SERVICE DEFINITION
CHECK IT HEALTH CHECK (ITHC)

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 — Pre-go-live assurance for citizen services platform

JUMPSEC assisted a council as it prepared to launch a consolidated revenues and benefits portal. Programme governance required a CHECK-aligned ITHC before go-live, so we scoped the engagement to cover web, API, identity, and cloud controls, coordinating supplier approvals. During testing, JUMPSEC identified IDOR vulnerabilities on case attachments, permissive storage policies, and weak Conditional Access exceptions for admin roles.

In the debrief, we sequenced remediation actions: we implemented strict object ownership checks, hardened storage policies with customer-managed keys, and enforced PIM with phishing-resistant MFA for administrators. After re-testing, JUMPSEC confirmed closure of the issues. The accreditation authority accepted our closure statement and the programme proceeded to a controlled go-live.

Central government department — Assurance for accreditation renewal

JUMPSEC supported a department that maintained a multi-tenant data exchange with several ALBs. We focused the ITHC on boundary controls, API isolation, and supplier connectivity. During testing, we discovered inconsistent mutual-TLS verification at one integration and found that a legacy appliance had an exposed management endpoint.

To remediate these issues, we enforced certificate pinning, rotated credentials, and restricted management access to a brokered path with audited elevation. JUMPSEC provided evidence and re-test results to support the department's accreditation renewal without conditions.

Engineering Group — CHECK ITHC ahead of network connectivity

JUMPSEC supported a construction and FM provider as they prepared to connect selected services to a protected network. We delivered a CHECK-aligned ITHC, covering external and internal infrastructure, device build reviews, MDM/Intune policy checks, wireless networks, remote access solutions, and performed authenticated testing on two business applications. Our approach mirrored typical scopes, so we also reviewed firewall rulesets, conducted sample authenticated vulnerability scans, and coordinated supplier approvals, while handling evidence securely and defining a re-test window.

During testing, we identified predictable identifiers and access-control weaknesses in one application, as well as permissive storage and remote access configurations, legacy SMB settings, and stale global exclusions that suppressed meaningful alerts. We responded with an action plan that tightened identity and storage controls, enforced managed identities for service accounts, hardened remote access, and corrected build baselines across a representative host sample. JUMPSEC then re-tested to confirm closure of the issues, supporting the programme's accreditation artefacts and enabling a controlled go-live under governance.

Service Overview

JUMPSEC delivers a formal, CHECK-aligned IT Health Check that provides credible assurance for UK public sector systems. We scope and test external and internal attack surfaces, applications and APIs, and configuration controls using non-destructive methods led by CHECK Team Members/Team Leaders. We align planning, conduct, and reporting to NCSC CHECK expectations and reference relevant NCSC guidance throughout. Where required, we coordinate with accreditation authorities and programme teams so findings land cleanly through governance.

Objectives

- Evidence exploitable weaknesses against NCSC CHECK expectations and UK public sector accreditation needs.
- Validate the effectiveness of technical and procedural controls without disrupting live services.
- Provide precise remediation with owners, acceptance criteria, and verification steps suitable for assurance close-out.
- Support re-test and statement of closure for governance, auditors, and accreditors.

Approach

We begin by confirming system boundaries, business impact, code freezes, and third-party dependencies. We agree safe testing windows and notification paths. We build a threat-led test plan that maps techniques to business impact and NCSC guidance. We execute manual-first testing supported by tooling, capture minimal evidence, and maintain a full audit trail. We debrief with delivery and assurance leads, prioritising fixes that remove whole classes of risk and facilitate timely re-test.

Method

- **Plan** — define scope, authority, stakeholders, safe-to-test criteria, evidence handling, and change windows.
- **Discover** — enumerate assets, trust boundaries, and controls across networks, apps/APIs, cloud components, and identity.
- **Validate** — exercise exploitable conditions with non-destructive techniques; confirm impact with constrained proofs.
- **Analyse** — link each issue to business/assurance risk; define exact fixes and acceptance criteria; prepare re-test plan.
- **Debrief** — present actions, owners, sequencing, and verification artefacts to support accreditation or go-live.

Deliverables

- Executive briefing setting out risk, accreditation impact, and expected posture after remediation.
- ITHC Report (CHECK-aligned) with evidence, reproducible steps, precise remediation, rollback notes where relevant, and acceptance criteria mapped to risk.
- Issue register with owners, due dates, and status for accreditation tracking.
- Optional re-test and or closure statement confirming remediation effectiveness.
- Embedded alignment: NCSC CHECK principles and testing conduct, NCSC cloud security guidance, NCSC logging/monitoring guidance, OWASP ASVS/Top 10 and OWASP API Security Top 10 mappings where applicable, and links to ISO/IEC 27001 control families for governance traceability.

Outcomes and benefits

- Credible, defensible assurance for public sector governance and accreditation.
- Fewer exploitable paths to compromise and clearer isolation choices.
- Actionable fixes that land cleanly through change control with evidence suitable for accreditors.
- Audit-ready artefacts for programme boards, SIROs, and insurers.

Pricing model

Fixed price per in-scope system or environment, or time-and-materials for complex, multi-supplier estates. Drivers include scope breadth (external/internal/app/API/cloud), third-party coordination, data classifications, and re-test depth.

Timelines

- Planning and access preparation: 3–7 working days.
- Execution and analysis: 5–15 working days, dependent on scope and environments.
- Report issue: 5–10 working days after testing completion.
- Optional re-test and closure statement: by agreement.

Team and roles

- Engagement Lead for governance, cadence, and quality.
- CHECK Team Lead / CHECK Team Member(s) for testing and analysis.
- Coordinator for logistics, evidence handling, and re-test scheduling.

Adjacent support is also available from JUMPSEC's NCSC CIR-accredited incident response team if required.

Buyer responsibilities

- Nominate technical and assurance owners; provide scope artefacts, network diagrams, and change windows.
- Arrange third-party approvals (hosting, SaaS, MSPs) and test accounts/data.
- Confirm evidence handling, retention expectations, and report distribution list.

JUMPSEC responsibilities

- Operate under written authority and NCSC CHECK conduct expectations.
- Use non-destructive techniques and minimise operational impact.
- Handle materials securely with least-privilege access, time-boxed retention, and approved destruction/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

- No denial-of-service or business-disruptive testing.
- Live production testing only under explicit agreement and controls.
- Third-party/hosted components require written consent.
- Personnel with BPSS/SC available where required
- Accessible materials available (WCAG 2.1 AA)

Related services

- Compromise Assessment / Threat Hunting Sweep
- IR Readiness Review / Breach Readiness Review
- Response Playbook Development

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com