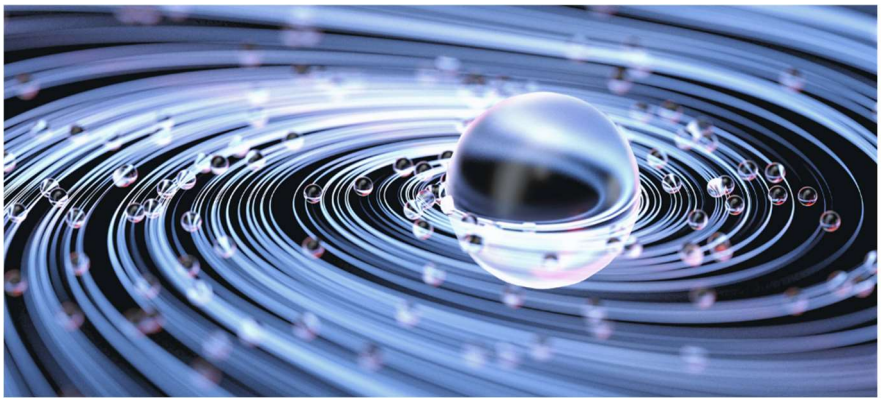


AI For Industry-based Cybersecurity Threats
Project Plan

Solution overview

The key deliverable of this project is a prototype microservice system that will enable a software program to gather data relating to recent cybersecurity threats and vulnerabilities from reliable open-source repositories. With this data, the proposed microservice will utilise machine learning to identify the highest priority threats and vulnerabilities impacting specific industries. When a user queries the service, the software will be capable of generating a list of high priority threats and vulnerabilities as well as relevant mitigation strategies for an industry of interest.

Team Members

Bianca Beaumont - n10242040

Christine Choy - n8597642

Connor McSweeney - n8844488

Koh Hei Luo - n10836209

Masayoshi Kamioki - n10838601

Academic Supervisor

Dr. Bhargavi Goswami

24 April 2022

Table of Contents

1. Introduction

1.1 Industry Context and Client Profile

Cyber security has never been more important, both as an enabler for Australian industry and as a source of economic growth itself (Smith & Ingram, 2017; Teoh & Mahmood 2017). Over the coming decade, Australia's cyber security industry is forecast to triple its revenue in response to increased demand for cyber security products and services (AustCyber, n.d.). In order to capitalise on this growth, providers of cyber security services must develop and leverage increasingly sophisticated and scalable solutions for their clients.

The Project Industry Partner – Securemation - is an Australian-based consulting company specializing in security strategy, managed security services, threat and risk management, and solution and enterprise architecture reviews. Their vision is to become the preferred and trusted service provider for securing small and medium businesses in Australia by providing pragmatic risk and compliance-based recommendations (Securemation, n.d.a).

1.2 Project Aim

1.2.1 Business Problem and Need

Currently, Securemation undertake a manual "cyber security health-check" for clients across all industries (Securemation, n.d.b). This involves assigning a specialised Security Analyst to manually research and assess industry-specific threats and vulnerabilities and develop appropriate recommendations to mitigate identified risks. This process requires a significant investment of time and labour resources and does not guarantee complete capture of all available data on current cyber security threats and vulnerabilities. Importantly, manual, unscalable processes hinder Securemation's ability to take advantage of the rapid growth being forecast in the demand for cyber security services.

1.2.2 Opportunities

Securemation has identified that significant internal time and cost efficiencies could be realised by partly or fully automating this process, leading to improved timeliness, cost, and accuracy of services provided to clients. By doing so, Securemation stands to increase the robustness of its clients' cyber security capabilities, enable them to pursue digitally-driven business strategies, and in turn support the growth of new and existing industries in Australia. Potential business benefits are expanded upon in section 1.4 further below.

1.3 Objectives

The high-level objectives of the project, as provided in the original Project Brief in Appendix 1. are broken down in to 'SMART' objectives per Table 1 below. More detailed objectives (in the form of user stories within a prioritised requirements list) are outlined in Table 3. Subsequent sections of this

document outline the scope, development and management approach applied to ensure the successful delivery of these goals.

Table 1. – Project SMART objectives

S	M	A	R	T
Specific objective	Measurable progress or result indicator	Benefit/s assigned to	Realistic benefit/s within available resources	Timeframe to realise benefit/s
Query and return a prioritised and current list of security threats and breaches for each major industry in Australia	Delivery of tested and working prototype microservice that meets functionality requirements	Securemation clients	- Maintain awareness of the current cybersecurity landscape of industry - Enhance cyber security protection measures	April-June 2022 (for capability development); annually thereafter per Securemation's business planning cycle
Return a current list of security recommendations to combat identified threats and breaches				
Document 'as delivered' system documentation	Provision of complete documentation	Securemation team	- Record, trace and reproduce/build upon prototype solution	
Partly or fully automate health-check process	Internal costings and direct feedback		- Reduce time, and cost of health check process - Increase client satisfaction	

1.4 Potential Impact

An overview of the As-Is and To-Be business processes relating to this project are shown in Figures 1 and 2 below. Within scope of the project are those steps outlined in red.

Figure 1. As-Is Process

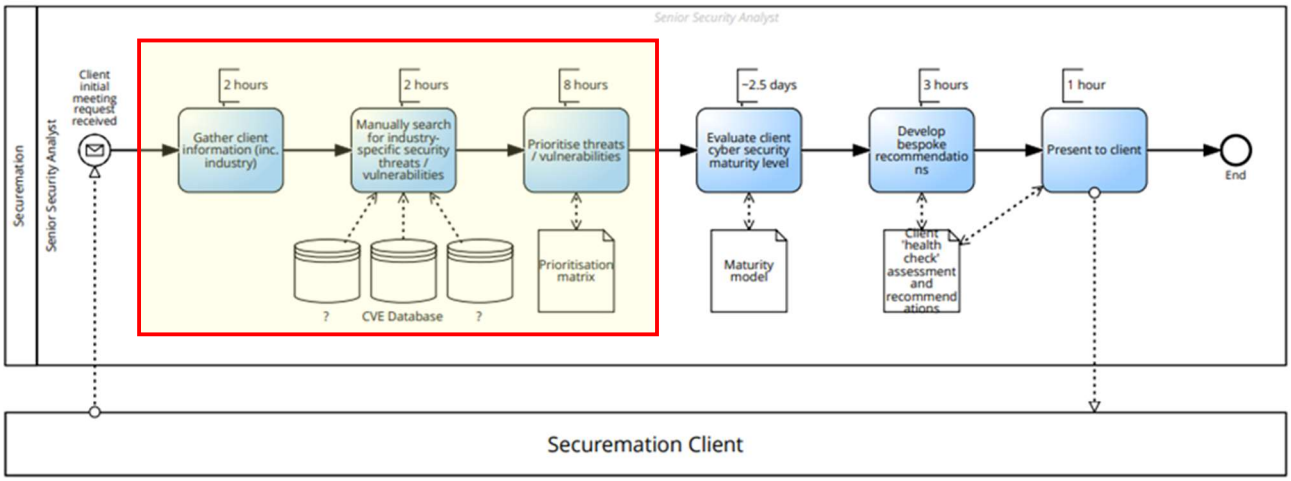
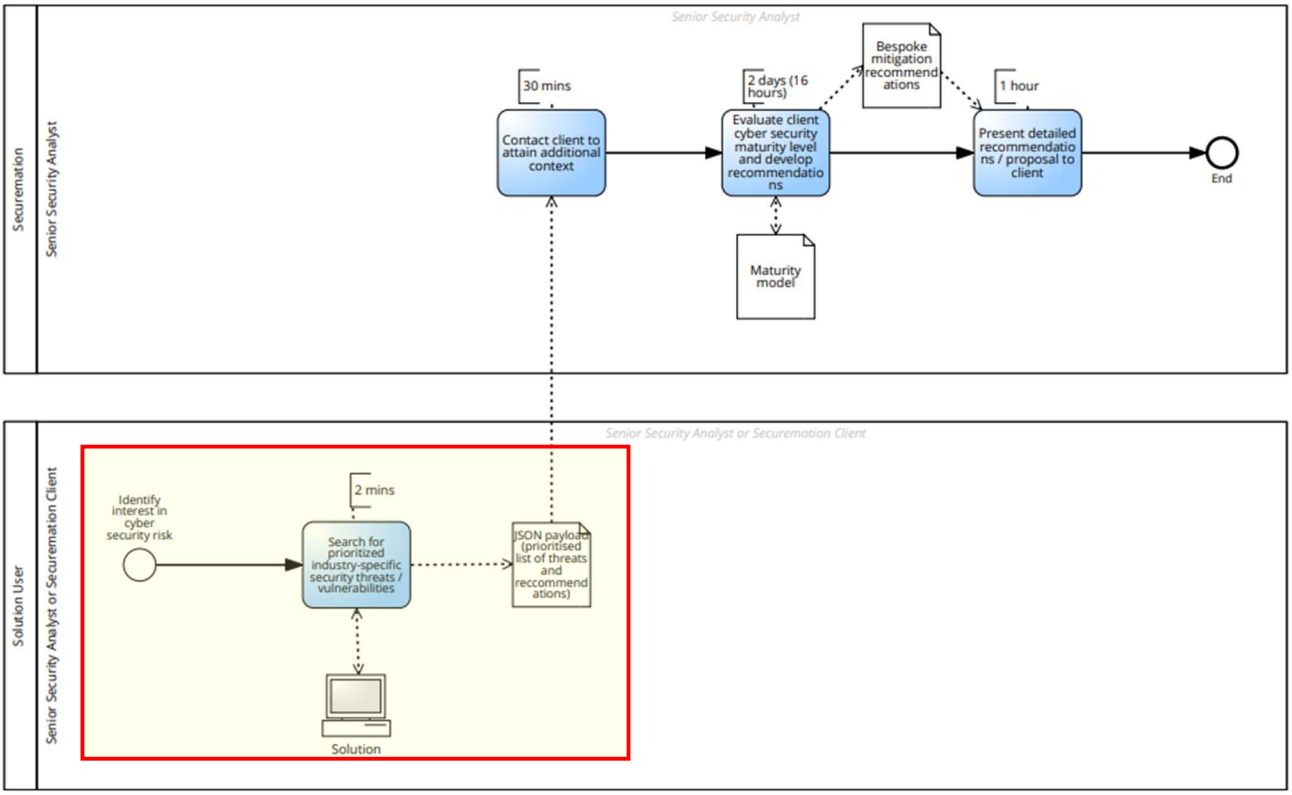


Figure 2. To-Be Process



By automating the health-check process as shown in Figure 2, Securemation stand to realise significant cost savings, shown in Table 2. In addition, successful delivery of a solution that meets the project's objectives will potentially provide significant competitive advantage over other small and medium consulting firms, and assist Securemation to leverage projected growth in demand for cyber security services over the coming decade.

Table 2. Indicative Cost Savings

	Manual tasks (for Securemation)	Hours per process instance	Cost per hour^	Cost per process instance
As-Is	6	36	$61	$2,196
To-Be	3	17.5	$61	$1,068
Potential cost saving per instance				$1,129 (51%)
Indicative annual saving in year 1*				$40,626
Indicative annual saving in year 10**				$121,878
Indicative cumulative savings year 1-10**				**$820,645**

** 3 instances per month*

*** Tripling to 9 instances per month in year 10, not adjusted for inflation*

^ Hourly rate benchmarked against annual cost of Senior Security Analyst via Talent.com (2022).

2. Defining the Scope

2.1 Scope Overview

2.1.1 In Scope

The scope of project deliverables includes:

- a tested and fully working prototype of software component that meets agreed user requirements; and
- 'as built' documentation capturing low-level design information.

Functional and Non-Functional requirements considered in scope are all items listed as 'Must' in the Prioritised Requirements List (PRL) further below.

2.1.2 Out of Scope

Out of scope are all requirements listed as 'Won't' in the below PRL, as confirmed with the Securemation team.

2.1.3 To be Confirmed/Scope Risks

In order to ensure time and cost constraints are met, there is flexible scope to include 'Should', and 'Could' items. Any additional specific features of the prototype not outlined in the PRL will be identified as part of detailed timebox (aka sprint) planning, as these may not all be known in advance.

Intermediary outcomes are listed in more detail in Section 5.

2.2 Prioritised Requirements List

The PRL in Table 3 below includes a total of 9 'Must-have' requirements/user stories (representing 70% of total requirements), 2 'Should-have' requirements (15%) and 2 'Could-have' requirements (15%). While this split of MoSCoW categories are not perfectly aligned with the recommended optimal split of 60% Must-have, 20% Should-have and 20% Could-have requirements, the PRL does reflect the careful scoping of strictly necessary requirements in partnership with the Securemation Industry Partners, and deliberate de-scoping of possible or 'nice-to-have' features in order to ensure the viability of a functioning prototype within the time allotted. Most of these requirements/user stories will be developed using a combined 'vertical-and-horizontal' approach, whereby they are addressed over the course of multiple timeboxes (Agile Business Consortium, 2014a), thus mitigating the disadvantages of one approach over the other.

