# SERVICE DEFINITION
# RESPONSE PLAYBOOK DEVELOPMENT


**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 and consent-then-rule playbooks

A unitary authority needed decisive steps for ransomware and mailbox-led data loss. We discovered permissive exemptions in Conditional Access, observed varied EDR policies across VDI pools, and found that no single owner managed supplier cut-over decisions. JUMPSEC wrote two playbooks that set activation thresholds based on service impact, mapped isolation routes for high-risk cohorts, and captured evidence at every stage. In the mailbox playbook, we joined consent events, rule creation, and endpoint activity into one flow, including communications inserts for public statements and care-provider notifications. We validated the hand-offs between SOC, IT operations, legal, and comms through short tabletop sessions. Leadership adopted the severity matrix, and the council scheduled quarterly verification checks.

### Central government department — Supply-chain compromise and data exfiltration

A department connected to several arm's-length bodies and contractors. The existing runbooks did not address scenarios where a supplier breach created conflicting obligations. We developed a supply-chain playbook that started with upstream notification, clearly defined the triage evidence to request, and set thresholds for network segmentation and key revocation. For data exfiltration, JUMPSEC established brokered export for forensics, triggered regulator prompts, and coordinated parallel communications to ministers and oversight bodies. We conducted a decision rehearsal to confirm the authority path for cutting supplier connectivity and issuing joint statements. After remediation, the department introduced a supplier attestation step as part of the close-out process.

### Global electronics manufacturer— Multi-region ransomware and ERP degradation

A global electronics group asked JUMPSEC to remove ambiguity around isolating finance and manufacturing platforms during ransomware. JUMPSEC discovered regional EDR variance, identified uneven backup immutability, and noticed there was no threshold for pausing intercompany transfers when ERP degraded.

We produced a ransomware playbook with region-specific branches for workstation and server isolation, directed hypervisor and storage evidence capture, and sequenced the hand-off from plant IT to the global incident manager. JUMPSEC created a finance annex that set payment holds, drafted supplier scripts, and established approval checkpoints for partial shipments. We ran a verification drill across two regions and a 3PL, confirming the call-tree, validating safe backups, and achieving faster isolation without missing carrier slots.

### Connected-device manufacturer (CNI) — Supply-chain compromise and safe field remediation

A CNI supplier producing connected edge devices asked us to create a playbook that balanced rapid risk reduction with safety and regulatory constraints. We found gaps such as unclear authority to revoke signing keys, limited field telemetry, and fragmented coordination across engineering, operations, and legal.

JUMPSEC wrote a supply-chain compromise playbook that covered evidence triage, bill-of-materials checks, and decision paths for key revocation and firmware rollback, along with regulator and operator notifications. We used staged containment via feature flags, established a brokered download path for signed updates, and ran a customer advisory process. Our rehearsal shortened the route to revoke artefacts, clarified owner-attributed actions, and proved a rollback plan that preserved service at critical sites.

# Service Overview

JUMPSEC designs incident response playbooks that people can execute under pressure. We translate threat scenarios, technology constraints, and supplier dependencies into clear, stepwise actions with decision thresholds, evidence checkpoints, and routes for legal, regulatory, and communications engagement. We align playbooks to your tooling and roles, reduce ambiguity at hand-offs, and build verification steps so teams can prove readiness and improve over time.

## Objectives

- Establish a consistent, actionable pattern for high-risk incidents across the estate.
- Define isolation criteria, evidence capture, and escalation logic that teams can follow.
- Embed supplier engagement, communications, and regulatory actions with clear ownership.
- Deliver verification artefacts and rehearsal guidance that keep playbooks current.

## Approach

We start by agreeing priority scenarios, target platforms, and the audiences who will run the playbooks. We map current response paths, tool capabilities, and supplier contracts to reveal gaps and friction. We then write task-level flows that specify triggers, roles, tools, commands, and acceptance checks. We run a debrief to confirm feasibility and adoption, followed by optional rehearsal to validate the design. We version the playbooks, document change control, and provide a lightweight maintenance cycle.

## Method

- **Plan** — confirm scenarios, stakeholders, tools, evidence handling, and governance.
- **Discover** — review existing IR materials, SOC runbooks, supplier contracts, and regulatory obligations; map constraints.
- **Validate** — prototype key flows in a safe environment; confirm feasibility and business impact.
- **Analyse** — write playbooks with triggers, actions, thresholds, owner hand-offs, and verification steps; define metrics.
- **Debrief** — present the set, agree ownership and update cadence, and schedule rehearsal or tabletop as required.

## Deliverables

- Playbook Pack covering agreed scenarios (e.g., ransomware, BEC, data exfiltration, supply-chain compromise, insider risk). Each playbook includes activation triggers, isolation thresholds, task sequences by role, tooling steps/queries, evidence capture points, supplier call-trees, comms inserts, and return-to-normal criteria.

- Decision Aids: quick-reference cards, isolation decision tree, severity matrix, and regulator/insurer notification prompts.
- Tooling Appendix mapping playbook steps to your stack (EDR/SOAR/SIEM, M365/Entra/Sentinel, backup/restore, collaboration, ticketing) with exact queries/commands where applicable.
- Verification & Rehearsal Guide with objectives, injects, and acceptance criteria to prove the playbooks work in practice.
- Governance Note defining version control, ownership, review cadence, and alignment to policies.
- Embedded alignment in reporting: NCSC Incident Management guidance, ICO/DPA notification triggers, UK sector expectations where relevant, and linkage to ISO/IEC 27035 for incident handling. (We integrate these standards into the deliverables rather than listing them separately.)

## Outcomes and benefits

- Clear, repeatable actions that reduce time-to-isolate and time-to-recover.
- Less escalations blocked by ambiguity; clean hand-offs between SOC, IT, legal, comms, and suppliers.
- Better evidence capture for investigation, regulator engagement, and insurers.
- A sustainable update cycle that keeps playbooks relevant as the estate changes.

## Pricing model

Fixed price per scenario set and platform scope, or time-and-materials for complex estates. Drivers include number of scenarios, platform diversity, supplier count, and rehearsal depth.

## Timelines

- Planning and discovery: 3–7 working days.
- Drafting and validation: 5–15 working days, depending on scenario count and tooling complexity.
- Report issue: 5–10 working days after testing completion.
- Optional rehearsal and re-issue: by agreement.

## Team and roles

- Engagement Lead governs cadence and quality.
- IR Lead/Detection Engineer authors technical steps and verification checks.
- Operations Advisor shapes legal, regulatory, and stakeholder inserts.
- Coordinator manages artefacts, sign-offs, and version control.

## Buyer responsibilities

- Nominate an executive sponsor and scenario owners.
- Provide access to SOC/IT leads, key suppliers, and tool owners; share relevant policies and contracts.
- Confirm change control and the owners who will maintain the playbooks.

## JUMPSEC responsibilities

- Write practical, tool-aware playbooks with explicit thresholds and evidence points.
- Minimise operational impact and align changes to agreed windows.
- 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; any live exercises are scoped and non-disruptive.
- Third-party participation requires consent and may affect timelines.
- BPSS/SC-cleared personnel available where required.
- Accessible materials (WCAG 2.1 AA) available on request

## Related services

- Cyber Incident Exercising (NCSC Assured)
- IR Readiness Review / Breach Readiness Review
- EDR Efficacy Assessment
- Microsoft-funded Security Workshops (Modern SecOps, Threat Protection)


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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com