CGI

Enhancing cyber security through comprehensive penetration testing

Our approach:

Our penetration testing approach combines a thorough, quality service with the flexibility to assess a wide range of IT systems. We integrate elements from respected standards such as the OSSTMM and OWASP, alongside industry best practices and the MITRE ATT&CK framework, ensuring a robust evaluation of security controls and capabilities.

Overview of Puple Team engagement:

In a Purple Team engagement, we utilise attack trees to provide clients with both offensive (Red Team) and defensive (Blue Team) consultancy. A technical lead oversees both teams, ensuring controlled execution of attack trees and effective reconciliation between Red and Blue Teams.

Red Team assessment:

Typically, our Red Team assessments simulate full-scope attacks or controlled scenario-based approaches. The objective is to test existing security measures by mimicking malicious user actions, gaining unauthorised access, and exploiting vulnerabilities. Our approach prioritises circumventing security measures and achieving engagement objectives without being detected.

Blue Team support:

During Red Team activities, our Blue Team specialists support the in-house Security Operations Centre (SOC), helping detect intrusion attempts. Periodic meetings between Red and Blue Teams provide detailed information on various stages of engagement, helping to gauge its status and fine-tune intrusion detection systems.

Advanced Threat Intelligence (ATI) support:

We can provide our ATI team using advanced toolkits to spot Advanced Persistent Threats (APTs) during engagements.

Objectives of Purple Team engagement:

Demonstrate achievability or un-achievability of objectives within the allocated time.

- Analyse a specialised simulated attack in real time.
- Provide clear, tailored recommendations for vulnerability mitigation.
- Assist clients in understanding the security posture of their infrastructure.

Scenario-based approach:

In contrast to attack simulations, a scenario-based approach involves creating malicious actions executed by a test team in coordination with the Blue Team. This iterative process aims to fine-tune attack methods and detection capabilities.

Reporting and recommendations:

Within ten working days of the engagement's conclusion, a comprehensive report is provided, outlining attack methods and detailed recommendations. This includes improvements to existing tooling, adjustments for tuning, deployment of additional tooling, updates to processes and procedures, and training recommendations for defensive staff and incident response governance.

Compliance and ethical testing:

All testing is conducted within the legal framework, adhering to acts such as the Computer Misuse Act, Data Protection Act, and European Convention of Human Rights. Permission is obtained from system owners and data owners before testing IT systems.

For further details on how our penetration testing services can benefit your organisation, please contact our cyber security team.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit: cgi.com/uk/cyber-security

Email: cyber.enquiry.uk@cgi.com