armadillo
part of cyberlab

Cyber Security and Penetration Testing Services

CyberLab is a specialist cyber security company combining Chess Cyber Security, Armadillo Sec, and Cyberlab Consulting into one entity, providing a one-stop shop for all UK business security needs.

The Armadillo team have decades of experience conducting a broad range of services, including expert penetration testing, simulated attack testing, vulnerability scanning and a wide range of security testing services.

Penetration Testing

Common Penetration Testing and
IT Health Check Services.

Penetration Testing

Penetration testing is an authorised simulated attack on a computer system, network or web application to identify vulnerabilities that could be exploited.

IT Health Check

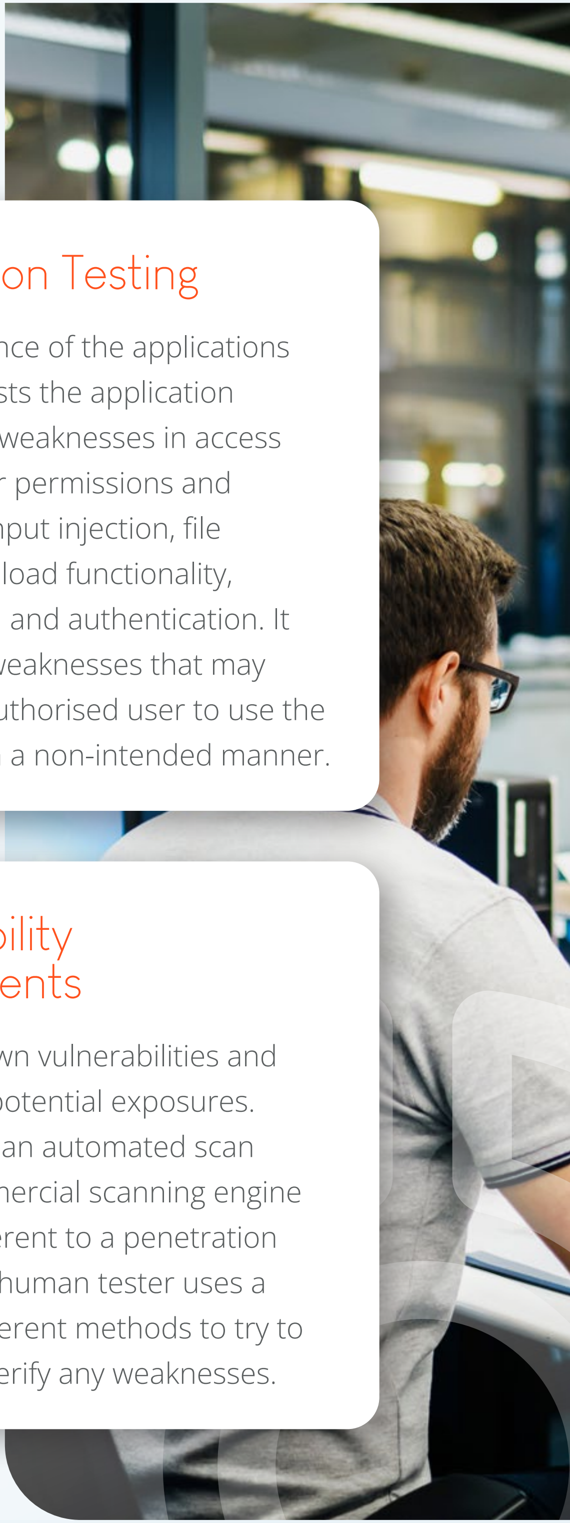
Also known as a ITHC, can be used to test an organisation's compliance with security policies, the security awareness of its staff and how effectively it can respond to security threats.

Infrastructure Testing

This involves conducting penetration testing or vulnerability assessments of external or internal systems and does not normally include application testing.

Cloud Security Testing

Is penetration test or vulnerability assessments of applications, infrastructure or the portal configuration of systems that are hosted within Cloud providers.



Application Testing

Gives assurance of the applications security. It tests the application manually for weaknesses in access controls, user permissions and separation, input injection, file upload/download functionality, authorisation and authentication. It can identify weaknesses that may allow an unauthorised user to use the application in a non-intended manner.

