Configuration Management
System Hardening

PCI Compliance & Sustainability

Payment Card Assessments, LLC

Build Clean / Keep Clean

2023

Table of Contents

Who Should Use This Guide

This guide is for any organization looking to mature their configuration management controls and implement automation opportunities.

- Network Engineering
- Server Administrators
- System Administrators
- Configuration Managers
- PCI ISAs
- PCI QSAs
- PCIPs

Disclaimer: (because we need to have one)

The intent of this guide is to help organizations understand how configuration m

This guide does not guarantee that you will receive a report on compliance from your QSA.

This guide does not absolve any merchant from their contractual and legal obligations with the PCI SSC, card brands, and their acquirer(s).

No part of this guide includes appliances or desktops (end user devices)

No part of this guide may be copied or published by any entity without permission from Payment Card Assessments, LLC.

Welcome

You've got this!

It's never too late to get your house in order and that means maturing your **"Key"** controls. To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an organizations overall security strategy.

Let's begin with Configuration Management, specifically how to Build Clean / Keep Clean.

As hard as an organization tries, there will always be known weaknesses that affect their operating systems, databases, and enterprise applications.

BAU activities enable an organization to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments.

So let's get started!

Here's to your success,

Peggy & Lisa

Configuration Management Controls

SYSTEM HARDENING IS A REQUIREMENT OF SECURITY FRAMEWORKS SUCH AS PCI-DSS AND YOUR REPORT ON COMPLIANCE OR SAQ DEPENDS ON IT.

Why?

Every system is hardened using a set of disciplines and techniques which improve the security of a server.

Unfortunately, just as soon as you implement a "Clean" server into Production, some known weakness will popup and just like that your server is no longer as secure as you thought.

Fortunately there are known ways to configure these systems to fix security vulnerabilities. Building the process into BAU activities is the most effective and efficient way to ensure the security of your servers.

This guide covers the following:

- Roles & Responsbilities
- Build Clean
- Configuration Policy
- Configuration Standards
- Configuration Scanning Policy
- System Hardening
- Keep Clean
- Configuration Scanning
- Scan Results
- Configuration Drift
- Drift Remediation
- Benefits of Build Clean/Keep Clean
- How to Develop and Implement a Build Clean/Keep Clean Process

Roles & Responsibilities

The process of building out, deploying, and maintaining system configuration may involve several teams depending on the organizations structure.

Most organizations will have some or all of the following teams:

- Network
- Engineering
- GRC
- Configuration Management
- Scanning
- Application / System
- Compliance
- Vulnerability Management

Key Roles and Responsibilities

- Network | Engineering
  - Creating the build packages based on each OS
  - Deploying new servers into Production
  - Assessing and deploying OS patches
  - Identifying the cause of any OS failure

- GRC
  - Assessing the organizations security controls
  - Reviewing industry-accepted system hardening standards and amend based on your organizations specific needs and each servers role

- Configuration Management | Scanning
  - Assessing the in-scope inventory for accuracy prior to scanning
  - Conducting scans on all in-scope systems
  - Assessing and updating scan policies to ensure accuracy
  - Communicating and reporting any configuration drift and ensuring that all failures in security controls are detected and responded to in a timely manner

- System Administrators | Application Owners
  - Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring
  - Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change

- Compliance
  - Monitoring security controls to ensure they are operating effectively and as intended
  - Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
  - Identifying and addressing any security issues that arose during the failure of the security control
  - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively

Your CIO, CISO, CFO and other members of senior leadership will need to be kept informed of any issues, challenges, and escalations during BAU activities.