Table 3. Prioritised Requirements List

Legend: F = Functional requirement; NF = Non-Functional requirement

ID	Category	Requirement (presented as user stories)	Complexity	Estimated Effort	MoSCoW ranking	Timebox alignment
1	F & NF	As a Security architect user of a security management tool, I would like to be able to gather data relating to cyber security threats from reliable or pre-vetted online sources, so that I can be reliably informed of current cyber security threats in my industry.	40	13	Must	1-4
2	F	As a Security architect user of a security management tool, I would like any identified threats and vulnerabilities related to my selected industry to be prioritised, so that I can pursue proportionate mitigation strategies and make informed investment decisions.	40	40	Must	1-4
3	NF	As a Security architect user of a security management tool, I would like to know that the solution components are adequately protected against cyber security threats, so that I can place trust in the accuracy of the output.	8	8	Must	5
4	F	As a Security architect user of a security management tool, I would like to receive threat mitigation recommendations for all high priority threats/vulnerabilities identified, so that I can ensure my organisation is adequately protected from identified threats.	13	8	Must	1-4
5	NF	As a Security architect user of a security management tool, I would like each component of the solution to be integrated to ensure seamless communication and compatibility between existing and potential software components.	8	8	Must	1-6
6	F	As a Security architect user of a security management tool, I would like to receive (at a minimum) the name of identified cyber security threats, industry queried, priority level, mitigation recommendation/s, and a measure of confidence, so that I can be well-informed prior to undertaking more bespoke analysis and recommendations.	2	2	Must	1-4
7	F	As a Security architect user of a security management tool, I would like the output of the solution to be in JavaScript Object Notation (JSON) format, so that I can easily manipulate this into other forms such as display on a webpage	1	1/2	Must	6
8	F	As a Security architect user of a security management tool, I would like identified threats and vulnerabilities for a selected industry to be categorised, so that I can quickly understand their nature and likely features.	20	40	Must	1-4
9	NF	As a Security architect user of a security management tool, I would like appropriate documentation outlining the functionality and user interaction of the solution, so that I can audit and build upon its functionality	3	5	Must	1-6
10	NF	As a Security architect user of a security management tool, I would like any solution design to be flexible enough to accommodate additional data in future, so that I can further build upon its functionality.	13	8	Should	1-6
11	F	As a Security architect user of a security management tool, I would like the recency of threats to be accounted for in the threat prioritisation so that I can make informed judgements on the likely relevance of the threat/s and appropriate mitigation strategies.	20	5	Should	1, 4

12	F	As a Security architect user of a security management tool, I would like to be able to access information from across the web so that I can have a better understanding of current cyber security threats.	40	40	Could	4
13	F	As a Security architect user of a security management tool, I would like to be able to gain an understanding of what threats are likely to occur in the future, so that I can be better prepared in proactively preparing mitigation strategies for clients	80	40	Could	1-4
14	F	As a Security architect user of a security management tool, I would like identified threats/vulnerabilities to be characterised by subsector industries, so that I can more easily identify relevant contextual factors and mitigation strategies for clients.	n/a	n/a	Won't	n/a
15	F	As a Security architect user of a security management tool, I would like a bespoke, standalone user interface, so that I can deploy the solution immediately.	n/a	n/a	Won't	n/a
16	F	As a Security architect user of a security management tool, I would like a bespoke API to be utilised so that I can have greater control over the integration of the solution.	n/a	n/a	Won't	n/a
17	F	As a Security architect user of a security management tool, I would like to be able to categorise threats/vulnerabilities by industry locales (geographic locations), so that I can segment and create bespoke insights based on customer State/City etc.	n/a	n/a	Won't	n/a
18	NF	As a Security architect user of a security management tool, I would like to be able to further enhance my toolkit of maturity assessments, so that I can better evaluate client cyber security maturity levels.	n/a	n/a	Won't	n/a

3. Justification of chosen project management approach

An adapted agile approach has been selected for this project, primarily drawing on Dynamic System Development Method (DSDM) (Agile Business Consortium, 2014b) and some elements of the more traditional Waterfall approach. This selection has been made in light of the following reasons:

- The Industry Partner (Securemation) have stated that time and cost of the project is fixed, leaving flexibility only for the specific aspects of features. Furthermore, as the project objective is to deliver a working prototype (as opposed to a perfectly polished end-product), it is accepted that the delivered solution must not include unnecessary or over-engineered features, while still meeting the core business need.
- Tools (technologies) have been suggested by Securemation but not specified, leaving scope for adaptation throughout the project (and re-prioritization if needed). Furthermore, it was evident at the outset of this project that there are many 'unknowns' and 'unknown-unknowns' within this project, requiring a degree of flexibility for what and how features are delivered (as opposed to explicitly defined features and rigid delivery approach, for which Waterfall may be a better suited as the dominant project management approach), consistent with the principles of the Cynefin framework (Wikipedia, 2022).
- Notwithstanding this, Securemation have stated a strong desire to leverage the benefits of comprehensive early technical design afforded by waterfall methodologies and tools (such as the Gantt chart in Table 7) in order to partly de-risk the project, however, still wish to approach the refinement and development of features in an agile manner.
- The comparably artefact-heavy DSDM approach (as opposed to 'document-light' approaches such as SCRUM) will mitigate for the relative inexperience of Team 1 in project management and documentation to reduce the likelihood of missed considerations, miscommunication, poor decision-making, and non-acceptance of the solution by the Industry Partner.
- IFN711 places a distinct focus on the actual management of the project and the context and needs of Securemation, broadening the necessary focus to the project (beyond the delivery of a single product or feature, for which SCRUM might be more appropriate).
- The close involvement of Securemation via the application of DSDM roles will encourage ownership and smooth the handover of the solution on completion.
- DSDM places strong emphasis on communication (for example via workshops), visualisation (such as diagrams, models, and demonstrated iterative development) and clearly defined responsibilities, and – importantly - DSDM is designed to be tailored for a variety of project contexts (Agile Business Consortium, 2014b).

4. Solution Overview

The key deliverable of this project is a prototype microservice system comprised of multiple integrated software components. The proposed microservice will gather data relating to recent cybersecurity threats and vulnerabilities from reliable open-source repositories. With this data, the service will utilise machine learning to identify the highest priority threats and vulnerabilities impacting specific industries, as well as relevant mitigation strategies. When a user queries the service, the software will generate a list of these high priority threats, vulnerabilities, and mitigation strategies for an industry of interest. The development of this solution will implement at least two existing technologies to achieve this functionality: jBPM and TensorFlow.

jBPM (https://www.jbpm.org/) is an open-source workflow program that enables the execution and automation of business processes and decisions (Red Hat, 2022). Management of the system's process flow, central APIs, and user interaction will utilise jBPM's capabilities. The workflow engine will allow for process automation set out as a graphical representation of the underlying processes. This will also enhance the transparency and comprehensibility of the design aiding in the eventual handover of the product. The lightweight and extensible nature of jBPM aligns well with the current and future needs of the Industry Partner, in addition to being their preferred business process management tool in this instance.

TensorFlow (https://www.tensorflow.org/) provides a robust and flexible platform to build, train and deploy the machine learning model for this service (Google Brain Team, 2022). The ML model developed will classify threats and vulnerabilities by priority using model weights based on researched metrics similar to those used by CVSS (https://www.first.org/cvss/) (FIRST, 2019). Due to the requirements of the solution, additional metrics such as the last and most recent occurrence of an incident, as well as the reliability of the source data used may be included in the model. Once priority levels have been identified, suitable and actionable mitigation strategies will be mapped to each threat accordingly. The results will be housed within a database, ready and available for user queries. The database conceptual schema seen in Figure 3 outlines the format of the data. Additionally, a high-level visualisation of the solution is shown in Figure 4 below.

Sequentially, the system is divided into two sections, with data gathering and ML classification separated from user interaction. A sequence diagram outlining the flow of interaction between each component can be seen in Figure 5 – with the user interaction limited to a managed database. This allows for the system to update data regularly and for the user to access the information they require immediately. Putting this information directly and speedily into the hands of the user will generate value in the awareness of relevant cybersecurity incidents while encouraging and facilitating the development of more bespoke mitigation strategies against known threats and vulnerabilities – in turn creating safer organisations and communities.

