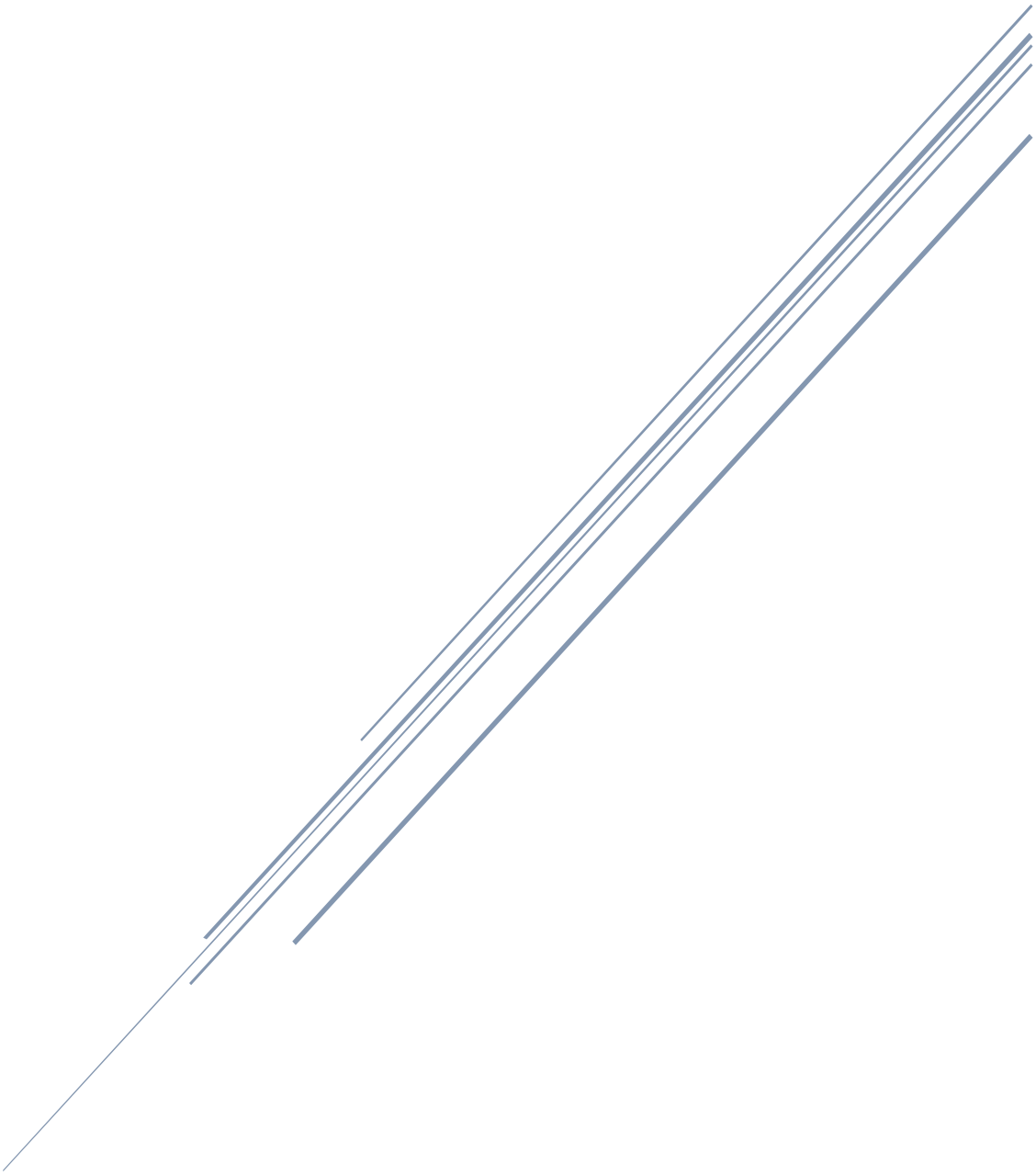
CYBERCRIME & IT SECURITY YR 4 PROJECT SPECIFICATION

Incident Monitoring System



Mark Doyle
C00257481

Table of Contents

Project Specification

Project Definition

The Cyber Security Incident Monitoring Tool is designed to actively monitor trusted sources of that provide informative reports of incidents involving a cyber security report. When a new report is found, the tool extracts critical information that holds key features of the reported attack, the tool's process of obtaining this information is precise and relevant to the information at hand.

