1/1/2024

Incident Monitoring Tool

Final Year Project

Mark Doyle
C00257481

Contents

Introduction

The Cyber Security Incident Monitoring Tool is an application designed to actively monitor a variety of trusted sources of information that's based on reported cyber security incidents. When a report is published, the tool extracts key information from it through the form of a RSS Feed. This information is show to the tool's user as seen below.

Home About IMT

Date	Title	Description	Link
Fri, 19 Apr 2024 10:38:15 ...	Is it safe to message other ...	WhatsApp will soon suppo...	https://www.kaspersky.co...
Fri, 19 Apr 2024 06:04:31 ...	Transatlantic Cable podca...	Episode 343 of the Kaspe...	https://www.kaspersky.co...
Wed, 17 Apr 2024 11:29:0...	How to prevent surveillanc...	Data collected by advertisi...	https://www.kaspersky.co...
Tue, 16 Apr 2024 16:51:1...	EM Eye: data theft from sur...	We explain in simple terms...	https://www.kaspersky.co...
Fri, 12 Apr 2024 16:12:13 ...	Mitigating the risks of resid...	What are residential proxi...	https://www.kaspersky.co...
Wed, 10 Apr 2024 15:02:0...	Transatlantic Cable podca...	Episode 342 of the Kaspe...	https://www.kaspersky.co...
Wed, 10 Apr 2024 11:00:0...	Kaspersky Next: our new p...	Kaspersky rolls out its ne...	https://www.kaspersky.co...
Tue, 09 Apr 2024 14:32:2...	How to verify the authentic...	An in-depth look at ways t...	https://www.kaspersky.co...
Fri, 05 Apr 2024 14:11:20 ...	Note-taking apps and to-d...	An overview of private and...	https://www.kaspersky.co...
Thu, 04 Apr 2024 17:26:1...	Transatlantic Cable podca...	Episode 341 of the Kaspe...	https://www.kaspersky.co...
Thu, 15 Feb 2024 08:38:1...	Cyber security – where too...	As low-quality content is g...	https://www.cshub.com/att...
Fri, 05 Jan 2024 09:02:27 ...	IOTW: Victoria Court recor...	Unauthorized access disr...	https://www.cshub.com/att...
Fri, 22 Dec 2023 08:42:51 ...	IOTW: Xfinity data breach i...	Exposed data includes us...	https://www.cshub.com/att...
Mon, 18 Dec 2023 11:31:0...	How ransomware extortion...	Dr Jason Nurse reflects o...	https://www.cshub.com/att...
Fri, 15 Dec 2023 08:27:50 ...	IOTW: Russia-linked cybe...	Powerful attack knocked ...	https://www.cshub.com/att...
Fri, 08 Dec 2023 09:01:16 ...	IOTW: HTC confirms cyber...	BlackCat/ALPHV ransom...	https://www.cshub.com/att...
Fri, 08 Dec 2023 09:54:14 ...	Russian FSB accused of s...	Star Blizzard has targeted...	https://www.cshub.com/att...
Thu, 07 Dec 2023 11:15:2...	BEC attacks on law firms s...	Law firms increasingly tar...	https://www.cshub.com/att...
Thu, 07 Dec 2023 14:52:1...	Cyber criminals attack bus...	Researchers warn of a sh...	https://www.cshub.com/att...
Wed, 06 Dec 2023 10:20:...	Fancy Bear group exploits ...	Threat actor leveraging p...	https://www.cshub.com/att...
Tue, 05 Dec 2023 10:49:4...	Sellafield nuclear site "att...	Sellafield reportedly infec...	https://www.cshub.com/att...
Mon, 04 Dec 2023 08:54:4...	DDoS attack-for-hire servi...	Threat actors continue to ...	https://www.cshub.com/att...
Wed, 31 Aug 2022 12:57:4...	Student Loan Breach Exp...	2.5 million people were aff...	https://threatpost.com/stud...
Tue, 30 Aug 2022 16:00:4...	Watering Hole Attacks Pus...	Researchers uncover a w...	https://threatpost.com/wate...
Mon, 29 Aug 2022 14:56:1...	Tentacles of '0ktapus' Thr...	Over 130 companies tangl...	https://threatpost.com/0kta...
Fri, 26 Aug 2022 16:44:27 ...	Ransomware Attacks are o...	Lockbit is by far this summ...	https://threatpost.com/rans...
Thu, 25 Aug 2022 18:47:1...	Cybercriminals Are Selling...	Tens of thousands of cam...	https://threatpost.com/cybe...
Wed, 24 Aug 2022 14:17:0...	Twitter Whistleblower Co...	Twitter is blasted for secur...	https://threatpost.com/twitt...
Tue, 23 Aug 2022 13:19:5...	Firewall Bug Under Active ...	CISA is warning that Palo ...	https://threatpost.com/firew...
Mon, 22 Aug 2022 13:59:0...	Fake Reservation Links Pr...	Fake travel reservations a...	https://threatpost.com/rese...
Fri, 19 Aug 2022 15:25:56 ...	iPhone Users Urged to Up...	Separate fixes to macOS a...	https://threatpost.com/ipho...
Thu, 18 Aug 2022 14:31:3...	Google Patches Chrome's...	An insufficient validation i...	https://threatpost.com/goo...

