SERVICE DEFINITION
WALK-IN INCIDENT RESPONSE (EMERGENCY IR)

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

Non-ministerial department — Supplier SaaS incident under contract and DPIA duties

When a multi-tenant SaaS supplier reported suspicious access, we moved ownership of governance, risk, and compliance to the vCISO. JUMPSEC activated the decision log, aligned authority under the major-incident policy, and framed risk against the organisation's appetite and register. We cross-checked the DPIA, ROPA, and data classifications during triage, confirmed potential Article 33 triggers, and preserved evidence with a documented chain-of-custody. We mapped obligations to internal policy and contract terms—covering incident notification timelines, Security Plan commitments, and logging/retention—and maintained an executive update cadence for the SIRO and Audit & Risk Committee.

JUMPSEC directed supplier assurance to provide a timeline, identify affected controls, outline containment steps, and propose remediations, benchmarking their actions against ISO/IEC 27035 and NCSC CAF (Detect/Respond). We translated control gaps into owner-attributed actions with acceptance criteria, linking them to ISO/IEC 27001 Annex A and updating relevant policies, such as access control, supplier management, and logging. We refreshed metrics—including MTTD/MTTR, parse success, and data-egress anomalies—drafted communications templates, and rehearsed the decision path for temporary isolation and service resumption. Our short verification drill demonstrated maturity uplift; JUMPSEC recorded the Article 33 position, identified contract levers in case remediation slipped, and set out a 60-day plan to close residual risks in board materials.

NHS provider — Data protection, incident readiness, and board reporting

JUMPSEC strengthened protection for clinical data and clarified incident decision-making for a healthcare provider. We rolled out Purview labelling, piloted DLP solutions, and implemented safer external sharing practices. JUMPSEC enhanced Sentinel content to deliver earlier signals for credential theft and staged exfiltration. We tracked sensitive-data coverage, precision, and drill outcomes through board materials. JUMPSEC conducted a verification exercise that confirmed clinician-in-the-loop paths and established a cadence for regulator engagement.

Loyalty platform — vCISO for fraud risk and data protection

A multi-tenant loyalty platform faced increased fraud, growing partner APIs, and tighter privacy demands. As vCISO, we set quarterly risk-based goals, mapped PCI and non-PCI data flows, and reviewed identity, API, and logging controls. JUMPSEC found issues like overly broad service accounts, weak app consent checks, permissive webhooks, inconsistent rate limiting, and limited event tracking. Detection for account enumeration and voucher abuse was imprecise, and break-glass access lacked drills.

To address these, JUMPSEC enforced PIM with approvals, rolled out phishing-resistant MFA, strengthened admin approval for app publishers, and secured webhooks with mTLS and signed payloads. We implemented per-client throttling, anomaly detection at API gateways, and reduced PCI scope via tokenisation. Logging was standardised for better incident timelines, and targeted playbooks were developed. KPIs showed improved alert accuracy, fewer false positives, quicker response to redemption spikes, and clearer audit trails.

Service Overview

JUMPSEC delivers rapid, NCSC CIR-accredited incident response with senior incident management and deep forensic capability. We stabilise operations, preserve evidence to a defensible standard, and contain threat activity while restoring essential services safely. We draw on our MXDR, detection engineering, and red/purple-team expertise to interpret attacker tradecraft and anticipate next moves, so containment and recovery stay one step ahead and decisions withstand regulatory and legal scrutiny.

Objectives

- Stop active compromise and prevent further data loss or disruption.
- Preserve forensic evidence and establish a defensible timeline.
- Clear communications across technical and non-technical teams
- Restore priority services safely and verify attacker eviction.
- Produce precise actions for hardening and regulator/insurer engagement.