Vulnerability Assessments

Look for known vulnerabilities and report back potential exposures. It is normally an automated scan using a commercial scanning engine tool. It is different to a penetration test where a human tester uses a variety of different methods to try to exploit and verify any weaknesses.

Targeted Attack Simulation

Simulated attack testing focused on Red Teaming, Phishing and Social Engineering.

Red Teaming

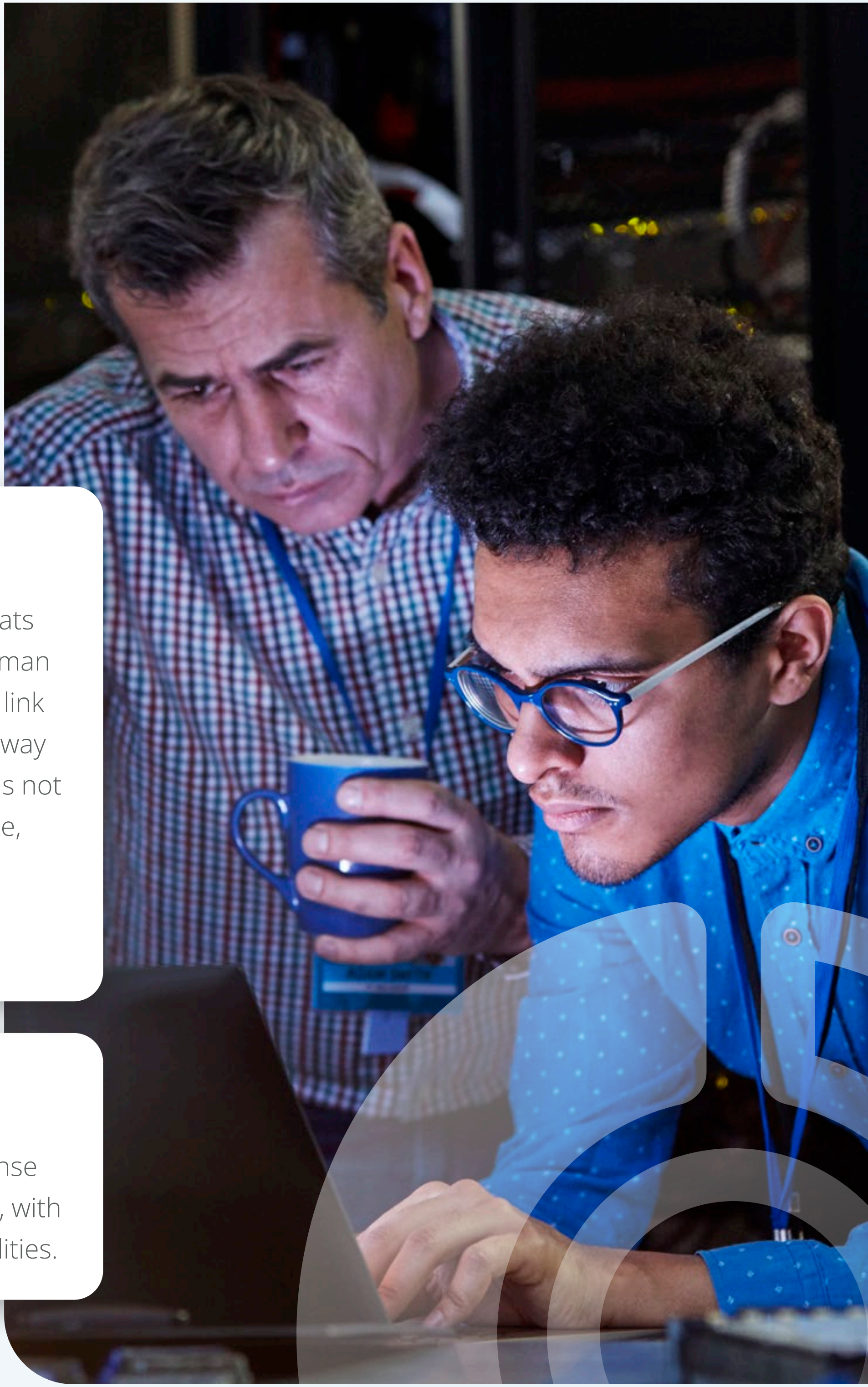
Is scenario-based penetration testing which aids organisations in gaining a clear understanding of the threats they face. Uniquely, Red Teaming allows business stakeholders to measure how effective their controls and processes are at detecting, containing and preventing highly sophisticated cyber attacks.

