Introducing boxxe's PenTesting service in partnership with CyberCrowd

The penetration testing service in partnership with CyberCrowd provides proactive, independent security assurance that finds and helps fix the weaknesses in your environment that matter most.

Our Penetration Testing Service combines boxxe's public sector delivery expertise with CyberCrowd's accredited testing capability to assess real-world attack paths across your external perimeter, internal network, cloud controls and critical configurations – including Microsoft 365 and Azure firewalls. The service leverages recognised methods, risk-rates findings, and delivers practical remediation guidance your teams can act on.

Assurance & Accreditation:

Delivered in partnership with CyberCrowd who hold CREST certification, NCSC Cyber Assured status, and audits against ISO 27001 and IASME Cyber Assurance.

What the Service Provides

- External infrastructure testing – evaluates internet-facing assets and defences.
- Internal infrastructure testing – simulates an insider/compromised device scenario across your LAN/WAN.
- Configuration reviews – targeted assurance for Azure Firewall and on-prem firewall configurations.
- Microsoft 365 security review – assessment against industry benchmarks to surface misconfigurations and risks.
- AI & LLM environment testing – specialist checks for emerging AI/LLM attack surfaces.

Scope	Typical Focus	Outputs
External Infrastructure Test	Internet-facing IPs, services, platforms	Executive Summary, CVSS-rated Vulnerability Matrix, exploitation evidence, remediation guidance
Internal Infrastructure Test	LAN/WAN segments, AD-joined hosts, internal services	Attack path analysis, configuration weaknesses, CVSS-rated findings, remediation guidance
Microsoft 365 Security Review	Tenant baseline, identity, device & data protections	Benchmark-driven findings and hardening recommendations

Firewall Config Review (Azure/on-prem)	Rule base, objects, NAT, threat intel settings	Misconfiguration analysis and policy/rule improvements

DELIVERABLES:

- Executive Summary for non-technical stakeholders.
- Vulnerability Matrix with CVSS-based risk scoring.
- Technical Findings & Evidence, including attack path narratives and affected assets.
- Actionable Remediation Guidance aligned to best practice.

Who the Service Is For

Central Government, Agencies and Arms-Length Bodies who need independent assurance of internet-facing services and internal networks.

Local Authorities, Blue Light and health organisations adopting Microsoft 365, Azure and hybrid architectures who want configuration-focused testing.

Any Public Sector teams experimenting with AI/LLM who require specialist testing of new attack surfaces.

Why boxxe

boxxe brings proven framework delivery discipline and the governance Public Sector buyers expect, paired with CyberCrowd's specialist testing team who offer independent, accredited expertise.

Assessments are performed to recognised standards with clear, evidence-backed reporting and risk scoring against CVSS with actionable outcomes and findings that translate directly into practical hardening steps across your infrastructure, Microsoft 365 and firewall controls.

Customer Problems Solved

- Unknown exposure on your internet perimeter – we identify externally exploitable weaknesses before adversaries do.
- Insider/compromised device risk – we reveal lateral-movement paths and control gaps inside your network.
- Misconfigurations in cloud and security controls – we surface issues in Microsoft 365 and Azure or on-premises firewalls that allow privilege escalation or data exposure.
- Stakeholder alignment – executive-level summaries make risk understandable, prioritised and fundable.

Customer Benefits & Outcomes

- Clarity on real-world risk with CVSS-rated issues and a consolidated Vulnerability Matrix.
- Faster remediation through specific, evidence-based guidance that maps directly to control changes.
- Assurance you can stand behind with delivery from an accredited Pen-tester with NCSC-recognised credentials.

Approach & Methodology

1. **Scoping & Discovery:** Confirm objectives, in-scope assets, timeboxes, escalation paths and authorised testing windows.
2. **Reconnaissance & Threat-led Testing:** We combine automated tooling with manual techniques to discover, validate and exploit realistic attack paths.
3. **Risk Rating & Analysis:** Findings are classified and prioritized using CVSS, consolidating results in a Vulnerability Matrix with business impact context.
4. **Reporting & Recommendations:** We deliver an executive summary, technical detail, and step-by-step remediation guidance suitable for infrastructure, Microsoft 365 and firewall teams to take rapid action.
5. **Optional Targeted Re-test & Verification:** Following attempted remediation, we can re-test specific areas to validate risk reduction and close findings.

Pricing Model

Services are provided on a day rate.

Please see separate Pricing Document.

Why Customers Choose This Service

Public Sector buyers choose this service because it blends boxxe's trusted Public Sector expertise with CyberCrowd's independent, accredited, hands-on testing. You can be confident of a partner who already operates to UK Government standards, and the clarity from reports that translate quickly into practical change across infrastructure, Microsoft 365 and firewall controls.

Customers also value the way we communicate risk. Findings are risk-rated with CVSS, grouped in a simple matrix, and accompanied by evidence-based and step-by-step remediation advice, so security, IT operations and leadership can align on what to fix first and why.

Finally, our flexbilirty allows us to focus where you need assurance most – from classic external and internal tests to targeted configuration reviews and emerging AI/LLM environments. This approach provides assurance that evolves with your architecture and threat landscape.