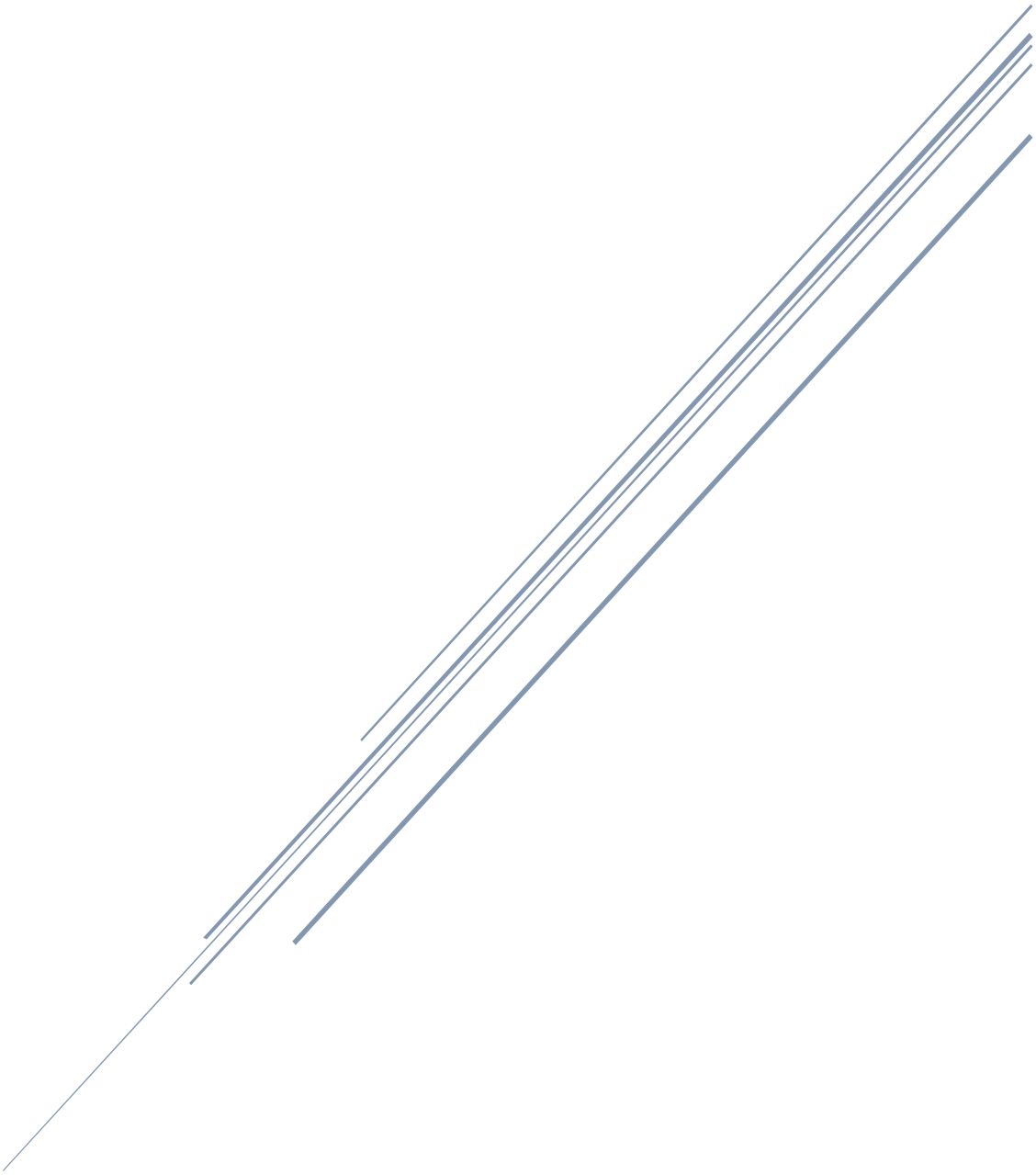
RESEARCH DOCUMENT

Cybercrime & IT Security Final Year Project

Incident Monitoring Tool



Mark Doyle
C00257481

Abstract

This Research document is an overview and a descriptive plan of the research and development of the Incident Monitoring Tool. An instrument that's vital to have in the environment that we live in today. The information that the tool uses, RSS Feed, MITRE ATT&CK and the users' specifications, are a vital combination in tackling the increasing rate of attacks and strain on the cybersecurity industry. As we've all seen through the news and social media, cyber threats are a major threat to any business that stores information by digital means. The Incident Monitoring Tool is a niche in the cyber security market because it takes in the information presented by the reports, extracts information from them, and presents the user with the recommendations needed to prevent the attack from happening to them. This is a major reason why that there's a need for a tool like this in the cyber industry as it fills the gaps that attackers slip through.

Table of Contents

Project Definition

The cyber security incident monitoring tool's design is to actively monitor a variety of trusted sources that provides their viewers with information on reported cyber security incidents. When a report is published and noted by the tool, it extracts key information from it and any critical facts that may be useful for the user to know along with the recommended mitigations retrieved by MITRE ATT&CK layers.

Introduction

With the ever-growing development of the digital environment comes just as much development in potential threats to any liable source, these cyber related threats are constantly evolving and becoming more unpredictable. In order to mitigate these threats, certain measures must be taken to ensure the safety of organisations that are of risk to such attacks.

The objective of this document is to demonstrate the creation of the Incident Monitoring Tool. The tool is not just a Plan B, a reaction after the fact, it is a constantly active tool that monitors trusted sources that report on cybersecurity incidents, reports that are combed through for vital information that will benefit the mitigate a future attempt on another target. This is done by presenting its user with ways of mitigating such threats based on the Tactics and Techniques by MITRE ATT&CK[1] and the user's custom preferences set out by them based on their pre-set vulnerabilities.

As stated above, with the ever-growing threat of cyber-attacks, the Cyber Security Incident Monitoring Tool is a critical asset in a start of defending and ensuring the safety of targets to such attacks. The success and effectiveness of this tool is determined by its ability to achieve its goal in a user-friendly and timely way. The below charts are based on the increase in cyber-attacks in the past 10 years and the most targeted sectors, sectors that the tool can help mitigate such attacks.

