SERVICE DEFINITION

RED TEAMING / COVERT ADVERSARIAL SIMULATION

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 — Covert OAuth consent and mailbox staging

We emulated actor tradecraft observed against UK public bodies. During reconnaissance, JUMPSEC identified permissive consent settings for unverified publishers and noted a training schedule that matched likely lures. We then obtained rogue consent, granting delegated scopes on several officer accounts. JUMPSEC created forwarding rules, enumerated mailboxes, and accessed document stores linked to policy drafts, leaving benign markers throughout the process.

JUMPSEC restricted publisher trust, added detections for consent and forwarding anomalies, and defined isolation criteria for risky scopes. We established a verification checkpoint that evidenced blocked consent attempts, accelerated escalation, and clarified the authority to isolate compromised identities.

NHS provider — Remote access replay leading to data staging

JUMPSEC discovered that staff emails overlapped with credentials found in breach corpuses. We targeted a legacy VPN realm using spray attempts, exploiting conditional MFA gaps for service roles. After gaining initial access, we identified internal portals that revealed software versions and located a vulnerable file service. JUMPSEC created benign artefacts to demonstrate directory enumeration and staged archives, ensuring we did not interact with clinical data.

We enforced phishing-resistant MFA, retired the legacy realm, and tightened access to internal portals as remediation. JUMPSEC hardened and segmented systems to close file-service paths. During a short purple team verification, we blocked replay attempts and improved alerting on staging behaviour.

Energy distribution operator (CNI) — Supplier jump path to deployment scripts

We mapped supplier documentation portals and identified contractor identities with access to shared jump infrastructure. JUMPSEC found that weak separation between staging and operational domains enabled lateral discovery. We observed a contractor account with poor hygiene accessing a repository that contained deployment scripts and historic secrets. To demonstrate the route to impact, JUMPSEC created safe artefacts without interacting with operational networks. We rotated contractor credentials, enforced just-in-time access, and separated staging from operational routes by implementing brokered admin paths as part of programme changes. JUMPSEC then verified that access was segmented and confirmed the removal of exposed secrets from history.

Local authority — Fraud-adjacent abuse of revenues workflows

We prioritised objectives that targeted the impact on business processes rather than just technical exploitation. JUMPSEC crafted sequences across staff and citizen portals to manipulate discount eligibility and payment schedules, ensuring minimal friction during the process. We found that logging did not correlate events, and approvals depended solely on email trails. JUMPSEC and the client team left benign artefacts to demonstrate the impact at the process level. We codified server-side checks, implemented dual approval for sensitive changes, and added analytics to detect unusual sequences. When we re-ran the exercise, JUMPSEC evidenced that enforced approvals, reliable audit trails, and timely alerts for anomalous flows were now in place.

Service Overview

JUMPSEC conduct covert, goal-oriented operations that emulate credible threat actors to assess how far an adversary could progress from first touch to material impact. Activity chains reconnaissance, initial access, privilege escalation, lateral movement, data staging, and objective actions—within strict authority and safety criteria. The exercise measures prevention, detection, response, and decision-making, evidencing risk through safe artefacts and timelines.

Objectives

- Demonstrate realistic attack paths that achieve agreed business objectives
- Exercise blue-team capability without prior notice, capturing dwell time and escalation
- Identify control gaps that, once fixed, break multiple attack chains
- Produce testable improvements and verification steps that sustain uplift

Approach

Engagements begin with a goal and constraint workshop to agree objectives, rules of engagement, abort criteria, and success measures. Intelligence informs TTP selection. Covert operations run across approved windows, coordinating through a single authority matrix. Activities may include open-source and technical reconnaissance, phishing or social engineering, exploitation of exposed services, post-exploitation, and controlled data staging. Where required, purple checkpoints provide discreet feedback without revealing full tradecraft.

Method

- **Plan** — objectives, hypotheses, authority matrix, escalation paths, evidence handling, safety gates
- **Recon** — map assets, suppliers, identities, processes, and likely ingress aligned to threat intelligence
- **Gain access** — exercise approved routes such as phishing simulations, credential attacks, and exposed services
- **Expand** — validate privilege escalation, lateral movement, and staging using non-destructive techniques
- **Demonstrate impact** — show objective-level risk with benign artefacts and time-boxed activity
- **Debrief** — present timelines, decisions, gaps, and priority actions with owners and acceptance criteria
- **Improve** — optional verification sprint or purple-run to confirm uplift

Deliverables

- Executive briefing (slide deck and debrief) describing achieved paths, business impact, and priority actions
- Red Team Report with full timeline, evidence, exploited conditions, detection/response observations, and precise fixes mapped to owners and acceptance criteria
- Attack path register (CSV/XLSX) linking chained conditions from ingress to objective with recommended controls to break each chain
- Detection and response improvement pack including analytics, playbook hooks, isolation criteria, and verification tests
- Optional verification after uplift or a short purple-team to validate coverage
- Standards and alignment embedded in reporting, referencing MITRE ATT&CK techniques used, NCSC guidance for incident management and internet-facing hygiene, and UK frameworks such as CBEST/GBEST/TIBER concepts where relevant to rationale and structure

Outcomes and benefits

- Independent evidence of how real attackers could achieve impact today
- Targeted fixes that remove multiple routes and reduce blast radius
- Measured improvement in detection, escalation, and containment
- Assurance artefacts suitable for boards, auditors, and insurers

Pricing model

Fixed price per campaign with defined objectives and constraints, or time-and-materials for extended operations. Cost drivers include objective complexity, estate breadth, supplier involvement, and depth of verification.

Timelines

- Planning and approvals in 3–7 working days
- Operations scheduled across agreed windows
- Report issue in 5–10 working days after testing completion
- Optional verification by agreement

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
- **Adversarial / Offensive Consultant(s)** - execution, tradecraft, and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate an executive sponsor and single engagement lead
- Approve objectives, authority matrix, and safety criteria
- Provide access routes or test accounts where agreed, and supplier contacts for coordination

JUMPSEC responsibilities

- Operate strictly within rules of engagement and change control
- Minimise operational impact and avoid destructive actions
- Handle evidence securely with time-boxed retention and approved destruction or 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

- Non-destructive techniques; no denial-of-service or data encryption
- Third-party and hosted service testing requires written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Threat-Led Penetration Testing
- Purple Teaming / Collaborative Adversarial Simulation
- Detection Engineering and SOC Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com