



E-SPIN

Web Application Security Solution

Acunetix Web Vulnerability Scanner



Copyrighted

Copyright (c) 2005 - 2011 by E-SPIN Sdn. Bhd. All rights reserved.

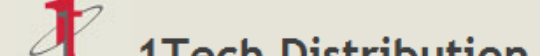
No part of this solution/product/training presentation/handout may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without either the prior written permission of E-SPIN, or authorization through payment of the appropriate per-copy fee to E-SPIN, tel (603) 7728 2866, fax (603) 7725 4757, or on the web at www.e-spincorp.com

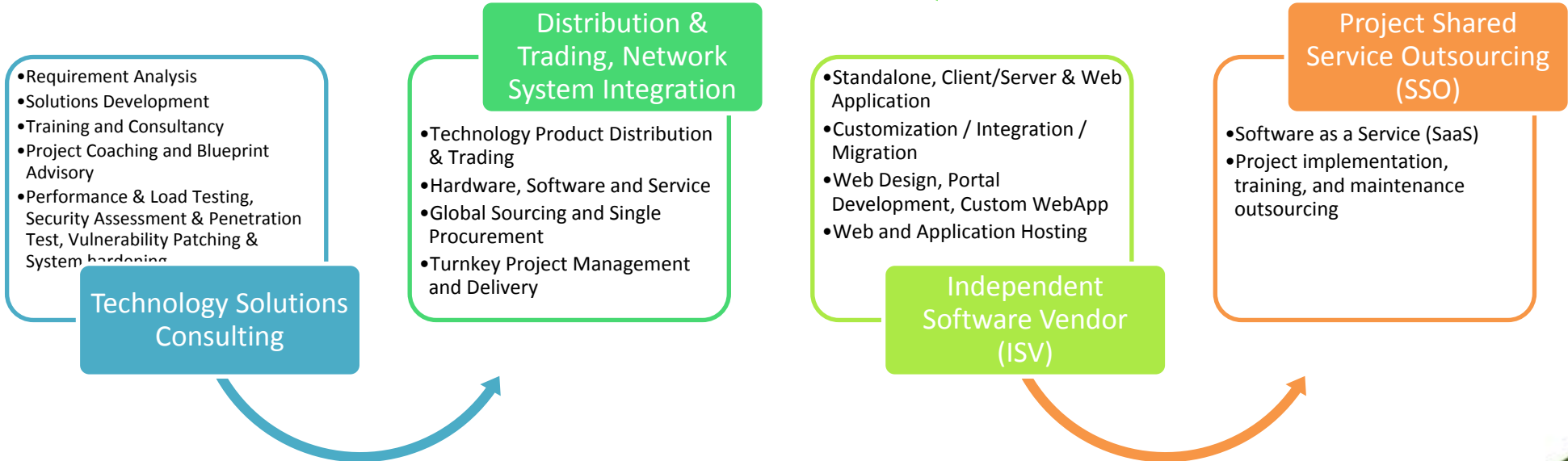
Limit of Liability / Disclaimer of Warranty: While the author have used their best efforts in preparing this solution/product/training presentation/handout, they make no representations or warranties with respect to the accuracy or completeness of the contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for any situation. You should consult with a professional where appropriate. Neither the author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our customer service department at (603) 7728 2866, fax (603) 7725 4757, or email info@e-spincorp.com.



E-SPIN Group Profile

- Enterprise Solutions Professional on Information and Network (E-SPIN)
- E-SPIN Sdn Bhd (Enterprise Technology Solution)
- **E-SPIN OUTSOURCING** (Project Outsourcing/ISV)
-  (International Technology Distribution)





E-SPIN Business Domain B.A.S.E.