Approach

We initiate an urgent triage to establish authority, objectives, and safety gates, then stand up incident management cadence and evidential handling. An experienced Incident Manager coordinates workstreams across identity, endpoints, network, and suppliers, while Lead Forensic Examiners collect and analyse volatile and at-rest artefacts to reconstruct ingress, persistence, lateral movement, staging, and egress. Detection engineers tune controls in-flight, using threat-led hypotheses and observed TTPs to predict likely pivot points and block them pre-emptively. Recovery proceeds in controlled phases with integrity checks and rollback points. Actions land through change control with owners and acceptance criteria.

Method

- **Mobilise** — confirm authority, roles, comms channels, decision thresholds, and incident cadence; establish secure evidence repositories and chain-of-custody.
- **Stabilise** — protect backups, enforce emergency identity controls, segment high-risk areas, and stop known egress; document decisions and rationale.
- **Investigate (forensics-led)** — acquire volatile memory, host and cloud artefacts, and key logs; build a defensible timeline of TTPs, affected accounts, hosts, and data. Validate findings against threat-led hypotheses and likely next steps.
- **Contain & Eradicate** — remove access, evict persistence, rotate secrets, and harden weak controls; deploy targeted detections to confirm eviction and catch re-entry.
- **Recover** — restore priority services in phases with integrity and performance verification; retain heightened monitoring during the burn-in period.

- **Debrief** — deliver executive briefing, technical forensic report, regulator/insurer artefacts, and a 30/60/90-day plan tied to measurable control uplift.

Deliverables

- Executive situation reports and incident management cadence pack (roles, decisions, status dashboards).
- Forensic Investigation Report: scope, evidence log/chain-of-custody, methodology, timeline of attacker activity, root-cause analysis, affected assets/data, and defensible conclusions.
- Containment & Recovery change set with exact steps, rollback, and acceptance criteria; integrity verification results.
- Optional Detection & Engineering uplift pack: content to detect observed and predicted TTPs, suppression of noise, and watchlists for high-risk entities.
- Optional insurer pack: decision logs, notification rationale (e.g., Article 33), evidence handling notes.

Outcomes and benefits

- Faster, defensible containment supported by disciplined incident management and chain-of-custody.
- Clear attacker timeline and rationale for actions; reduced reinfection risk by pre-empting likely pivots.
- Safer recovery and measurable control uplift evidenced by verification artefacts..

Pricing model

Time-and-materials mobilisation, moving to fixed bundles when scope stabilises. Pricing drivers: incident scale, platforms in scope, data/forensic needs, out-of-hours coverage, and retest depth.

Timelines

- Mobilisation: immediate following commercial cover and written authority to proceed.
- Stabilisation: first 24–72 hours (incident-dependent).
- Investigation/containment: typically 3–10 working days as evidence permits.
- Report issue: 5–10 working days after testing completion.
- Optional retest/closure: by agreement.

Team and roles

- Incident Director for strategy, authority, and executive communications.
- Lead Forensic Responder for triage, evidence handling, and timeline.
- Detection/IR Engineer for containment, detections, and verification.
- Coordinator for logistics, documentation, and stakeholder cadence.
- Adjacent support available from JUMPSEC's NCSC CIR team and MXDR where telemetry access is required.

Buyer responsibilities

- Nominate executive and technical leads; provide written authority and required access.
- Preserve logs, snapshots, and backups; avoid unauthorised "cleanup".
- Align supplier approvals (hosting, MSP, SaaS) for rapid action.

JUMPSEC responsibilities

- Operate under written authority and NCSC CIR expectations.
- Minimise operational risk; preserve evidence; document decisions.
- Handle artefacts securely with least-privilege access and agreed retention.

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

- No destructive testing unless explicitly scoped via adjacent services.
- Third-party participation subject to their consent and contract terms.
- BPSS/SC-cleared personnel available where required.
- Accessible reports available (WCAG 2.1 AA)

Related services

- Incident Response Retainers (NCSC CIR) — reactive/proactive models
- Compromise Assessment / Threat Hunting Sweep
- Log Validity Assessment
- Response Playbook Development

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com