Figure 3. Relational Database Schema

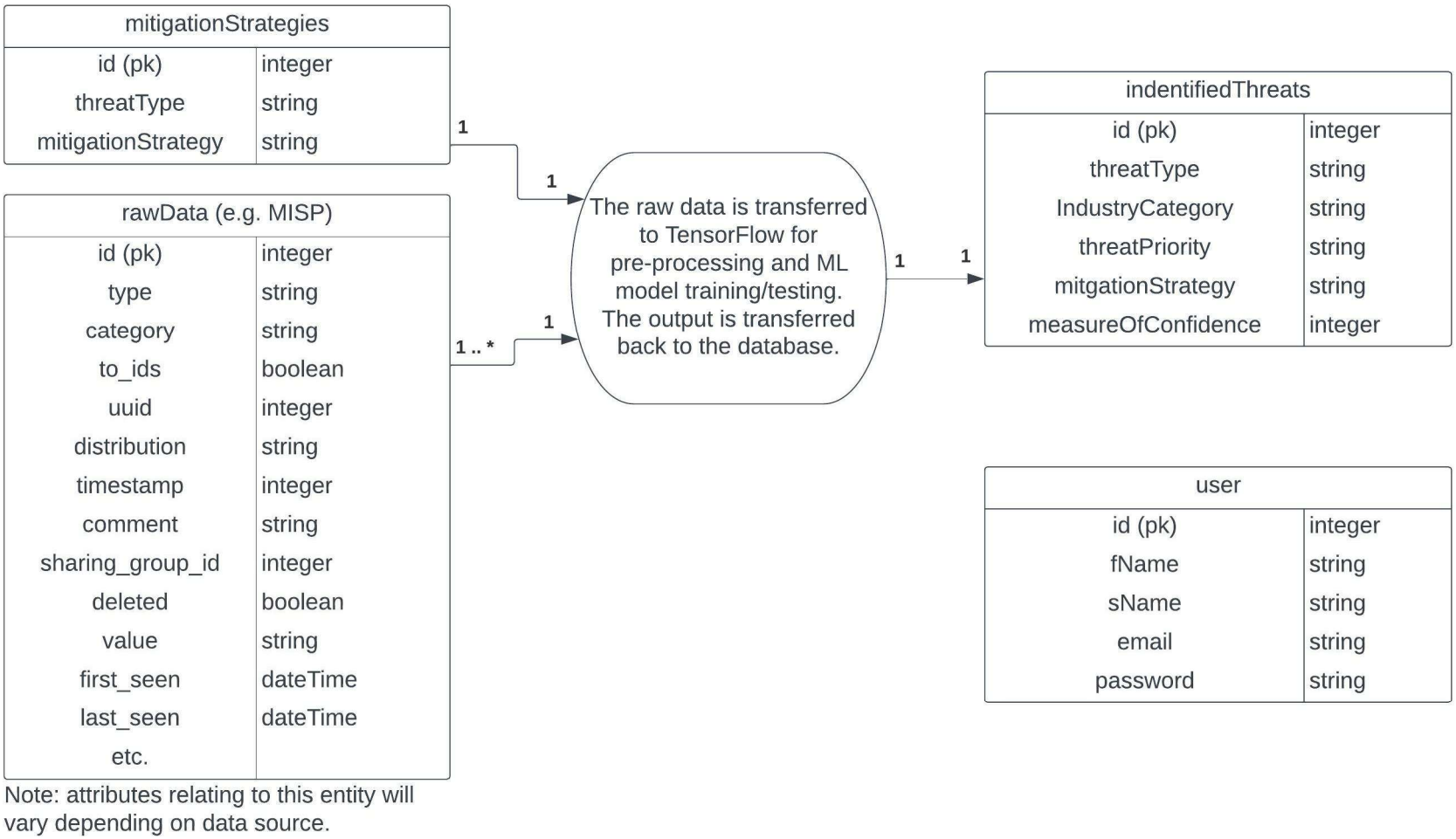


Figure 4. Microservice solution logical architecture

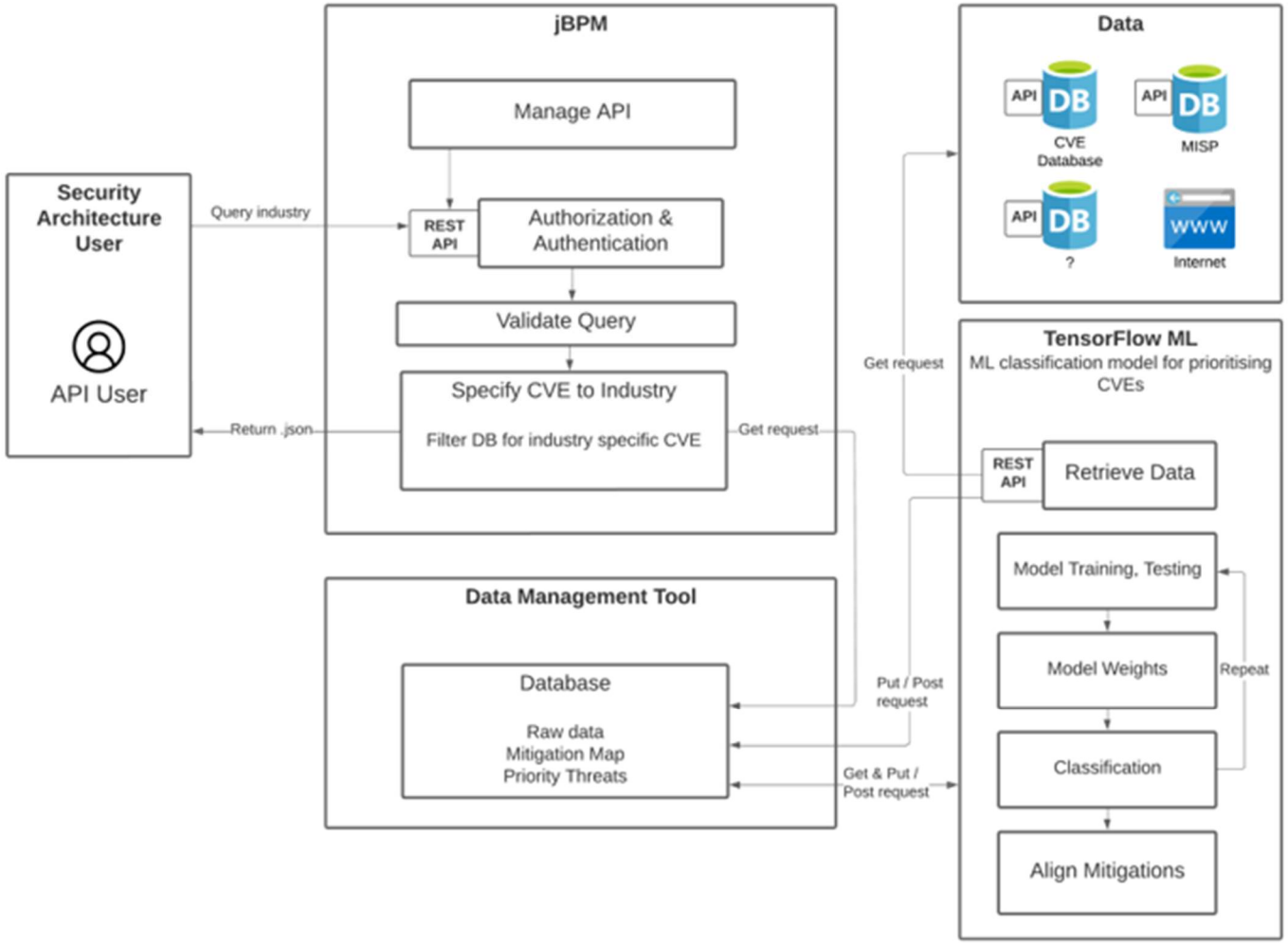
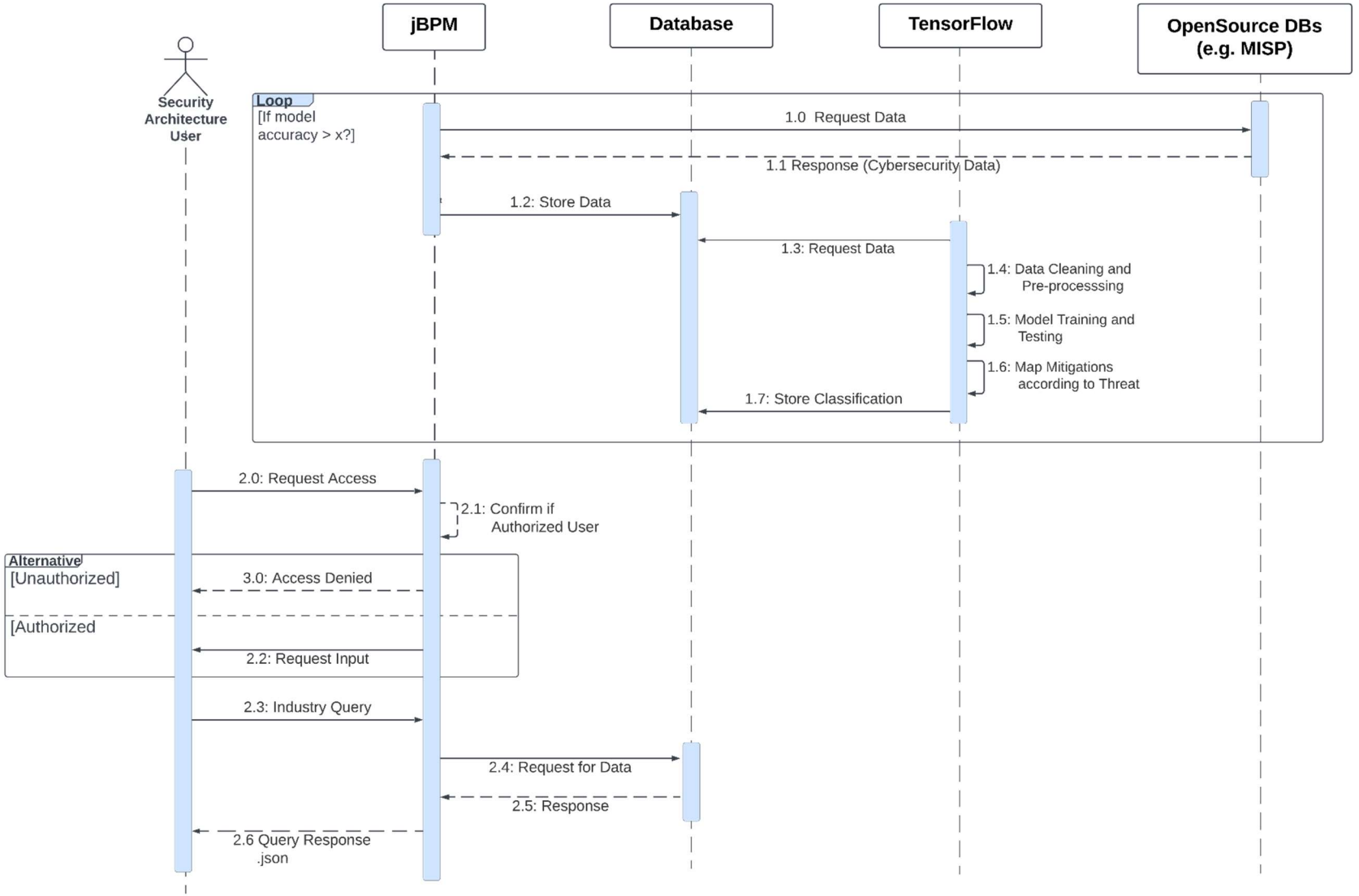


Figure 5. Microservice UML Sequence diagram



5. Schedule of Intermediate and Final Deliverables

5.1 Planning tools and techniques

An agile DSDM approach was utilised to collaboratively brainstorm, analyse, and estimate the complexity and effort required to deliver on each requirement/user story, and allocate relative 'story points'. The process of discussion and joint estimation helped tease out just enough detail to provide confidence in the overall project delivery approach and proposed solution.

This in turn helped create the Work Breakdown Structure (WBS) shown in Figure 6 on page 15, providing slightly greater granularity in the deliverables required. Interim and Final deliverables were then plotted on the Gantt Chart shown in Figure 7, in which more complex or effort-intensive tasks are allocated longer timeframes.

The detail contained in the Gantt Chart serves as the 'Delivery Plan' in DSDM terms, and Trello Board cards serve as a dynamic 'Timebox Plans', which guide evolutionary development at the lowest level of task granularity. A visualisation of this Timebox planning approach is shown in Figures 8 and 9 on pages 18-19, for illustrative purposes (noting that this is subject to regular updates throughout the project).

5.2 Increment Objectives

As visualised in the Gantt Chart in Figure 7 on pages 16-17, the Evolutionary Development phase spans a total of 7 weeks, comprising three two-week increments, plus one week for solution deployment. Each increment contains two week-long timeboxes (also referred to informally as sprints) running from Monday-Sunday, with Weekly Sprint Meetings held with the Industry Partner each Friday to demonstrate progress as well as obtain clarification and input prior to the timebox's formal close. High-level objectives for each increment are set out in Table 4 below.

Table 4. Schedule of Increment Objectives

No.	Date range	Increment Objective
1	25 April – 8 May	Establish project environment (including data sources, key terms, templates and key systems) and create basic functionality to enable subsequent, more comprehensive development work.
2	9 May – 22 May	Initial, then detailed design, build, and test of system components (likely jBPM and TensorFlow).
3	23 May – 5 June	Develop and test security measures, refinement of solution, and comprehensive testing of full system integration.

5.3 Interim Deliverables

To support optimal transparency and tracking of progress toward the final deliverable, the following interim deliverables have been identified, and align with the 'milestones' (diamonds) shown in the Gantt Chart in Figure 7. These interim deliverables will be shared / demonstrated during weekly sprint meetings with Securemation.

Table 5. Schedule of Interim Deliverables

No.	Date	Interim Deliverable
1	24 April	Detailed Project Plan (Shared with Industry Partner via Academic Supervisor by 1 May)
2	29 May	Source dataset and key terms
3	6 May	Basic jBPM and TensorFlow and Database configurations
4	13 May	Full TensorFlow configuration
5	20 May	Full jBPM configuration
6	29 May	*Individual Project Reflections
7	3 June	Tested / functioning solution artefact (all components)
8	6 June	Project Presentation (Week beginning 6 June)

**while not a product or project deliverable per se, the collective insights gained through these reflections will aid the team's functioning throughout the final deployment and inform additional retrospective analysis, therefore is considered an important interim deliverable. Top line items can be shared with the Industry Partner if desired.*

5.4 Final Deliverables

The final deliverable (working prototype solution and documentation) will be deployed in the week ending 10 June, with a full Project Review Report to be submitted by 19 June.

Figure 6. Work Breakdown Structure (WBS)

