Penetration Testing

Vulnerability Assessment

FORTIS CYBER®

PENETRATION TESTING OVERVIEW

FORTIS INFORMATION SECURITY & RISK MANAGEMENT

An Introduction to Fortis Information Security & Risk Management

Fortis is an ISO 9001 certified UK based Information Security and Risk Management consultancy

Fortis has constructed an arsenal of information security and risk management services, allowing organisations of any size or industry to stay in control of their cyber security. By being able to identify security risks and detect vulnerabilities, companies will be armed with the knowledge required to more easily protect themselves and meet and respond to omnipresent and evolving cyber threats.

Core Values: Trust, Discretion, Delivery, and Privacy

- Founded by a senior cyber expert with 30 years' first-hand experience in the UK Militvary and Global Enterprise.
- Fortis is a trusted partner of the UK Home Office and Police Forces – Cyber Resilience Centre.
- Fortis can provide you with access to cross industry skilled, experienced, and certified information security subject matter experts.

The Core Team Members of Fortis:

- Trusted - All Fortis Consultants are skilled, experienced, and certified professionals, who have an invaluable depth of knowledge in their respective security fields.
- Enterprise Experience - held senior information security architecture and leadership positions for Juniper Networks, Thomson Reuters, Airbus, WorldPay and Atomic Weapons Agency.
- Government Experience - Information Security at government levels, gained from within the UK Defence, UK Home Office, and UK FCO.
- Insight - Security specialists drawn from leading security organisations: HM Forces, global enterprise, and UK intelligence services.

Fortis Industry Accreditations and Certifications

Penetration Testing

Vulnerability Assessment

Security Penetration Testing

As part of Fortis' suite of security risk assessment services, our penetration testing service enables client to identify, assess and prioritise vulnerabilities and security flaws across their applications, APIs, platforms and infrastructure.

Over the last decade threat vectors only previously encountered by nation states have become increasingly common among enterprises. The Fortis team has been mitigating and managing the risks from these attacks for our clients for years and as the threat landscape shifts, so too have the number of organisations that require access to our trusted and experience security professionals.

Penetration testing helps to identify security vulnerabilities which might otherwise leave your company open to compromise. Fortis has a proven track record of finding such vulnerabilities in some of the most complex and sophisticated IT environments.

With our broad industry experience Fortis can work alongside your organisation to provide the benefit of situational awareness, usually reserved for those associated with government departments, together with the context and understanding of corporate environments and the associated challenges and culture.

Our security testing services are designed to:

- **Improve business awareness and understanding of your cyber security exposure to risk**
- **Identify and fix security vulnerabilities before they can be exploited by cyber criminals**
- **Support ISO 27001, PCI DSS, GDPR and PAS 499 ID & authentication compliance**
- **Provide independent technical security assurance of your security controls**
- **Enable the prioritisation of security investments through actionable intelligence**
- **Demonstrate a continuous commitment to security to customers and partners**

The Fortis Approach

The Fortis approach to security testing is based upon your requirements and required outcome. Tests can be performed from the perspective of an external attacker with no knowledge of the target services or infrastructure, as an authenticated user, or with comprehensive understanding of the service and its design.

Some of the more common types of penetration test we offer:

- External network (or infrastructure) penetration testing
- Internal network penetration testing
- Web application penetration testing
- Cloud penetration testing including AWS, Azure and GCP
- Mobile iOS, Android applications and API penetration testing
- Wireless Network (Wi-Fi) penetration testing
- Social Engineering (both physical and digital social engineering penetration testing)
- Red Team, full spectrum attack simulation
- Biometric systems penetration testing

Fortis Credentials

Fortis Cyber's penetration testing and red teaming group are extremely well certified, holding multiple certifications awarded by bodies such as CREST, Offensive Security and the Tiger Scheme. Fortis also complements this focused knowledge with National Cyber security Centre (NCSC) Certified Cyber professionals to provide a valuable wider viewpoint to penetration testing assurance.

Alongside certifications our testers also engage with the security community, present at specialist security testing conferences and have co-authored books on testing.

Fortis Cyber is CREST accredited for both penetration testing and vulnerability assessments. Through CREST's demanding accreditation process, organisations buying security testing services get the assurance that:

