SERVICE DEFINITION DOCUMENT
RANSOMWARE READINESS ASSESSMENT

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 — Communications cadence and citizen service continuity

Tabletop and light live-play target shared file services and document management platforms used across departments. Decision logs track escalation timing, external comms drafts, and criteria for isolating shared systems without disproportionate disruption.

Refinements introduce pre-approved comms templates, service continuity options for priority functions, and a clear call-tree for supplier engagement. Subsequent rehearsal evidences faster executive decisions and reduced disruption to citizen-facing services during isolation and recovery.

We delivered tabletop and light live-play exercises that targeted shared file services and document management platforms used across departments. JUMPSEC maintained decision logs, which recorded escalation timing, drafted external communications, and defined criteria for isolating shared systems without causing disproportionate disruption.

We introduced refinements such as pre-approved communications templates, service continuity options for priority functions, and a clear call-tree for supplier engagement. JUMPSEC then conducted a subsequent rehearsal, which demonstrated that executive teams made faster decisions and experienced reduced disruption to citizen-facing services during isolation and recovery.

Consumer electronics manufacturer — Home IoT fleet and cloud control plane

Ransomware simulation targets the OTA update path, device telemetry APIs, and mobile app backends supporting millions of home devices. Benign implants emulate discovery and encryption triggers inside staging environments while monitoring for mass file access and unusual token use. Findings highlight permissive service account scopes in CI/CD, weak separation between customer data and telemetry stores, and incomplete backups of firmware signing keys and device configuration metadata.

Remediation locks down CI secrets, enforces short-lived credentials for build agents, and isolates firmware signing with hardware-backed keys and dual control. Backup policy adds immutable storage and periodic restore tests for configuration and key material. Playbooks introduce customer communication templates, phased app updates, and kill-switch criteria for OTA. A follow-up exercise evidences smaller blast radius, recoverable signing infrastructure, and faster time-to-restore cloud services supporting in-home devices

Service Overview

JUMPSEC conduct technically led assessments and controlled simulations to evaluate an organisation's preparedness for a ransomware attack. Engagements deploy benign implants that emulate realistic threat-actor behaviours (discovery, staging, encryption triggers) and test containment, backup integrity, privileged access governance, and recovery orchestration. Outputs prioritise technical and organisational gaps with clear, testable fixes.

Objectives

- Validate ability to detect, contain, and eradicate ransomware-like activity
- Confirm backup resilience, immutability, and time-to-restore for critical services
- Assess identity and endpoint guardrails that limit spread and blast radius
- Exercise decision-making, communications, and regulator-facing documentation

Approach

Delivery combines environment review, tabletop planning, and controlled live-play in approved windows. Benign implants exercise discovery and encryption-trigger paths without impacting production data. Stakeholders include Technology, Security/IR, Business Continuity, Communications, and key suppliers

Method

- **Plan** — define scenarios, success measures, critical systems, authority boundaries, safety gates
- **Prepare** — create test tenants/accounts, safe datasets, and isolate blast zones for live-play
- **Simulate** — run benign implants to emulate discovery, staging, and encryption triggers; observe detection/containment
- **Validate recovery** — test restore workflows, credentials, and sequence for priority services
- **Debrief** — capture timelines, decision points, gaps, and a prioritised uplift plan
- **Improve** — optional re-run to confirm uplift and measure time-to-contain/restore

Deliverables

- Executive briefing (slide deck + debrief): key observations, material risks, and priority actions
- Ransomware Readiness Report:
    - Detection & Containment: alert fidelity, isolation paths, authority checkpoints
    - Identity Guardrails: privileged access, break-glass governance, segmentation
    - Backup & Recovery: immutability, privilege to delete/expire, RTO/RPO evidence

  - Communications & Governance: decision thresholds, stakeholder call-trees, regulator-facing artefacts

- Simulation artefacts (sanitised): benign implant behaviours, timelines, and containment action
- Standards and alignment (embedded): NCSC ransomware guidance, CIS controls for backup/identity, and ATT&CK behaviours used to structure simulation and rationale

Outcomes and benefits

- Evidence-based confidence in containment and recovery readiness
- Reduced blast radius through tighter identity and segmentation controls
- Reliable restores with immutability verified and time-to-restore measured
- Clear playbooks, decision thresholds, and regulator-ready documentation

Pricing model

Fixed price per simulation package (tabletop, live-play, or combined) or time-and-materials aligned to SFIA. Price drivers: number of scenarios, systems in scope, supplier involvement, and level of artefact depth.

Timelines

- Planning and preparation: 1–2 weeks
- Simulation windows: as agreed (tabletop and/or live-play)
- Report issue: 5–10 working days after testing completion
- Optional rerun/verification: by agreement

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement Lead** — scope, governance, quality, stakeholder alignment
- **Technical Lead(s)** — implant build/execution, recovery validation, evidence capture
- **Coordinator** — logistics, comms, supplier alignment, action tracking

Buyer responsibilities

- Nominate executive sponsor and single engagement lead
- Approve scenarios, authority matrix, and simulation windows
- Provide access to representative systems, backup platforms, and relevant runbooks
- Coordinate supplier participation and communications

JUMPSEC responsibilities

- Operate within agreed authority boundaries and safety criteria
- Conduct controlled, non-destructive simulation and minimise operational risk
- Secure handling and time-boxed retention of data and artefacts

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 benign implants; no encryption of production data
- Third-party coordination requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Managed Extended Detection and Response (MXDR)
- IR Readiness Review / Breach Readiness Review
- DFIR: Containment, Forensics, Recovery Support
- 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