Server Hardening and Data Protection

Developed by Shield Wall IT for Valhalla Systems

Table of Contents

---

1. Purpose

The purpose of this SOP is to ensure the security and protection of data on Valhalla Systems' servers by implementing CIS-compliant configurations, encrypting data at rest and in transit, and deploying security logging mechanisms.

---

2. Scope

This SOP applies to all Windows Server Domain Controllers (DC) hosted on a private subnet of a VPC and Linux server instances containing Personally Identifiable Information (PII) and Payment Card Information (PCI) data within Valhalla Systems.

---

3. Responsibilities

- **IT Security Team:** Responsible for configuring, maintaining, and auditing the server settings and ensuring compliance with this SOP.
- **System Administrators:** Implement the hardening measures and monitor the server activities.

- **Employees and Contractors:** Must follow the data protection policies and report any security incidents.

---

4. CIS-Compliant Windows Server DC

Network Configuration

1. **Private Subnet:** Host the Windows Server DC on a private subnet within the VPC.
2. **VPN Access:** Ensure the server is accessible only via VPN tunneling to maintain secure access.

Data Encryption

1. **Encryption at Rest:**
   - Use BitLocker to encrypt the data on the Windows Server.
   - Regularly update encryption keys and manage them using AWS Key Management Service (KMS).
2. **Encryption in Transit:**
   - Use TLS/SSL to encrypt data transmitted over the network.
   - Implement HTTPS for any web-based interfaces.

Sysmon Deployment

1. **Sysmon Installation:**
   - Download and install Sysmon on the Windows Server DC.
   - Configure Sysmon to generate security-relevant system logs.
2. **Configuration:**
   - Use a Sysmon configuration file that includes rules for monitoring and logging key activities.
   - Regularly review and update the Sysmon configuration to cover new security requirements.

---

5. CIS-Compliant Data Server

Linux Server Configuration

1. **Compliance:**
   - Follow CIS benchmarks for hardening the Linux server.
   - Regularly audit the server to ensure compliance with CIS guidelines.

Data Encryption

1. **Encryption at Rest:**

    - Use LUKS to encrypt the disks on the Linux server.
    - Manage encryption keys using a secure key management solution.
2. **Encryption in Transit:**
    - Use OpenSSL or GnuTLS to encrypt data transmitted over the network.
    - Implement SSH for secure remote access to the server.

---

6. Monitoring and Logging

1. **Log Management:**
    - Use AWS CloudWatch to collect and analyze logs generated by Sysmon on Windows Server and syslog on Linux servers.
    - Implement log retention policies and ensure logs are stored securely.
2. **Audit Trails:**
    - Enable and review audit trails for both Windows and Linux servers.
    - Regularly conduct security audits and take corrective actions based on audit findings.

---

7. Review and Revision

This SOP will be reviewed annually or as needed based on changes in security best practices or organizational requirements. All revisions will be documented in the revision history section below.

Revision History

Date	Version	Description	Author
5/28/2024	1.0	Initial Version	Gilbert Collado

Approval: I have read and understand the terms and conditions of this Server Hardening and Data Protection SOP.

Employee Name (Print): ______________________________

Employee Signature: ______________________________

Date: _________________________