SERVICE DEFINITION
ATTACK PATH MAPPING

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, as we provide our clients with 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

IT managed service provider — Shared infrastructure cross-tenant pivot

We mapped a mid-market MSP, identifying shared RMM servers, centralised backup repositories, and a multi-tenant Active Directory used for privileged support. Our team discovered that service accounts had been reusing credentials across clients, and VPN concentrators were terminating into flat management networks. We traced a credible attack chain: phishing an MSP operator led to RMM console access, which enabled script pushes to multiple tenants, followed by browsing backup repositories and staging data. At client sites, we noted that logs failed to provide visibility into MSP-originated administrative actions, which delayed triage efforts.

To address these issues, we introduced per-tenant management enclaves, implemented just-in-time privileged access with multi-factor authentication, and enforced signed script execution using allow-lists. We migrated backups to tenant-segregated, immutable stores and tightened admission policies to block unsigned tooling. RMM actions were streamed to client SIEMs with correlation IDs for full traceability. Our verification demonstrated successfully blocked cross-tenant pushes, fully auditable MSP activity, and constrained access paths, all aligned with updated contracts and incident engagement rules.

Large consumer services provider — Identity to claims-data staging via supplier portals

We identified widespread identity sprawl across customer portals, partner integrations, and field-dispatch systems, including unverified app consent, verbose error disclosures, predictable identifiers, and exploitable attack chains. Attackers could gain delegated mailbox access, create mailbox rules, and use email-based resets to pivot into supplier portals, enabling data exports via shared accounts. Logging lacked correlation between consent, rule creation, and portal activity.

To mitigate these risks, we enforced stricter publisher trust, phishing-resistant MFA for sensitive roles, and blocked external auto-forwarding. Supplier portals now have server-side checks, idempotent recovery, and verified contact for resets. Shared accounts were replaced with just-in-time, least-privilege access. SIEM analytics now correlate consent, mailbox rules, and portal access, with enriched alerts. Our controls successfully blocked risky consent, improved alerting, enforced recovery, and limited data staging during peak periods.

Energy utility (CNI) — Contractor jump host to OT-adjacent historians

JUMPSEC identified that supplier VPNs terminated close to the OT DMZ, utilising shared jump hosts and long-lived accounts. Our team observed that historians were accepting legacy protocols from mixed subnets, while backups were traversing shared file services. We traced a credible attack chain running from contractor identity, through the jump host, to historian access and ultimately to data staging. To address these risks, we brokered vendor access using just-in-time privileges and implemented session recording. We segmented historian access behind authenticated brokers and protected backups with immutable snapshots. Our verification demonstrated that we had successfully established segmented routes, ensured auditable privileged sessions, and secured configuration artefacts.

Service Overview

Attack Path Mapping reveals to technical and non-technical audiences how discrete weaknesses chain into realistic routes from first touch to material impact. The engagement documents ingress points, trust boundaries, identities, controls, and business processes, then validates feasible chains using safe techniques. Outputs provide a ranked set of attack paths, explicit break-points, and backlog-ready changes that remove whole classes of risk.

Objectives

- Identify and evidence end-to-end attack paths across identity, endpoint, cloud, email, network, and process
- Prioritise controls that break multiple chains with minimal operational friction
- Clarify ownership, sequencing, and acceptance criteria for permanent fixes
- Seed detections and playbooks that surface these paths early

Approach

Our approach combines design analysis, selective technical checks, and stakeholder interviews. Mapping covers assets and suppliers, identity and access flows, change and support processes, data staging and exfil routes, and recovery pathways. Validation remains non-destructive and uses benign artefacts. Business impact guides ranking and remediation order.

Method

- **Plan** — confirm objectives, systems, and processes in scope; agree windows, escalation, and evidence handling
- **Model** — inventory assets, identities, controls, suppliers, and trust boundaries; chart critical business journeys
- **Trace** — enumerate plausible chains from ingress to objective across people, process, and technology
- **Validate** — safely confirm feasibility of selected links (e.g., configuration review, benign proofs, read-only exports)
- **Prioritise** — rank paths by impact, likelihood, and ease of fix; define owners and acceptance criteria
- **Debrief** — present paths, break-points, fixes, and verification checks; agree retest approach

Deliverables

- Executive briefing (slide deck + debrief) highlighting the top attack paths, business impact, and priority break-points

- Attack Path Map visualising each chain from ingress to objective with contributing conditions, affected controls, owners, and acceptance criteria
- Remediation playbook detailing control changes that collapse multiple paths
- Detection and response pack with ATT&CK-mapped recommendations
- Standards and alignment embedded in reporting: ATT&CK technique tags for path steps; NCSC guidance for internet-facing hygiene and incident handling; OWASP ASVS/API references where application vectors appear; ISO 27005 language for risk rationale; IEC 62443 concepts where OT boundaries feature

Outcomes and benefits

- Fewer viable routes from outside to impact; reduced blast radius
- Controls that address families of risk rather than isolated findings
- Measurable improvement via verification tests and enriched detections
- Clear ownership and sequencing that lands in BAU without churn

Pricing model

Fixed price per system/estate band or time-and-materials for complex, multi-supplier environments. Price drivers include domain breadth, supplier involvement, identity complexity, path validation depth, and verification.

Timelines

- Planning and artefact collection: 3–5 working days
- Workshops, execution and analysis: typically 1–3 weeks depending on breadth and validation depth
- Report issue in 5–10 working days after testing completion
- Optional verification and updates: by agreement

Team and roles

- Engagement Lead for governance, ethics, and quality
- Adversarial Consultant(s) facilitating workshops and analysis
- Detection Engineer supporting analytics and playbook design

Buyer responsibilities

- Nominate an executive sponsor and single engagement lead
- Provide architecture and identity artefacts, change windows, and contact points for suppliers
- Enable read-only exports and safe checks where required

JUMPSEC responsibilities

- Operate within agreed authority and change control
- Use non-destructive validation and minimise operational risk
- Handle materials 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 techniques; no denial-of-service or data encryption
- Third-party coordination and hosted service checks require 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