How it can be done

The Incident Monitoring tool is a combination of MITRE ATT&C and the information is holds on effective mitigation techniques. Creating a visually appealing and informative display using a WindowBuilder for the user means that the information gathered from RSS Feeds based on recent. This information is then combined with MITRE's Tactics & Techniques in order to provide the user with relevant and up to date information.

Indexing

MITRE's Tactics & Techniques are indexed and compared against the RSS Feed's reports, Once the ky information within the report is identified, it's then categorized by the kind of attack that is reported, this information is then compared to the mitigations of such attack to MITRE's Tactics & Techniques. Given the information provided by the user, the threats and mitigations are categorized according to their level of threat, the most severe being on the top of the list presented to the user

[1]Globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tools Used

A large majority of the tool can be made using a combination of Java, and Eclipse's WindowBuilder. Using websites that report on cyber security incidents and using the tool we can reference these by retrieving key information on the reported cyber-attack. This information can be used to recommend effective mitigation techniques that're related to the reported cyber-attack.

Why?

Java

The reason why I have chosen to use java as the programming language because it has a wide variety of libraries such as Jsoup and Apache's http client that can be used to suit the flexibility of the tool, java is a language that is used for heavy workload applications by using an object-oriented approach which is easily integrable with Eclipse's WindowBuilder. This benefits the tools performance and integration with RSS feeds and MITRE.

Eclipse WindowBuilder

Eclipse's WindowBuilder is a unique interface which uses a drag and drop method which allows the user to easily design their own interface which is a benefit to designing a visually appealing tool which outputs very important and confidential information. The making of this window is turning a complex piece of code into something easy to read which helps its user's network security.

Considerations:

Although there are other programming languages and tools available to use to create the tool, these other tools and languages are as follows.

Languages

PHP:

PHP is mainly for web-based applications although this is the style of application that the tool, however it lacks the performance and most importantly, the scalability that the tool needs to deliver such efficient and up-to-date information which makes it less efficient than java as java is more reliable and has a large variety of libraries compared to PHP.

