SERVICE DEFINITION
LOG VALIDITY 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 — Recoverable timelines for mailbox rule and consent abuse

A council asked us to reconstruct consent-then-rule attack sequences. We collected data spanning Entra ID sign-ins, consent events, Exchange rule creations, and endpoint alerts. However, our parsers dropped critical fields and clocks drifted across services, making it difficult for analysts to correlate sign-ins, mailbox changes, and process lineage without resorting to manual effort.

In our assessment, JUMPSEC introduced reliable time synchronisation, fixed the parsers to preserve actor, resource, and decision fields, and added joins to link consent, rule creation, and endpoint events. We built dashboards to expose missing sources and parse failure rates. When we re-tested, our analysts built a clear timeline within minutes, with earlier, higher-confidence alerts routed to the right queue.

NHS trust — Evidence integrity for patient-impacting investigation

A trust needs defensible evidence for regulator and insurer scrutiny. Log transport uses mixed agents and ad-hoc collectors; integrity checks are inconsistent and retention doesn't match policy. During drills, exported artefacts lack hashing and provenance.

An integrity pathway is designed: clock discipline, hashing at collection, immutable storage for priority streams, and a documented export procedure with access logging. Parsers are hardened and normalisation maps are standardised. Verification demonstrates tamper-evident artefacts, complete timelines, and faster legal review, with no clinical system disruption.

A trust required defensible evidence for regulator and insurer scrutiny. Log transport relied on mixed agents and ad-hoc collectors; integrity checks varied and retention did not align with policy. During drills, we exported artefacts that lacked hashing and provenance.

JUMPSEC designed an integrity pathway: we enforced clock discipline, performed hashing at collection, and used immutable storage for priority streams. We documented the export procedure and implemented access logging. Our team hardened parsers and standardised normalisation maps. We verified tamper-evident artefacts, complete timelines, and enabled faster legal review, all without disrupting clinical systems.

Retail group — Blind spots in cloud ingress and egress

A national retailer ingests firewall and proxy logs but misses cloud ingress/egress events and several SaaS admin actions. Analysts see symptom alerts without the surrounding narrative.

Cloud audit sources are added, schema mismatches fixed, and joins created that link identity, network egress, and storage actions. A coverage dashboard tracks source health and drop rates. Post-change metrics show fewer false positives, richer context on first alert, and measurable reductions in investigation time during peak trading.

Managed service provider — multi-tenant parsing and tenancy isolation

An MSP forwards client logs through a shared broker. Parser versions differ by tenant; a shared index allows accidental cross-tenant lookups. Triage is slow and risky.

Parser deployment is standardised, tenant-scoped indices with access controls enforced, and per-tenant health dashboards provided. A small correlation pack supplies high-confidence joins without breaking isolation. Re-test confirms clean tenancy boundaries, higher parse success, and faster client-specific investigations.

Service Overview

JUMPSEC validates whether your security logging is present, trustworthy, and usable for detection and investigation. We test that the right events exist at the right fidelity, arrive in the right place, and can support incident timelines without gaps or integrity doubt. We focus on source coverage, schema and time accuracy, end-to-end transport, normalisation and enrichment, and the controls that protect evidence during and after an incident.

Objectives

- Prove that priority event sources generate complete, accurate, and timely logs.
- Confirm transport, parsing, and normalisation preserve meaning and integrity.
- Evidence that analysts can reconstruct an incident with defensible timelines.
- Deliver precise fixes and acceptance tests that sustain logging quality.

Approach

We start by agreeing the critical systems and the attacker behaviours you care about. We map sources to required events, review collection and transport, and sample records at source and destination. We verify time synchronisation, schema consistency, parsing success, and enrichment quality. We then trace exemplar attack sequences through your tooling to confirm joins, pivots, and retention are adequate. Changes are sequenced for safe adoption and include rollback notes.

Method

- Plan — confirm objectives, priority behaviours, sources, retention targets, and evidence handling.
- Discover — inventory sources, agents, collectors, brokers, SIEM/XDR parsers, schemas, and time sync.
- Validate — generate safe test events and replay benign sequences; compare source vs destination, check loss, drift, and parse failures.
- Analyse — quantify coverage, fidelity, and timeline reconstructability; define exact fixes with acceptance criteria.
- Debrief — present actions, owners, sequencing, and verification artefacts; agree re-test.

Deliverables

- Executive briefing describing material gaps, business impact, and expected uplift after change.

- Log Validity Report with evidence: per-source findings, sample events (redacted), observed/expected fields, parse and drop rates, time-drift metrics, and exact remediation with rollback and acceptance criteria.
- Optional Detection Enablement Pack: updated parsers/normalisers, field maps, sample KQL/Sigma queries, correlation joins, and watchlists for high-value entities.
- Optional Chain-of-Custody & Integrity memo: time sync design, hashing and immutability options, access control, and export procedures for investigation and legal defensibility.
- Embedded alignment in materials: NCSC Logging and Protective Monitoring guidance, MITRE ATT&CK mapping for chosen behaviours, Microsoft/Splunk hardening notes where relevant, and ISO/IEC 27001 Annex A links for governance traceability

Outcomes and benefits

- Analysts see earlier, clearer signals with reliable entity context.
- Incident timelines become defensible and faster to assemble.
- Fewer blind spots and parse failures; reduced false positives.
- Better insurer, auditor, and regulator assurance.

Pricing model

Fixed price per estate band and platform set, or T&M for complex estates. Price drivers: source count, platform diversity, retention objectives, behaviour set, and re-test depth. Regular review and analysis available on subscription pricing model.

Timelines

- Planning and access preparation: 3–7 working days.
- Execution and analysis: 5–15 working days, dependent on scope and environments.
- Report issue: 5–10 working days after testing completion.
- Optional re-test and closure statement: by agreement.

Team and roles

- Engagement Lead for governance and quality.
- Detection Engineer(s) for source review, parsing, and correlation design.
- Coordinator for logistics, evidence handling, and re-test scheduling.

Buyer responsibilities

- Nominate platform/SIEM owners and a single engagement lead.
- Provide access to logging consoles, sample hosts, and time sync configuration.
- Align change windows for parser and policy adoption.

JUMPSEC responsibilities

- Operate within agreed authority using non-destructive tests.
- Minimise data handling; redact evidence where practicable.
- Provide precise, auditable fixes with 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 denial-of-service or business-disruptive testing.
- Third-party/hosted components require written consent.
- Personnel with BPSS/SC available where required
- Accessible materials available (WCAG 2.1 AA)

Related services

- Detection Engineering and SOC Use Case Tuning
- EDR Efficacy Assessment
- 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