SERVICE DEFINITION DOCUMENT: WIRELESS NETWORK 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

Central government department — Cross-subscription privilege growth

JUMPSEC reviewed multi-subscription Azure estates and exposed overly broad role assignments and management group inheritance, which granted unexpected admin rights. Our teams identified trust policies that permitted lateral use of service principals and unmonitored emergency access accounts.

We scoped roles to workload boundaries, applied policy-driven guardrails, and enforced phishing-resistant MFA on privileged operations. We adopted deny-by-default patterns for management groups, with clear exception lifecycles. Our verification demonstrated constrained privilege paths and a cleaner audit of administrative actions.

Energy network operator (CNI) — Flat peering and shared services

JUMPSEC mapped the network and identified broad VPC/VNet peering, as well as shared services bridging environments with differing risk profiles. We found that security groups and NSGs permitted lateral movement to admin interfaces and logging backends.

We introduced a roadmap that implemented hub-and-spoke segregation, restricted east-west flows to explicit service dependencies, and isolated administration behind brokered jump paths. Our verification confirmed a smaller blast radius and reduced access to privileged services.

Local authority — Secrets management and key governance

JUMPSEC enumerated long-lived credentials in CI pipelines and application settings, identifying weak separation of duties over KMS/Key Vault. We audited trails and found inconsistent key rotation and incomplete alerting for key misuse.

We remediated these issues by migrating secrets into managed stores, enforcing short-lived credentials, and tightening key permissions with dual control. Our teams added alerts on creation, use, and deletion events. Subsequent validation confirmed reliable rotation and improved visibility over sensitive keys.

Service Overview

For a Cloud Infrastructure Assessment, JUMPSEC conduct manual-first security testing of Azure, AWS, and GCP estates to identify exploitable weaknesses in identity, network, data, and platform configuration. This evaluates external exposure, control-plane hardening, intra-cloud pathways, and guardrails such as policies and SCPs. Findings include reproducible evidence and prioritised actions suitable for engineering backlogs and governance packs.

Objectives

- Identify and validate exploitable weaknesses across identity, network, and data planes
- Reduce external exposure by locating risky services, keys, and artefacts
- Strengthen least-privilege, segmentation, and control-plane protections
- Provide clear fixes with rationale and acceptance criteria

Approach

Testing reflects business context, regulatory needs, and provider specifics. Activities run in safe windows and use non-destructive techniques. Read-only access and controlled test accounts support validation without service impact. Where required, third-party participation is arranged in advance.

Method

- **Plan** — Confirm objectives, clouds/accounts/subscriptions, test windows, escalation, evidence handling
- **Discover** — Enumerate identities, roles, policies, networks, storage, secrets, and internet exposure
- **Validate** — Safely confirm exploitability (e.g., privilege growth, data access, lateral paths)
- **Control-plane review** — Sssess guardrails, logging, monitoring, and break-glass governance
- **Debrief** — Classify severity, provide precise fixes, and sequence changes with rollback points
- **Improve** — Optional verification to confirm remediation outcomes

Deliverables

- Executive briefing (slide deck + debrief): key risks, exposure themes, and priority actions
- Cloud Security Report:
    - Identity & Access: IAM roles, trust policies, privilege paths, emergency access
    - Network & Segmentation: VPC/VNet design, peering, route tables, security groups/NSGs
    - Storage & Data: object/blob stores, snapshots, encryption, public access policies

  - Secrets & Keys: KMS/Key Vault policies, rotation, discovery of hard-coded secrets
  - Control Plane: policies/SCPs/Blueprints, guardrails, break-glass, MFA enforcement
  - Logging & Monitoring: audit coverage, tamper resistance, alerting of material events
- Exposure register (CSV/XLSX): issues, severity, owners, due dates, acceptance criteria
- Standards and alignment (embedded): CIS Benchmarks, provider-native guidance (AWS/Azure/GCP), NCSC cloud security principles, and ATT&CK cloud techniques referenced for rationale

Outcomes and benefits

- Reduced external footprint and safer identity pathways
- Stronger segmentation and data protections across environments
- Backlog-ready remediation with measurable checkpoints
- Governance artefacts that support audit and assurance

Pricing model

Fixed price per subscription/account or time-and-materials aligned to SFIA. Price drivers: provider mix, account count, service breadth, artefact depth, and optional verification

Timelines

- Planning and access: 3–5 working days
- Testing and reviews: 1–2 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification review based on findings and recommendations

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
- **Cloud Security Tester(s)** — technical testing and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Provide read-only access, documentation, architecture diagrams, and inventories
- Confirm change windows and arrange third-party consents where required

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Use non-destructive validation and minimise operational impact
- Secure handling and time-boxed retention of data and artefacts

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 activities performed in approved windows
- Third-party involvement requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Microsoft Security Configuration (Azure/Defender/M365/Entra/Sentinel)
- Internal Network Penetration Testing
- Detection Engineering and Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com