Enterprise Solutions Portfolio

Business and Technology Applications

- Business Process and Workflow Automation
- Sales Force Automation and Customer Relationship Management (CRM)
- Business Intelligence, Data Warehousing and Performance Management System (PMS)
- Datacenter Global Integration, Server Consolidation and Infrastructure Virtualization
- WAN / Web Application Acceleration and Bandwidth Optimization, Open Source Application and Initiative
- Media and Broadcasting Technologies and Automation
- Network Management System (NMS), Network/System/App Monitoring, Alerting, Reporting
- Helpdesk and Remote Support; Computer lab and classroom training management

Availability, Storage and Business Continuity

- Data integrity, anti-hacking/ web defacement and availability assurance
- Data backup, storage archiving, replication, mirroring
- Continuous Data Protection (CDP) and Online Storage Protection
- Network, System and Data High Availability, Continuous Availability
- Business continuity and disaster recovery (BCDR)
- External storage, Network Attached Storage (NAS) and Storage Area Network (SAN)
- Internet link load, bandwidth aggregation, application traffic server load balancing
- Non-Stop mission critical system hardware and network infrastructure
- High availability, system/network hardware and software clustering, auto failover and redundancy
- High Availability, Continuous Availability Network, System and Data
- Windows Event and Syslog Consolidation Log Management and Storage

Security, Risk and Compliance Management

- Network & Wireless Security, Firewall / VPN, IPS, ID Mgt, Network Access Control (NAC)
- Vulnerability Management, Security Assessment, Penetration Testing (Web/Application/Network/Database/ Patch Mgt & Security Hardening, Security Event Management (SEM), Incident Correlation Analysis and Reporting System; wired and wireless TCP/IP traffic analysis; Exploitation
- Content Security, Employee PC Activity Monitoring, Virus, Spyware, Phishing, Web, E-mail, IM, P2P Blocking and Filtering, Endpoint Security and Port Management, Data Theft Prevention
- Data Encryption, Code, Files, E-mail, Database, Folders, Virtual Disk, Full Disk Encryption; Digital Steganography, Watermarking and Digital Fingerprinting; Secure Data Erasure and Destruction
- Digital Signature and Signing, Multi Factor Authentication, Managed, Automated, Secure File Transfer (SFTP) and Application Tunnelling, Secure Document Exchange and Storage
- IT Governance, Risk Management, and Regulatory Compliance

End-to-End Complete One-Stop Solutions

- Technology consulting, requirement assessment and solution development
- Ongoing education, training and development (in-house or on-site)
- Solution sourcing, integration, migration, project implementation, main / sub contracting and maintenance support
- Independent Software Application development, integration and customization (standalone, client/server, web application)
- E-Business and Web Solutions, web design, portal development, e-commerce, web / domain / email / application hosting service
- Project information technology share service and outsourcing (SSO)



Clients Overview (Domestic & International)





How WVS can help?