Social Engineering

Is one of the biggest security threats organisations face, as typically human behaviour is the weakest security link in any network. Often the easiest way to breach a company or network is not via externally hacking their website, it is simply via tricking employees to gain access to the building.

Phishing Simulation

Is the process of testing your staff's awareness and response to phishing emails in a safe and constructive environment, with the aim of improving their detection and reporting capabilities.



cyberlab

Wireless and Mobile Testing

Wireless, mobile and lost device testing.

Wireless Testing

Assesses the configuration and deployment of wireless networks and devices to ensure that only the intended end users can use the network and associated services.

Mobile Testing

Covers many areas such as the device configuration, the management of the device and the applications used on the device.

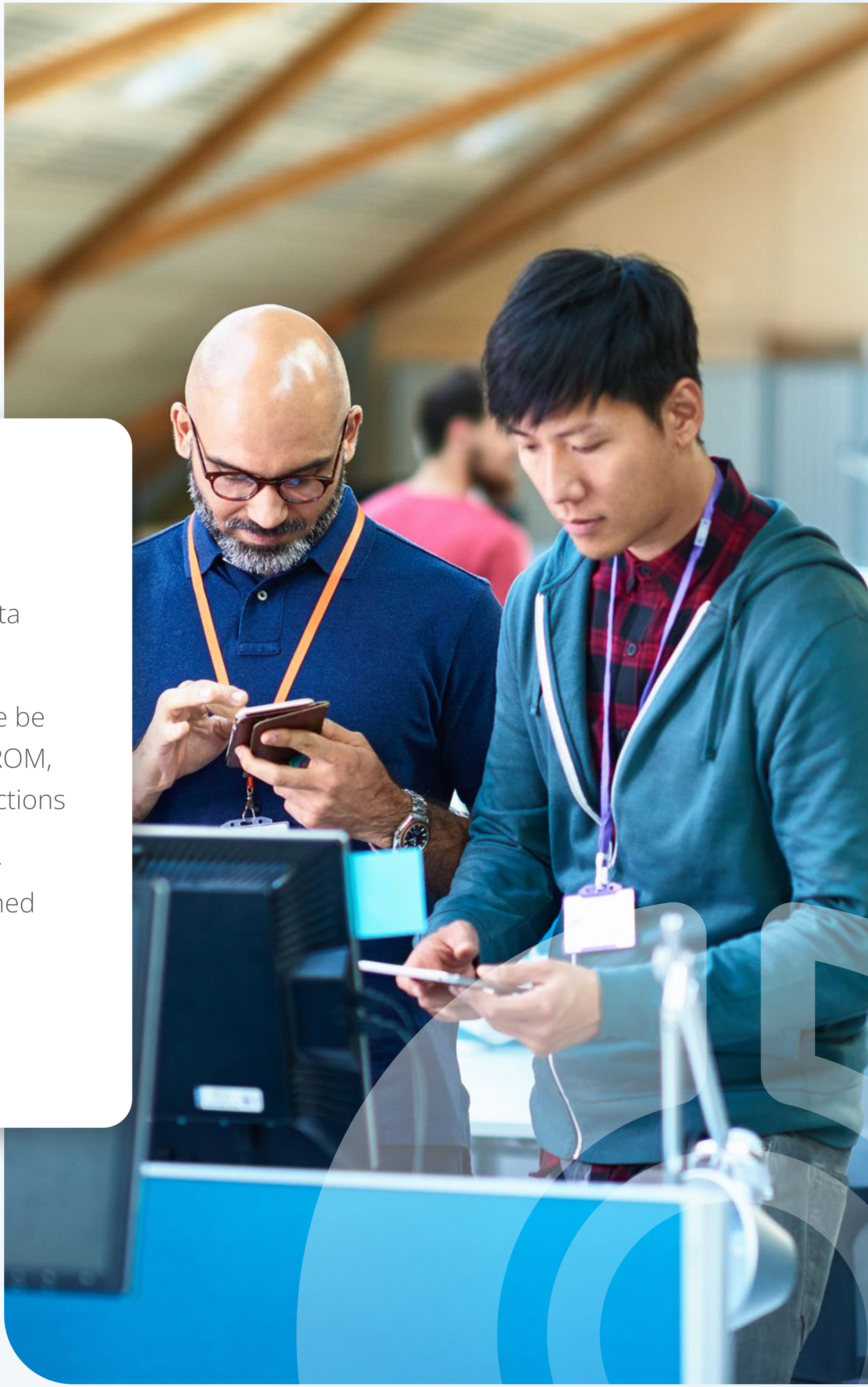
Lost Device Testing

This typically includes:

Encryption review – can any data be read from the hard disk,

Physical review – can the device be compromised via the USB, CDROM, Firewire or Thunderbolt connections

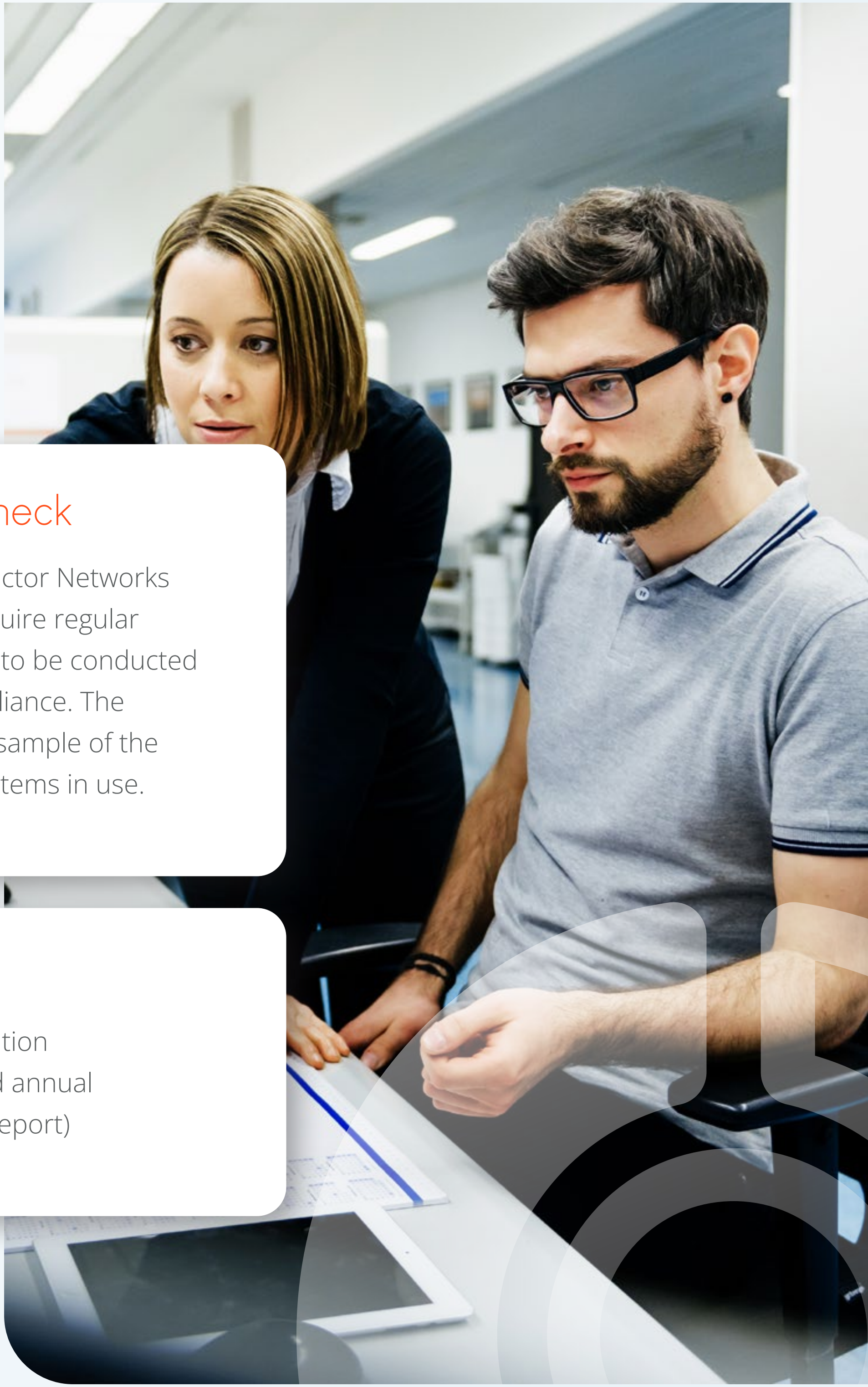
Mobile or tablet device review - what information can be obtained from the mobile device.



