//Penetration Testing

Penetration Testing is a form of 'ethical hacking' that will assess and test your systems for potential vulnerabilities and weaknesses

About Cyberfort

Cyberfort exists to provide our clients with the peace-of-mind about the security of their data and the compliance of their business, which is much needed in our increasingly data hungry world.

Since we were established in 2017, we have brought together technology, people, expertise, facilities and leaders in cybersecurity to create a capability that is second to none. Our vision is to create a safer world for us all to live, by creating safer organisations. To do this we want to be recognised and trusted for our excellence in everything we do. We aim to be an authentic leader, with a human voice in a world that is increasingly digitised and robotic.

Cyberfort's Penetration Testing service is designed to give you the confidence that the technology you are using or developing is as secure as it possibly can be. Whether you are developing software for your clients, designed to hold their customers' data, or you want to ensure your own infrastructure is secure, you need to test your technology for vulnerabilities.

Your prospective clients will rigorously test your software before they consider buying from you, or will seek assurances from you that it is resilient to cyberattack. But if they discover any weakness, or can't be confident that your internal systems are secure, it is likely to be the end of that relationship.

This is where Cyberfort's range of services can help you. You know you need to carry out a penetration or 'pen test' of your IT infrastructure. Some businesses see this process as simply a hoop to jump through on the journey to get their technology to market. But, not all pen tests are created equal. The most effective pen tests aren't a linear process, they're an exploration. Cyberfort pen testers are renowned for finding system vulnerabilities other pen testers just haven't dug deep enough to uncover. We tell you what you don't know, not what you know already, allowing you to make informed decisions about where best to invest your resources and budget.

Our pen testers are all CHECK-accredited and CREST-certified and Cyberfort is recognised as a partner of the National Cyber Security Centre (NCSC) under its Assured Service Provider scheme. We are also a CREST-accredited Cyber Essentials certifying body, meaning we can help you achieve and assess Cyber Essentials and Cyber Essentials Plus.

Following your pen test, we'll debrief you of our findings, and provide you with a report written in language understandable at Board level as well as by your technical experts. Your report will provide pragmatic, actionable steps to fix any vulnerabilities we've found. An important part of our delivery is sharing our knowledge with you, and empowering you to move forward with robust security processes in place. Cyberfort will give you the confidence that your technology is as secure as it is possible to be, and that your technology is absolutely ready to go to market.

Cyberfort's services encompass four separate activities:

Application Penetration Testing

Cyberfort's application penetration testing service is an authorised, simulated attack on your applications and associated infrastructure performed to identify vulnerabilities and strengths within your environment.

We provide reliable independent assurance that your infrastructure is protected from security threats.

Network Infrastructure Testing

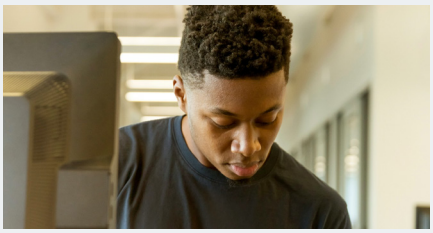
An infrastructure penetration test is an authorised, simulated attack on your infrastructure. We offer black box (unauthenticated) and white box (authenticated) testing.

We provide actionable technical remediation advice and support to help ensure best practice security controls are implemented.

Oversight Monitoring

Cyberfort's 24/7/365 monitoring service guarantees complete coverage of your network perimeter. The service proactively detects changes and vulnerabilities in external-facing infrastructure as and when they occur.

False positives are removed by CREST consultants, and alerts with remediation instructions are emailed to decision makers who can then take remedial action.

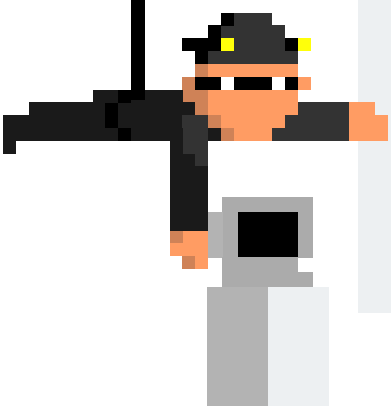


Configuration Review

The secure configuration of networked devices is vital to your overall cybersecurity. Poorly patched or misconfigured devices leave your business open to compromise by internet or internal threats.

Cyberfort's CREST and Check-accredited pen testers will perform in-depth analysis of your standard device builds, databases and system configurations, identifying deviations from industry-standard best practices.

We'll help you minimise your attack surface and remove vulnerabilities from incorrectly configured devices.



Your cybersecurity 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 your business to adequately assess the security of your complex business systems
- **Lack of knowledge** or understanding of security models as they apply to your organisation's ecosystem
- **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
- **Managing a suitable penetration** testing programme in your enterprise
- **Implementing follow-up actions** and measuring benefit realisation

How Cyberfort can help you

- A reduction in information and communications technology (ICT) costs over the longer 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 to deliver a full range of cost effective testing
- Eliminate the need to employ specialist (and expensive) staff, reducing training costs