CIS HARDENING SERVICES

REDUCE CONFIGURATION RISK WITH A PRACTICAL, MAINTAINABLE SECURITY BASELINE

As Linux environments evolve, configurations can drift. Unnecessary services remain enabled, permissions become inconsistent and security settings vary between otherwise similar systems.

BACKGROUND

Tiger Computing helps organisations assess and strengthen Linux configurations against an agreed CIS Benchmark. We combine recognised configuration guidance with practical Linux expertise, helping you improve security while considering application dependencies, performance and service continuity.

WHAT ARE CIS BENCHMARKS?

CIS Benchmarks are prescriptive, consensus-based configuration recommendations developed by the Center for Internet Security for operating systems, cloud platforms and other technologies.

Level 1: Base recommendations intended to reduce the attack surface while limiting impact on usability and business functionality.

Level 2: Builds on and extends Level 1 with additional defence-in-depth recommendations for environments where security is paramount. These require careful assessment and testing because they can affect system operation.

A PRACTICAL ROUTE FROM ASSESSMENT TO ONGOING ASSURANCE

Assessment

The initial assessment is a defined consultancy engagement:

- Scope the systems, distributions, workloads and security objectives
- Select the applicable CIS Benchmark and target profile
- Review current configurations against the agreed baseline
- Consider failed checks, operational dependencies and legitimate exceptions
- Produce a prioritised remediation plan

Deliverables

- Current-state CIS Benchmark assessment
- Operational impact and dependency review
- Prioritised findings and remediation plan
- Identified exceptions requiring review

Remediation

Remediation is separately scoped consultancy. Depending on the number of systems, findings and operational complexity, it may be delivered as one project or several phases.

Work can include testing and implementing agreed changes, planning rollback, documenting exceptions and validating the resulting configuration.

Deliverables

- Testing and implementation of agreed changes
- Documented exceptions and rationale
- Post-implementation validation
- Updated secure-configuration baseline

Ongoing Support

The destination is a maintainable security baseline, not a one-off hardening exercise.

Under an appropriate ongoing support arrangement, Tiger can run automated assessments at an agreed frequency to check systems against the customised baseline. Results are reviewed to identify configuration drift and any actions needed to restore alignment.

Ongoing support can also keep the baseline aligned with minor revisions to the relevant CIS Benchmark. Significant changes, including major Benchmark versions or remediation requiring substantial system changes, are assessed and scoped separately.

Deliverables

- Automated assessments at an agreed frequency
- Identification of configuration drift
- Review of results and recommended actions
- Baseline maintenance for applicable minor Benchmark revisions
- Identification of major changes requiring separate assessment

POTENTIAL TECHNICAL AREAS

- Filesystem, partition and mount options
- Bootloader and kernel-related configuration
- Packages, services and listening ports
- Firewall and network parameters
- User, password and privileged-access controls
- sudo, SSH and remote administration
- File permissions and ownership
- Logging, auditing and time synchronisation
- Update and repository configuration
- Consistency across comparable systems

The precise scope depends on the Benchmark, Linux distribution and workload.

SUCCESS STORY

Tiger has implemented CIS hardening for Sucden Financial and supports more than 36 critical Linux systems within its trading-platform environment, where uptime, security and compliance are essential.

START WITH YOUR ENVIRONMENT

Book a discovery call to establish which systems and Benchmarks may be in scope, whether Level 1, Level 2 or a tailored baseline is appropriate, and how to scope the initial assessment.

Book a CIS hardening discovery call
info@tiger-computing.co.uk
01600 483 484
Schedule a call

Assessment → Remediation → Ongoing assurance

WHY TIGER COMPUTING?

- Linux specialists since 2002
- Practical assessment and remediation support
- Risk-based, phased implementation
- Independent, vendor-neutral advice
- ISO 27001 certified organisation
- Experience supporting security-critical Linux environments

Tiger Computing

WE DO LINUX. YOU DO BUSINESS.