SERVICE DEFINITION

PURPLE TEAMING / COLLABORATIVE ADVERSARIAL SIMULATION

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 — MXDR-led uplift during phishing and mailbox rule abuse

During our MXDR engagement with a metropolitan council, JUMPSEC identified that high alert volumes with low precision plagued Microsoft 365 and Sentinel. We found that default analytics duplicated signals, and mailbox rule creation following credential reuse became lost in the noise, especially during payroll and benefits peaks. We also discovered that the council permitted OAuth consent from unverified publishers, and forwarding to external domains went unchallenged. Through our case handling, we noticed that triage was slow because enrichment for user role sensitivity, device posture, and recent admin activity was missing.

To address these challenges, we—JUMPSEC—rationalised content, introduced sequence-based analytics for consent-then-rule creation, and added detections for archive-and-exfiltration patterns in SharePoint and OneDrive. We implemented suppressions for maintenance windows and migration tasks. Our playbooks gained clear isolation criteria for privileged identities and guided revocation steps. After these changes, our post-engagement reporting showed that alert volumes dropped materially, triage became faster, case conversion rates increased, and we interrupted credential replay attempts against staff and contractor accounts earlier, which boosted confidence ahead of election and year-end workloads.

Retail bank — Business-email compromise to payment fraud sequence

JUMPSEC ran campaigns across regional finance teams and discovered weak controls around delegated mailbox access and payment approval via email. We emulated attacker behaviours by gaining a foothold with benign OAuth consent, creating forwarding rules, and staging supplier-change requests that exploited month-end pressure. JUMPSEC observed that existing analytics triggered on generic indicators but failed to recognise the consent-to-rule sequence or correlate with payment workflow systems. Our analysts experienced delays in triage, having to chase context across identity, email, and ERP logs.

We designed sequence-based detections for rogue consent followed by forwarding rules, surfaced high-risk scopes, and enriched alerts with ERP vendor records and recent bank detail changes. JUMPSEC updated playbooks to include step-up verification for supplier amendments and rapid revoke steps for risky consent events. Our post-engagement metrics demonstrated fewer false positives, faster isolation of compromised mailboxes, and blocked supplier-change attempts before release cut-offs.

Emergency services organisation — Identity misuse during incident surges

During major incidents, operational surges often masked abnormal access. We emulated attacker behaviours by using benign artefacts to access shared incident folders, escalate privileges with stale service accounts, and stage exports from CAD and records systems. JUMPSEC observed that existing rules only triggered on thresholds and did not correlate with duty rosters, device posture, or authorised incident IDs, which resulted in late or noisy alerts during periods of peak demand.

Through our purple team iterations, we introduced roster-aware analytics, correlated access with incident tickets, and added device-health context for privileged sessions. JUMPSEC defined isolation criteria in response runbooks to preserve core dispatch while containing suspect identities. We evidenced that these changes delivered prompt, context-rich alerts during surge windows, enabled faster containment decisions, and ensured uninterrupted front-line operations.

Service Overview

JUMPSEC conduct collaborative, goal-driven programmes that pair adversary techniques with live detection and response improvement. Offensive operators emulate realistic TTPs in short, controlled iterations while defenders observe, tune, and verify detections and playbooks in real time. Each iteration finishes with measurable uplift: clearer analytics, faster triage, and reliable isolation steps aligned to change control.

Objectives

- Exercise priority attacker behaviours end-to-end and make them observable
- Design and deploy high-fidelity analytics with suppression for expected patterns
- Harden response playbooks with explicit triggers, owners, and rollback points
- Evidence improvement with before/after metrics and verification tests

Approach

Work begins with a goals and hypotheses workshop to select behaviours, data sources, and success measures. Iterations run in agreed windows using safe, non-destructive techniques and benign artefacts. Activities include emulate-observe-tune cycles, A/B testing of rules, hunt query development, and playbook rehearsal. Stakeholders usually include SOC, Detection Engineering, IR, and platform owners.

Method

- **Plan** — prioritise behaviours, confirm data availability, define metrics, change windows, and evidence handling
- **Emulate** — execute controlled techniques mapped to ATT&CK across identity, endpoint, email, cloud, and network
- **Observe** — trace signals, enrich context, and document false-positive drivers and blind spots
- **Tune** — design analytics, suppression, watchlists, and hunt queries with test artefacts
- **Validate** — run verification tests and promote content via change control with rollback
- **Debrief** — record results, ownership, and next-iteration goals with acceptance criteria

Deliverables

- Executive briefing (slide deck + debrief) describing objectives, behaviours exercised, observed gaps, and priority actions
- Purple Content Pack including new and/or updated detections with logic, rationale, test artefacts, enrichments, suppressions, and hunt queries

- Response playbook updates defining triggers, isolation criteria, evidence checkpoints, and escalation paths
- Coverage and Noise Report with before/after alert volume, precision indicators, MTTD/MTTR proxies, and case conversion where available
- Issue register (CSV/XLSX) assigning actions, owners, due dates, and acceptance criteria
- Standards and alignment (embedded) mapping behaviours to MITRE ATT&CK, and linking outcomes to NCSC CAF/NIST CSF functions and vendor best practice for the target SIEM/XDR

Outcomes and benefits

- Higher signal quality and reduced alert fatigue
- Faster, more consistent investigations and isolation decisions
- Measurable coverage against priority behaviours with verification tests
- Repeatable engineering cycle owned by SOC and platform teams

Pricing model

Fixed price per sprint (e.g., 2–3 weeks) or time-and-materials aligned to SFIA. Price drivers include platform mix, behaviour count, telemetry breadth, and reporting depth.

Timelines

- Planning and scoping: 3–5 working days
- Purple iterations: 1–3 weeks depending on behaviours and environments
- Report issue: 5–10 working days after testing completion
- Optional follow-on sprints scheduled by agreement

Team and roles

- **Engagement Lead** for governance, cadence, and quality
- **Adversarial Simulation and Offensive Consultant(s)** for controlled emulation and artefact creation
- **Detection Engineer(s)** for content design, testing, and promotion
- **Coordinator** for logistics, evidence handling, and action tracking

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

- **Engagement Lead** — scope, governance, quality management, stakeholder alignment
- **Adversarial / Offensive Consultant(s)** - execution, tradecraft, and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a service owner and SOC contact
- Provide access to content libraries, telemetry, and case data (redacted where needed)
- Approve promotion windows and response playbook changes

JUMPSEC responsibilities

- Operate within agreed authority and change control
- Provide reproducible test artefacts and clear rollback plans
- Handle data securely with 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

- Non-destructive techniques only and no denial-of-service
- 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

- Detection Engineering and SOC Use Case Tuning
- Cyber Incident Exercising (NCSC Assured)
- Compromise Assessment / Threat Hunting Sweep

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com