CMMC

CONFIGURATION MANAGEMENT

Security Starts with Knowing What Changed

Configuration Management keeps your systems consistent, documented, and secure. It means tracking every change, software, settings, or devices, so nothing slips through unnoticed. In short, it's how you stay in control of your IT environment and prevent small mistakes from becoming costly problems.

Proof of Practice

Examples

- **Configuration Management Policy**
  Outlines how configuration changes are requested, approved, and documented; defines authorized personnel; and includes procedures for maintaining secure system baselines.
- **Endpoint Management Policies & Compliance Screenshots**
  Shows enforced device and software compliance settings, patch policies, and restrictions preventing unauthorized installations or configuration changes.
- **Change Log or Tracker**
  Records system or software modifications with date, description, responsible person, and approval status to provide traceable evidence of configuration control.

The Business Impact

Uncontrolled changes create risk. Solid configuration management keeps your systems trustworthy, your documentation audit-ready, and your customers confident that you run a disciplined, secure operation. Without it, unauthorized software, misconfigurations, or forgotten updates can open the door to breaches, downtime, and costly rework.

Available Resources

- **DoD Security Technical Implementation Guides (STIGs)**
  https://www.cyber.mil/stigs/downloads
- **NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems**
  lhttps://csrc.nist.gov/pubs/sp/800/128/upd1/final
- **Ansible: Open-source Automation**
  https://docs.ansible.com/
- **Microsoft Intune: Endpoint Management Platform**
  https://www.microsoft.com/en-us/security/business/microsoft-intune
- **ninjaOne: Endpoint Management**
  https://www.ninjaone.com/government/federal/

Quick Wins

1. Publish a CM Policy that defines what's allowed (and what's not)
2. Review all installed software and system features; remove anything unnecessary.
3. Apply OS security baselines (STIG/CIS)
4. Block users from installing software
5. Implement a change log to track what changed, when, and by whom.

CyberNEX TECHNOLOGY

www.CyberNEX.io