Infrastructure Penetration Testing

Arcturus

Part of the CYBERFORT group

// Service Overview

Using CREST and CHECK ITHC accredited methodologies we perform state-of-the-art automated vulnerability scanning, and carefully targeted manual testing to deliver an outstanding assessment encompassing internal and external estates.

An infrastructure penetration test is an authorised simulated attack on infrastructure, performed to identify vulnerabilities and strengths within the environment. We offer black box (unauthenticated) and white box (authenticated) testing of all internal and external facing infrastructure ensuring systems are evaluated and protected from external and internal threats. Comprehensive vulnerability reporting clearly communicates threats and risks in their business context. Actionable technical remediation advice and support are provided to help ensure best practice security controls are implemented.

Contents

Service Overview 2

Client Challenges 3

Client Benefits 3

Unique Service Points 4

Case Study 5

// Client Challenges

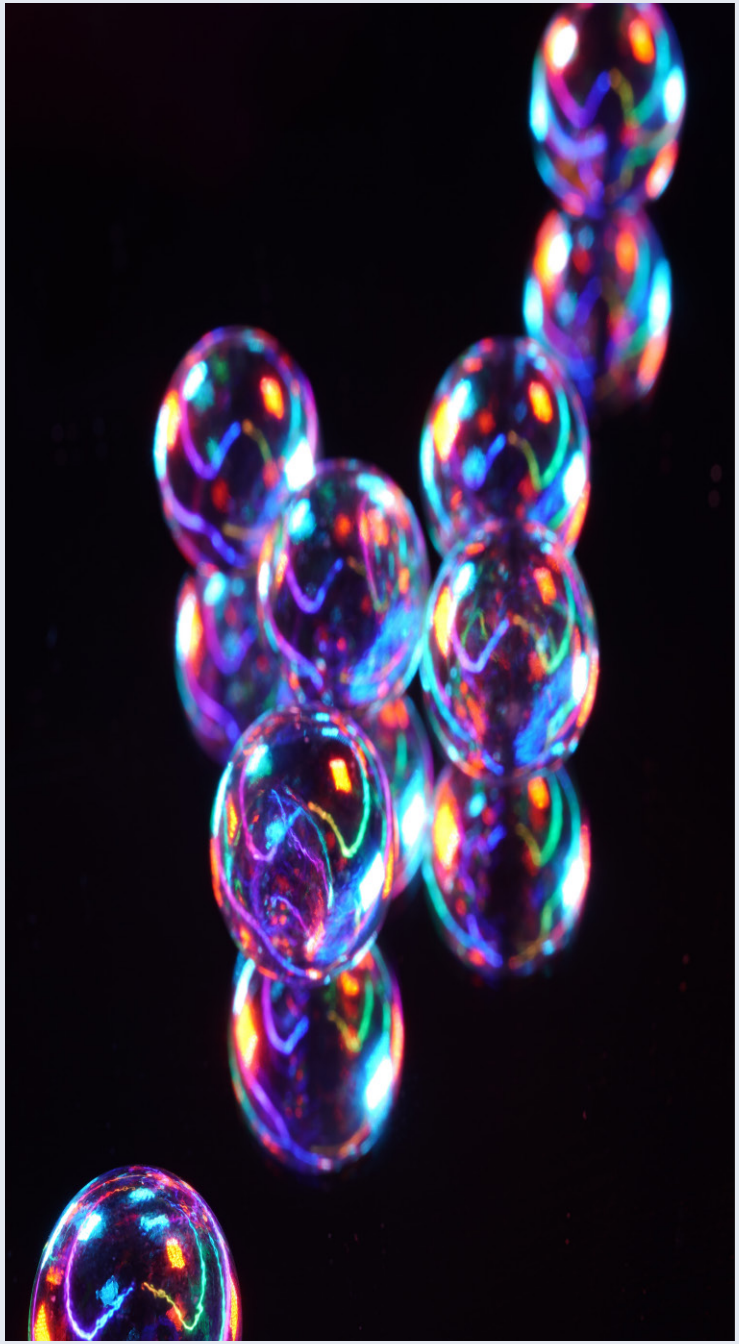
- Assessing and managing risk associated with system compromise, failure and exposure of sensitive data.
- Resource constraints, lack of appropriate internal skills and capabilities to enable organisations to adequately assess the security of complex business systems.
- Lack of knowledge or understanding of Security Models as they apply to organisations' eco-systems.
- Key stakeholders require support in assessing the risks, impacts and proximity of security vulnerabilities.
- Defining a security assurance framework and determining the depth and breadth of testing coverage.
- Ensuring tests are conducted against the latest threat intelligence and vulnerability databases.
- Understanding the drivers for testing, its purpose and correct scoping.
- Agreeing targets and frequency of automated and manual testing.
- Managing a suitable penetration testing programme in the enterprise.
- Implementing follow up actions and measuring benefit realisation Securing budget to satisfy CoCo and PSN compliance requirements.
- Justifying effective infrastructure penetration testing.

// Client Benefits

- A reduction in information and communications technology (ICT) costs over the long term.
- Translate security issues into business language and help focus organisational priorities.
- Communicate issues effectively to secure stakeholder and management endorsement.
- Greater levels of confidence in the security of IT application environments Visibility of risks and prioritised remediation advice.
- Experienced, dedicated technical staff deliver a full range of cost-effective testing.
- Eliminate the need to employ specialist (and expensive) staff, reduce training costs.