Cybersecurity is a shared responsibility, and it boils down to this: Cybersecurity, the more systems we secure, the more secure we all are.
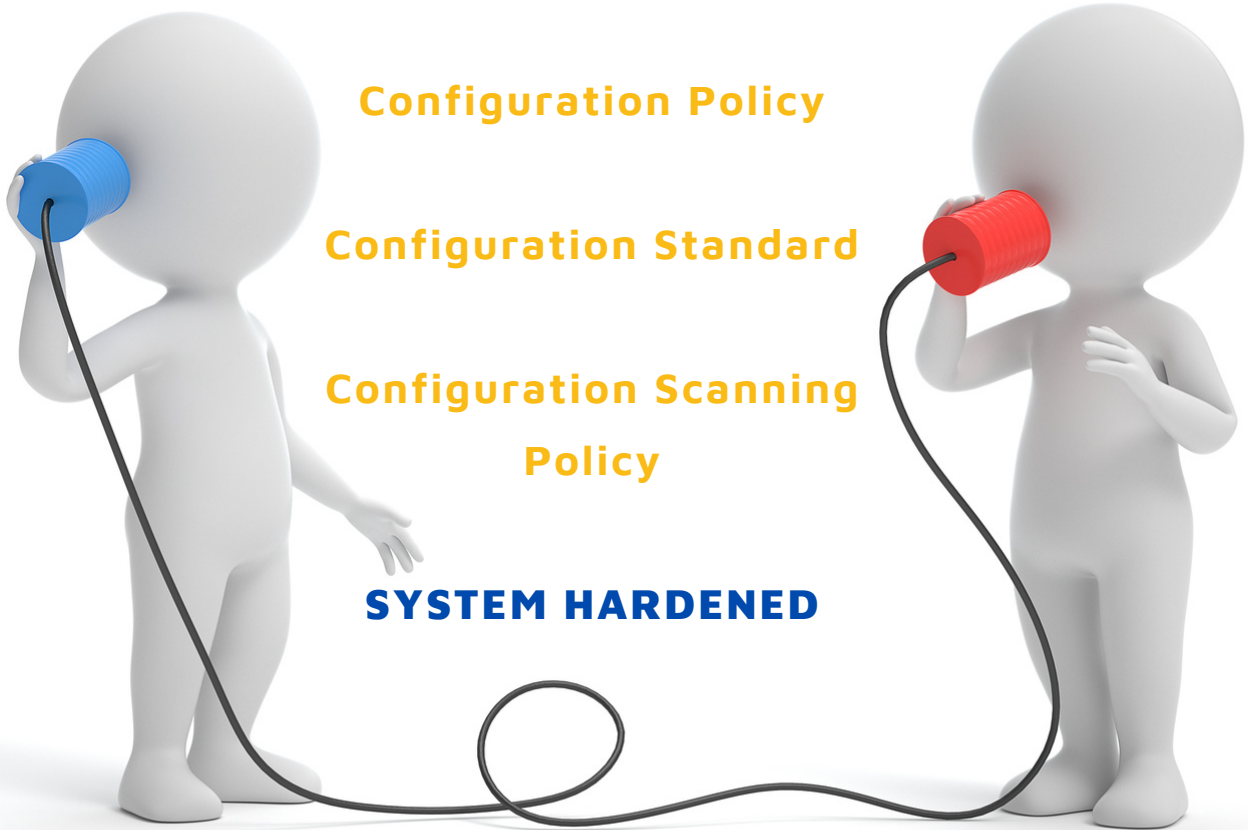
BUILD CLEAN

Configuration Policy

Configuration Standard

Configuration Scanning Policy

SYSTEM HARDENED

COMMUNICATE

Build Clean Processes

Per Requirement 2.2 of the PCI DSS all new PCI in-scope systems need to be hardened prior to deploying to production. Every organization should have controls in place that meet this requirement.

Because of the name you might think Build Clean refers to the actual task of building a new system, but Build Clean actually starts long before a request for a new system is ever submitted.

To Build Clean an organization must have a Configuration Management program and it must consist of the following components:

