SERVICE DEFINITION DOCUMENT
MOBILE APPLICATION PENETRATION TESTING

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- to reduce the risk of significant security incidents
- to speed up the detection and containment of threats, and
- to demonstrate robust governance to stakeholders such as boards, auditors, and insurers

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Local authority — Payments and booking app with logic flaws

JUMPSEC reviewed the booking and payment workflows and discovered mass assignment vulnerabilities on profile updates, as well as incomplete server-side checks for discounts and fee waivers. We found that the rate-limits permitted repeated attempts on payment retries, and error handling disclosed partial PII.

We remediated these issues by restricting update schemas to allow-lists, enforcing server-side validation for discounts, and introducing per-endpoint throttling. JUMPSEC also implemented generic error response patterns with correlation IDs. Our verification showed that updates were controlled, rates were predictable, and exposure of personal data was reduced.

National retailer — loyalty and payments app exposing account takeover paths

We assessed the consumer app and identified weak rate-limits on the login and OTP endpoints, encountered verbose error flows that confirmed account existence, and discovered deep links that accepted manipulated parameters. JUMPSEC found that API calls allowed password reset token reuse and lacked device binding for high-risk actions.

We remediated these issues by enforcing strict throttling with progressive delays, standardising non-enumerative errors, and validating deep-link intent server-side. JUMPSEC updated password reset flows to adopt single-use tokens with short lifetimes and added device binding for payment and profile changes. When we re-tested, we found that enumeration was blocked, reset behaviour was stable, and high-risk actions were controlled.

Service Overview

JUMPSEC conduct manual-first security testing of iOS and Android applications and their supporting APIs. The engagement assesses authentication, authorisation, storage, transport, client integrity, and anti-tamper measures. Testing maps priority user journeys and validates exploitability with safe techniques. Outputs provide reproducible evidence and backlog-ready fixes.

Objectives

- Identify and validate vulnerabilities with clear business impact
- Harden authentication, session management, and authorisation across app and API
- Reduce exposure from insecure storage, transport, and client-side logic
- Provide precise remediation with acceptance criteria and re-test scope

Approach

Testing runs in agreed windows using test builds or production-equivalent environments. Activities include static and dynamic analysis, API testing, and limited reverse-engineering within rules of engagement. Findings emphasise impact, evidence, and practical fixes aligned to delivery pipelines.

Method

- **Plan** — confirm objectives, platforms, builds, test accounts, environments, and evidence handling
- **Discover** — enumerate attack surface, roles, device permissions, API endpoints, and data flows
- **Validate** — confirm exploitability for authn/authz, storage, transport, integrity, and business logic
- **Analyse** — document root cause and preventive patterns for future releases
- **Debrief** — prioritise fixes, owners, and acceptance criteria; agree re-test
- **Improve** — optional re-test to confirm remediation and prevent regression

Deliverables

- Executive briefing (slide deck + debrief) describing key risks, impact, and priorities
- Mobile Application Security Report with evidence, reproduction steps, and exact fixes
- Issue register (CSV/XLSX) listing severity, owners, due dates, and acceptance criteria
- Optional re-testing confirming remediation outcomes
- Standards and alignment (embedded) referencing OWASP MASVS and OWASP Mobile Top 10, CWE mappings, CVSS for severity rationale, and relevant NCSC guidance for citizen-facing services

Outcomes and benefits

- Lower risk of account takeover, data exposure, and fraud
- Stronger controls across app, device, and API layers
- Backlog-ready actions that land cleanly in development sprints
- Assurance artefacts suitable for governance, audit, and stores' review

Pricing model

Fixed price per application and platform or time-and-materials aligned to SFIA. Price drivers include platform count, role complexity, API breadth, environment availability, and re-test needs

Timelines

- Planning and access in 3–5 working days
- Execution based on scope and complexity
- Report issue in 5–10 working days after testing completion
- Optional re-test by agreement

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement** Lead responsible for scope, governance, and quality
- **Mobile Security Tester(s)** responsible for testing and evidence capture
- **Coordinator** managing logistics, supplier comms, and action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Provide builds, provisioning profiles, test accounts across roles, and API documentation

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Use non-destructive validation and minimise service impact
- Handle evidence securely and retain only for agreed periods

- Arrange third-party consents where suppliers or payment providers are in scope

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- Non-destructive testing only and no denial-of-service
- Store policies and signing requirements observed for test builds
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- API Penetration Testing
- Secure SDLC / DevSecOps Assessment
- Source Code Review

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com