# SERVICE DEFINITION
# THREAT-LED 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

### Local authority — Business-process abuse in revenues and benefits

We focused our threat hypotheses on workflow abuse rather than purely technical exploitation. During testing, JUMPSEC demonstrated how we could manipulate discount eligibility and payment schedules by crafting specific sequences across staff and citizen portals, encountering minimal friction. We identified that the logging did not correlate events effectively, and approvals relied solely on email trails. Using benign proofs, we showed the process-level impact without altering any live records.

To improve the situation, JUMPSEC codified server-side checks, required dual approval for sensitive changes, and added analytics to detect unusual sequences. When we retested, we provided evidence that enforced approvals, delivered reliable audit trails, and generated alerts for anomalous process flows.

### NHS shared service — Credential replay against remote access with partial MFA

JUMPSEC identified password reuse in breach corpuses for staff emails. We targeted a legacy VPN realm using spray activity and found conditional MFA gaps for service roles. JUMPSEC used one account to access internal portals, which exposed software versions and a vulnerable file service. We demonstrated directory enumeration and read access to staging shares using benign proof.

JUMPSEC enforced phishing-resistant MFA universally, retired the legacy realm, and tightened access to internal portals. We hardened and segmented the file service to close the path to staging. Our follow-up showed that we blocked replay, reduced information leakage, and established safer internal access patterns.

### Energy distribution operator (CNI) — Supplier jump path to staging repositories

We mapped supplier documentation portals and identified contractor accounts with access to shared jump infrastructure. JUMPSEC discovered that weak separation between staging and operational domains allowed lateral movement. Our team used a contractor account with poor credential hygiene to access a code repository containing deployment scripts and historical secrets. Using safe artefacts, we demonstrated the potential for privilege escalation without interacting with operational networks.

We rotated contractor credentials, enforced just-in-time access, and split staging from operational routes by implementing brokered admin paths. JUMPSEC's reassessment confirmed that access was segmented and exposed secrets had been removed from history.

# Service Overview

JUMPSEC's threat-led penetration testing models realistic attacker goals and methods using current intelligence. Activities chain findings across reconnaissance, initial access, privilege escalation, lateral movement, and objective actions such as data staging or business-process abuse. Testing remains safe and non-destructive, uses clear abort/safety criteria, and produces evidence that shows feasibility, impact, and practical fixes.

## Objectives

- Validate exposure to current threat behaviours, not just generic vulnerability classes
- Demonstrate credible attack paths from first touch to material impact
- Prioritise fixes that remove whole classes of risk or break attack chains
- Provide repeatable verification so improvements remain measurable

## Approach

Delivery starts with a goal and hypothesis workshop that selects targets, constraints, and success measures informed by threat intelligence. Operations run in windows with executive awareness, change control, and defined authority. Activities cover open-source and technical recon, phishing or credential attacks where approved, exploitation of in-scope systems, and post-exploitation steps using benign proofs.

## Method

- **Plan** — define target objectives, hypotheses, rules of engagement, escalation, and evidence handling
- **Recon** — map assets, suppliers, identities, and likely ingress based on TI and business context
- **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 safe artefacts and time-boxed activity
- **Debrief** — present timelines, decisions, and prioritised actions with acceptance criteria
- **Improve** — optional verification sprint to confirm uplift and measure residual exposure

## Deliverables

- Executive briefing (slide deck + debrief) describing objectives, achieved paths, impact, and priority actions
- Threat-Led Penetration Test Report including timelines, evidence, exploited conditions, and precise fixes mapped to owners and acceptance criteria
- Attack path register (CSV/XLSX) showing chained conditions from ingress to objective, with recommended controls to break each chain
- Detection and response observations with suggested analytics, playbook hooks, and verification tests
- Optional re-test confirming effective mitigation after change
- Standards and alignment embedded in reporting, referencing MITRE ATT&CK behaviours used, NCSC guidance relevant to internet-facing services and incident handling, OWASP/ASVS or OWASP API materials where application vectors arise, and CIS control references where hardening supports mitigation

## Outcomes and benefits

- Clear sight of how real attackers could achieve impact today
- Fixes that remove multiple routes, reduce blast radius, and strengthen detection
- Evidence suitable for boards, audit, and insurers showing measurable improvement
- Repeatable checks to sustain risk reduction across releases

## Pricing model

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

## 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** - execution, evidence capture, and safe-ops adherence
- **Coordinator** — logistics, communications, evidence handling, action tracking

## Buyer responsibilities

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

## JUMPSEC responsibilities

- Operate strictly within rules of engagement and safety criteria
- Minimise operational impact and avoid destructive actions
- Handle evidence securely with time-boxed retention and approved destruction/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 testing; no denial-of-service or data encryption
- Third-party coordination and hosted service testing require written consent

Personnel with BPSS/SC available where required

- Reports available in accessible formats (WCAG 2.1 AA)

## Related services

- Red Teaming / Covert Adversarial Simulation
- WAF Bypass Testing
- 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