Bash Scripting

Using Bash scripts causes is less efficient in error handling when compared to java. Given the nature of the tool, the programming behind the tool needs to flexible with automation and scalability which is something that bash scripting lacks in compared to java.

Tools:

Microsoft Visual Studio

Although Visual Studio is a powerful tool, it lacks the cross-platform compatibility compared to Eclipse Window Builder. This level of compatibility is vital for the web-based design that the tool is using.

Swing Designer

This is a more common tool to be used alongside java, but it has an outdated look with less interactive and customization options. The Incident Monitoring Tool requires a more flexible and modern UI design tool.

Statistics

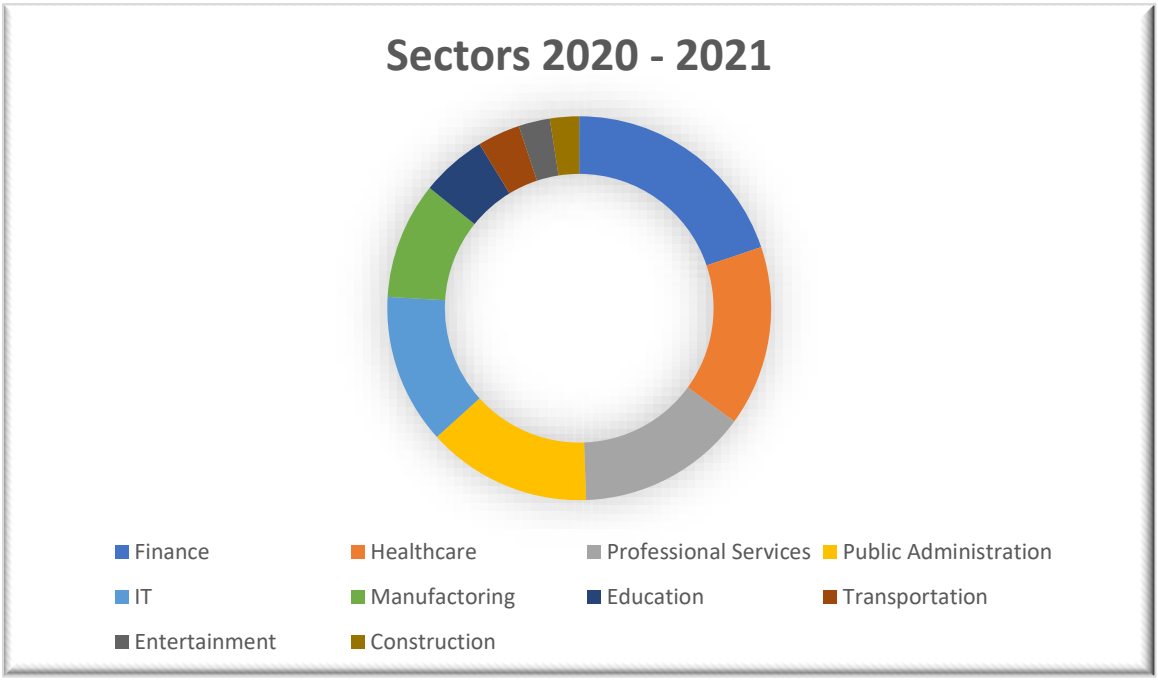


Figure 1

Harriss and Villanueva, 2022.

The statistics shown in Figure 1 shows the industries and their rate of how often that they were attacked during the period of 2020 to 2021 during a time where both heavily publicly reported about and how they were affected by their reported cyber-attack. The top 5 industries and their frequency of attack by a “basic web application” are as follows.