Tools Used

The Incident Monitoring Tool is made using a combination of Java, Eclipse's WindowBuilder and MITRE ATT&CK. These tools allow for a collection of RSS Feeds and presents the user with that information along with information from a valid library of cyber security Tactics & Techniques from MITRE. The following tools and considerations were what I considered and chose in the early development stages of the tool.

Why These Tools

Java

As a programming language, java has a wide range of libraries that can be used to suit the flexibility of the tool. Java is mainly used for heavy workload applications by using an object-orientated approach, which is easily integrable with Eclipse's WindowBuilder. These features benefit the tool's overall performance and integration with RSS Feeds and MITRE.

Eclipse

Eclipse's WindowBuilder's interface is the best option for designing the tool. It's easy to use with other programming languages especially java. It's able to handle the workload of the Incident Monitoring Tool.

Mitre

Because MITRE has a vast library of information and is a major stepping stool in cyber security. Having this integration between the tool and MITRE is one of the many reasons why this library is a critical part of the tool.

Considerations

Languages

PHP

This coding language is mainly used to develop web-based applications. The tool follows this design idea, but the language isn't able to handle the performance and it doesn't have the ability for managing the data that java can, the language also doesn't have the wide range of languages when compared to a language such as java.

Bash Scripting

This is more commonly used to automate scripts, while the tool actively checks sources of information it wasn't the best choice for the tool. Error handling isn't something that Bash scripting can do which holds some challenges as the tool requires this function in order for it to handle the retrieval of the RSS Feeds.

Research

The research that I had to do to help develop the tools is to understand what the tool has to do and what it has to be a positive impact to cyber security. This starts off by learning the impact that cyber-attacks have on everyday environments and the costs it takes to rectify them.

Once that was done, I started researching how I can pull the information needed for what the user wants to see and what information is beneficial.