- Configuration Policy
- Configuration Standard
- Configuration Scanning Policy
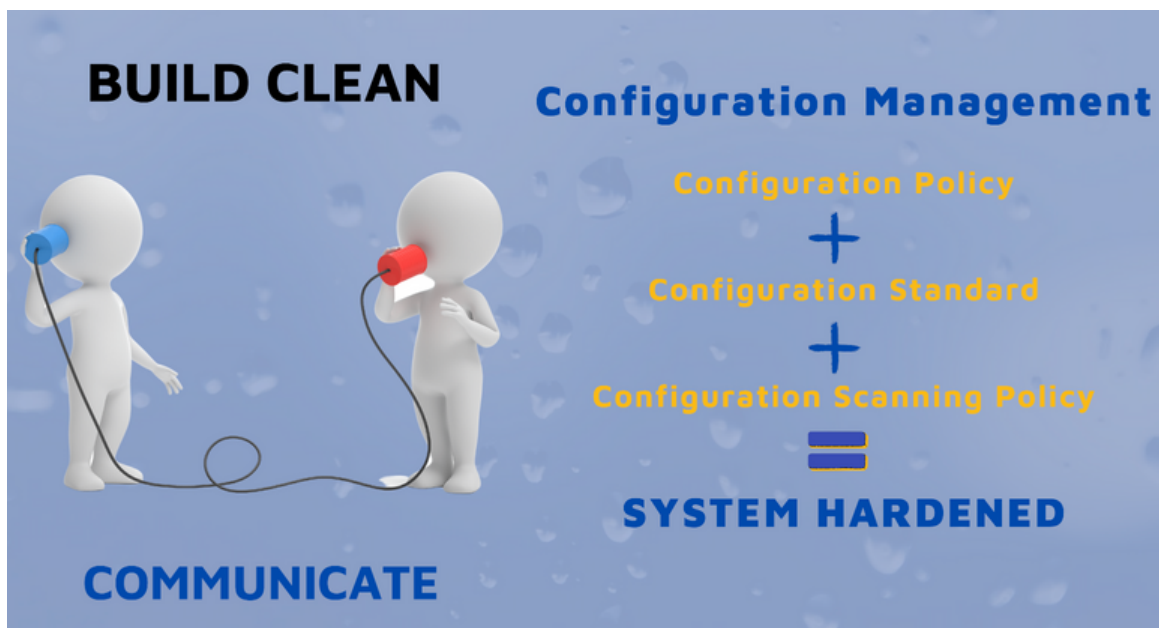
**What's the Guys Name on First Base?
"Yes"**

Whose on first base, by Abbott & Costello

Configuration Management

 Configuration management is a discipline with a set of policies, procedures, and processes that outlines how the organization will maintain computer system, servers, and software in a desired, consistent state.

It's a way to make sure that a system performs as it's expected to as changes are made over time.

Configuration Management is viewed as an IT management best practice.

How a system and its components are built and deployed into an environment has a direct impact on the security posture of the system.

Configuration Policy

The Configuration Policy should define how system configurations will be managed to ensure appropriate configuration methods are applied and maintained in the environment.

The Configuration Policy must define the following:

- The scope of the environment

- The role and responsibilities related to configuration management

- The use of a configuration framework (NIST, ISO, CIS etc.). They may even call out the specific framework in this document

- The baseline configuration which is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time. The baseline configuration is used as a basis for future builds, releases, and/or changes.

- And since the baseline can only be changed through change control procedures, this document will also include a section on the Change Management Policy.

Configuration Standards

All systems come with default configurations (like default accounts and passwords) so it is easier for the organization to setup the system. In many cases, these default configurations may be insecure.

In addition, all organizations will make changes to the systems before they install the technology on their network. They do this to secure them and to also configure them based on the role and function of the system.

This is why they develop Configuration Standards.

The standards are a document or collection of documents that describe how a technology should be configured (hardened) and how they intend to keep up-to-date with current industry guidance.

There are different operating systems (OS) depending on the system, so you will see that they develop a different configuration standard for each operating system (OS).

These standards need to incorporate specific compliance regulatory guidelines in the standards document itself:
1. Eliminate default accounts and passwords
2. Develop the standards using an industry accepted hardening framework(NIST, ISO, CIS, etc.)
3. Must be applied to all new systems and must be hardened before the system is installed on the network
4. Implement only one primary function per server
5. Enable only necessary services, protocols, daemons, etc. as required for the function of the system

Once the configuration standards have been developed, they release them to the team developing the OS build packages (that could be engineering, could be network depends on your organization) and to the Scanning team.

Most Common Configuration Management Errors - #1

Vendors offer systems of all shapes and sizes, providing a wide range of options for organizations.

Organizations have many reasons for purchasing vendor built systems:

- What security framework did they follow when developing their configuration standards? They need to know if the vendors configuration standard is as secure as their own. If it is not they may need to implement compensating controls.
- Who is responsible for system changes and upgrades? Does the organization implement upgrades or are they at the whim of the vendor. The release of vendor patches can take forever leaving the system at risk.
- What is their maintenance agreement?

Example:
Your organization purchases CyberArk Vaults from a vendor and deploys them into production. The vaults were delivered and antivirus software could not installed and if we had installed antivirus software on the vaults it would have voided the maintenance agreement. In this scenario the organization would have to collect the vendor documentation and present a defensible position to the QSA.

