SERVICE DEFINITION DOCUMENT
MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

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

- **Central government agency — Conditional access and privileged access strategy**

JUMPSEC conducted an estate-wide review and found that MFA strength varied across user groups, several break-glass accounts were overly permissive, and legacy protocols were still allowed on certain services. We scoped roles in a way that granted standing admin access when just-in-time admin would have sufficed. JUMPSEC configured Sentinel to ingest sign-ins, but we did not include rules to track misuse of emergency access.

We consolidated conditional access templates and enforced phishing-resistant MFA for administrators. JUMPSEC placed emergency accounts under strict usage and monitoring protocols. We replaced standing admin with PIM, and JUMPSEC created Sentinel rules to highlight high-risk sign-ins and role activations. Our verification confirmed that we applied policies consistently and established clearer accountability for privileged actions.

- **Local authority — email security and collaboration controls**

During our Microsoft 365 configuration review, JUMPSEC identified that authentication on shared mailboxes was weak, external sharing in Teams and SharePoint was too permissive, and Safe Links and Safe Attachments policies were not fully implemented. We also found that audit logs did not retain information for a sufficient duration to support investigations.

We strengthened shared mailbox access, applied sensitivity labels, and introduced scoped external sharing policies. JUMPSEC enabled Safe Links and Safe Attachments across priority groups, and extended retention settings to provide broader audit coverage. Our subsequent assessment demonstrated that there were fewer risky shares, improved resistance to phishing, and greater investigative depth.

- **NHS Shared Service — Defender/XDR and Sentinel coverage**

JUMPSEC assessed the environment and identified gaps in Defender sensor deployment on non-persistent endpoints, noted that ASR rules were disabled in clinical images, and found that duplicate Sentinel analytics contributed to alert fatigue. We also discovered that connector configuration omitted several Microsoft sources and key third-party logs. To address these issues, we drove full sensor coverage, staged the enablement of ASR with compatibility testing, and rationalised rules using suppression logic and watchlists. JUMPSEC added additional connectors to increase coverage of identity and endpoint events. In our follow-up review, we demonstrated that incidents became higher in quality and containment readiness improved.

- **Energy utility (CNI) — Azure guardrails and key governance**

We analysed the subscriptions and found inconsistent policy baselines, noted that role assignments at management group level were too permissive, and observed that deployment pipelines used long-lived credentials. JUMPSEC identified a lack of separation of duties in Key Vault permissions and saw that alerting failed to capture key rotation failures. To address these issues, we applied deny-by-default guardrails, narrowed roles to workload boundaries, and moved pipelines to use short-lived credentials. JUMPSEC adopted dual control for key governance and implemented rotation alerts. Our verification confirmed that we constrained privilege paths, improved reliability of key rotation, and established clearer audit trails..

Service Overview

JUMPSEC's managed detection and response service built on Microsoft Defender XDR and Microsoft Sentinel. The service delivers continuous monitoring, investigation, containment support, detection engineering, and incident handling aligned to public-sector operating constraints. Outcomes focus on faster time-to-detect, safer containment, and clearer accountability during and after security events.

Objectives

- Provide 24/7 monitoring, triage, and investigation across Microsoft security telemetry
- Contain and mitigate threats with agreed response actions and playbooks
- Improve signal quality via targeted detection engineering and rule tuning
- Support leadership with clear incident communications and post-incident improvement
- Continuous Improvement model, operating in sprints, to incrementally improve over time

Approach

Operations run from a UK-based team with agreed rules of engagement and change control. Onboarding aligns tenant settings, connectors, and playbooks to local context, data policy, and regulatory needs. Runbooks set who does what, when, and how decisions escalate. Continuous improvement sprints reduce noise and raise fidelity without disrupting service.

Method

- **Plan and onboard** — confirm objectives, assets, response matrix, contacts, and data connectors
- **Stabilise** — baseline telemetry, enable priority analytics, and establish containment pathways
- **Operate** — 24/7 alert handling, investigation, and case management with measurable SLAs
- **Engineer** — tune rules, build custom analytics, and retire noisy detections
- **Review** — service reviews, metrics, and targeted uplift actions; optional purple-test cycles

Deliverables

- **Runbook and RACI pack:** escalation paths, roles, authority boundaries, and regulator engagement channels
- **Operations handbook:** onboarding checklist, connector status, priority analytics catalogue, suppression and watchlists
- **Case artefacts:** investigation notes, evidence captures, and analyst timelines for each security case
- **Containment actions:** user/device isolations, token revocation steps, policy changes executed under authority matrix

- **Continuous Service Performance Metrics and Monthly service report:** KPIs (MTTD/MTTR), alert volumes, case outcomes, attack themes, and improvement backlog
- **Detection engineering outputs:** tuned rules, custom analytics, hunting queries, and suppression logic with acceptance criteria
- **Service review deck:** risks, recommendations, and next-step roadmap with owners and dates
- **Standards and alignment (embedded):** mappings to NCSC CAF/NIST CSF functions, Microsoft recommended practices for Sentinel/Defender, and ATT&CK technique references used for rationale

Outcomes and benefits

- Faster detection and safer, auditable containment actions
- Higher signal quality with less noise and clearer triage paths
- Consistent incident documentation for governance and insurance
- Continuous uplift in posture driven by measured service metrics

Pricing model

Fixed multi-year subscription based on intensive scoping and solution design.

Timelines

- Onboarding and stabilisation: 2–12 weeks (scope dependent)
- Live operations: from go-live with agreed SLAs

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

- **Service Owner** — governance, quality, contract performance
- **Shift Lead / Senior Analyst** — case oversight and escalations
- **Detection Engineer / Content Author** — analytics, hunting, tuning
- **Service Coordinator** — communications, change control, reporting

Buyer responsibilities

- Nominate executive sponsor and operational lead
- Approve authority matrix for containment; provide contact rota
- Provide tenant access/exports, architecture context, and change windows
- Participate in service reviews and approve prioritised improvements

JUMPSEC responsibilities

- Operate within the agreed runbook and authority matrix
- Maintain 24/7 coverage (where contracted) and case documentation quality
- Protect buyer data; retain only for agreed periods; support audits

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-disruptive changes unless explicitly authorised in the runbook
- Third-party coordination requires prior consent and defined contacts
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Cyber Incident Exercising (NCSC Assured)
- Microsoft Security Configuration (Azure/Defender/M365/Entra/Sentinel)
- Detection Engineering and Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com