SERVICE DEFINITION DOCUMENT: COMPROMISE ASSESSMENT / THREAT HUNTING SWEEP

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 — Unauthorised OAuth consent and data staging in revenues services

We collected logs across identity, email, and collaboration platforms and flagged new OAuth consent grants to an unverified app from a small group of officer accounts. Our audit trails recorded off-hours Graph/API calls that enumerated council tax and benefits folders, followed by bulk downloads from a shared workspace. On two laptops, we identified endpoint artefacts, including recent browser extension installations, token cache files, and scheduled tasks that aligned with the access window.

We remediated the incident by revoking the rogue app consent tenant-wide, invalidating refresh tokens, and resetting affected credentials. We applied Conditional Access controls to add consent restrictions and device/state requirements for privileged roles. In addition, we removed mailbox rules and delegated accesses and enforced API throttles to limit large exports pending review. Our verification sweeps confirmed that no further unauthorised API calls had occurred, inbox rule sets were clean, and no new token artefacts appeared on the examined endpoints.

Energy distribution operator (CNI) — Persistence and lateral movement traces

We hunted across admin jump hosts and directory services, identifying new local users, modified startup entries, and service configurations that matched common persistence techniques. We observed Kerberos ticket patterns that indicated repeatable lateral movement between specific hosts during maintenance windows.

To remediate the incident, we disabled suspect accounts and services, rotated credentials on affected systems, and enforced hardened admin paths. In our follow-up checks, we confirmed the removal of persistence points and a return to normal ticket patterns during subsequent maintenance cycles.

Charity — Suspicious mailbox activity and contractor access

We analysed email telemetry and discovered forwarding rules that had been created on several shared mailboxes, along with anomalous sign-ins originating from contractor IP ranges. We identified token refresh behaviour in identity logs from unmanaged devices, which coincided with spreadsheet exports from donor systems.

To remediate, we revoked sessions, removed unauthorised rules, and reissued credentials. We tightened guest and contractor access, shortened token lifetimes, and enabled alerts for rule creation and large export events. Our verification sweeps confirmed clean mailboxes, expected sign-in behaviour, and the absence of further large exports from donor data stores.

Service Overview

JUMPSEC conduct a point-in-time assessment and targeted threat hunt to identify evidence of historical or ongoing compromise. The engagement analyses endpoint, identity, and infrastructure telemetry, correlates artefacts, and runs hypothesis-driven hunts using current threat intelligence. Outputs prioritise credible leads, explain impact, and provide clear next steps for containment and recovery.

Objectives

- Detect residual indicators of compromise across hosts, identities, and infrastructure
- Validate or refute hypotheses derived from threat intelligence or suspicions
- Provide reproducible evidence, timelines, and recommended actions
- Improve future readiness through targeted gaps and verification steps

Approach

Activities combine retrospective analysis, live sweeps, and hypothesis-driven hunts. Work covers high-value systems, representative endpoints, identity platforms, and key SaaS/cloud services. Delivery uses read-only access and non-disruptive methods in agreed windows. Stakeholders include Technology, Security, and, where relevant, Legal/IG and Communications.

Method

- **Plan** — clarify concerns, scope priority assets, confirm windows, escalation, and evidence handling
- **Collect** — gather logs/artefacts (endpoint, identity, email, proxy, VPN, DNS, cloud), deploy lightweight collectors if required
- **Hunt** — run TI-led and behaviour-led hypotheses (persistence, credential misuse, lateral movement, data staging)
- **Correlate** — pivot across sources, build timelines, and assess impact/feasibility
- **Debrief** — document findings, provide actions (containment, eradication, recovery), and define verification tests
- **Improve** — optional verification sweep to confirm closure and uplift

Deliverables

- Executive briefing (slide deck + debrief): what was found, why it matters, and immediate actions
- Compromise Assessment & Hunting Report:
    - Findings with evidence, affected hosts/accounts, and timelines
    - Hypotheses tested, rationale, and outcomes (confirmed/refuted/inconclusive)

  - Gaps impacting detection/response with targeted uplift recommendations
  - IOC/IOA pack (CSV/JSON): hashes, domains, IPs, regex, and detection queries for follow-up checks

- Exposure register (CSV/XLSX): issues, severity, owners, due dates, acceptance criteria
- Verification checklist: discrete tests to confirm eradication and safe recovery steps
- Standards and alignment (embedded): ATT&CK technique names for rationale, NCSC incident handling principles, and mapping to CAF/CSF functions to support governance

Outcomes and benefits

- Clear confirmation or refutation of suspected compromise
- Actionable steps to contain, eradicate, and recover with confidence
- Better readiness through resolved visibility and process gaps
- Credible artefacts for governance, audit, and insurer dialogue

Pricing model

Fixed price per defined scope/sweep or time-and-materials aligned to SFIA. Price drivers: log coverage, estate size, source diversity, artefact depth, and optional verification sweep.

Timelines

- Planning and access: 2–5 working days
- Collection and hunting: 1–2 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification sweep

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
- **Threat Hunter(s) / DFIR Consultant(s)** — collection, analysis, hypothesis testing
- **Coordinator** — ownership routing, comms, action tracking

Buyer responsibilities

- Nominate executive sponsor and operational lead
- Provide access to telemetry, platform exports, and priority asset lists
- Confirm change windows and coordinate any supplier participation

JUMPSEC responsibilities

- Operate within agreed rules of engagement and authority boundaries
- Minimise operational impact during collection and validation
- Secure handling and time-boxed retention of evidence 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-disruptive collection and hunting in approved windows
- 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

- MXDR
- IR Readiness Review / Breach Readiness Review
- DFIR: Containment, Forensics, Recovery Support
- 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