One of the key features of the Incident Monitoring Tool is the Implementation of MITRE ATT&CK's Tactics and Techniques Matrix which assists the tool is creating a classification scheme which the tool uses to systematically categorize reported incidents based on the information obtained with the report, this method ensures that in the information is relevant and accurate to a set Framework of mitigations and techniques.

The tool's outputted results consist of a generated dynamic threat profile for every reported incident, the profile serves as a guide to the intended organization by evaluating the severity of each incident and shows an informative plan on how to mitigate an attacked based on the report.

In order to have a more reliable and user-friendly approach, the tool allows its users to create their own layers tailored to MITRE, meaning that they can add specific settings to the overall design to suit their needs and guidelines within their organisation's rules and regulations.

Overall, this tool is a dynamic way of combining the information gathered by the system about new threats and risk profiles with the Tactics and Techniques of MITRE ATT&CK.

Tools Used

A combination of Java and Eclipse's Window Builder will be used to develop a large majority of the tool. RSS Feed and ATT&CK Layer integration is possible by referencing sites that report on cyber-attacks such as,

- cybermap.kaspersky.com
- https://www.crowdstrike.com
- https://threatpost.com

The tool would navigate through these sites retrieving key information on the reported cyber-attack, this key information in then presented to the user along with any recommendations for mitigating such an attack by using https://attack.mitre.org/resources/working-with-attack/.

What the project is supposed to be

The goal of this project is to improve the current level in cybersecurity, The tool's purpose is to be an overseer of trusted sources for cybersecurity incident reports, this means, when a new report is generated, the tool will extract the key information and the cause of the report.

With the above in hand, using MITRE ATT&CK's Tactics and Techniques as a blueprint to help sort incidents based on the methods used by the attackers to breach an organisation. However, using the information that the tool has found, it creates a dynamic threat profile which help its user assess the nature of each incident and recommends what steps need to be taken to prevent the reported attack from happening to them.

Given the nature and seriousness of such a tool, the user will be able to customise their MITRE ATT&CK layers. This means that each version of the tool is specific to its user as not all organisations have the same level of threats and security. These organisations can set specific threats that they're vulnerable to and what they aren't.

Both the Threat Profile and the organisations own MITRE ATT&CK layers help the tool is filtering information and setting an overall risk level for the organisation, this risk level shows the organisation how vulnerable they really are and how they can make themselves more secure.

What will the project deliver?

The Cybersecurity Incident Monitoring Tool is designed to manage a variety of functionalities while also upholding a responsibility in providing effective and ethical information to its user.

Main Deliverables

The main deliverables of the Cybersecurity Incident Monitoring Tool are what make the tool whole, each deliverable has their own unique part in how effective the tool is at monitoring and responding to a reported cyber incident. Below are the following main deliverables which include what they do and their features.

Incident Monitoring

This deliverable is the most important part of the tool as it is the project and tool's main objective and end goal. Without this, the tool wouldn't be able to monitor, analyse and report on, on-going or recent cybersecurity incidents that happen outside the organisation, and report them to its user along with the information that the below deliverables provide effectively and actively.

MITRE ATT&CK

Including MITRE ATT&CK's Tactics and Techniques is a major part of the tool as it provides an organised framework which categorizes common attack methods used by threat actors during an on-going or recent cyber-attack. Utilising MITRE's Layers will allow the tool to escalate the notification's priority of the likelihood of an impending attack on or within the organisation to the user.

Threat Profiling

For the tool to help its user mitigate any future attack on its organisation, the tool must create a dynamic threat profile based on the reported cybersecurity incidents by identifying key phrases within the incident report that relate to MITRE's framework, the threat profile evaluates the severity and nature of the incident, with this information it shows the user its recommended mitigations against the given attack.

Risk Assessment Level & Alerts

For the tool to alert it user about a reported threat, the tool assesses the level of risk associated with each threat. The basis behind the assessment is the detailed information gathered by the tool while issuing real time alerts when a significant threat to the user is noticed.

