SERVICE DEFINITION DOCUMENT
CONTINUOUS ATTACK SURFACE MANAGEMENT

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

Copyright (c) 2026 JUMPSEC Ltd | All Rights Reserved: This document or any part of it should not be duplicated or the contents transmitted to any third party without the express approval of JUMPSEC Ltd.

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 — Look-alike domains and citizen phishing risk

JUMPSEC reviewed threat intel feeds and identified dozens of typosquats, some of which held little relevance, and observed that these overwhelmed internal teams. We filtered the data to focus on attacker-useful assets, such as MX-enabled domains, live payment-page clones, and staging infrastructure hosting phishing kits. JUMPSEC analysed kit fingerprints, linking them to payment windows and social-media lure patterns, which enabled us to elevate the handful of cases that genuinely mattered.

JUMPSEC registered priority look-alike domains, carried out registrar and host takedowns, tightened DMARC and SPF alignment, and proactively issued citizen communications referencing only verified domains. We supplied the SOC with watchlists and queries for brand terms, mailbox-rule creation, and unusual egress associated with payment flows. In follow-up runs, we saw a marked reduction in live look-alikes and faster takedown cycles, with fewer false positives reaching the frontline teams.

Energy utility (CNI) — Public cloud storage and secrets exposure

JUMPSEC reviewed TEM/CAASM inventories and found long lists of open buckets and generic "key in code" findings with little context. We emulated attacker sequencing using CASM: repo → key → endpoint → data path. We validated exploitability without carrying out exploitation. Through this approach, we identified a small number of keys that provided live access to telemetry stores, uncovered open object listings linked to migration projects, and detected supplier-owned namespaces leaking operational relationships.

We closed public access, rotated exposed secrets into managed stores, and introduced signed URLs with short TTLs as remediation. JUMPSEC worked to add concrete controls and takedown routes to supplier contracts. We set up SIEM watchlists to flag future appearances of utility namespaces and repo patterns in paste sites and CT logs. Our verification evidenced that we had closed exposures and reduced the time-to-takedown for supplier misconfigurations.

Central government body — Unknown public services and DNS drift

We found that multiple domains and legacy suppliers had created shadow services and stale DNS. Generic EASM/TI feeds generated hundreds of low-value alerts with near-duplicates, which overwhelmed teams. JUMPSEC replicated adversary reconnaissance by chaining CT logs, DNS history, and search engine artefacts, then traced ownership via change trails.

Through this process, we isolated a small set of genuinely abusable endpoints, wildcard exposures, and mis-issued certificates linked to sensitive subdomains. We focussed remediation on five actions: we collapsed wildcards, retired orphaned VIPs, enforced ACME enrolment with expiry gates, gated staging via authenticated ingress, and assigned named owners in DNS. JUMPSEC verified that these steps removed whole classes of drift and cut the external surface area. We supplied the SOC with detections for certificate issuance anomalies and unexpected DNS deltas, enabling them to catch future sprawl early.

Service Overview

JUMPSEC provide ongoing external reconnaissance and validation to identify, verify, and track exposures across internet-facing assets. The service aggregates signals from DNS, TLS, web, cloud, code repos, and third-party sources, then confirms exploitability through safe checks. Outputs prioritise what matters, who owns it, and how to fix it—before attackers exploit it.

Objectives

- Maintain a live inventory of public assets, owners, and business context
- Detect meaningful changes and new exposures quickly
- Validate risk with safe, reproducible checks and clear evidence
- Drive timely remediation and measure risk reduction over time

Approach

Continuous collection and correlation across domains, IP ranges, certificates, cloud resources, and code artefacts. Analysts review signals, remove noise, and confirm impact with non-destructive techniques. Governance embeds ownership, deadlines, and acceptance criteria so fixes land and stay fixed.

Method

- **Plan & seed** — define attack surface scope, ownership model, success measures
- **Discover** — enumerate assets (domains, subdomains, IPs, cloud, apps, repos)
- **Validate** — confirm exposures (config, patching, auth, storage, secrets, DMARC/TLS)
- **Triage & assign** — prioritise, route to owners, set due dates and acceptance tests
- **Verify & track** — re-check fixes, prevent recurrence, and report risk movement

Deliverables

- Executive briefing (slide deck + debrief): exposure themes, material risks, and priority actions
- Attack Surface Inventory (CSV/XLSX): assets, technologies, owners, criticality, exposure flags
- Exposure register (CSV/XLSX): severity, evidence, owners, due dates, acceptance criteria
- Change intelligence**:** weekly/monthly deltas, newly observed services, expired/weak TLS, DNS drift
- Cloud and storage checks**:** public buckets/containers, permissive policies, repo secrets indicators
- Email and brand controls**:** SPF/DMARC/DKIM posture, look-alike domains, abuse takedown support
- Service health snapshots**:** CVE signals, banner issues, default/admin interfaces, weak auth markers

- Standards and alignment (embedded): NCSC internet-facing guidance, CIS controls for inventory and exposure management, provider hardening references cited for rationale

Outcomes and benefits

- Fewer surprises: earlier detection of risky external changes
- Faster, owned fixes with audit-ready evidence of closure
- Smaller external footprint and stronger trust signals for citizens and partners
- Clear trend lines that show risk reduction month by month

Pricing model

Fixed multi-year subscription based on surface size ((domains/IPs/cloud accounts) and initial scoping.

Timelines

- Onboarding and seeding: 1–2 weeks
- Continuous monitoring: from go-live

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, reporting
- **Analyst(s)** — discovery, validation, triage, verification
- **Coordinator** — ownership routing, comms, action tracking

Buyer responsibilities

- Nominate executive sponsor and operational lead
- Seed lists (domains, IP ranges, cloud accounts, brands) and ownership map
- Approve change governance for remediation and verification
- Participate in service reviews and approve prioritised improvements

JUMPSEC responsibilities

- Operate within agreed scope and safe-check rules
- Reduce false positives; provide clear, reproducible evidence
- Protect buyer data; retain only for agreed periods

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

- MXDR
- Network Architecture / Asset Discovery
- Cloud Infrastructure Penetration Testing
- Phishing and Vishing Simulation

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com