CLOUD SECURITY ENGINEER ASSESSMENT

Task 1 – Coding Exercise

Write the "wordcloud" program in python.

A word cloud (tag cloud) is a representation of text data, typically used to depict keyword metadata (tags) on websites, or to visualize free form text.

Write a program that will create a word cloud from the content of 5 or more files. You can use any text you like. You are not required to visualize the tags; you need to create a text file, which will contain the following information:

1. The words, ordered by frequency.
2. How many times the word appears.
3. Font size. The font size is calculated by the following simple rule:

    a. The most frequent word should be –> Huge
    b. > 60% (of max frequent word) –> Big
    c. > 30% (of max frequent word) –> Normal
    d. Less than 30% –> Small

4. The words that appear once should not be present.

Additional requirements:

- The program should read all text files from the specific folder.
- Read text files in different threads / tasks (in parallel).
- One thread / task should read one file.

Output Example:

The example of the output file:

a	10	Huge
was	8	Big
and	7	Big
catholic	6	Big
the	6	Big
nothing	5	Normal
pain	4	Normal
her	3	Normal
mother	3	Normal
had	3	Normal
because	3	Normal
of	2	Small
father	2	Small
or	2	Small
i	2	Small
been	2	Small
in	2	Small
known	2	Small

The example of UI

Task 2 – Security Ingestion – Handbook

Scenario:

Your organization needs to monitor the activity on the employees using Windows workstations, this will allow the security team to create rules to detect malware installed in the workstations.

For that, the security team needs to send to the IT team a handbook with a step-by step guide on what configuration they need to apply on the Windows to send the information to a SIEM (Security Information and Event Management) to centralize all the information on it.

Exercise:

Create a step-by-step guide on how to send Windows Logs to a SIEM solution via TCP Protocol.

Notes:

1. You can consider any SIEM solution.
2. You can choose additional setup tools if required.
3. Feel free to use pictures if you think it will be easier to understand.
4. The handbook should be in English.

Task 3 – Security Automation - Playbook

Scenario:

Your organization has recently been experiencing a high volume of phishing attacks targeted at the finance department. These attacks are delivered via email and contain malicious links or attachments that, when clicked, install malware on the victim's machine. The security team concluded that it needs to create automation to deal with all the emails sent to the organization.

Exercise:

Create a mock playbook (using a drawing tool) that can detect and respond to suspicious emails.

Notes:

1. The playbook runs for all emails (suspicious or not)
2. You have access to the sender email address and the content of the email (external URLs and attachments)