// Unique Service Points

- As a dedicated Cybersecurity Consultancy, our approach is designed to help organisations to detect, remediate and reduce the risk posed by malicious actors.
- We pride ourselves on having the ability to deliver a holistic approach to penetration testing, considering the organisation in its entirety, deconstructing complexities, delivering actionable steps and prioritising Cybersecurity across the whole organisation.
- Clients benefit from a truly independent assessment of infrastructure security controls.
- Comprehensive assistance with requirements definition and scoping.
- A clearly defined, systematic, structured approach to penetration testing.
- Clear reporting of threats and risks in their business context, communicating impact analysis and assisting with required remediation.
- Integrated project management office (PMO) and service management support provide capabilities to achieve where other service providers fail.
- Supporting clients to build in innovative security underpinned by Cybersecurity best practices.
- Bespoke methodology blending automated and manual testing techniques to deliver a comprehensive, cost effective solution.
- Access to highly-skilled Cybersecurity Practitioners and Consultants across multiple disciplines ensures effective programmes and complete governance.



// Case Study

Provider Of Shipping And Mailing Services To Central Government

Issues:

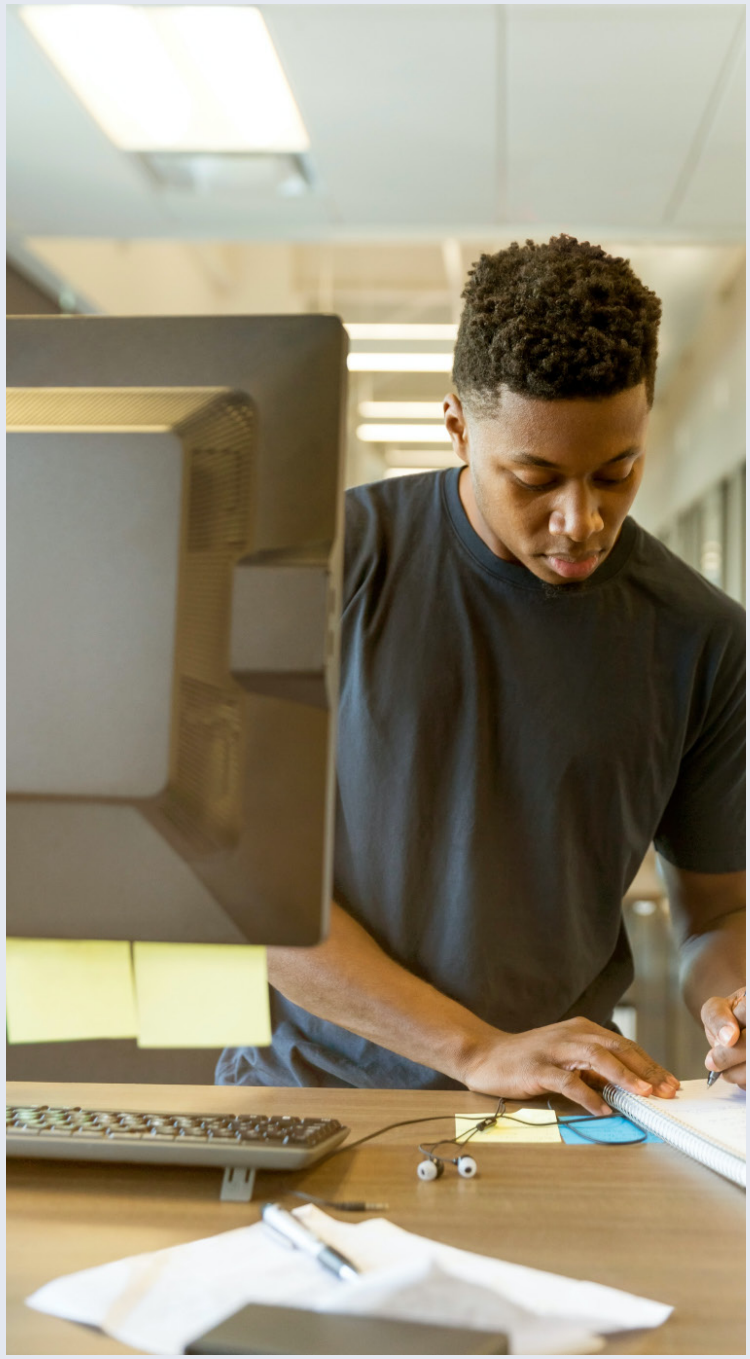
- Client requirement to validate security of internal infrastructure and data communication following migration to a Cloud Service provider and thin client implementation.

Solution:

- A comprehensive authenticated penetration assessment of all aspects of the internal infrastructure.
- Authenticated and unauthenticated assessment of network end points, clients and VPN infrastructure.
- Reporting of vulnerabilities and advice during implementation of strategic fixes. Follow up program of retesting.

Results, Benefits:

- Modular managed testing programme incorporated into busy BAU environment.
- Independent accreditation of assessed components following approved CREST and CHECK methodologies.



Infastructure Penetration Testing

01635 015600 *arcturussecurity.com* *info@arcturussecurity.com*

Arcturus

Part of the CYBERFORT group