5/12/2023

Wells College

Jorge trujillo 18574

Assessment Task 2

Case Study

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Jorge Trujillo | ID | 18574 |

Table of Contents

[Case scenario 1](#_Toc134993750)

[Heaven Systems internal IT Service Agreement 3](#_Toc134993751)

[Task 1: Prepare team support and monitor 5](#_Toc134993753)

[Task 2: Review client support 7](#_Toc134993754)

[Task 3: Submit both report to your trainer for approval 7](#_Toc134993755)

**Assessment 2 – Case Study**

***Instructions:***

This is a group of 2 student assessment.

You need to analyse a case scenarios and complete tasks mentioned after scenario.

You need to demonstrate your develop ICT solution ability to identify the solution, determine client support and manage the team in development an awareness of cyber security in workplace.

***Duration:***

Trainer will set the duration of the assessment.

***Evidence required:***

|  |  |  |
| --- | --- | --- |
| *Tasks* | *Evidence* | *Submission* |
| Supporting Plan Report | A complete report on team supporting and monitoring team performance, and client support for the case study. | In printing |

# Case scenario

Established in 1999 with offices located throughout the western Sydney, Heaven Systems is a world-class, full-service provider of residential, commercial, and logistics-based transportation solutions for businesses and individuals. Many of the world’s largest, most respected corporations rely on the company’s unwavering commitment to innovation, quality, and customer service to move their employees, offices, and industrial facilities—domestically and internationally—anywhere in the world. Heaven Systems was experiencing an increase of phishing emails that were reaching employee inboxes and introducing the risk of a data breach. As phishing attacks increased, productivity slowed down while end users waited for IT to investigate the suspicious emails. “Phishing emails were getting more specific and sophisticated, and we worried that an employee might open one and cause serious damage,” said David Potter, IT Director at Heaven Systems. While there are multiple layers of security to filter email as it enters Heaven Systems’ network, it’s still possible for some targeted phishing emails to slip through and get into employee in-boxes. For this reason, IT must rely on end users to determine whether an email is safe to open. But it’s not always easy to tell. “For instance,” said Potter, “one area of the company was getting phishing emails that looked legitimate. They appeared to come from a customer, but the attachment was malicious.” Refer to employee background statistic show below:



To help employees identify phishing emails, IT holds annual training to show them what red flags to look for. Then, IT sends mock phishing attacks to test them. If a user clicks on a couple simulated phishing emails, they’re required to take the security training again. Human nature being what it is, some users were ignoring legitimate email because they didn’t want to make a mistake that would require them to take the training again. Others decided to play it safe and send every questionable email they received to IT to see if it was OK. While IT recognized the obvious threats, even they had to question some of the attachments. “You can imagine the amount of time we spent investigating emails,” said Potter. “It took about an hour per email to copy the attachment to a USB drive and then spin up a machine to test the file off network,” he explained. “That’s valuable time that IT could spend doing other things.”

You are work as an IT project manager assigned by Potter to handle this problem in the company. The company decide to use the system to detect a Spear-Phishing. To accelerate suspicious email analysis and response, Heaven Systems implemented MailMon, an automated phishing incident reporting and response service that empowers end users to report suspicious emails directly from the inbox. MailMon runs on Microsoft Exchange 2013 or newer and Office365; it is deployed to end users as an Outlook plug-in, including Outlook App for Android and iOS devices.

You and your friend are 10 years’ experience staff in the company. After you evaluate the MailMon, it generates a report in the complex form, many of the staff including a current IT department are not familiar with the system. Potter approved on new project team recruitment, and HR organised 3 **new graduated** IT staffs joining your team. Potter would like your team to gain more awareness on this cyber security incidence

<https://tepjet4.github.io/heavenby18574/Heaven%20Systems%20Cybersecurty%20by%2018574-chart.html>

