NCSC CHECK IT Health Check and Penetration Testing

SERVICE DEFINITION FOR THE G-CLOUD 15 FRAMEWORK

Overview

We offer an extensive range of technical security assessments and penetration testing services to the public and private sector, including NCSC CHECK IT Health Checks (ITHCs), to identify technical vulnerabilities and weaknesses across multiple systems and technologies, to mitigate the threats of data assets compromise.

We use comprehensive and proven testing methodologies which have been reviewed by NCSC and CREST as part of the membership process.

Personnel

Our consultancy team is highly qualified and very experienced, holding certifications including Cyber Scheme Team Leader (Infrastructure), CREST Certified Application Tester, Cyber Scheme Team Leader (Applications), CREST Certified Red Team Specialist and CREST Certified Red Team Manager.

We also have a number of consultants that hold the Chartered Professional title for Security Testing (ChCSP) and others at Principal level and below.

Tests are undertaken by experienced CHECK accredited staff, with HMG SC Clearance.

All ITHCs are conducted in line with CHECK Assured guidance and are led by an experienced CHECK Team Leader in the relevant discipline.

We have considerable experience in working across the public sector and have delivered ITHCs and penetration tests to central government departments, local government, arm's length bodies and a wide-range of suppliers to government. Our consultants have conducted testing of many common public-sector networks.

IT Health Check and Penetration Test Engagement Model

All penetration tests and IT Health Checks are tailored to the unique requirements of the system risk, the project, the organisation and/or the Accreditor, and other related stakeholders. We will have an initial scoping call or meeting with you and your stakeholders to discuss the systems and applications under assessment, the business threat landscape, principal security concerns, and the technical assurance requirements. From this, we will produce a formal Statement of Work within a commercial proposal which will be subject to customer review and acceptance. Engagements are priced on a day rate basis – see the Pricing document for more information.

Cyberis Limited
Unit E, The Courtyard, Tewkesbury Business Park, Tewkesbury, Gloucestershire, GL20 8GD
T: +44 1684 353514 | E: info@cyberis.com | W: cyberis.com

The following testing disciplines may be included as part of any penetration test or as an ITHC where required and the scope aligns with the CHECK Assured requirements:

- Infrastructure Penetration Test — including cloud and on-premise networks, internal/external/perimeter networks, IaaS/PaaS cloud solutions, virtualisation and containerisation technologies, VPN and remote access, DMZs, segregation testing, servers/endpoints, networked devices, MFPs/MFDs, scenario-based testing, VoIP networks, thin client/VDI environments and kiosk environments.
- Application Penetration Test — web applications, websites, web services, APIs, e-commerce solutions and desktop applications.
- Cloud Security Configuration Review — we provide configuration auditing, technical assessment and advice that supports moves towards hosting functions, services and data at all major cloud platforms – including AWS, Azure and Google Cloud Platform.
- Wireless Penetration Test — design and configuration reviews, review of authentication and access control mechanisms, penetration testing, segregation testing and rogue access point detection.
- Mobile App Penetration Test — mobile apps and associated web services.
- Build / Configuration Assessments and Reviews — servers, endpoints, applications, mobile devices (laptops, smartphones and tablets) and network devices (switches, routers etc). Build / configuration assessments and reviews may be based on government standards, industry standards, internal standards or specific system requirements.
- Security Control Assessments and Configuration Reviews — firewalls, intrusion detection systems, web-application firewalls, and cloud hosting solutions such as AWS, Azure and Google Cloud Platform.
- Active Directory Security Review – security review including RBAC reviews, Entra ID for hybrid environments, conditional access controls and alignment with industry and vendor security recommendations (such as CIS Benchmarks, NCSC Security Principles and Microsoft guidance).
- Scenario-based penetration testing – such as stolen endpoint assessments, data loss prevention controls reviews, third-party access / BYOD security assessments.
- Social Engineering — phishing, spear-phishing and direct contact (in person and/or by phone).
- Adversary Simulation and Red Teaming — realistic attack simulations, threat intelligence-led testing, multi-layer attacks, red teaming and purple team exercises.
- AI systems – implementation reviews of AI models and LLM in business environments, including active testing and knowledge transfer to internal teams where appropriate.

The results of a penetration test or ITHC can be fed into your organisation's risk management process and can help to shape your organisation's information security strategy. Our consultants have many

years of experience working with industry and government, and will help you contextualise the risks identified, offering constructive and pragmatic remediation advice.

We recommend that a debrief conference call is arranged following report delivery, to discuss the technical vulnerabilities, business risks and best course of remediation.

Service Management

We operate a service management process that is integrated with our ISO 9001 Quality Management System.

All projects are assigned a lead consultant and a project manager throughout delivery of the testing. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 15 submission, this procedure has never been used.

Service Constraints and Levels

We do not have service constraints and levels, other than those specifically tailored and agreed in each 'Statement of Work' within a proposal.

Financial Recompense

We do not have a formal recompense model; as part of our ISO 9001 certification and commitment to customer service, we monitor the quality and delivery of all testing services very carefully.

Training

Training is offered in several of the testing service disciplines we offer; we are happy to discuss training options with our customers.

During a penetration test or ITHC with Cyberis, we are happy to provide knowledge transfer to individuals, by shadowing our test specialists; we are happy to discuss the approach and format with our customers.

Ordering and Invoicing Process

Our normal process is to produce a 'Statement of Work' within a commercial proposal and once acceptance is given (through a signed order form or purchase order) we will commence the scheduling process.

Fixed price projects are invoiced on acceptance of the deliverables of each work task. Projects undertaken on a time and materials basis are invoiced monthly in arrears. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

Refer to the separate 'Terms and Conditions' document.

Data Restoration / Service Migration

Data restoration and service migration is not included in our price.

Customer Responsibilities

All customer responsibilities will be defined in the 'Statement of Work' for each engagement/project.

Technical Requirements

All technical requirements and service dependencies are discussed with the client during scoping, as in most cases each project has different requirements. Technical requirements and testing pre-requisites will be documented in the 'Statement of Work' within the proposal.