SERVICE DEFINITION DOCUMENT
EXTERNAL NETWORK 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—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

Central government service — Unmanaged subdomains and takeover risk

JUMPSEC assessed a large, multi-domain estate and discovered legacy DNS records and stale delegations that allowed subdomain takeover. We combined passive and active discovery to catalogue candidate hostnames, validated dangling targets, and evidenced the impact with controlled proofs. Our blast radius analysis traced a clear chain from exposure to potential data access, covering session hijack, credential capture, and brand abuse.

We focused remediation on ownership and process rather than isolated fixes. JUMPSEC clarified domain custodianship, applied registry locks to high-risk domains, and updated change request templates to require validation of DNS decommissioning steps. We introduced external monitoring to detect future dangling records and lookalike domains. During the debrief session, we aligned Digital, Security, and Procurement teams on takedown workflows and set SLA expectations for suppliers with delegated zones.

Local authority — Perimeter identity hygiene and MFA expansion

JUMPSEC identified that public authentication portals accepted weak credentials and permitted limited password spraying without swift detection. We documented realistic thresholds for attempts, mapped responses across IdP, email, and remote access, and connected behaviour to a plausible initial access scenario. Our evidence demonstrated how a small number of low-and-slow attempts enabled attackers to establish footholds that evaded basic alerting.

The authority acted on our findings by expanding MFA coverage, tightening conditional access rules, and adjusting lockout policies to frustrate automation without impeding service desks. JUMPSEC introduced detection content for repeated failed attempts by ASN, geolocation, and device fingerprint, which improved signal over noise. After our engagement, metrics showed the team triaged identity-led incidents more quickly, and we added a short playbook addendum to clarify when to revoke sessions, reset tokens, and notify affected users.

Critical national infrastructure supplier — Legacy remote access with excessive reach

JUMPSEC identified an outdated remote access gateway with weak security and significant internal access. After obtaining authorisation, we demonstrated potential attacker movement to critical systems. Our report linked technical risks to operational effects, such as outages and maintenance dependencies, and proposed a phased change plan to minimise disruption.

The gateway was retired and replaced with a secure broker featuring device checks and step-up authentication. Network segmentation limited lateral movement, break-glass procedures were improved, and privileged session monitoring was established. Validation showed a smaller attack surface, better detection of risky admin actions, and clear remote access accountability.

Service Overview

External Network Penetration Testing evaluates the security of internet-facing infrastructure and services under realistic attack conditions. JUMPSEC consultants emulate credible adversaries to identify exploitable weaknesses, demonstrate impact, and present a risk-prioritised remediation plan. Our approach is manual, evidence-led, and informed by current threat activity. Results enable buyers to reduce exposure quickly and convert findings into detection content where appropriate.

Objectives

- **Identify externally exploitable vulnerabilities and misconfigurations**. We pinpoint weaknesses that matter on the public perimeter, such as exposed services, weak authentication, and unsafe configurations, providing clear evidence and affected asset lists to accelerate triage.
- **Evidence realistic attack paths and business impact**. Showing how an attacker could progress from exposure to outcome. JUMPSEC describe the blast radius, affected users or data, and the decision points that would have limited progression.
- **Prioritise remediation by risk, effort, and dependency**. Presenting an ordered plan that balances likelihood, impact, and implementation complexity. We seek to highlight changes that quickly reduce risk without major architecture work.
- **Provide audit-ready artefacts and clear stakeholder communication**. Delivering an executive summary, reproducible technical steps, and an issue register with owners and due dates. This supports governance, insurer discussions, and future verification through re-testing.

Approach

Targets include owned IP ranges, domains, and cloud-hosted perimeter services. Typical components include VPN and remote access, email and secure gateway technologies, web applications and APIs, device management portals, and exposed network services such as SSH, RDP, and databases. Password spraying and credential hygiene checks can be performed also.

