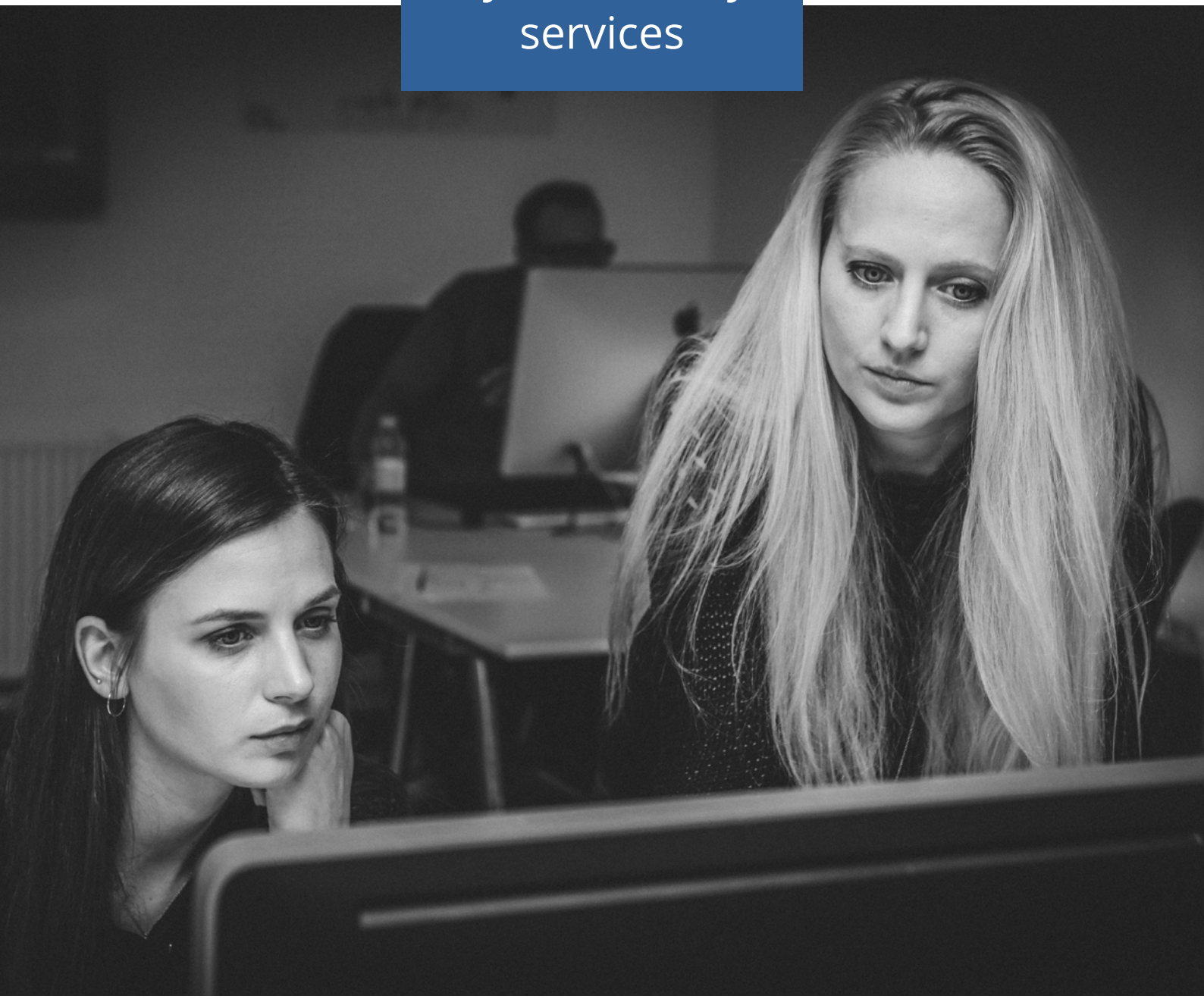
Quiss

Excellence through experience

Cyber security services



Powered by illume

Keep your data safe, prevent regulatory fines and avert financial extortion

Know your weaknesses and stay secure with our range of cyber security services

Phishing simulation & training

Simulation

You could have the latest and greatest spam filter to stop phishing emails, but it only takes one email to go undetected. Suppose a staff member is untrained in spotting and reporting phishing emails, then potentially, your whole network could be compromised from just one click.

Phishing simulation sends phishing emails to your team members at an interval that suits you. See what emails your team has received and their actions when they received them.