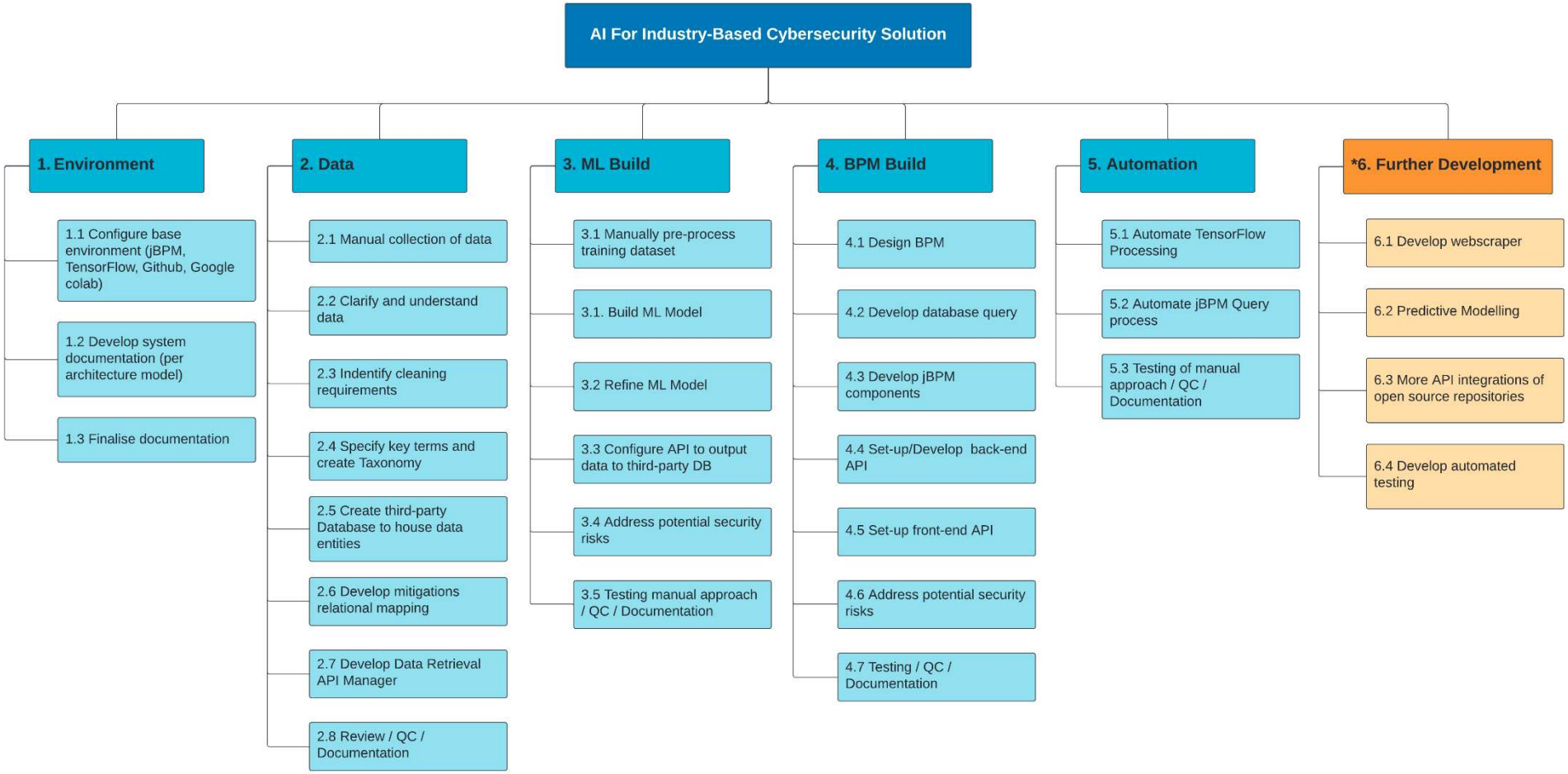
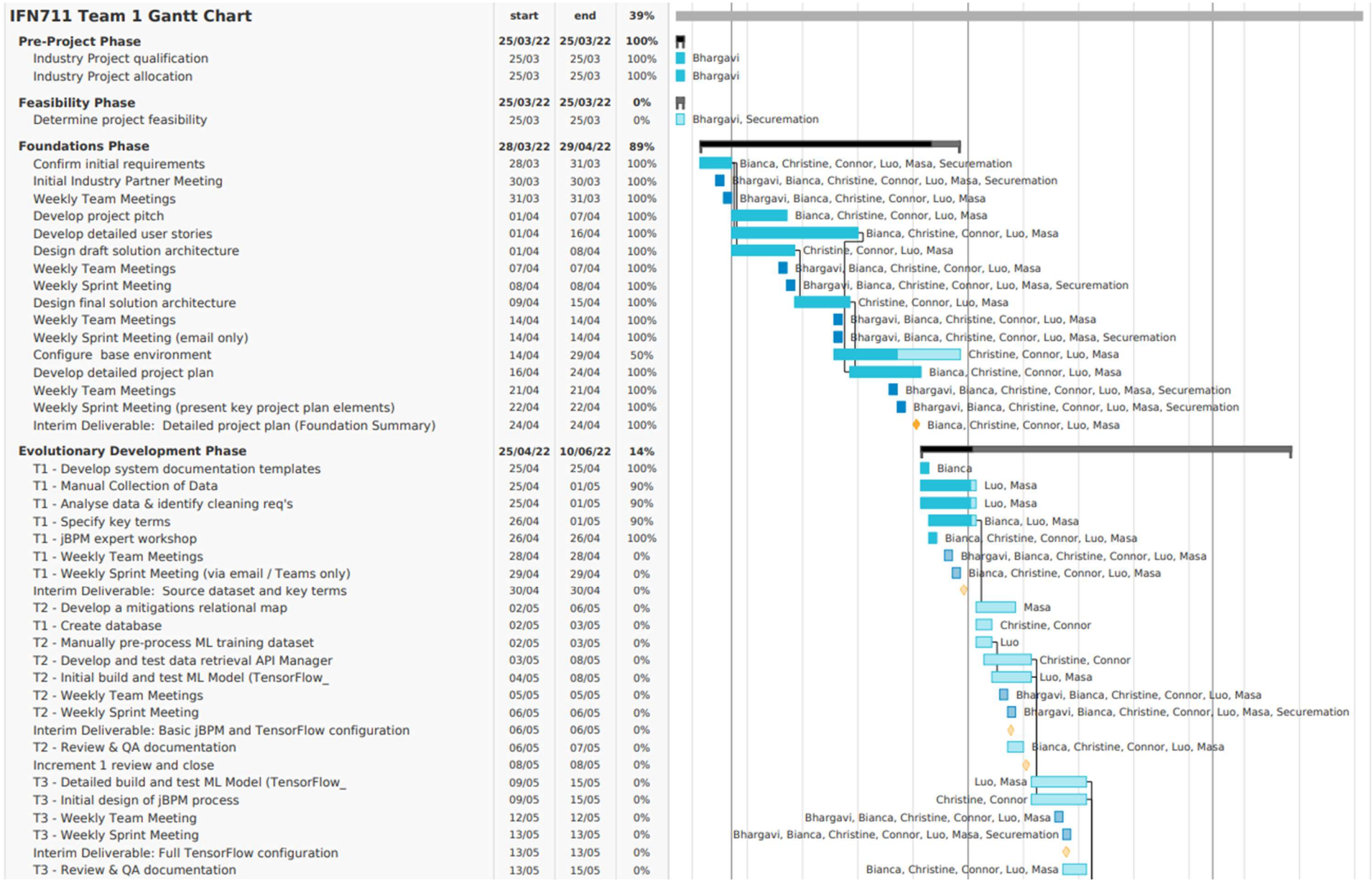


Figure 7. Gantt Chart



IFN711 Team 1 Gantt Chart	start	end	39%
Pre-Project Phase	**25/03/22**	**25/03/22**	**100%**
Industry Project qualification	25/03	25/03	100%
Industry Project allocation	25/03	25/03	100%
Feasibility Phase	**25/03/22**	**25/03/22**	**0%**
Determine project feasibility	25/03	25/03	0%
Foundations Phase	**28/03/22**	**29/04/22**	**89%**
Confirm initial requirements	28/03	31/03	100%
Initial Industry Partner Meeting	30/03	30/03	100%
Weekly Team Meetings	31/03	31/03	100%
Develop project pitch	01/04	07/04	100%
Develop detailed user stories	01/04	16/04	100%
Design draft solution architecture	01/04	08/04	100%
Weekly Team Meetings	07/04	07/04	100%
Weekly Sprint Meeting	08/04	08/04	100%
Design final solution architecture	09/04	15/04	100%
Weekly Team Meetings	14/04	14/04	100%
Weekly Sprint Meeting (email only)	14/04	14/04	100%
Configure base environment	14/04	29/04	50%
Develop detailed project plan	16/04	24/04	100%
Weekly Team Meetings	21/04	21/04	100%
Weekly Sprint Meeting (present key project plan elements)	22/04	22/04	100%
Interim Deliverable: Detailed project plan (Foundation Summary)	24/04	24/04	100%
Evolutionary Development Phase	**25/04/22**	**10/06/22**	**14%**
T1 - Develop system documentation templates	25/04	25/04	100%
T1 - Manual Collection of Data	25/04	01/05	90%
T1 - Analyse data & identify cleaning req's	25/04	01/05	90%
T1 - Specify key terms	26/04	01/05	90%
T1 - jBPM expert workshop	26/04	26/04	100%
T1 - Weekly Team Meetings	28/04	28/04	0%
T1 - Weekly Sprint Meeting (via email / Teams only)	29/04	29/04	0%
Interim Deliverable: Source dataset and key terms	30/04	30/04	0%
T2 - Develop a mitigations relational map	02/05	06/05	0%
T1 - Create database	02/05	03/05	0%
T2 - Manually pre-process ML training dataset	02/05	03/05	0%
T2 - Develop and test data retrieval API Manager	03/05	08/05	0%
T2 - Initial build and test ML Model (TensorFlow_	04/05	08/05	0%
T2 - Weekly Team Meetings	05/05	05/05	0%
T2 - Weekly Sprint Meeting	06/05	06/05	0%
Interim Deliverable: Basic jBPM and TensorFlow configuration	06/05	06/05	0%
T2 - Review & QA documentation	06/05	07/05	0%
Increment 1 review and close	08/05	08/05	0%
T3 - Detailed build and test ML Model (TensorFlow_	09/05	15/05	0%
T3 - Initial design of jBPM process	09/05	15/05	0%
T3 - Weekly Team Meeting	12/05	12/05	0%
T3 - Weekly Sprint Meeting	13/05	13/05	0%
Interim Deliverable: Full TensorFlow configuration	13/05	13/05	0%
T3 - Review & QA documentation	13/05	15/05	0%

T4 - Detailed build and test database query and APIs (jBPM)	16/05	22/05	0%
T4 - Incorporate additional data source(s) and refine ML model	16/05	22/05	0%
T4 - Develop and test web-scrape capability	16/05	22/05	0%
T4 - Weekly Team Meetings	19/05	19/05	0%
T4 - Weekly Sprint Meeting	20/05	20/05	0%
Interim Deliverable: Full jBPM configuration	20/05	20/05	0%
T4 - Review & QA documentation	20/05	22/05	0%
Increment 2 review and close	22/05	22/05	0%
T5 - Develop and test security measures	23/05	29/05	0%
T5 - Refine and test jBPM process and APIs	23/05	29/05	0%
T5 - Weekly Team Meetings	26/05	26/05	0%
T5 - Weekly Sprint Meeting	27/05	27/05	0%
T5 - Review & QA documentation	27/05	29/05	0%
Interim Deliverable: Individual Project Reflections	29/05	29/05	0%
T6 - Configure and test system	30/05	05/06	0%
T6 - Weekly Team Meetings	02/06	02/06	0%
T6 - Weekly Sprint Meeting	03/06	03/06	0%
Interim Deliverable: Tested / functioning solution (all components)	03/06	03/06	0%
T6 - Review & QA documentation	03/06	05/06	0%
Increment 3 review and close	05/06	05/06	0%
Deployment Phase	**-**	**-**	**0%**
Finalise documentation	05/06	09/06	0%
Deploy solution	06/06	10/06	0%
Class Project Presentations	06/06	06/06	0%
Weekly Team Meetings	09/06	09/06	0%
Finalise Working Prototype	09/06	09/06	0%
Weekly Sprint Meeting	10/06	10/06	0%
Close project	10/06	10/06	0%
Post-project Phase	**17/06/22**	**19/06/22**	**0%**
Benefits assessment	17/06	17/06	0%
Project Review Report submission	19/06	19/06	0%

