TASK 3 Security & Compliance (ISO, GDPR, SOC 2)

Overview

Integrating operations into a continuous development process introduces various security challenges in guaranteeing a threat-free system. Addressing these compromises requires strategies consistent with internationally recognized frameworks, such as ISO 27001, GDPR, and SOC 2.

Security Risks Identification and Mitigation Strategies

1. Insecure CI/CD Pipeline & Secrets Management

Risk: Exposure of sensitive information (API keys, tokens, database credentials, etc.) due to insecure storage of environment variables or incorrect configurations of the CI/CD pipeline.

Mitigation Strategies:

- **Secret Management:** Manage secrets securely using AWS Secrets Manager or AWS Systems Manager Parameter Store.
- **Encryption:** Ensure secrets stored in AWS services are encrypted in transit and at rest using AWS Key Management Service (KMS).
- **Isolation of Environments:** Limit exposure by using separate AWS accounts or Virtual Private Clouds (VPCs) for production, staging, and development environments.
- **Regular Auditing:** Use AWS CloudTrail and AWS Config to continuously monitor and audit CI/CD configurations.

Compliance Alignment:

- **ISO 27001:** Aligns with requirements for secure access controls and encryption policies.
- **SOC 2:** Addresses the security and confidentiality of information.
- **GDPR:** Mandates a high level of protection for personal data.

2. Inadequate Access Control & Privilege Escalation

Risk: Overly permissive roles or policies can allow unauthorized access or privilege escalation, increasing the attack surface.

Mitigation Strategies:

- **Role-Based Access Control (RBAC):** Implement AWS IAM to enforce the principle of least privilege.
- **Multi-Factor Authentication (MFA):** Enforce MFA for users accessing AWS environments.

- **Regular Reviews:** Regularly review IAM roles and permissions to ensure they meet evolving security requirements.

Compliance Alignment:

- **ISO 27001:** Requires strict access management and regular review of permissions.
- **SOC 2:** Mandates controls to protect operational environments from unauthorized access.
- **GDPR:** Least-privilege access helps mitigate the risk of unauthorized personal data exposure.

3. Third-Party & Supply Chain Vulnerabilities

Risk: Using untrusted third-party libraries, container images, or external plugins can introduce vulnerabilities.

Mitigation Strategies:

- **Vulnerability Scanning:** Regularly scan dependencies and container images using tools like AWS Inspector or Amazon ECR.
- **Trusted Registries and Code Signing:** Use trusted registries for container images and implement code signing.
- **Update Policies:** Maintain an effective patch and update management process.

Best Practices in AWS Cloud Deployments

- **Data Encryption:** Encrypt data in transit using TLS/SSL and at rest using AWS KMS.
- **Logging & Monitoring:** Implement effective monitoring using AWS CloudWatch, X-Ray, and CloudTrail.
- **Patch Management:** Regularly apply patches using services like AWS Systems Manager.
- **Network Segmentation:** Use Amazon VPC, security groups, and NACLs to isolate critical resources.