Continuous Vulnerability Assessment

SERVICE DEFINITION FOR THE G-CLOUD 14 FRAMEWORK

Overview

Cyberis' continuous vulnerability assessment managed service is compatible with your external perimeter, website and application estate, cloud platforms, and internal systems. Your systems and networks will be assessed on a regular basis – such as daily, weekly or monthly, or on demand. This ensures a continuous baseline of security assurance between comprehensive penetration tests, and provides warning of any new vulnerabilities and changing exposure.

Our vulnerability scanning provides a systematic assessment of security at regular intervals, helping you minimise the window of opportunity for adversaries and move to a proactive security management posture.

In addition to real-time access to your vulnerability information, we provide expert triage and review of your exposure on a regular basis – highlighting issues which need prioritised attention and identifying patterns which should be addressed.

The National Cyber Security Centre (NCSC) recommends that organisations perform monthly vulnerability assessments of their entire estate. Our managed service simplifies that process, giving you expert insights as often as you need them.

Approach

We provide a managed continuous vulnerability assessment service, backed by the industry-leading vulnerability assessment products, Tenable Vulnerability Management (VM) and Tenable Web Application Scanning (WAS).

Tenable VM and WAS are cloud-based Vulnerability Management tools that enable automated scanning of the external internet perimeter, internal and external web applications and APIs, internal systems, and cloud platforms. Tenable gathers vulnerability information via agents installed on your internal systems, scanning servers deployed in your networks, connections to cloud platforms, and using public external scanners.

We'll work with you to make sure you have the right coverage of your estate and to set up a scanning schedule that suits your needs. We'll configure your users and make sure you have real-time access to your vulnerability information and access to historic trend analysis on demand.

We'll also show you how to run your own ad-hoc scans whenever you want an updated picture.

Using our extensive knowledge and expertise as penetration testers, we will fine-tune your scan policies to reduce inaccuracies and enhance the scan coverage. Our service can also be used to provide quarterly PCI ASV scanning, helping with your compliance programme.

As part of our managed service, we will regularly review the results of your scans, and provide expert analysis and triage. You'll receive an executive summary report including vulnerability identification and

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

remediation trends, together with prioritisation recommendations for review. Where you need additional support, we can customise our approach and deliverables to meet the needs of your teams.

Personnel

Our consultancy team is highly qualified and very experienced, holding certifications including:

- Tenable Certified Sales Associate and Engineer – Vulnerability Management
- Tenable Certified Sales Associate and Engineer – Tenable.ad
- Tenable Cloud Security Administrator
- CREST Certified Infrastructure Tester
- Cyber Scheme Team Leader (Infrastructure)
- CREST Certified Application Tester
- Cyber Scheme Team Leader (Applications)

Initial scan configuration, optimisation, triage and reviews are undertaken by experienced staff, with HMG SC Clearance.

Service Management

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

All subscriptions are assigned a lead consultant and a project manager throughout the service. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 14 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 and invoicing processes. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

If the customer wishes to cancel the service, fees that have already been paid or are owing will not be refunded or credited.

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 subscription. Generally, to ensure the initial configuration is successful and the vulnerability scans are effective, the customer's IT team or provider will need to deploy Nessus Agents on all Licensed Assets; deploy Tenable Core Nessus Scanner's in the relevant network subnets, and where required, establish connections to Cloud platforms. Provision of credentials for web applications may also be necessary.

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.