**Black Sabre Response**

**PROJECT CHARTER**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Modification** | **Modifier** |
| 01/08/2017 | 1.0 | Plan created |  |
| 24/06/2023 | 2.0 | Updated | Brayden, Dylan, Muzamill and Syed |
| 31/06/2023 | 2.1 | Updated | Elan Sithirasenan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# INTRODUCTION

## PURPOSE OF PROJECT CHARTER

The Project Charter serves as a cornerstone document that lays the foundation for the successful execution of the incident response project at Black Sabre Response. 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 Black Sabre Response'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

Black Sabre Response, 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policy audit conducted by the CIO revealed a significant concern— Black Sabre Response's incident response plan is outdated and insufficient to address the evolving cybersecurity landscape.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 Black Sabre Response'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

The justification for the incident response project stems from several critical factors affecting Black Sabre Response'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 Black Sabre Response's security resilience and ensure the protection of sensitive data, intellectual property, and client information. By developing and implementing a robust incident response plan, Black Sabre Response 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 Black Sabre Response'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 Black Sabre Response'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:

* Develop and implement an updated and comprehensive incident response plan to strengthen Black Sabre Response's security posture.
* Conduct an incident response team exercise (IRTx) to test the effectiveness of the newly developed incident response plan.
* Enhance the incident response capabilities of Black Sabre Response's cybersecurity team.
* Identify and address potential weaknesses in the organization's incident response procedures.
* Foster collaboration and coordination among incident response team members.
* Improve incident detection, containment, eradication, and recovery processes.
* Minimize the impact of security incidents on business operations and client services.

## 4.2 High-Level requirements

The high-level requirements are as follows:

* The incident response plan should cover a wide range of potential security incidents, including malware infections, data breaches, insider threats, and denial-of-service attacks.
* The incident response team exercise should simulate realistic scenarios to challenge the team's response capabilities effectively.
* Incident response team members must have access to up-to-date information and resources during the exercise.
* The incident response plan should outline clear roles, responsibilities, and communication channels for team members.
* The exercise should include cross-functional collaboration involving IT, security, legal, and executive teams.
* The incident response plan should comply with relevant industry standards and regulations.

## 4.3 Major Deliverables

## The major deliverables are as follows.

* Updated incident response plan document detailing procedures and guidelines for handling various security incidents.
* Incident response team exercise scenario design and preparation documentation.
* Incident response team exercise report outlining findings, lessons learned, and recommended improvements for the incident response plan.
* Communication and training materials for incident response team members to ensure a common understanding of the plan's implementation.

## 4.4 Boundaries

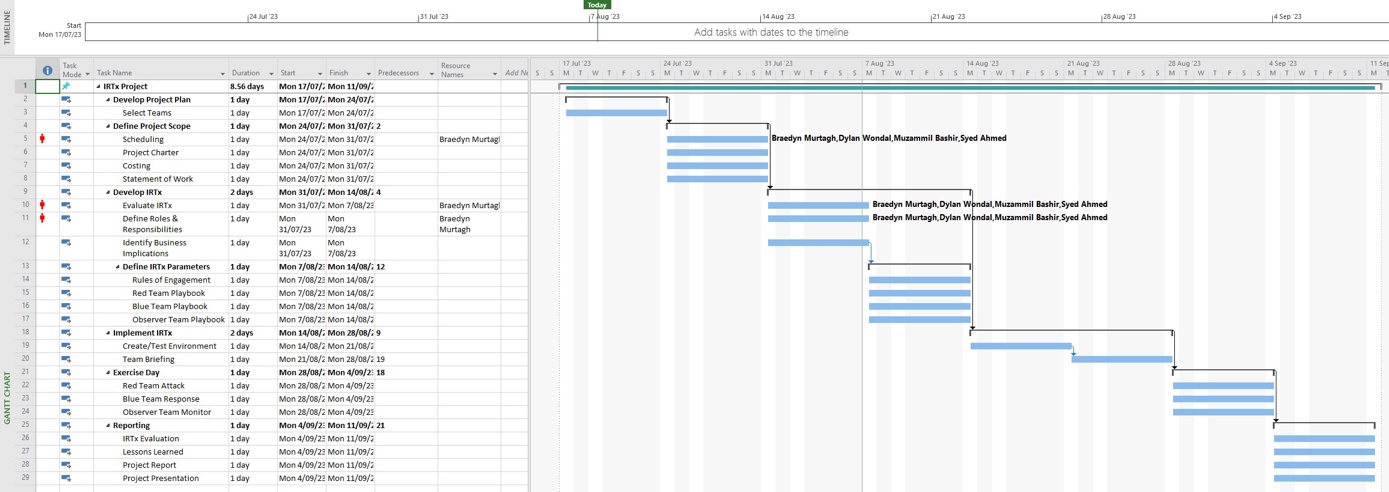
The incident response team exercise (IRTx) will be limited to a duration of four hours to minimize operational disruptions while providing sufficient time for thorough testing.

