Initial Requirement Elicitation

Interview style:

- A mix of structured and unstructured interview modes.
- A combined interview along with Team-Wombat
- Prepared questionnaire

Interview preparation

1. Research existing solutions to understand how the problems are addressed.
2. Organise a team meeting to discuss and list the questions to be asked to the client.
3. Check the team availability to set up an interview with the client.
4. Organise a meeting with the corresponding team DN-Wombat to discuss the meeting questions and list down the final interview questions in the document.
5. Assign roles and responsibilities to each team members.

Team Member	Role
Luke Hawkins	Interviewer
Nikunj Patel	Note-taking
Ishan Goyal	Interviewer
Daniel Jiang	Note-taking
Joel Kenna	Note-taking

Interview setup

1. Send an introductory email to the client and suggest the meeting time for the interview.
2. Promptly respond to the client correspondences to confirm the meeting time and send a Zoom meeting invite accordingly.

Interview process

1. Introduce the team and ask the client for permission to record the meeting.
2. Request the client for a brief introduction of the Project.
3. Assigned interviewers will begin interviewing the client.
4. Assigned note-takers will note down important points.
5. Conclude the meeting by providing an opportunity for all the interview attendees to ask questions.
6. If possible, set a subsequent meeting time.

Post-interview

1. Conduct a debrief meeting with the team and the corresponding team.

Interview Questions:

Scope	Question
Project background	1. Can you describe the problem background? 2. What problem are we looking to address? 3. The current process for normalising the data? 4. Is it just the security team using the normalized data? 5. What are security threats and anomalies? 6. How are you currently solving the problem? 7. Who will be using the product, will they be technical users or non-technical 8. How much time and often are they spending on this data normalisation? 9. How accurately does the data normalisation have to be? 10. Is all of the data essential, can we skip some columns? 11. Is there any more documentation that you could provide?

System as is	1. How is this problem being solved today? 2. What are the pain points? 3. Is the entire process manual? 4. Is there any documentation that you could provide?
System users	1. The goal of primary users & their technical expertise 2. The goal of the secondary user & their technical expertise
System to be	1. What do you expect the system to accomplish? 2. What are the objectives of the system to be built? 3. What business environment is this system used in? 4. What medium will it be provided on (web, desktop app, tool)? 5. Is it just as simple as comparing field names from different file formats and matching them together, eg (DateTime and Date)? 6. Is there a standardised data format for the normalized output, eg(date, time format, epoch, UTC)? 7. What kind of input load for this system a. Number of peak users b. Amount of daily data ingest c. Peak data ingest d. How accurately does the data normalisation have to be? 8. Required to collect / Ingest data or will all data be locally available to the tool? 9. Preferred application type? (web, desktop, existing solution)? 10. How much scope of incorporating existing solutions (elastic / Splunk / LogDNA / Fluentd)?

Primary User Project Elicitation

Goal:

- Guide for interview with Petrina (Telstra), currently seen as a primary user of the expected system. Interview to be held on Wednesday 24th March, 2021.
- To gain insight into specifically how the primary user is currently solving the problem, and what would be a good solution to them.

Team Member	Role
Luke Hawkins	Notes
Nikunj Patel	Notes
Ishan Goyal	Interviewer
Daniel Jiang	Notes
Joel Kenna	Notes

Process:

1. Set up interview times with clients
2. Formally email clients the zoom link
3. Start the interview off by introducing ourselves and introducing themselves.
4. Ask permission to record the meeting.
5. Ask them to explain the problem
6. 2 interviewers will be asking questions to the client to explore the problem.
7. 2 note takers noting the information.
8. Anyone can jump in with a new question.
9. Pre made draft of a Do/Be/Feel - Model to then be updated with including the client ~20 min (Created with the other team)

Questions:

1. Detailed outline of current process.
2. Do you pull all your logs from the data lake?
3. Would be convenient for the tool to exist on the data lake, or externally?
4. Is the data normalization input format files, co-located together, or are they dispersed across the system?
5. What happens when your log files do change format,
    a. What is the severity? Do bugs occur? Does the whole system break.
    b. How do you handle check, how long does it take.
    c. How frequent do these change.
6. Do have keep track of all the normalizations made together
7. What is the current normalization technique, (programming language, libraries)
    a. Documentation for unformatted log being manually formatted
8. Ask for logs raw, and expected normalization

Generated Do-Be-Feel Model from meeting:

WHO	DO	BE	FEEL	CONCERN
Data Scientist	Normalise the data automatically	Reliable	Intuitive	Internal Data security
Data Analyst	Map output to Elasticsearch, Splunk, Cloudera	Secure	Easy to use	Accuracy
Telstra Engineer	Track changes in log files	Extendible (addition of new formats)	Productive	Regex works for current data sample,but won't cover external cases
Telstra Data Science Intern	Explore the raw data for normalization purposes	Accurate	Not frustrated	
Security Team	Summarize properties of fields in raw data (availability)	Scalable	Easily accessible suggestions	
Telstra Data Engineer	Learns from past mappings for future suggestions /mappings	Documented	Less complex	

Integration and tuning team	Suggests better mapping by learning formatting of values to then inferred the field mapping	Informative		
Security Analyst	Regex matching validations			
	Validate mappings, give summary of mapping with the larger data set			