Infrastructure Hardening Cheatsheet

Network Security

- Implement defense-in-depth strategy with segmented networks
- Deploy next-gen firewalls with application awareness
- Use NAC to control device access (except for the CEO's ancient iPad)
- Enable TLS 1.2+ and disable outdated protcols [sic]

Endpoint Protection

- Deploy EDR solutions with central management
- Enforce application whitelisting where possible
- Implement disk encryption on all devices
- Patch systems regularly or face the wrath of ransomware gods

Identity Management

- Implement SSO with MFA for all access points
- Use privileged access management for administrative accounts
- Enforce strong password policies that users will immediately write down
- Review access rights quarterly - remove the guy who left 3 years ago

Server Hardening

- Remove unnecessary services and applications
- Apply CIS benchmarks (or at least pretend to)
- Implement file integrity monitoring
- Configure proper logging that no one will ever read

Cloud Security

- Use security groups and NACLs to control traffic flow
- Enable cloud-native monitoring and alerting
- Implement least privilege for service accounts
- Check your S3 buckets before they check the headlines

Physical Security

- Secure server rooms with proper access controls
- Monitor environmental conditions (servers don't like swimming)
- Implement visitor management systems
- Secure your dumpsters - one man's trash is another man's treasure trove

Data Protection

- Classify data according to sensitivity
- Implement DLP solutions for exfiltration prevention
- Encrypt data at rest and in tranist [sic]
- Maintain backups using the 3-2-1 rule (3 copies, 2 types, 1 offsite)