SERVICE DEFINITION
CYBER INCIDENT EXERCISING

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 — ransomware affecting citizen services

We designed a scenario in which a supplier compromise propagated into council systems. During the exercise, we surfaced unclear decision thresholds for network isolation and supplier cut-over. We focused our actions on escalation logic, third-party engagement, and coordinated communications. In a verification rehearsal, we confirmed that executive decision-making was faster and time-to-contain for priority systems was reduced.

NHS-adjacent provider — third-party breach escalation

JUMPSEC tested how Technology, IG, Legal, and Communications coordinated when an upstream provider disclosed a breach. We evidenced hand-offs, approval points, and media handling through decision logs. Our work resulted in a revised supplier playbook, clearer data-sharing thresholds, and an agreed channel for rapid regulator engagement.

Manufacturing group — OT-adjacent incident with production risk

JUMPSEC conducted a live-play rehearsal that modelled credential misuse bridging into plant systems. During the exercise, we uncovered bottlenecks between corporate IT and operations and identified the need for break-glass governance. Our actions established segmented access routes, formalised supplier call-trees, and clarified role-scoped decision rights. In a follow-up rehearsal, we enabled safer recovery choices and achieved shorter containment timelines.

Service Overview

Cyber Incident Exercising is a structured programme of rehearsals that tests how people, processes, and technology perform under realistic pressure. Exercises follow NCSC assured exercising principles, using tailored scenarios, timed injects, and realistic artefacts. Formats range from tabletop through functional drills to selected live-play. The goal is to validate governance, accelerate critical decisions, and create an audit-ready evidence trail that demonstrates readiness to leadership and stakeholders.

Objectives

- **Rehearse roles, escalation, and governance.** Clarify who decides what, when, and with which inputs.
- **Validate playbooks and tools.** Confirm plans, communications, and technical steps work end-to-end under time pressure.
- **Expose bottlenecks and information gaps.** Link each gap to an owned action with acceptance criteria.
- **Deliver a prioritised, verifiable action plan.** Define owners, due dates, and how fixes will be tested.
- **Evidence readiness.** Provide materials suitable for boards, auditors, regulators, and insurers.

Approach

Exercises are built around the organisation's threat profile, critical services, and regulatory context. Typical participants include Technology, Operations, Security, Legal, Information Governance, Communications, and key suppliers. Decision-making is rehearsed from initial alert through containment, stakeholder notification, and recovery. Outcomes include agreed thresholds for isolation and cut-over, refined communications, and integration points with third parties.

Method

- **Planning and Rules of Engagement.** Confirm objectives, audience, scope, roles, safety boundaries, change windows, and evidence handling.
- **Scenario Design.** Construct narrative and injects mapped to credible threats; prepare artefacts (alerts, tickets, emails, "press" drafts); define timings and success measures.
- **Exercise Delivery.** Facilitate sessions; capture decisions and timings; log actions with owners and due dates; maintain safety and non-destructive constraints.
- **Debrief Session.** Present observations; prioritise recommendations by impact/effort; agree acceptance criteria and verification steps.
- **Improve.** Optional verification rehearsal to confirm changes hold under the same pressure.

Deliverables

- **Exercise plan** covering objectives, roles, timings, injects, materials, and safety rules.
- **Facilitated delivery** with live capture of decisions, timings, and actions.
- **Debrief report** with observations and prioritised recommendations.
- **Action log (CSV/XLSX)** with owners, due dates, acceptance criteria, and verification steps.
- **Optional verification letter** following a re-run to attest improvement.

Outcomes and benefits

- **Faster executive decisions** for priority incidents; reduced decision latency.
- **Shorter time-to-contain** and safer recovery choices for critical services.
- **Clear accountability** across Technology, Operations, Legal, Comms, and suppliers.
- **Assurance artefacts** suitable for board papers, audits, and insurance discussions.
- **Detection and telemetry uplift** where behaviours map to SOC/EDR use cases.

Pricing model

Fixed-price per exercise or per programme; or time-and-materials aligned to SFIA rate card. Price drivers include participant scope, scenario complexity, format (tabletop vs live-play), artefact preparation, number of sessions, and whether verification rehearsals are included. Out-of-hours delivery can be scheduled and may attract a premium.

Timelines

Typical cadence includes 1–2 weeks for planning/design (subject to stakeholder availability), followed by delivery within the agreed window. The debrief report is issued within 5–10 working days of the final session. Verification rehearsals are usually scheduled 30–60 days later to allow for action completion.

Security and assurance

Facilitation is delivered by experienced practitioners using peer-reviewed methods and internal quality checks. Materials are reproducible and traceable to session evidence. Where appropriate, observed behaviours are mapped to MITRE ATT&CK and translated into detection opportunities for SOC/EDR teams. Accessibility options are available on request.

Team and roles

- **Engagement Lead.** Scope, governance, quality management, and stakeholder alignment.
- **Facilitator(s).** Exercise delivery, inject management, and live capture of decisions.

- **IR Specialist(s).** Scenario realism, technical credibility, and linkage to playbooks.
- **Coordinator.** Logistics, participant comms, evidence handling, and action tracking.

Buyer responsibilities

- Nominate a senior sponsor and a single exercise lead.
- Provide relevant policies, plans, contact rosters, and participant list.
- Confirm rooms/VC logistics and ensure third-party approvals are in place where required.

JUMPSEC responsibilities

- Operate strictly within agreed rules of engagement and change control.
- Minimise disruption and maintain defined safety boundaries.
- Preserve chain-of-custody for materials; handle and store data securely; retain only for agreed durations before verified deletion.

Data protection and privacy

The buyer remains the data controller; JUMPSEC acts as processor. Only the minimum necessary evidence is collected and retained. Secure transfer, access control, and agreed retention periods apply throughout the engagement.

On completion, data and credentials are returned or securely destroyed. Final artefacts include the action log, debrief materials, and an evidence-retention statement

Constraints and assumptions

- Exercises are non-destructive and time-boxed.
- Activities run in approved windows with agreed participants.
- Third-party involvement requires prior written consent.
- Data is processed under UK GDPR/DPA with an agreed data location.
- Personnel with BPSS/SC clearance are available where required.
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA)

Related services

- Incident Response Retainer
- Ransomware Readiness and Simulation
- Detection Engineering and SOC Use Case Tuning
- Compromise Assessment / Threat Hunting
- Red Teaming and Purple Teaming

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com