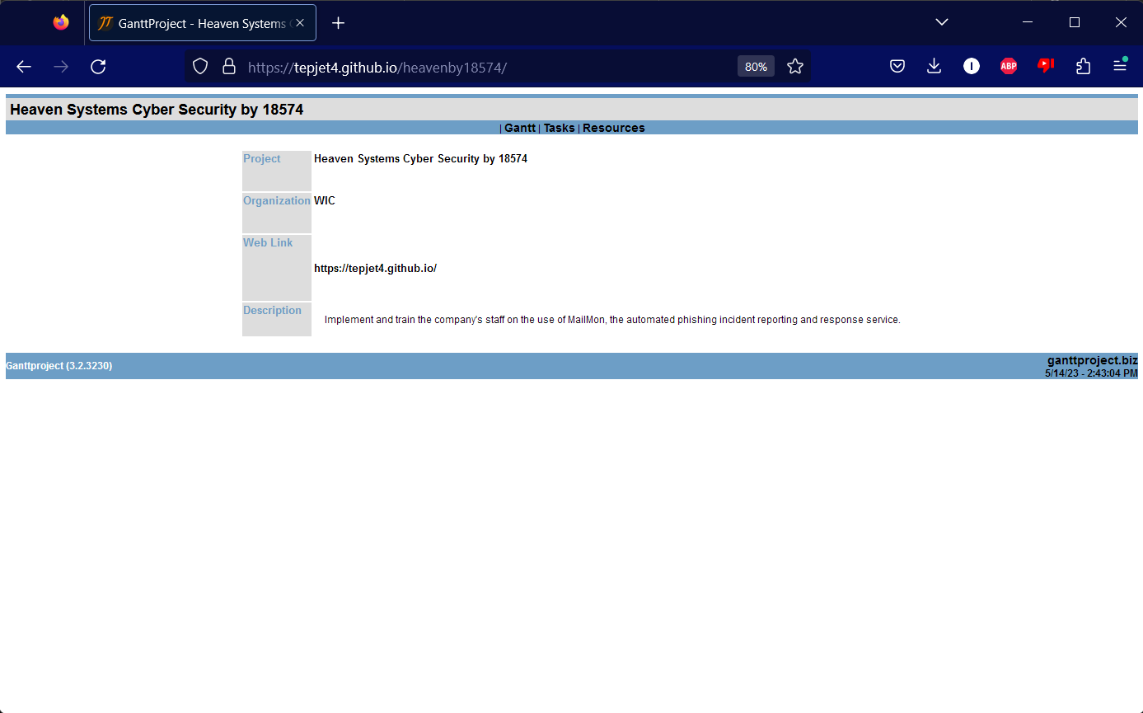




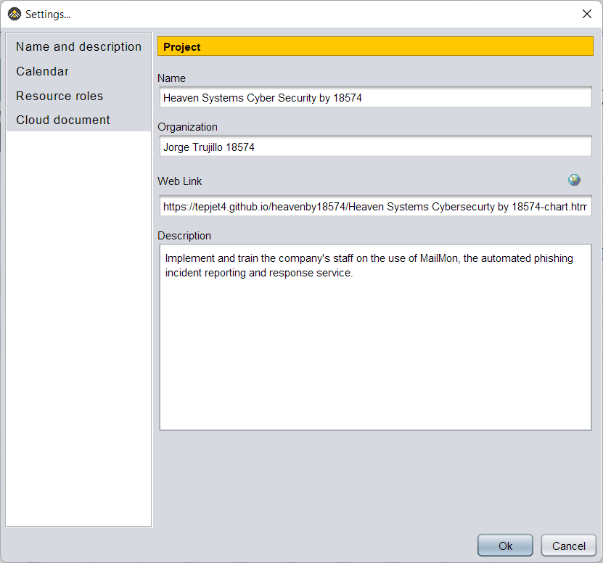
Figure: MailMon Monitoring Sample

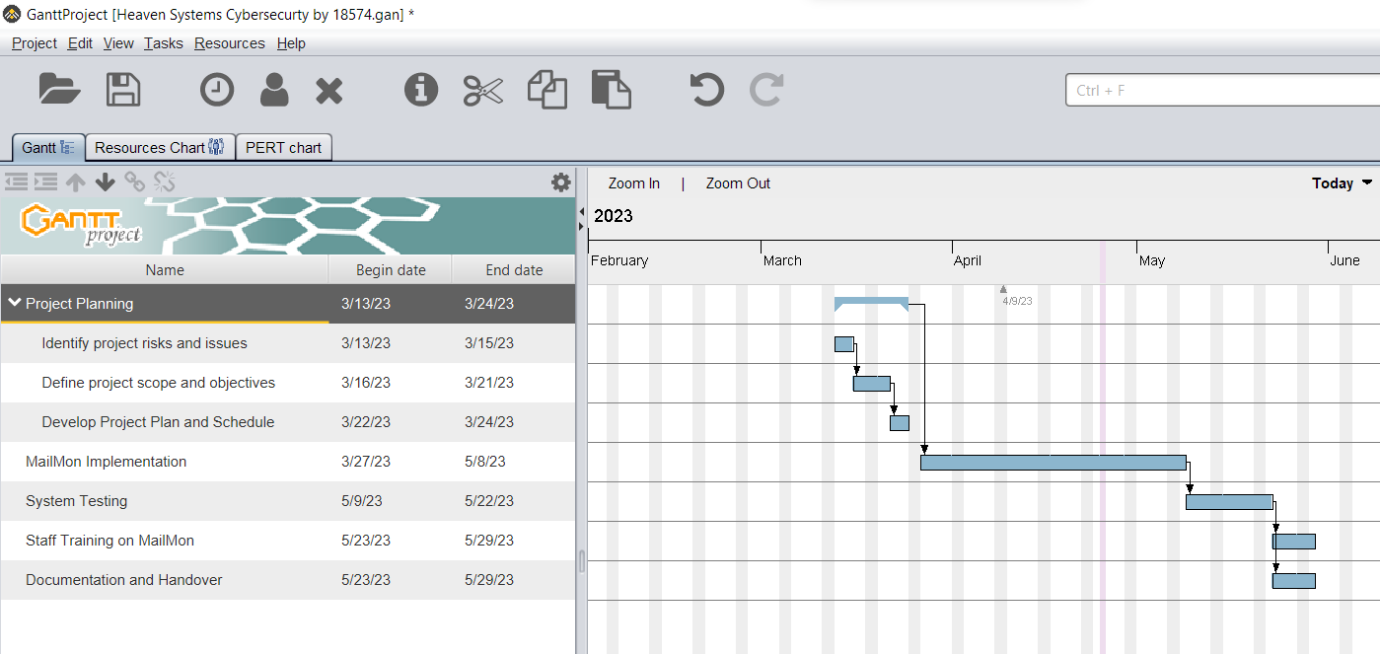
# Heaven Systems internal IT Service Agreement

|  |  |  |
| --- | --- | --- |
| **Severity Level** | **Description** | **Target Response** |
| 1 (Outage) | Entire Company Server down | Immediately |
| 2 (Critical) | Entire Department Server down | Within 15 Minutes |
| 3 (Urgent) | Staff computer down | Within 1 hours |
| 4 (Important) | Staff computer not work properly or potential for interrupt their routine work | Within 3 hours |
| 5 (General) | Upgrade software  Training request | Within 48 hours |

Sample link: <https://tepjet4.github.io/heavenby18574/Heaven%20Systems%20Cybersecurty%20by%2018574-chart.html>

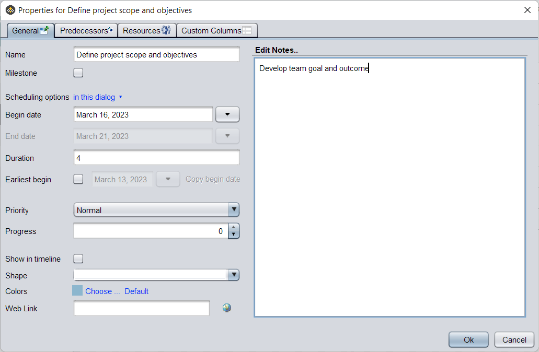
