Technical Challenge (Controls Deployment)

Overview:

This technical challenge is designed to evaluate a candidate's proficiency in cybersecurity, container security and orchestration, IaaS, and CI/CD pipeline management. The challenge is divided into three parts: Cybersecurity Scenario, Container Security Implementation, and CI/CD Pipeline Setup. In the scenarios below use either AWS or Azure, whichever you're most comfortable with. Feel free to make any assumptions about the environment, just document your assumptions where applicable.

Part 1: Cybersecurity Scenario (30 points)

Objective: Assess the candidate's understanding of security operations, cyber defense, threat intelligence, and incident response.

Scenario: You are a security analyst at a financial company. Recently, your organization experienced a security breach. The attack vector was an unpatched vulnerability in a web application that allowed attackers to gain unauthorized access to the network.

Tasks:

1. **Threat Intelligence Report (10 points):**
   - List the types of attack that could be use.
   - Explain how a vulnerability exploited can provide access to the network.
   - Suggest preventive measures to avoid similar incidents in the future.
2. **Incident Response Plan (10 points):**
   - Outline an incident response plan to address the breach.
   - Include steps for containment, eradication, and recovery.
3. **Network Security Measures (10 points):**
   - Recommend network security measures to enhance the organization's defense posture.
   - Include at least three different security technologies or practices (e.g., IDS/IPS, firewalls, network segmentation).

For Part 1, assume you have access to the cloud provider security tools/services available like Azure Defender or AWS Security hub.

Part 2: Container Security Implementation (30 points)

Objective: Evaluate the candidate's experience with container security, orchestration tools, and IaaS.

Scenario: Your team is deploying a microservices-based application using Docker and Kubernetes. Security is a top priority, and you need to ensure that the container environment is secure from potential threats.

Tasks:

1. **Docker Security Best Practices (10 points):**
   - List and explain five Docker security best practices.
   - Implement one of these practices in a Dockerfile and provide the code.
2. **Kubernetes Security Configuration (10 points):**
   - Describe three Kubernetes security features.
   - Write a Kubernetes YAML configuration that includes securityContext settings for a pod.
3. **IaaS Security Measures (10 points):**
   - Explain the concept of Infrastructure as a Service (IaaS) and its security implications.

Part 3: CI/CD Pipeline Setup (40 points)

Objective: Assess the candidate's familiarity with configuration management tools and CI/CD pipeline integration.

Scenario: Your organization uses Jenkins or GitHub to manage their CI/CD pipelines. You are tasked with setting up a new pipeline for a cloud-native application.

Tasks:

1. **Configuration Management with Ansible/Chef/Puppet/Terraform (15 points):**
   - Choose one configuration management tool (Ansible, Chef, or Puppet, terraform).
   - Write a script/playbook to automate the deployment of a web server on a virtual machine.
2. **CI/CD Pipeline Configuration (25 points):**
   - Create a Jenkins pipeline configuration (Jenkinsfile) that includes stages for building, testing, and deploying a sample application to Azure.
   - Ensure that the pipeline includes security scanning as a step.

   OR
3. **GitHub Actions for AWS (25 points):**
   - Write a GitHub Actions workflow that builds and deploys a serverless application to AWS Lambda.
   - Include steps for linting, testing, and deployment.

For Part 3, you only need to choose ONE pipeline in either Jenkins or Github, you don't need to do both.

Submission Guidelines:

- Candidates must submit their solutions as a GitHub repository.
- Include a README.md file with instructions for any area you see fit.
- Ensure all the documentations in Part 1 and 2 are included in the repo as well, markdown or other formats like power point, word are also acceptable.
- Ensure that all scripts, configurations, and code are well-documented and follow best practices.

Evaluation Criteria:

- **Accuracy and Completeness (40 points):** Solutions should be correct, complete, and address all aspects of the tasks.
- **Security Awareness (20 points):** Demonstrated understanding of cybersecurity principles and best practices.
- **Technical Proficiency (20 points):** Proficiency in using tools and technologies relevant to the challenge.
- **Documentation and Code Quality (20 points):** Code should be well-documented, clean, and follow industry standards.

It is OK to skip Part 1, Part 2 or Part 3, however, provide an explanation why it was skipped.