Statistics

Affected Sectors

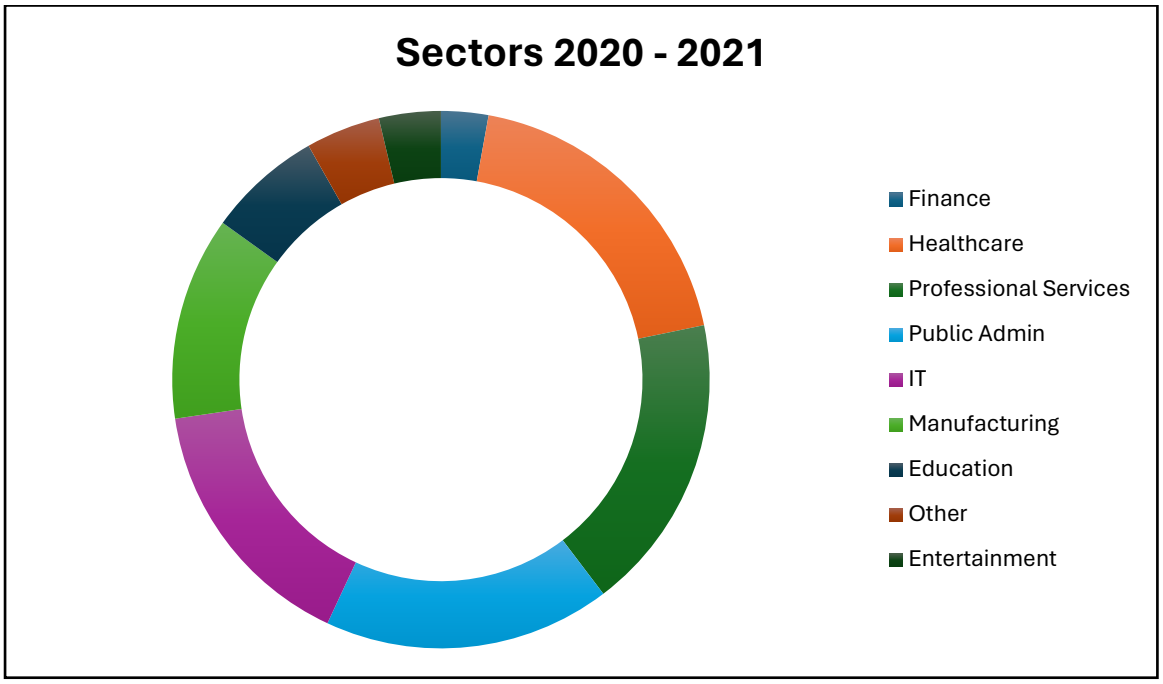


Figure 1

Harriss and Villanueva, 2022.

The statistics shown in Figure 1 are industries and their rate of how often that they were attacked during the period of 2020 – 2021. This timeframe was heavily and publicly reported about and how they were affected by their reported cyber-attack. The below figures are the top 5 industries affected by a "Basic Web-Application "and how often they were attacked.

