SERVICE DEFINITION DOCUMENT
MULTI CAPABILTY CYBER SERVICES

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 — Ransomware affecting citizen services

JUMPSEC provided a unitary authority with a single route to uplift detection, reduce external exposure, and offer assurance to the Audit & Governance Committee. We combined Microsoft-based MXDR (Defender, Sentinel, Entra ID), drove continuous log and detection improvements, implemented Continuous Attack Surface Management, and enhanced incident readiness, incident response, penetration testing, and annual CHECK ITHCs. JUMPSEC established a rolling 30/60/90-day plan, maintained a shared backlog, and hosted monthly service reviews with quarterly outcomes boards. We focused MXDR on alert precision, full sensor coverage, and tailored use-case tuning to mailbox rule abuse, credential theft, archive-and-exfiltration, and lateral movement. Our CASM team proactively hunted typosquats, leaked credentials, exposed storage, and stray services, and we coordinated takedown workflows and DNS changes in advance. To bolster incident readiness, we introduced playbooks, set decision thresholds, and ran executive debrief drills. JUMPSEC mobilised NCSC CIR for urgent responses with a verified chain-of-custody. We delivered penetration tests and ITHCs with clear acceptance criteria and scheduled re-tests aligned to change windows.

In the first year, we fixed log validity issues, established baseline detections, and achieved CASM takedown velocity targets. By the second year, JUMPSEC deepened use-case coverage, tightened privileged access, and embedded restore verification on priority systems. In the third year, we refined steady-state efficiency and prepared handover options. The authority exercised a two-year extension clause, and we delivered targeted surges for elections and major platform changes. JUMPSEC tracked KPIs, including alert precision, MTTD, MTTR, coverage by source, exposure backlog burn-down, mean time to takedown, and remediation closure rates. We used CAF Detect and Respond outcomes to inform the governance narrative. Our evidence packs demonstrated that the authority received earlier, clearer signals, encountered fewer public-facing exposures, and made faster isolation decisions for citizen-facing services. The authority reported cleaner audits, less scrutiny from insurers, and stable operations throughout peak periods.

Central government department — Continuous assurance and surge response

JUMPSEC worked with a department that required a consistent cadence of CHECK ITHCs and application reviews, along with the flexibility to pivot to incident response as needed. We scheduled quarterly ITHCs, carried out monthly application tests, and retained emergency IR mobilisation. We maintained a single governance pack to track remediation closure, CAF outcomes, and expenditure. When an upstream supplier issue arose, we mobilised an IR package under the same contract and evidence model.

NHS provider — Platform hardening, targeted testing and incident response

JUMPSEC and our team combined an IR Retainer, host and OS build reviews, M365 and Entra tenant hardening, and Red Teaming for the trust. We carried out periodic app and API tests to validate secure changes. These outputs evidenced that we improved control coverage without disrupting clinical throughput. We adjusted the backlog to regulatory priorities and responded to audit observations.

Service Overview

JUMPSEC provides a flexible, outcome-driven vehicle to procure any combination of services from the G-Cloud catalogue under a single, governed call-off. We set up a scalable framework that supports small, targeted engagements through to multi-year programmes, combining assessment, testing, engineering, detection, and incident response. We align draw-downs to risk and budget cycles, maintain a shared backlog, and evidence measurable uplift after each work package.

Objectives

- Create a single route to buy that reduces procurement friction and time to value.
- Enable mix-and-match service draw-downs with clear outcomes and acceptance criteria.
- Provide governance, transparency, and audit-ready artefacts across all work packages.
- Deliver measurable control and resilience improvements that align to strategy and frameworks.

Scope (what you can call off)

Any service listed in JUMPSEC's G-Cloud submission, including but not limited to penetration testing (CHECK ITHC), red/purple teaming, application and cloud reviews, detection engineering, MXDR advisory, log validity, ransomware readiness/simulation, incident exercising (NCSC Assured), walk-in IR (NCSC CIR), vCISO, framework maturity assessments, and Microsoft-funded workshops. Each work package is defined by a mini-scope, deliverables, timelines, and fixed price or capped T&M as appropriate.

Supported managed services may include: MXDR on Microsoft stack, Continuous Reconnaissance/CASM, Incident Response Retainer (reactive/proactive), Detection Engineering & Use Case Tuning, vCISO. Each managed service is defined by a mini-SoW: outcomes, KPIs, volumes, SLAs, pricing basis, and exit terms.

One-off onboarding covers design, enablement, and acceptance tests before BAU starts

Approach

JUMPSEC establishes a simple operating model: a shared backlog of approved items, a rolling 30/60/90-day plan, and a cadence for governance and reporting. For each package we confirm outcomes, in/out, assumptions, and acceptance tests; deliver the work with minimal disruption; and verify uplift with evidence. Governance tracks value delivered, risks, and spend against budget lines. The model scales up for surge needs (e.g., incidents, regulatory deadlines) and scales down for focused tasks.

