Project Initiation Report
Splunk CTF Environment

Sergio Rodriguez Chavez, Mab Leslie, Robert Kister, Octavia-andreea Constantin, Christopher McGrail, and Calum Rae

Table of Contents

Introduction

The Project Initiation Report is a ‘snapshot’ of the initial group project documentation. It is used as a way of underpinning the project by merging all completed documents into one single report, while also ensuring that any future progression is made in a controlled manor. The report itself is created by using the P3.express methodology, which is a simple and easy to use project management system. The body of the Initiation Report is comprised of the Project Description, which is used to outline the entire scope of the project, including the purpose for the project, the clients’ expectations, and any requirements. The Project Description helps the group to stay aligned with the high-level goals of the project throughout its execution. Within the appendices of the Initiation Report, a Deliverables mind map will be included that outlines the requirements for the project to be considered a success. As well as a diagram which shows the priorities of these requirements using the MoSCoW methodology. Finally, a Follow-Up register is included. This is used to highlight any potential risks that could impact the project, the effect they could have, and the team response to these risks should they occur.

1.0 Project Description

1.1 Purpose and Expected Benefits

The main purpose of the Splunk Capture the Flag (CTF) Environment project is to create a product which is to be used as an introductory or basic level training tool for new Security Analysists hired by the client. The new employees will be given access to the product prior to starting their new position, allowing them to gain valuable knowledge required within their new role. From this, the expected benefits of the Splunk CTF Environment will include employees attaining a greater understanding of their responsibilities and what is expected of them as a Security Analysist. It will also offer them the opportunity to develop their independent working and problem-solving skills, which are skills that will benefit them throughout their career.

1.2 Expected Cost and Duration

1.2.1 Cost

The initial estimated costs for the Splunk CTF Environment project are considered to be relatively low, this is due to the planned usage of free and widely available software throughout the entirety of the project. Splunk Enterprise, the software used by the client's employees and where the CTF environment will be created, is offered as a free trial over a 60-day period. This trial period should provide a sufficient timeframe for the development, testing, and presentation of the finished product to the client. Should the client be satisfied with the final product, it can then be transferred over to clients own Splunk Enterprise environment. The Splunk Enterprise package will be hosted using Amazon Web Services (AWS), which offers students the opportunity to use certain services free of charge for up to 12 months. Hosting Splunk this way will allow all project team members the ability to work collaboratively on one instance of the product, while also proving useful for the demonstration during the presentation to the client. Should any of the chosen software or services have unexpected costs, an alternative solution would be to contact Edinburgh Napier University to enquire about any resources they may be able to provide.

1.2.2 Duration

The duration of the project is expected to take no longer than a total of 15 weeks. This timeframe has been set out by Edinburgh Napier University, and the key stages can be seen in the table below. The dates stated to complete each stage are non-negotiable, although the university may provide an extension due to unforeseen circumstances.

Stage	**Start**	**End**
Project Initiation	24th January 2022	11th February 2022
Development	14th February 2022	1st April 2022
Development Review Week	4th April 2022	8th April 2022
Easter Break	11th April 2022	22nd April 2022
Presentation Development Week	25th April 2022	29th April 2022
Presentation	6th May 2022	6th May 2022

1.3 Requirement and Quality Expectations

1.3.1 Functional Requirements

- Splunk CTF Environment App
- Question dashboard
- Home screen/Introduction page
- Tutorials
- Logs/scripts to check answers

The functional requirements outlined above are the quality expectations and set of criteria as specified by the client to determine whether the project is a success. The product will be created as an App on the Splunk platform, which when utilized by the user will offer an introduction to the CTF Environment. This will then lead onto the question dashboard as well as offering in-depth tutorials on how to answer the questions.

1.3.2 Non-functional Requirements

- Transferable to the client's environment
- Admin only modification
- Code readability
- User-friendly
- Relevancy/Difficulty of questions
- Minimum number of questions

The non-functional requirements shown above, are the constraints as defined by the client and will be used to determine the overall quality of the finished product. The CTF Environment app should be easily transferable to the clients Splunk environment for continued use by future employees. The app should provide a high level of security by restricting access to modification to administrators only. To accommodate for any employee's lack of experience use Splunk software, the app should be user friendly and detailed explanations should be used throughout. The types of questions being asked should be relevant to new Security Analysts who have no prior experience, but difficult enough so that users are challenged. Finally, a minimum number of questions must be asked to cover all types of learning.

1.4 Stakeholder List

The table below lists those who have an interest within the Splunk CTF Environment project and can have an impact on the outcome of the project. For each of the stakeholders their name, role, and emailed address have been provided.

