Security Operations Plan (SOP) for Client Cloud Infrastructure

- ***This document outlines the security operations plan (SOP) for the client's cloud infrastructure hosted on Amazon Web Services (AWS). This plan encompasses security controls, monitoring solutions, incident response procedures, and compliance documentation.***

Security Controls

Identity and Access Management (IAM) Procedures:

- ***Root Account Security:***

Strong Credentials Required:

- Generate a complex and unique password for the root account, exceeding at least 16 characters and using a combination of upper/lowercase letters, numbers, and symbols.
- Never share passwords with anyone

- ***Disable Direct Login:***
  - Disable all methods of direct login to the root account, including console access, programmatic access, and API calls.

- ***IAM User Accounts:***
  - Utilize IAM user accounts with appropriate permissions for all administrative tasks, eliminating the need for root access in day-to-day operations.

Team Member Access Management:

- ***Least Privilege Principle:***
  - Implement the principle of least privilege for all team members, granting them only the minimum permissions necessary to perform their specific roles and responsibilities.
  - Regularly review and adjust user permissions based on changes in roles or responsibilities.

- ***Individual IAM Users:***
  - Create individual IAM users for each team member
  - Avoiding shared accounts that pose security risks.
  - Assign permissions to each user based on their specific needs, utilizing IAM policies and roles for efficient management.

- ***Multi-Factor Authentication (MFA):***
  - Enforce mandatory MFA for all user accounts, including a combination of something you know (password) and something you have (security token, app authenticator).
  - Educate team members on the importance of MFA and enforce its use for all access attempts.

❖ Server Hardening and Data Protection:

This SOP outlines the procedures for hardening a Windows Server Domain Controller (DC) and protecting associated data within a private subnet. It emphasizes CIS compliance, secure access, encryption, and comprehensive logging.

- **Windows Server Domain Controller**
  - The Domain Controller will displayed through a secure VPN

- Will restrict inbound traffic to authorized ports and protocols necessary for DC functionality
- Will utilize firewall rules to further restrict access and prevent unauthorized connection
- Implement CIS recommendations such as:
    - Strong passwords
    - Secure group policies
    - Regular Security Updates
- Focus on secure configurations for:
    - User accounts and privileges
    - Local security policies
    - Firewalls and network security
    - Logging and auditing

Linux Data Server Deployment with PII and PCI Data

- Is a server designed to store and manage data installed with Install a supported Linux distribution certified for PCI DSS compliance. https://aws.amazon.com/compliance/services-in-scope/PCI/
- CIS benchmarks are applied for system hardening
- Implement full disk encryption at rest using industry-standard algorithms.
- Securely manage encryption keys using a dedicated key management solution.
- Encrypt data in transit using strong protocols like SSH with public-key authentication and TLS/SSL for network traffic.
-

- Security Information and Event Management (SIEM):
    - Log Aggregation: Implement a SIEM solution to centralize and analyze event logs from key assets like EC2 instances.

- Threat Detection and Response:
    - Attack TTP (Threat, Tactics, and Procedures): Simulate an attack scenario leveraging a new Python library, triggering an event captured by the SIEM solution.

- AWS Lambda Function: Develop an AWS Lambda function triggered by specific SIEM events, initiating pre-defined response actions like alerting administrators or modifying security controls.
- Cloud Monitoring: Utilize VPC Flow Logs and additional tools to monitor network traffic for suspicious activity.
- Security Log Monitoring: Continuously monitor security logs for anomalies, particularly failed SSH attempts on instances.
-

Incident Response Plan

- Detection and Analysis: Leverage monitoring tools and SIEM alerts to identify potential security incidents.
- Containment: Isolate affected systems and restrict access to minimize further damage.
- Eradication: Identify and remove the root cause of the incident.
- Recovery: Restore affected systems and data to a known good state.
- Reporting: Document the incident, analyze root cause, and implement corrective actions to prevent future occurrences.

Compliance Documentation

- This plan adheres to the General Data Protection Regulation (GDPR) framework. Documentation will showcase compliance through measures like:
- Data encryption at rest and in transit.
- Access control mechanisms within IAM.
- Logging and monitoring practices for data access and modification.
- Incident response procedures aligned with GDPR guidelines.