Recommending Mitigations

After identifying a threat and providing a level of risk, the tool provides a proactive method of managing risks and threats by providing informative steps to take that will mitigate notable attacks based on the organisation's identified vulnerabilities and the methods of the attack noted by the

RSS Feed Integration

Integrating a source of information via an RSS Feed allows the tool to gather a variety of critical information from trusted sources. Using this method allows for a broader scope for gathering vital and critical information but it also enables cross-verification for certain aspects of a reported attacks.

End User Interface

While information gathering and mitigation is the primary design of the tool, The vital information must be presented to the user in an informative and visually appealing way which allows the user to easily navigate through the information and makes understanding the structure.

Who is going to use it?

This incident monitoring tool is intended to provide crucial information to a variety of users, from cyber security operators to teams of major organizations such as,

Security Analysts

Cyber Security Analysts are responsible for monitoring and analysing any security incidents that effect their organization, they have an important role in the mitigation of cyber-attacks. They need accurate information given to them without delay or error.

SOC Teams

A Security Operations Center is the frontline of defense against any cyber threat, similar to an analyst they rely on accurate incident information to be given to them so they're able to mitigate to threat that's reported. This is why they are one of the top users who would be reliant on using the Incident Monitoring Tool.

IT Admins

The role of an IT Admin is managing its organisation's technical infrastructure Using the Incident Monitoring Tool helps them in detecting potential vulnerabilities in their system and recommends mitigations which helps them defend against future threats.

Risk Management Team(s)

A Risk Management Team's priority is to identify, assess and mitigates any identified risks that could affect the organisation that they work for. Having this tool in their arsenal relieves the amount of stress put on the team as it reduces the team's analyses time and leaves more time for them to implement the recommended mitigations.

Incident Response Team(s)

While the above teams are dedicated to identifying and assessing reported threats. In the event of a security breach, the incident response team is responsible for following guidelines in containing and most importantly, eradicating the successful breaches. Using the Incident Handling Tool

Metrics

To gauge whether this is a successful project, we have to consider the following aspects of the tool, such as its performance, design, and its effectiveness in achieving the intended results. This can be done by assessing those aspects, such as the ones below.

Threat Assessment Accuracy

One of the major indicators of a successful project is the accuracy of its threat assessments. The tool is designed to cross-reference data from generated incident reports and data based on its organisation. This feature is a major part in the overall functionality of the tool, without this, the tool would be redundant.

Effectiveness of Mitigations

The tool is designed to show effective mitigation techniques, using its threat assessment it creates a list of effective mitigations against the attack by cross-referencing MITRE ATT&CK's Tactics and Techniques. Evaluating the mitigations' effectiveness is how an assessment of this part of the tool can be done.

Incident Response Time

When an incident report is created, the tool's response should be somewhat instantaneous rather than several weeks to months later of detecting a report. Assessing the speed of which the tool notifies the user of an incident and the time it takes to show effective mitigations is how this aspect of the tool can be graded.

Usability and User Satisfaction

The information presented to its user should be in a visually appealing way. although a major assessment can't be done on the initial appearance of the tool's outputted display, a user can supply feedback on what they'd like the design of the tool to look like.

Scalability and Resource Utilization

Given the nature of the tool, it handles a large amount of data and its devices' resources such as storage and memory, assessing its capabilities and its resource allocation is an effective way of judging whether the tool's performance is affected by its workload.

Compliance and Adherence to Standards

Using MITRE ATT&CK's Tactics and Techniques sets a level of compliance for the tool to follow. This is because it handles private and sensitive information and having a set of guidelines prevents any misuse of information. Any misuse of this information is serious cause or concern and is a major part in the tool's grading and assessment.

F.U.R.P.S Report

This report provides an evaluation of the Incident Monitoring Tool's performance and how well it functions, it's useability and reliability to its users.

Functionality

This part of the report examines what the tool can do and its main capabilities in monitoring incidents while cross-referencing using MITRE ATT&CK's Tactics and Techniques. Given the level of importance that the tool has on mitigating cyber-attacks, for security reasons the tool is to be managed on a local device within the organisation limiting the risk of a device such as a laptop being stolen in the event that it has the tool installed which is a risk to the company given the information the tool stores and provides.