The IRTx will be monitored by the Purple Team, which will play the role of an independent evaluator and provide objective feedback on the team's performance.

As part of the development team's commitment to security and confidentiality, each member will be bound by a non-disclosure agreement (NDA) regarding the details and outcomes of the IRTx. This ensures that sensitive information related to the exercise is not disclosed to external parties.

# 5. Duration

## 5.1 Timeline



## 5.2 Milestones

The table below lists milestones and their estimated completion dates.

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

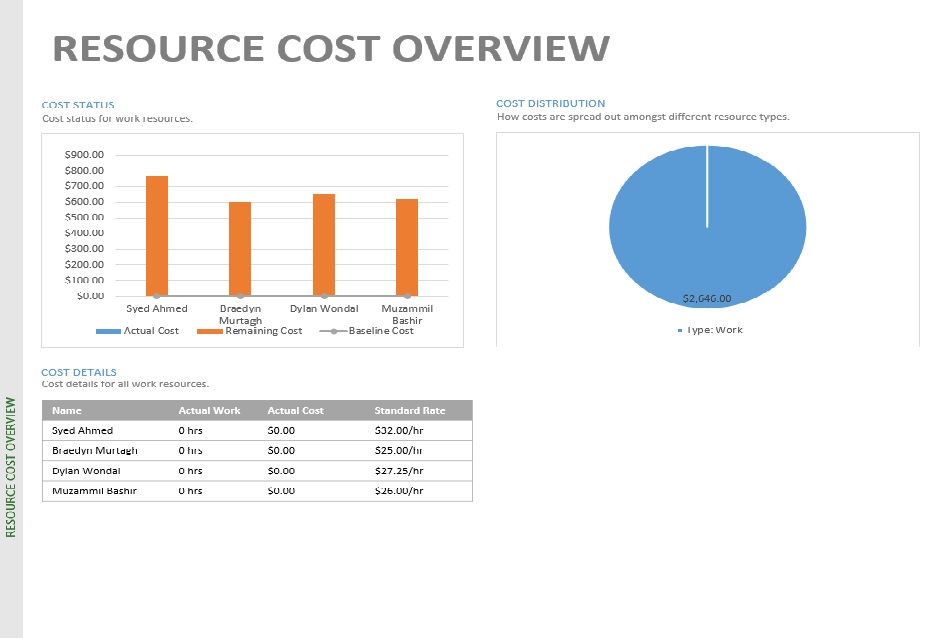
# 6. Budget Estimate

## 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.



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

# 7. ASSUMPTIONS, CONSTRAINTS AND RISKS

* 1. **Assumptions:**
* All members know their roles and how to perform them
* All handbooks have been created and verified
* When performing exercise, Red team IP won’t be blocked to completely render them useless.
* A clear objective has been set

**7.2 Constraints:**

Time Constraints:

Only 2-3 Hours allowed to test machines for vulnerabilities

2.5 Months for full IRTx

**Resource constraints:**

Power and CPU resources allocated to NUTANIX machines

**Technical constraints:**

Limited to team members knowledge

**7.3 Risks:**

* Taking down network while testing
* Exposing potentially vulnerable machines to public network

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Name** | **Project Role** | **Responsibilities** |
| Elankayer Sithirasenan | Project Sponsor | Function as the liaison between projects team, and the client Black Sabre Response. This member aims to provide guidance and resource allocation for this project, in addition to any other project that they are overseeing. |
| Syed Ahmed | 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. |
| Muzammil Bashir | Communication Manager | Responsible for managing communication between Sponsor and Team and ensuring all information is conveyed to the required members. |
| Dylan Wondal | 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. |
| Braedyn Murtagh | 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. |