Cyberfort

Expert-led. Security Driven.

Penetration Testing

SERVICE OVERVIEW

Evidencing assurance and delivering confidence with Real-World Testing

Welcome to Cyberfort's Penetration Testing Services

Why Penetration Testing Matters

In today's digital world, every organisation relies on technology to store, process, and communicate sensitive data. This makes them prime targets for cybercriminals, nation-state actors, and malicious insiders. Penetration testing, or "ethical hacking," is a proactive measure to:

- Identify unknown vulnerabilities before attackers do
- Validate your existing security controls and configurations
- Demonstrate due diligence and regulatory compliance
- Reduce business risk by understanding the real-world impact of potential attacks
- Support cyber insurance requirements with evidence of regular testing
- Prioritise your security investment based on data-driven insights

Business Benefits of Regular Testing

Reduce Risk: Mitigate loss of critical services from high-profile attack vectors such as ransomware, credential theft and abuse, and cloud compromise

Protect Reputation: Avoid brand damage from breaches

Reduce Costs: Fixing security issues proactively is far cheaper than recovering from an incident

Enable Compliance: Satisfy requirements for GDPR, ISO 27001, PCI DSS, NIS2 and more

Build Customer Trust: Show your commitment to security with formal test reports and certifications

Support Secure Growth: Launch applications and services with confidence knowing security has been validated

With cyber threats growing in complexity and volume, regular penetration testing is a vital component of any organisation's cyber risk management strategy.

At Cyberfort, we go beyond traditional security testing. As a CREST and CHECK-certified provider, we deliver trusted penetration testing services to government bodies and enterprises across the UK. Our expert testers hold Security Clearance (SC) as well as Non-Police Personnel Vetting (NPPV3) certifications, leveraging deep technical knowledge and real-world experience to identify and validate security weaknesses before adversaries can.

Our Coverage includes:

- Internal and External Infrastructure Testing
- Web & Mobile Application Security Assessments
- Cloud Configuration Reviews (Azure, AWS, M365)
- Active Directory and Workstation/Server Build Reviews
- Secure Code and Infrastructure as Code (IaC) Reviews
- Red Team and Purple Team Engagements
- Wireless, Firewall and Network Segmentation Reviews
- Cyber Essentials and Cyber Essentials Plus Certification

We test against today's real threats – not just checklists.

Core Testing Services in Detail

Each of our core testing services is designed to uncover real-world risks using modern adversarial techniques. Here's an overview of what's tested, the key benefits to your organisation, and common examples of the threats mitigated.

Cyberfort
Expert-led. Security Driven.

Internal Infrastructure Penetration Testing

Identification and exploitation of internal vulnerabilities and weaknesses, from the mindset of an insider threat or a compromised device. We test:

- Service discovery and enumeration
- Exploitation of misconfigured services and vulnerabilities
- Privilege escalation and lateral movement
- Domain dominance and sensitive data access

Benefits

- Validates internal segmentation and privilege boundaries
- Helps you uncover paths to domain admin or sensitive systems
- Supports zero trust initiatives and insider threat resilience

Example Risk Covered
An attacker gains unauthorised access to an unused office computer, and exploits poor segmentation and weak credentials to reach finance systems and exfiltrate payroll data.

External Infrastructure Penetration Testing

Replicates advanced attacks from the public internet targeting:

- Web, email, VPN, DNS and other perimeter services
- OSINT reconnaissance
- Safe exploitation of known vulnerabilities

Benefits

- Identifies internet-facing weaknesses before attackers do
- Emulates known threat actor tools and techniques
- Provides assurance to stakeholders and insurers
- Supports compliance with cyber regulations (e.g. CE+, NIS2)

Example Risk Covered
A legacy file transfer service with an unpatched RCE vulnerability is discovered and exploited to gain a remote foothold on your network systems and exfiltrate payroll data.

Web Application Testing

- OWASP Top 10-aligned methodology
- Tests for well-known web vulnerabilities including authentication and authorisation, input validation, logic flaws, session handling, and injection vulnerabilities
- Use of end-to-end encryption
- Backend and frontend analysis, including API and database interaction and third-party plugin testing

Benefits

- Identifies critical flaws before your users or attackers do
- Hardens login flows, session security, and sensitive input validation
- Helps prevent brand-damaging breaches or data leaks

Example Risk Covered
An unauthenticated SQL injection vulnerability allows an attacker to dump your customer database, including PII and credentials.

