SERVICE DEFINITION
EDR/XDR EFFICACY ASSESSMENT

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 — EDR inside an IT managed service with weak security depth

JUMPSEC assessed a council's EDR setup provided through an IT managed service and found that stability was prioritized over actual risk. Prevention features were disabled, outdated exclusions let threats slip by, and incident responses relied on generic playbooks lacking context. Updates lagged, and leaders could only view broad metrics, not detailed security data.

To address this, JUMPSEC reviewed efficacy and tested various attack scenarios, tracing weak alerts to policy gaps and missing enrichments. The team enforced tamper protection, removed legacy exclusions, and introduced improved detection with consolidated alerts. Governance changes separated IT operations from security assurance, established content update windows, and set new isolation criteria. These steps led to faster, clearer alerts and containment, maintaining service SLAs.

Global law firm — Outsourced SOC with noisy alerts and blind spots

JUMPSEC worked with a global practice operating a single EDR platform alongside an outsourced SOC. We found that alert queues frequently flooded with low-value noise on generic behaviours, while incidents involving credential theft and archive-and-exfil events surfaced with weak context. During our emulation exercises, we targeted token theft from browser stores, LSASS-adjacent access, and staged compression to network shares across fee-earner laptops and VDI pools. Our results revealed that exclusion sets muted detections on high-load endpoints, missing telemetry on ephemeral VDI sessions, and enrichment gaps obscured user and matter context.

We remediated the issues by replacing broad exclusions with targeted performance profiles, enabling credential access protections, and introducing multi-signal analytics that joined process lineage, network destinations, and archive operations. JUMPSEC also provided the SOC with new triage checklists and established isolation thresholds tied to case impact. Our verification confirmed that we reduced false alerts, delivered richer context in the first alert, and enabled faster isolation decisions during cross-time-zone hand-offs.

Retail bank — hybrid MDR with in-house analysts

A retail bank split responsibility between an MDR provider and its internal team, with controls differing across teller devices, trading endpoints, and remote workforce laptops. We modelled persistence, data staging, and selective exfiltration to cloud storage in our emulations. Our analysis revealed that tamper protection was inconsistent, sensor rollout in payment testing VMs was incomplete, and analytics often keyed on noisy indicators without confirming with peer data. To address these issues, JUMPSEC enforced tamper protection across the bank, completed sensor coverage using gold-image pipelines, and deployed content that joined process, registry, and network evidence into single, high-confidence alerts. We introduced runbooks with decision thresholds for containment on regulated devices and created an auditable bypass path for critical trading sessions. When we retested, we confirmed consistent coverage, higher precision on exfiltration alerts, and reduced investigation time across shifts

Service Overview

JUMPSEC independently assesses your EDR/XDR to prove real-world prevention, detection, and response performance. We examine policy posture, sensor coverage, telemetry quality, alert precision, response playbooks, and SOC runbooks. We exercise ATT&CK-mapped techniques using safe emulations, chaining behaviours such as archive-and-exfiltration, credential theft, and lateral movement. We then deliver tuned analytics, policy changes, and response triggers that land cleanly through change control with verification artefacts.

Objectives

- Measure prevention, detection, and response performance against priority behaviours.
- Close coverage gaps and raise signal quality while reducing false alerts.
- Deliver tested analytics, policy changes, and response triggers with acceptance criteria.
- Leave behind verification artefacts that sustain performance through platform updates

Approach

The engagement starts with scoping to confirm models, orchestration framework, retrieval stack, tools/plugins, data classifications, and acceptable use boundaries. JUMPSEC analyses system prompts and safety policies, then exercises adversarial inputs that chain injection with tool calls, RAG pivots, or downstream actions. Testing deliberately targets model overreliance and excessive agency, validates output sanitisation and content provenance, and inspects the supply chain for model, embedding, or plugin trust issues. Work remains non-destructive and uses synthetic or redacted data wherever possible. Recommendations are sequenced for safety, include rollback, and align to your change windows.

Method

- **Plan** — confirm objectives, authority, artefacts, and safety gates; agree target behaviours and KPIs.
- **Discover** — review policies, coverage, logging, integrations, and runbooks; map asset groups and control variances.
- **Validate** — run controlled emulations for agreed techniques and sequences; capture alert paths, enrichment, and response steps.
- **Analyse** — quantify precision, context, and time-to-detect; define policy changes, analytics, and runbook updates with acceptance criteria.
- **Debrief** — present actions, owners, sequencing, and verification tests; agree retest and adoption plan

Deliverables

- Executive briefing that explains measured performance, material gaps, and expected uplift after change.
- EDR Efficacy Report with evidence per behaviour: inputs, expected signals, observed signals, root cause, exact remediation, rollback, and acceptance criteria.
- Detection Content Pack (platform-native queries/rules, Sigma/KQL where applicable), watchlists, enrichments, and suppressions to reduce noise.
- Policy and Configuration Change Set covering prevention controls, exclusions, sensor health, tamper protection, and data retention.
- Runbook and Playbook Updates describing triggers, isolation thresholds, evidence capture, and escalation routes.
- Verification artefacts: replay steps, event IDs, alert IDs, dashboards, and a short retest plan.
- Embedded alignment in reporting: ATT&CK technique mapping, NCSC guidance on logging and monitoring, and references to platform hardening baselines

Outcomes and benefits

- Higher signal quality with richer context and fewer false alerts.
- Assured coverage of priority behaviours and sequences that matter to the organisation.
- Evidence to support service uplift discussions with third party providers.
- Faster investigations and clearer isolation decisions with auditable response paths.
- Confidence for boards, auditors, and insurers backed by verification evidence.

Pricing model

Fixed price based upon scope, or time-and-materials for complex, multi-platform environments. Price drivers include endpoint count, OS mix, integration breadth, behaviour set size, and retest depth.

Timelines

- Planning and access preparation: 3–5 working days.
- Execution and analysis: 5–20 working days depending on scope.
- Report issue: 5–10 working days after testing completion.
- Optional validation and support by agreement

Team and roles

- Engagement Lead for governance and quality.
- Adversarial/Offensive Consultant(s) for configuration review, emulations, and content development.
- SOC Advisor for runbook tuning and operational adoption.
- Coordinator for logistics, artefacts, and change control

Buyer responsibilities

- Nominate a single engagement lead and SOC/platform owners.
- Provide policy exports, coverage reports, access to test hosts, and logging views.
- Align change control and windows for policy and content adoption.

JUMPSEC responsibilities

- Operate within agreed safety gates and authority.
- Use non-destructive emulations and minimise operational impact.
- Provide precise fixes with rollback notes and verification 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

- No destructive payloads or denial-of-service.
- Third-party managed platforms require written consent for policy changes.
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Purple Teaming / Collaborative Adversarial Simulation
- Detection Engineering and SOC Use Case Tuning
- 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