SERVICE DEFINITION
ROGUE CLIENT / ROGUE DEVICE 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 — Visitor SSID and contractor network segregation

JUMPSEC identified that the council used a shared PSK for visitor Wi-Fi and permitted contractor devices onto a lightly filtered VLAN. During our tests, we discovered PSK reuse across buildings, bypassed captive portals by manipulating DNS, and reached exposed printers and admin interfaces through lateral movement. We also found that logs did not attribute devices or record session expiry.

We introduced per-site PSK rotation with short validity periods, moved contractors to certificate-based 802.1X with posture checks, and tightened inter-VLAN ACLs. JUMPSEC added device fingerprinting to portals and enforced logout timers. When we re-tested, we demonstrated constrained access, clear device attribution, and generated alerts for unusual east-west traffic.

Healthcare campus — Rogue wired client in clinical annex

A hospital engaged JUMPSEC to ensure that an unused network port within a clinical annex could not be exploited for unauthorised access. Our team attempted to join the network using forged device identities and performed passive reconnaissance. Through our assessment, we discovered that overly permissive LLDP configurations were present and a fallback VLAN was accessible, providing entry to middleware supporting imaging systems. Additionally, we observed that network access control (NAC) logs were not being forwarded to the SIEM, resulting in a lack of real-time incident creation.

To address these issues, JUMPSEC advised the adoption of robust switchport templates requiring authentication, the restriction of LLDP on non-administrative ports, and the integration of NAC logs into the SIEM with device risk tagging enabled. We also developed an isolation playbook detailing the responsibilities of estates and IT personnel during out-of-hours incidents. Following the implementation of these measures, our subsequent testing showed that unauthorised connection attempts were successfully blocked, prompt alerts were issued, and the isolation protocols did not disrupt clinical operations.

National retailer — Rogue device in distribution centre

A retailer asked JUMPSEC to conduct testing across distribution centres with mixed vendors. We connected a controlled client via an unlabelled port on a mezzanine. JUMPSEC found that MAC caching and broad MAB exceptions gave short-lived network access, which allowed us to reach warehouse management systems. During wireless tests, we discovered long-lived PSKs across sites.

We removed broad MAB, enforced certificate-based access, and rotated PSKs with site scoping. JUMPSEC updated warehouse SSIDs to include device categories and rate-limit profiles for unknown clients. When we re-tested, we confirmed that spoof attempts were denied access, the controller generated early alerts, and handheld workflows remained stable.

Service Overview

JUMPSEC tests whether an unauthorised device can connect, obtain network access, and operate undetected on your estate. We simulate hostile or misconfigured clients on wired and wireless segments to validate NAC enforcement, certificate posture, 802.1X/EAP settings, guest and contractor segregation, switchport and DHCP controls, wireless PSK rotation, captive portals, and monitoring/alerting. We design all activity to be non-disruptive and evidence-led, focusing on the controls that actually stop or expose rogue devices in production.

Objectives

- Prove NAC and wireless controls prevent unauthorised device access.
- Validate segmentation, VLAN assignment, and access lists restrict lateral movement.
- Confirm monitoring, alerting, and incident routes surface rogue activity quickly.
- Deliver precise hardening steps with verification artefacts and owners.

Approach

We plan safe windows, high-risk locations, and approval paths. We introduce controlled rogue devices to target areas (e.g., meeting rooms, technical corridors, IDF/MDF spaces) and exercise join, authentication, and pivot attempts under agreed limits. We collect packet, switch, controller, and NAC evidence to show what the device could access and how the environment responded. We prioritise changes that remove whole classes of bypass and provide rollback notes for adoption through change control.

Method

- **Plan** — confirm sites, segments, SSIDs, switch stacks, authority, and evidence handling; agree safety gates.
- **Discover** — review NAC/wireless configuration, certificates, switchport templates, DHCP, guest portals, and monitoring.
- **Validate** — attempt wired/wireless joins, spoof identities, test fallback methods, and try VLAN pivots within strict limits.
- **Analyse** — map observations to business risk; define exact config changes, owners, and acceptance criteria.
- **Debrief** — present actions, sequencing, and verification tests; agree optional re-test.

Deliverables

- Executive briefing describing material exposures, likely attack paths, and expected reduction after change.

- Rogue Device Assessment Report with evidence (switch/controller logs, captures, screenshots), precise fixes (port-security/NAC/wireless settings), rollback notes, and acceptance criteria.
- Network Control Pack: switchport templates, NAC policy adjustments, 802.1X/EAP guidance, MAC-bypass restrictions, guest/contractor patterns, and PSK rotation approach.
- Optional Detection & Response memo: recommended alerts, dashboards, and playbook inserts for rogue-device sightings.
- Embedded alignment in materials: NCSC network security principles, vendor hardening baselines for NAC/WLC/switching, and ISO/IEC 27001 Annex A links where relevant.

Outcomes and benefits

- Fewer viable paths for covert access and lateral movement.
- Faster detection and clearer isolation actions for facilities, IT, and SOC teams.
- Repeatable port and SSID templates that reduce configuration drift.
- Audit-ready evidence supporting assurance and insurer expectations.

Pricing model

Fixed price per site bundle and segment set, or Time and Materials for complex estates. Pricing Drivers: site count, wired/wireless scope, vendor diversity, and re-test depth.

Timelines

- Planning and discovery: 3–5 working days.
- Drafting and validation: typically 3–7 working day per site .
- Report issue: 5–10 working days after testing completion.
- Optional re-test by agreement.

Team and roles

- Engagement Lead for governance and quality.
- Network Security Tester(s) for NAC/Wi-Fi testing and switching analysis.
- Coordinator for logistics, permits, and artefact handling.

Buyer responsibilities

- Nominate a site lead and network owners; confirm site access and safety rules.
- Provide network diagrams, NAC/WLC access (read-only), and change windows.
- Arrange third-party approvals for managed networks where needed.

JUMPSEC responsibilities

- Operate within written authority and safety gates; avoid service disruption.
- Minimise data handling; capture only necessary evidence.
- Provide precise, auditable guidance 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, RF jamming, or destructive activity.
- Live production testing only under explicit agreement and controls.
- Third-party managed networks require written consent.
- BPSS/SC-cleared personnel available where required.
- Accessible materials (WCAG 2.1 AA) available on request

Related services

- Network Architecture / Asset Discovery
- Firewall / Segmentation Review
- Compromise Assessment / Threat Hunting Sweep

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com