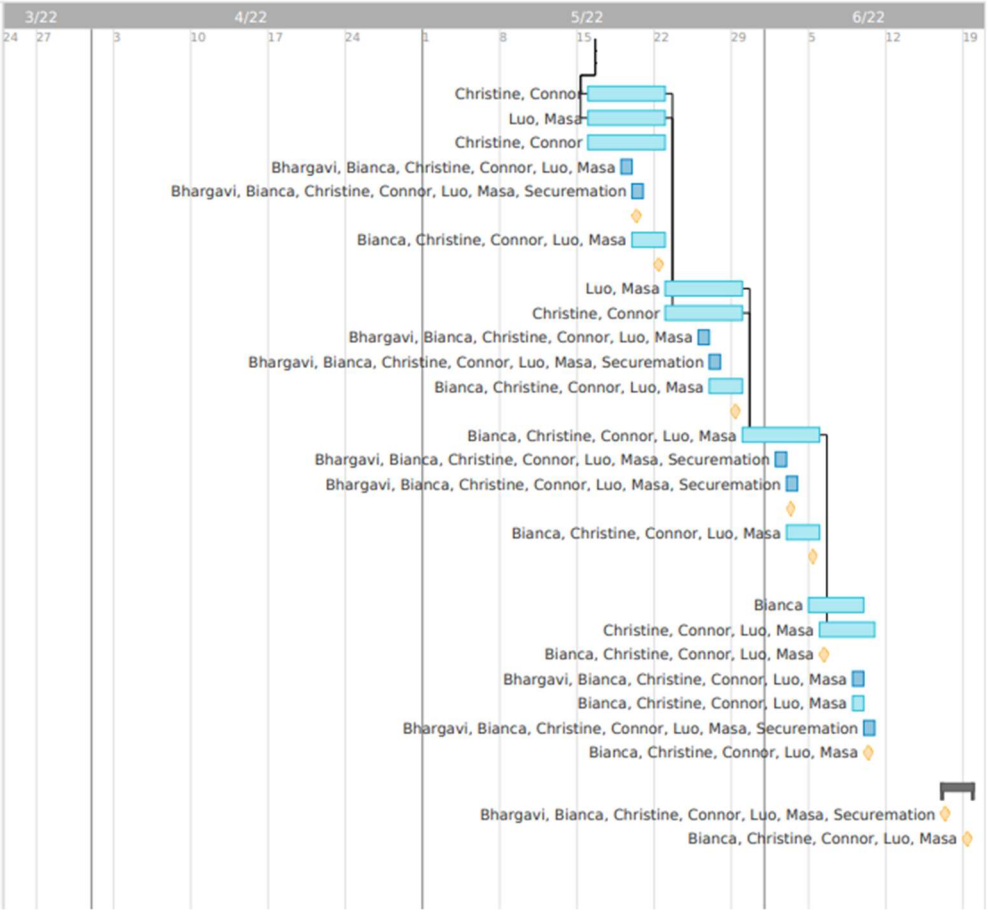


Figure 8. Example of Agile Project Planning approach via Trello

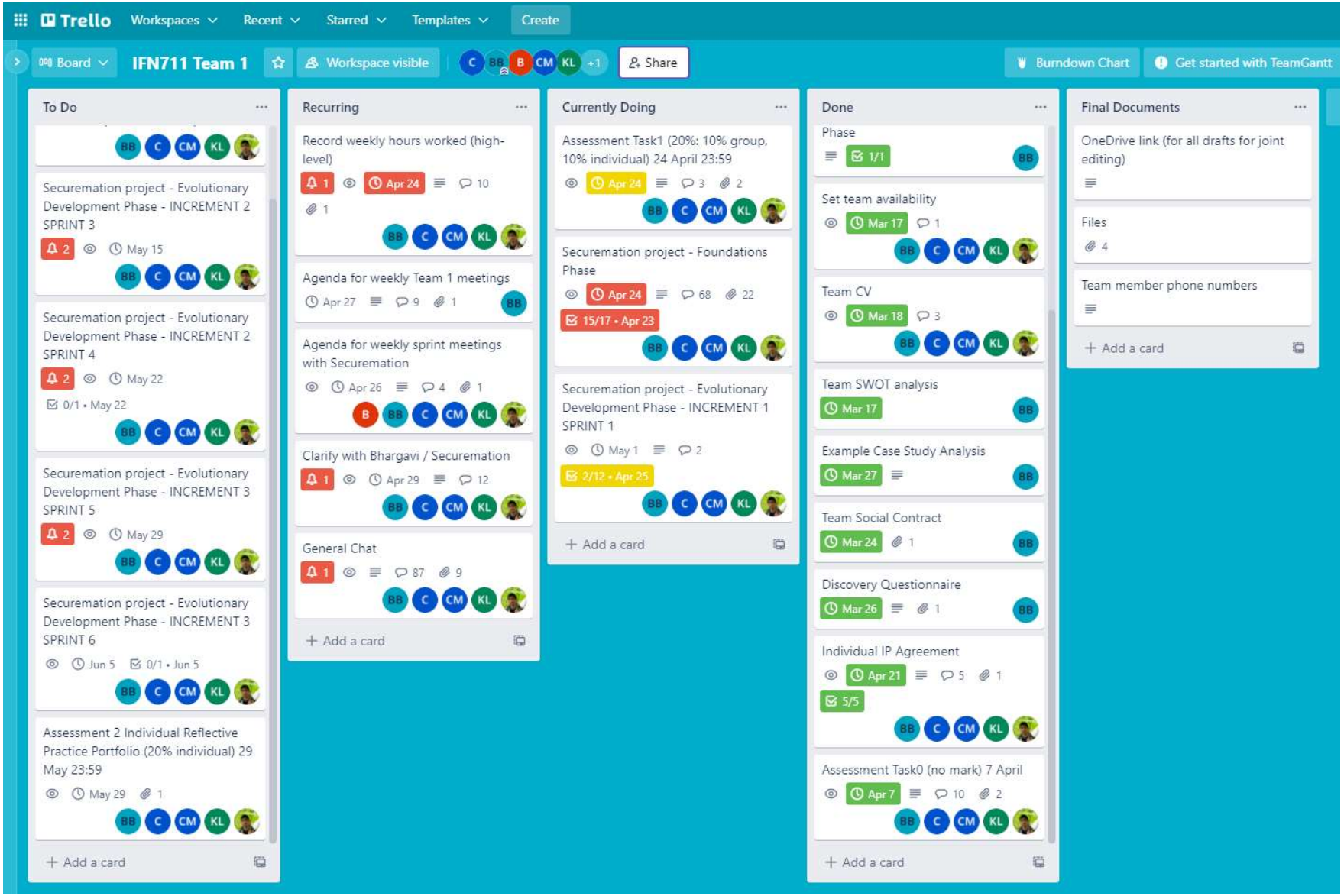
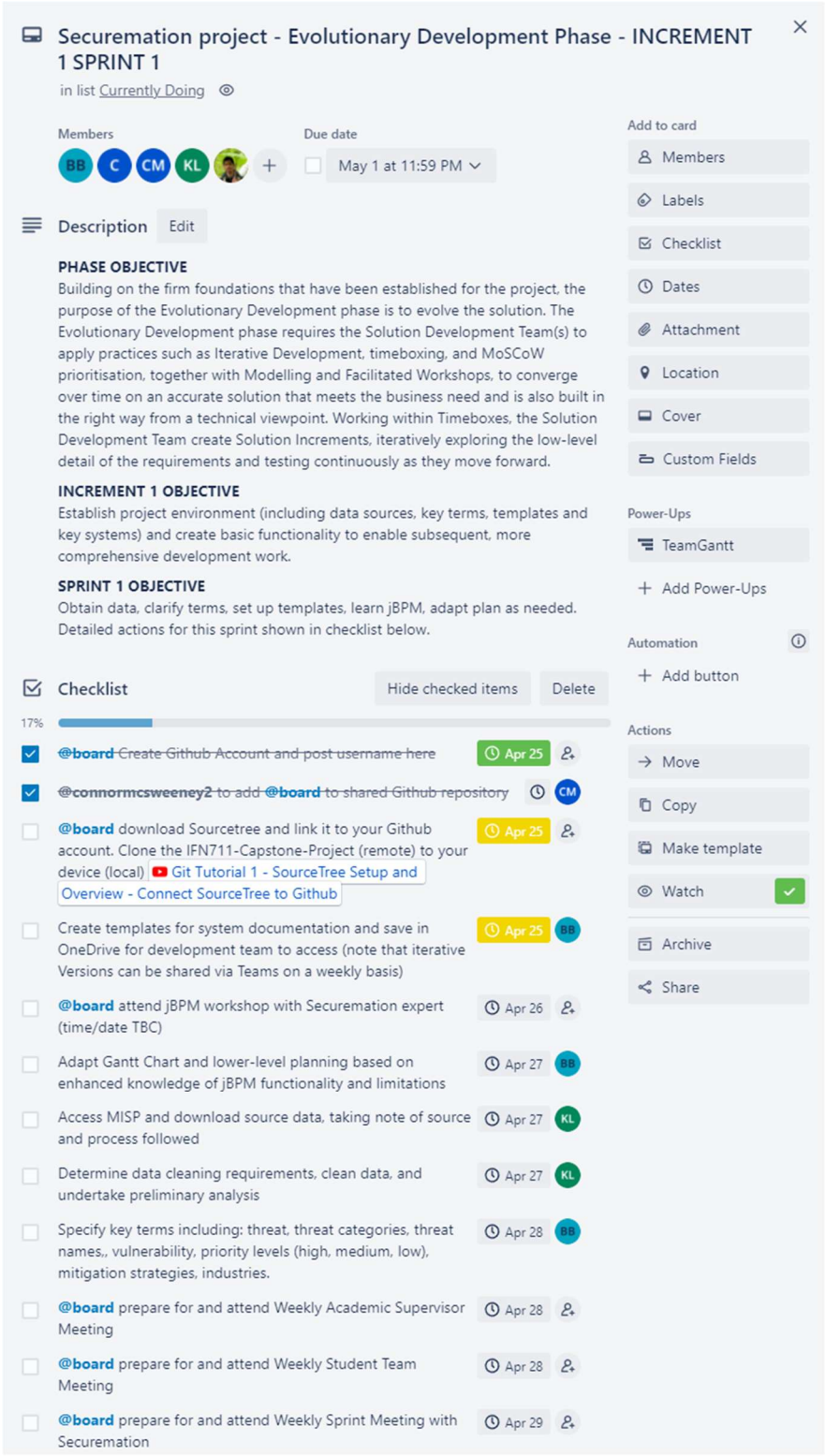


Figure 9. Example of detailed timebox (aka sprint) planning approach via Trello



6. Communications and Risks

6.1 Communication

Communications across all stakeholders are listed in the Communication Plan in Table 7. The project team have planned for weekly Face to Face (F2F) meetings as a means for planning effective and high-fidelity communications in cases where the project requires detailed clarification. In addition to this, the DSDM approach utilises all available options to share information including digital channels where suited to support collaboration. The Project Manager coordinates key communications with support from the project team to ensure that channels are organised, complete, and timely. To ensure the effectiveness across all communications, the team will apply the following strategies throughout the duration of this project:

- Ensuring all team members have completed onboarding training for channels such as Trello, Teams and Zoom.
- Adhering the agreed rules of engagement according to the Team Social Contract available in Appendix 3, namely attending stakeholder meetings on time, ensuring everyone has a turn to speak and communicating respectfully.
- Following the RACI Matrix in Table 7. below to direct appropriate levels of communication to the most suitable stakeholder.

Individual roles and responsibilities (including communications) are aligned with the DSDM roles (Agile Business Consortium, 2014c) set out in Table 6 below, and further elaborated on in Appendix 3.

Table 6. DSDM Role Alignment

Internal Stakeholder	
Academic Supervisor	Bhargavi Goswami
External Stakeholder	
Industry Partner	Securemation Project Team
Project Level Team	
Business Sponsor	Ashwin Sharma
Business Visionary	Ashwin Sharma
Technical Coordinator	Ashwin Sharma (or Manjeet Kaur and Murilo Oliveiro as delegated)
Project Manager	Bianca Beaumont
Solution Development Team	
Team Leader	Bianca Beaumont
Business Analyst	Bianca Beaumont
Business Ambassadors	Manjeet Kaur and Murilo Oliveiro
Solution Developers	Connor McSweeney, Christine Choy, Koh Hei Luo and Masayoshi Kamioki
Solution Testers	Connor McSweeney, Christine Choy, Koh Hei Luo and Masayoshi Kamioki
Supporting Team	
Business Advisors	Manjeet Kaur and Murilo Oliveiro
Technical Advisors	Murilo Oliveiro, Manjeet Kaur and Bhargavi Goswami
Workshop Facilitator	Bhargavi Goswami / Bianca Beaumont
DSDM Coach	Bhargavi Goswami
Legend	
	Business interests, roles representing the business view
	Solution/technical interests, roles representing the solution/technical view
	Management interests, roles representing the management/leadership view
	Process interests, roles representing the process view

Table 7. RACI Matrix for Key Stakeholders

No.	Task	Business Visionary / Project Sponsor	Technical Advisors/Business Ambassadors	Project Manager /Team Leader/Business Analyst	Solution Testers /Developers	Academic Supervisor
Phase 1: Foundations						
1.1	Ensure Consistency of Agile DSDM practices across teams	I	I	R	A	C
1.2	Provide vision and goal for the product	R	C	A	A	I
1.3	Provide Resources with the right skills and mindset	C	R	I	I	R
1.4	Prioritize and Manage product backlog	C	C	R	A	I
1.5	Report on time to management	I	I	A	R	I
1.6	Ensure Quality of the product	C	C	C	R	I
1.7	Manage risks according to Risk Assessment	C	C	A	R	C
1.8	Organise weekly sprint meetings	C	C	R	A	A
1.9	Approve user stories to meet acceptance criteria	C	C	R	R	C
1.10	Organise weekly Team meetings	I	I	R	A	I
Phase 2: Evolutionary Development						
2.1	Database structure	I	C	A	R	C
2.2	Key Terms and Taxonomy	I	C	R	R	I
2.3	Mitigations and relational mapping	C	C	A	R	C
2.4	Front-end API	I	C	A	R	I
2.5	Back-end API's	I	C	A	R	I
2.6	jBPM Workflow	I	C	A	R	I
2.7	Machine Learning Module	I	C	A	R	C
2.8	Solution testing	I	C	A	R	C
2.9	Component integrations	I	C	A	R	C
2.10	Testing and Quality Control	C	C	R	R	C
Phase 3: Deployment						
3.1	Assess potential security risks	C	A	R	R	I
3.2	Review of assembled solution	C	C	R	R	C
3.3	Finalised Documentation of system	C	C	R	R	C
3.4	Finalisation of working Prototype	C	C	R	R	C
Phase 4: Post-Project						
4.0	Benefits Assessment	I	I	R	R	C

RACI Legend	
Responsible	Person who is completing the task
Accountable	Person who is making decisions and taking actions on the task(s), answerable to the success of the task
Consulted	Person who will be communicated with regarding the decision-making process and specific tasks. Subject matter expertise as required for advice.
Informed	Person who will be updated on decisions and actions during the project

Created based on a template from stakeholdermap.com (n.d.).