Method

- **Plan:** Stand up the procurement and operating vehicle: onboarding, roles, RACI, commercial model, reporting templates, risk/issue/change logs, and an initial pipeline of candidate packages.
- **Discover:** Gather drivers, dependencies, and constraints for each package; confirm success measures.

- **Deliver:** Execute using the relevant service method (non-destructive, evidence-led), coordinate suppliers, and manage change control.
- **Verify:** Present deliverables with acceptance criteria, before/after evidence, and adoption notes.
- **Debrief:** Update backlog, KPIs, and roadmap; agree next priorities and schedule.

Deliverables

- Master artefact set: governance pack (RACI, cadence, dashboards), draw-down process, change control, and reporting templates.
- Per-package SoW: scope, outcomes, acceptance criteria, owners, timelines, pricing, and risks.
- Per-package outputs: service-specific deliverables (reports, content, playbooks, configurations, attestations) with verification artefacts.
- Quarterly outcomes report: progress against KPIs, risk posture, spend vs budget, and next-quarter plan.
- Embedded alignment within outputs: NCSC CAF outcomes, ISO/IEC 27001 control families, CIS Controls, OWASP references, and Microsoft security baselines where relevant.

Outcomes and benefits

- **One contract** covering diverse needs, reducing lead times and supplier sprawl.
- **Consistent quality** and evidence across heterogeneous work.
- **Clear line of sight** from spend to risk reduction and resilience.
- **Rapid mobilisation** for high-priority work without renegotiating terms.

Pricing model

Blend of fixed-price work packages and capped T&M for variable or surge tasks. Rate cards by role, with discounts for committed volumes or multi-year terms. Pricing Factors include complexity, urgency, environment breadth, third-party coordination, and re-test depth.

Examples of managed service draw-downs

- MXDR on Microsoft stack: 24×7 triage, incident handling, detection engineering. Per-endpoint or per-identity pricing; SLA-backed.
- Continuous Reconnaissance/CASM: continuous external exposure hunting and takedown workflow. Per-brand/domain tiering.
- IR Retainer (reactive/proactive): guaranteed mobilisation; optional quarterly threat-hunting and exercises. Monthly fee plus call-off days.

- Detection Engineering: monthly content sprints, KPIs on precision and noise reduction. Fixed monthly with sprint backlog.
- vCISO: fractional leadership, outcomes plan, board reporting. Monthly retainer with quarterly objectives

Timelines

Timelines are aligned to client requirements stated during the scoping stage.

Operating model and SLAs

- Service hours:
    - MXDR/CASM: 24×7 monitoring and high-severity response.
    - IR Retainer: 24×7 mobilisation per agreed SLA (e.g., P1 within 60–120 minutes).
    - Professional Services / Consultancy are typically business hours
- Incident severities with time-to-acknowledge and time-to-action targets.
- Change control via standard and emergency routes; maintenance windows agreed quarterly.

Team and roles

- Engagement Director for governance, quality, and value realisation.
- Service Leads (testing, detection/engineering, IR/CIR, advisory/vCISO) assigned per package.
- Delivery Consultants/Engineers matched to package scope and platforms.
- Coordinator for scheduling, artefacts, and commercial administration.

Security and assurance

Facilitation is delivered by experienced practitioners using peer-reviewed methods and internal quality checks. Materials are reproducible and traceable to session evidence. Where appropriate, observed behaviours are mapped to MITRE ATT&CK and translated into detection opportunities for SOC/EDR teams. Accessibility options are available on request.

Buyer responsibilities

- Nominate an executive sponsor and technical owners for each work package.
- Provide timely access to artefacts, platforms, and decision-makers.

JUMPSEC responsibilities

- Operate within agreed authority, minimising disruption and handling artefacts securely.
- Produce clear, auditable outputs with acceptance criteria and verification steps.

- Provide and maintain required licences, connectivity, and test data.
- Approve per-package scopes, priorities, and change control.
- Coordinate third-party permissions (hosting, MSPs, SaaS) where needed.
- Maintain transparent governance, decision logs, and value tracking.

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.

On completion, data and credentials are returned or securely destroyed. Final artefacts include the action log, debrief materials, and an evidence-retention statement

Constraints and assumptions

- No destructive testing unless explicitly scoped in a relevant package.
- Third-party environments or involvement require written consent.
- Data is processed under UK GDPR/DPA with an agreed data location.
- Personnel with BPSS/SC clearance are available where required.
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA).
- Standards and regulatory mappings are integrated into per-package deliverables.

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com