What Are CIS Benchmarks? A Simple Guide to a Stronger Security Foundation

1. Introduction: A Building Code for Your Digital World

Imagine constructing a house. You wouldn't start without a detailed blueprint, and you certainly wouldn't ignore the local building codes that ensure the structure is safe, sound, and secure. These codes, developed by experts, represent a collective agreement on the best way to build something that lasts. In the digital world, where we build our businesses and store our most valuable information, a similar set of "building codes" exists: **CIS Benchmarks**. But unlike building codes for a house, these digital codes must be applied to a living, breathing system, a distinction that requires not just diligence, but wisdom.

This guide is designed to demystify these foundational cybersecurity standards. It will explain what CIS Benchmarks are, who creates them, how they are structured, and why they are essential for anyone using technology today, from servers and cloud accounts to laptops and applications. Whether you are an executive, a member of a sales team, or simply curious about how to build a stronger defense against cyber threats, this document will provide a straightforward explanation of this critical security resource.

Let’s begin by defining what CIS Benchmarks are at their core.

2. Decoding CIS Benchmarks: The What, Who, and Why

To trust a standard, it is vital to understand its origin and purpose. CIS Benchmarks are not arbitrary rules; they are the product of a rigorous, collaborative process designed to create a global standard for security. This section breaks down their fundamental nature.

- **What They Are:** CIS Benchmarks are expert-developed, consensus-driven configuration guidelines for securing technology systems. Think of them as a "master checklist" or a "secure setup recipe" created by the world's top cybersecurity professionals. Instead of leaving system security to guesswork, the benchmarks provide prescriptive, step-by-step guidance for establishing a secure configuration posture.
- **Who Creates Them:** The benchmarks are created and maintained by the **Center for Internet Security (CIS)**, a non-profit organization. More importantly, they are developed through a global community of subject matter experts. This community includes professionals from diverse backgrounds, such as consulting, software development, government, security research, and legal fields, who collaborate through a consensus review process to create, test, and validate the recommendations. This community-driven approach is what gives the benchmarks their credibility and real-world relevance.
- **What They Cover:** The scope of CIS Benchmarks is incredibly broad, reflecting the complexity of modern IT environments. There are over **100 individual benchmarks**

that cover more than **25 different vendor product families**. This includes foundational technologies that power nearly every organization, such as:
    - **Operating Systems** (e.g., Windows Server, Ubuntu Linux)
    - **Cloud Services** (e.g., Amazon Web Services - AWS)
    - **Applications & Software** (e.g., Kubernetes)

This extensive coverage ensures that organizations can apply a consistent security philosophy across their entire technology stack.

3. Inside a Benchmark: Understanding the Structure

CIS Benchmarks are more than just a simple list of "dos and don'ts." They are highly structured documents designed for practical use, helping users understand not just *what* to do, but *why* they should do it and *what* the potential consequences might be. Here are the key components you'll find inside.

- **Recommendations:** These are the individual, specific security settings that make up the core of a benchmark. Each one is a clear, actionable instruction.
    - **Analogy:** Think of each recommendation as a single, clear instruction in a recipe, like "Set oven to 350°F" or "Add two teaspoons of salt." Each is a specific, testable action.
- **Profiles (Level 1 vs. Level 2):** Because not all systems have the same security needs, recommendations are grouped into profiles. This allows organizations to apply the right level of security for the right environment.
    - **Level 1:** This profile represents a baseline level of security—essential best practices that should be applied to all systems. These recommendations are designed to be practical and should not cause significant disruption to service or performance.
        - **Analogy:** Level 1 is the essential security for a **family home**—strong locks on doors and windows that don't get in the way of daily life.
    - **Level 2:** This profile is for high-security environments where data is more sensitive or the risk of attack is greater. These recommendations are stricter and may have a performance or functionality trade-off.
        - **Analogy:** Level 2 is the security for a **bank vault**. It's much more restrictive and might be less convenient, but it's absolutely necessary when protecting high-value assets.
- **Rationale and Impact:** Every recommendation is accompanied by two critical explanations:
    - **Rationale:** This section explains *why* the setting is important. It details the security vulnerability the recommendation is designed to prevent.
    - **Impact:** This section describes the potential consequences of applying the recommendation, such as potential conflicts with other applications or changes in functionality. This empowers users to make informed decisions rather than applying settings blindly.

These structural elements ensure the benchmarks are not just theoretical documents but practical, actionable tools for building a secure digital foundation.

4. CIS Benchmarks in Action: Simple, Real-World Examples

To move from theory to practice, let's look at a few concrete examples from different CIS Benchmarks. These illustrations show how the recommendations translate into tangible security controls that protect systems every day.