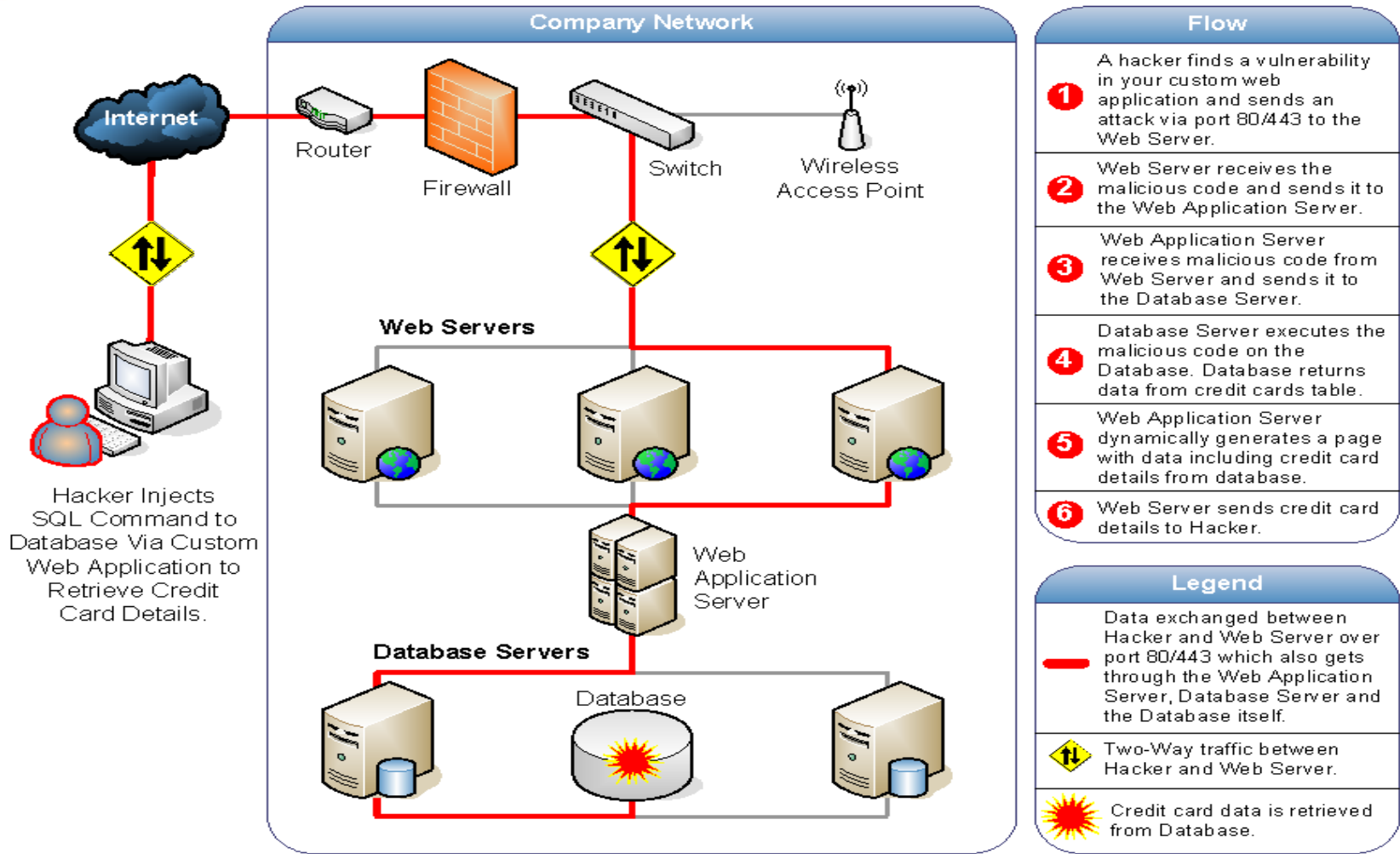
- Known static methods:
 - Specific Web Applications known exploits
 - Directory enumeration
 - Known Web Server exploits
 - Known Web technology exploits (e.g. php vulnerabilities)
 - Known network services exploits (e.g. DNS, FTP, SMTP)
- Unknown dynamic methods:
 - SQL Injection
 - Cross-site Scripting
 - Directory and Link Traversal
 - File Inclusion
 - Source Code Disclosure
 - Code Execution
 - Common File Checks
 - Parameter Manipulation
 - Arbitrary file creation or deletion
 - CRLF Injection
 - Path Truncation
 - Java Applet reverse engineering
 - Session Hijacking
 - Authentication Attacks
 - Google Hacking Database

Acunetix WVS searches for all of the above hacking methods and much more.



E-SPIN Web Application Security Solution

How Does Hacking Work?





Who use it for webapp VA audit/QA



US Army

Bank of China

The Pentagon

IBM Denmark

University of Reading

Panasonic Asia Pacific

The armed forces of Norway

Wescom Credit Union

ActionAid UK

US Air Force

Fujitsu

Adidas Group

France Telecom

PricewaterhouseCoopers

Lonely Planet

State of North Carolina

California department of Justice

and many more...





