OFFICIAL

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

Zero Trust Architecture Advisory

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

1. Overview

Cyber Security Defence Consultants delivers Zero Trust architecture advisory services to help UK government and public sector organisations transition from traditional perimeter-based security to modern, identity-centric security models.

Zero Trust operates on the principle of "never trust, always verify"—assuming that threats exist both inside and outside the network. Our advisory services help organisations assess their current maturity, design target architectures, and develop practical roadmaps for Zero Trust adoption aligned to NCSC guidance.

All services are delivered by SC-cleared consultants with extensive experience implementing Zero Trust architectures across government and critical national infrastructure sectors.

2. NCSC Zero Trust Principles

Our services align to the NCSC Zero Trust architecture design principles:

1. **Know your architecture:** including users, devices, services, and data
2. **Know your user, service, and device identities:** create a single source of identity
3. **Assess user behaviour, service, and device health:** use signals to make access decisions
4. **Use policies to authorise requests:** build policies that use multiple signals
5. **Authenticate and authorise everywhere:** assume hostile network
6. **Focus your monitoring on users, devices, and services:** comprehensive logging
7. **Don't trust any network, including your own:** build for hostile environments
8. **Choose services designed for Zero Trust:** prefer modern, cloud-native services

3. Service Components

3.1 Zero Trust Maturity Assessment

We assess your current security architecture against Zero Trust principles:

- Current state architecture documentation review
- Stakeholder interviews across IT, security, and business teams
- Gap analysis against NCSC Zero Trust principles
- Maturity scoring across identity, device, network, application, and data pillars
- Quick wins identification for immediate security improvements

3.2 Target Architecture Design

We design target Zero Trust architectures tailored to your organisation:

- Identity and access management architecture
- Conditional Access policy framework design
- Network segmentation and micro-segmentation strategy
- Device trust and endpoint compliance model
- Data classification and protection architecture
- Integration with existing security tooling and investments

3.3 Roadmap Development

We develop practical, prioritised roadmaps for Zero Trust transformation:

- Phased implementation plan aligned to risk and budget
- Dependencies and sequencing across workstreams

- Resource and capability requirements
- Business case development with cost-benefit analysis
- Success metrics and KPIs for measuring progress

4. Typical Engagement

4.1 Zero Trust Assessment and Roadmap (10-15 days)

9. **Discovery (2-3 days):** Documentation review, stakeholder interviews, current state mapping
10. **Assessment (3-4 days):** Gap analysis, maturity scoring, quick wins identification
11. **Design (3-4 days):** Target architecture, policy framework, integration planning
12. **Roadmap (2-4 days):** Prioritised initiatives, phasing, business case, final reporting

5. Pricing

Services are priced based on SFIA day rates. See separate Pricing Document for full rate card.

- SFIA Level 4 (Senior Practitioner): £500/day
- SFIA Level 5 (Senior Consultant): £700/day
- SFIA Level 6 (Principal Consultant): £900/day
- SFIA Level 7 (Lead Consultant): £1,150/day
- Working day: 7.5 hours

Typical Zero Trust assessment and roadmap (10-15 days): £7,000 - £12,000 depending on scope and consultant level.

6. Support

Standard Support (included): Pre-engagement scoping, dedicated consultant contact during engagement, 30 days post-engagement support for report clarification and implementation guidance.

Enhanced Support (additional cost): Ongoing advisory, implementation support, vendor selection, proof of concept delivery at SFIA day rates.

Response Times: 4 business hours initial response during UK working hours. Documentation delivery within 10 working days of engagement completion.

7. Qualifications

- All consultants hold Security Clearance (SC)
- Staff screening to BS7858:2019
- Cyber Essentials Plus certified
- Zero Trust implementation experience across government sectors
- Professional certifications: CISSP, CCSP, Microsoft, AWS, Azure security certifications