SERVICE DEFINITION
DETECTION ENGINEERING AND SOC USE CASE TUNING

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

Global education group — untuned detections and missed behaviours

JUMPSEC inherited a multi-tenant Microsoft estate that had been plagued by excessive, low-value alerts. The previous SOC had left default analytics switched on, resulting in duplicate alerts across Defender and Sentinel, with no suppression for recurring patterns. Consequently, identity abuse slipped through the cracks—OAuth consents from unverified publishers, mailbox rule exploitation, and risky sign-ins were buried within the alert noise. Data staging in SharePoint and OneDrive only triggered threshold-based notifications, lacking the necessary context. Case conversion rates remained low, mean-time-to-detect stayed high, and analysts repeatedly reopened incidents due to insufficient enrichment and unclear ownership.

We rationalised the content, eliminating alert overlap and introducing entity- and sequence-based analytics. Our team enriched detections with device posture, role sensitivity (student, staff, faculty), and geovelocity. We deployed new rules to capture rogue OAuth consents, suspicious mailbox rule creation, archive-and-exfiltration sequences, and contractor access outside approved windows. Suppression logic was implemented to account for maintenance periods and migration tasks. Our post-implementation reporting demonstrated a significant reduction in alert volume, increased detection precision, faster triage, and clearer escalation pathways. This restored confidence in the security service for both regional schools and central IT teams.

Water utility (CNI) — contractor misuse and time-bound access

JUMPSEC identified that contractor identities had accessed administrative pathways outside of authorised timeframes. The detection rules triggered inconsistently because the relevant schedules were maintained in disparate systems and had not been properly normalised. As a result, our analysts struggled to reliably differentiate between legitimate maintenance activities and potential misuse.

We developed new content that cross-referenced contractor groups, approved maintenance windows, and associated change tickets. Our updated analytics generated incidents only when contractors accessed systems outside approved windows or without corresponding change tickets. We implemented suppression logic to exclude authorised maintenance activities. Subsequent metrics demonstrated more accurate detections, a reduction in false positives, and clearer, actionable evidence to support supplier management.

Local authority — mailbox rule abuse and OAuth consent

JUMPSEC delivered detection packs that incorporated patterns for suspicious rule creation and consent from untrusted publishers, all enriched with user risk and inbox behaviour. We implemented suppression to exclude recognised administrative tasks and migration windows. Our service reporting demonstrated that we identified genuine abuse more quickly and significantly reduced alert fatigue for the SOC team.

Service Overview

JUMPSEC conduct a targeted uplift of SOC content to raise ingestion and alert quality and reduce noise. The engagement analyses current analytics, hunts, enrichments, and suppression logic. It then designs, tests, and deploys high-value detections with clear ownership and acceptance criteria. Outcomes focus on better fidelity, faster response, and traceable improvement.

Objectives

- Identify coverage gaps against priority threats and high-risk behaviours
- Tune or retire noisy rules and add context-rich analytics
- Provide hunt queries, playbook hooks, and suppression strategies
- Embed measurement so improvements persist across releases

Approach

Evidence-led review of existing content, telemetry, and incident patterns. Work runs in non-production first, then promotes to live via change control. Activities include content design, test data generation, A/B comparisons, and documentation for handover. Stakeholders usually include SOC, Detection Engineering, and Platform owners.

Method

- **Plan** — prioritise threats/use cases, confirm success metrics, define change windows
- **Assess** — evaluate current rules, hunts, enrichments, false-positive drivers, and gaps
- **Engineer** — build/test detections, enrichments, and suppressions with test artefacts
- **Promote** — deploy via change control with rollback points and monitoring
- **Debrief** — document results, owners, and measures; schedule follow-on sprints

Deliverables

- **Executive briefing** (slide deck + debrief): where value increases, what changes, who owns it
    - Detection Content Pack:
    - New/updated analytics with logic, rationale, and test artefacts
    - Enrichments (watchlists, context joins), and suppression criteria
    - Hunt queries aligned to high-risk behaviours and threat intel
    - Playbook hooks for response and ticketing

- **Coverage and Noise Report:** before/after metrics (precision/recall, alert volume, case conversion, dwell indicators)
- **Runbook updates:** deployment steps, rollback, and maintenance notes
- **Issue register (CSV/XLSX):** actions, owners, due dates, acceptance criteria
- **Standards and alignment (embedded):** mappings to ATT&CK techniques, NCSC CAF/NIST CSF functions for governance context, and vendor best practices for the target SIEM/XDR

Outcomes and benefits

- Higher-fidelity alerts with reduced noise and clearer triage paths
- Faster investigations with richer context and fewer escalations
- Measurable coverage against priority threats and behaviours
- Repeatable engineering cycle with accountable ownership

Pricing model

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

Timelines

- Planning and preparation: 1–2 weeks
- Simulation windows: as agreed (tabletop and/or live-play)
- Report issue: 5–10 working days after testing completion
- Optional rerun/verification: by agreement

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, stakeholder alignment
- **Detection Engineer(s)** — content design, testing, and deployment
- **Coordinator** — logistics, comms, supplier alignment, 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 change control and authority boundaries
- Provide reproducible test artefacts and clear rollback plans
- Secure handling and time-boxed retention of 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 testing in staging before promotion
- 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 on Microsoft stack (Managed Detection and Response)
- Compromise Assessment / Threat Hunting Sweep
- IR Readiness Review / Breach Readiness Review

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com