Training

Not only are your team receiving simulated phishing to help better their knowledge regarding phishing emails, but we will also provide bite-sized video training.

Armed with the data from the simulation, your team can receive relevant training covering core topics based on information security and compliance.

Cyber Essentials & Plus

Cyber Essentials

Cyber Essentials allows organisations to demonstrate that they have a consistent and effective level of cyber security measures implemented, which provides assurance and reassurance to clients and investors that they are safe to do business with.

Cyber Essentials certification is often mandated within specific sectors as well as being a go-to standard for managing the security risks of supply chains.

The basic level can either be completed via self-assessment or guided.

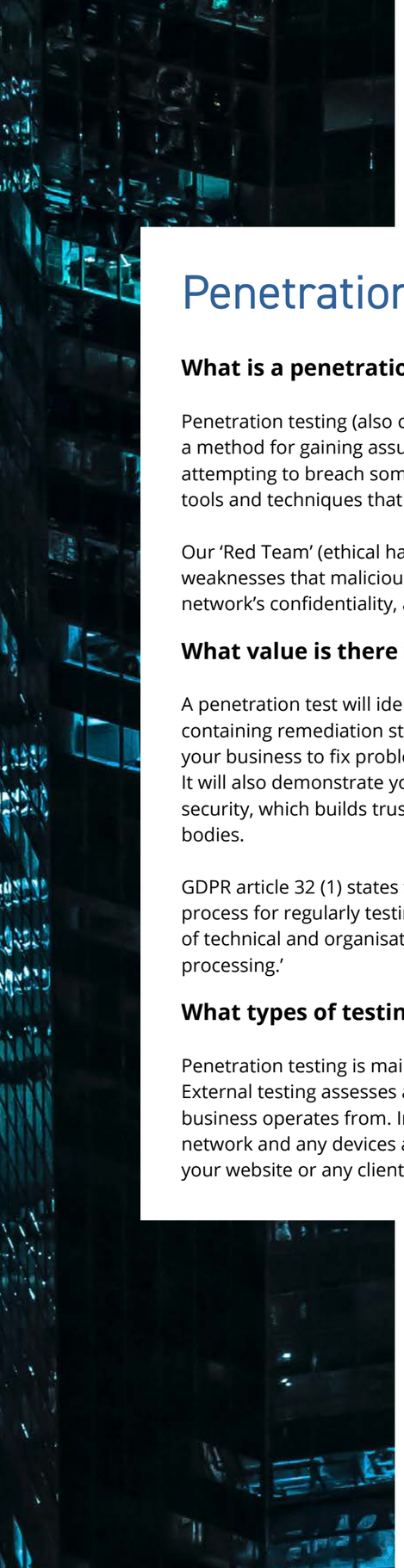
Cyber Essentials Plus

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard. Cyber Essentials requires organisations to have several technical and procedural controls to improve their information security to mitigate common internet-borne cyber-attacks.

Cyber Essentials Plus is a series of tests that further assure that these technical controls have been successfully implemented and are working effectively within an organisation.

Organisations must have successfully obtained the Cyber Essentials standard first before being eligible to apply for Cyber Essentials Plus.

CYBER ESSENTIALS



Penetration testing

What is a penetration test?

Penetration testing (also called ‘pen testing’ or ‘ethical hacking’) is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system’s security, using the same tools and techniques that a malicious hacker might.

Our ‘Red Team’ (ethical hackers) examines your IT systems for any weaknesses that malicious attackers may exploit to compromise the network’s confidentiality, availability, integrity, and associated data.

What value is there in penetration testing?

A penetration test will identify any issues with your systems. A report containing remediation steps and guidance will be produced, allowing your business to fix problems before a malicious attacker exploits them. It will also demonstrate your commitment to responsible and secure data security, which builds trust with your clients, partners, and regulatory bodies.

GDPR article 32 (1) states that organisations should implement ‘a process for regularly testing, assessing and evaluating the effectiveness of technical and organisations measures for ensuring the security of processing.’

