SERVICE DEFINITION
CONTAINER / KUBERNETES 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

Central government digital service — RBAC and admission control drift

During our review, we identified widespread use of cluster-admin privileges, uncovered long-lived tokens, and found permissive namespace roles that had been provisioned during urgent delivery phases. We observed that admission controls allowed privileged containers and hostPath mounts, while exceptions were created without clear expiry dates or defined ownership. Our assessment also revealed that build pipelines had pushed unsigned images from mixed base layers directly into production registries.

We remediated these issues by scoping RBAC to enforce least privilege, introducing short-lived workload identities, and enforcing Pod Security Standards with well-defined exception lifecycles. We implemented admission policies to block privileged settings and required all images to be signed before deployment. Our follow-up checks confirmed that privileges were appropriately restricted, unsafe workloads were rejected, and registry provenance was reliable.

Water utility (CNI) — supply chain and registry governance

During our assessment, we identified unsigned images sourced from public registries, observed that CI pipelines used permissive CVE thresholds, and discovered shared credentials for build agents. We found that orchestrator nodes operated with outdated kernels that lacked essential hardening, and the runtime permitted elevated capabilities for maintenance containers.

We addressed these issues by enabling image signing and verification, enforcing CVE gates with exception workflows, and introducing per-agent credentials with regular rotation. We hardened both the kernel and runtime to reduce container privileges. Our verification confirmed that pipelines were trusted, CVE exposure was lower, and reliance on elevated capabilities had been reduced.

Local authority — multi-tenant cluster with mixed workloads

During our discovery phase, we found nodes were shared between citizen-facing and internal applications. We identified broad node selectors and noted the absence of taints and tolerations. As a result of horizontal scaling, sensitive workloads ended up running alongside less trusted services. Our review also revealed that registry retention allowed outdated images to remain accessible, which led to accidental deployments.

We remediated these issues by segregating nodes using taints and tolerations and enforcing placement rules for sensitive workloads. We implemented policy-as-code to block the use of deprecated images and enforced retention policies. Our follow-up assessment confirmed that workload isolation was reliable and that misdeployments caused by stale artefacts had been reduced.

Service Overview

JUMPSEC's independent security assessments of container platforms and Kubernetes clusters identify misconfigurations, excessive privileges, unsafe defaults, and supply chain risks. Engagements review control plane, node and workload security, identity and access, network policy, image provenance, and admission controls. Outputs provide reproducible evidence and a prioritised remediation plan suitable for platform and application teams.

Objectives

- Reduce privilege across clusters, namespaces, service accounts, and CI integrations
- Strengthen isolation with network policies, Pod Security Standards, and runtime guardrails
- Improve image trust: signing, provenance, vulnerability posture, and secrets handling
- Embed governance with admission controls, policy as code, and change checkpoints

Approach

Assessment reflects platform maturity, regulatory needs, and provider specifics (managed or self-hosted). Activities run in agreed windows using read-only access, controlled tests in non-production, and targeted validation that avoids service disruption. Stakeholders usually include Platform/SRE, Security, Application, and DevOps teams.

Method

- **Plan** — objectives, target clusters/namespaces, artefacts, windows, escalation, evidence handling
- **Discover** — enumerate RBAC, service accounts, admission controls, network policy, images, registries, secrets, and workload settings
- **Validate** — confirm risk via safe checks: privilege reach, isolation gaps, secret exposure, and admission bypasses
- **Supply chain review** — CI/CD integration, image build/signing, dependency controls, and registry governance
- **Debrief** — classify severity, document precise fixes, and sequence changes with rollback points
- **Improve** — optional verification to confirm remediation outcomes

Deliverables

- Executive briefing (slide deck + debrief): platform risks, exposure themes, and priority actions
- Kubernetes & Container Security Report:
    - Identity & RBAC: cluster/namespace roles, service accounts, tokens, workload identities

- Isolation & Policy: network policies, Pod Security Standards, seccomp/AppArmor, capabilities
- Admission & Governance: OPA/Gatekeeper/PSA rules, policy-as-code, exception lifecycle
- Workload & Node Hardening: hostPath/use of privileged, kernel/hardening baseline, logging
- Images & Registries: provenance/signing (Sigstore/Cosign), CVE posture, base image hygiene, secrets in layers
- CI/CD & Automation: build pipeline controls, secret management, artifact retention

- Exposure register (CSV/XLSX): issues, severity, owners, due dates, acceptance criteria
- Configuration packs (where applicable): exemplar policies for network, admission, and pod security
- Standards and alignment (embedded): CIS Kubernetes/Docker Benchmarks, NCSC/Kubernetes hardening references, NSA/CISA guidance, provider-native controls (AKS/EKS/GKE), and ATT&CK for Containers used for rationale

Outcomes and benefits

- Reduced blast radius through tighter RBAC and network policy
- Stronger workload baselines and fewer privileged containers
- Trusted images with clearer provenance and faster remediation of CVEs
- Predictable governance via admission controls and policy-as-code

Pricing model

Fixed price per cluster or time-and-materials aligned to SFIA. Price drivers for engagements include cluster count, namespace/workload volume, provider mix, artefact depth, and optional verification.

Timelines

- Planning and access: 3–5 working days
- Testing and reviews: 1–2 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification review based on findings and recommendations

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
- **Cloud Security Tester(s)** — technical assessment and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Provide cluster access (read-only), manifests, CI/CD context, registry details, and diagrams
- Confirm change windows and arrange third-party consents where required

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Use non-destructive validation and minimise operational impact
- Secure handling and time-boxed retention of data and 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

- Non-disruptive activities performed in approved windows
- Third-party involvement requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Secure SDLC / DevSecOps Assessment
- Cloud Infrastructure Penetration Testing
- Detection Engineering and Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com