SERVICE DEFINITION
MICROSOFT FUNDED BRIEFINGS AND WORKSHOPS

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 — Data protection and insider-risk controls

JUMPSEC worked with a council seeking practical improvements in data classification and sharing safety. We secured funding for a Data Security workshop. During discovery, we identified overly permissive external sharing and limited labelling coverage.

In the hands-on session, JUMPSEC walked through Purview sensitivity labels, auto-labelling policies, insider-risk indicators, and DLP controls across Exchange, SharePoint, and Teams, using masked sample data. We then rolled out labels to priority services, set DLP policies to be monitored then enforced, and introduced periodic guest-access attestation. As outcomes, we measured label adoption, reduced uncontrolled sharing, and provided clearer audit evidence for FOI and ICO engagement.

NHS trust — Threat protection alignment with IR playbooks

JUMPSEC worked with an NHS provider seeking clearer isolation thresholds and earlier detection of credential theft and exfiltration. We secured funding for a Threat Protection workshop. During discovery, we identified inconsistent Defender policies and muted alerts within shared VDI environments. In the hands-on workshop, JUMPSEC demonstrated ASR rules, device tags, device-based Conditional Access, and Sentinel analytics that joined process, archive, and egress events.

We enforced tamper protection, deployed targeted ASR rules, and rolled out correlation content with incident owner routing in the roadmap. Verification tracked that we generated earlier, context-rich alerts and achieved faster containment, with no impact on clinical throughput.

Education group — Sentinel and Defender adoption plan

JUMPSEC worked with a global education provider aiming to achieve faster visibility without placing a heavy burden on their small security team. We confirmed eligibility and secured funding for a Modern SecOps workshop. During discovery, we uncovered disjointed alerting and limited automation.

In the immersion, JUMPSEC demonstrated data connectors for M365 and key SaaS platforms, established baseline analytics, implemented UEBA, and introduced safe playbook automation for high-confidence alerts. We then sequenced connector onboarding, set up watchlists for high-risk identities, and rolled out automation in measured phases with approval gates. Follow-up checkpoints tracked improvements in alert precision, mean time to detection (MTTD), and investigation time during busy term periods.

Retail group — Board-ready plan for peak trading

JUMPSEC worked with a retailer that required a concise, costed plan ahead of the seasonal peak. We secured funding to deliver a blended Threat Protection and Modern SecOps session. In the immersion workshop, we demonstrated practical steps to reduce consent-then-rule abuse, hardened privileged elevation using PIM, and deployed targeted Sentinel analytics.

We aligned the adoption roadmap to trading milestones, defined acceptance metrics, and ran a verification drill following the content rollout. JUMPSEC presented leadership with a clear summary of spend, project milestones, and the risk reduction achieved before promotions went live.

Service Overview

JUMPSEC delivers Microsoft-funded workshops that accelerate understanding and safe adoption of Defender, Sentinel, Entra, and Purview. We tailor each engagement to your estate, priorities, and licensing. We combine discovery, targeted demos in your tenant, and hands-on immersion to turn platform capability into an actionable adoption plan with measurable outcomes. We manage Microsoft eligibility and funding mechanics so you can focus on decisions and next steps.

Objectives

- Confirm funding eligibility and align workshop scope to your goals.
- Evidence priority use cases in your tenant with safe, curated data.
- Produce a practical adoption plan with owners, milestones, and success measures.
- Reduce time to value for Microsoft security investments

Approach

We start by validating funding routes and the applicable workshop type: Threat Protection Immersion Briefing, Modern SecOps Envisioning Workshop, or Data Security Envisioning Workshop. We run a short discovery to capture business drivers, risk themes, and current deployment. We then configure a safe demonstration space in your tenant or a JUMPSEC sandbox linked to representative data. We facilitate an executive-level briefing, a technical deep-dive, and a guided hands-on session. We close with an adoption roadmap that sequences quick wins and lays out a verification plan for benefits realisation.

Method

- **Plan** — confirm workshop type(s), funding route, stakeholders, and desired outcomes; agree artefacts and access.
- **Discover** — capture current posture, licences, data locations, priority scenarios, and constraints.
- **Validate** — prepare safe demo datasets, permissions, and use-case scripts; confirm change windows.
- **Deliver** — run briefing, deep-dive, and hands-on modules; capture decisions and dependencies.
- **Debrief** — present the adoption roadmap, owners, milestones, and success measures; agree follow-up checkpoints.

Deliverables

- Executive briefing tailored to sector and objectives.
- Hands-on immersion pack with curated scenarios for Defender, Sentinel, Entra, or Purview, as applicable.

- Adoption roadmap with 30/60/90-day actions, owners, and acceptance criteria.
- Benefit realisation plan with KPIs (e.g. alert precision, MTTD/MTTR, sensitive-data coverage).
- Funding summary and next-steps memo (including eligible follow-on activities).

Outcomes and benefits

- Clear decisions on what to deploy, in what order, and why.
- Faster time-to-value from existing licences.
- Measurable uplift in detection, response, or data protection capability.
- Executive alignment around investment, ownership, and cadence.

Pricing model

Microsoft funded (where eligible), part-funded, or buyer-funded. Drivers and eligibility: number of workshop days, breadth of scenarios, tenant preparation effort, and follow-on support.

Timelines

- Eligibility check and planning: 3–5 working days.
- Discovery and preparation: 5–10 working days (scope dependent).
- Briefing delivery: 90 minutes
- Workshop delivery: 1–3 days per workshop stream (over extended timeframe)
- Adoption roadmap issued: 5–10 working days after testing completion

Team and roles

- Engagement Lead for governance and quality.
- Microsoft Security Specialist(s) prepare the tenant, run deep-dives, and facilitate hands-on modules.
- Senior Consultant to facilitate/deliver workshops with senior stakeholder.
- Coordinator for logistics, evidence handling, and re-test scheduling.

Buyer responsibilities

- Nominate an executive sponsor and technical owners.

JUMPSEC responsibilities

- Operate within agreed authority using non-destructive tests.

- Provide tenant access, sample data sources, and licence information.
- Approve any configuration required for safe demonstrations.
- Complete end-of-engagement Microsoft survey.
- 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

- Microsoft funding is subject to Microsoft approval and budget availability.
- Eligibility requires alignment with Microsoft's current workshop programmes and incentive rules.
- A Microsoft account team or Partner Centre nomination may be required.
- The customer must hold appropriate Microsoft licences or commit to an agreed adoption path.
- Funding typically applies once per customer per workshop stream within Microsoft's programme limits.
- If funding is declined or exhausted, JUMPSEC can deliver the same scope on a buyer-funded basis.
- Tenant access, permissions, and data required for safe demos must be granted in advance.

Related services

- MXDR on Microsoft stack (Managed Detection and Response)
- Detection Engineering and SOC Use Case Tuning
- Microsoft 365 / Entra ID / Azure AD Tenant Review

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com