Learn how to using GanttProject: <https://www.youtube.com/watch?v=5FukJpd_VNs&t=1242s>





# 

# Task 1: Prepare team support and monitor

1. Develop team goal and outcome

Team Goal: To successfully implement MailMon at Heaven Systems and improve the organization's cybersecurity posture by reducing the risk of data breaches caused by targeted phishing emails.

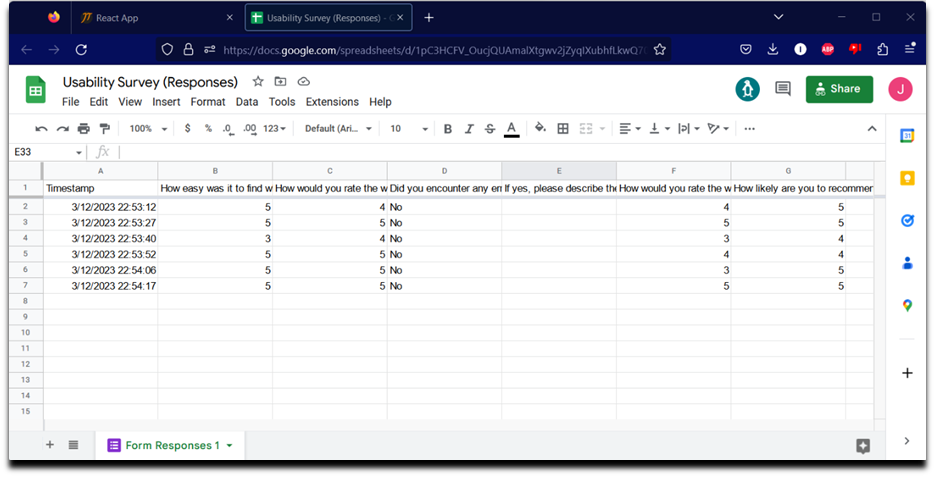
Team Outcome: By the end of the project, the team will have successfully deployed MailMon, trained end users on how to report suspicious emails, and reduced the number of suspicious emails forwarded to the IT department. The team will have improved the efficiency of IT incident response and increased end user awareness of phishing attacks. The project will be delivered on time and within budget.