cyberlab

Compliance Testing

Penetration testing to assist with PCI-DSS, ISO 27001 and PSN CoCo compliance.



PCI DSS Testing

The Payment Card Industry Data Security Standard (PCI DSS) version 3.2 requires that regular security testing is conducted. Requirement 11.3 states that penetration testing should be conducted on both external and internal systems to ensure requirements are met.

PSN IT Health Check

The PSN CoCo (Public Sector Networks Code of Connection) require regular annual IT Health Checks to be conducted and submitted for compliance. The ITHC typically involves a sample of the external and internal systems in use.

ISO 27001 Testing

The ISO 27001:2013 standards control A.12.6.1 of Annex A requires that penetration testing or vulnerability assessments are conducted. As part of your ISO initial and annual compliance audit, your auditor will require evidence (such as a penetration test report) that you have conducted sufficient checks relating to security vulnerabilities.

cyberlab

Building Reviews

Build reviews of operating systems and databases against industry benchmarks.

Build Reviews

A build review assesses the configuration of the operating system, device configuration and its settings against industry benchmarks.

Gold Build Review

A gold build review involves conducting a software build review of your master template used in group wide deployments.

Database Security Review

A database review assesses the configuration of the database server operating system, the server software and the configuration of the database and its settings against industry benchmarks.

cyberlab

Network Security

Network device testing, configuration reviews and segregation testing.

Network Security

A typical network security review consists of a manual review of the running configuration of the device itself to identify any security configuration issues.

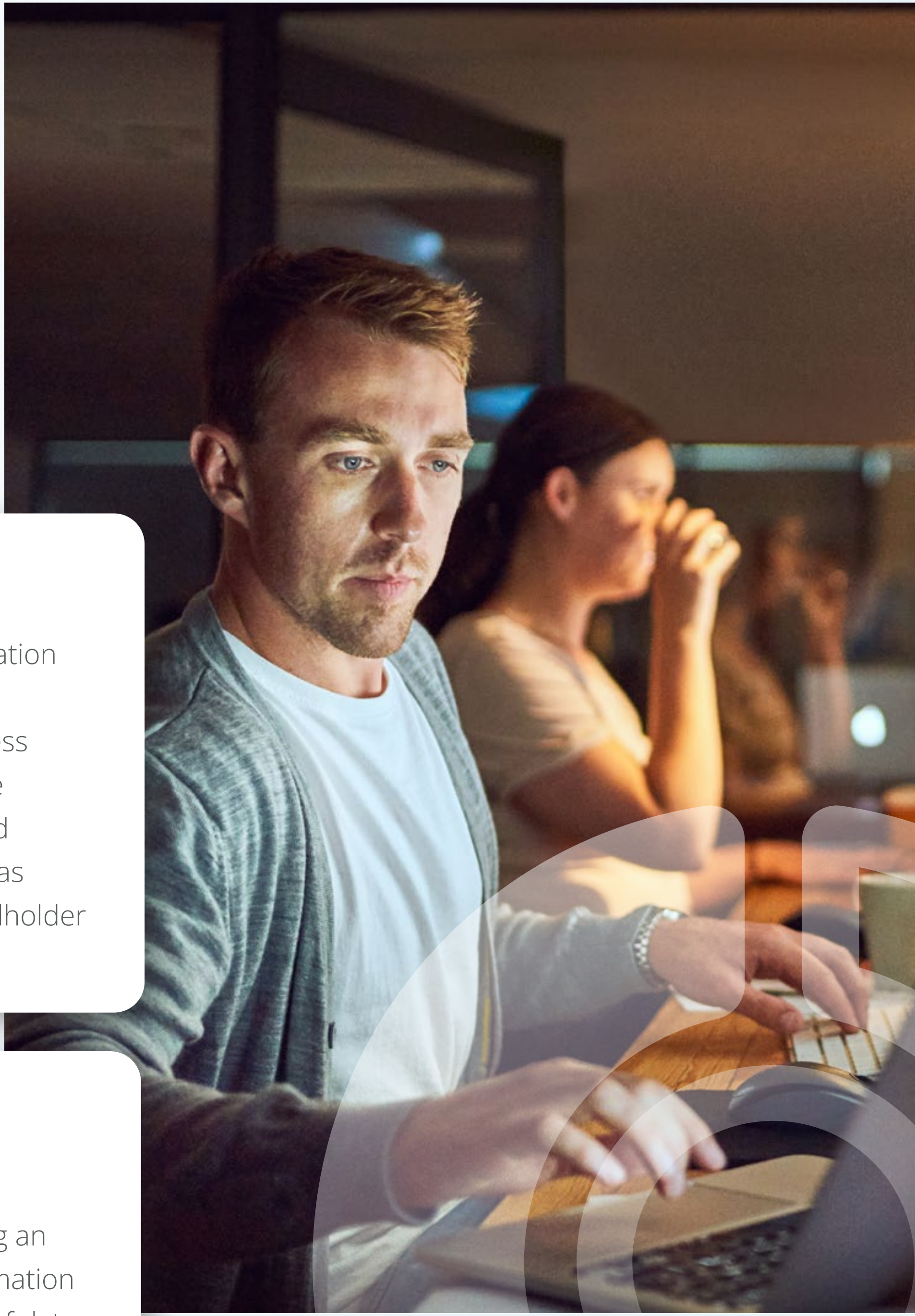
This is a much more detailed review than a vulnerability scan and can identify missconfigured devices that could leave the network or the management of the device at risk.