Usability

The tool's design should be somewhat based on its user's preference, this allows for easy to navigate aesthetic making it look more appealing to the user as they can set what documents and information that they want to see and how they want to see it.

Reliability

The importance of the tool relies on its main functions being able to perform without any error or inaccuracy. In the event that a major incident is reported, accurate information should be presented to the user and a variety of effective ways of mitigating such threats.

Performance

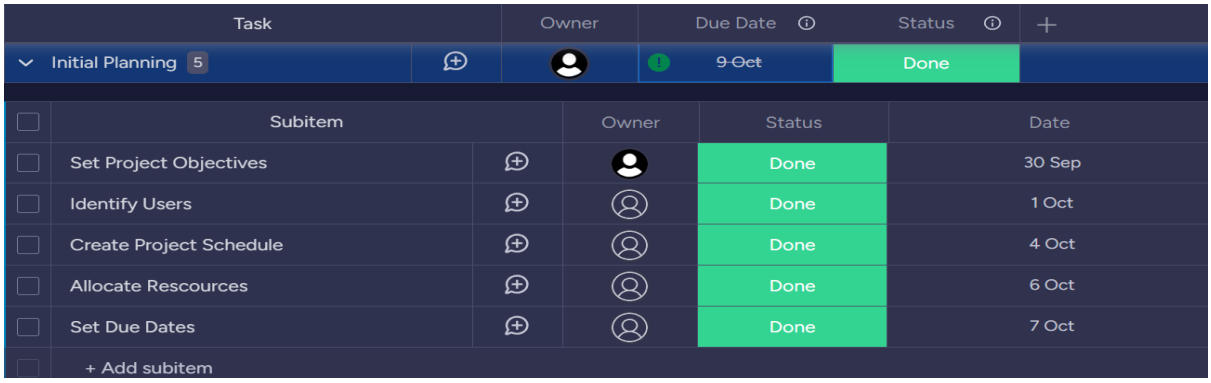
Evaluating the performance begins with assessing how well the tool performs in terms of its responsiveness to threats and displaying its mitigations and how fast it delivers that information to its users.

Supportability

Having a such important and relied on tool means the software being windows based and its frequent updates to be able to hold the large amounts of data it runs through and organises, but its compliance with an organisation's standards and their own metrics that they must uphold means that the software should be effective and maintained to support these requirements.

Gantt Chart

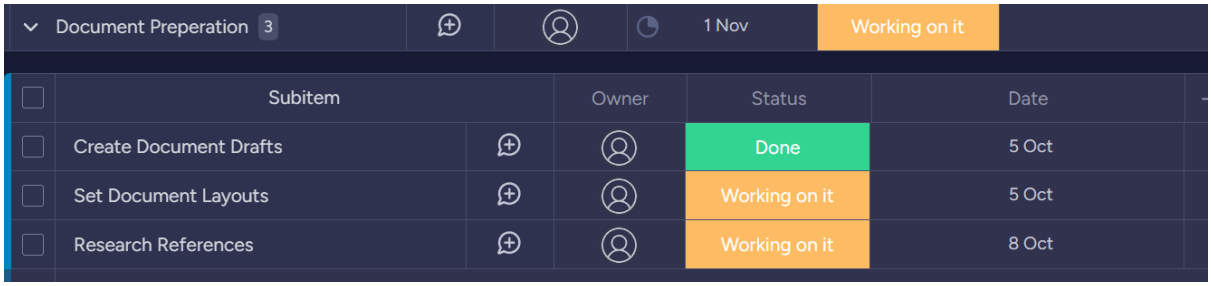
Initial Planning



Task	Owner	Due Date	Status
Initial Planning 5		~~9 Oct~~	Done

Subitem	Owner	Status	Date
Set Project Objectives		Done	30 Sep
Identify Users		Done	1 Oct
Create Project Schedule		Done	4 Oct
Allocate Rescources		Done	6 Oct
Set Due Dates		Done	7 Oct
+ Add subitem			

