Test Challenge

Congratulations.

You have made it to the test challenge stage.   This means you are a finalist for the position, and we are seriously considering you.

This is a three-part test challenge to confirm your ability to work as part of modern OpenSource development teams, and your knowledge of security topics that we currently use.

You are required to have a GitHub account with two-factor authentication (2fa) enabled.

Each candidate will be assigned a GitHub repository for their test.

Please do your best and submit what you have by the end of the allotted time period as we will be evaluating even if you provide an incomplete solution.

Scoring

Part 1	Presentation/Quality	5
	Ability to follow instructions	5
	Correctness	10
Part 2	Presentation/Quality	5
	Ability to follow instructions	5
	Correctness	10
Part 3	Presentation/Quality	5
	Ability to follow instructions	5
	Correctness	10
Total		60

Part 1.

You have been assigned a GitHub code repository for submission of your response.

These instructions are purposely left vague as part of the challenge.

Your task is to perform the following steps:

1. Clone the repo
2. Create a branch called part_1
3. Author your response as valid markdown, with any files stored in what looks like the logical place to store them. Consider that other team members or even the public may need to reuse or update artifacts you create like diagrams. Choose an appropriate format that can be edited without barriers (like operating system type or high software expense) to doing so.
4. Once complete, do a pull request (PR) against the repo that was assigned to you. Attach the Apache license file you were given to the PR.

Here is the question:

A client has approached you with their proposed application architecture and needs your advice to ensure their system will be well protected from security related harm.

Their legacy system is hosted within the Government Data Centre in a Protected Zone, which is only accessible from within the Gov network (via VPN) or through a firewall in the DMZ. This system is hosted a server in a subnet with 10 other application and database servers.

Their legacy system has worked well for the past 10 years, but is getting difficult to maintain, and re-writing in place is not an option.

The client is standing up web facing components of the application on AWS (Canada Central) but will need to connect to the legacy system for certain queries related to business financial information. The AWS hosted system also leverages Lambda functions for complex GIS jobs (anonymized).

The web facing components are used by 3 separate groups:

- Citizens (accessing services)
- Businesses (supplying equipment)
- Internal Staff (administering program)

Your task:

1) Draw a logical diagram of the deployment.
    a. Label the diagram with data flows and network boundaries.

2) Make security observations based on what was described to you.
3) Make recommendations to address security concerns.
4) Write a 300 word (max) executive summary of your findings, highlighting any AWS security tools used and why.

Part 2.

Use the same repo as part 1, examine the contents of the “Question 2 artifacts.zip” file located in the code-challenge directory.

These instructions are purposely left vague as part of the challenge.

Your task is to perform the following steps:

1. Clone the repo
2. Create a branch called part_2
3. Author your response as valid markdown, with any files stored in what looks like the logical place to store them.
4. Once complete, do a pull request (PR) against the repo that was assigned to you. Attach the Apache license file you were given to the PR.

Here is the question:

A business client has an application that has been experiencing some performance issues lately.

You are asked to review their main web server log file to see if there are any security concerns.

Find up to 3 log entries of concern, and if any exist, rank them in order of severity. Document how any security related events were discovered (include queries/tools used).

If any items of concern are found, provide a recommended remediation.

Part 3.

Use the same repo as part 1.

These instructions are purposely left vague as part of the challenge.

Your task is to perform the following steps:

1. Clone the repo

2. Create a branch called part_3
3. Author your response as valid markdown, with any files stored in what looks like the logical place to store them.
4. Once complete, do a pull request (PR) against the repo that was assigned to you. Attach the Apache license file you were given to the PR.

Here is the question:

All in one file for your response, please provide short one sentence answers to the following questions:

1. Please provide your definition of the DevOps Mindset.
2. What is the primary rationale for a CI/CD pipeline?
3. Explain the security benefit from OpenSource development with respect to keys, secrets, and credentials.
4. What is the main security benefit over time of using a product like the Government of Canada's Secure Environment Accelerator?