VLAN Hopping

Is the process of testing separation between networks. This is typically conducted between less sensitive networks, such as the internal corporate network and more sensitive networks such as management networks or cardholder data environments (CDE).

Traffic Sniffing

Involves capturing traffic at a scheduled time and conducting an analysis on the captured information to ensure that the encryption of data in transit is working as it should be.



Specialist Testing

VoIP phone systems, IoT device testing and SCADA security.

VoIP Security Testing

In many organisations, video conference units or telephones are placed within meeting rooms or public areas where visitors will have physical access.

Testing can identify if the devices can be used to connect to and compromise the internal corporate network.

IoT Security Testing

Is an essential service to ensure the device or the software used to control the IoT hardware is not vulnerable to security weaknesses that could allow the device to become compromised and data obtained.

SCADA Security

As SCADA systems often looks after critical infrastructure essential for manufacturing or national infrastructure, penetration testing should be performed to ensure no vulnerabilities exist within internal systems, applications and from the Internet.

Capabilities, Accreditations and Frameworks

Armadillo Sec Ltd are a CREST approved Penetration Testing, Vulnerability Assessment and a STAR and GBEST Attack Simulation testing company. We are also accredited by the NCSC as a green light company authorised to perform CHECK ITHC assessments for government departments.

We have a highly experienced team of consultants, with 70% holding the highest CREST CCT level infrastructure or web application certifications, with the remainder holding the CREST CRT or the equivalent Tiger QSTM certifications. Our consultants are also CHECK Team Leaders (CTLs) or CHECK Team Members (CTMs) and are approved to conduct government CHECK testing. Additionally, our attack simulation consultants also hold the CREST CSAS and CSAM certifications, allowing us to work on STAR and GBEST attack simulation engagements.

Our team have many decades of experience conducting a broad range of central government, public sector, health care, financial services and commercial testing engagements and always aim to go the extra mile for our customers.

