SERVICE DEFINITION
SOURCE CODE REVIEW

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

NHS provider — Input handling and deserialisation in integration services

We identified that code handling HL7/FHIR transformations used permissive YAML deserialisation and did not fully sanitise user-controlled fields that were passed to database queries. JUMPSEC retained legacy libraries due to build constraints, and IaC templates exposed public storage for staging artefacts.

JUMPSEC replaced unsafe deserialisation with vetted parsers, added parameterised queries with strict encoding, and modernised dependencies. We closed public storage in IaC and introduced signed URLs for short-lived artefact access. In our follow-up, we validated that injection paths had been closed and that clinical payloads were handled more securely.

Local authority — secrets and configuration hygiene

We found that repositories contained long-lived API keys and connection strings in appsettings files and CI variables. JUMPSEC observed that build logs echoed sensitive values and commit history revealed historic secrets. We noted that CSP and CORS settings defaulted to permissive patterns in production.

JUMPSEC migrated secrets to managed stores with short-lived access, rotated compromised material, and prevented secret echo in logs. We adopted strict defaults for security headers with environment-specific overrides. After re-assessment, we confirmed that repositories were clean, configurations were constrained, and safer defaults were in place.

Energy supplier (CNI) — business logic and privilege escalation

We discovered that a billing platform permitted users to alter tariff identifiers by manipulating payloads. JUMPSEC observed that server-side checks depended on client assertions, and the use of shared code resulted in admin and user roles being mixed. We also found that feature flags exposed privileged routes during staged rollouts.

JUMPSEC introduced server-side validation using authoritative sources, separated admin and user route guards, and enforced flag scopes. We enhanced testing by adding negative cases for privilege boundaries, and our verification confirmed that we robustly enforced business rules and reduced the risk of privilege escalation.

Service Overview

JUMPSEC conduct a manual-first, context-aware review of source code for security weaknesses across application and infrastructure layers. The engagement evaluates authentication, authorisation, input handling, error management, cryptography, secrets, and business logic. It also inspects supporting artefacts such as configuration, Infrastructure as Code, pipelines, and dependency manifests. Findings include precise code references, exploitability rationale, and backlog-ready remediation.

Objectives

- Identify defects with clear business impact and exploitability
- Improve defensive patterns and eliminate recurring weakness classes
- Strengthen secrets, crypto, and configuration hygiene across environments
- Provide actionable fixes with acceptance criteria and verification steps

Approach

Review aligns to business context, threat models, and technology stack. Activities combine static analysis tooling with deep manual inspection focused on trust boundaries and high-risk paths. Supporting artefacts (IaC, CI/CD, container files) are in scope where supplied. Delivery uses read-only access and agreed handling of sensitive materials.

Method

- **Plan** — confirm objectives, codebase scope, languages, frameworks, and artefacts; define evidence handling and escalation
- **Map** — understand architecture, trust boundaries, identity flows, data objects, and critical journeys
- **Inspect** — perform manual review augmented by targeted SAST; assess crypto use, input handling, authn/authz, error models, and secrets
- **Broaden** — review dependencies, configuration, IaC, container files, pipelines for supply-chain risk
- **Debrief** — present issues with code pointers, fixes, owners, and acceptance criteria; agree re-test or PR support

Deliverables

- Executive briefing (slide deck and debrief): key risks, affected components, priority actions
- Code Review Report: per-finding code locations, exploitability, and exact remediation; coverage notes for authn/authz, input handling, error models, crypto, secrets, file handling, SSRF, deserialisation, and logic
- Patch-ready guidance: secure patterns, code snippets, and guardrails for future commits

- Dependency and configuration register (CSV/XLSX): vulnerable packages, risky settings, owners, due dates, acceptance criteria
- Optional pull-request support or re-test letter: validation of fixes and secure patterns
- Standards and alignment (embedded): OWASP ASVS/Top 10, OWASP ASRM/SAMM, CWE mappings, SEI CERT guidelines, SLSA supply-chain concepts, and relevant NCSC guidance referenced for rationale

Outcomes and benefits

- Reduced risk of exploitable defects and faster remediation
- Repeatable secure patterns that improve developer velocity
- Tighter secrets, crypto, and configuration management
- Assurance artefacts suitable for governance, audit, and release gates

Pricing model

Fixed price per repository or module band, or time-and-materials for larger monorepos. Price drivers: language mix, LOC and module count, dependency breadth, IaC/pipeline scope, and re-test or PR support.

Timelines

- Planning and access: 1 week
- Review and analysis: 1–3 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional re-test or PR review

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
- **Application Security Reviewer(s)** — manual review, SAST triage, evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a single engagement lead and technical owners
- Provide access to repositories (read-only), build instructions, and environment context
- Share architecture diagrams, data flows, threat models, and critical user journeys where available

JUMPSEC responsibilities

- Operate within agreed rules of engagement and evidence handling
- Minimise disruption and protect intellectual property
- Retain artefacts only for agreed periods and support secure destruction or return

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

- Read-only repository access or supervised sessions where required
- Third-party code and licensed components reviewed on a best-efforts basis per licence terms
- Third-party participation requires prior written approval
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Secure SDLC / DevSecOps Assessment
- Web, API, Mobile, and Thick Client Penetration Testing
- Cloud-Hosted Application Penetration Testing

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com