SERVICE DEFINITION DOCUMENT

IR READINESS REVIEW / BREACH READINESS REVIEW

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 — Communications cadence and external notifications**

We reviewed the communications materials and found outdated templates, missing approval steps, and no pre-agreed lines for citizen updates. JUMPSEC noted that, although regulatory triggers were listed, they were not linked to decision thresholds or evidence checkpoints.

We introduced pre-approved templates, set a timed communications cadence, and established criteria for public messaging. JUMPSEC tied reporting triggers in playbooks to evidence quality gates. Our subsequent assessment showed that communications became timely and accurate, with notification decisions easier to audit.

- **Energy transmission operator (CNI) — Supplier integration and isolation routes**

We conducted scenario walkthroughs and identified conflicting supplier SLAs for incident engagement and unclear ownership for isolation of shared platforms. JUMPSEC observed that network teams lacked a documented path to broker isolation without risking OT-adjacent services.

We aligned SLAs to a unified escalation model, defined brokered isolation routes, and rehearsed cross-supplier hand-offs. JUMPSEC verified a coordinated supplier response and safer isolation choices for systems near operational networks.

- **Manufacturer & distributor — ERP/WMS recovery and supplier hand-offs**

We ran scenario walkthroughs across ERP, warehouse management, and 3PL integrations and surfaced unclear authority to pause despatch and switch to contingency picks. JUMPSEC found that contracts listed differing incident SLAs for EDI, carrier portals, and label services, which created hand-off gaps. We also noted that backup access for the ERP database required shared credentials, and finance delayed restore approvals, making testing slower. We spotted that runbooks omitted the sequence for re-enabling goods-in, printing, and stock reconciliation after a cyber event.

We defined a single authority matrix for stop/start decisions, added brokered isolation for EDI and carrier links, and moved ERP restores to named roles with pre-staged credentials. JUMPSEC codified the recovery order in playbooks: database restore, interface checks, label services, then reconciliation. Our verification demonstrated faster approve-to-restore timings, more coordinated supplier engagement, and predictable restart of picking and despatch without stock drift.

Service Overview

JUMPSEC conduct an independent assessment of incident response readiness focused on governance, processes, evidence, and decision-making. The review tests whether people, runbooks, tooling, and suppliers can detect, contain, investigate, and recover without unnecessary delay. Outputs provide prioritised, testable improvements and clear ownership to raise confidence before the next incident.

Objectives

- Validate the end-to-end incident lifecycle: detect, assess, contain, eradicate, recover, document
- Clarify decision rights, escalation paths, and regulator/reporting triggers
- Improve evidence handling, log coverage/retention, and chain-of-custody
- Align suppliers and internal teams to a single authority matrix and RACI

Approach

Evidence-led review using document analysis, structured interviews, tabletop walkthroughs, and light control checks. Activities run in agreed windows and avoid production impact. Stakeholders usually include Technology, Security, Legal/IG, Communications, Business Continuity, and key suppliers.

Method

- **Plan** — confirm objectives, priorities, success measures, and stakeholders
- **Collect** — gather runbooks, contracts, SLAs, contacts, logging/backups, and comms templates
- **Assess** — test escalation, authority, evidence handling, and supplier integration through scenario walkthroughs
- **Validate** — spot-check controls supporting IR (logging, retention, access to backups, isolation routes)
- **Debrief** — agree priorities, owners, and acceptance criteria; schedule verification reviews

Deliverables

- Executive briefing (slide deck + debrief): top risks, decision bottlenecks, and priority actions
- IR Readiness Report, covering:
    - Governance & Authority: RACI, decision thresholds, regulator/reporting triggers
    - Process & Playbooks: containment/eradication/recovery steps, approval gates, documentation standards
    - Evidence & Forensics: log sources/retention, access, chain-of-custody, time sync
    - Supplier & Third Parties: contracts, SLAs, call-trees, data/process hand-offs

  - Communications: internal/external comms, media lines, customer and partner notifications
  - Business Continuity: backup access, restore authorisation, prioritised service recovery

- Gap register (CSV/XLSX): issues, owners, due dates, acceptance criteria
- Authority matrix & RACI pack: decision rights, escalation paths, roles, and contact rotas
- Playbook set (updated or new): regulator-aware templates with step-by-step actions
- Verification checklist: discrete tests to confirm readiness uplift
- Standards and alignment (embedded): mappings to NCSC incident management guidance, ISO/IEC 27035, NIST CSF/800-61, and relevant UK reporting obligations used for rationale

Outcomes and benefits

- Faster, clearer decisions during incidents with traceable accountability
- Better investigative depth through reliable evidence and retention
- Aligned suppliers and internal teams executing the same playbook
- Regulator- and insurer-ready documentation and artefacts

Pricing model

Fixed price per organisation/estate. Price drivers: stakeholder count, supplier landscape, artefact depth, and number of playbooks to update/create.

Timelines

- Planning and artefact collection: 3–5 working days
- Interviews, walkthroughs, and checks: 1–2 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional rerun/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, stakeholder alignment
- **IR Specialist(s)** — assessment, scenario walkthroughs, control validation

- **Coordinator** — logistics, comms, supplier alignment, action tracking

Buyer responsibilities

- Nominate sponsor and single engagement lead
- Provide documents, contact lists, and access to representatives
- Confirm change windows and supplier participation

JUMPSEC responsibilities

- Operate within agreed rules of engagement and authority boundaries
- Minimise operational impact; maintain confidentiality of artefacts
- Secure handling and time-boxed retention of materials

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 coordination requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Cyber Incident Exercising (NCSC Assured)
- DFIR: Containment, Forensics, Recovery Support
- 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