SERVICE DEFINITION
VCISO

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 flagged suspicious access, JUMPSEC led governance, risk, and compliance efforts, activating incident protocols, assessing risk, and coordinating evidence preservation. The team mapped obligations to policy and contracts, kept leadership informed, and ensured regulatory triggers were addressed. Supplier assurance was tasked with a timeline, impact assessment, and remediation plan, aligned with ISO/IEC 27035 and NCSC CAF standards. Control gaps were assigned for action, policies updated, and metrics refreshed. JUMPSEC documented key decisions, completed a verification drill, and set out a 60-day plan to mitigate remaining risks.

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

JUMPSEC strengthened clinical data protection and clarified incident decision-making for a healthcare provider. We deployed Purview labelling, piloted DLP, and enabled safer external sharing. JUMPSEC enhanced Sentinel content to provide early warnings for credential theft and staged exfiltration. We tracked sensitive-data coverage, precision, and drill results in board materials. To validate improvements, JUMPSEC conducted a verification exercise to confirm clinician-in-the-loop processes and established a regular cadence for regulator engagement.

Loyalty platform — vCISO for fraud risk and data protection

JUMPSEC supported a multi-tenant loyalty platform amid increasing fraud, API growth, and privacy demands. We set quarterly risk-based outcomes, mapped data flows, and baselined identity, API, and logging controls. Key gaps found included broad service accounts, weak app consent, permissive webhook access, uneven rate limits, and limited tracking of consent and redemption events. Detection for account and voucher abuse lacked precision, and emergency access wasn't regularly tested.

To address these, we enforced PIM with time-bound approval, introduced phishing-resistant MFA, strengthened admin approval for publishers, secured webhooks with mTLS and signed payloads, and implemented per-client throttling and anomaly detection. Data minimisation and tokenisation reduced PCI scope. We unified logging, enabling clear incident timelines, and developed targeted playbooks. KPIs showed more precise alerts, fewer false positives, faster incident containment, and better audit evidence.

Service Overview

JUMPSEC provides an outcome-driven vCISO service that blends board-level guidance with deep technical leadership. We translate threats and obligations into an executable security plan, then drive measurable control uplift across identity, endpoint, network, cloud, and application stacks. We embed with your leadership, architects, and operations, chair governance, direct technical remediation, and verify improvements through testing, detection content, and drills. The model scales from fractional oversight to hands-on technical stewardship during high-change or high-risk periods

Objectives

- Establish a clear security strategy, risk appetite, and roadmap tied to business goals.
- Deliver measurable technical uplift across priority controls and platforms.
- Strengthen governance, metrics, and assurance for executives, regulators, and insurers.
- Prove readiness through exercises, re-tests, and operational KPIs.

Approach

We begin with a short discovery to understand strategy, operating model, risk drivers, and constraints. We baseline control maturity and technical posture across identity, endpoints, network, cloud, data, applications, and logging. We then agree a 30/60/90-day plan and a quarterly outcomes cadence. JUMPSEC chairs security governance, directs remediation workstreams with your teams and suppliers, and validates progress with evidence, metrics, and targeted tests.

Method

- **Plan** — agree goals, scope of authority, governance cadence, and evidence handling; set outcome measures.
- **Discover** — baseline risks, controls, architectures, licences, supplier contracts, and incident history.
- **Validate** — confirm assumptions with focused tests and data (e.g., config reviews, kill-chain spot checks, logging validity).
- **Execute** — drive remediation, content development, policy improvements, and supplier alignment; unblock issues.
- **Debrief** — report outcomes, KPIs, and residual risks; update the roadmap and next-quarter plan.

Deliverables

- Quarterly Security Outcomes Plan aligned to strategy, budgets, and risks.
- Risk Register and Decision Log with owners, tolerances, and evidence.

- Control Uplift Packs (identity, endpoint, email, cloud, data, appsec, logging) with exact changes, rollback, and acceptance criteria.
- Threat-Led Assurance: targeted re-tests, detection content updates, and verification drills tied to recent uplift.
- Board & Audit Materials: metrics pack (MTTD/MTTR, coverage, precision), policy updates, and insurer/regulatory artefacts.
- Embedded alignment in materials: NCSC Cyber Assessment Framework themes, ISO/IEC 27001/2 control families, CIS benchmarks/Microsoft baselines, OWASP ASVS/API/LLM Top 10 where relevant, and linkage to sector-specific expectations.

Outcomes and benefits

- Security strategy tied to business value and risk appetite.
- Technical hardening that collapses whole attack paths, evidenced with metrics.
- Cleaner governance and faster, clearer decisions during incidents and investments.
- Improved standing with auditors, insurers, and regulators.

Pricing model

Retainer (fractional days per month) with outcome-based milestones, or time-and-materials for surge periods. Drivers include estate size and complexity, supplier count, regulatory scope, and desired cadence of technical assurance.

Timelines

- Onboarding and baseline: 10–20 working days (calendar spread).
- Quarterly outcomes cadence with monthly checkpoints.
- Targeted artefacts (e.g., policies, reports) issued within agreed windows.
- Exercise and verification events scheduled in the plan.

Team and roles

- **vCISO Lead** accountable for strategy, governance, and outcomes.
- **Technical Domain Leads** (identity, cloud, endpoint, detection, AppSec) to direct hands-on uplift.
- **IR/Assurance Lead** to plan drills, re-tests, and metrics.
- **Coordinator** for artefacts, diaries, and change control.

Buyer responsibilities

- Nominate an executive sponsor and technical owners.
- Provide access to existing artefacts, platforms, and suppliers.
- Align budget, change control, and communications to adopt agreed actions.

JUMPSEC responsibilities

- Operate within agreed authority and minimise disruption.
- Prioritise high-impact, low-friction technical changes and prove them with evidence.
- Handle artefacts securely with least-privilege access, time-boxed retention, and approved destruction/return.

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

- Executive and Board Cyber Briefing / Board Coaching
- Microsoft 365 / Entra ID / Azure AD Tenant Review
- Detection Engineering and SOC Use Case Tuning
- Cyber Incident Exercising (NCSC Assured)

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com