicity and readability. Flask, FastApi, and Django are popular Python web frameworks

Storage

For the storage of the Cyber Threat Intelligence Sharing Platform (CyberTIP), we used both relational and NoSQL database technologies.

Relational database

A relational database is a type of database that stores data in tables. Each table has a number of columns, and each column can store a specific type of data, such as text, numbers, or dates. Relational databases are well-suited for storing structured data, such as user metadata, such as passwords, usernames, and roles. We would use a relational database like PostgreSQL to store user metadata in the Cyber Threat Intelligence Sharing Platform (CyberTIP). PostgreSQL is a popular relational database management system that is known for its reliability and scalability.

NoSQL database

A NoSQL database is a type of database that does not use the traditional table-based structure of relational databases. NoSQL databases are well-suited for storing unstructured data, such as the reports that would be generated and other relevant documents used by and on the system. We would use a NoSQL database like MongoDB to store non-relational information in the CyberTIP. MongoDB is a popular NoSQL database management system that is known for its flexibility and scalability.

AI Automation System

The AI automation system in the Cyber Threat Intelligence Sharing Platform (CyberTIP) would be responsible for the following tasks:

- Automation and report generation: The AI system could automate the generation of reports, such as incident reports, security posture reports, and threat intelligence reports. This would free up security analysts to focus on more complex tasks.
- Anomaly detection in files and information provided: The AI system could scan files and information provided by users for anomalies. This could help to identify potential security threats, such as malware or malicious code.
- User and entity behavior analysis: The AI system could analyze the behavior of users and entities on the network to identify suspicious activity. This could help to detect advanced persistent threats (APTs) and other sophisticated attacks.

How the AI automation system would work

When an incident occurs, a user would submit an incident report to the Cyber Threat Intelligence Sharing Platform (CyberTIP). The AI system would then analyze the information in the incident report to identify the root cause of the incident and to suggest appropriate countermeasures. The AI system would also generate a report that summarizes the incident, its root cause, and the recommended countermeasures. This report would then be sent to the appropriate security teams and supervisors

Building the AI automation System

The AI automation system could be built using a variety of AI tools and frameworks, such as TensorFlow, PyTorch, and scikit-learn. However, the newly introduced GPTs, such as ChatGPT, are particularly well-suited for building this type of system. GPTs are large language models that can be trained to perform a variety of tasks, including text generation, translation, and code generation. To build a GPT-based AI automation system for the CyberTIP, we first train the GPT on a dataset of security incident data. This dataset would include information about the types of incidents that have occurred, the root causes of the incidents, and the countermeasures that were taken. Once the GPT is trained, we could use it to develop AI agents that can perform the tasks described above, such as report generation, anomaly detection, and user and entity behavior analysis.

5. Outcome / Result of the System

1. AI-driven automation

The CyberTIP can automate a variety of security tasks, such as incident reporting, report generation, anomaly detection, and user and entity behavior analysis. This can free up security analysts to focus on more complex tasks and improve the overall efficiency of the security team.

2. Improved organization efficiency

The CyberTIP can help to improve the overall efficiency of the organization by providing a centralized repository for security data and reports. This can make it easier for security analysts to identify and respond to security incidents, and can help to improve the organization's overall security posture.

3. Detecting Advanced and Unknown Threats

The CyberTIP can use AI to detect advanced and unknown threats that may be missed by traditional security solutions. This can help the organization to protect itself from the latest cyber threats and reduce the risk of a data breach or other security incident.

4. Real-time Alerting

The CyberTIP can provide real-time alerts about security incidents. This allows the organization to respond to incidents quickly and effectively, and can help to minimize the damage caused by a security incident.

5. Dashboard and reporting

The CyberTIP provides a dashboard and reporting features that can be used to track security trends and identify areas where improvement is needed. This information can be used to improve the organization's security posture and reduce the risk of future security incidents.

Overall, the CyberTIP can provide a number of benefits to organizations, including improved security posture, reduced risk of security incidents, and improved organizational efficiency.

Here are some specific examples of how organizations can benefit from the CyberTIP:

- A security analyst at a financial services company can use the CyberTIP to automate the generation of incident reports, freeing them up to focus on investigating and responding to incidents.
- A security manager at a healthcare organization can use the CyberTIP to track security trends and identify areas where improvement is needed, such as areas where employees are most likely to click on phishing emails.
- A security engineer at a retail company can use the CyberTIP to detect advanced and unknown threats, such as malware that is designed to evade traditional security solutions.

6. Conclusion

The CyberTIP platform is a powerful tool that can help organizations to improve their security posture and reduce the risk of security incidents.

The CyberTIP can be used by organizations of all sizes and industries to improve their security posture and reduce the risk of security incidents. It is highly recommended that all organizations consider implementing a CyberTIP solution. The benefits of the CyberTIP far outweigh the costs, and can help organizations to protect themselves from the latest cyber threats and reduce the risk of a data breach or other security incident.

References

1. T. Magele, "E-security in South Africa: White paper prepared for the Forge Ahead E-Security Event," 2005. [Online]. Available: www.forgeahead.co.za. [Accessed: Jan. 2, 2018].
2. G. Arthur-Mensah, "Ghana records GH¢49.5m losses through cyber fraud in first half of 2023," Ghana News Agency, Sep. 4, 2023. [Online]. Available: https://gna.org.gh/2023/09/ghana-records-gh%C2%A249-5m-losses-through-cyber-fraud-in-first-half-of-2023/
3. National Cyber Security Policy & Strategy," International Telecommunication Union, 2015. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/ National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf. [Accessed: Date of Access
4. K. K. Adu, "Framework for digital preservation of electronic government in Ghana," Doctoral dissertation, University of South Africa, 2015.
5. R. Boateng, L. Olumide, R. S. Isabilija, and J. Budu, "Sakawa-cybercrime and criminality in Ghana," Journal of Information Technology Impact, 2011.
6. Africa Cyber Report," in Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness, 2016.
7. National Communications Authority, "National Cybersecurity Policy and Strategy for Ghana," 2019. [Online]. Available: https://www.nca.org.gh/documents/official-documents/. [Accessed: Date of Access]
8. Fig. 1. [Online]. Available: www.cybersecurity.gov.gh/report. [Accessed: Date of Access].
9. O. Zimmermann, "Microservices tenets," Comput. Sci., vol. 32, pp. 301-310, 2017, doi: 10.1007/s00450-016-0337-0.