Name	**Role**	**Email**
Fake Client	Client	fake@client.co.uk
Jawad Ahmad	Sponsor	j.ahmad@napier.ac.uk
Sergio Rodriguez Chavez	Project Manager	40479334@live.napier.ac.uk
Mab Leslie	Team Member	40429125@live.napier.ac.uk
Robert Kister	Team Member	40215046@live.napier.ac.uk
Octavia-andreea Constantin	Team Member	40479260@live.napier.ac.uk
Christopher McGrail	Team Member	40540926@live.napier.ac.uk
Calum Rae	Team Member	40479327@live.napier.ac.uk

Professor Bill Buchanan from Napier University has offered to provide guidance to the team throughout this project if needed. Bill is widely renowned for his skills within the Cybersecurity industry and is very knowledgeable when it comes to using the Splunk software, while also running and hosting his own Splunk Enterprise environment for educational purposes. He will be a great asset should the team require assistance during the development stage.

Doctor Jawad Ahmad is the sole project sponsor for the Splunk CTF Environment group project. Jawad will meet with the team on a weekly basis to share progress updates, and the first point of contact should any issues arise.

2.0 Appendix

2.1 Deliverables Map

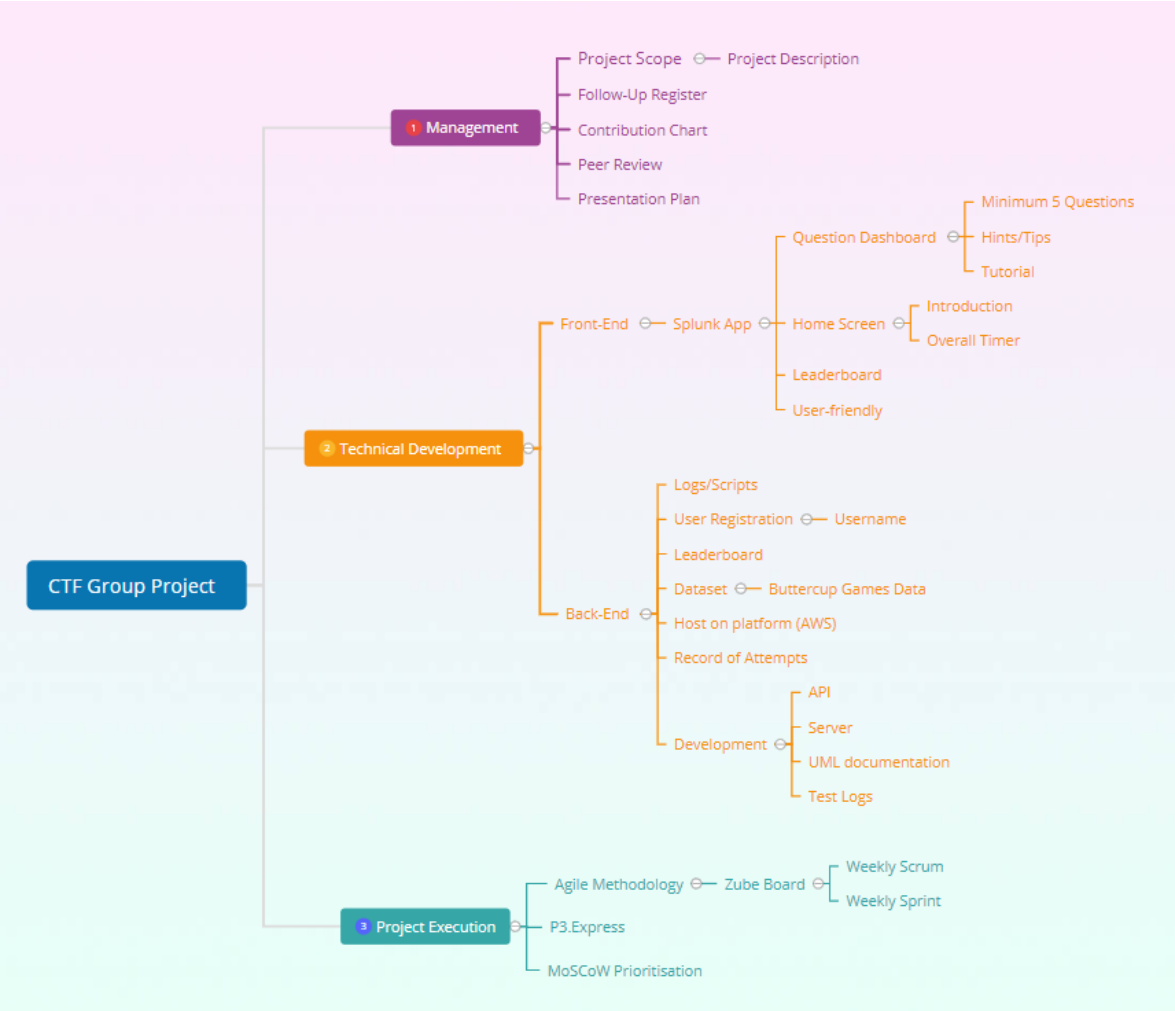

Figure 2.1

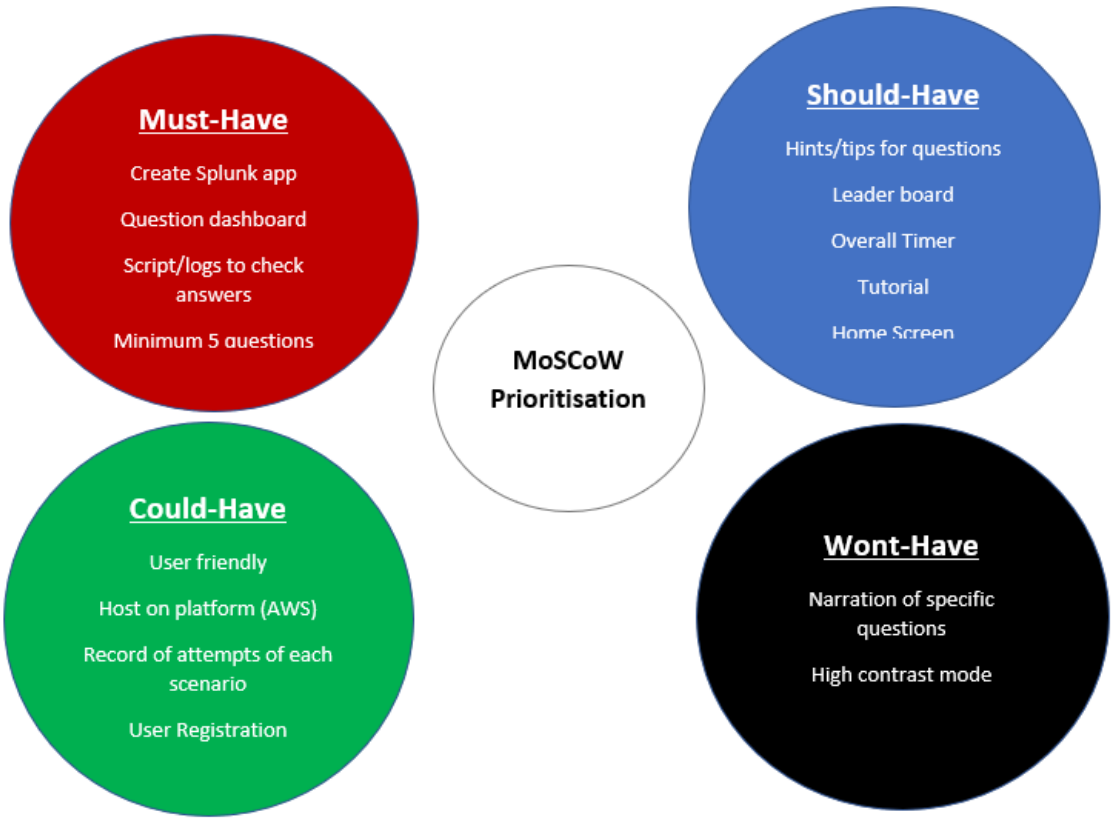
Must-Have
Create Splunk app
Question dashboard
Script/logs to check answers
Minimum 5 questions
Should-Have
Hints/tips for questions
Leader board
Overall Timer
Tutorial
Home Screen
MoSCoW Prioritisation
Could-Have
User friendly
Host on platform (AWS)
Record of attempts of each scenario
User Registration
Wont-Have
Narration of specific questions
High contrast mode

