CREST accredited, expert-led pen testing

- ✓ Expose vulnerabilities within infrastructure, networks, web and mobile applications, and cloud environments.
- ✓ We highlight preventative countermeasures and provide advice on remediation
- ✓ If you need to reschedule we will not charge a penalty fee

Get a faster, clearer, and simpler view of your vulnerabilities

Our teams use a mix of automated technologies and human skills to accurately mimic techniques used by cyber attackers targeting organisations in the UK, providing valuable insights for remediation.

Our approach to penetration testing

- Phase 1: Scoping
- Phase 2: Reconnaissance and enumeration
- Phase 3: Mapping and service identification
- Phase 4: Vulnerability analysis
- Phase 5: Service exploitation
- Phase 6: Pivoting and post-exploitation
- Phase 7: Reporting and debrief

CREST certified testers bring extensive experience from across multiple sectors.

Aegis uses the results to create actionable and tracked task lists, aligned to GRC demands.

No waiting for a test to end. Real-time reporting gives you immediate visibility of findings

We get it. Businesses are busy. If you need to move a start date, we will not charge a penalty fee.

For a clearer view of cybersecurity

Click here to start your journey

vambrace

vambrace.co.uk

Our testing services

Cloud Security Testing

Cloud environments bring agility, but also unique security challenges. We test to uncover misconfigurations, permission issues, control gaps, and risky exposures in your AWS, Azure, or Google Cloud environments.

External Infrastructure Testing

External infrastructure **i**s often the first target for attackers probing defences. From perimeter routers, firewalls, and VPNs to avoidable misconfigurations and exposed APIs, we show how attackers could gain access and how to stop them.

Mobile Application Testing

Advanced testing techniques on iOS and Android apps simulate real-world attack scenarios, uncovering weaknesses before they can be exploited. Whether your app is in development or on the open market, our penetration testers will surface any issues around API misconfigurations, insecure data storage, or authentication.

Web Application Testing

Web applications are the face of most organisations. We simulate skilled attackers operating against your customer facing or internal web applications and API's to find exploitable vulnerabilities and insecure configurations.

Red Teaming

While penetration tests are great for surfacing vulnerabilities, Red Teaming combines threat intelligence and human-led initiative to recreate the tactics, techniques, and procedures used by real-world attackers. We demonstrate how access can be gained and movement across your environment can occur to provide clear, prioritised actions.