Configuration Scan Policy and Pre-Production Scanning

The organizations Configuration Scan Policy is developed to meet the configuration standards and should define how system configurations will be managed to ensure appropriate configuration methods are applied and maintained in the environment.

The standards are released to the scanning team who develop the scanning policy. The scan policy is used to refine the scan settings/rules in a tool like (Tripwire, Nessus, etc.).
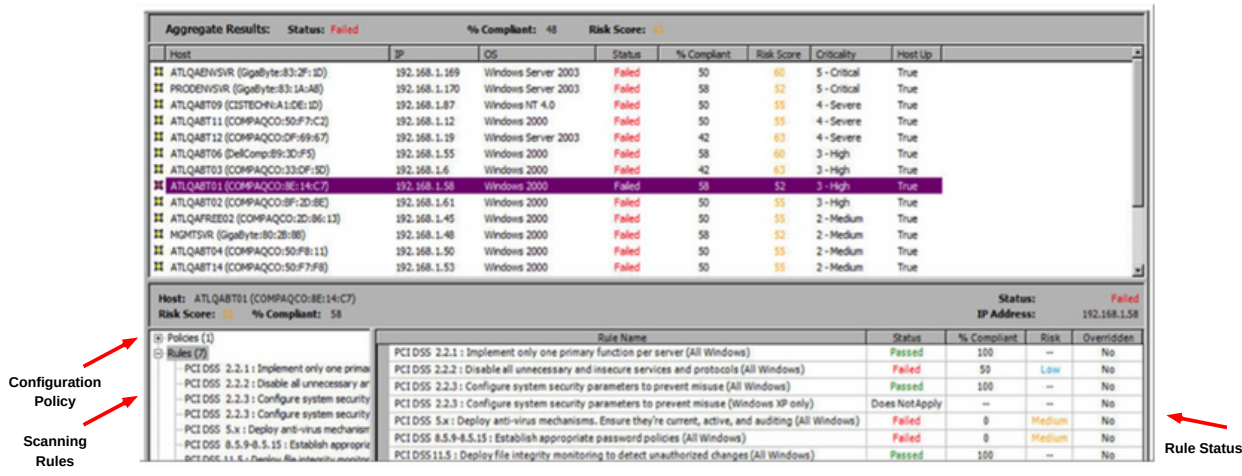

Fig. 1 Tripwire CCM Express Aggregate Results from enterprise scan, with Percent Compliant and Risk Scores, plus actionable details.

After an OS build package has been developed and applied to a system in dev and the scanning policy has been created, the system will be scanned in dev.

This will create the configuration baseline hardening of a system (aka known good state).

If the build package and scanning policy are not in sync the scanning results will show configuration setting failures and will not be considered hardened.

When the scan settings/rules all show as passing the system will be considered hardened and ready to be deployed to the production environment.
.

System Hardening

The goal of system hardening is to remove all unnecessary components and access to the server in order to maximize its security. Server hardening disciplines and techniques improve the security of a server.

Before a system is built, the engineering team typically puts a significant amount of time and effort into the hardened build packages that will be applied during the build process. This process must be well documented and well defined.

But, once a system is built, hardened and deployed into a production environment, it is critical to maintain its level of security and make sure that a system performs as it's expected to as changes to the system are made over time.

Changes like:

- A quick work around to a software bug
- Patching
- Firewall modifications
- New Firewall Rules

As updates and patches are being performed to mitigate new vulnerabilities and weakness that are being discovered, the engineering team will update the baseline configuration and hardening processes to include these new patches or software versions so that the next time a similar system is deployed old vulnerabilities are not re-introduced into your environment.

System hardening is a requirement of security frameworks such as PCI-DSS and your Report on Compliance or SAQ depends on it.