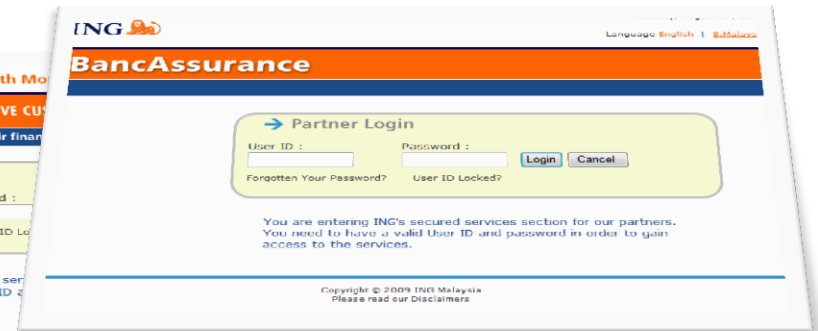
Show Case – ING Group’s all Custom Web application portals



ING Portal



ING Employee Benefits Corporate Client



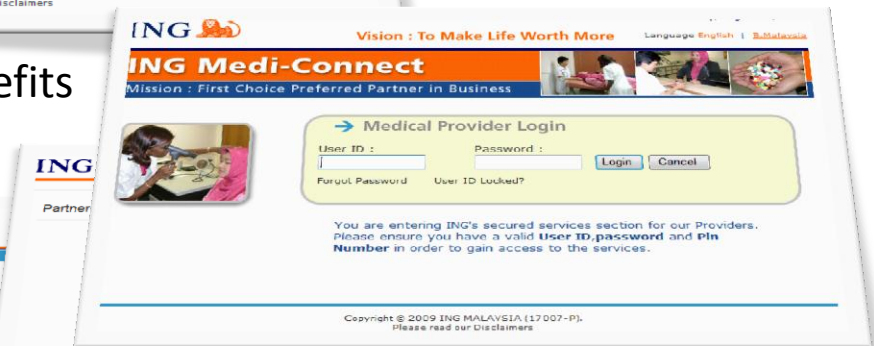
ING Banca Network



ING@My Services



ING Agency Network



ING Medi-Connect

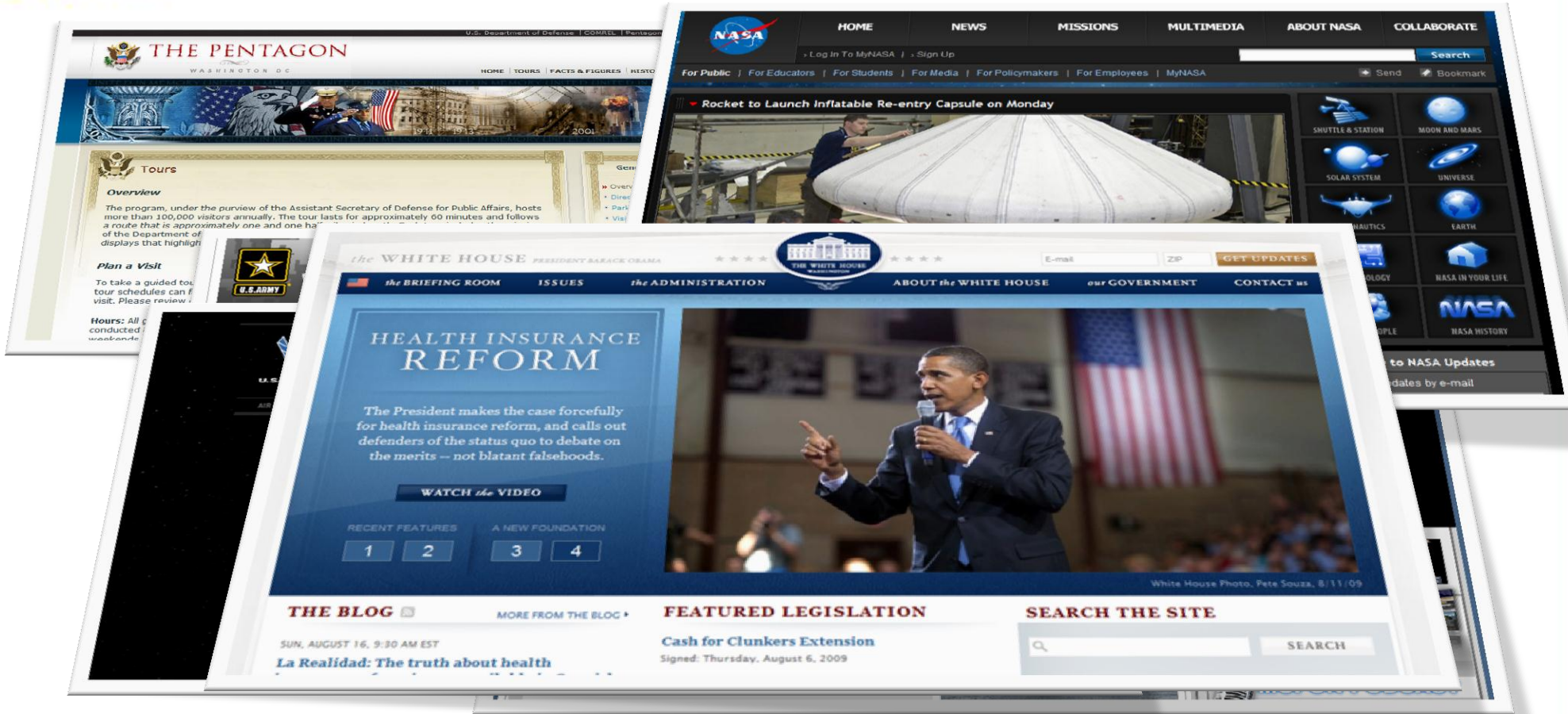


ING Business Partner





Protected World Most Attacked Site, Portals, Web Applications



U.S. Department of Defense | COMRL | Pentagon.gov

THE PENTAGON

WASHINGTON DC

HOME TOURS FACTS & FIGURES HISTORY

Tours

Overview

The program, under the purview of the Assistant Secretary of Defense for Public Affairs, hosts more than 100,000 visitors annually. The tour lasts for approximately 60 minutes and follows a route that is approximately one and one half miles long. The tour includes a visit to the Department of Defense's main displays that highlight the history of the Department of Defense.

Plan a Visit

To take a guided tour, you must check the tour schedules on the website. Please review the tour schedule for more information.

Hours: All tours are conducted on weekdays.

U.S. ARMY

NASA

