SERVICE DEFINITION
HARDWARE / EMBEDDED SYSTEMS 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

Medical device OEM — Secure boot and update

JUMPSEC conducted a teardown and firmware analysis and identified that the bootloader was unsigned and accepted arbitrary images through a local update routine. We discovered that environment variables had debug flags left enabled in production builds, and a recovery mode trusted USB media without signature checks. JUMPSEC also found that device keys originated from a shared seed used during manufacturing, and the update scripts failed to enforce rollback protection.

We introduced a hardware-backed root of trust, implemented signed boot stages, and provisioned per-device unique keys with protected processes. JUMPSEC required signed images, metadata integrity, and anti-rollback counters for the update path. We disabled debug flags in production builds, and ensured recovery only accepted signed media. JUMPSEC verified these controls on a pre-production spin and demonstrated that the device rejected tampered images and enforced rollback prevention.

Consumer appliance manufacturer — Peripheral trust and tamper resistance

We found that the device accepted firmware via removable media and trusted unverified peripherals over USB. Through side-channel observations, JUMPSEC identified debug messages transmitted over a secondary serial interface in production. We also noted that the boot configuration did not securely store keys.

To address these issues, JUMPSEC restricted peripheral trust by implementing signed accessory programmes, disabled production debug messaging, and migrated keys to secure elements. We updated the firmware to enforce signature checks for removable-media updates. In our follow-up tests, we confirmed that the device blocked peripheral-based code paths and verified only trusted updates.

Industrial controller (CNI) — Safety and maintenance pathways

We discovered that a PLC-adjacent controller exposed an engineering console with default credentials and included an undocumented telnet service used by field engineers. JUMPSEC found that updates relied on FTP transfers without integrity checks, while backups stored configuration and credential files on shared servers with broad write permissions.

To remediate these issues, we removed telnet, enforced unique credentials with vault-managed rotation, and JUMPSEC replaced FTP with signed update bundles delivered over authenticated channels. We moved backups to controlled repositories with immutable snapshots. JUMPSEC then verified that maintenance access was controlled, updates were trusted, and configuration artefacts were protected.

Service Overview

Independent, manual-first testing of hardware and embedded platforms to identify exploitable weaknesses across device boot, firmware integrity, debug and maintenance interfaces, local services, and trusted execution boundaries. The assessment spans physical attack surface, firmware and file systems, interconnects, and the device's interactions with companion apps, gateways, and cloud control planes. Activities prioritise safe, non-destructive validation with reproducible evidence and backlog-ready remediation.

Objectives

- Establish trust in boot and update chains with signed firmware and rollback protection
- Reduce attack surface on debug, maintenance, and peripheral interfaces
- Harden credential, key, and secret handling from manufacturing to field operation
- Link device-level findings to ecosystem risk in apps, gateways, and cloud backends

Approach

Work reflects safety constraints, service criticality, and regulatory context. Delivery combines teardown and interface mapping, firmware extraction and analysis, protocol inspection, and targeted fault or glitch testing where safe and agreed. Companion software and backends are sampled to validate end-to-end risk while avoiding service disruption.

Method

- **Plan** — objectives, variants, safety gates, teardown rights, escalation, evidence handling
- **Discover** — enumerate SoC, boot chain, firmware, file systems, keys, interfaces, peripherals, and local services
- **Validate** — confirm exploitability for boot, update, debug access, storage protections, and trust boundaries using agreed techniques
- **Analyse** — link issues to business and safety impact, root cause, and feasible remediation
- **Debrief** — prioritise fixes, owners, acceptance criteria, rollout sequence, and rollback points
- **Improve** — optional verification on new hardware spins, firmware builds, or staged rollouts

Deliverables

- Executive briefing describing material device and ecosystem risks, abuse paths, and priority actions
- Hardware/Embedded Security Report with evidence, reproduction steps, and exact fixes across boot/chain-of-trust, update integrity, debug/maintenance control, storage protections, interconnects, and local services; ecosystem linkages to apps, gateways, and cloud

- Issue register (CSV/XLSX) listing severity, owners, due dates, and acceptance criteria
- Prototype hardening guidance covering secure boot, key provisioning, debug lockdown, tamper detection, and update signing with rollback prevention
- Optional verification confirming remediation outcomes on revised hardware or firmware
- Standards and alignment embedded in reporting, referencing ETSI EN 303 645, NCSC connected device guidance, OWASP IoT and Firmware Testing Methodologies, CWE mappings, CVE/CVSS severity rationale, and relevant MITRE ATT&CK/ICS techniques used for rationale

Outcomes and benefits

- Trusted boot and update processes that resist tampering and downgrades
- Reduced device takeover and data exposure via locked-down debug and interfaces
- Safer key and credential lifecycle from factory to field
- Evidence suitable for regulators, insurers, and enterprise buyers

Pricing model

Fixed price per device family and ecosystem scope or time-and-materials aligned to SFIA. Price drivers include device variants and spins, interface breadth, firmware complexity, supplier coordination, and verification needs.

Timelines

- Planning and access: 3–7 working days
- Assessment and analysis in 1–3 weeks depending on device and ecosystem scope
- Report issue in 5–10 working days after testing completion
- Optional re-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 management, stakeholder alignment
- **Embedded Security Specialist(s)** responsible for hardware/firmware testing and evidence capture
- **Application/API Security Tester(s)** responsible for companion app and backend sampling
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Provide representative devices, accessories, documentation, test jigs or breakout boards, and firmware images
- Arrange third-party consents with OEMs, contract manufacturers, and platform suppliers

JUMPSEC responsibilities

- Operate within safety gates, change control, and documented abort criteria
- Use non-destructive techniques and minimise operational risk
- Handle evidence and IP securely with time-boxed retention and approved destruction/return

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 testing without explicit written approval
- RF, side-channel, and fault injection executed within legal and safety limits
- Third-party/OEM cooperation may gate specific checks
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- IoT / IIoT Device Security Review
- Cloud-Hosted Application Penetration Testing
- Secure SDLC / DevSecOps / Pipeline Assessment

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com