1. Develop team goal and outcome

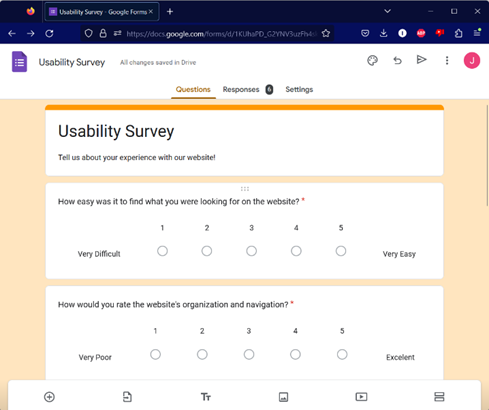
* Identify Stakeholders: The first step in creating a communication plan is to identify all stakeholders who need to be informed about the project progress, including senior management, project sponsors, project team members, and other key stakeholders.
* Communication Objectives: Once you've identified stakeholders, establish clear objectives for each communication. These objectives should be measurable and achievable and should focus on keeping all stakeholders informed about project progress, risks, and issues.
* Communication Methods: Determine the best communication methods for each stakeholder group. For example, regular team meetings can be used to update project team members, while weekly or monthly reports can be sent to senior management.
* Frequency: Determine how often each stakeholder group needs to receive updates. This may vary depending on the level of involvement and interest in the project.
* Message Content: Ensure that the message content is clear, concise, and relevant to each stakeholder group. Use plain language and avoid technical jargon.
* Feedback Mechanisms: Establish feedback mechanisms for each stakeholder group to provide feedback and input. This can be done through regular meetings or surveys.
* Escalation Plan: Establish an escalation plan in case of any issues or delays that need to be addressed. This plan should outline who to contact, when to contact them, and how to escalate issues.
* Schedule: Create a schedule for all communication activities, including regular team meetings, progress reports, and other updates. Make sure that all stakeholders are aware of the schedule and receive updates as scheduled.
* Review and Update: Regularly review and update the communication plan to ensure that it remains effective and relevant to the project.

1. Develop team KPI and action plan to address team training needs
   * Tools and Method for the training
   * Cost and budgeting
   * Schedule
   * Feedback collection plan
   * Evaluation process after the training

Here’s the feedback collection

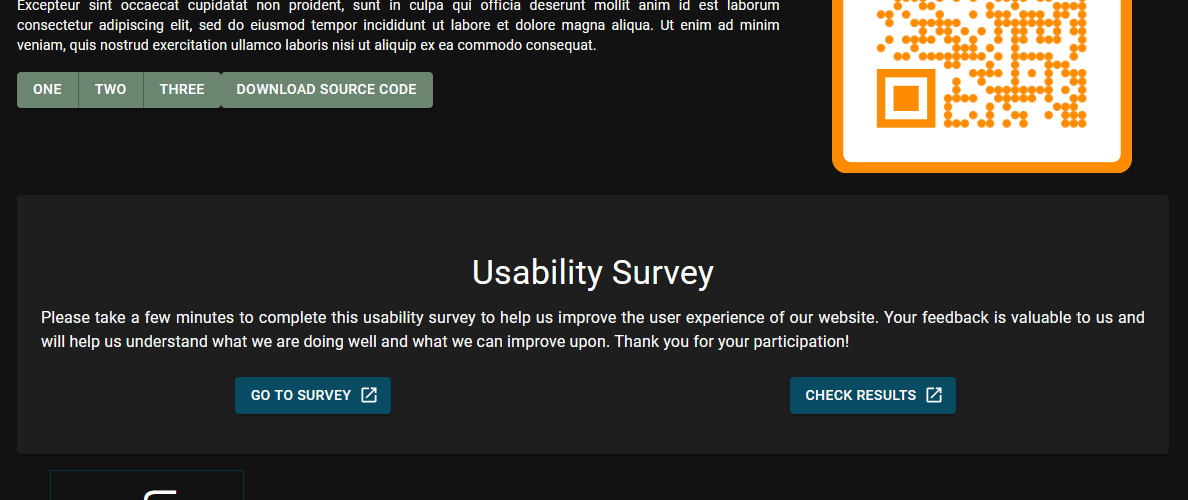


Survey:



