“Leading with inspiration and courage, obsessed with future possibility and in a love affair with change. Our mission to manage with greatness and untamed strength, improving everything daily “

DIASPORA
INSPIRING TECHNOLOGY

315, Jalan SS9/2
Plaza Seri Setia
47300 Petaling Jaya, Selangor
Tel: +603 7877 9033
Fax: +603 7877 7722
www.diaspora-tech.com

DIASPORA
INSPIRING TECHNOLOGY

Security Posture Assessment

consulting
sales
staffing
support

Security Posture Assessment Services

CONNECTING YOUR BUSINESS TO THE TECHNOLOGY RESOURCES YOU NEED

Our security assessment strategy and approaches based on globally entrusted OPST (OSSTM Professional Security Tester) program and ISO/IEC 27001:2013 standard guideline. We will address client security assessment requirements through a professional services engagement with highly qualified security consultants and engineers leveraging on the world-renowned security certifications. In a nutshell, there are several services that will be provided by **Diaspora Sdn Bhd** in this SPA services such as:

1. Network Architecture Security Assessment
2. Host and Appliance Configuration Security Assessment
3. Application and Database Security Testing
4. Internal and External Penetration Testing
5. Wireless Testing
6. Physical Security Assessment
7. Social Engineering
8. Transfer of Technology / Transfer of Knowledge Session

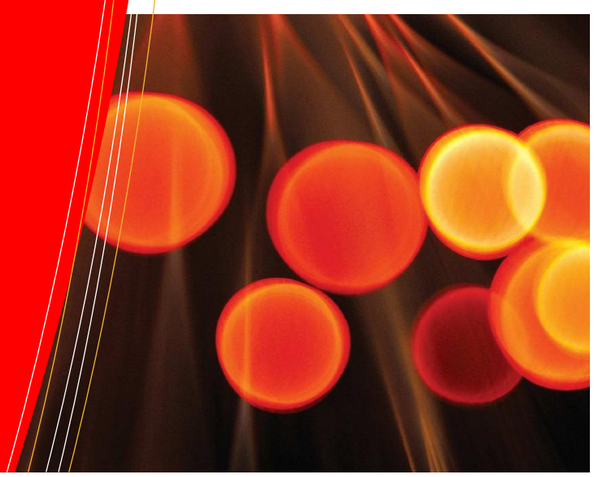
flexible solutions for your business needs

TECHNOLOGY CONSULTING PROVIDES A TOTAL END TO END SOLUTION.

1. Network Architecture Security Assessment

We will perform activity such as;

* Maps current network infrastructure implementation against document architecture
* Review network security parameter configuration and setup such firewall, Intrusion Prevention/Detection System, Load Balancer, VPN Gateway.
* Review network equipment configuration and setup such as router and switch.
* Review VLAN setup and configuration
* Scan selected one user VLAN segment for any malicious activity and configuration.
* Spoof selected VLAN segment to monitor traffic in the network.



2. Security Assessment on Server/Host Operating Systems

Regardless of the operating system we will assess the server to identify level of the security setting and vulnerability exist into the server locally. Meaning our consultant should have Administrative login privilege to access the server.

* Operating System latest patch update (Hotfix, Kernel or package update)
* Local security policy configuration
* Basic Services running and install in the server
* Third party application installed and patches update.
* High risk security setting on the registry.
* Local Log Policy
* Access Control Policy for User in the System
* File access control

4. Internal and External Penetration Testing

We are following Open-Source Security Testing Methodology Manual (OSSTMM) as our guideline in performing our penetration testing activity. For every success penetration test a proof of concept snapshots will be provided as reference. DSB will propose a suitable best practice to counter measure for identified vulnerability in order to mitigate the issue.

3. Security Assessment on Web-Application and Database

Based on Gartner Group finding, 70 percent of attacks against a company's website or web application come from the 'Application Layer'. It shows that web application has become favorite loop hole for the hackers. We will analyses vulnerability for Web application base on Open Web Application Security Project (OWASP) standard best practice which includes of:

* SQL Injection
* Cross-Site Scripting (XSS)
* Broken Authentication and Session Management
* Insecure Direct Object References
* Cross-Site Request Forgery (CSRF)
* Security Misconfiguration
* Insecure Cryptographic Storage
* Failure to Restrict URL Access
* Insufficient Transport Layer Protection
* Invalidated Redirects and Forwards

5. ICT Security Physical Assessment

Security assessment normally been ignored by organization, this normally is the weakest link in Information security management. Area of coverage is inclusive of:

* Data center / Server room / Floor switch physical environment such as air conditioner, cabling, UPS, server rack and lock.
* Monitoring method of physical access to secure area.
* Media handling policy such as backup and disposable of media.
* Firefighting technology to secure secured area.

6. Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information. Diaspora provides both remote and onsite social engineering services. Tests include social engineering attacks by physical and technical approaches. The goal is to determine if controls are in place to prevent unauthorized disclosure of information.

7. Wireless Testing

In this activity client will be "Wireless technology such as 802.11 as become increasingly cheaper and easier to implement. Because of this security is easily forgotten about with these devices. Surveys in the past that have revealed that 60% of wireless networks are wide-open. A wide-open wireless network can allow anyone with just a laptop and wireless card to access your resources network. Securing your wireless network devices will make sure that only authorized persons are using your resources, and accessing your information.

8. Transfer of Knowledge

In this activity client will be thought the methodology of vulnerability assessment and penetration testing. It starts from fingerprinting, enumeration, scanning and penetration. Participant will be exposed to the tools use during SPA activity. Step by step approach will be share with participant for better understanding and exposure.