1. Finance: 226
2. Healthcare: 173
3. Professional Services: 164
4. Public Administration: 158
5. IT: 144

Average Costs

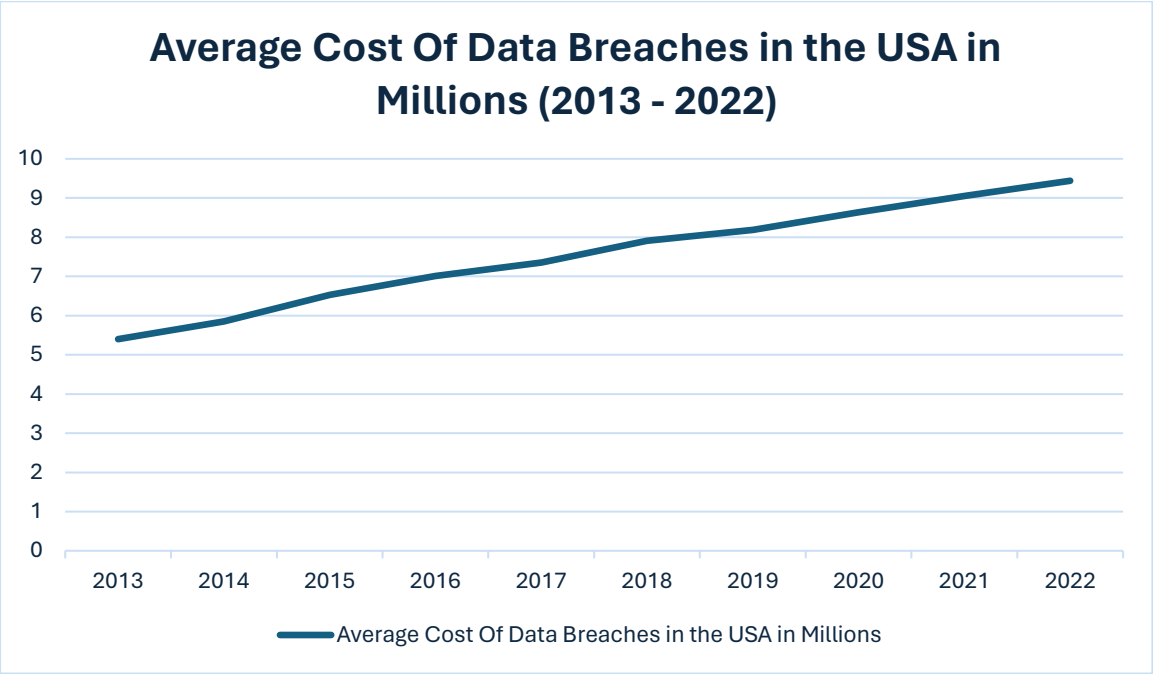
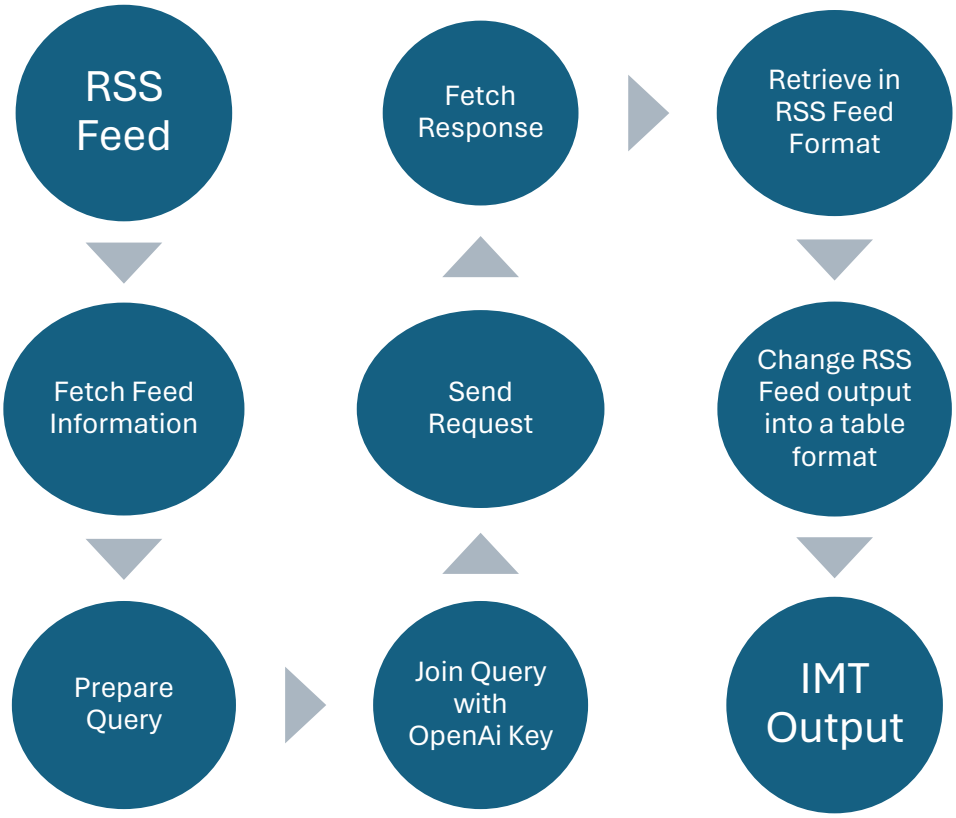


Figure 2
Harriss and Villanueva, 2022

The figures shown in Figure 2 are one dating from 2013 to 2022. These figures are the average costs to recover from data breaches within the USA in millions. The highest amount being in the years 2021 – 2022, this is because of the Covid-19 Pandemic which was a difficult time for not just retail and healthcare workers but for IT Infrastructure too.

