SERVICE DEFINITION
API 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, as we provide our clients with clear scopes, well-defined engagement terms, daily testing updates, 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 provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards, supporting clients in highly regulated sectors where security and accessibility are mandatory.

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

Central government — Citizen identity brokerage API

JUMPSEC conducted testing which modelled staff, contractor, and citizen flows across OAuth/OIDC. Assessors found weak redirect handling, inconsistent request-freshness checks, and scope creep between relying parties. The recommended remediation actions introduced strict redirect allow-lists, robust token validation, and least-privilege scopes, and re-testing showed stable authorisation and cleaner audit trails.

NHS Trust — EPR and e-Referral interfaces

Our assessment covered patient, clinician, and admin roles across FHIR-style endpoints. The issues JUMPSEC identified included BOLA on appointment objects, verbose errors, and weak input validation. Recommended remediation actions enabled to client to prioritise object-level checks, error sanitisation, and schema allow-lists. Verification confirmed correct role isolation and reduced information leakage.

Energy network operator (CNI) — Telemetry and maintenance APIs

JUMPSEC's review focused on device registration, telemetry ingest, and engineer workflows. Testing revealed mass assignment on device profiles, weak key rotation, and missing rate-limits. JUMPSEC provided several remediation actions, including strict field allow-listing, short-lived tokens with rotation, and per-endpoint throttling. Follow-up testing evidenced controlled updates and resilient throttling.

Local authority — Revenues and benefits partner APIs

The engagement targeted tenancy boundaries and supplier callbacks. Findings included ID enumeration via error codes, JWT claim handling gaps, and permissive webhook allow-lists. JUMPSEC's recommended remediations added consistent error handling, stricter claim verification, and validated callback domains. Re-test confirmed blocked enumeration and safer partner integrations.

Service Overview

JUMPSEC conducts manual-first security testing of APIs to identify exploitable weaknesses in authorisation, data handling, and abuse resistance. Our assessment covers endpoint coverage, object relationships, token flows, schema validation, and error handling. Findings are reproducible and prioritised with clear remediation guidance suitable for engineering backlogs and governance packs.

Objectives

- Identify and validate exploitable AP
- Identify weaknesses with evidenced impact
- Provide reproducible requests/responses and precise fix guidance
- Reduce recurrence by addressing schema, authorisation, and control gaps
- Support governance with risk-based prioritisation and traceable outcomes

Approach

Our testing approach respects data sensitivity, roles, scopes, and partner integrations. Activities run in safe environments and approved windows using non-destructive techniques. JUMPSEC ensure representative accounts and datasets are used to demonstrate impact without affecting production.

Method

- **Plan** — objectives, scope, data classes, environments, and windows
- **Test** — assess authentication, authorisation, endpoint exposure, schema, and error handling
- **Abuse testing** — evaluate rate-limits, enumeration paths, and misuse of w orkflow steps
- **Validate** — demonstrate impact using controlled data and reproducible steps
- **Debrief** — classify severity, document fixes, and outline secure patterns
- **Improve** — optional re-test to confirm remediation and prevent regression

Deliverables

- Executive summary highlighting key risks and priorities
- Technical report with evidence (requests/responses, screenshots, payloads)
- Issue register (CSV/XLSX) with severity, owners, and due dates
- Optional re-test letter confirming remediation status

Outcomes and benefits

- Stronger authorisation across object relationships and tenants
- Safer data handling with tighter schemas and sanitised errors
- Backlog-ready remediation tasks with clear acceptance criteria
- Governance artefacts suitable for audit and assurance reviews

Pricing model

Fixed price per application/scope or time-and-materials aligned to SFIA. Price drivers include auth complexity, integration count, environment availability, required artefacts, and optional re-testing.

Timelines

- Planning and access: 3–5 working days
- Execution: per agreed scope and complexity
- Report issue: 5–10 working days after testing completion
- Optional re-test: typically, 30–60 days post-remediation

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** — scope, governance, quality management, stakeholder alignment
- **API Security Tester(s)** — testing and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Provide API documentation, schemas, and test accounts/tokens
- Supply environment access, sample datasets, and integration details
- Arrange third-party consents where partner endpoints are in scope

JUMPSEC responsibilities

- Operate within rules of engagement and change control
- Use non-destructive techniques and agreed abort criteria
- Secure handling and time-boxed retention of data and artefacts

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

- No denial-of-service or production data modification
- Third-party participation requires prior written approval
- 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