**Black Sabre Responce**

**PROJECT CHARTER**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| 01/08/2017 | 1.0 | Plan created |  |
| 14/11/2021 | 2.0 | Updated | Zac, Rory and Tarsha |
| 16/02/2022 | 2.1 | Updated | Elan Sithirasenan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## INTRODUCTION

## 1.1 PURPOSE OF PROJECT CHARTER

The purpose of this document is to provide an understanding of this project’s objectives, scope, time and budget plus the responsibilities of the team members.

Quarter to half page

The Project Charter serves as a cornerstone document that lays the foundation for the successful execution of the incident response project at RightPoint. Its primary purpose is to provide stakeholders with a comprehensive understanding of the project's objectives, scope, timeline, budget, and the roles and responsibilities of team members. By defining these critical aspects, the Project Charter facilitates effective planning, coordination, and communication throughout the project's lifecycle.

The incident response project aims to address a crucial gap in RightPoint's security infrastructure—the absence of an updated incident response plan. In light of recent cyber threats and emerging vulnerabilities, the newly appointed Chief Security Officer (CIO) recognized the need for a proactive and systematic approach to handle potential security incidents. As part of the strategy to enhance the organization's security posture, the CIO proposes the implementation of an incident response team exercise (IRTx).

## 2. PROJECT AND PRODUCT OVERVIEW

After completing an audit of the security policy at RightPoint the new Chief Security Officer (CIO) discovered that the organization lacks an updated incident response plan and believes it would be beneficial to conduct an incident response team exercise (IRTx).

Quarter to half page

RightPoint, a reputable organization in the digital services industry, has been operating with a dedicated focus on client satisfaction and innovation. The recent security policy audit conducted by the CIO revealed a significant concern—RightPoint's incident response plan is outdated and insufficient to address the evolving cybersecurity landscape. This vulnerability poses potential risks to the confidentiality, integrity, and availability of critical information and data assets.

In response to these findings, the incident response project aims to introduce a comprehensive incident response plan and conduct an IRTx to assess its effectiveness. The incident response plan will outline the necessary actions, procedures, and communication protocols required to identify, contain, eradicate, and recover from security incidents effectively. It will encompass a wide range of potential scenarios, ensuring that RightPoint's incident response capabilities are well-prepared for any eventuality.

The IRTx, a simulated exercise, will allow the incident response team members to practice their roles, collaborate, and test the incident response plan in a controlled environment. By simulating various security incidents and crisis scenarios, the exercise will enable the team to identify strengths, weaknesses, and areas for improvement in the plan and their overall response capabilities.

# 3. Justification

RightPoint’s current security posture and procedures are simplistic, and the company’s new chief security officer has previously identified that their policies and procedures are inadequate for their current needs.

Half page

The justification for the incident response project stems from several critical factors affecting RightPoint's cybersecurity posture. The existing security policies and procedures have been deemed simplistic and inadequate to meet the growing challenges posed by sophisticated cyber threats. The appointment of the new Chief Security Officer reflects the organization's commitment to addressing these shortcomings and strengthening its overall security framework.

The incident response project is a proactive measure to enhance RightPoint's security resilience and ensure the protection of sensitive data, intellectual property, and client information. By developing and implementing a robust incident response plan, RightPoint can reduce the potential impact of security incidents, minimizing business disruptions and financial losses.

Furthermore, this project aligns with industry best practices and compliance requirements, demonstrating RightPoint's dedication to maintaining the highest standards of cybersecurity and data protection. A well-prepared and efficient incident response team, coupled with an updated incident response plan, will enhance customer trust, reinforce the organization's reputation, and foster stronger relationships with clients, partners, and stakeholders.

In conclusion, the incident response project serves as a strategic initiative to bolster RightPoint's security posture, address vulnerabilities, and proactively respond to the dynamic cybersecurity landscape. By focusing on incident preparedness, the organization can mitigate risks, protect its assets, and uphold its commitment to maintaining a secure and resilient digital environment.