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

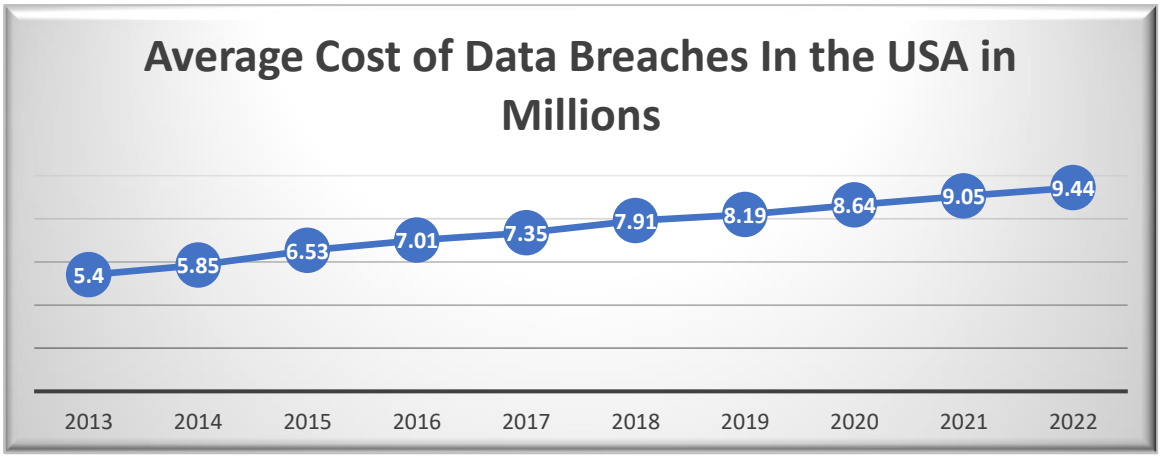


Figure 2: Average Cost of Data Breaches in the USA in Millions $

Harriss and Villanueva, 2022

The Statistics shown in Figure 2 are ones dating from 2013 to 2022 of the average cost in millions, it took to recover from data breaches within the USA. The highest amount being in the years 2021-2022. In the next part of this report, I'll discuss that time and the effect that a major event had on the cybersecurity industry.

Reasoning

Having the Incident Monitoring Tool as a resource in the organisation automatically warns of a potential and a critical attack. This increases the security of the organisation and alerts them to vulnerabilities, and they may not be aware of, the tool may also educate its users on effective mitigation techniques. This differs from other system as it's an early warning system against an attack that doesn't need to reach the organisation for it to be detected.

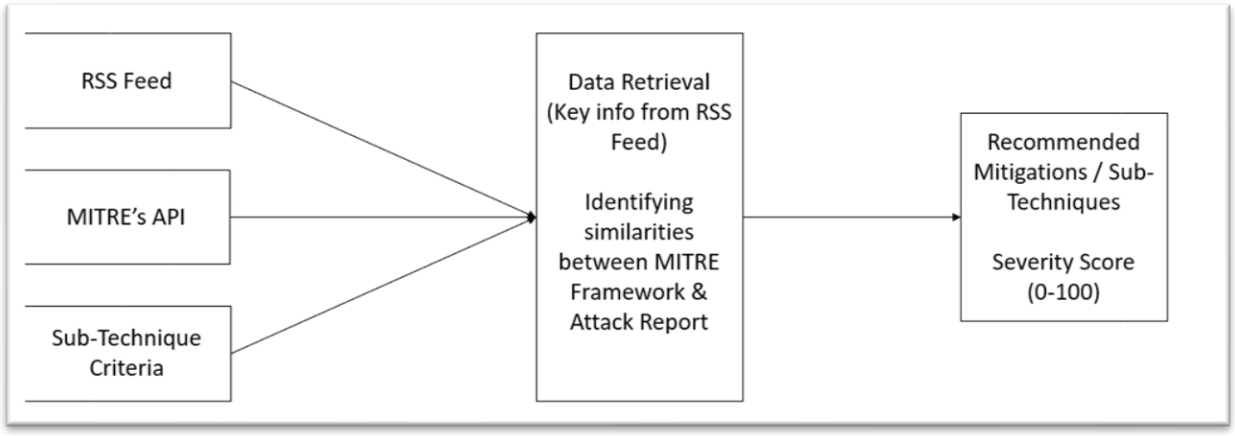


Figure 3: Model of Inputs to Outputs

The data in Figure 3 shows an outline on how the tool's input, the data it uses to create the output and then what it shows to the user.

Inputs

RSS Feed

The RSS Feeds are a crucial part and input of the Incident Monitoring Tool, they provide real-time data on reported cyber threats. The feeds are a constant and continuous source of information for the tool to obtain and use.