Table 8. Communication Plan

Description	Audience	Objective	Schedule	Channel/s	Owner
Team Meeting	Student Team	Report status, identify issues, develop solutions as a team, review new information	Weekly (Thursday 9:00AM-10:30AM)	F2F Meeting / Trello / OneDrive	Project Manager
Team Progress Presentation Meeting	Student Team, Academic Supervisor	Advise of current progress, plan for project status meeting with Securemation, Academic related questions	Weekly (Thursday 10:30AM-11:00AM)	Zoom / Trello	Project Manager
Weekly Sprint Meetings	Student Team, Academic Supervisor, Securemation (All Project Stakeholders)	Present progress (interim deliverables), identify issues, develop solutions as a team, review new information, confirm acceptability criteria	Weekly (Friday 11:30AM-12:30PM)	F2F Meeting / MS Teams (Chat and Files tabs) supported by meeting pack (PPT and attachments)	Project Manager
Project check-ins and discussion (akin to daily stand-up)	Student team	Report status and communicate pressing issues	Daily	Trello / OneDrive	Project Manager
Academic Advice	Student team members, Academic Supervisor	Seek advice relating to assessment, cyber security requirements, TensorFlow, and project management techniques/processes	As Needed	E-mail / WhatsApp	Project Manager
Securemation resources	Technical Coordinator, Academic Supervisor and Solution Development Team	Shared documents from Securemation (e.g. examples, training materials etc)	As Needed	Microsoft Teams	Project Manager
Milestone Review	All Project Stakeholders	Review status, present deliverables, gather feedback	At Milestones	F2F Meeting / MS Teams	Project Manager
Symposium	All Project Stakeholders	Demonstrate project artefact and receive peer feedback	At project end	F2F presentation	Student Team
Final Review	All Project Stakeholders	Review successes and failures to capture improvements for future projects	At project end	F2F Meeting / Zoom	Project Manager

Created based on a template from Martins (2021)

6.2 Risks

A risk assessment was undertaken with the use of the DSDM Project Approach Questionnaire (Appendix 2), and via discussion with Securemation and development team members (summarised in Table 8). Aligning with Securemation's own risk tolerance line, treatments/mitigations for all 'high' risks have been identified, with all moderate and low risks either accepted and/or mitigated. Time and resources required to implement listed mitigation actions – such as comprehensive testing and documentation – is built into the detailed delivery plan (Gantt chart) and corresponding budget.

Table 9. Project Risk Register

ID	Likelihood	Impact	Risk	Risk Response Category	Risk Owner	Risk Type	Risk Description	Risk Response Details
A	Likely	Minor	Medium	Accept / Mitigate	Project Manager	People	Due to variable levels of understanding of the DSDM approach (philosophy, roles, principles and practices) within the project team, work practices stymie smooth project progress.	Student team to carefully study DSDM approach, utilise DSDM Coach as needed, and apply flexibility in their partnership with Securemation through client-focussed approach. The Project Manager and DSDM Coach will carefully support engagement with all project stakeholders and support via training as required. Approaches detailed within this project plan (including clarity of DSDM role responsibilities) will significantly mitigate this risk.
B	Possible	Major	High	Accept / Mitigate	Project Manager	People	Due to limited technical expertise of Student Team, there are an insufficient breadth / depth of skills to collaboratively develop an optimal business solution.	Team members to leverage complementary knowledge and skills in development languages, including proactively drawing on expertise of DSDM Coach and Securemation team, and scope according to reasonable achievements.
C	Possible	Moderate	Medium	Mitigate	Project Manager	Technology	Under or overfitted machine learning model caused by training dataset being noisy and having garbage values, in which the model output accuracy does not represent the actual performance of the model and could mislead the users to make faulty decisions.	Perform data cleaning process to ensure the consistency, completeness and usability of the data prior to model training. Proactively monitoring to review accuracy / fitting and using appropriate data inputs accordingly.

D	Possible	Moderate	Medium	Accept / Mitigate	Project Manager	Technology	Due to limited technical expertise of Student Team, there is a likelihood the proposed existing technologies utilised in the design of the project solution may not include all the expected functionalities required to adequately develop the solution.	Research and training in existing technologies as well as guidance from industry experts has been scoped within the evolutionary development phase with the aim of illuminating any gaps in functionality. If gaps arise, additional technologies targeting bespoke needs will be incorporated into the design, and requirements marked 'Should/Could' will be de-prioritised.
E	Unlikely	Catastrophic	High	Mitigate	Project Manager	Technology	Due to the potential for certain data sources to be unreliable, outdated, duplicative or compromised, the accuracy and reliability of the ML model may be affected, thereby leading to unintended or poor decisions.	Draw on expertise of solution development team and technical advisors to source data from reliable and secured databases, provide less 'weight' to data gathered from potentially unreliable source within the ML model.
F	Unlikely	Catastrophic	High	Mitigate	Project Manager	Technology	Due to insufficient cyber security measures, unauthorised back-end access to jBPM and TensorFlow development projects housing API and machine learning model may result in the failure to uphold ethical responsibilities including the maintenance of confidentiality, integrity and availability of data and/or model, and complete or partial non-delivery of the solution.	Draw on expertise of solution development team and technical advisors to implement adequate protections such as authorisations and authentication, and make use of multiple versions for backup purposes. Implement a consistent workflow process and code control with regular peer reviewing. Ensure that any sensitive and personalised data is handled with care and adequately secure, including privacy and information management statements as needed.
G	Unlikely	Catastrophic	High	Mitigate	Project Manager	Project	Due to incomplete or incorrect understanding of Securemation's needs, the solution delivered is not 'fit for purpose' and/or fails acceptance.	Apply greater rigour in scoping and planning upfront in feasibility and foundations phase, including use of waterfall tools (Gantt) and regular meetings with Securemation.
H	Unlikely	Moderate	Medium	Mitigate/ Transfer	Project Manager	Project / Technology	Due to lack of recorded system documentation, ongoing maintenance and further development of solution is hampered, and business benefits are not fully realised by Securemation.	Complete comprehensive system documentation throughout the project and schedule detailed handover, with increased allocation in final increment. Securemation will take carriage of the prototype to further develop in light of their ongoing business needs.

I	Unlikely	Major	Medium	Accept / Mitigate	Project Manager	Project	Due to high percentage (70%) of requirements within the 'Must' category, team is unable to deliver expected minimum viable product within the timeframe and budget available.	Undertake early and comprehensive scoping with Industry Partner, borrow waterfall tools (Gantt chart) to de-risk forward planning of development phase, allocate sufficient time and effort to the understanding of the environment and technologies used within the project, particularly during the foundation and evolutionary development phases. Requirements marked 'Should/Could' can be de-prioritised.
J	Rare	Catastrophic	High	Mitigate	Project Manager	Technology	Due to unforeseen technical failure, there is a significant loss of data or infrastructure, resulting in complete or partial non-delivery of the solution.	Undertake comprehensive testing prior to each deployment, housing and backing-up all data securely and continuously, and use only known / reliable infrastructure providers.
K	Rare	Major	Medium	Mitigate	Project Manager	Technology	Due to unexpected changes to component compatibility or functionality, solution integration and functioning is negatively impacted or temporarily disabled.	Separate ML model and API integration functionality, and undertake regular automated testing of component connectivity (out of scope of this project prototype).
L	Rare	Major	Medium	Mitigate	Project Manager	Project / Technology	Due to novel threat types emerging in source databases, some outputs do not have corresponding mitigation strategies, rendering the solution not 'fit for purpose' and/or failing acceptance.	Manual or automated testing for unidentified threat types to aid in identify emerging gaps and assigning corresponding strategies.
M	Rare	Moderate	Low	Accept / Mitigate	Project Manager	Technology	Due to insufficient system capacity, business as usual demands cannot be met resulting in downtime.	Utilise cloud services and known / reliable providers to enable scaling and service reliability.
N	Rare	Moderate	Low	Mitigate	Project Manager	Technology	Due to threat actors intentionally overloading system via multiple requests, the solution becomes temporarily unavailable for users.	Limit querying by an individual IP address via use of authentication (see above).

7. Project Resourcing and Costs

An indicative project budget is provided in Table 9 below. Personnel costs broadly align with resource allocation shown in Figure 7 of the Gantt Chart . QUT Project Team personnel costs reflect a minimum time investment of 20 hours per week by each of the QUT Student Team. Personnel daily 'charge-out' rates have been benchmarked against industry rates where possible (ClicksIT, 2022), and a small contingency has been included for DSDM coaching and technical assistance, reflecting the risk mitigation strategies listed in section 6.2. Due to the relatively short timeframe and size of this project, typical project management costs such as office space, IT infrastructure, physical and professional insurances, as well as hardware purchases and depreciation have not been included in this project budget, though it is acknowledged such costs may be relevant in an expanded/extended project format.

Table 9. Project budget

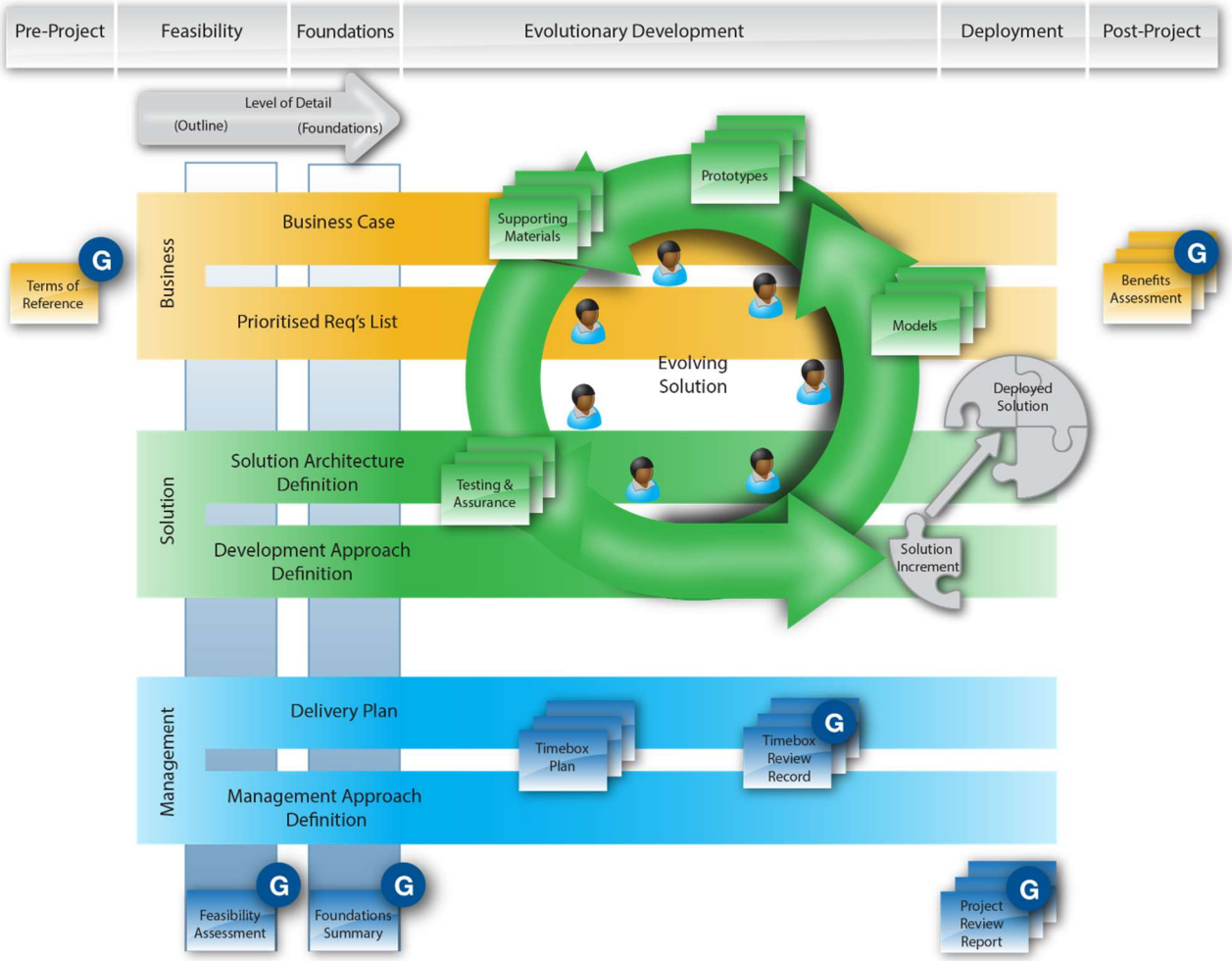
Personnel costs										
				Increment 1		Increment 2		Increment 3		
Team	Role	Resource role and name	Daily Rate	Days	Cost	Days	Cost	Days	Cost	Total
Industry Partner (Securemation)	Business Sponsor / Visionary / Technical Coordinator	Ashwin Sharma	$1,250	0.5	$625	1	$1,250	0.5	$625	$2,500
Industry Partner (Securemation)	Business Ambassadors / Technical & Business Advisors	Murilo Oliviera and Manjeet	950	2	$1,900	3	$2,850	2	$1,900	$6,650
QUT Project Team	Workshop Facilitator / DSDM Coach	Bhargavi Goswami	$950	1	$950	2	$1,900	1	$950	$3,800
QUT Project Team	Project Manager / Solution Developers & Testers	Bianca Beaumont, Connor McSweeney, Masayoshi Kamioki, Koh Hei Luo, Christine Choy	$400	25	$10,000	25	$10,000	25	$10,000	$30,000
SUBTOTAL										$42,950