# 4. Scope

## 4.1 objectives

The objectives are as follows:

List in dot points

### 4.2 High-Level requirements

The high-level requirements are as follows:

List in dot points

### 4.3 Major Deliverables

**The major deliverables are as follows.**

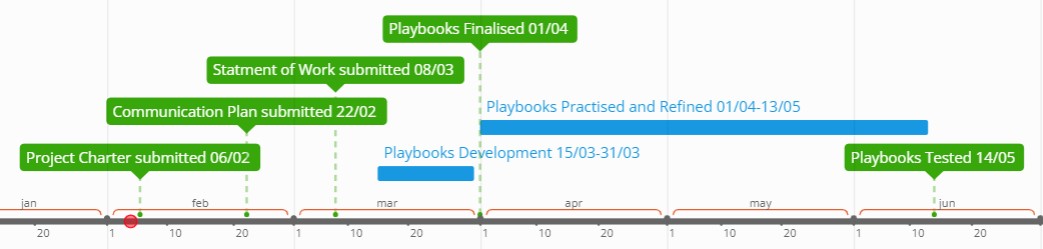
List in dot points

### 4.4 Boundaries

The IRTx will run for four hours and be monitored by the Purple Team. If any security flaws are found each member of the developing team will be bound by a non-disclosure agreement (NDA).

# 5. Duration

## 5.1 Timeline



## 5.2 Milestones

The table below lists milestones and their estimated completion dates.

|  |  |
| --- | --- |
| **Milestone** | **Estimated completion time**  **frame** |
|  |  |
|  |  |
|  |  |

# 6. Budget Estimate

## 6.1 Funding source

The Red, Blue and Purple playbooks are being developed as part of a student project for certificate IV in cyber security at TAFE Coomera.

## 6.2 Estimate

This section provides a summary of estimated spending to meet objectives and deadlines described in this project charter. This summery of spending is preliminary and reflects costs for the entire investment lifecycle. It is intended to present probable funding requirements and assist in budgeting acquisition.

Complete table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Budget Item** | **Month1** | **Month 2** | **Month 3** | **Month 4** | **Total** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 7. ASSUMPTIONS, CONSTRAINTS AND RISKS

* 1. **Assumptions:**

List in dot points

**7.2 Constraints:**

* **Time constraints:**
* **Resource constraints:**
* **Technical constraints:**

**7.3 Risks:**

List in dot points

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Name** | **Project Role** | **Responsibilities** |
| ~~Teacher~~ | ~~Project sponsor~~ | ~~Function as the liaison between projects team, and the client RightPoint. This member aims to provide guidance and resource allocation for this project, in addition to any other project that they are overseeing.~~ |
| ~~Student 1~~ | ~~Project manager~~ | ~~Oversee the daily function and performance of the project. They are to ensure that each stage of the project is completed to the standard and timings required to ensure that the project is completed as intended and within the scope the client and project sponsor has requested. The project manager is responsible for liaising with the project sponsor as required during the conduct of this project.~~ |
| ~~Student 2~~ | ~~Blue team lead~~ | ~~The blue team technical lead is responsible for overseeing the creation, testing and auditing of the blue team playbooks that will be generated within this project. This member is to work with the blue team technical writer to generate these documents. As the team leader, this member is to ensure that these are done within the times outlined in the project schedule. The team leader is to liaise with the project manager throughout the conduct of this project.~~ |
| ~~Student 3~~ | ~~Red team lead~~ | ~~The red team technical lead is responsible for overseeing the creation, testing and auditing of the red team playbooks that will be generated within this project. This member is to work with the red team technical writer to generate these documents. As the team leader, this member is to ensure that these are done within the times outlined in the project schedule. The team leader is to liaise with the project manager throughout the conduct of this project.~~ |
| ~~Student 4~~ | ~~Blue team~~ | ~~The blue team technical write is responsible for helping create, test and audit the blue team playbooks. This member is to work with the blue team technical lead to ensure these documents are completed to the standard outlined in the projects scope, and within the timeframe dictated by the project schedule.~~ |
| ~~Student 5~~ | ~~Red team~~ | ~~The red team technical write is responsible for helping create, test and audit the red team playbooks. This member is to work with the red team technical lead to ensure these documents are completed to the standard outlined in the projects scope, and within the timeframe dictated by the project schedule.~~ |