PRICING DOCUMENT

G-Cloud 15 – Cloud Support Services

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

Rate Card

The rates for each of JUMPSEC's core capability areas is provided below, aligned with the Skills Framework for the Information Age (SFIA) Levels of Responsibility.

	Daily Rate			
Capability Area	**SFIA Grade 4**	**SFIA Grade 5**	**SFIA Grade 6**	**SFIA Grade 7**
Security Audit / GRC	£1,150	£1,300	£1,450	£1,650
Security Assurance	£1,150	£1,300	£1,450	£1,650
Security Hardening	£1,250	£1,400	£1,550	£1,750
Cyber Resilience	£1,250	£1,400	£1,550	£1,750
Attack Simulation	£1,250	£1,450	£1,600	£1,750
Incident Response	£1,400	£1,500	£1,750	£2,450

Managed Services

Pricing is dependent on scope for the following services:

- Managed Vulnerability Scanning / Continuous Vulnerability Management
- Continuous Reconnaissance (Continuous Attack Surface Recon and Exposure Management)
- Incident Response Retainers
- MXDR on Microsoft stack (Managed Detection and Response)
- Continuous Attack Surface Management (CASM)
- Multi capability service

Additional Fees

Managed Services may also incur the following fees, which are liable to change based on the specific nature of the client deployment.

- Licensing
- Hosting
- Data Storage
- Tooling Deployment
- Out-of-hours Support

Terms and Conditions

- **Working Day** – 8 hours exclusive of travel and lunch
- **Working Week** – Monday to Friday excluding national holidays
- **Normal Working Hours** – Weekdays 9:00am to 5:30pm

- **Out-of-hours** – Additional charges for out-of-hours support can be found in the Terms and Conditions
- **Travel & Subsistence** – Charged at cost in line with client policy
- **VAT** – All prices are quoted exclusive of VAT

Services by Capability Area

This list of services is not the limit of JUMPSEC's possible offering and alternative solutions may also exist for each Capability Area.

Capability Area	G-Cloud Service Mapping
Attack Simulation	Social Engineering Testing Physical Penetration Testing Threat-Led Penetration Testing Red Teaming / Covert Adversarial Simulation Purple Teaming / Collaborative Adversarial Simulation Ransomware Simulation / Ransomware Readiness Assessment Phishing and Vishing Simulation Attack Path Mapping Endpoint Detection and Response (EDR) Efficacy Assessment Ransomware Readiness Assessment / Ransomware Simulation
Cyber Resilience	Business Continuity Planning Response Playbook Development Cyber Incident Exercising (Tabletop and Live-Play) IR Readiness Review / Breach Readiness Review Executive and Board Cyber Briefing / Board Coaching Microsoft-funded Security Workshops (Threat Protection, Modern SecOps, Data Security) – Funding based upon Microsoft Qualification
Incident Response	Walk-in Incident Response (Emergency IR) Compromise Assessment / Threat Hunting Sweep DFIR: Containment, Forensics, Recovery Support
Security Assurance	External Network Penetration Testing Internal Network Penetration Testing Wireless Network Penetration Testing Firewall / Segmentation Review Network Architecture / Asset Discovery OT / ICS / SCADA Penetration Testing IoT / IIoT Device Security Review Active Directory / Domain Configuration Review Host / OS Build Review Web Application Penetration Testing

	API Penetration Testing Mobile Application Penetration Testing Thick Client / Desktop App Penetration Testing Cloud-Hosted Application Penetration Testing Web Application Firewall (WAF) Bypass Testing Hardware / Embedded Systems Penetration Testing Rogue Client / Rogue Device Assessment Source Code Review Secure SDLC / DevSecOps / Pipeline Assessment Cloud Infrastructure Penetration Testing Container / Kubernetes Security Assessment AI / LLM Penetration Testing IT Health Check (ITHC) (CHECK)
Attack Simulation	Cyber Attack Simulation Cyber Breach Simulation Threat Detection Efficacy Assessment GBEST Intelligence-led Simulated Attack
Security Audit / GRC	vCISO Framework Maturity Assessment Framework Advisory and Consultancy
Security Hardening	Microsoft 365 / Entra ID / Azure AD Tenant Review Threat Modelling Microsoft Security Configuration (Azure, Defender, Microsoft 365, Entra, Sentinel) Detection Engineering and SOC Use Case Tuning Log Validity Assessment

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com