KEEP CLEAN
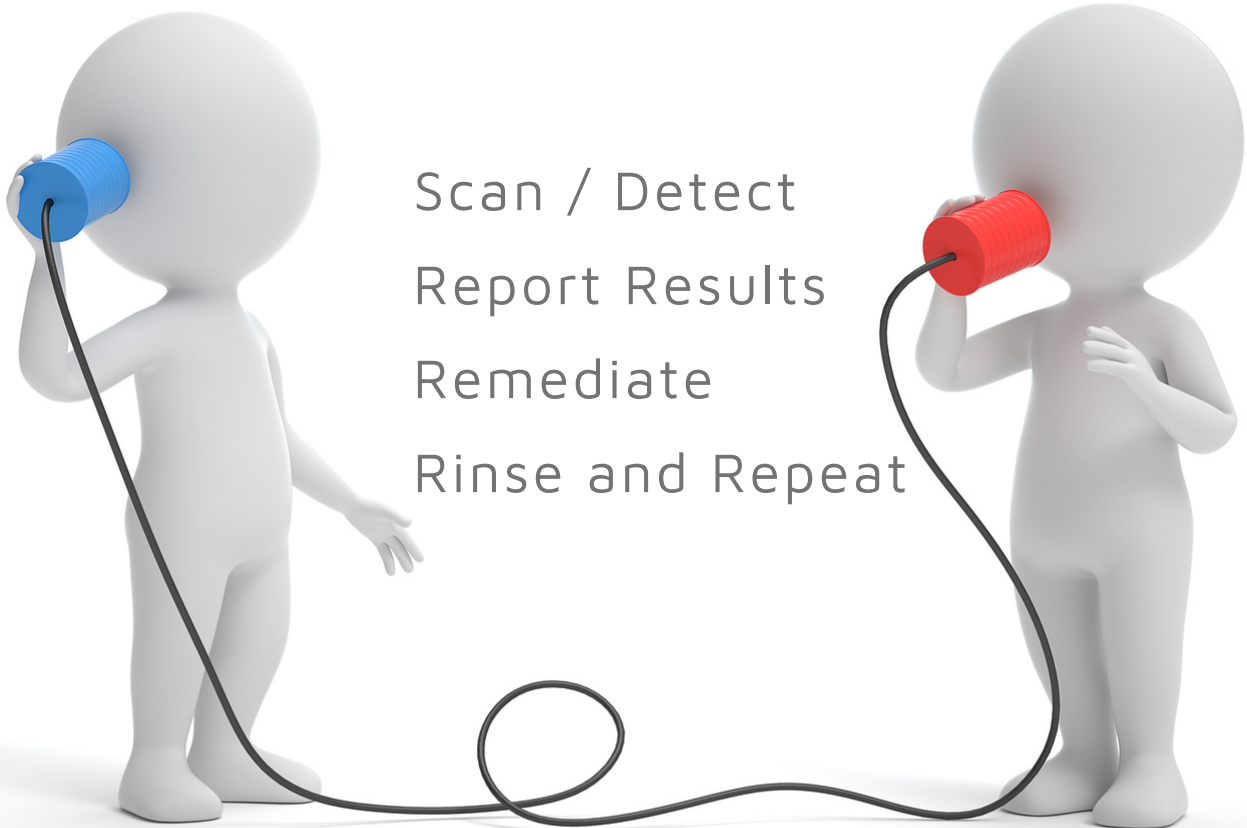
Scan / Detect

Report Results

Remediate

Rinse and Repeat

COMMUNICATE

Things don't turn up in this world until somebody turns them up

-James A. Garfield

Configuration Scanning
Post Production

Configuration scanning is a process for scanning operating system to identify and mitigate vulnerabilities that threaten compliance, including software flaws, missing patches, malware, and misconfigurations across operating systems, devices, and applications.

- Scan regularly for configuration changes
- Maintain your device inventory
- Create baselines
- Monitor continuously and audit regularly
- Prioritize documentation and communication

Configuration Scanning
Post Production

Once In production, scans are scheduled on a recurring basis for continuous monitoring purposes. This enables an organization to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments.

**PCI DSS requires internal scanning quarterly and after any significant change. If an organization scans monthly they will pickup any issues caused by the significant changes.

Depending on how the organization has "risk ranked" their environment, this drift has a direct impact on the security of the system as well as the ability to maintain compliance.

Perform cross validation (in-scope asset inventory to scanning inventory) at least weekly. *Depending on the size of your organization, this will require you to implement automation.

Most Common Configuration Management Errors - #2

Many organizations become lulled into a false sense of security because they are scanning their assets on a regular basis.

What they may not realize is that there are a number of scenarios that can lead to a system not being scanned.

These are considered missed opportunities that can lead to compliance issues.

