# DISA STIG-Aligned System Hardening

Security Engineering • Compliance Awareness • Defensive Configuration

| DISA STIG Concepts | Linux Hardening | Ansible | SSH Security |
|---|---|---|---|

## Overview

This case study summarizes a Linux system hardening project using DISA STIG-aligned concepts. The public version highlights the security categories and business value while removing exact implementation details that should stay private.

## Business Challenge

Unhardened cloud servers can expose unnecessary services, weak authentication settings, insecure remote access, and logging gaps. Businesses need stronger configurations before systems are placed into production.

## Example Solution

Security controls were organized into high, medium, and low priority categories. The work emphasized SSH hardening, removal of unnecessary services, password policy strengthening, session timeout settings, audit readiness, and secure baseline documentation.

## Technologies / Methods Demonstrated

- DISA STIG Concepts
- Linux Hardening
- Ansible
- SSH Security
- Audit Logging
- Password Policy
- Service Reduction

## Business Outcomes

- Improved defensive posture for Linux cloud systems.
- Reduced attack surface by focusing on unnecessary services and remote access controls.
- Created a repeatable security baseline approach suitable for future deployments.

## What This Shows a Client

- Shows familiarity with security control frameworks.
- Shows practical system hardening knowledge.
- Shows troubleshooting ability across automation and Linux environments.

## Details intentionally not published

- Exact STIG playbook logic.

- Screenshots containing tokens, addresses, or internal names.
- Step-by-step hardening procedure.
- Full list of implementation commands.

This document is designed to give website visitors confidence in EPIC TECH LLC capability without publishing full implementation playbooks or reusable client deliverables.