An online comparison of the certifications we hold can be found on the official CREST website at https://service-selection-platform.crest-approved.org/ and our NCSC CHECK green light status can be validated at https://www.ncsc.gov.uk/professional-service/armadillo-sec-ltd-check-service.

cyberlab

CREST. VA PEN TEST

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

Crown Commercial Service Supplier

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing

CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS

TRUSTED PARTNER

CREST Certifications	Certified Testers
Practitioner Security Analysts (CPSA)	✓
Registered Penetration Testers (CRT)	✓
Certified Web Application Testers (CCT APP)	✓
Certified Infrastructure Testers (CCT INF)	✓
Certified Simulated Attack Specialist (CSAS)	✓
Certified Simulated Attack Manager (CSAM)	✓

CHECK Certifications	Certified Testers
CHECK Team Member (CTM)	✓
CHECK Team Leader (CTL) – Infrastructure	✓
CHECK Team Leader (CTL) – Applications	✓

Our information security controls, and quality management systems meet and exceed the high standards set by the ISO 27001:2013 and ISO9001:2015 standards. We are also Cyber Essentials Plus certified.

We are an approved HM Government supplier and part of the Crown Commercial Supplier G-Cloud and Cyber Security Services 3 frameworks, as well as an assured service provider of NCSC approved security testing services.

bsi ISO 9001 Quality Management Systems CERTIFIED FS32851

QMS ISO 27001 : 2013 REGISTERED

Our People. Our Platform. Protects You.

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

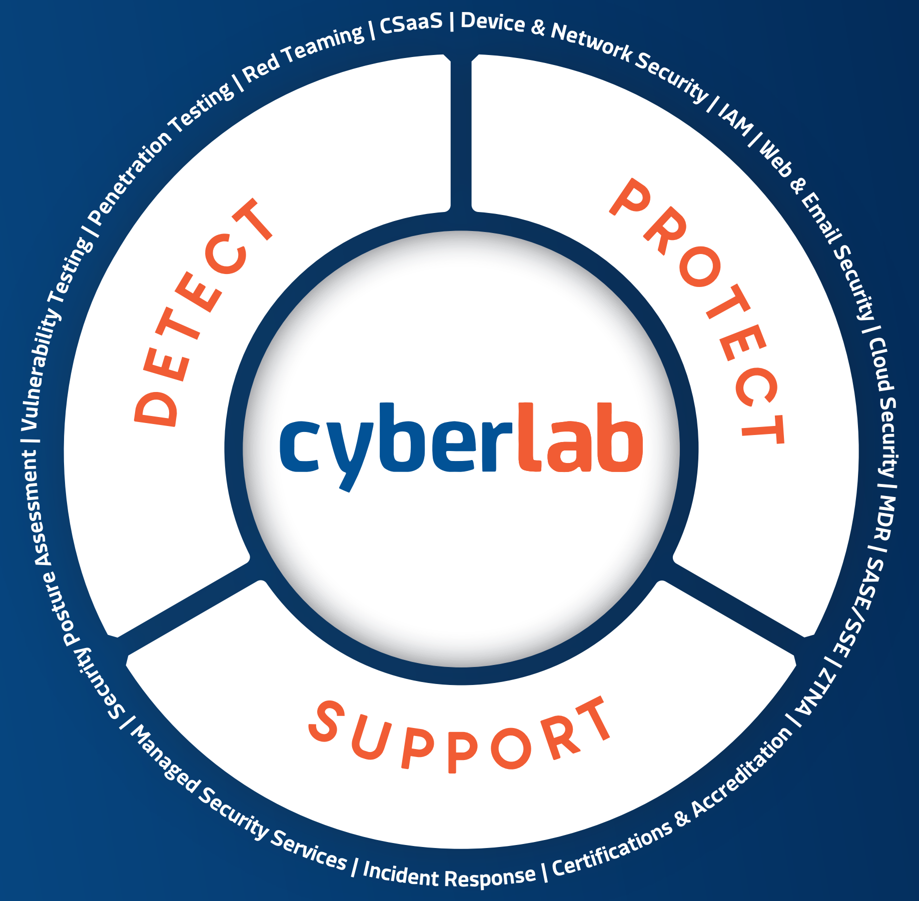
By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reenforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk I 0333 050 8120 I cyberlab.co.uk

cyberlab



cyberlab
DETECT
PROTECT
SUPPORT
Security Posture Assessment | Vulnerability Testing | Penetration Testing | Red Teaming | CSaaS | Device & Network Security | IAM | Web & Email Security | Cloud Security | MDR | SASE/SSE | ZTNA | Certifications & Accreditation | Incident Response | Managed Security Services |

cyberlab

cyberlab.co.uk