SERVICE DEFINITION
THREAT MODELLING

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

Petrochemical operator (CNI) — OT/IT trust boundaries and vendor access

We mapped the enterprise IT, DMZ jump infrastructure, and OT zones hosting historians, HMIs, and safety instrumented systems. Our diagrams highlighted where vendor VPNs terminated close to the OT DMZ, where shared jump hosts were used, and where long-lived accounts were reused across turnarounds. JUMPSEC identified that engineering tools depended on legacy protocols within mixed subnets. We also traced backup paths that crossed shared file services with broad write permissions.

We introduced brokered, just-in-time vendor access, including device posture checks and session recording. JUMPSEC enforced segmentation by implementing one-way data diodes for historian feeds and isolating admin paths behind authenticated brokers. We tied OT maintenance to signed update packages and mTLS through change control. Our acceptance tests validated that we blocked lateral movement from IT into control zones and denied unsigned tooling. JUMPSEC developed detection ideas to monitor out-of-window access, protocol misuse, and configuration writes to controllers, thereby supporting IEC 62443 zone/conduit intent while maintaining safety and availability

Local authority — payments and benefits workflows

We focused on threats involving business-process manipulation and service-desk social engineering. JUMPSEC used STRIDE to identify tampering and elevation paths, while we leveraged ATT&CK initial-access and collection techniques to shape the detection strategy.

JUMPSEC codified server-side eligibility checks, implemented dual approval, and performed out-of-band verification with verified directories. We aligned the requirements and tests to ASVS, and presented audit-ready evidence for the outcomes.

Energy supplier (CNI) — cloud control plane and OT boundaries

We illustrated long-lived keys, broad roles, and staging-to-operational pathways through our diagrams. JUMPSEC used STRIDE and applied IEC 62443 zone/conduit intent to define boundary choices, while we leveraged ATT&CK techniques to shape our monitoring approach.

We introduced workload identity federation, implemented short-lived credentials and just-in-time admin, and enforced the use of signed artefacts. JUMPSEC monitored privileged actions occurring outside change windows, and we framed risks using ISO 27005 language for board reporting.

.

Service Overview

JUMPEC conducts a structured analysis of systems, processes, and data to identify plausible threats, attack paths, and control gaps before adversaries exploit them. The engagement maps assets, actors, trust boundaries, data flows, and business objectives, then applies threat patterns to prioritise risks. Outputs convert insights into backlog-ready security requirements, detection ideas, and verification tests that land cleanly in delivery.

Objectives

- Create a shared, accurate view of the system and its attack surface
- Identify credible threats and misuse cases with business impact
- Prioritise risks and define security requirements and acceptance criteria
- Seed detection use cases and test plans for future verification

Approach

Workshops bring together architects, product owners, engineers, security, and operations. The team documents context and critical journeys, then analyses threats using recognised patterns. Where helpful, small proofs demonstrate feasibility. The result is a clear set of actions that align to delivery cadence and governance.

JUMPSEC selects from the following industry standard frameworks to fit context and audience

- STRIDE for technical threat classes across apps/services.
- LINDDUN where privacy risks and UK GDPR concerns apply.
- PASTA to sequence from business objectives to misuse cases and controls.
- MITRE ATT&CK to map behaviours and seed detections/playbooks.
- NCSC Security Design Principles to anchor design choices for UK buyers.
- OWASP ASVS/SAMM to express control requirements and assurance levels.
- ISO 27005 terminology for likelihood/impact to align with governance.
- IEC 62443 for OT/ICS contexts (zones, conduits, supplier access).

Method

- **Plan** — confirm scope, participants, artefacts, objectives, and evidence handling
- **Model** — document architecture, data stores, trust boundaries, identities, suppliers, and critical journeys
- **Analyse** — apply STRIDE (and LINDDUN where relevant), use PASTA to link organisational goals to misuse cases, and reference ATT&CK behaviours for realism

- **Prioritise** — rate risks using ISO 27005 language; agree owners, due dates, and acceptance criteria
- **Specify** — produce OWASP ASVS/SAMM-aligned security requirements and non-functional controls mapped to components and journeys
- **Seed assurance** — define verification tests, detection ideas, and playbook hooks
- **Debrief** — walk through results, resolve assumptions, and agree verification path

Deliverables

- Executive briefing (slide deck + debrief) highlighting material risks, hot paths, and priority actions
- Threat Model Package including architecture and data-flow views, threat catalogue, misuse/abuse cases, and risk prioritisations with rationales
- Standards and alignment embedded in reporting, referencing NCSC security design principles, OWASP Threat Modeling and ASVS control areas, ISO/IEC 27001 Annex A themes, and relevant cloud provider guidance

Outcomes and benefits

- Fewer late security surprises and cheaper fixes through early clarity
- Controls that address whole classes of risk, not isolated issues
- Clear ownership and measurable acceptance criteria for delivery teams
- Seeded detections and tests that sustain security over time

Pricing model

Fixed price per system or product journey set, or time-and-materials for complex estates. Price drivers include domain complexity, integration count, participant availability, and artefact depth

Timelines

- Planning and artefact collection: 3–5 working days
- Workshops and analysis: typically 1–10 working days, depending on scope
- Report issue in 5–10 working days after testing completion
- Optional verification and updates: by agreement

Team and roles

- Engagement Lead for governance, ethics, and quality
- Adversarial Consultant(s) facilitating workshops and analysis

- Security Architect / Engineer supporting requirement design and feasibility

Buyer responsibilities

- Nominate a product or service owner and technical leads
- Provide architecture artefacts, data classifications, and supplier lists
- Ensure participation from key stakeholders across engineering, ops, and security

JUMPSEC responsibilities

- Facilitate efficient workshops and keep outputs decision-ready
- Document assumptions, residual risk, and verification steps
- Handle materials securely and retain only for agreed periods

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

- Work is non-destructive and design-focused; live testing is out of scope
- Supplier participation may be required for integration clarity
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Attack Path Mapping
- Secure SDLC / DevSecOps / Pipeline Assessment
- Detection Engineering and SOC Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com