SERVICE DEFINITION

EXECUTIVE AND BOARD CYBER BRIEFING / BOARD COACHING

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

FTSE-listed retailer — Investment choices under ransomware exposure

After observing that sector peers had experienced disruptive ransomware attacks, we worked with the board to clarify isolation thresholds and prioritise spend. In our briefing, JUMPSEC directly linked identity weaknesses, backup immutability, and time-to-recover with margin risk and trading windows. We led a short rehearsal where directors made decisions on isolating finance systems before the payroll cut-off and coordinated supplier cut-over for logistics. JUMPSEC developed an action plan that sequenced identity hardening, backup controls, and detection content, aligning milestones with budget governance. As a result, directors made decisions more quickly and consistently, and we established clearer ownership between operations, finance, and technology.

Local authority — Statutory services and supplier dependency

JUMPSEC worked with a unitary authority that depended on a single managed service provider for its core platforms. We helped leadership establish clear decision logic for invoking cut-over and managing communications with care providers and the public. During our session, we presented realistic threat routes and mapped them directly to statutory duties and communications obligations. We led a rehearsal that walked leadership through escalating from suspicious activity, to partial isolation, and then to supplier fail-over. We clarified thresholds for service reduction, pre-approved messaging, and regulator liaison in our outputs. The council adopted a concise action register, and JUMPSEC scheduled a verification check to ensure ongoing assurance.

National charity — Board narrative and donor trust

JUMPSEC provided trustees with a business-focused perspective on cyber exposure, ensuring the balance between fundraising, services, and regulatory requirements. In our briefing, we framed phishing-led business email compromise and data leakage in terms of their impact on donor confidence and potential operational disruption. We ran a rehearsal in which trustees made decisions about suspending outbound campaigns and engaging insurers, legal counsel, and regulators.

We strengthened controls around consent, mailbox rules, and supplier access, and JUMPSEC implemented measures to demonstrate improved assurance to donors and the audit committee.

Global manufacturing group — executive playbook for plant operations

JUMPSEC worked with executive leadership to establish explicit decision thresholds for isolating corporate services whilst maintaining safe plant operations. We connected identity compromise and lateral movement to the blast radius in OT-adjacent environments. During the session, we led a rehearsal where leadership made isolation decisions, communicated with key customers, and determined the sequence for staged recovery. We developed an action plan that assigned ownership for privileged access reforms, logging coverage, and supplier engagement. JUMPSEC set progress checkpoints for the audit and risk committee to monitor these activities.

Service Overview

JUMPSEC equips senior leaders to make confident, timely decisions on cyber risk, resilience, and investment. We translate threat activity and control posture into business impact, obligations, and options. We run focused briefings and decision rehearsals that sharpen roles, escalation thresholds, and communications under pressure. We align recommendations to your strategy, budget cycle, and regulatory context, so actions land quickly and stick.

Objectives

- Establish a shared executive view of current risk, resilience posture, and regulatory exposure.
- Define decision rights, escalation logic, and crisis communications expectations.
- Prioritise investments with measurable outcomes and time-bound ownership.
- Improve incident decision-making through short, realistic rehearsals.

Approach

We open with a short discovery to confirm objectives, attendees, recent incidents, and board expectations. We analyse your posture and current plans, then tailor a briefing that connects threats to business operations and obligations. We facilitate a decision rehearsal that tests escalation logic and comms. We close with a concise action plan and metrics, aligned to governance and budget windows.

Method

- **Plan** — confirm aims, stakeholders, materials, and the decision topics to rehearse.
- **Discover** — review posture, incidents, supplier dependencies, and KPIs.
- **Validate** — map risks to impact on services, finance, safety, and reputation.
- **Analyse** — define options, costs, and trade-offs; set decision thresholds.
- **Debrief** — present actions, owners, timelines, and verification checks.

Deliverables

- Executive briefing deck tailored to sector and board priorities.
- Decision playbook excerpts covering isolation thresholds, supplier cut-over, and regulatory notifications.
- Action register with owners, milestones, and acceptance criteria.
- Optional rehearsal notes and follow-up coaching plan.

- Embedded alignment in materials: NCSC Board Toolkit themes, UK Companies Act director duties, DPA/UK GDPR notification triggers, and insurer/governance expectations.

Outcomes and benefits

- Faster, clearer board decisions during incidents and investments.
- Shared language across leadership, risk, and technology.
- A prioritised, costed plan with evidence of control uplift.
- Improved regulator and insurer confidence.

Pricing model

Fixed price per session or small programme. Price drivers: attendee count, tailoring depth, rehearsal scope, and follow-up coaching.

Timelines

- Preparation: 5–10 working days from confirmed inputs.
- Session delivery: 90–150 minutes per module.
- Action notes issued: within 5–10 working days after testing completion

Team and roles

- Engagement Lead facilitates and assures quality.
- Senior Consultant/IR Lead shapes content and rehearsal flow.
- Coordinator manages materials, diaries, and action tracking

Buyer responsibilities

- Nominate an executive sponsor and session attendees.
- Provide recent risk papers, incident summaries, and key policies.
- Confirm comms and legal contacts for rehearsal segments.

JUMPSEC responsibilities

- Tailor content to sector, obligations, and current posture.
- Facilitate an inclusive discussion that surfaces real constraints.
- Produce clear, actionable outputs with owners and verification steps.

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

- Third-party managed platforms require written consent for policy changes.
- Personnel with BPSS/SC available where required
- Accessible materials available (WCAG 2.1 AA)

Related services

- Cyber Incident Exercising (NCSC Assured)
- vCISO
- Framework Advisory and Consultancy

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com