

Cyber Security Testing Service

“ABeam understands the need to be agile, introduce new systems, and ways of working to be competitive. By using our cyber security testing services at regular intervals, our clients will stay one step ahead of potential attackers, enabling their IT systems to grow with their business, without lowering the defenses of the enterprise.”

THE BEST DEFENSE IS GOOD OFFENSE

Organizations depend on business and IT systems to operate effectively and competitively in this digital age. These systems are frequently updated because of the fact that even a small change can introduce new vulnerabilities to the firms. Security Testing helps to detect, analyze and help organizations make informed decisions about how to fix inevitable vulnerabilities and misconfigurations.

WHAT MAKES US DIFFERENT

Apart from providing deep technical cyber security testing by certified team members, ABeam also includes business impact and priorities into the testing result which help provide insight to executive management. Moreover, ABeam not only provides short term technical recommendations but also provides the strategic action plan to remove the root causes of weakness. This will help prevent the same issues from reappear in the future.

A WEALTH OF TESTING SCENARIOS

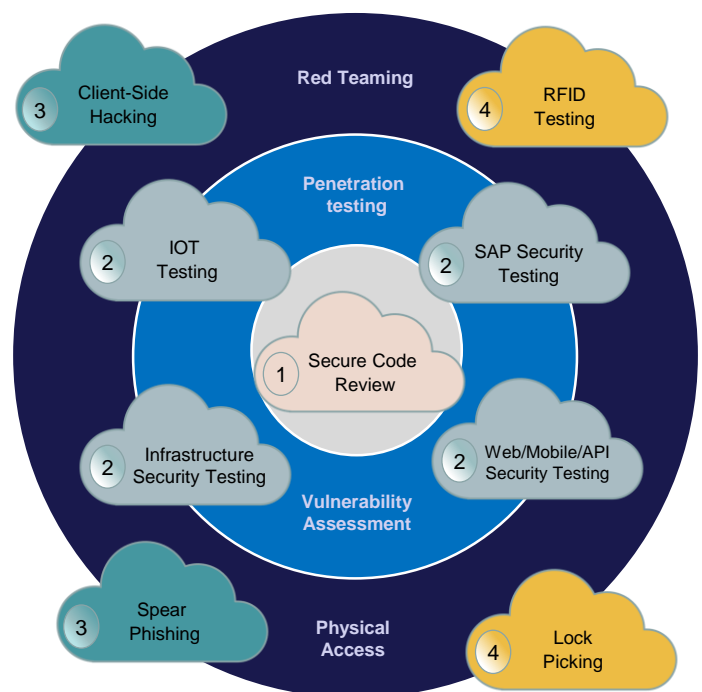
1. Secure Code Review: used for highlight possible vulnerabilities within “static” (non-running) source code.

2. Grey and black box testing: Through defined methodologies which cover the attack paths taken by real-world hackers, we can perform infrastructure, web and mobile application penetration testing across all technology types

3. Social engineering: We can simulate scenarios such as e-mailing Trojans to specific e-mail accounts to investigate whether perimeter references can be breached via such mechanisms and persistent backdoor access planted in your organization.

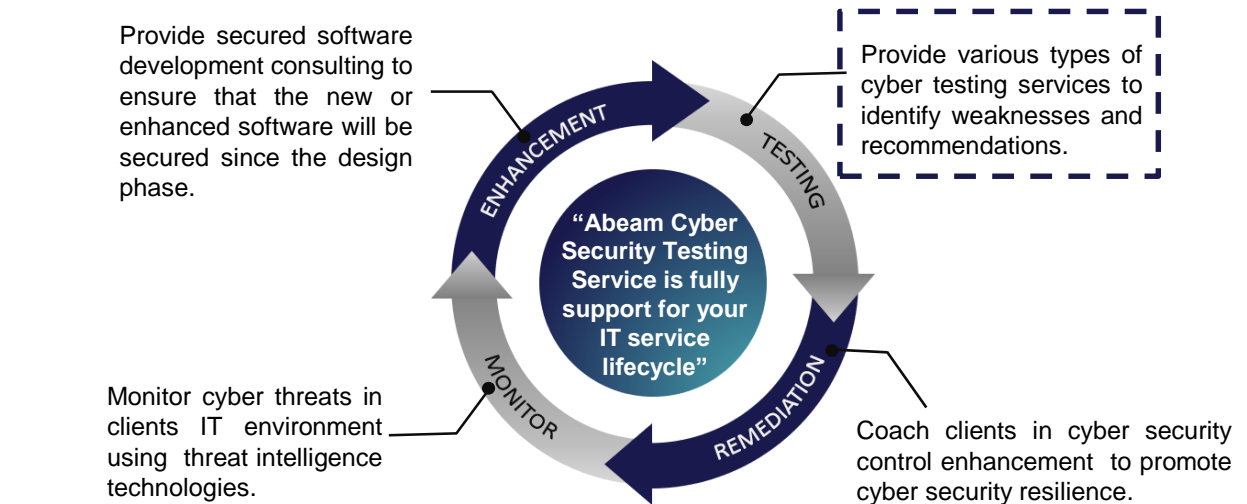
4. Physical access testing : Many organizations rely on the physical security of their building to a greater extent than their firewalls, yet do not test the physical security controls in place.

To provide complete cyber security testing service, ABeam tailors varieties of testing scenarios to suit with client conditions.



CYBER SECURITY STARTS WITH THE EYES

Among various cyber security activities, ABeam recommends clients to start with cyber security testing. This will help client to understand their risks and rapidly mitigate associated vulnerabilities to promote cyber security resilience of the IT services.



| | Project Preparation | Execution of Fieldwork | Follow-up |
|----------------|--|---|---|
| Key Activities | <ul style="list-style-type: none">Confirm project's objectives and scope including responsibilities.Get written permission for testing.Conduct business logics and understanding session.Address concerns and practices for safe testing on production environment.Conduct Kick-off meeting. | <ul style="list-style-type: none">Perform business logic test.Perform vulnerability identification and exploit testing.Develop recommendation for the remediation activities.Translate technical impact to business language and provide strategic improvement approach.Develop and present draft of penetration testing report. | <ul style="list-style-type: none">Perform reassessment for the reported findings.Document follow-up status and Develop final report. |
| Deliverables | <ul style="list-style-type: none">Details plan | <ul style="list-style-type: none">Draft security testing report | <ul style="list-style-type: none">Final Security testing report |

WE DELIVER CLEAR AND ACTIONABLE RESULTS

Our service is based on the most popular industry-recognized penetration test and security assessment methodologies, frameworks and standards, including Open Web Application Security Project (OWASP) Testing Guide v4, U.S. National Institute of Standards and Technology (NIST), Special Publications series and Public source security Advisories, whitepapers and articles.

- Effort put into presented findings in a clear and actionable hand-written report of findings;
- Includes a concise executive summary;
- Summary of findings shows:
 - priority of each significant vulnerability;
 - possible remediation actions;
 - direct links to relevant bulletins, patches and advisories.
- Detailed results are presented in clear language;
- Findings are grouped by Risk level.



For more information about our Cybersecurity Professional Services, contact your ABeam representative or visit <https://www.abeam.com/th/en>