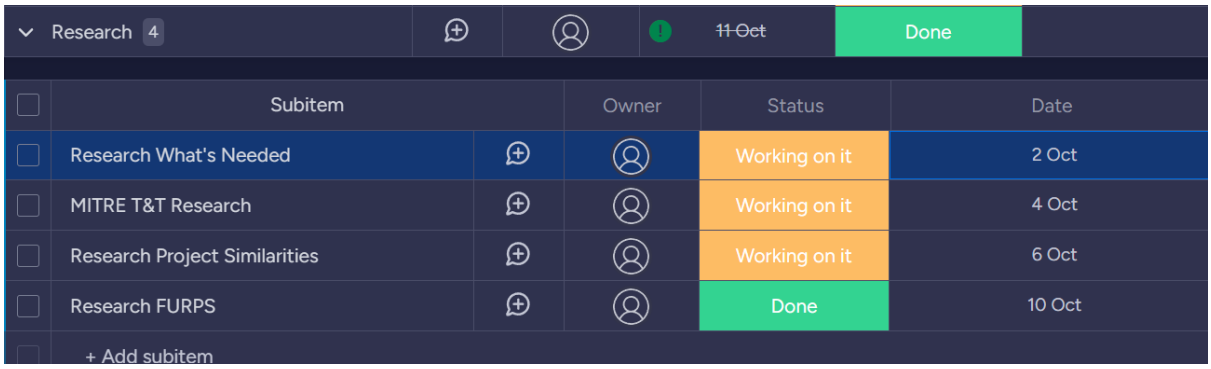
Document Preparation



Document Preperation 3		1 Nov	Working on it

Subitem	Owner	Status	Date
Create Document Drafts		Done	5 Oct
Set Document Layouts		Working on it	5 Oct
Research References		Working on it	8 Oct

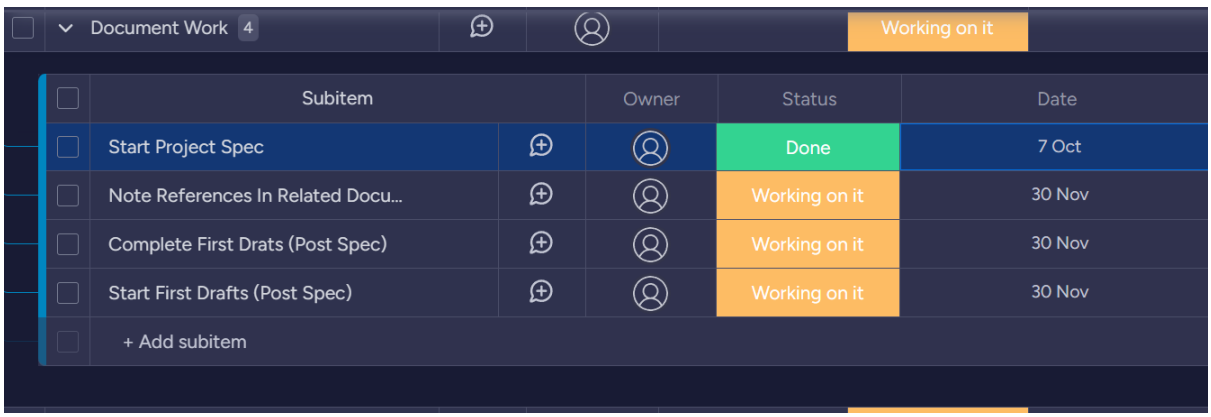
Research



Research 4		~~11 Oct~~	Done

Subitem	Owner	Status	Date
Research What's Needed		Working on it	2 Oct
MITRE T&T Research		Working on it	4 Oct
Research Project Similarities		Working on it	6 Oct
Research FURPS		Done	10 Oct
+ Add subitem			

Document Work



Document Work 4			Working on it

Subitem	Owner	Status	Date
Start Project Spec		Done	7 Oct
Note References In Related Docu...		Working on it	30 Nov
Complete First Drats (Post Spec)		Working on it	30 Nov
Start First Drafts (Post Spec)		Working on it	30 Nov
+ Add subitem			

References

The main plan and overall requirements for the tool were thought of during weekly meetings. Any technical information such as tools needed for developing the user interface and the languages needed were learned during college term(s)