Vulnerability Assessment

SERVICE DEFINITION FOR THE G-CLOUD 15 FRAMEWORK

Overview

Cyberis offers an extensive range of technical security assessments and penetration testing services to the public and private sector, including vulnerability assessments combining automated security assessments with analysis, consultancy and remediation advice from our skilled technical staff.

Vulnerability assessment is an integral part of any comprehensive information security strategy. When used in conjunction with complementary strategies, such as in-depth penetration testing for your infrastructure and applications, regular vulnerability assessments can provide you with an on-going assurance baseline for your systems.

Personnel

Our consultancy team is highly qualified and very experienced, holding certifications including Cyber Scheme Team Leader (Infrastructure), CREST Certified Application Tester and Cyber Scheme Team Leader (Applications). This includes individuals holding Chartered Cyber Security Professional (ChCSP) status, as well as a number at Principal level and below.

Tests are undertaken by experienced staff, with HMG SC Clearance and CHECK scheme accreditation.

We have considerable experience in working across the public sector and have delivered ITHCs and vulnerability assessments 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.

Vulnerability Assessment Engagement Model

All vulnerability assessments 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 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.

Our vulnerability assessments are carried out in the follow phases:

- Target Discovery: In the first stage of the assessment, we will probe the infrastructure in scope to identify systems present and to map the layout of the environment. Having identified target

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

hosts, we will perform scans to identify services available on the systems. Where possible, we will identify the versions of applications in use on the target systems and assess the function of each host.

- Vulnerability Identification and Verification: We will perform a full vulnerability assessment against services accessible on the remote hosts, using automated scanning tools. Scans at this stage will also include automated application security assessments conducted against any web-based applications identified during the target discovery phase. Exploitation of identified vulnerabilities will not be attempted during a vulnerability assessment.
- Scan Analysis: A review of the results will be conducted by skilled technical staff, who will remove false positives, and assess the risk posed by each issue in the context of the business environment.

The results of a vulnerability assessment can be fed into your organisation's threat and vulnerability programme, and wider risk management processes.

Our consultants have many years of experience working with industry and government, and can also help you contextualise the vulnerabilities identified, prioritise remediation, and offer constructive and pragmatic remediation advice.

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.

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.