

What is Security Testing

Security weaknesses can be hard to identify and remediate. Infrastructure penetration tests, web application tests, and mobile application tests use the tactics and tools that a real-world attacker would use on your systems and help you to identify weaknesses and remediation steps needed to fix vulnerabilities. Firewall and end point configuration reviews identify what is required to harden your security posture at the network boundary and on user devices.

How does it work?

Our security testing team will start by discussing your requirements and recommending suitable testing services. We'll then scope the testing and provide you with a statement of works. The testing team will agree testing dates and key contacts and carry out the work. Once completed we will draft a report setting out our findings and recommendations and arrange a call with you to talk you through the report and discuss next steps.

KEY FACTS

- Comprehensive detailed testing of your infrastructure or applications
- Flexible one-off or managed testing services delivered over 12 months
- Clear easy to understand reporting with clear remediation priorities
- Supportive consultants on hand to discuss findings and recommendations
- Reassuring access to Softcat cyber security experts

What are the benefits?



Infrastructure Testing - Internal & External



Security testing for your internet facing network and for your internal infrastructure to test and improve your network boundary security and your internal infrastructure defences. Detailed reporting including risk prioritisation and clear remediation advice.





Web Application Testing

Web application security testing for weaknesses including those in the OWASP Top 10 critical application risks including injection flaws, authentication issues, security misconfiguration and sensitive data exposure.



Mobile Application Testing

Security testing for your iOS and Android mobile apps to industry standards to identify vulnerabilities including insufficient cryptography, insecure communication, and improper platform usage with detailed reporting and clear remediation guidance.



Firewall Configuration & Ruleset Review

Review of your firewall setup and ruleset to identify weaknesses and improvements, covering configurations, access rules and security policies and providing prioritised remediation advice and detailed reporting.



End Point Security Configuration Review

Build configuration reviews and remediation advice for servers, workstations and laptops to ensure your end points are securely configured and hardened and meet compliance requirements and standards including CIS, NIST, Cyber Essentials and ISO 27001.

WHY SOFTCAT



- Best practice industry standard testing methodologies
- Tried and tested experienced testers and consultants
- Post-test assurance support when remediating issues
- Flexibility bespoke testing services to meet your objectives.