Initial Design

The initial design started off as a process of data retrieval and processing that data into something the user can use and learn from



This design incorporates pulling RSS Feed information and presenting it to OpenAI to deliver an effective approach in mitigating the reported attack, the output is that of an RSS Feed making it easier to output via a tabled approach.

Inputs

RSS Feed

The RSS Feeds are a crucial part in the operation of the Incident Monitoring Tool. This is because they provide real-time data on reported cyber threats. These feeds are a constant and continuous source of information for the tool to obtain and use. Below is an example of a typical RSS Feed.

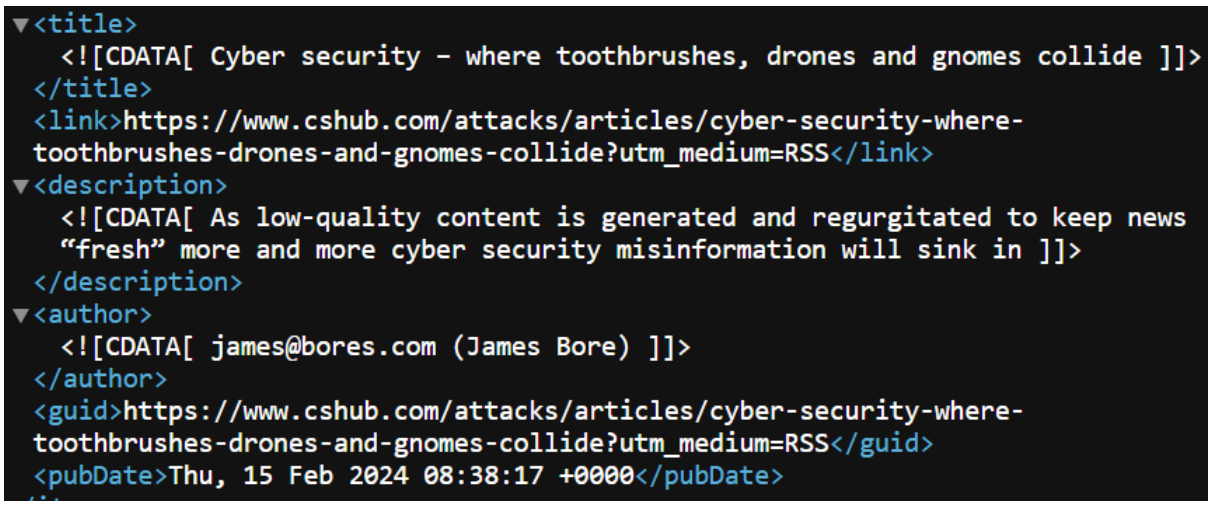


Figure 3

MITRE's API

Incorporating MITRE's Tactics & Techniques API enhances the Incident Monitoring Tool's capabilities, this is because the API gives the tool and its user access to a library of cybersecurity knowledge and information on threats and methods of attacks used by cyber criminals. This combination allows the tool to present the user with a detailed report on the incident that includes verified data on cyber threats from a reliable source.

Sub-Technique Criteria

The outputted sub-techniques criteria need to relevant to each reported attack. The tool uses these as a guide and specific to what they're looking for based on MITRE's TTID's[1]

[1] Tactics & Techniques ID

Processes

Data Retrieval

The Incident Monitoring Tool needs to actively monitor the mentioned trusted sources which includes MITRE's API and RSS Feeds, the sources provide accurate information to the tool, this information is not only accurate but is up-to-date and recent.

MITRE Similarities

MITRE's framework provides an effective way of mitigating cyber related threats. Although other platforms such as CrowdStrike and Kaspersky's Cyber Map offer the same support which I'll talk about later, but MITRE allows its users to limit what they see and see certain categories that relate to them within their organization.

