PENETRATION TESTING for Digital Health Technologies.

acorn compliance

“

Pen Testing are like vaccines for Health Technologies.

Penetration testing, AKA Pen testing, is a self-inflicted cyberattack against your own computer systems.

It usually involves **hiring an expert who will try to breach the security** of your application with the aim of uncovering vulnerabilities in your mobile apps, web apps, cloud infrastructure and any Internet of Things (IoT) devices that form part of **your HealthTech innovation**.

Michael Bell

Partner. Acorn Compliance.

Pen testing gives you invaluable information as to **where the weak spots are** within your HealthTech innovation and it’s essential you know this **before hackers do**.

Only once you know the vulnerabilities that exist in your HealthTech innovation, can you **start the work to address them**.

PENETRATION TESTING IS MANDATORY.

Pen testing is a very important part of the **Digital Technology Assessment Criteria (DTAC).** If your systems are secure so are the patient data they hold. And this is a crucial aspect for **the NHS** to determine that your solution is safe.

NHS

Digital Technology Assessment Criteria (DTAC)

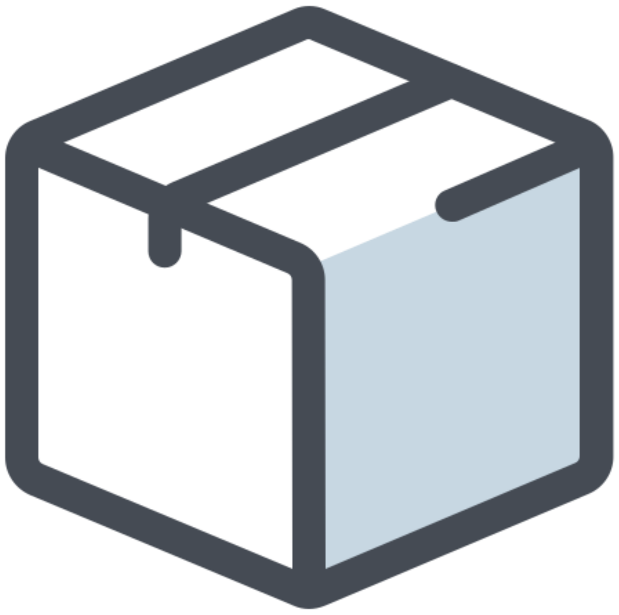
PENETRATION TESTING IS NOT A ONE OFF EXERCISE.

Pen testing results relate to a specific point in time, or to **a particular version of your innovation**.

Therefore, it’s essential that you run penetration testing **as frequently as required given the context of your innovation** and your product release life cycle.

A comprehensive Pen test will look across all aspects of your innovation and will test against the current **Open Web Application Security Project (OWASP) Top 10** and other vulnerability lists.

Robust Pen testing will include both **black box** and white box methods of testing as a minimum to locate vulnerabilities within your HealthTech innovation.



BLACK BOX TESTING

Black box testing determines vulnerabilities just like a hacker would, **with no inside knowledge** of your innovation.

WHITE BOX TESTING

White box testing **leverages inside knowledge of your infrastructure** and applications to uncover the possibility of insider attacks.

A key part of any Pen testing output is the **penetration testing report**. This should contain:

- **An executive summary** of the findings and ideally a graphical representation of vulnerabilities
- An outline detailing the **scope of the testing** that was performed
- The **testing methodology used** including a list of tests and test cases
- The **list of vulnerabilities identified**
- A **classification of the severity** of these vulnerabilities: critical, high, medium, low against the CVSS framework.
- A **description of these vulnerabilities** including the impact they have.
- A **list of recommendations** to address these vulnerabilities

CONTINUOUS PEN TESTING

Continuous scanning (series of regular assessments) can also be employed to ensure that you **do not introduce further vulnerabilities** into your HealthTech innovation following the initial Pen test.

Continuous scanning as part of a defence in depth strategy for Cyber Security can make the difference **between a once-safe system and a continuously safe one**.

Hope you found this helpful!

This is a series we are making to help HealthTech Innovators access better resources.

Just our small way of helping!