SERVICE DEFINITION
INCIDENT RESPONSE RETAINERS

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 email compromise during payroll cycle (Reactive)

After the finance team flagged unverified supplier bank changes, we quickly activated our incident response. JUMPSEC took charge within an hour, traced risky sign-ins to rogue OAuth consent, and found mailbox rules sending messages externally. We revoked access, blocked forwarding, enforced re-enrolment, and set up enhanced logging to monitor further activity. Our investigation mapped the attack pathway and uncovered two linked accounts. Recovery included credential rotation and removal of malicious rules. Post-incident, JUMPSEC improved publisher trust, added better consent detections, and required finance verification through separate channels. These measures sped up triage and reduced false escalations in subsequent payroll cycles.

Retail group — Promotion surge vishing and reset abuse (Proactive)

A national retailer faced significant service-desk pressure during peak trading, so we launched a proactive uplift targeting identity compromise patterns. JUMPSEC's team hunted for look-alike domain lures, clusters of reset requests, and instances where mailbox rules were created on approver accounts. We found that baseline analytics were noisy and duplicated across platforms.

To address this, our detection engineers introduced roster-aware rules that linked near-match domains, reset attempts, and recent admin activity, applying suppressions for genuine rollouts. We mandated playbooks requiring agents to handle all cases by ticket first, call back to verified numbers, and obtain step-up approval for privileged resets, equipping agents with refusal scripts. During the next campaign, our verification confirmed that we promptly detected coordinated vishing, consistently refused resets without ticket linkage, and issued quicker advisories to stores. As a result, fraudulent resets dropped, investigation times shortened, and trading remained stable.

Global entertainment group — Suspected supply-chain compromise ruled benign (Reactive)

JUMPSEC received a vendor alert about unusual build-pipeline activity, which suggested potential downstream risk. We immediately activated the P1 hotline, and our incident manager took command within the agreed SLA. During triage, we matched vendor advisories to Sentinel signals and recent change windows. To contain the situation, JUMPSEC paused non-essential promotions, enforced step-up approvals for deployments, and enabled enhanced logging across CI/CD, registries, and admission controllers. We coordinated communications between leadership and legal to keep everyone aligned and avoid unnecessary alarm. Our forensics team reviewed build logs, signature metadata, and admission records, while our identity analysts confirmed there were no privileged sessions outside approved windows.

JUMPSEC's detection engineers deployed sequence analytics to spot suspicious build-to-deployment patterns. Within hours, we confirmed that admission controls had blocked unsigned artefacts, no workloads had pulled suspect images, and there were no signs of lateral movement. Our incident manager gave the all-clear with clear next steps: continue heightened logging for one week, require signed artefacts for hotfixes, and schedule a verification drill with the vendor.

Service Overview

JUMPSEC delivers assured incident response through a dedicated team accredited at NCSC CIR Level 2, ensuring that every engagement is led by experts who adhere to the highest standards of evidence handling and operational governance. When an incident occurs, JUMPSEC's specialists mobilise rapidly—often within the hour—as pre-established authority matrices, contact protocols, and secure data transfer arrangements are set during onboarding.

JUMPSEC guarantees strict service-level agreements (SLAs), providing clients with the assurance of on-call mobilisation and clear, pre-agreed commercial terms. This means that whenever an incident arises, clients can rely on JUMPSEC to respond swiftly and effectively, with all costs, processes, and responsibilities transparently defined in advance.

JUMPSEC have two models:

- **Reactive IR Retainer:** rapid triage, containment, forensics, and recovery.
- **Proactive IR Retainer:** everything in Reactive plus scheduled threat hunting against likely actors, and continuous readiness uplift. Requires telemetry access (e.g., Microsoft 365/Defender/Sentinel, EDR, identity, cloud).

Objectives

- Mobilise fast under clear authority and SLAs.
- Stabilise incidents and limit spread.
- Provide evidence for decisions, comms, and regulator engagement.
- Continuously reduce time-to-detect and time-to-recover.

Approach

The service follows NCSC CIR methods and recognised evidence-handling standards. Preparedness comes first. Onboarding establishes governance, the authority matrix, contacts, secure data transfer, and access to required consoles. Playbooks align to the buyer's platforms across identity, email, endpoint, cloud, and network. Change control and safety gates are agreed up front.