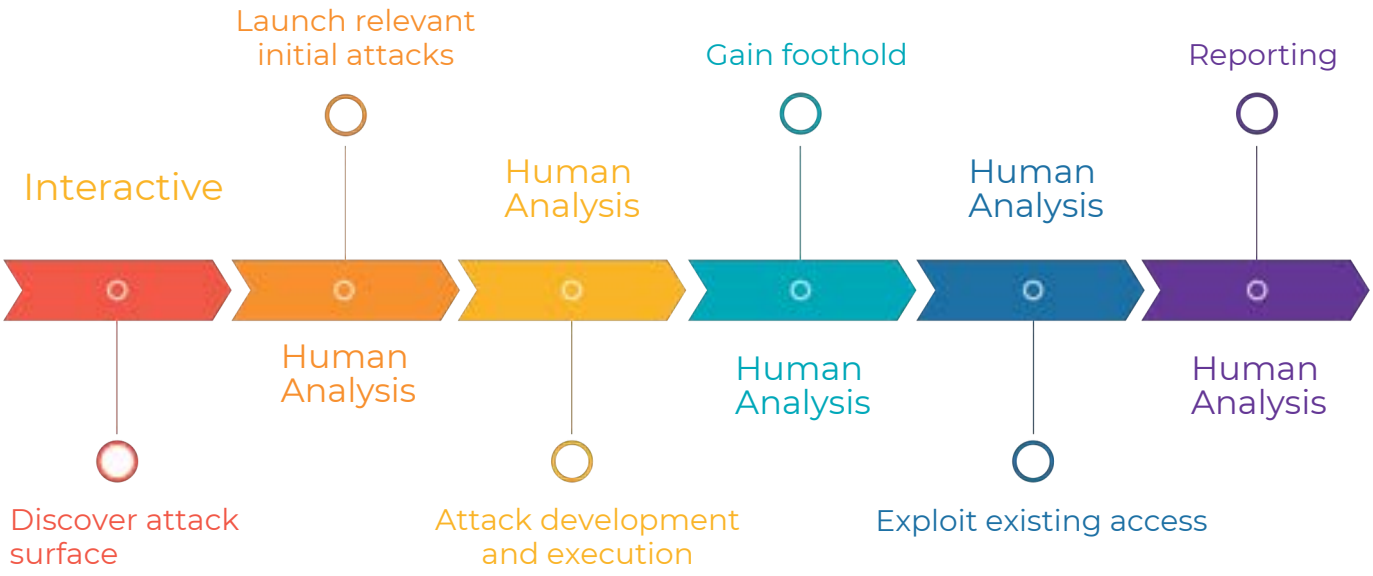
- The services will be delivered by trusted companies with best practice policies and procedures.
- The work will be conducted by highly-qualified individuals with the up to date knowledge, skill, and competence to deal with all the latest vulnerabilities and techniques used by real attackers.
- Both the company assessments and individual qualifications and underpinned by a meaningful and enforceable codes of conduct.

CREST SECURITY TESTING
Penetration Testing

CREST SECURITY TESTING
Vulnerability Assessment

Fortis Penetration Testing Methodology

As the penetration testing industry has matured, certifying bodies have increasingly demanded a standard way of performing penetration testing activities. However, there is only so much standardisation that can be done before the creativity inherent in “hacking” is removed and the benefit of the service is lost. Nevertheless, this same standardisation encourages better quality testing exercises by making sure that a minimum level of testing is completed.



The Fortis methodology is iterative in nature, this means that the process repeats itself until either all options have been exhausted or the testing time period has expired.

1. Discover Attack Surface - each iteration starts with attack surface discovery. This can be at any level of the target, for example, authenticated or unauthenticated, or as a result of the exposure produced by another attack.

2. Launch Relevant Initial Attacks - next, exploratory attacks are launched in order to further understand the attack surface. These attacks are tuned to be as relevant as possible for the context.

3. Attack Development & Execution - once the results of the initial attacks are known, the attacks that are most likely to be successful are developed further to maximise the chance of success and then executed.

4. Gain Foothold - should the attack be successful, the attacker has gained a foothold. The attack may require further tuning in order to gain firm access.

5. Controlled Exploitation of Access - in this iteration's final stage, the attacker will look to take advantage of whatever access has been gained. This may simply be access to data and information, or it may be that the successful attack now opens up the possibility of further attacks.

6. Reporting - a detailed penetration test report is supplied. Vulnerabilities and security flaws will be ranked in order of criticality using the open industry standard Common Vulnerability Scoring System (CVSS) framework. This will detail all the vulnerabilities and security flaws found and the recommended remedial actions.

Your Benefit

The majority of the testers Fortis employs work on red teaming engagements as well as penetration testing.

This ensures clients receive the highest level of quality, with testers often recognising scenarios that a normal penetration tester may not have the experience to detect.

Recently a large UK client benefitted from this as the experienced testers identified that the client had unfortunately been breached as they recognised the red team modus operandi during a regular pen test.

Fortis only employs highly skilled and experienced penetration testers which, when coupled with our governance, risk and compliance team's vast industry experience and our excellent service management support ensures unparalleled technical deliverable, business alignment and client satisfaction.

Fortis Information Security & Risk Management (ISRM) offers bespoke engagements to client requirements and will always work with clients to define and deliver the most appropriate service based on their needs. Fortis is technology agnostic and remains independent. This ensures clients receive a service that is contextualised to their business environment and challenges.

To understand how Fortis ISRM can help your organisation, email enquiries@fortiscyber.co.uk or visit **https//fortiscyber.co.uk/services** for more information.

FORTIS CYBER®

Please get in touch

https://www.fortiscyber.co.uk/contact

enquiries@fortiscyber.co.uk

+44 (0) 207 898 3971

Fortis Cyber Security Limited is a limited company registered in England and Wales.

Company Registration Number: 11162256

VAT Registration Number: 291874659