Mobile Application and Device Testing

- iOS and Android apps reviewed for storage, network, and API risks
- Devices audited for encryption, OS security, access control, and data protection

Benefits

- Protects mobile users from data exposure and malicious tampering
- Verifies that apps meet store security guidelines (App Store, Play Store)
- Assesses stolen device risks and hardens user authentication

Example Risk Covered
A mobile app fails to encrypt authentication tokens, allowing an attacker with filesystem access to hijack sessions and access user accounts.

Advanced Configuration Reviews

Active Directory Assessment

- User and group policy review
- Kerberos & NTLM analysis
- Exploitation of domain services (trusts, certificate services, databases, etc)
- Privilege escalation paths
- Attack simulation across domain controllers

Server and Workstation Build Reviews

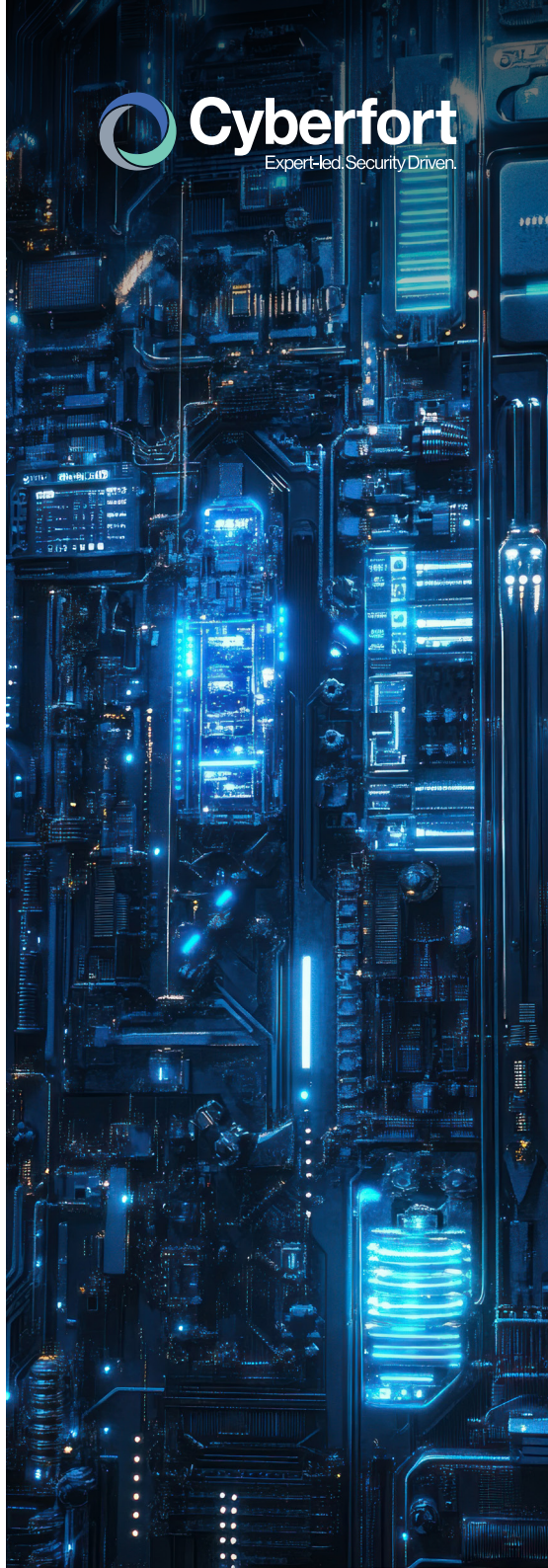
- Secure build hardening validation
- Patch level analysis
- Local service misconfiguration testing
- Endpoint security analysis (AV, Disk encryption, EDR)
- Logging and Monitoring

Firewall & Switch Configuration Reviews

- Rule base and segmentation evaluation
- VPN security and logging review
- VLAN configuration and STP hardening
- Use of native device security features

Network Segmentation Reviews

- Multi-protocol segmentation testing
- Use of policy enforcement
- Lateral movement attempts
- Cloud/on-premise boundary validation



Cloud & Strategic Testing

Cyberfort
Expert-led. Security Driven.

Azure, AWS & M365 Configuration Reviews

- Identity and Access Management (IAM)
- Use of external facing services and systems
- Virtual network and host configuration
- Management of keys and secrets storage
- Secure data storage and leakage prevention
- Appropriate use of logging and monitoring
- Data redundancy configuration
- Defender for Cloud / GuardDuty / Microsoft Purview alignment

Web Services & API Security Assessments

- API authentication, authorisation, and access control testing
- Potential injection vectors
- Rate limiting and DoS resistance
- Logging and sensitive data exposure testing

Infrastructure as Code Review

- Use of automation and IaC frameworks (Terraform, CloudFormation, Ansible, etc)
- Code repository security
- Hardcoded secrets and credential detection
- IAM misconfigurations
- Secure coding practices and library dependency scanning

Wireless Network Testing

- Rogue AP detection
- Use of appropriate Wi-Fi encryption types
- Evil twin simulations and credential capture
- VLAN isolation and segmentation testing

Threat Simulation and Certification

Cyberfort
Expert-led. Security Driven.

