Siteweb: https://pedromelloq.github.io/PedroMelloAssessments.github.io/

Google Sheets: https://docs.google.com/spreadsheets/d/179bIbuwNDTd72VSdBz0bs4IWagSH43SzDAIWUs81EYM/edit#gid=0

**Assessment 1 – Presentation**

## 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.

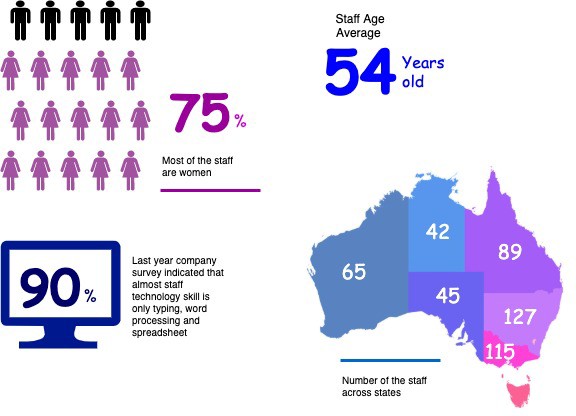
***Evidence required:***

|  |  |  |
| --- | --- | --- |
| *Tasks* | *Evidence* | *Submission* |
| Identifying issue and | A complete issue report and selected solution, including a presentation. | Presentation in front of the class and the trainer. Also 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.

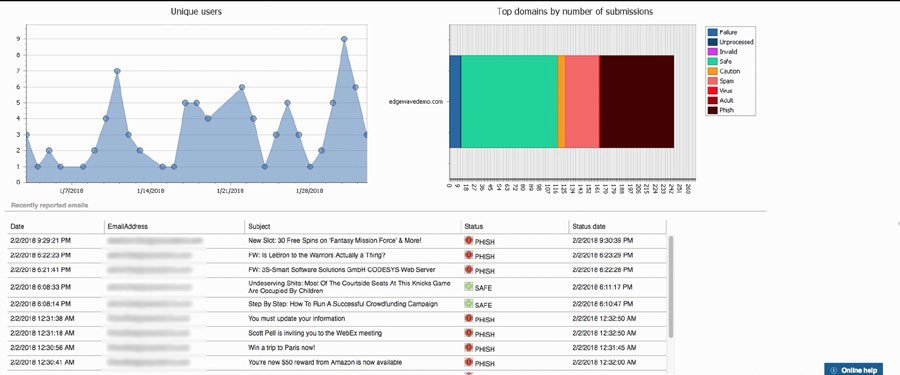


Figure: MailMon Monitoring Sample

# 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 |

**Task 1: Scope issue**

Now, in the mid of November, you are required to prepare the report for the management team on company security awareness. The report should indicate:

1. The company current issue

Heaven Systems could solve the Phishing Mails problem with mastery, increasing the security with new programs which identify the hide virus inside these emails, the constant training of all employees to be more conscious about virus and the hiring of 3 new employees to work directly with the security of our company and our employees.

With the same effort as Heaven Systems had to improve the security, these criminals are also improving their methods of how to harm companies. The new method found was entering to our system directly from our employee accounts, which we identify not safe and warned us to get a new method to protect our system’s users.

When inside our system, these criminals can steal information about our costumer, use of this access to implant malware and other bad intentions. The solution must be found as soon as possible.

1. Brief for possible solution to identified issue. Each solution must be assessed on
   * commercial potential
   * suitability for the target audience or purpose
   * feasibility of implementing solution

We are looking ways of how to get harder to find out our employee accounts access, which have too many information about our costumer and also how to minimize the prejudice in the case that it happens again.

Could be something around stronger passwords, more authentication steps, limited access to some information and an access registration in our system.

These implementations will increase our commercial potential when our company and costumer will trust even more the security found in our work, will require some training and update to our employees and will be a fast solution for our company.

# Task 2: Selected solutions

1. Conduct a brainstorm on identified issue

In the brainstorm the best ideas identified were:

* Multi-Factor Authentication
* Regular Security Training
* User Access Controls
* Behavioral Analytics
* Privileged Access Management (PAM)
* Continuous Monitoring
* Regular Security Audits
* Endpoint Security
* Data Encryption
* Incident Response
* Plan Vendor Security
* Employee Offboarding
* Security Culture Zero
* Trust Architecture
* Continuous Education
* Adaptation

1. Compare an idea solution for identified issue

Comparing the ideas: **Continuous Education**, **Multi-Factor Authentication**, **User Access Controls** and **Behavioral Analytics** we can conclude that:

* Continuous Education: As important as constant training of our employees is, this does not give us the necessary tools to block possible hacker intrusions into our accounts.
* Multi-Factor Authentication: It would be extremely useful to make access to our system go through multiple levels of security.
* User Access Controls: Depending on the employee's position, some information and access may be deactivated, thus reducing the chance of being accessed by hacked accounts.
* Behavioral Analytic: By analyzing records of activity in our systems, we can identify anomalies and suspicious movements within our system, making it easier to identify hackers who have access to us.

1. Selected the solution and communicate to stakeholder (Your trainer)

After analyzing our options, the next implementation to our security system will be:

1. Multi-Factor Authentication and Strong Password Requirement in all of our employee access.
2. User Access Controls will be implemented, reducing access to users who don’t really need it.
3. Behavioral Analytic will be done constantly by our cybersecurity team, to reduce damage caused by hackers.
   1. Prepare some (15) presentation slides to present the following items to your trainer (All group members have to present equally)
      * Identified issue
      * Brainstorming evidence
      * Selected solution

https://docs.google.com/presentation/d/1xMRmw2p9DtnUewe8jD2eeKMRMU4vBUPj2uiYAvHMgk0/edit?usp=sharing

1. Record a feedback from your trainer and finalised the solution