SERVICE DEFINITION
IOT / IIOT DEVICE SECURITY REVIEW

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

Smart metering supplier (CNI-adjacent) — OTA trust and device identity

JUMPSEC assessed a gateway and meter pair and discovered that unsigned firmware images were accepted over an authenticated but unpinned channel. We found that device identities bootstrapped from a shared seed and reused per-batch credentials. We identified that debug UART remained enabled on production units. Our team saw that backend APIs accepted weak client attestation and permitted device state changes from broad IP ranges.

We introduced signed firmware with hardware-backed verification, established per-device unique identities, and implemented short-lived bootstrap credentials. JUMPSEC disabled debug paths in production images, and we required backend APIs to use mutual TLS with attestation and per-identity allow-lists. Our verification of a staged OTA confirmed trusted updates, enforced device identity, and restricted control-plane access.

Healthcare device vendor — PHI exposure via mobile and cloud backends

JUMPSEC tested a home telemetry device and companion app and uncovered plaintext caches of patient identifiers, permissive API scopes for data retrieval, and predictable device IDs embedded in QR onboarding. We discovered that the firmware exposed an update endpoint that accepted unauthenticated requests in pairing mode.

We encrypted sensitive mobile stores, constrained API scopes, and randomised onboarding IDs with server-side validation. JUMPSEC gated firmware update endpoints behind authenticated pairing and time-bound windows. Our follow-up confirmed safer mobile handling, correct API authorisation, and closed unauthenticated update paths.

Local authority housing provider — BMS sensors and resident devices

JUMPSEC assessed a mixed estate of building sensors and resident devices and identified open MQTT brokers, default credentials on management consoles, and public dashboards with verbose information. We found that cloud storage for logs allowed directory listing and that time sync drifts across gateways complicated incident reconstruction.

We enforced broker authentication with certificate-based access, rotated credentials, hid dashboards behind authenticated ingress, and closed public listings with lifecycle rules. JUMPSEC standardised time sync across gateways. Our re-assessment demonstrated controlled messaging, protected management access, and auditable logs.

Service Overview

JUMPSEC conduct independent, manual-first assessment of connected devices and their ecosystems—firmware, mobile or desktop apps, local services, gateways, and cloud backends. The engagement validates exploitability across device hardening, authentication, crypto, update integrity, local and remote interfaces, and data handling. Testing emphasises safe techniques and staged validation to avoid service disruption, with clear, backlog-ready fixes tied to engineering workflows.

Objectives

- Identify exploitable weaknesses across device, gateway, and cloud control planes
- Harden identity, firmware integrity, and update trust to prevent takeover
- Reduce attack surface on local, RF, and remote interfaces and management APIs
- Provide precise remediation with acceptance criteria that fit product lifecycles

Approach

Assessment reflects device criticality, safety constraints, and regulatory context. Work combines teardown and firmware review, interface mapping, OTA pipeline analysis, and backend/API testing in controlled environments. Where live fleets exist, sampling and staging are used to avoid service impact. Stakeholders usually include Product, Engineering, Cloud/Platform, Mobile, and Supplier/OEM contacts.

Method

- **Plan** — confirm objectives, device variants, interfaces, environments, teardown rights, escalation, evidence handling
- **Discover** — enumerate hardware interfaces, services, protocols, credentials, keys, update paths, and backend APIs
- **Validate** — confirm exploitability for authn/authz, crypto, storage, debug/console access, OTA integrity, and backend controls using safe checks
- **Analyse** — link findings to business impact, safety/availability risks, and root causes across device and platform
- **Debrief** — prioritise fixes, owners, acceptance criteria, rollout sequence, and rollback points
- **Improve** — optional verification on new builds or staged OTA to confirm uplift

Deliverables

- Executive briefing (slide deck + debrief) highlighting material risk, likely abuse paths, and priority actions

- IoT/IIoT Security Report detailing device, gateway, and backend findings with evidence, reproduction steps, and exact fixes; coverage notes for secure boot/chain-of-trust, key management, storage protections, interface exposure, OTA/update integrity, and API controls
- Issue register (CSV/XLSX) listing severity, owners, due dates, and acceptance criteria
- Optional PR/rebuild review confirming remediation outcomes
- Standards and alignment (embedded) referencing ETSI EN 303 645, NCSC connected device guidance, OWASP IoT/ASVS where applicable, CWE mappings, CVE/CVSS severity rationale, and ATT&CK for ICS/Enterprise technique names used for rationale

Outcomes and benefits

- Lower likelihood of device takeover, data exposure, and unsafe remote control
- Trusted updates and firmware provenance across the device lifecycle
- Reduced fleet attack surface and clearer ownership of security changes
- Assurance artefacts suitable for regulators, customers, and insurers

Pricing model

Fixed price per device family and backend scope, or time-and-materials aligned to SFIA. Price drivers include device variants, interface breadth (wired/wireless/RF), OTA and backend complexity, supplier coordination, and verification or re-test requirements

Timelines

- Planning and access: 3-7 working days
- Assessment and analysis: 1–3 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification sprint or staged OTA review: 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
- **IoT/Embedded Security Specialist(s)** - device/firmware testing and evidence capture
- **Application/API Security Tester(s) -** backend and app/API assessment

- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Provide representative devices, accessories, documentation, test builds, keys or staging identities, and backend access/exports
- Arrange third-party consents with OEMs, contract manufacturers, and platform suppliers

JUMPSEC responsibilities

- Operate within agreed rules of engagement, safety constraints, and change control
- Use non-destructive validation and minimise operational impact
- 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

- Non-destructive techniques; no live fleet disruption without explicit approval
- RF testing and regulated spectrum activities performed within legal allowances
- 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

- Hardware / Embedded Systems Penetration Testing
- 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