SERVICE DEFINITION DOCUMENT
INTERNAL NETWORK PENETRATION TEST

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 — Privilege escalation exposing citizen data

JUMPSEC modelled a scenario in which a standard user gained administrative privileges on the council network. We identified weak local admin controls, discovered cached credentials, and noted poor workstation hardening. JUMPSEC then prioritised baseline hardening, improved credential hygiene, and implemented tiered admin models. When we conducted a verification re-test, we blocked escalation paths and found fewer high-risk findings.

NHS Foundation Trust — Lateral movement affecting clinical services

We simulated movement from a compromised endpoint towards domain services and shared drives. During the engagement, JUMPSEC exposed flat network segments, identified the use of legacy protocols, and noted inadequate workstation logging. We then drove segmentation changes, hardened protocols, and improved build baselines. In our follow-up testing, JUMPSEC evidenced restricted traversal and reduced exposure of clinical data.

Retail bank — Relay attacks against legacy protocols

JUMPSEC reproduced NTLM relay from user subnets to privileged interfaces and backup systems during testing. We identified weak SMB signing, permissive firewall rules, and stale service accounts. JUMPSEC prioritised protocol signing, rotated service accounts, and cleaned up firewall rules. When we conducted a re-test, we confirmed that relay attempts failed and privileged paths were more tightly controlled.

University — Misconfigured identity paths into research data

JUMPSEC explored a scenario where privilege escalation occurred through group nesting and excessive rights within file services. We uncovered over-broad groups, unsecured admin endpoints, and unused legacy trusts. JUMPSEC then focused our actions on refining role scopes, isolating admin endpoints, and decommissioning legacy trusts. When we verified the results, JUMPSEC observed that privilege pathways had been reduced and access to sensitive research stores was safer.

Service Overview

JUMPSEC conduct an assessment of internal networks to identify exploitable weaknesses and practical attack paths to sensitive systems and data. Engagements reproduce realistic attacker behaviours under safe operating constraints, focusing on lateral movement, privilege escalation, and bypass of existing controls. Evidence is reproducible, risk-rated, and written for both engineering and senior leadership to support rapid remediation and measurable detection uplift.

Objectives

- Identify and validate exploitable security weaknesses
- Assess segmentation, authentication, and host hardening effectiveness
- Provide reproducible evidence and precise remediation guidance
- Support governance with risk-based prioritisation

Approach

The engagement reflects business context, critical services, and regulatory needs. Activities run in agreed testing windows using non-destructive methods and agreed abort criteria or mitigation strategies to avoid production impact. Stakeholders typically include Technology, Security, and Operations

Method

- **Plan** — objectives, scope, data sensitivities, windows, escalation, evidence handling
- **Discover** — host/service enumeration; configuration and credential analysis (as authorised)
- **Validate** — controlled exploitation to confirm impact and feasibility
- **Debrief** — reproduce steps, classify severity, and prioritise fixes
- **Improve** — optional re-test to confirm remediation

Deliverables

- Executive summary highlighting key risks and priorities
- Technical report with reproducible steps and evidence - CVSS/CWE classification for findings, governance references to NIST CSF and NCSC CAF where appropriate
- Issue register (CSV/XLSX) with severity, owners, and due dates
- Optional re-testing with confirmation of remediation status

Outcomes and benefits

- Reduced internal exposure to common attacker techniques
- Clear, risk-aligned remediation tasks for engineering teams
- Improved assurance for governance, audit, and insurance

Pricing model

Fixed price per scoped engagement, or time-and-materials aligned to SFIA. Variation factors include environment scale, complexity, testing depth, evidence requirements, and re-testing requirements.

Timelines

- Planning and access: 1–2 weeks post project confirmation
- Execution: scheduled within agreed windows
- Report issue: 5–10 working days after assessment 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 can be provided in accessible formats

Team and roles

- **Engagement Lead —** Scope, governance, quality management, and stakeholder alignment.
- **Lead Consultant(s)** — technical testing and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and a single engagement lead.
- Provide documentation, target lists, representative hosts, and access approvals
- Confirm change windows, break-glass contacts, and third-party consents

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Minimise disruption and maintain defined safety/abort criteria
- Secure handling and time-boxed retention of data and artefacts

Data protection and privacy

The buyer remains the data controller; JUMPSEC acts as processor. Only the minimum necessary evidence is collected and retained. Secure transfer, access control, and agreed retention periods apply throughout the engagement.

Constraints and assumptions

- Exercises are non-destructive
- Third-party involvement requires prior written consent
- Data is processed under UK GDPR/DPA with an agreed data location.
- Personnel with BPSS/SC clearance are available where required.

Related services

- Active Directory / Entra ID Configuration Review
- Host / OS Build Review
- Firewall / Segmentation Review

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com