Missed Opportunities Lead to Compliance Issues

⚠ Configuration scanning schedules are typically set to monthly or quarterly

⚠ Configuration scanning can only be performed during the off hours, typically between 1:00 am & 6:00 am EST.

⚠ Systems that are down due to maintenance or other outages will not be scanned

⚠ Risk rankings will vary based on an organization's environment and risk assessment strategy.

When the scanning schedule isn't frequent enough systems can be missed during the scanning cycles and any configuration drift that the system may have will go undetected until the next scan cycle.

**PCI DSS states that all "critical" vulnerabilities must be remediated in 30 days. Risk rankings will vary based on an organization's environment and risk assessment strategy.

Configuration Scanning Results

When configuration failures occur the default behavior for the scanning tool is to then skip every other setting down the line.

The configuration management team must provide a summary of scanning results. Each scan result submission must be accompanied by a summary of the scan performed. The summary must include a listing of all the scan files submitted, which scanning tools were used, and a summary of the purpose of the scan (e.g., monthly scans, re-scans, verification scans, etc.).

Most Common Configuration Management Errors - #3

You have to get a handle on your scope by performing a scope assessment.

The scanning team should perform cross validation (in-scope asset inventory to scanning inventory) at least weekly.

If you do not have a process for managing your in-scope asset inventory on a weekly basis (at minimum) your scanning team will not be scanning all of your assets or they could be trying to scan assets that have been demoted, retired, etc.

Incorrect Scope ...

✗ A scope assessment has not been completed since your last RoC/Assessment

✗ Your in-scope asset inventory is not maintained on a daily or weekly basis

✗ In-scope assets come and go (new builds, demotions, retirements

*Depending on the size of your organization, this will require you to implement automation.

Configuration Drift Scenarios

When a server is scanned the configuration scan policy will look for security settings on the server that are not configured correctly. If a misconfiguration is detected it will show on the scan reports as a failure (we refer to this as "drift").

Develop Configuration standards for all systems (PCI DSS 2.2.b)

All in-scope servers are scanned prior to being deployed to production. This is done to ensure that the standards address all known security vulnerabilities and are consistent with system hardening standards.

Microsoft releases a new OS called Microsoft 2020. The engineering team creates the build package and they collaborate with the GRC team to review and test it in Non-prod and everything looks great!

The GRC team makes sure that they update the Configuration Standards but they forget to communicate with the scanning team, so the configuration scanning policy does not get updated. The next time the servers are scanned multiple failures are detected and reported to the system owners for remediation.
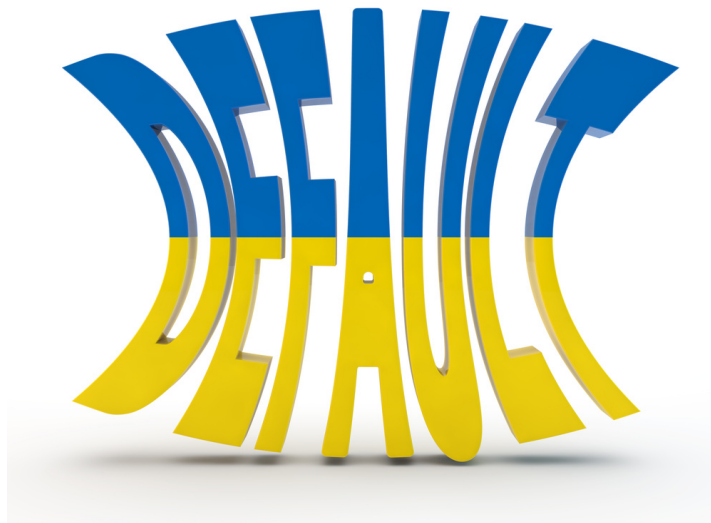
Configuration Drift Scenarios

Vendor supplied defaults (PCI DSS 2.1)

Vendor defaults make device installation and support easier, but it also means that every model originates with the same username and password. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.

When those defaults aren't changed, malicious individuals (external and internal to an organization) will often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed.

Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.
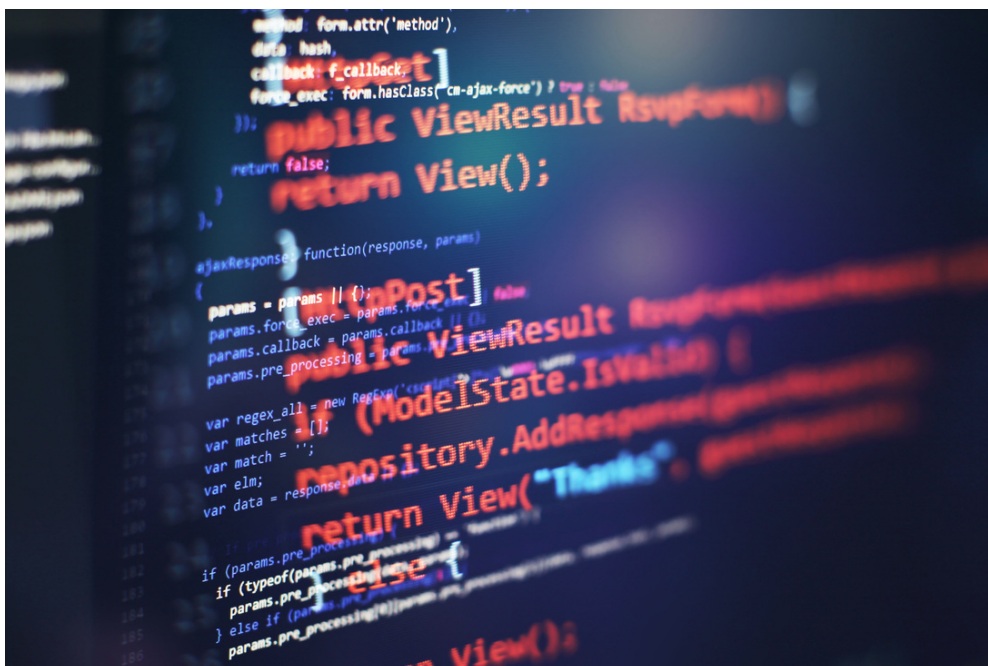
Configuration Drift Scenarios

Implement only one primary function per server (PCI DSS 2.2.1)

You have a new Web server built and that server is also used for your Disaster Recovery (DR) exercises. There are functions being performed by this server when in Production that require a different security level than when that server is demoted to Non-prod during the DR exercises.

If you were to put both functions on one server the security level of the functions with higher security needs would be reduced due to the presence of the lower-security function when that server is demoted to Non-prod during the DR exercises.

For instance, you have 2FA functions on the web server while it is in Production, but when you demote the server to Non-prod for DR exercises 2FA is not being used. This could allow a malicious individual easy access to accounts and passwords.

Configuration Drift Remediation

Let's talk about what you do with configuration "drift".

STAKEHOLDER COMMUNICATION

Scanning team communicates to the server owners that a scan was completed and there are server(s) configuration failures. This can be done using incident tickets or project engagements (depending on the quantity).

SCHEDULE CHANGE WINDOW

The server owners need to schedule a "change window" to have the failures mitigated.

REMEDIATE AND TEST

The server configuration failures are remediated and tested during the established "change window".

RE-SCAN

Re-scan the server to ensure that the failures were corrected.

This sounds pretty easy right?

Well, it is, but it depends on how your organization "risk ranks" their configuration failures. **PCI DSS 6.2** states that all "critical" vulnerabilities which means includes configuration "drift", must be remediated within 30 days or you must report this control as Non-Compliant.

This requirement will absolutely cause chaos

What are the Benefits?

- Sustain compliance more effectively and efficiently

- Better positioned to respond to changes in the environment or security landscape overall

- Move from a project based compliance posture to a more formal sustainability program

- Understand critical controls and their impact on other controls

- Being pro-active vs reactive saves time and effort

- Saves time for process improvements

It makes it a whole lot easier to meet the intent of the PCI DSS Requirements

YOU ARE MATURING YOUR CONTROLS

How to Develop and Implement a Build Clean / Keep Clean Process

This will be a project you need to plan and implement methodically. You will be changing "the way it has always been done". Getting buy-in could be a challenge.