MITRE's API

MITRE's API enhances the Incident Monitoring Tool's capabilities in its overall performance, this is because it provides the tool access to MITRE's Tactics & Techniques Matrix. It assists the tool in aligning the reported incidents obtained by the RSS Feeds with cyber-attack techniques that help create a current, effective, and structured framework.

Sub-Technique Criteria

These techniques set specific parameters for the tool to follow and assists in the evaluation and relevance of the reported incident which relates to the user and how severe the attack may be on their organisation if not mitigated depending on the level of severity the attack has.

Output Creation

Data From RSS Feed

The data that the RSS Feeds provide are the foundation to the tool's output, the data includes the nature of the attack, the exploited vulnerabilities, and the methods that the attacker used. This data provides a thorough overview of the analysis.

Similarities Between Framework & Attack Report

By combining MITRE's framework and the data gathered from the RSS Feeds, it allows for an improved categorization of incidents being classified in the means of prompting the user with informative tactics and techniques which are classified based on their effectiveness.

Outputs

Recommended Mitigations & Sub-Techniques

This output is the most crucial and important part of the tool. The outputted mitigations and sub-techniques, as stated previously, are tailored to its user, the recommendations are effective in mitigating the reported attack. The systematic approach ensures that the recommendations are relevant to the attack and the mitigation technique.

Severity Score

The outputted severity score is a threat level number based on the severity the associated attack has on the user's company. The higher the score, the more dangerous the reported attack is on the company. How would the tool be able to determine the severity score? As mentioned above, the tool puts together the information gathered from RSS Feeds and the information about the company from the user, it then determines a suitable ranking of each report and presents the user with the attack most harmful to them starting from the highest risk to the lowest risk.

Covid-19

As difficult as 2020-2022 was for healthcare workers, it was also a difficult and vulnerable time for IT infrastructure with the world adapting to different work environments, which meant a company's network had to change to allow its workers to work from home, changes that allowed for attacks on their network and staff. These worldwide changes open the floodgates for risk and data breaches caused by cyber-attacks. The most common attacks during that time are as follows.

Ransomware

A well-known example of a Ransomware[2] is the 2021 HSE Incident which cost the country over €600 million in upgrading their infrastructure. This attack caused mass panic across the country and healthcare services which effected the lives of people who are of high risk.
(Harris and Villanueva, 2022)

System Vulnerabilities

Ireland's Cybersecurity Centre reported a major system vulnerability[3] within an Apache Log which only effected users that operate the infrastructure of its web server.
(Harris and Villanueva, 2022)

Cryptocurrency Attacks & Fraud

Cryptocurrency[4] attacks and Fraud are some of the most common forms of tools used by attackers in an attempt at Money Laundering[5] and evading being charged with fraud. In an effort to mitigate these attacks within the finance industry, these attacks are being tracked and traced back to the attackers which was difficult to manage during the pandemic.
(Harris and Villanueva, 2022)

Malware

At the beginning of 2021 a decrease in malware was highlighted by the European Union Agency for Cybersecurity, this is linked to the above pandemic causing employees to work from home. However, when restrictions were eased and employees could continue working in their offices, this notable decrease started rising.
(Harris and Villanueva, 2022)

Final Analysis

Overtime, companies, and cyber security experts have then since learned from these attacks and ways of protecting from the above attacks. The incident monitoring tool takes advantage of this to present its user with relevant, accurate and effective information.

[2] Type of malicious software designed to block access to a computer system until a sum of money is paid.
[3] Flaw / weakness in a computer's system, security procedures, internal controls that could be exploited to violate the system security policy.
[4] Digital currency which is an alternative form of payment created using encryption algorithms.
[5] Disguising the origins of illegally obtained proceeds so that they appear to be legitimate.

MITRE ATT&CK

MITRE's framework provides its users with a detailed understanding of its Tactics and Techniques which outline varies methods that attackers use to achieve their objective. These are known as high level goals that include gaining initial access, execution, and evasion of their attack. MITRE uses a variety of data sources that are used to detect and investigate specific methods of attack. This is vital to organisations that rely on enhancing their methods of security.

