Cyberfort
Expert-led. Security Driven.

Rapid Pen Test Sprint

Targeted penetration testing with executive-ready reporting

Introduction

Cyber attackers do not wait for the right moment. Vulnerabilities in applications, cloud environments and external infrastructure are actively and continuously probed, often within hours of exposure. Yet many organisations either delay penetration testing because of the perceived complexity and cost of traditional engagements or carry out superficial scans that fail to identify real, exploitable weaknesses.

The result is a false sense of assurance, systems that have never been properly tested against realistic attack techniques, and leadership teams that cannot honestly answer the question "could we be breached through this?"

The Challenge

Industry research shows that 70%+ of successful breaches exploit known, unpatched vulnerabilities, weaknesses that structured penetration testing would have identified. Yet fewer than half of mid-sized UK organisations conduct annual penetration testing, and many of those that do, rely on automated scanning alone, which misses the logic flaws, misconfigurations and chained vulnerabilities that skilled attackers actively exploit.

The cost of discovering a vulnerability through a pen test is a fraction of the cost of discovering it through a breach. The average cost of a UK data breach now exceeds £3.4 million, and that figure does not account for regulatory fines, customer attrition or reputational damage.

These statistics point to the same root cause: penetration testing has historically felt too slow, too expensive and too disruptive for organisations without a dedicated security team. The Rapid Pen Test Sprint service by Cyberfort is designed to remove every one of those barriers.

What our customers say about this service

"We had a new customer portal going live and needed independent assurance before launch. Cyberfort scoped and completed the test quickly, and the executive report gave our board exactly what they needed. Two critical findings were caught before go-live, findings our internal team had missed entirely."

Head of Technology Solutions, Financial Services Organisation

"Our cyber insurer required evidence of penetration testing at renewal. We had six weeks. Cyberfort turned it around with time to spare, and the report format was exactly what the insurer asked for. We'll be doing this annually from now on."

IT Director, Professional Services Firm

"We'd had a security incident and the board wanted to know if there were other weaknesses in our external estate. The Rapid Pen Test Sprint gave us that answer quickly, without the disruption of a large engagement. The findings were sobering but the remediation guidance was practical and clear."

Group Risk Director, Car Manufacturer

This service becomes particularly relevant in the following situations

A new application, API or cloud environment is approaching go-live and has not been independently tested

A customer, insurer or regulator has asked for evidence of recent penetration testing

Cyber insurance renewal requires proof of security assurance activity

A compliance deadline is approaching (ISO 27001, PCI DSS, SOC 2, DORA)

A previous pen test found critical findings and the organisation needs to validate remediation

M&A due diligence requires a rapid assessment of the target's external attack surface

A recent security incident has raised questions about wider vulnerability exposure

Who is this service for?

This service is designed for **IT Directors, Heads of Security, CTOs, and Compliance Managers** in organisations that need to validate their security posture quickly, without committing to a large-scale, open-ended testing programme.

Ask yourself: Do you have a new application, cloud environment or external-facing system that has never been independently tested? Are you approaching a compliance deadline, an insurance renewal or a customer audit that requires evidence of security testing? If so, this service is built for you.

What a typical Rapid Pen Test engagement looks like

1

Step 1 - Scoping & Rules of Engagement

We work with you to define the exact scope, including the systems, applications, environments or IP ranges to be tested. Rules of engagement are agreed and a testing window is confirmed. This step requires minimal effort from your team and ensures the test is tightly focused on what matters most.

2

Step 2 - CREST-Aligned Penetration Testing

Our CREST-qualified testers conduct structured, manual-led penetration testing against the agreed scope. This goes beyond automated scanning to include exploitation attempts, privilege escalation, lateral movement testing and business logic analysis, the techniques real attackers use. Testing is conducted with minimal disruption to live environments.

3

Step 3 - Findings Analysis & Risk Prioritisation

All identified vulnerabilities are assessed for exploitability and business impact. Findings are rated by severity, with clear context provided for each, not just what was found, but what an attacker could do with it and why it matters to the business.

4

Step 4 - Executive & Technical Reporting

Two reports are produced: a concise Executive Summary for board and leadership consumption, covering the overall risk posture and the highest-priority actions; and a detailed Technical Findings Report for the security or IT team, including full vulnerability details, evidence, and step-by-step remediation guidance. An optional retest is available to validate that critical findings have been successfully remediated.

Key deliverables

- CREST-aligned Penetration Testing
- Executive Summary Report
- Technical Findings Report with remediation guidance
- Risk-prioritised vulnerability register
- Optional Retest to validate remediation

Business Value

- Identify exploitable vulnerabilities before attackers do
- Validate security posture against realistic, current attack techniques
- Satisfy compliance, insurance and customer assurance requirements
- Prioritise remediation spend on the vulnerabilities that matter most
- Provide board-level confidence in your security posture

Outcomes which can be achieved by using this service

- A clear, evidenced picture of your real-world vulnerability exposure
- Prioritised remediation guidance - the highest-risk issues first, with practical fixes
- Board-ready reporting that translates technical findings into business risk
- Confidence that your systems have been tested against the techniques real attackers use
- Evidence of independent security testing for compliance, insurance or customer assurance purposes

Why use Cyberfort for Rapid Pen Testing

Cyberfort's penetration testing team combines CREST-certified expertise with a deep understanding of the threat landscape facing UK mid-market and enterprise organisations. Our testers are not just technical, they think like attackers, and they communicate like business advisers.

Every engagement is scoped to deliver maximum insight with minimum disruption, and our dual reporting model means findings land with the right audience: the board gets the risk story, the technical team gets the fix list.

We combine offensive security skills with the broader Cyberfort capability, meaning findings don't sit in isolation. Where a Rapid Pen Test Sprint surfaces systemic issues, our managed services and advisory teams are on hand to help you act on them.

Next Steps

Don't wait for an attacker or an auditor to find what your systems are exposing. Book a 30-minute call with one of our penetration testing specialists by emailing **info@cyberfortgroup.com**. On the call they will define your scope, understand your options, and give you independent assurance on the systems that matter most to your business.

For more information about Cyberfort security services visit **cyberfortgroup.com**.