SERVICE DEFINITION DOCUMENT
OT-ICS-SCADA SECURITY 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

Food manufacturer — Flat segments between corporate IT and packaging lines

We mapped routed pathways from corporate subnets into OT-adjacent services, including backup, printing, and engineering tools. JUMPSEC identified that legacy SMB and RDP were accessible from broad address ranges. Our team found that workstations used for line changeovers ran mixed antivirus and allowed unsigned macros, which created lateral movement routes into OT support systems.

We enforced a hub-and-spoke model with explicit allow rules to broker required services, removed legacy protocols, and isolated administration behind dedicated jump infrastructure. JUMPSEC adopted controlled application whitelisting and signed macro policies for engineering workstations. Our follow-up review demonstrated that we reduced traversal options from IT to OT and provided safer operational changeovers.

Local authority energy network — Contractor laptops and toolchain risk

During maintenance, contractors connected using unmanaged laptops that carried legacy tooling and shared credentials. We observed that VPN profiles permitted access to monitoring and configuration interfaces without conducting device posture checks. JUMPSEC also found that service accounts persisted across projects, providing broad access and lacking rotation once contracts ended.

We required device posture checks for remote access, enforced per-contractor identities with short-lived privileges, and removed shared credentials from the toolchain. JUMPSEC moved service accounts to scoped roles and rotated them at hand-off. Our subsequent validation evidenced that contractor endpoints were compliant, use of shared credentials was reduced, and ownership over privileged access routes became clearer.

Service Overview

JUMPSEC conduct manual-first testing of operational technology environments to identify exploitable weaknesses without disrupting safety or availability. The engagement validates exposure across remote access, jump infrastructure, engineering workstations, HMIs, historians, and supporting Windows/Linux services. Activities emphasise non-destructive techniques, strict change control, and observable improvement with reproducible evidence for engineering and security teams.

Objectives

- Identify externally and internally exploitable weaknesses that impact safety, availability, or integrity
- Validate segmentation and brokered pathways between IT and OT networks
- Harden remote access, identity, and workstation build standards used for operations
- Produce prioritised, testable fixes aligned to outage windows and OEM constraints

Approach

Work begins with risk scoping, asset criticality mapping, and method selection to respect safety constraints. Testing runs in approved windows using read-only discovery, controlled validation on cloned or representative systems, and careful sampling on production pathways when required. Stakeholders include Engineering, OT operations, Network, Security, and relevant OEMs and integrators.

Method

- **Plan** — goals, critical assets, safety gates, abort criteria, OEM coordination, evidence handling
- **Discover** — enumerate assets, services, trust boundaries, remote access routes, and jump paths
- **Validate** — confirm exploitability for identity, segmentation, protocol exposure, and build weaknesses using non-destructive checks
- **Analyse** — map findings to consequence (safety, quality, availability), root cause, and feasible remediation
- **Debrief** — present fixes with owners, outage sequencing, rollback points, and verification tests
- **Improve** — optional verification during maintenance to confirm outcomes

Deliverables

- Executive briefing (slide deck and debrief) highlighting material risk to safety, availability, and quality, and the highest-value actions
- OT Security Assessment Report covering remote access and brokered pathways, segmentation and zone-to-zone flows, workstation and server hardening, protocol and service exposure (including

legacy stacks), logging and time sync relevant to incident response, and OEM or integrator dependency notes

- Exposure register in CSV or XLSX listing issues, severity, owners, due dates, and acceptance criteria
- Optional re-testing confirming remediation outcomes
- Standards and alignment embedded in reporting, referencing IEC 62443 concepts, NCSC OT guidance, CIS controls adapted for OT support systems, and MITRE ATT&CK for ICS techniques used as rationale where applicable

Outcomes and benefits

- Reduced likelihood of unsafe or disruptive changes to control environments
- Smaller blast radius through enforced segmentation and controlled admin pathways
- Hardened engineering workstations, HMIs, and supporting services with clearer ownership
- Evidence suitable for regulators, insurers, and board-level assurance

Pricing model

Fixed price per site or zone set, or time-and-materials aligned to SFIA. Price drivers include site count, OEM/integrator coordination, allowable test depth, and verification during maintenance windows

Timelines

- Planning and coordination in 1–2 weeks, dependent on OEM and change windows
- Execution scheduled around maintenance and access constraints
- Report issue in 5–10 working days after testing completion
- Optional re-test 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 responsible for scope, governance, and quality
- **OT Security Tester(s) and ICS Specialist(s)** responsible for testing and evidence capture
- **Coordinator** managing logistics, supplier comms, and action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead from Operations or Engineering
- Provide network diagrams, OEM contacts, maintenance calendars, and remote access details
- Arrange third-party approvals where OEMs or integrators control systems or gateways

JUMPSEC responsibilities

- Operate within safety gates, change control, and documented abort criteria
- Use non-destructive validation and minimise operational risk
- Handle evidence 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

- Non-destructive testing only and no denial-of-service
- Live control loops and safety systems remain out of destructive scope
- Third-party and OEM involvement requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Network Architecture / Asset Discovery
- Firewall / Segmentation Review
- Rogue Client / Rogue Device Assessment

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com