The incident Monitoring tool uses these features as a primary source of information which the tool categorizes and analyses the reported incidents providing a groundwork for how the tool operates. The Framework's organised approach allows the tool to interpret and navigate through the information in a report and output its respected mitigation.

Navigator Layer

Figure 4: Navigation Layer

Figure 4 is an example of MITRE's layers and the information that they contain. The variety of information that MITRE contains is used to the tool's advantage both in visualisation and output. The mitigations shown to the user are taken from MITRE but shown to them in a more visually appealing and effective way.

Users & Impact

The most important piece of information that will help the Incident Monitoring tool to improve and adapt is feedback. The tool's users are a prime example of how their feedback will help develop the tool even further. The following users are pivotal in providing feedback for the tool.

Security Analysts

Their Role:

A cybersecurity analyst's job is to protect and monitor their company's network against any threats, they are responsible for the safety of their data and the information they collect.

Their Impact:

Given the role in an organisation is a major reason why the incident monitoring tool is something that they should use as it will provide them with accurate information on real-time cyber related incidents, the tool also provides a threat assessment and successful mitigations on how they can protect against the reported attack.

Security Operations Center

Their Role

Much like a security, is more important as they are a collective of highly dependent analysts who are assigned high level threats to manage and mitigate.

Their Impact

The incident handling tool would be a great asset to a SOC as would they be to the tool. The rate of which that they manage incoming threats will test the tool's performance and accuracy, having this will reduce the time and the stress of handling a particular incident, this is because the toll will provide them with accurate methods of mitigating the reported attack.

IT Administrators

Their Role

An IT Administrator is responsible for a company's network layout, infrastructure, and security. They oversee the function and maintenance of the IT devices in the company.

Their Impact

A strong IT infrastructure is the first step to a secure organization and a strong network, Attacks such as a DDOs attack can compromise a network and their organisation's primary function. The tool would benefit them greatly by helping them in strengthening a network by implementing the suggested and backed up mitigations.

Risk Management Team

Their Role

Similar to the above roles, a Risk Management Team manage threats that could have a big impact on the organisation if the attack was successful. They follow a strategic plan in monitoring and mitigating a reported attack.

Their Impact

Having precise and informative pieces of information provided by the monitoring tool would benefit their workload and how long each incident takes to handle and mitigate their threat, this also allows the team to streamline their effectiveness and time to allocate their time and resources to each threat.

Similarities

Given the nature of the tool being incident monitoring and reporting, there are some similarities to the purpose of the tools such as,