These filtered / set categories is a consistent and effective way for a user to find relevant information that they can use, Similar to the IMT monitoring tool it allows the user to receive effect information that's related to them.

OpenAI

As sceptical and mis-informative that ChatGPT and its services are told to be, they can be used as a valuable source of information in certain areas. Using OpenAI[2], the IMT[3] tool can retrieve relevant information about a reported attack. Such as effective mitigation techniques along with TTID's relating to them.

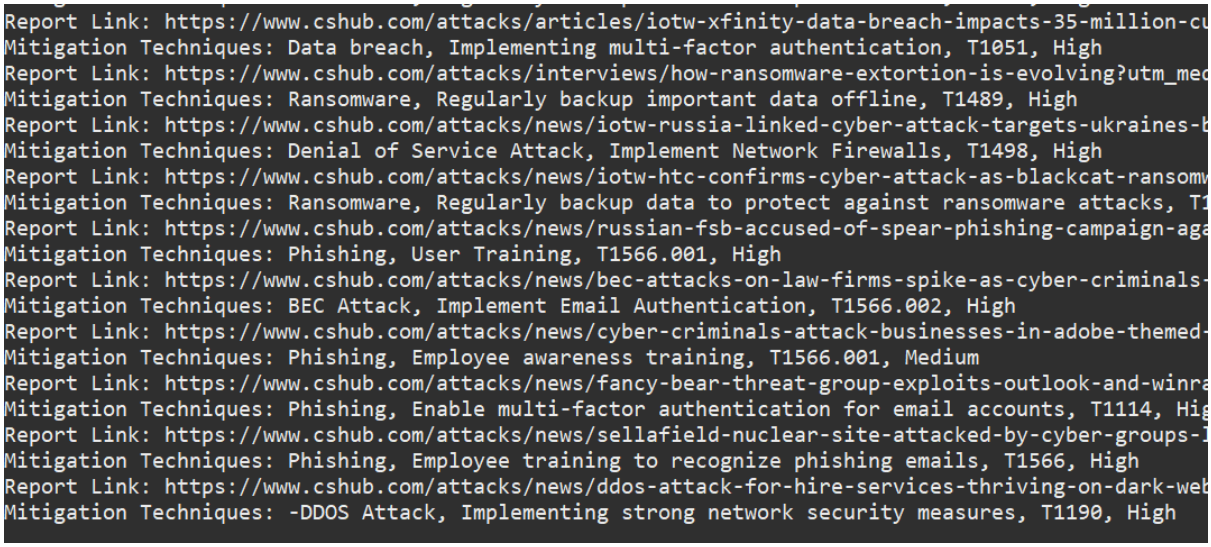


Figure 4: OpenAI Response

The information shown in Figure 5 is the output of the response "Using the link, list the following in the shortest way possible, in a list/brief style. Type of attack, Top 3 mitigation techniques and an associated TTID, Severity Level" given by the tool. OpenAI then gives the above response associated by the RSS Feed Report Link. The Tool takes this and adds this to the overall output.

Using a GUI based output, the question would have to be changed so that a suitable response is given back. This request tells OpenAi to respond in an RSS Feed format so that the code in the application knows what headings it needs to remove and what information it takes from the response. Both for clarity and efficiency, the best query/request was decided to be

"Using the link " + link + ", list the following in a concise RSS feed format: <Kind_of_attack>, <One_Mitigation_Technique>, <MITRE_TTID>, <Severity_Level>"

[2] Developer of AI technologies that use language processing and machine learning.
[3] Abbreviation for Incident Monitoring Tool

Outputs

Severity Score

The Severity Score, which can be seen in Figure 5, during my development stage I had considered using a numbered system but for simplicity and formatting, I decided to use a worded approach. This is because a numbered approach can be technical with regards to opinions and the use of OpenAI, so the user may question the numbered score they get back but when it's a worded approach it's a more effective way of showing the severity of the attack.