PRE-MEETING

STEP 1 - White board your approach/strategy
- Who are the key players
- Clearly identify "Ownership"
- How will you get buy-in from Senior Management

STEP 2 - Start socializing your idea
- **Bring it up in meetings with key players**
- **Communicate your approach and the benefits**
- **Ask them for their "Runbooks / Standard Operating Procedures"**

STEP 3 - Analyze the data
- Review the "Runbooks / Standard Operating Procedures

STEP 4 - Schedule the meeting
- Invite all key players
- The agenda should be an outline of your approach

How to Implement a Build Clean / Keep Clean Process

MEETING DAY(S)

Day 1

- Start at the top and work your way through each key players tasks
- Document this on a white board using a process flow theme

Day 2

- Walk through the entire process flow with the key players. Make note of the following:
  - Process Gaps
  - PCI DSS Requirement touch points
  - Communication and hand-off touch points
  - What steps in the process would be impacted by a change? (example: adding a configuration setting)
  - Clearly identify "Ownership" of each step in the process flow

How to Implement a Build Clean / Keep Clean Process

POST MEETING

STEP 1

- Update the end-to-end process flow based on your notes

STEP 2 - Communicate to Key Stakeholders

- Send the recommended process (incl. process flow diagrams and Roles and Responsibilities matrix
- Get sign-off

STEP 3 - Create the process documentation

- Include process flow diagrams, Roles and Responsibilities Matrix
- Send to key stakeholders

STEP 4 - Communicate to Senior Management

- Include the benefits of implementing a Build Clean/Keep Clean process
- Include pre-meeting analysis data and results of the 2 day workshop incl. before and after process flow diagrams
- Include the newly created process documentation
- Get sign-off (or Rinse and Repeat until you do)

STEP 5 - Implement

Build Clean Process Flow

Build Clean Process Flow

Build Standard

QA Review

Configuration & Vulnerability Standards

Group Policy

INPUT Firewall Request

INPUT Middleware Svcs Request

YES

Build Request → Server Build

OUTPUT Hardened Server

Middleware Services

NO

PRODUCTION Data Center OR Enclave

END

Configuration & Vulnerability Scans

OUTPUT Vulnerability Scan Results

OUTPUT Configuration Scan Result

YES — Scan Failures — NO

Keep Clean Process Flow

Keep Clean Process Flow

Change Successful

Build Standard

Testing During Change Window

Configuration & Vulnerability Standards

Schedule Change Window

NO

Configuration & Vulnerability Scan Policy

Remediate

YES

PRODUCTION Data Center OR Enclave

Configuration & Vulnerability Scans

INPUT Open Incident Tickets

OUTPUT Vulnerability Scan Results

OUTPUT Configuration Scan Result

Scan Failures?

YES

Failure Analysis

Reasons for Failures / Drift
* *a setting changed on the server*
* *the standard changed after annual review*
* *the standard changed due to vulnerability in the environment*
* *the scan policy is not up-to-date*

NO

END

SYSTEM HARDENING CHECKLIST

PCI DSS Requirement 2.2 v3.2.1: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening security experts, a number of security organizations standards.

Sources of industry-accepted system hardening standards may include, but are not limited to:
• **Center for Internet Security (CIS)**
• **International Organization for Standardization (ISO)**
• **SysAdmin Audit Network Security (SANS) Institute**
• **National Institute of Standards Technology(NIST).**

This checklist provides a starting point as you create or review your server hardening policies.

💡 When considering server hardening, remember the applications that will run on the system and not just the operating systems.

☐ Change default credentials and remove (or disable) vendor-supplied default accounts before a system is installed on the network (PCI DSS Requirement 2.1 v3.2.1).

💡 Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

☐ Wireless - change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

💡 If wireless networks are not implemented with sufficient security configurations, wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. In addition, firmware for devices should be updated to support more secure protocols.

☐ Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server

☐ Enabling only necessary services, protocols, daemons, etc., as required for the function of the system – this includes scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

💡 Windows systems - only activate the Roles and Features you need.
Linux systems - remove package that are not required and disable daemons that are not needed

OS HARDENING CHECKLIST

☐ System configuration standards must be kept up-to-date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

☐ Configure NTP servers to ensure all servers (and other network devices) share the same timestamp.

💡 It is much harder to investigate security or operational problems if the logs on each device are not synchronized.

☐ Configure perimeter and network firewalls to only permit expected traffic to flow to and from the server.

☐ Configure operating system and application logging so that logs are captured and preserved.

💡 Consider a SIEM solution to centralize and manage the event logs from across your network.

AUTOMATE

EDUCATE

OPERATE