Above site could be access by my web support site:

<https://tepjet4.github.io/#Survey>

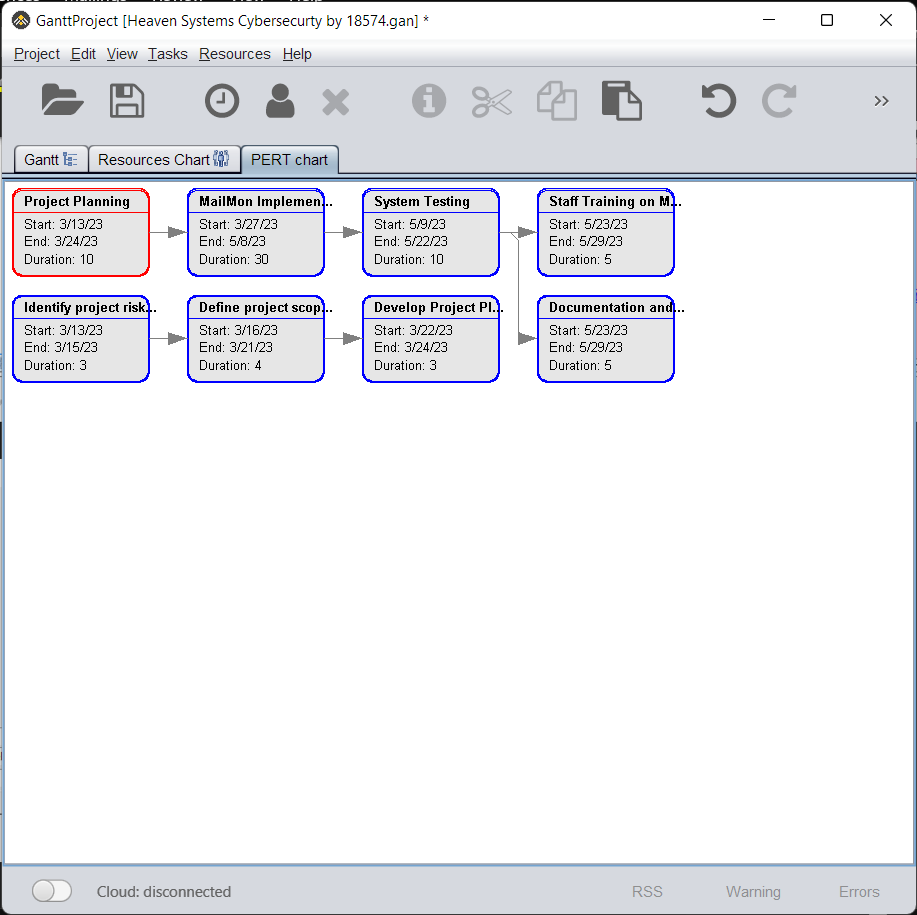


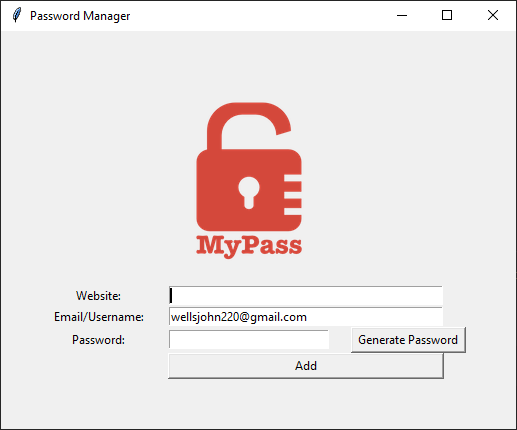
# Task 2: Review client support

1. Identify and documenting client needs
   * Gap between current organizational support and their needs
2. Develop a client support plan and evaluation plan against company SLAs
   * Area of the support
   * Resources needs
   * Cost and budgeting
   * Schedule
3. Develop a review process on the selected solution
   * Tools and Method
   * Schedule
   * Responsibility

# Task 3: Submit both report to your trainer for approval

1. Get feedback from your trainer
2. Amend the document if required





My Subject Web Site: <https://tepjet4.github.io/> already showing linked above project.