Sub-Techniques

These offer a unique view of cybersecurity tactics, providing people with detailed insights into attack methods that are used by attackers. These Sub-Techniques give their user a fresh take and understanding on how to defend against these kinds of attack by using TTID's to easily identify them. The IMT uses these TTID's to give its user something to research further and a legitimate source that they can reference in their research if they need to.

Challenges

This semester was the starting – early development stage for creating the tool. During this time I started researching and identifying ways that I could create the tool. The following are the challenges that I faced during this time.

Structure:

What does the user need?

One of the major points I had to consider while in the early development stage is, What does the user need? Most applications & websites have the user's needed information but it's full of useless, loose-ended information that the user may find confusing and misleading. What the user needs is a straightforward information and mitigations.

What information needs to be shown?

As mentioned above, the user needs to see straightforward information. This information needs to be related to the user and the attack that's being reported, information including,

- Date of the reported Attack
- Kind of Attack
- Description of the Attack
- Recommended Mitigations
- The level of risk the attack has on the user.

Back-End

How can the code be structured?

In the event that the application needs to be updated or modified, having the code's structure in a readable and organised manner is the best approach to handle any changes to it. During the early development stage, I had to structure the code in a way that makes it functional and understandable.

How can the code connect to sources?

During the development stage

Customisation

What can the user change?

The IMT is a user driven application that allows them to customise the information, as mentioned in '**What information needs to be shown**?' the user sees a variety of information,

What customisation options can be given?

The user can change the layout of the table so they can view it in a different order than, date, title

Security

How can the information be verified as legitimate?

During the research phase, each source was verified for legitimacy, the selected sources of information are well known, updated and informative. This is what the tool needs to provide the best information possible for the user.

Database

Due to an unknown fault in my devices xampp, there were many errors involving the user-based system and its database meaning the tool now only does a standard approach rather than a user specific/based approach. However, attempts were made, and examples are below of how it can be done.

```
private JTextField nameField;
private JTextField usernameField;
private JPasswordField apiKeyField;
private JPasswordField passwordField;
private JButton signupButton;
private JButton loginButton;
```

Figure 5

```
private void layoutComponents() {
    JPanel mainPanel = new JPanel(new GridLayout(6, 2, 5, 5));
    mainPanel.setBorder(BorderFactory.createEmptyBorder(10, 10, 10, 10));

    JLabel welcomeLabel = new JLabel("Welcome to The Incident Monitoring Tool");
    welcomeLabel.setFont(new Font("Arial", Font.BOLD, 14));
    welcomeLabel.setHorizontalAlignment(JLabel.CENTER);
    mainPanel.add(welcomeLabel);
    mainPanel.add(new JLabel(""));

    mainPanel.add(new JLabel("Name:"));
    mainPanel.add(nameField);
    mainPanel.add(new JLabel("Username:"));
    mainPanel.add(usernameField);
    mainPanel.add(new JLabel("OpenAI Key:"));
    mainPanel.add(apiKeyField);
    mainPanel.add(new JLabel("Password:"));
    mainPanel.add(passwordField);
    mainPanel.add(signupButton);
    mainPanel.add(loginButton);

    add(mainPanel, BorderLayout.CENTER);
}
```

Figure 6

Figures 5 & 6 show what the gui would ask the user to input, given the user-based experience, they would input their OpenAI key and the code would use that from now on rather than just the same for every user.

```java
private String createHash(String password) {
    try {
        MessageDigest digest = MessageDigest.getInstance("SHA-256");
        byte[] encodedHash = digest.digest(password.getBytes(StandardCharsets.UTF_8));
        return bytesToHex(encodedHash);
    } catch (NoSuchAlgorithmException ex) {
        ex.printStackTrace();
        return null;
    }
}
```

Figure 7

The code in Figure 7 shows how the code would hash the users' passwords when signing up, when they log in the password would then be hashed and if both the stored password and inputted one match, then the system will allow them access

