SERVICE DEFINITION

SECURE SDLC / DEVSECOPS / PIPELINE ASSESSMENT

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 software provider — Secret sprawl and runner permissions

We discovered repositories and CI variables containing long-lived credentials that teams had shared widely. JUMPSEC found that self-hosted runners used overly broad machine permissions and persistent workspaces, which allowed artefacts to leak between jobs.

To address these risks, JUMPSEC migrated secrets to a vault with short-lived federation, scoped runner permissions to least privilege, and used ephemeral runners to isolate workspaces. In follow-up, we confirmed that secret exposure had reduced and build isolation had tightened.

Energy supplier (CNI) — Dependency and container hygiene

We scheduled dependency scanning, but it did not block vulnerable builds. JUMPSEC left base images unpinned, and we allowed registries to deploy outdated images. We changed our approach by pinning and signing base images.

JUMPSEC enforced SCA and container scan gates with exception lifecycles, and we blocked the deployment of deprecated artefacts. During re-assessment, we evidenced lower exposure to vulnerable packages and achieved predictable image provenance.

Local authority — Branch protection and review governance

We allowed direct pushes to main on critical services and permitted team members to self-approve pull requests. JUMPSEC ran security tests after merges, which limited our ability to catch defects early.

To address this, JUMPSEC enforced branch protection with mandatory reviews, required status checks for security tests before merging, and implemented code-owner rules for sensitive components. In follow-up assessments, we observed higher-quality reviews and reduced the number of security defects escaping into production.

Food manufacturer — recipe IP protection and CI/CD hardening

We found long-lived credentials in Git and CI variables, unsigned containers from shared runners, secrets in build logs, and broad deployment access to cloud storage. Staging and production used the same base images, leading to outdated deployments, while security tests ran post-merge, letting defects through.

To fix this, we moved secrets to a vault with short-lived authentication, enforced signed container images, limited deployment privileges, required mandatory branch reviews, and added pre-merge security scans. Registry policies blocked outdated images and enforced version pinning. After follow-up checks, we saw secure logs, verified artefacts, and minimized IP risk across manufacturing and supplier systems.

Service Overview

JUMPSEC conduct an independent assessment of the software delivery lifecycle across planning, build, test, release, and operate stages. The engagement examines developer workflows, branch and review policies, CI/CD pipelines, dependency and container hygiene, artifact signing, environment segregation, and secret management. Outputs prioritise high-value control improvements with clear owners, acceptance criteria, and change checkpoints aligned to engineering cadence.

Objectives

- Reduce supply-chain risk by strengthening provenance, signing, and artifact trust
- Eliminate secret sprawl and enforce short-lived credentials across delivery systems
- Embed effective security gates: SAST, SCA, IaC, container scanning, and DAST where relevant
- Align least-privilege access for developers, runners, and deployment identities
- Provide backlog-ready improvements with measurable acceptance tests

Approach

Assessment uses read-only access to repositories, pipeline definitions, runners/agents, registries, and deployment targets. Workshops map delivery flows, trust boundaries, and exception paths. Changes are designed to land with minimal friction, favouring platform-native controls and policy-as-code.

Method

- **Plan** — confirm objectives, in-scope repos/pipelines, environments, stakeholders, and evidence handling
- **Discover** — map delivery flows, identities, secrets, artifact paths, testing gates, and promotion rules
- **Validate** — analyse controls for provenance, signing, dependency hygiene, scanning coverage, and permissions
- **Debrief** — present priorities, owners, sequencing, rollback points, and verification steps
- **Improve** — optional verification sprint to confirm uplift and prevent regression

Deliverables

- Executive briefing (slide deck and debrief) highlighting supply-chain risk themes, priority fixes, and delivery impact
- Secure SDLC & DevSecOps Assessment Report covering repository governance, branch protection and review rules, secret management, CI/CD identity and permissions, artifact signing/provenance, dependency and container hygiene, test-gate coverage and quality, environment segregation, and release promotion controls

- Issue register (CSV/XLSX) listing actions, owners, due dates, and acceptance criteria
- Policy-as-code exemplars for branch protection, runner permissions, artifact signing, and scanning gates
- Standards and alignment (embedded) referencing OWASP SAMM and ASOC practices, SLSA levels for provenance, CIS benchmarks for runners/registries, NCSC supply-chain guidance, and MITRE ATT&CK references where pipeline abuse techniques inform rationale

Outcomes and benefits

- Trusted artifacts from signed, reproducible builds with clear provenance
- Lower likelihood of secret leakage and compromised build infrastructure
- Fewer exploitable defects reaching production through effective quality gates
- Clear ownership and metrics that sustain improvements over time

Pricing model

Fixed price per programme or repo/pipeline band, or time-and-materials for large estates. Price drivers include repository and pipeline count, platform diversity, registry footprint, and depth of artefacts and verification.

Timelines

- Planning and access: 3-5 working days
- Assessment and analysis: 1–3 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification sprint: 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** — scope, governance, quality management, stakeholder alignment
- **DevSecOps Specialist(s)** — technical assessment and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Provide read-only access to repos, pipelines, registries, and deployment platforms
- Share architecture and environment diagrams and identify critical delivery paths
- Arrange third-party consents where managed platforms or suppliers are in scope

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Minimise operational impact and safeguard intellectual property
- Handle evidence securely with time-boxed retention

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-disruptive review using read-only access and test artefacts
- Third-party coordination requires prior written consent
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Source Code Review
- Container / Kubernetes Security Assessment
- 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