SERVICE DEFINITION
MANAGED VULNERABILITY SCANNING

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 — Internet footprint growth after supplier changes

JUMPSEC actively monitored domains and certificates, quickly identifying new subdomains and endpoints that suppliers introduced during a website refresh. We scanned and discovered that some staging origins were left accessible with outdated TLS stacks and default admin paths. Additionally, JUMPSEC found several historic records that still resolved to retired SaaS tenants.

In response, we assigned ownership of services to the relevant service managers, proactively retired stale DNS entries, and brokered admin utilities behind authenticated ingress. JUMPSEC also aligned TLS configurations to standard profiles. We then conducted verification scans, which confirmed that we had closed admin surfaces and established a consistent certificate posture. Our trend reporting demonstrated that, as a result, the client's internet footprint became smaller and safer, with clear ownership of all new assets.

Energy distribution operator (CNI) — Emergent threat response

When a new CVE affected an externally exposed component and appeared on the CISA KEV list, JUMPSEC swiftly conducted targeted differential scans to pinpoint impacted versions across a subset of sites. We implemented rapid mitigations during maintenance windows, applying compensating controls at the edge while we scheduled patches.

JUMPSEC documented the risk, interim controls, and verification steps in our advisories. We evidenced closure through verification scans and updated build standards and monitoring in an after-action note. Our programme metrics demonstrated that we shortened the time to mitigate KEV-listed issues.

National charity — Cloud misconfigurations and key exposure

JUMPSEC scanned the cloud environment and surfaced public object storage with directory listing enabled and long-lived access keys present in build logs. We also found that API gateways permitted wildcard origins.

We remediated these issues by closing public listings, rotating keys into a managed vault with short-lived access, and tightening CORS. JUMPSEC validated closure through re-scans and tracked sustained compliance via cadence reporting. We provided evidence to support audit needs ahead of a major campaign.

Service Overview

JUMPSEC conduct continuous discovery and vulnerability management across external and internal assets. The service maintains an accurate asset inventory, runs scheduled and event-driven scans, validates exploitability for priority findings, and drives remediation with owners, SLAs, and verification. Coverage spans on-premises, cloud, containers, and remote endpoints where feasible. Delivery emphasises clear risk reduction, not scan volume.

Objectives

- Maintain a live, owner-attributed asset inventory
- Identify and validate exploitable vulnerabilities and misconfigurations
- Prioritise fixes using business context, exploitability, and exposure
- Provide measurable risk reduction with verification of remediation

Approach

Operations combine automated discovery and scanning with analyst triage and targeted validation. External assets are enumerated continuously; internal scans run to agreed cadences and windows. Severity is contextualised with exploit data, asset criticality, exposure, and compensating controls. Remediation is coordinated through ticketing integrations and tracked to closure.

Method

- **Plan** — confirm scope, inventories, risk model, cadences, maintenance windows, SLAs, and evidence handling
- **Discover** — enumerate assets, owners, technologies, and service exposure across environments
- **Scan** — run authenticated and unauthenticated scans on agreed schedules; trigger ad-hoc scans for emergent threats
- **Validate** — confirm exploitability for high-risk items; reduce false positives; identify compensating controls
- **Prioritise** — translate findings into actions with owners, due dates, and acceptance criteria
- **Verify** — re-scan and evidence closure; adjust baselines to prevent recurrence
- **Debrief** — cadence reviews with trend metrics, blockers, and targeted improvements

Deliverables

- Executive briefing (slide deck + debrief) showing risk trends, material exposures, and priority actions

- Continuous Asset & Exposure Register (CSV/XLSX) with owners, criticality, technology, and exposure attributes
- Monthly or quarterly Vulnerability Management Report with validated findings, exploitability rationale, business context, fixes, and verification notes
- Ticketing integration and workflow pack with issue templates, SLAs, and acceptance criteria
- Emergent Threat Advisories for high-risk CVEs with curated actions and verification tests
- Re-scan and remediation support for governance checkpoints
- Standards and alignment (embedded) referencing NCSC vulnerability management guidance, CIS Controls (Inventory, Vulnerability Management, Secure Configuration), ISO/IEC 27001 Annex A themes, and CVSS/CISA KEV context for prioritisation

Outcomes and benefits

- Smaller exploitable footprint across internet-facing and internal services
- Clear ownership and predictable remediation workflows that land in BAU
- Evidence of risk reduction for boards, regulators, and insurers
- Faster response to emergent threats with targeted verification

Pricing model

Subscription per asset band and scan scope, or time-and-materials for bespoke estates. Price drivers include asset count and diversity, authentication depth, integration complexity, reporting cadence, and validation effort.

Timelines

- Onboarding and discovery baseline in 1–2 weeks
- Cadenced scanning as agreed (e.g., weekly external, monthly internal, ad-hoc for emergent threats)
- Report issue for onboarding baseline in 5–10 working days after testing completion
- Ongoing cadence reports per schedule; verification letters on request

Team and roles

- **Engagement Lead** for governance, cadence, and quality
- **Vulnerability Analyst(s)** for triage, validation, and advisory creation
- **Coordinator** for logistics, evidence handling, and action tracking

Buyer responsibilities

- Nominate a service owner and technical contacts per platform
- Provide inventories, access for authenticated scanning, and change windows
- Integrate ticketing and endorse SLAs and acceptance criteria

JUMPSEC responsibilities

- Operate within agreed windows and change control
- Minimise impact on production and maintain confidentiality of outputs
- Handle data 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 scanning; no denial-of-service or stress testing
- Third-party and hosted services require written consent
- Authenticated scans contingent on suitable accounts and safe controls
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Continuous Attack Surface Management (CASM)
- Detection Engineering and SOC Use Case Tuning
- Cloud Infrastructure Penetration Testing

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com