SERVICE DEFINITION DOCUMENT
CONTINUOUS RECONNAISSANCE (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

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 — Brand abuse and supplier shadow IT

A council saw phishing complaints that referenced council branding. Continuous recon surfaced multiple typosquats with MX enabled, look-alike subdomains on a third-party platform, and a supplier-hosted webform capturing resident details without council approval.

The programme issued immediate takedown requests, tightened DMARC to reject, and added domain and mailbox watchlists to SOC dashboards. Third-party onboarding gained a DNS and branding checkpoint. Follow-up scans showed no active typosquats, and phishing complaints dropped during the next billing cycle.

National charity — Credential leakage and open storage

A charity relied on volunteers and partner agencies. Recon found staff email/password pairs in recent dumps and a public cloud bucket with event photos that included metadata revealing internal URLs. Actions forced password resets with phishing-resistant MFA, rotated app passwords, and locked the bucket with least-privilege IAM and object-level logging. Detections flagged future appearances of charity addresses in new dumps. Donor-facing portals added stricter sharing defaults. Subsequent sweeps reported no further exposures.

Managed service provider — Multi-tenant namespace sprawl

An MSP's growth created overlapping subdomains and shared storage patterns across clients. Recon mapped assets to clients, identified shared naming schemes that leaked client relationships, and found permissive public links.

The fix introduced per-tenant naming, hardened sharing defaults, and takedown of stale links. A per-tenant exposure register and watchlists gave faster SOC triage while preserving isolation. Subsequent trends showed a steady reduction in public links and cleaner DNS hygiene across tenants.

Global retailer — CT log drift and exposed test endpoints

Certificate Transparency monitoring showed unexpected new certs for a forgotten subdomain. Enumeration revealed a test endpoint with default creds and verbose errors.

DNS and WAF rules retired the endpoint, keys were revoked, and CT alerts fed a watchlist to catch future drift. Build pipelines added ownership tags and a DNS approval step. Later digests showed stable namespaces and no new stray endpoints during peak trading.

Service Overview

JUMPSEC runs continuous, attacker-style reconnaissance against the external estate to surface anything useful to an adversary before it is exploited. The service goes beyond vulnerability scanning. It hunts for exposed assets, misconfigurations, leaked credentials, code and secrets, weak email posture, shadow IT, risky third-party footprints, and brand or domain abuse.

Coverage spans internet-facing services, DNS/TLS, cloud object storage, code and package registries, mobile app stores, paste sites, CT logs, BGP/ASN changes, and phishing or typosquat infrastructure. Outputs arrive as rapid alerts for urgent items and a curated backlog that can be fixed, blocked, or taken down

Objectives

- Identify externally visible exposures an attacker would weaponise at any stage.
- Track asset changes and third-party drift to prevent surprise attack paths.
- Enable swift takedown, blocking, or hardening with owner-attributed actions.
- Feed detections and playbooks so SOCs spot related activity earlier.

Approach

JUMPSEC establishes a safe, permissioned recon programme that mirrors real attacker workflows under strict legal and rate-limit controls. Discovery combines domain intelligence, certificate transparency, platform enumerations, search engine dorks, code and credential sweeps, storage probing using non-destructive methods, OSINT, and continuous differential monitoring.

Findings are validated, de-duplicated, and risk-ranked. Urgent items trigger alerts with clear actions and owners and lower-risk items managed with acceptance criteria. Takedown and registrar/provider engagement are initiated and tracked. Detections and response inserts are supplied to close the loop.

Method

- **Planning and Rules of Engagement.** confirm owned namespaces, brands, ASNs, clouds, and third-party scope; define alerting, takedown authority, and evidence handling.
- **Discover.** Enumerate assets and signals: DNS, CT, TLS, MX/SPF/DMARC, object storage, code repos, package registries, containers, app stores, paste sites, social, search engines, Shodan/Censys, vendor portals.
- **Validate.** Verify ownership and risk; confirm read-only access only; avoid exploitation; enrich with WHOIS, hosting, geos, and related indicators.
- **Analyse.** Rank impact and ease of abuse; define exact actions (block, rotate, remove, reconfigure, takedown) with owners and acceptance tests.
- **Deliverables.** Push rapid alerts, weekly digests, and a living exposure register; supply SIEM/SOAR detections and a short retest plan for closed items.

Deliverables

- **Rapid alerts** for high-risk exposures with evidence, business impact, and exact next steps.
- **Exposure Register** covering assets, findings, ownership, action status, acceptance criteria, and verification notes.
- **Takedown & Brand Protection pack:** pre-filled registrar/host templates, DNS changes, and block-list updates.
- **Detection & Response inserts:** KQL/Sigma queries, watchlists, and playbook steps tied to recon signals.
- **Weekly/monthly digest and trend view:** new assets, drift, recurring issues, and third-party movements.
- **Embedded alignment in reporting:** NCSC guidance on monitoring and supply-chain risk; MITRE ATT&CK "Reconnaissance" and "Resource Development" tactics; DMARC/SPF/ DKIM best practice.

Outcomes and benefits

- **Fewer easy wins for attackers;** reduced brand and domain abuse.
- **Earlier SOC visibility** of staging and domain/tooling set-up by adversaries.
- **Faster remediation** and takedown with owner-attributed, auditable actions.
- **Measurable reduction** in exposed surface and credential/secret leakage.

Pricing model

Subscription based on scale thresholds and or bespoke scopes. Pricing drivers include organisational scale and threat profile, namespace breadth, third-party count, alerting SLAs, , and integration depth

Timelines

- Typical Onboarding and baselining: 5–20 working days.
- Continuous monitoring: ongoing; urgent alerts in near real-time.
- Digests/Reports and exposure register updates: weekly or monthly.

Security and assurance

Facilitation is delivered by experienced practitioners using peer-reviewed methods and internal quality checks. Materials are reproducible and traceable to session evidence. Where appropriate, behaviours are mapped to MITRE ATT&CK and translated into detection opportunities for SOC/EDR teams. Accessibility options are available on request.

Team and roles

- **Engagement Lead.** Scope, governance, quality management, and stakeholder alignment.
- **Recon and TI Analysts.** OSINT, enumeration, validation, and takedown workflow.
- **Detection Engineer.** SIEM/SOAR/KQL content and watchlists.
- **Coordinator.** Artefacts, ownership tracking, and supplier/registrar liaison.

Buyer responsibilities

- Confirm owned domains/brands, clouds, and third-party scopes.
- Takedown authority routes and change windows for DNS and controls.
- Align SOC and comms contacts for alert routing and brand protection.

JUMPSEC responsibilities

- Operate within agreed legal and technical boundaries; no exploitation.
- Validate and de-duplicate results; minimise noise; provide clear actions.
- Handle artefacts securely with least-privilege access and agreed retention.

Data protection and privacy

The buyer remains the data controller; JUMPSEC acts as processor. Only the minimum necessary evidence is collected and retained. Secure transfer, access control, and agreed retention periods apply throughout the engagement. On completion, data and credentials are returned or securely destroyed.

Constraints and assumptions

- Public/permissionless collection only; no intrusive testing or service disruption.
- Takedown outcomes depend on registrars, hosts, and platforms; timelines can vary.
- Third-party assets require contractually agreed inclusion or owner consent.
- Rate limits and provider APIs may throttle collection.
- Exercises are non-destructive and time-boxed.
- Third-party involvement requires prior written consent.
- Personnel with BPSS/SC clearance are available where required.
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA)

Related services

- Threat Modelling
- Log Validity Assessment
- Detection Engineering and SOC Use Case Tuning
- Red Teaming and Purple Teaming

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com