SERVICE DEFINITION DOCUMENT

DFIR — CONTAINMENT, FORENSICS, RECOVERY SUPPORT

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 agency — Token theft and email rule abuse

We actively responded to the incident by identifying risky sign-ins and anomalous token use across admin and shared mailboxes. Our analysts correlated OAuth consent grants from unverified publishers and tracked forwarding rules that were created during off-hours. We gathered evidence from endpoints, including browser token artefacts and scripts that automated rule creation.

JUMPSEC contained the threat by revoking sessions, removing rules and rogue consents, and tightening conditional access for privileged roles. During recovery, we rotated credentials, reset app secrets, and added detections for future consent and rule changes. We provided debrief materials that included a clear decision log, a revised authority matrix, and an IOC/IOA catalogue for follow-up checks.

Energy utility (CNI) — Domain admin compromise with persistence

We investigated across jump hosts and domain controllers, uncovering credential theft, service account misuse, and persistence established via startup processes. We identified Kerberos ticket patterns that showed lateral movement during maintenance windows. Our team found evidence such as modified services and newly created local admin accounts on selected systems.

We contained the incident by disabling suspect accounts, resetting privileged credentials, and brokering admin paths through hardened jump infrastructure. During recovery, we rebuilt critical hosts and confirmed that we had removed persistence. To improve future resilience, we introduced just-in-time access, Privileged Access Workstations (PAWs), and enhanced logging for privileged operations.

Local authority — Ransomware detonation and restore orchestration

We observed rapid file modifications and discovered ransom notes scattered across shared areas of the file servers. Our team noted that backup platforms recorded attempts to delete recent restore points. We assembled evidence packs that included process trees, ASR blocks, and access timelines.

We immediately isolated affected servers, protected backups by applying immutability controls, and validated clean restore paths. During the recovery phases, we prioritised restoring critical services and verified applications before re-admitting users. For improvement, we tightened backup delete privileges, enforced write-once retention, and introduced rehearsed restore procedures with timed checkpoints.

Service Overview

JUMPSEC conduct hands-on incident response covering rapid containment, forensic acquisition and analysis, and recovery support. The service stabilises the environment, preserves evidence, identifies root cause and blast radius, and supports a safe return to operations. Delivery aligns to UK public-sector needs, including clear decision logs, regulator-aware documentation, and auditable actions.

Objectives

- Contain active threats and prevent further impact
- Acquire and analyse evidence to establish timelines and causality
- Support eradication and clean-build recovery with verified controls
- Produce clear artefacts for governance, legal, and insurer engagement

Approach

Response runs under an agreed authority matrix with defined abort/safety criteria. Teams prioritise containment, then execute forensically sound acquisition and analysis. Recovery support aligns rebuild and restore to verified indicators. Regular briefings keep executives, IT, Legal/IG, and Communications aligned.

Method

- **Mobilise** — confirm authority, stakeholders, comms channels, and initial scope
- **Stabilise & contain** — isolate accounts/devices, revoke tokens, broker network controls
- **Acquire** — capture volatile and at-rest evidence (endpoints, servers, identity, SaaS/cloud)
- **Analyse** — reconstruct timelines, identify initial access, persistence, lateral movement, exfiltration
- **Eradicate & harden** — remove persistence, rotate credentials, uplift priority controls
- **Recover** — guide clean rebuild and restore; validate before re-admission to production
- **Debrief** — deliver reports, decision logs, and targeted improvement action

Deliverables

- Executive situation reports (SITREPs): concise status, decisions, risks, next actions
- Containment change log: isolations, revocations, control changes with timestamps and owners
- Forensic acquisition register: what was taken, from where, by whom, and chain-of-custody
- Forensic Analysis Report: initial access, techniques used, affected assets/accounts, timelines, IOC/IOA catalogue

- Optional recovery playbook updates: rebuild/restore steps, validation checks, and re-admission criteria
- Optional regulator/insurer pack: decision timeline, notifications, evidence summaries, and impact statement
- Standards and alignment (embedded): ISO/IEC 27035 and NCSC incident management principles; ATT&CK techniques cited for rationale and IOC/IOA mapping

Outcomes and benefits

- Faster containment and reduced blast radius
- Evidence-backed understanding of cause, impact, and spread
- Safer, verified recovery with clearer decision rights
- Credible artefacts for governance, legal, and insurance

Pricing model

Time-and-materials for emergency mobilisation, with fixed-price options for defined investigation phases and recovery support packages. Cost drivers: estate size, evidence scope, data volume, supplier coordination, and reporting depth.

Timelines

- Mobilisation: as agreed under retainer or emergency call-off
- Initial containment: hours to days, based on access and authority
- Forensic reporting: phased; Report issue: 5–10 working days after testing completion for each defined phase
- Verification and recovery support: 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

- **Incident Director / Manager** — command, stakeholder alignment, reporting cadence
- **DFIR Lead & Investigators** — containment support, acquisition, analysis, timelines
- **Platform and Offensive Specialists** — identity, email, cloud, endpoint, network
- **Coordinator** — comms, evidence handling, supplier engagement, action tracking

Buyer responsibilities

- Nominate executive sponsor and single incident lead
- Approve authority matrix for containment and control changes
- Provide access to platforms, logs, backups, and supplier contacts
- Support briefings, decisions, and post-incident improvement activities

JUMPSEC responsibilities

- Act within the authority matrix and change control
- Preserve evidence integrity and maintain chain-of-custody
- Minimise operational impact while prioritising containment and recovery

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

- Actions occur in approved windows or under emergency authority
- Third-party coordination requires named contacts and consents
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- IR Readiness Review / Breach Readiness Review
- Cyber Incident Exercising (NCSC Assured)
- Ransomware Readiness Assessment / Simulation

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com