Figure 2.2

2.2 Follow-Up Register

Cause	Effect	Impact	Response	Custodian	Dates
Hosting issues	• Unable to demo product to client	**Very High**	**Prepare:** • Choose a reliable hosting service		03/02/2022
Team members intentionally not completing tasks	• Project completion is delayed • Friction between team members	**High**	**Mitigate:** • Regular team meetings • Commit to support each other	Sergio - PM	03/02/2022
Time contingencies due to unforseen circumstances	• Tasks may not be completed on time • Resources taken away from other tasks	**High**	**Mitigate:** • Clear communications between team members • Sharing responsibilities	Sergio - PM	03/02/2022
Poor communication between team members	• Tasks may not be completed to desired specification • Ideas and opinions may be missed	**High**	**Mitigate:** • Agree working routines and communications • Decide on a shared loction for the	Sergio - PM	03/02/2022
Conflict of ideas between team members	• Project could be delayed until team members come to an agreement • Team members may become unmotivated	**Medium**	• Openly discuss all ideas during team meetings • Allow members to vote on conflicting ideas	Sergio - PM	03/02/2022
Project specification is difficult to implement	• Product does not work as intended • Project cannot be completed within the specified timeframe	**Medium**	• Adjust product specification for the team skill level • Sufficient product testing • Cross-evaluate		03/02/2022
Final product does not match initial specification	• Product not suitable for intended purpose • Client unsatisfied with final product	**Medium**	• Review and follow client specification document		03/02/2022
Software issues	• Completed tasks may no longer work • Stalls progression of other tasks	**Medium**	• Update software if required • Troubleshoot software issues		03/02/2022
Final product is not user friendly	• The client may be unable to use the product as intended • Affects user engagement	**Low**	• Create detailed tutorial as a guide for new users • Informative introduction page		03/02/2022
Complexity of questions	• Product not suitable for intended purpose • Users may be unable to progress through questions	**Low**	• Consider the intended users • Ensure questions are informative		03/02/2022

Figure 2.2

2.3 Project Initiation Peer Review

Reviewer: Alan Miller **Team: 99**

Reviewee: Sergio Rodriguez Chavez **Team: 142**

Date of review: 09/02/22

1. Project description

Reviewer's comments and recommendations

Within various sections within the report, you are using the words "our", "we" and "us". This type of language should be avoided in formal documentation. A simple rewording in these sections will mean the report follows a formal format rather than an informal, conversational format. These sections are named here: Expected Cost and Duration, Stakeholder List

Purpose and Expected Benefits section is explained well, and I understand from this alone the goal of your project.

The expected cost and duration section also explains how long you expect the project to take and any expected costs, this is informative and easy to understand.

The Requirements and Quality Expectations section is laid out in a formal and easy to follow manner.

The stakeholder list I feel could be lacking some stakeholders, namely, your client, project manager etc. Other than that, good use of descriptions to specify stakeholder responsibilities.

Response and actions taken

Reviewed the sections stated above and edited to not use words such as "our", "we" and "us" to have a more formal documentation throughout the entire report. Other sections were also reworded to include more detail. Stakeholder list was edited to include a fake client since we don't have a client.

2. Deliverables map

Reviewer's comments and recommendations

My initial impressions of the design and colours used as part of the diagram allow easy distinction between each major section, those being, Management, Technical Development and Project Execution. However, I do think you may have missed a key point which in this case could be named "System Design and Analysis". You have thought of your Front-End via your "Splunk App" and what it will contain, but you have not considered the design process of this app. My recommendation would be to create a new Major Section with the intention of listing Design elements of your system. This

could contain tasks to do with System Design including UML in the form of Use Case Diagrams, Class diagrams etc. What do you think?

Other than that, well presented and you have a good start here.

Response and actions taken

Added a back-end development branch to include potential testing, documentation and the use of a server and API. Edited the mind map to be easier to read and professionally presented.

3. Follow-up register

Reviewer's comments and recommendations

This piece of documentation covers the expected risks that could be associated with this project and has appropriate responses in place for these risks.

The only thing to note is that some of the sections might require more detail to be less vague, for example, in the "Effect" section this could contain more detail about how these risks might affect:

- The client
- The reputation of the business
- The overall experience of the users using it.

When thinking of this section, it is important to ask: Why will this affect them? And in what way?

Also, in the "Impact" section, from documentation I have seen online on Follow-up Registers, this section explains what the impact will be rather than stating if it is high or low, why will this impact or not impact them as much? So, as well as stating "Very High", you could go into more detail as to why this is the case.

Other than needing more detail, this overall covers the expected risks, reads very well, and is presented professionally. Great start and really there is not much to add or correct.

Response and actions taken

Very good advice on adding some detail on the Effect and Impact sections of the follow-up register. The effect section could allow us to highlight some risks and how they might affect the client as well as the overall experience for the user and added some detail to account for this.

4. Quality of document (clarity, presentation, etc.)

Reviewer's comments and recommendations

As touched on in previous sections, I think you have done well with the presentation and clarity of your documentation. Other than the brief points touched on in the previous sections, nothing to complain about here. Well done.

Response and actions taken

Reviewed the entire Initiation Report and edited some sections to make them clearer and more detailed. The overall presentation was modified to make it clearer and well presented.