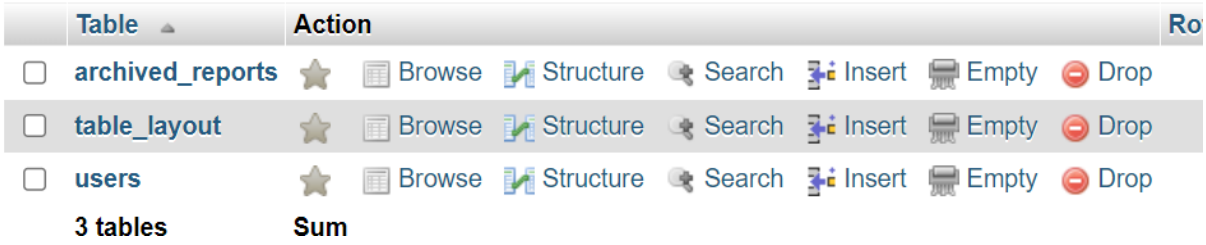


Figure 8

Figure 8 shows the database and the tables it holds which go from users (storing all the users, passwords & OpenAI Key), Table Layout (Storing the saved table layout set by the user) and archived reports (storing any reports the user would like archived for either future research or because they no longer need the report).

Similarities

Although some other applications and websites provide similar information, the IMT has more functionality than just a blog for cyber threats and attacks, below are some examples.

Kaspersky's Cyber Map

Uses a live interactive map providing users with a list of live attacks and their location along with their detected origin. This is a good function to incorporate into the IMT, but it requires a lot of testing and better equipment to handle the live requests, constant updates and effects for the GUI.

CrowdStrike

Unlike Kaspersky's Cyber Map, CrowdStrike provides its user with a less interactive approach in showing reported attacks and more of a blog/article-based approach which the user may find less appealing to Kaspersky.

Security Implications

Tactics & Techniques & Mitigations

The TTID's used are outputted from OpenAI but are linked to MITRE that provide effective mitigations, each one has their own ID which OpenAI retrieves and is corresponded with the given report(s). Each Mitigation that's outputted is the best approach to responding to the reported attack and an effective way of defending against such.

RSS Feeds

RSS Feeds give a brief explanation regarding a reported incident such as its date, the title, and the link for the full report. This information doesn't risk any security to the publisher or the user, however it does advertise/show a reported user's vulnerabilities within the report based on the information given by the organisation.

Legitimacy

As mentioned before, The IMT is an informative, sensitive, protective, but most importantly, it's a legitimate tool. So, in order to uphold these traits, the tool uses verified sources of information to gather information both from a reported attack perspective and a MITRE perspective. This allows the tool to up hole its legitimacy.

Conclusion

Overall, as a whole the Incident Monitoring Tool offers a streamline and effective approach to showing its user an effective way of mitigating against threats, this information is pulled from various legitimate sources of information and through the use of OpenAI, they receive up-to-date and accurate information both in a user friendly and real-time approach. This application is the beginning of teaching users how evolving the cyber industry is and how secure we have to be in order to protect our information.

References

Harris, M., & Villaneuva, R. (2022). Cost of Cybercrime. Grant Thornton, Dublin. Available online: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grantthornton---cost-of-cybercrime-2022.pdf (last accessed April 19, 2024).

Ilyin, Y. (2014). Cyberthreats Map: watch global threats in real time. Kaspersky, Moscow. Available online: https://www.kaspersky.com/blog/cyberthreats-map-watch-global-threats-in-realtime/14939/ (last accessed April 19, 2024).

CISA. (2021). Best Practices for MITRE ATT&CK® Mapping. Available online: https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (last accessed April 19, 2024).

Robertson, A. L. (2023). ATT&CK V14. Available online: https://medium.com/mitre-attack/attackv14-fa473603f86b or https://mitre-attack.github.io/attack-navigator/ (last accessed April 19, 2024).

Crowdstrike. (2023). Crowdstrike Blog. Available online: https://www.crowdstrike.com/blog (last accessed April 19, 2024).