|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Arthur Leonard LESMANA | ID | 18780 |

All my assessments and works could be found in this link: <https://arthleo.github.io/ict2/>

**Assessment 1 – Presentation**

***Instructions:***

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 |

Heaven Systems, established in 1999, is a prominent provider of transportation solutions for residential, commercial, and logistics needs. They serve both businesses and individuals worldwide, emphasizing innovation, quality, and customer service. The company faced a rising number of phishing emails in recent times, causing productivity issues and data breach concerns. Despite multiple security layers, some sophisticated phishing emails still infiltrated employee inboxes. IT Director David Potter noted that these emails often appeared legitimate, making it challenging to discern their malicious nature. Refer to employee background statistic shown below:



To enhance employee awareness and response to phishing emails, the company conducts annual training and tests with mock phishing attacks. Employees who click on these simulated phishing emails must retake the security training, which some were avoiding to prevent mistakes. Some individuals opted to forward all suspicious emails to IT, creating a time-consuming investigation process for the IT team.

In response to this issue, the company, under your management as the IT project manager, implemented MailMon, an automated phishing incident reporting and response service, to detect Spear-Phishing. This service allows end users to report suspicious emails directly from their inbox, thereby accelerating the analysis and response to potentially harmful emails. MailMon is compatible with Microsoft Exchange 2013 and newer, as well as Office365, and it is deployed as an Outlook plug-in, including the Outlook App for Android and iOS devices.

To address the challenges of a complex reporting system and to improve overall cyber security awareness, your team, which now includes three new IT staff members, will work to ensure that employees, including the existing IT department, become familiar with MailMon. This initiative aims to streamline the response to cyber threats and optimize the use of resources within the company.



Figure: Email Analytics

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:

* The company current issue:

Artheral Company faces several security awareness challenges:

* Phishing Awareness: We've observed a rise in phishing attacks, and some employees have fallen victim to these scams. Despite annual training, some continue to click on suspicious links or open malicious attachments.
* Resistance to Training: Some employees avoid security training to prevent the inconvenience of retaking it if they make mistakes during mock phishing exercises.
* Over-Reporting: Some employees send all questionable emails to IT for verification, causing inefficiencies and inundating our IT department.
* Brief for possible solution to identified issue. Each solution must be assessed on

To address these issues, we have identified the following solutions, each assessed for its commercial potential, suitability for the target audience or purpose, and feasibility of implementation:

Automated Email Analysis Tool (MailMon):

* Commercial Potential: Moderate. Such tools can be marketed as part of cybersecurity services.
* Suitability: Ideal for empowering employees to report suspicious emails.
* Feasibility: Implementation involves further training and awareness campaigns about using MailMon efficiently.

Dedicated Security Awareness Team:

* Commercial Potential: Limited. Primarily an internal resource.
* Suitability: Ideal for continuous education and awareness campaigns.
* Feasibility: Establishing a dedicated team requires human resource allocation.

Security Awareness Workshops:

* Commercial Potential: Limited. Targeted at internal audiences.
* Suitability: Effective for interactive learning and addressing specific issues.
* Feasibility: Requires scheduling and resource allocation for workshops.

Task 2: Selected solutions with Presentation

[ACSC - What is Phishing on Vimeo](https://vimeo.com/497805556)

* Conduct a brainstorm on identified issue
* Compare an idea solution for identified issue
* Selected the solution and communicate to stakeholder (Your trainer)

a. **Prepare some (10-15) presentation slides** to present the following items to your trainer (All group members have to present equally)

* Identified issue
* Brainstorming evidence
* Selected solution
* Record feedback from your trainer and finalised the solution

Presentation

My Presentation could be seen from this slideshow link:

<https://docs.google.com/presentation/d/1c5OYC7YK9J51SL_75KesFVo0Ab998GHryFYT4-dyVyI/edit?usp=sharing>

**REFERENCE:**

Visit my site: <https://arthleo.github.io/ict2/>