Non-personnel costs and contingencies					
Item	Description	Cost	Cost	Cost	Total
Software	Trello Premium/Powerups, TeamGantt Premium and Canva Premium	$90	$45	$45	$180
Project / Workshop consumables	Stationery, meeting catering and sundries, and end of project close-out celebration	$117	$117	$217	$450
Travel contingency	Taxis to attend weekly sprint meetings at QUT / Securemation site or occasional parking if required	$50	$100	$100	$250
Risk Mitigation contingency (project delivery)	Provision for 2 days DSDM Coaching and workshops if required	$950	$475	$475	$1,900
Risk Mitigation contingency (product development)	Additional 3 days of Security Analyst time to help customise JBPM components if required	$950	$950	$950	$2,850
SUBTOTAL					$5,780
TOTAL COSTS					$48,730
Funding					
Funding (QUT School of Information Systems contribution for Course / Project Coordination in-kind contribution)					$16,230
Funding (QUT Student Team in-kind contribution)					$32,500
TOTAL FUNDING					$48,730
PROJECT BALANCE (ADDITIONAL FUNDING REQUIRED)					$0

8. Project Controls

AgileBusiness.org sets out a number of artefacts that are typically delivered in each phase of a DSDM project, as shown in Figure 10 below (Agile Business Consortium, 2014d, p. 54).

Figure 10. – DSDM cycle and key artefacts.



Note: From The DSDM Agile Project Framework Handbook (p. 54), by Agile Business Consortium, 2014, DSDM Consortium, Copyright 2014 by Dynamic Systems Development Method Limited.

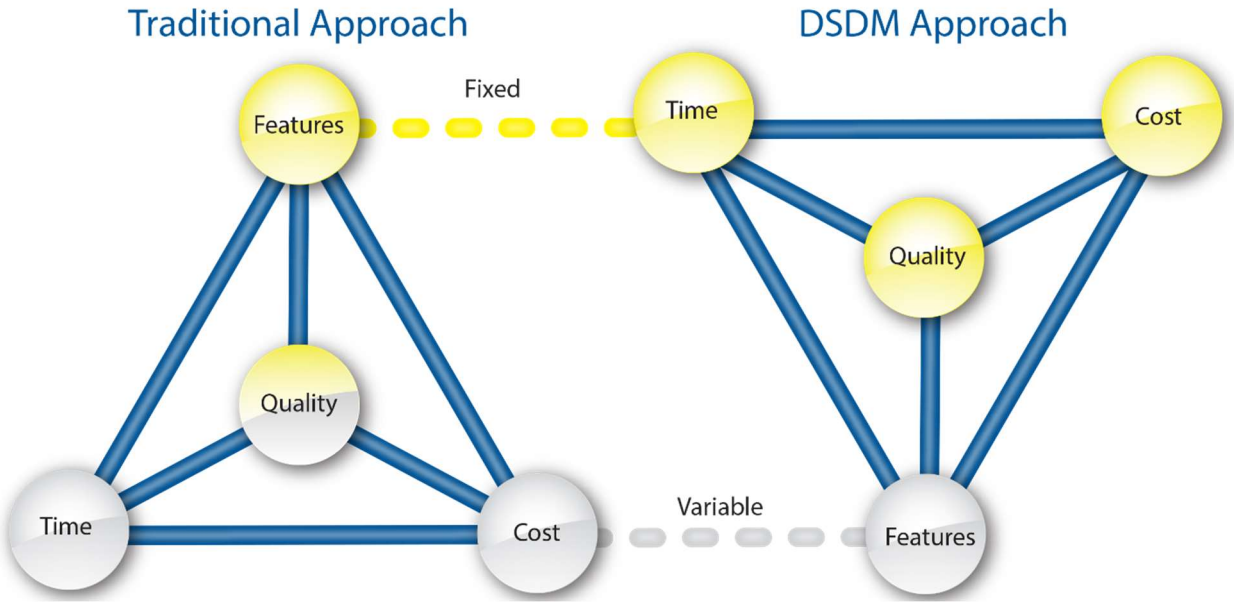
In keeping with the Agile Manifesto's emphasis on functioning software over comprehensive documentation (Beck et al., 2001) the approach to DSDM and the development of this project plan has been lightly adapted to deliberately exclude the reproduction of detail-heavy governance documentation in order to optimise time available for requirement elicitation, scoping, and evolutionary development planning. Indeed, DSDM documentation (products) should only be created where they add genuine value to the project and/or to the solution (Agile Business Consortium, 2014d). This lightly-adapted approach has been particularly appropriate in light of the steep learning curve presented by the introduction of multiple new technologies (such as TensorFlow, jBPM, and Microsoft Teams).

As such, various DSDM-typical documentation (namely a Terms of Reference, Feasibility Assessment, and (detailed) Business Case) was deliberately excluded from this plan as standalone products. These were deemed duplicative with the detail contained in the PRL, Gantt, and Trello Board, and would in fact detract from the overall 'agile' project management process by adding an unnecessary layer of administrative complexity. Recordings of the weekly team meetings and sprint meetings (with Securemation) will serve as Timebox Review records in lieu of additional written documentation. The Project Review Report and Benefits Assessment (if possible) will be captured within the final IFN711 Project Review Report. Notwithstanding the reduced documentation, a number of project controls will continue to be implemented to manage the following key project challenges:

8.1 Trade-off Management

An agile DSDM approach was deliberately chosen in response to the known challenge of fixed *Time* (as detailed in the Gantt Chart (Figure 7), fixed *Cost* (Table 10) as set by the Academic Supervisor and Securemation, and *Quality* as determined by Securemation representatives; thus only leaving room for flexibility of *Features* (Agile Business Consortium, 2014e, p. 19) (Figure 11, below).

Figure 11 - variables across traditional and DSDM approaches.



Note: From The DSDM Agile Project Framework Handbook (p. 19), by Agile Business Consortium, 2014, DSDM Consortium, Copyright 2014 by Dynamic Systems Development Method Limited.

To overcome this challenge, prioritisation of features (expressed as requirements) using 'MoSCoW' (Must/Should/Could/Won't) was adopted as part of the DSDM approach, in order to enable the dropping or deferral of lower priority features if needed, and with agreement by the Business

Visionary (Agile Business Consortium, 2014e). Importantly, this will be done in a highly adaptable and flexible approach, at all times applying common sense and pragmatism.

An acceptable level of *Quality* will be assured by taking an iterative and incremental approach to solution development, and by presenting progress, seeking feedback, making amendments where required, and confirming quality acceptance via weekly sprint meetings with Securemation.

8.2 Artefact Quality Assurance

One of the key principles of the DSDM approach is to '*Never compromise quality*' (Agile Business Consortium, 2014f). Accordingly, the adoption of the DSDM approach for this project requires agreement on what constitutes 'good enough' (i.e. acceptance criteria) in terms of the quality of the features to be delivered.

This is to occur prior to development commencing, at the Weekly Sprint Meeting with Securemation (in accordance with the Communication Plan). Additionally, preparation of detailed documentation and integration of constant review and continuous quality assurance / testing processes throughout the Evolutionary Development Phase will ensure that the delivered solution and its component artefacts will meet the expected quality standards of Industry Partner Securemation. The Project Manager will ensure that all team members are empowered and supported to deliver on this commitment.

8.3 Progress Tracking and Reporting with Academic Supervisor

As outlined in section 5, a Gantt Chart and Trello Board will be used to schedule tasks and milestones, and provide high-level visibility and tracking of progress against agreed dates. This will be communicated via regular meetings and adhoc electronic communication with our Academic Supervisor. Tracking and reporting on progress will be comprehensively summarised at each Weekly Sprint Meeting, which will follow the below (indicative) standing agenda:

1. Demonstration of previous weeks' work (*via PPT or live demo*) per Gantt Chart "Interim Deliverables"
2. What was NOT completed in the previous week if applicable *(reporting by exception)*
3. What help or clarity is required (*e.g. blockages/tech support*)
4. What is planned for the coming week (*next sprint*)
5. Confirmation of quality (*i.e. acceptance criteria*) of upcoming deliverables/features
6. Feedback / questions / other business / next meeting

To ensure that the above project controls are implemented consistently, a social contract and list of individual contributions are provided in Appendix 3, outlining how the team will work together toward their shared goals, and ultimately help create business value for our partners at Securemation.

9. References

1. Agile Business Consortium. (2014a). Chapter 11: Iterative Development. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 77-86). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_11_IterativeDevelopment
2. Agile Business Consortium. (2014b). Chapter 2: Choosing DSDM. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 9-16). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_02_ChoosingDSDM
3. Agile Business Consortium. (2014c). Chapter 7: Roles and Responsibilities. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 41-52). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_07_RolesResponsibilities
4. Agile Business Consortium. (2014d). Chapter 8: Product. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 53-60). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_08_Product
5. Agile Business Consortium. (2014e). Chapter 3: Philosophy and Fundamentals. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 17-20). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_03_PhilosophyFundamentals
6. Agile Business Consortium. (2014f). Chapter 4: Principles. In Agile Business Consortium (Ed.), *The DSDM Agile Project Framework Handbook* (pp. 21-26). DSDM Consortium. https://www.agilebusiness.org/page/ProjectFramework_04_Principles
7. Australian Cyber Security Growth Network Limited. (n.d). *Australian Cyber Security Industry Roadmap – Executive Summary.* https://www.austcyber.com/resources/industryroadmap
8. Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, RC., Mellor, S., Schwaber, K., Sutherland, J. & Thomas, D. (2001). *Manifesto for agile software development.* http://agilemanifesto.org
9. Clicks IT Recruitment. (n.d.) *Scrum Master Salary & Rates Guide*. Retrieved April 23, 2022, from https://clicks.com.au/job-salary/scrum-master/
10. Clicks IT Recruitment. (n.d.) *Security Analyst Salary & Rates Guide*. Retrieved April 23, 2022, from https://clicks.com.au/job-salary/security-analyst/

11.FIRST. (2019). *The Common Vulnerability Scoring System version 3.1*. https://www.first.org/cvss/specification-document

12.Google Brain Team. (2022). TensorFlow (Version 2.8.0) [Machine learning library]. Zenodo. https://www.tensorflow.org/

13.Martins, J. (2021). *Why a clear communication plan is more important than you think.* https://asana.com/resources/communication-plan

14.Red Hat. (2022). jBPM (Version 7.68.0) [Computer software]. Red Hat. https://www.jbpm.org/

15.Securemation Consulting. (n.d.a). *About Us.* https://www.securemation.com/about-us/

16.Securemation Consulting. (n.d.b). *Threat and Risk Assessment.* https://securemation.com/threat-and-risk-assessment/

17.Smith, F. & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, 71:6, 642-660.