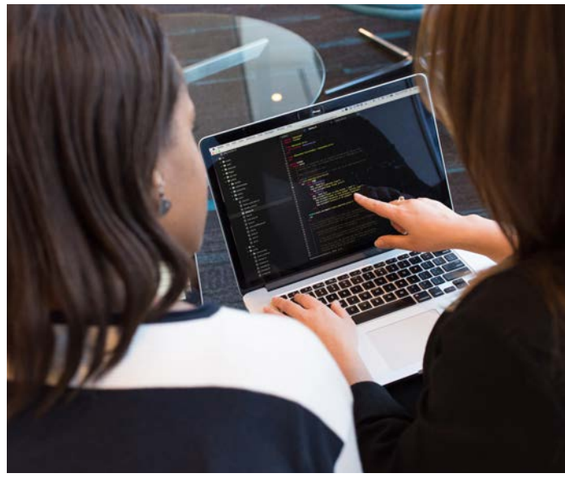
What types of testing are there?

Penetration testing is mainly broken down into three main variants. External testing assesses any public-facing infrastructure that your business operates from. Internal testing assesses your private corporate network and any devices attached to it. Web application testing assesses your website or any client portals you offer to clients.

External testing

External testing evaluates the threat of a hacker gaining access to your corporate network. Like a malicious hacker, we will attempt to gain access using advanced social engineering and exploit any vulnerabilities with your public-facing infrastructure. An illume external penetration test includes advanced social engineering as standard, mimicking the most realistic attack scenario facing your business today.

One size does not fit all. We work closely with you and your business to understand your needs and requirements to provide you with an appropriate testing frequency to help keep your business secure.



Internal testing

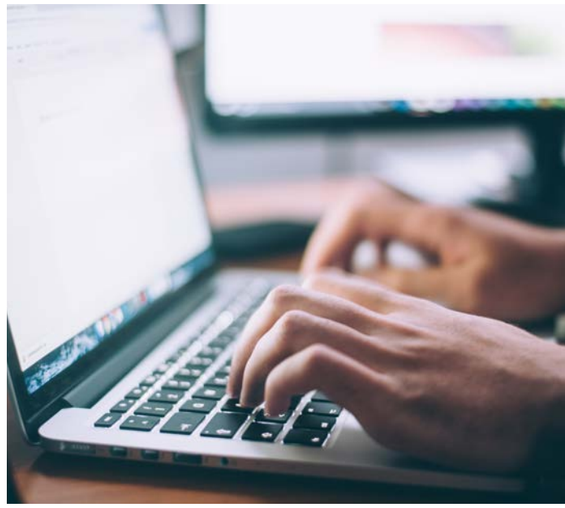
Internal testing assesses your infrastructure inside your corporate network, think staff computers, internal servers, printers, etc. Often people think, “well, someone has got to get into my office first” but that is not true. A malicious hacker could gain access to your network by an employee clicking on a link or perhaps a rogue employee or third-party contractor.

An internal test will not only highlight any technical vulnerabilities on your systems but will also identify any employees who may be using weak passwords, or in fact, store passwords unencrypted on their system.

Web Application testing

A web application penetration test assesses the risk of a malicious attacker compromising your website. A couple of common issues we regularly see across web applications is the ability to view other customers’ data, such as past orders/confidential documents or hijacking another person’s account.

If your website does not hold sensitive information, there is still a reputational risk with your ‘brochure website’. What if a malicious hacker gained access to your website and defaced it or even uploaded some malware that prospective clients could download? A web application penetration test identifies any vulnerabilities present across your web applications.



Social engineering/Red teaming

Have you ever wondered how far a malicious attacker could go to obtain access to your corporate network?

In the past, our team has been known to pretend to be a delivery driver and walk straight into a client's office to deliver a malicious USB stick directly to an employee, which, when plugged in, would provide direct access to the employee's computer.

Our social engineers can tailor a genuinely bespoke attack to your situation.