Breakout Testing

This assessment simulates attempts to escape restricted environments, such as VDI sessions or kiosk systems, and pivot laterally within your internal environment.

Benefits

- Identifies configuration weaknesses in lockdown environments
- Validates endpoint containment and privilege separation
- Enhances endpoint hardening policies

Example Risk Covered
A user on a locked-down VDI bypasses application control to access PowerShell, downloads malicious tooling, and laterally moves across internal systems.

Virtualisation Security Assessments

Assessment of hypervisors and virtualisation platforms (e.g., VMware, Hyper-V) for misconfigurations, weak isolation, and exploitable services.

Benefits

- Hardens virtualised infrastructure hosting critical services
- Identifies lateral movement and breakout vectors between VMs
- Validates console access restrictions and management interface security

Example Risk Covered
An attacker escalates from a low-privileged user on a misconfigured guest VM to gain access to the hypervisor and control other VMs.

Container Security Assessments

Assessment of Docker, Kubernetes, or similar environments to identify misconfigurations, excessive permissions, and runtime risks.

Benefits

- Validates isolation and namespace controls
- Identifies vulnerable orchestration or secret handling practices
- Prevents container escapes or abuse of misconfigured services

Example Risk Covered
A container running with root privileges is compromised, allowing the attacker to break out of the container and control the underlying node.

Secure Code Review

Manual and automated analysis of source code to uncover security flaws such as injection issues, insecure APIs, or poor cryptographic use.

Benefits

- Reduces risk early in the development lifecycle
- Strengthens SDLC and secure development practices
- Provides targeted remediation advice for developers

Example Risk Covered
A critical authentication routine lacks proper input validation, allowing attackers to bypass login controls using crafted payloads.

Red & Purple Team Operations

Cyberfort
Expert-led. Security Driven.

Red Team Engagements (Including Assumed Breach)

- Adversary emulation using real-world TTPs
- Persistence, lateral movement, and exfiltration
- Blue Team detection and response evaluation

Benefits

- Identifies blind spots in your detection and response capabilities
- Provides realistic validation of incident response readiness
- Demonstrates risk to leadership using real-world scenarios

Example Risk Covered
A simulated APT actor uses phishing and credential harvesting to gain a foothold, maintains access for 21 days without detection, and exfiltrates intellectual property from R&D servers.

Cyber Essentials & Cyber Essentials Plus

- Readiness assessments
- Configuration audits
- Independent CE+ testing against IASME requirements
- Remediation and certification support

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

Purple Team Engagements

- Collaborative, MITRE ATT&CK-based threat simulation
- Detection tuning and SOC hardening support
- Real-time threat validation with your internal team

Benefits

- Aligns offensive testing with defender capabilities
- Accelerates maturity of SOC and detection engineering teams
- Promotes cross-team collaboration and knowledge sharing

Example Risk Covered
Simulated lateral movement using PowerShell Remoting exposes gaps in log correlation and detection. SOC analysts receive real-time coaching to detect and respond effectively.

Deliverables Across All Services

- Tailored reports with executive summaries
- Technical details with POCs and CVSS scoring
- Clear remediation guidance
- Post-test debrief with your team

Why organisations choose Cyberfort for Penetration Testing

In an age where cyber threats are more sophisticated, persistent, and damaging than ever, organisations can no longer rely on reactive security. At Cyberfort, we deliver expert-led penetration testing services that simulate real-world attacks to uncover vulnerabilities before malicious actors do. Our CREST and CHECK-certified team combines deep technical knowledge with operational experience to help you protect critical assets, maintain compliance, and strengthen trust — all while supporting your organisation's secure growth.

Cyberfort's penetration testing services are more than just a box-ticking exercise, they are a strategic investment in your resilience. Whether you're defending against nation-state threats, validating internal segmentation, or preparing for certification, our tailored assessments provide the insight and assurance needed to stay ahead of evolving risks. Our solutions mean you'll take control of your cyber security posture with confidence, clarity, and capability.

Cyberfort
Expert-led. Security Driven.

For more information on our Penetration Testing services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you