Cyber Security
Defence Consultants

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

Cyber Security Defence Consultants Limited
St John's Innovation Centre Cowley Road
Cambridge CB4 0WS
T: 01223 421577
W: cybersecuritydefence.co.uk

AWS Cloud Security Architecture Review

Cyber Security Defence Consultants

Table of Contents

Service Definition Document

Check Point Harmony Email and Collaboration MSSP

1 OVERVIEW

Cyber Security Defence Consultants delivers comprehensive AWS cloud security architecture reviews for UK government departments and public sector organisations.

Our consultants assess AWS environments against the AWS Well-Architected Framework security pillar and NCSC cloud security principles, identifying misconfigurations, security gaps, and opportunities for improvement. We deliver practical, prioritised recommendations that balance security requirements with operational needs.

All consultants hold SC clearance and relevant professional certifications including AWS Security Specialty, CISSP, and CISM. Our team has direct experience securing AWS environments for central government departments.

2 SERVICES

2.1 Assessment Scope

Our AWS security architecture review covers the following domains:

2.1.1 Identity and Access Management

- IAM policies, roles, and trust relationships
- AWS Organizations and Service Control Policies
- Federation and SSO configurations
- Privileged access management and root account security

2.1.2 Network Security

- VPC architecture and segmentation
- Security groups and Network ACLs
- Internet and NAT gateway configurations
- VPC peering and Transit Gateway security

2.1.3 Data Protection

- Encryption at rest and in transit
- KMS key management and policies
- S3 bucket policies and access controls
- Data classification and handling

2.1.4 Logging and Monitoring

- CloudTrail configuration and coverage
- CloudWatch alarms and metrics
- GuardDuty and Security Hub findings
- Log retention and SIEM integration

3 Key Features

1. IAM policy and permissions analysis including roles and trust relationships
2. Network security review covering VPCs, security groups, and NACLs
3. Data protection assessment including encryption and key management
4. Logging and monitoring evaluation against security best practice
5. AWS Well-Architected Framework security pillar alignment
6. NCSC cloud security principles compliance assessment
7. Multi-account and AWS Organizations security review
8. Serverless and container security configuration analysis
9. Prioritised remediation roadmap with implementation guidance
10. Executive summary and technical findings report

4 Key Benefits

1. Identifies security misconfigurations before they become incidents
2. Provides clear prioritised remediation roadmap
3. Aligns AWS environment with government security requirements
4. Reduces attack surface through configuration improvements
5. Demonstrates security due diligence to stakeholders
6. Supports compliance with NCSC cloud security guidance
7. Transfers knowledge to internal teams during engagement
8. Validates existing security controls against best practice
9. Identifies cost optimisation opportunities in security tooling
10. Delivered by SC-cleared consultants with AWS experience

5 Pricing

Services are delivered on a time and materials basis using SFIA day rates. Rates range from £500 to £1,150 per day depending on consultant seniority (SFIA Levels 1-7). Fixed price engagements available for defined scope assessments.

Travel and subsistence within M25 included. Outside M25 charged at departmental rates. See separate Pricing Document and SFIA Rate Card for full details.

6 Support

Standard Support (included): Pre-engagement scoping, dedicated assessor contact throughout engagement, post-engagement support for 30 days including report clarification and remediation guidance.

Enhanced Support (additional cost): Extended support, annual reassessments, ongoing maturity tracking. Available at SFIA day rates.

Response Times: Initial response within 4 business hours during UK business hours (09:00-17:00 Monday to Friday). Urgent matters escalated immediately.

7 QUALIFICATIONS AND CERTIFICATIONS

- All assessors hold Security Clearance (SC)
- Staff screening to BS7858:2019
- Cyber Essentials Plus certified
- Professional certifications: CISSP, CISM, ISO 27001 Lead Auditor/Implementer
- Engagement process aligned to NCSC Certified Cyber Security Consultancy Standard