Vulnerability scanning

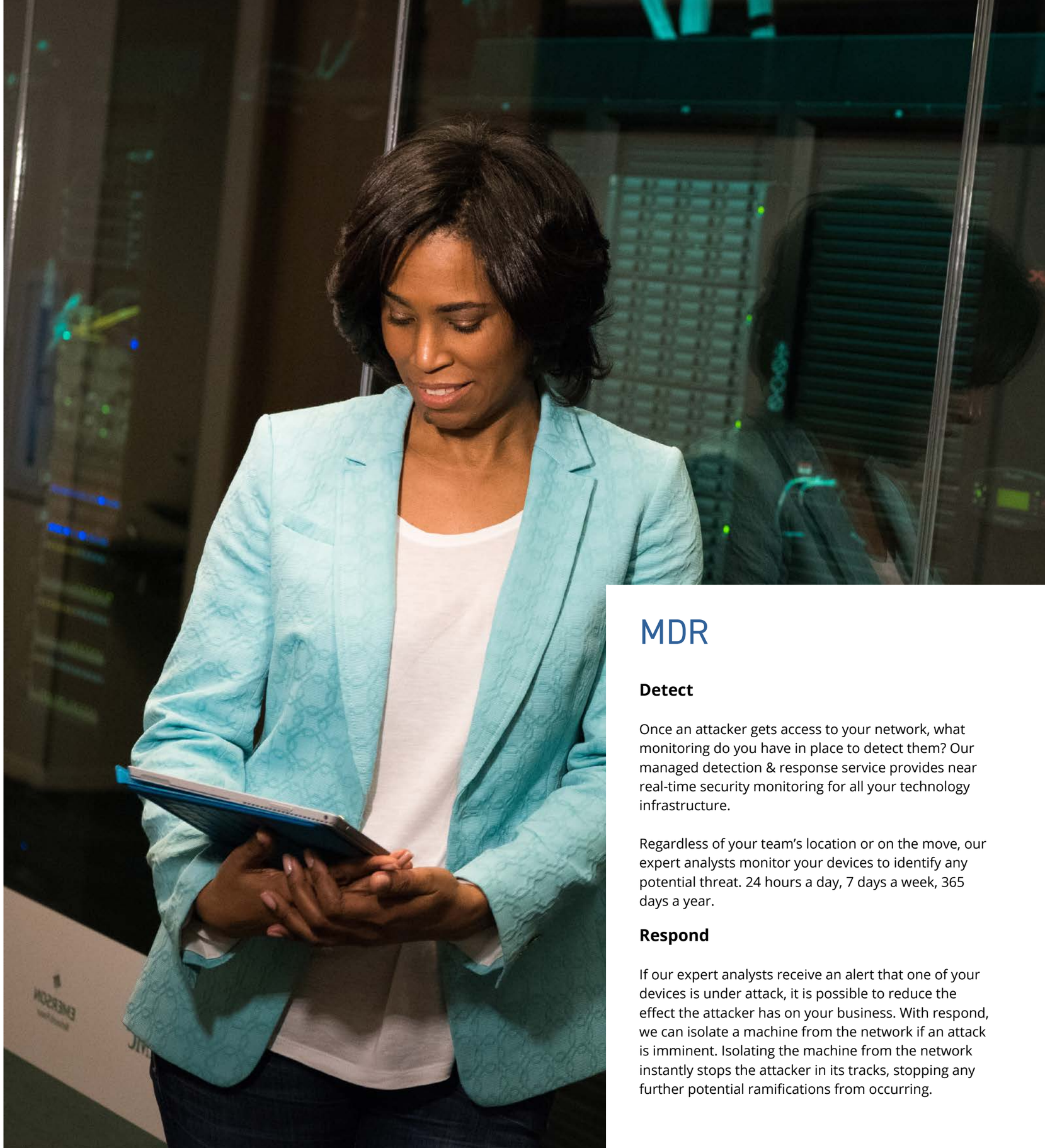
Agent based

As technology advances, vulnerabilities will continue to be discovered at an increasing rate. Use the same technology that many Fortune 500 companies use. Vulnerability scanning will highlight any issues with your infrastructure regardless of the location. Most of your team are on the move or remote? No problem.

Receive a notification when your infrastructure is vulnerable, so you and your team can resolve it before it is exploited.

Agentless

Are all of your team still based in the office? That's not a problem. The illume vulnerability scanner can be deployed to your local area network. Ensuring all connected devices are scanned regularly, providing you and your team with the intelligence to know what needs patching before a hacker exploits it.



MDR

Detect

Once an attacker gets access to your network, what monitoring do you have in place to detect them? Our managed detection & response service provides near real-time security monitoring for all your technology infrastructure.

Regardless of your team's location or on the move, our expert analysts monitor your devices to identify any potential threat. 24 hours a day, 7 days a week, 365 days a year.

Respond

If our expert analysts receive an alert that one of your devices is under attack, it is possible to reduce the effect the attacker has on your business. With respond, we can isolate a machine from the network if an attack is imminent. Isolating the machine from the network instantly stops the attacker in its tracks, stopping any further potential ramifications from occurring.

Registered Office: Quiss Technology PLC,
Claymore, Tamworth, B77 5DQ

0333 222 4334
enquiries@quiss.co.uk

Quiss
Excellence through experience
www.quiss.co.uk