Incident Response Plan for AWS Data Breach

---

1. Detection Method

To detect security incidents within AWS environments, we could use:

- **Automated System Alerts:** Configure alerts from AWS services like Amazon GuardDuty and AWS CloudTrail to monitor unusual activities, unauthorized access attempts, and abnormal network traffic patterns.
- **User Reports:** Encourage reports from AWS users and staff who notice unusual behavior, such as unexpected account lockouts or sluggish system performance.
- **Audit Log Analysis:** Regularly review AWS CloudTrail logs to detect unusual login patterns, changes in user permissions, and data transfers.

Example of Cyber Attack: Malware, often deployed through phishing campaigns, could be injected into AWS systems to manipulate configurations, steal data, or introduce vulnerabilities.

---

2. Containment Strategy

For containment, we recommend isolating and securing compromised resources to prevent the breach from spreading. Steps include:

- **Network Isolation:** Remove affected S3 buckets or EC2 instances from the network.
- **User Account Restriction:** Temporarily disable compromised IAM user accounts and reset access keys.
- **Firewall Rules:** Enforce emergency firewall rules to block unauthorized outbound/inbound traffic from affected systems.

---

3. Eradication and Recovery Steps

- **Malware Removal:** Use Amazon Inspector to identify and remove malicious files.
- **Reconfigure Security:** Resolve any misconfigurations in S3 bucket permissions and close any vulnerabilities.
- **Data Restoration:** Restore any impacted data from clean backups and test data integrity.
- **Monitoring:** Gradually reconnect resources while monitoring with Amazon CloudWatch for signs of reinfection.

Comprehensive Security Policy

1. Key Security Guidelines

- **Access Control:** Implement the principle of least privilege using AWS IAM roles and policies to limit user access.
- **Regular Audits:** Schedule periodic audits of all AWS services to detect configuration drift and maintain compliance.
- **Multi-Factor Authentication (MFA):** Enforce MFA for all users to strengthen access control, especially for high-privilege accounts.

2. Incident Response Plan Summary

In the event of a breach, this response plan will prioritize rapid containment, thorough eradication of threats, and structured recovery, using AWS's logging, monitoring, and access control tools.

3. CIA Triad Compliance

- **Confidentiality:** Encryption policies ensure all sensitive data in S3 is encrypted using AWS KMS.
- **Integrity:** Automated alerts (e.g., CloudWatch) detect unauthorized changes to data and configurations.
- **Availability:** Regular backups and disaster recovery protocols maintain service availability even during incidents.

Encryption Techniques

- **SHA1 input: french fries output: eb2b0b0c3ca7c9cfea008783cd0fd2170edb6378**

- **AES Encryption:French Fries Password: Its so Good output:53616c7465645f5f6175106992e57b62b71bd65d63635f41f524f59574d533f0**

Legal and Ethical Compliance

- **Laws/Regulations:** Compliance with **GDPR** for EU data subjects and **CCPA** for California residents ensures legal handling of personal data.
- **Ethical Considerations:** We prioritize transparency and user notification in case of data breaches. This plan upholds ethical principles by protecting user data and informing affected individuals when appropriate.