During an incident, a single call or email activates the on-call rota. An incident manager takes command, opens comms, and starts the SLA clock. Triage defines scope and immediate risks. Containment applies safe isolation, revokes access, blocks routes, and enables enhanced logging without unnecessary disruption. Investigation acquires and preserves artefacts, then analyses identity, endpoint, email, cloud, and network evidence to support decisions. Recovery restores services in stages under change control and confirms hardening before return to business as usual. A debrief follows with reporting, actions, and verification tests.

The Proactive IR Retainer adds scheduled hunts and continuous readiness uplift. Threat hypotheses draw on recent sector activity and intelligence. Read-only access to SIEM/XDR, identity, email, cloud, and endpoint

telemetry enables zero-impact queries. Each hunt produces findings, tuned detections, backlog items, and a short verification step so improvements persist

Method

- **Plan** — onboarding workshop, authority matrix, call-out process, secure transfer.
- **Prepare** — light readiness review, playbook alignment, access to consoles.
- **Mobilise** — single P1 contact, incident manager assigned, SLA clock starts.
- **Triage** — scope, attack stage, immediate risks, comms plan.
- **Contain** — isolate safely, revoke access, block routes, enhance logging.
- **Investigate** — acquire and preserve artefacts; analyse identity, endpoint, email, cloud, network.
- **Recover** — eradicate, harden, restore in stages with change control.
- **Debrief** — report, actions, verification tests, targeted uplift.

Proactive add-on (IR+Hunt):

- **Hunt design** — actor hypotheses from TI and recent sector activity.
- **Data access** — agreed access to SIEM/XDR, identity, email, cloud.
- **Execution** — monthly or quarterly hunts, zero-impact queries, benign artefacts.
- **Outcome** — findings, tuned detections, backlog items, and re-tests

Deliverables

- Executive incident briefings for senior leadership.
- IR Runbook Pack: activation, authority, contacts, comms templates.
- Incident Timeline & Evidence Log (chain of custody where required).
- Technical Findings & Containment Actions with exact changes and acceptance criteria.
- Post-Incident Report: root causes, attack paths, regulatory considerations, improvements.
- Proactive hunts: Hunt Plan, Hunt Results, tuned rules/playbooks, backlog items.
- Standards embedded: NCSC incident management guidance, ISO/IEC 27035, ACPO/NCA digital evidence principles, MITRE ATT&CK.

Outcomes and benefits

- NCSC CIR assurance for boards, regulators, and insurers.

- Faster mobilisation and containment.
- Audit-ready artefacts and measurable uplift.
- Earlier detection through recurring hunts (proactive tier).

Pricing model

Annual subscription. Tiers define SLAs, on-call breadth, and draw-down hours/days.

- Reactive: call-out SLAs, investigation/forensics hours at preferential rates.
- Proactive: Reactive benefits plus scheduled hunts, content tuning, and mini-exercises

Timelines

- Onboarding and readiness uplift: ~1–2 weeks from contract start.
- Activation: 24×7 or business-hours per tier (e.g., P1 within 1–2 hours).
- Post-incident reporting: agreed per incident size and evidence availability.
- Proactive hunts: monthly or quarterly cadence by agreement.

Team and roles

- **Incident Director / Manager** — command and stakeholder comms.
- **Lead Investigator(s)** — forensics, triage, containment guidance.
- **Detection/Platform Engineer(s)** — telemetry uplift, content tuning, verification.
- **Coordinator** — call-out handling, logistics, document control.

Buyer responsibilities

- Nominate executive sponsor and incident manager.
- Maintain contact lists and authority matrix.
- Provide access to required platforms; enable supplier engagement.
- Endorse isolation criteria and change windows.

JUMPSEC responsibilities

- Maintain on-call rota and activate per SLA.
- Operate within agreed authority and evidence standards.
- Minimise impact; prioritise containment and safety.
- Handle data securely with time-boxed 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

- Non-destructive actions unless explicitly approved.
- Third-party coordination may gate specific steps or acquisition.
- Effectiveness of hunts depends on available telemetry and retention
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Walk-in Incident Response
- Cyber Incident Exercising (NCSC Assured).
- Detection Engineering and SOC Use Case Tuning.
- Compromise Assessment / Threat Hunting Sweep

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com