18.Stakeholdermap.com (n.d.). Project Management Templates: RACI Chart. https://www.stakeholdermap.com/project-templates/RACI.xlsx

19.Talent.com. (n.d). *Senior Security Analyst average salary in Australia 2022.* https://au.talent.com/salary?job=senior+security+analyst#:~:text=The%20average%20senior%20security%20analyst%20salary%20in%20Australia%20is,year%20or%20%2461.09%20per%20hour

20.Teo, C. S. & Mahmood, A. K. (16-17 July 2017). *National cyber security strategies for digital economy.* [Conference paper]. 2017 International Conference on Research and Innovation in Information Systems, Langkawi, Malaysia. https://ieeexplore.ieee.org/abstract/document/8002519

21.Wikipedia. (2022). *Cynefin framework.* https://en.wikipedia.org/wiki/Cynefin_framework

Appendix

Appendix 1. Original Project Overview

Unit	IFN711 - IT Industry Project
Position title	CISO
Business phone	422120526
Business email	ashwin.sharma@securemation.com
Title of the Proposed Project	AI for Industry based Cyber Security Threats
Primary Discipline Area of the Project	Network/Security
Secondary Disciplines	AI
Your organisation	We are a cyber security company that is trying to simplify the management of cyber security concerns for any organisation. We are passionate about increasing the ability of organisations to self-serve more cyber security needs then they do currently, thereby reducing cost and increasing the security posture and agility of the business
Project description	"Goal: To create a capability that allows a software program to scan the internet and open source repositories for recent cyber security threats and categorise the threats to particular industries/market segments, threat criticality, and vulnerabilities leading to potential exploitation via the threat vector. Requirements: AI engine, Micro-service architecture, API based integration to utilise the service. E.g. a consumer can provide an industry type, and the service will return a json payload listing the current high priority threats/vulnerabilities/exploits facing the industry
Project deliverables	Prototype micro-service
Time Commitment	Engage remotely - via Microsoft Team's sessions. Some face to face sessions would be required initially for establishing relationships. Some catch-ups can be done in our Brisbane office as well. I would estimate a minimum of 1.5 days per week of effort by the students with a weekly 1-1.5 hour supervision sessions with us
Required Knowledge and Skills	Basic software development e.g. python, AI knowledge e.g. Tensorflow -https://www.tensorflow.org. Cyber security awareness and understanding of threat vectors, vulnerabilities and exploits
Project IP and Confidentiality Requirements	
Project review comments	SP Feb 2022: Will suit students with Security and CS backgrounds. The project deliverables need to be listed for better clarity. For example, prototyping the micro service would include 1. designing the micro-service architecture, 2. basic AI dev requirements, 3. ..... etc.

Appendix 2. Project Approach Questionnaire

Project Approach Questionnaire (PAQ)

Project: AI FOR INDUSTRY-BASED CYBER SECURITY THREATS		Name: BIANCA BEAUMONT
Date: 7 APRIL 2022		Position: PROJECT MANAGER

		Indicate the closest collective opinon					*Where appropriate, comment on issues or risks related to a more negative response to this aspect of the DSDM approach*
Ref	**Statement**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**	
1	All members of the project understand and accept the DSDM approach (Philosophy, Principles and Practices)		Y				SOMEDETAILED DSDM THEORY IS NEW TO SOME MEMBERS OF THE TEAM, HOWEVER ALL ARE VERY FAMILIAR WITH AGILE WORKING
2	The Business Sponsor and the Business Visionary demonstrate clear and proactive ownership of the project.	Y					
3	The business vision driving the project is clearly stated and understood by all members of the project team	Y					
4	All project participants understand and accept that on-time delivery of an acceptable solution is the primary measure of success for the project	Y					
5	The requirements can be prioritised and there is confidence that cost and time commitments can be met by flexing the scope of what's delivered.	Y					
6	All members of the project team accept that requirements should only be defined at a high level in the early phases of the project and that detail will emerge as development progresses.		Y				WE ACKNOWLEDGE THAT THERE IS A DESIRE TO DEFINE REQUIREMENTS UP FRONT AS MUCH AS POSSIBLE TO DE-RISK THE DEVELOPMENT PROCESS IN THIS PROJECT
7	All members of the project team accept that change in requirements is inevitable and that it is only by embracing change that the right solution will be delivered.	Y					
8	The Business Sponsor and Business Visionary understand that active business involvement is essential and have the willingness and authority to commit appropriate business resources to the project.	Y					
9	It is possible for the business and solution development members of the Solution Development Team to work collaboratively throughout the project.	Y					
10	Empowerment of all members of the Solution Development Teaam is appropriate and sufficient to support the day-to-day decision-making needed to rapidly evolve the solution in short, focussed Timeboxes	Y					
11	The DSDM roles and responsibilities are appropriately allocated and all role holders understand and accept the responsibilities associated with their role.		Y				ENSURE SECUREMATION ARE COMFORTABLE WITH ROLES IN DISCOVERY QUESTIONNAIRE PER DSDM FRAMEWORK AT https://www.agilebusiness.org/page/ProjectFramework_07_RolesResponsibilities
12	The Solution Development team has the appropriate collective knowledge and skills (soft skills and technical skills) to collaboratively evolve an optimal business solution.		Y				WE ACKNOWLEDGE SOME RISK DUE TO 'UNKNOWN UNKNOWNS' IN THE DEVELOPMENT AND SKILLSET OF TEAM MEMBERS
13	Solution Development Team members are allocated to the project at an appropriate and consistent level sufficient to fully support the DSDM timeboxing practice	Y					
14	Tools and collaborative working practices within the Solution Development Team are sufficient to allow effective Iterative Development of the solution.		Y				WE ACKNOWLEDGE SOME RISK DUE TO 'UNKNOWN UNKNOWNS' IN THE DEVELOPMENT AND AVAILABILITY OF ALL TEAM MEMBERS
15	All necessary review and testing activity is fully integrated within the Iterative Development practice.	Y					
16	Project progress is measured primarily through the incremental, demonstrable delivery of business value.	Y					
17	There are no mandatory standards or other constraints in place that will prevent the application of the DSDM Philosophy and Practices on this project.	Y					

Appendix 3. Team Contract Sheet (social contact and individual contributions)

QUT Student Team Social Contract

Team: Walking on SCRUMshine

Purpose

The following are a number of principles which will govern and guide how we engage and work together as a team. Each team member has agreed formally to abide by and model each of these principles. It is important to note that the below are not ranked or weighted; all apply equally, and to all team members.

Troubleshooting

- In the event that one or more of the below principles are challenged, needs to change, or is at odds with another principle or preferred way of working, the team social contract can be amended jointly and with full agreement of all team members.
- In the event that a team experiences conflict or concerns that cannot be resolved within the team, the Project Manager will escalate via an in-person meeting with our tutor Bhargavi in the first instance.

1. Meetings

- As a minimum, we will meet weekly via 'stand-ups' between 9:00am-11:00am each Thursday at P Block, GP Campus.
- We will meet with our Academic Supervisor Bhargavi Goswami and Industry Partners Securemation between 11:30am-12:30pm each Friday via Teams, or a location convenient to Securemation.
- Our weekly meetings will focus on a) work to be covered in tutorials (early part of Semester), and b) our industry project more specifically (increasingly in latter part of Semester).
- We will always be on time for our team meetings (including meetings with our Industry and Academic Supervisors). We will give advance-notice if running late unavoidably.
- We will only meet with our Academic and Industry Partners if all team members are present; this can include altering the meeting time/date and meeting via zoom if need be.
- We will endeavour to schedule adhoc meetings to accommodate the work and personal commitments of all team members, according to the 'Team Non-Availability Matrix' completed in Week 1 (in OneDrive).
- We will avoid lengthy meetings prior to the final delivery of a product, in order to maximise time available for fast, focused work.
- The Project Manager will ensure all formal meetings have an agenda and that actions are recorded / assigned in Trello.
- All team members will come prepared to meetings, having completed any prior work assigned.
- We will minimise distractions during meetings where possible, for example by turning mobile phones to silent or turning off notifications.
- We will acknowledge and respect the time and standing of our Academic Supervisor Bhargavi and other QUT staff members who are kindly representing our team as the key interface with

the industry partner/s. We will do our best to ensure that the quality of work presented via QUT Staff is of a high quality and reflective of the professionalism of QUT Staff.

2. Communication and team interaction

- Our communication preferences are (in order of preference) face to face, Trello (Student Team internal project management and file sharing), Microsoft Teams (SecureMation interaction and file sharing) email, and phone.
- Notwithstanding the above, we will work to accommodate the communication preferences of the Industry Partner and Academic Supervisor.
- We will engage with one another with the understanding that all members have equal voice, value, and responsibility.
- We will feel comfortable to raise problems (including work or team / interpersonal issues) however awkward of uncomfortable this may be. We will approach this 'awkwardness' as a potential opportunity for personal growth.
- Prior to each tutorial or internal student team meeting, templates and drafts will be populated in OneDrive to enable a) review of requirements and agenda, and b) concurrent group editing.
- Final documentation will be uploaded to the Documents card in Trello and shared with the Industry Partner via Microsoft Teams.
- We will respect each other's views and appreciate the natural differences in perspectives, backgrounds and knowledge areas. We will approach knowledge gaps as 'opportunities for growth'.
- We agree up-front that there are "no stupid questions", and we will all feel welcome to ask or question things that don't make sense, in order to identify and challenge assumptions.
- We will not interrupt others while talking as much as possible, and if on Zoom, will raise our hand instead of speaking over others.
- We will adhere to the QUT Student Code of Conduct and maintain a 'zero tolerance' for disrespectful behaviour toward team members, staff, and industry partners.
- We will jointly celebrate the successes of individuals and within the team as they occur throughout the project by formally marking each milestone to maintain team momentum and morale.

3. Agile way of working

- When assigned a task individually, team members will take full responsibility for delivery.
- We will notify our team member directly prior to formally handing over a task to ensure there is no confusion or concern.
- Whoever breaks the build, fixes the build, but all team members will be available to help.
- When Pair Programming, we will turn off distractions such as emails and instant messaging to create focus and respect for the programming partner.
- We will maintain documentation of our progress and project artefacts, however, will not prioritize very detailed documentation over progress and agility in working.

- We will endeavor to use the "*Skills for the Information Age 8 framework*" as an additional tool to guide our behaviour and skillset development. We will use this as a tool to aid personal reflective journaling, and align our development with the broad demands of industry.

The above social contract was originally formally agreed to by all student team members on 24 March 2022, and is further supplemented by the below summarised list of individual contributions which broadly align with the Roles and Responsibilities set out by the Agile Business Consortium (2014c).

Bianca Beaumont

Project Manager / Team Leader

- Assume the responsibility of ensuring effective, prompt and regular communication regarding progress, issues, and feedback within and between the team, Industry Partner and Academic Supervisor.
- Coordinate high-level planning and scheduling of the project in collaboration with relevant stakeholders.
- Supervise and be aware of any internal or external issues/risks; and keep track of the project progress against the expected plan.
- Motivate, inspire, empower and encourage the team to work together toward shared objectives.
- Provide support, guidance and facilitate discussion to help the team resolve any issues and manage any risks whenever difficult circumstances arise.
- Facilitate regular review and reflections with the team at the end of each timebox.
- Facilitate effective and appropriate scheduling of individual task and ensure all these tasks (including testing and review activity for each project increment, agreed products) are delivered or carried out as per the schedule.
- Track the progress of every team activity on a daily basis.
- Facilitate regular team meetings and adhoc workshops.

Business Analyst

- Help elicit and model requirements and vision of stakeholders regarding the product/solution, analyse the requirements and ensure that they (both functional and non-functional) are achievable and are of good quality, and communicate these to relevant stakeholders.
- Monitor and keep the PRL and other project documents up-to-date as the project evolves.
- Enable effective and timely communication and dialogue between Securemation and the technical team.
- Ensure that both the business and technical components of the solution work well collaboratively, and are be 'fit for purpose' for the business.

Connor McSweeney*, Christine Choy*, Masayoshi Kamioki**, Koh Hei Luo**

Solution Developers & Testers

- Actively working on the project at the detailed and technical level on a daily basis.
- Carry out work sprints in accordance with the PRL and project schedule.
- Communicate the progress of the project with peers and Project Manager on a regular basis.
- Develop, review and test the Solution Increment throughout and at the end of each Timebox.
- Develop detailed documentation to guide and support the deployment of the solution in live use.
- Communicate and report any changes or updates on the requirements and information that may likely affect the ongoing evolution of the solution.
- Define and develop test products such as test scenarios, test cases etc.
- Carry out any testing tasks required for quality assurance purposes to make sure that the delivered products are 'fit for purpose' and report the testing results.

** Connor & Christine will serve as leads on tasks associated with jBPM, namely management of system processes, automation of workflow, central API, etc.*

*** Luo & Masa will serve as leads on tasks associated with TensorFlow, such as the preparation and analysis of source data, and machine learning model development.*

Notwithstanding the above 'lead' allocations, the agile approach adopted is such that any and all resources – including the Project Manager/Business Analyst – can and will be assigned to the delivery of a task as part of regular forward-planning at the beginning of each weekly sprint, as needed, in a flexible and collaborative manner.

Team Signatures

Bianca Beaumont	*Bianca Beaumont, 24th April 2022*
Koh Hei Luo	*Koh Hei Luo, 24 April 2022*
Masayoshi Kamioki	*Masayoshi Kamioki , 24th April 2022*
Connor McSweeney	*Connor McSweeney , 24 April 2022*
Christine Choy	*Christine Choy , 24th April 2022*