cowbell® PT

Powered by GMI

Penetration Testing

Uncover hidden vulnerabilities in your applications and networks by simulating real-world attacks, strengthening your defences and fortifying your security.

Key Benefits of GMI Penetration Testing

Our expert "white hat" hackers use a combination of automated tools and manual techniques to simulate real-world attacks, delivering actionable insights and strengthening your cyber security defences.

1. Actionable Knowledge is Power

Our ethical hackers leave no stone unturned, delivering detailed reports with context, recommended resolutions, and compensating controls. This empowers leadership with risk-based insights to support informed decision-making.

2. Cost Savings and Avoidance

The average cost of a data breach in the U.K. is £3.58 million. Investing in penetration testing saves money on incident response and potential damages.

3. Compliance and Public Assurance

Our services enhance internal processes and strengthen security posture, while ensuring regulatory compliance, safeguarding customer data, and protecting your brand.

4. Identify and Prioritise Risks

Regular penetration testing helps assess security and prioritise risks, giving organisations a competitive edge in anticipating and preventing attacks.

5. Prevent Hackers from Infiltrating Systems

Penetration tests simulate real-world attacks, exposing security gaps and providing the opportunity to remediate weaknesses before genuine threats arise.

6. Mature Your Environment

Ongoing improvements in security posture demonstrate your commitment to information security and compliance, enhancing your competitive advantage in the eyes of clients.

7. Avoid Costly Data Breaches and Loss of Business Operability

Recovering from data breaches can be extremely costly. Regular penetration testing helps prevent financial loss and protects your brand's reputation.

Penetration Testing Packages

STANDARD PACKAGE*

✓ Internal and External Network

- Initial Nessus Vulnerability scan utilizing Client PC or server infrastructure
- Black Box network penetration test of up to 20 internal IPs and 3 external IPs utilizing manual scripts, Metasploit and other custom penetration testing tools
- Specialised vulnerability identification for up to 3 servers showing critical missing patches, vulnerable services, directory indexing, improper error, exception management, and information leaks.
- Cursory test of workstations based on common builds for up to 3 samplings

✓ Website

- BurpSuite, manual scripts, and custom penetration testing tools on up to 1 website

ADVANCED PACKAGE

✓ Internal and External Network

- All services included in the standard package for up to 50 internal IPs, 10 external IPs, and 10 servers

✓ Website

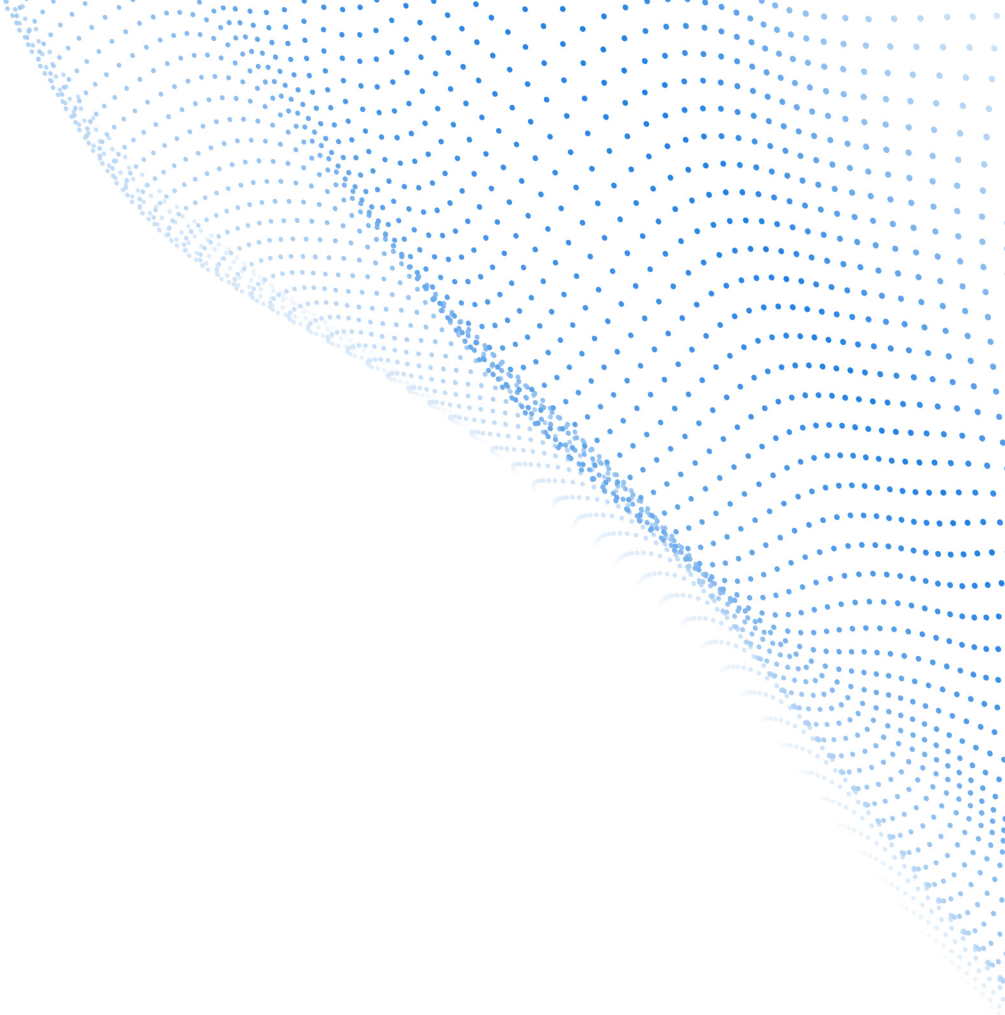
- All services included in the standard package for up to 2 websites

✓ External Web Application

- Black Box testing of the external web application
- Application can have up to 1 Login System, 4 API Inputs, 4 Functions, and 4 Roles.
- Utilisation of BurpSuite, manual scripts, and custom testing tools
- No code review included

*Testing will be limited based on access provided by the client. GMI prefers jump box access for remote access.

To get started, visit **cowbell.ai** or email **crs@cowbell.ai**.



cowbell®

RESILIENCY SERVICES CRS

Cowbell Inc., D/B/A Cowbell Resiliency Services ("CRS") does not in any way engage in, is not licensed to engage in and does otherwise take part in the sale, solicitation and/or negotiation of insurance. CRS only engages in the distribution of resiliency and/or similar security services. As such, the resiliency and other security services described herein are only being offered by and through CRS.