Method

- **Planning and rules of engagement.** Consultants confirm targets, windows, escalation contacts, and evidence handling. Dependencies and change-freezes are recorded.
- **Reconnaissance and mapping.** Asset discovery, service fingerprinting, technology identification, and version enumeration establish the attack surface.
- **Analysis and verification.** Automated discovery supports manual testing. Manual techniques validate findings, reduce false positives, and uncover misconfigurations missed by tooling.
- **Controlled exploitation (where authorised).** Exploitation is limited to agreed objectives. Evidence captures include screenshots, request/response pairs, and indicators suitable for SOC use.
- **Impact assessment and risk rating.** Findings are rated using CVSS and business context, including likelihood, blast radius, and compensating controls.

- **Debrief and re-test.** Results are presented to stakeholders. A re-test can confirm remediation and reduce residual risk.

Deliverables

- Executive summary describing key risks, likely attacker routes, and recommended remediation.
- Technical report containing evidence, reproducible steps, and precise remediation guidance.
- Issue register (available in multiple formats) with CVSS, ownership and due dates.
- A debrief session for technical and business stakeholders.
- Optional re-test letter or executive summary confirming the status of fixes and any remaining exposure.

Outcomes and benefits

- Clear visibility of true external risk and the quickest path to reduce it.
- Stakeholder-ready evidence to support governance, assurance, and insurer discussions.
- Detection opportunities and logging improvements derived from observed behaviours.
- Practical guidance that balances risk reduction with operational realities.

Pricing model

Day-rate or fixed-price models are available in line with the SFIA rate card. Price drivers include asset volume, architectural complexity, authorised exploit depth, report format, and re-test scope. Out-of-hours work can be scheduled and may incur additional cost.

Timelines

Typical cadence includes one to two to four weeks for planning and approvals, followed by execution within the agreed window. Reporting is delivered within five to 7 working days from the end of testing. For validity reasons, re-testing is to be conducted within 90 days of report delivery, subject to remediation progress and change windows.

Security and assurance

Engagements are performed by accredited consultants using peer-reviewed methods and internal quality checks. Reporting is reproducible, traceable to raw evidence, and written for both technical and executive audiences. Where the buyer operates Microsoft security tooling, findings can be translated into Sentinel and Defender detection content.

Team and roles

An engagement lead manages scope, governance, and reporting. Senior penetration testers conduct manual assessment and controlled exploitation. An analyst curates evidence, maintains the issue register, and performs quality assurance.

Buyer responsibilities

- Nominate an engagement owner and technical contact.
- Provide target lists, ownership confirmation, and approved testing windows.
- Confirm rules of engagement and escalation paths.
- Secure permission for third-party-hosted targets where required and coordinate any provider notifications.

JUMPSEC responsibilities

- Operate strictly within agreed rules of engagement and change control.
- Minimise service impact and notify the buyer on discovery of critical exposures.
- Preserve chain-of-custody for evidence where relevant to legal or regulatory processes.
- Handle and store data securely and only for agreed durations before verified deletion.

Data protection and privacy

The buyer remains the data controller. JUMPSEC acts as a processor. Only the minimum evidence necessary is collected and retained. Secure transfer, access controls, and agreed retention periods are applied throughout the engagement lifecycle.

Data and credentials are returned or securely destroyed. The final issue register, re-test artefacts, and evidence retention statement are handed over. A short roadmap can be provided to transition findings into hardening or monitoring work.

Constraints and assumptions

- Testing is non-destructive and time-boxed.
- Activities run in approved windows.
- Third-party assets require prior written consent.
- Data is processed under UK GDPR/DPA with an agreed data location.
- Personnel with BPSS/SC clearance are available where required by the call-off
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA).

Related services

- Internal Infrastructure Testing
- Web, API, and Mobile Testing
- Red Teaming and Purple Teaming
- Ransomware Readiness and Simulation
- Compromise Assessment
- Incident Response Retainer

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com