Kaspersky's Cyber Map

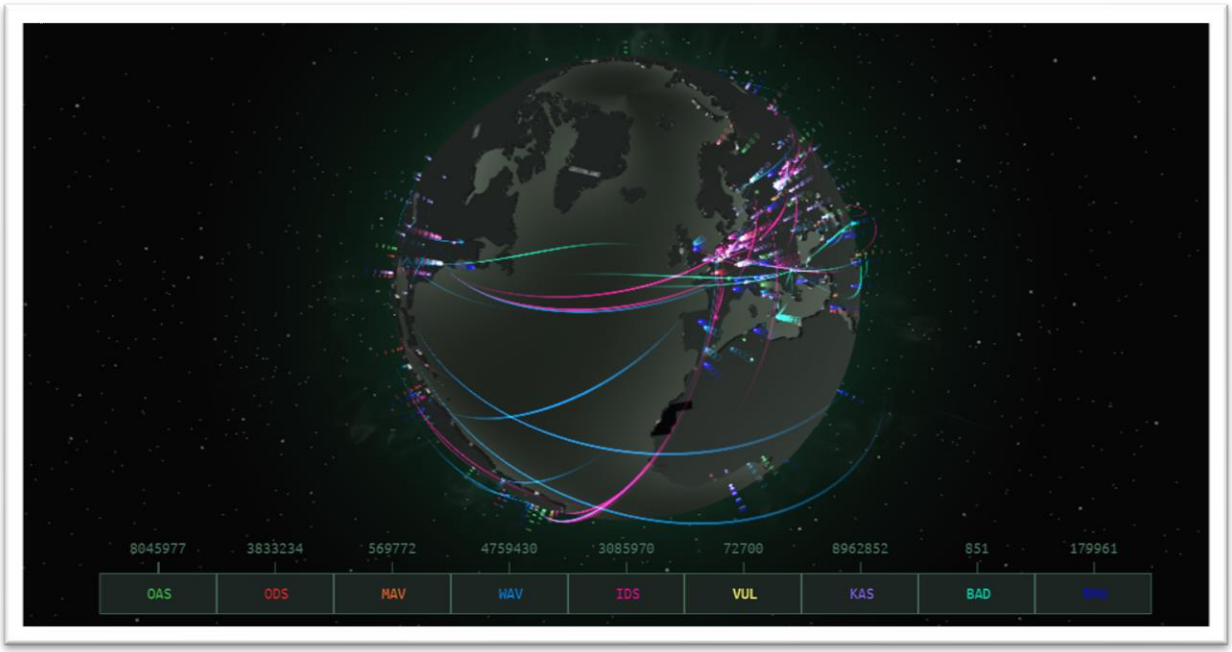


Figure 5: Cyber-Map

It's an interactive globe that provides real-time cybersecurity events around the world which includes statistics on what attacks are more common than other and rates the countries based on the rate that they're attacked.

CrowdStrike

CrowdStrike's Blog provides its users with real-time "endpoint security events" and their data that's needed to identify the attack and how to respond to it.

Security Implications

The Incident Monitoring Tool relates to cybersecurity because of its functionality and capabilities. It's a tool that utilizes cyber related frameworks such as MITRE's Tactics and Techniques and RSS Feeds on cyber-attacks around the world.

Tactics & Techniques

As stated previously, MITRE ATT&CK has an extensive understanding of cyber security and security implications based on the information of effective mitigations. This allows the Incident Handling Tool to present its user with up-to-date and strategic information.

Mitigation Strategies

The outputted mitigation strategies provide the user with a blueprint to how they can help prevent against major threats to their organisation. The tool maps MITRE's framework to present the user with the strategies that they'll need to defend their organisation.

RSS Feeds

The tool's combination with RSS Feeds allows for real-time monitoring o cyber attacks around the world. Not only do the feeds give the tool a level of knowledge, but they provide the tool with a way of verifying the source of information as a trusted source for reported attacks.

Legitimacy

The nature of the tools is one of great security and compromise, if the tool doesn't perform to standard, it may provide ineffective methods of mitigating an attack therefore causing further risk to an organisation and compromising the integrity of the tool.

Conclusions

The Incident Monitoring Tool utilises modern day cyber security tools and sources such as MITRE ATT&CK and RSS Feeds. Using these tools, The Incident Monitoring Tool is a proactive approach to cyber security and mitigation. This method of cyber security actively monitors trusted sources of information by extracting key information about the reported threat, and with the combination of MITRE ATT&CK, presents the user with an effective way of protecting against attacks that're reported and identified as a threat by the tool.

In conclusion, The Incident Monitoring Tool is a vital piece of cyber security by combing the already available and moderns means of reporting and mitigation that benefits its user, whether it be a lone cyber security analyst handling minor threat or a SOC Team handling major and dangerous threats

References

Harris, M., and Villaneuva, R. (2022) Cost of Cybercrime, Grant Thornton, Dublin. Available online: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---cost-of-cybercrime-2022.pdf

(last accessed, 8th December 2023)

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-real-time/14939/#:~:text=April%202%2C%202014-,Kaspersky%20Lab%20presents%20its%20new%20interactive%20Cyberthreats%20Realtime%20Map.,the%20world%20in%20real%20time.

(Last Accessed, 8th December 2023)

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, 8th December 2023)

Robertson, Amy L (2023) ATT&CK V14. Available online https://medium.com/mitre-attack/attack-v14-fa473603f86b or https://mitre-attack.github.io/attack-navigator/

(Last Accessed, 8th December 2023)

Crowdstrike (2023) Crowdstrike Blog, Available online https://www.crowdstrike.com/blog
(Last Accessed, 8th December 2023)