- **Example 1: Stronger Passwords (Windows Server)**
  - **Recommendation:** A password must be at least 14 characters long.
  - **Analogy:** Think of a password like a lock on a door. A short, simple password is like a basic doorknob lock that's easy to pick. A long, complex password is like a heavy-duty deadbolt, making it exponentially harder for intruders to break in.
- **Example 2: Preventing Brute-Force Attacks (Windows Server)**
  - **Recommendation:** Lock a user's account for 15 minutes after 5 incorrect login attempts.
  - **Analogy:** This is like your front door automatically locking itself for 15 minutes if someone tries the wrong key five times in a row. It stops a thief from endlessly trying every key on their ring.
- **Example 3: Reducing the Attack Surface (Ubuntu Linux)**
  - **Recommendation:** If a server is not used for printing, the printing service (CUPS) should be disabled or removed.
  - **Analogy:** Every running service is like a door or window to your house. If you have a back door you never use, it's safer to board it up completely. This reduces the number of potential entry points for an attacker.
- **Example 4: Securing Cloud Accounts (Amazon Web Services)**
  - **Recommendation:** Enforce Multi-Factor Authentication (MFA) for all users.
  - **Analogy:** This is like requiring two forms of ID to enter a secure building—something you have (your phone) and something you know (your password). It ensures that even if a password is stolen, your account remains secure.

These examples highlight how CIS Benchmarks address common security weaknesses with clear, common-sense controls. Now, let's explore how organizations actually implement these hundreds of settings across their infrastructure.

5. Putting Benchmarks to Work: From Theory to Practice

Applying hundreds of security settings across dozens, or even thousands, of systems is a significant undertaking. While the benchmarks provide the blueprint, success hinges on practical, "from the trenches" implementation strategies. Organizations use a combination of specialized tools and proven methodologies to implement CIS Benchmarks effectively and safely.

- **Automated Assessment Tools.** While it's possible to check configurations manually, it is impractical at scale. Most organizations use automated tools to scan systems and compare their live configurations against the CIS Benchmark recommendations. The official tool from CIS, **CIS-CAT Pro Assessor**, is a prime example. These tools generate detailed reports that show compliance scores, highlight security gaps, and help teams track their progress over time.

- **CIS Hardened Images.** For new deployments, especially in the cloud, organizations often use CIS Hardened Images. These are pre-configured, secure-by-default system templates (for operating systems like Windows or Linux) that already meet the standards of a CIS Benchmark.
    - **Analogy:** This is like buying a car with top safety ratings and features, like airbags and anti-lock brakes pre-installed, rather than building a car from parts and hoping you installed everything correctly.
- **The Golden Rule: A Guideline, Not a Law.** While security teams push for 100% compliance, operations teams know the reality: blindly applying hundreds of settings is a recipe for disaster. A security setting that works for 99% of systems might break a critical business application. The standard practice is to use the benchmarks as a starting point, test all settings in a non-production environment, and establish a formal **exception process**. This process is a crucial bridge between security goals and operational reality. Typically, the operations team identifies conflicts and justifies exceptions, while the security team is responsible for evaluating the risk and formally accepting it.
- **Break It Down: Avoid Monolithic Policies** Experienced system administrators advise against applying an entire benchmark as a single, monolithic policy (like one giant Group Policy Object or GPO). Trying to troubleshoot which of the 400+ settings broke an application is a nightmare. Best practice is to break large benchmarks into smaller, logical chunks for testing and deployment. This allows teams to roll out changes incrementally, isolate issues faster, and manage exceptions with greater precision.

CIS Benchmarks are a powerful but flexible framework. When implemented thoughtfully, they provide a robust foundation for an organization's security posture.

6. Why CIS Benchmarks Matter: The Real-Life Impact

Adopting CIS Benchmarks provides strategic value that extends far beyond the IT department. Their impact can be felt across the entire organization, from strengthening day-to-day security to enabling business goals.

- **For Business Leaders & Executives:** CIS Benchmarks provide a defensible, industry-recognized standard for cybersecurity. Adhering to them demonstrates due care in protecting company and customer data. Crucially, they serve as a foundation for meeting the compliance requirements of major regulatory frameworks, including **PCI DSS**, **FISMA**, and **FedRAMP**, helping to unlock new business opportunities and avoid costly penalties.
- **For IT and Security Teams:** For technical teams, the benchmarks provide a reliable, expert-backed roadmap that eliminates guesswork. Instead of debating which security settings are important, teams can start with a globally accepted baseline. This creates a common language for discussing security configurations and frees up valuable time to focus on more complex, organization-specific threats.
- **For Everyone:** Ultimately, CIS Benchmarks represent a foundational layer of **"cyber hygiene."** Most cyberattacks are not sophisticated, zero-day exploits; they are

automated, opportunistic attacks that take advantage of common misconfigurations. By closing these common, easily exploitable gaps, CIS Benchmarks defend against the vast majority of automated and opportunistic attacks, creating a powerful foundation of proactive defense that makes the digital world safer for everyone.