See What Others Miss: Penetration Testing That Drives Real Security Outcomes

In today's fast-moving digital world, security blind spots are inevitable. With mobile workforces, cloud adoption, and complex networks, it can be challenging to see where all your vulnerabilities lie. Without true visibility, you can't measure your security or plan effective defences. Recent high-profile exploits and attacks prove just how critical this is.

Sapphire's Testing services go beyond ticking the compliance box. We deliver actionable insights, not just lists of vulnerabilities. Our expert, CREST and CHECK-accredited team provides the clarity you need to understand your risks and the confidence to address them—before attackers do.

Flexible Service Options

Project-based Service

On-demand, real-world attack simulations to identify vulnerabilities in your systems, networks, or applications—ideal for compliance or one-off needs.

Subscription Service

On-demand testing and retesting of critical or newly deployed assets throughout the year. Stay ahead of threats and maintain a strong, adaptive security posture.

Key Benefits

- ✓ Actionable insights
- ✓ Comprehensive reporting
- ✓ Faster Remediation
- ✓ Improved visibility
- ✓ Compliance support
- ✓ Cost-effective

You will benefit from:

Advanced, Thematic Reporting: Going beyond surface-level findings, we analyse historical test data to highlight recurring issues and inform long-term improvements.

Tailored Insights: Reports are customised for your environment, making it easy for all stakeholders to understand and act.

Expert-Led Assurance: Our multi-disciplinary team delivers the visibility and assurance you need to drive measurable improvement.

Extended Service Offering

Security Improvement & Remediation

Less than half (48%) of pentest findings get resolved. We don't just find problems—we help you fix them. Sapphire provides pathways to resolution, helping customers overcome recurring issues and drive real progress.

Why Choose Sapphire?

Actionable Insights: We don't just find issues, we show you what matters and how to fix it.

Comprehensive Reporting: Clear, contextualised reports for both technical teams and business leaders.

Faster Remediation: Prioritised findings and guidance to accelerate your response.

Improved Visibility: See your environment as attackers do, closing security gaps.

Compliance Support: Meet regulatory and certification requirements with ease.

Cost-Effective: Get maximum value and measurable improvement from your security investment.

Flexible Service Options: From annual or standalone tests to year-round testing, with the cost spread across the term of the contract.

Driving Results for Your Business

With Sapphire's testing services, you build a resilient security posture that evolves with the threat landscape. Our continuous visibility and expert guidance empower your teams to stay secure, compliant, and confident

Don't wait for a breach to reveal your blind spots. Speak to us today.

Penetration tests are performed based on an organisation's objectives and threat profile. Below are some of the common types of penetration tests we provide.

CHECK Testing	**Internal Testing**
Enhances the availability and quality of the NCSC approved IT health check services that are provided to government in line with HM Government policy.	Identifies weaknesses in the security of computer systems connected to the internal network, including workstations, servers and network equipment.
External Testing	**Web Application Testing**
Identifies potential weaknesses in the security of your systems and technology at your perimeter.	Comprehensively assess web applications for vulnerabilities that can lead to unauthorised access or data exposure.
API Endpoint Testing	**Mobile Application Testing**
Verifyies the functionality of individual endpoints within an application's API.	Comprehensively assesses the security of mobile devices and installed applications available from the relevant store.

Cloud Assessments	Active Directory
Evaluates the security posture of your cloud environments, including configuration reviews, identity and access management, logging, monitoring, and adherence to best-practice frameworks across platforms such as Azure, AWS, and Google Cloud.	Asses the security and resilience of your Active Directory environment, identifying misconfigurations, excessive privileges, insecure authentication methods, and opportunities for lateral movement or privilege escalation.
Container Assessments	**Network Devices**
Review containerised environments such as Docker and Kubernetesfor vulnerabilities, insecure configurations, exposed services, and weaknesses within images, registries, and orchestration platforms.	Examines the configuration and security of routers, switches, firewalls, and other network appliances to identify weaknesses that could allow unauthorised access, misrouting, or disruption of services.
Mobile Device Reviews	**Physical Assessments**
Evaluates the security of mobile endpoints and applications, including device configuration, OS versioning, management profiles, and application permissions to ensure alignment with organisational security policies.	Assesses the physical security controls protecting your sites and infrastructure, including access controls, surveillance, environmental protections, and potential risks related to on-site intrusion or tampering.

CREST SECURITY TESTING
Penetration Testing

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS

CYBER ESSENTIALS CERTIFIED PLUS