HOME NEWS MISSIONS MULTIMEDIA ABOUT NASA COLLABORATE

Log In To MyNASA | Sign Up

Search

For Public | For Educators | For Students | For Media | For Policymakers | For Employees | MyNASA

Send | Bookmark

Rocket to Launch Inflatable Re-entry Capsule on Monday

SHUTTLE & STATION | MOON AND MARS | SOLAR SYSTEM | UNIVERSE | AERONAUTICS | EARTH | NASA IN YOUR LIFE | NASA HISTORY

to NASA Updates | Updates by e-mail

the WHITE HOUSE PRESIDENT BARACK OBAMA

the BRIEFING ROOM ISSUES the ADMINISTRATION ABOUT the WHITE HOUSE our GOVERNMENT CONTACT us

HEALTH INSURANCE REFORM

The President makes the case forcefully for health insurance reform, and calls out defenders of the status quo to debate on the merits -- not blatant falsehoods.

WATCH the VIDEO

RECENT FEATURES A NEW FOUNDATION

1 2 3 4

White House Photo, Pete Souza, 8/11/09

THE BLOG MORE FROM THE BLOG

SUN, AUGUST 16, 9:30 AM EST

La Realidad: The truth about health

FEATURED LEGISLATION

Cash for Clunkers Extension

Signed: Thursday, August 6, 2009

SEARCH THE SITE

SEARCH



Show Case – Government/ Government Agencies



Malaysia Anti Corruption Commission (MACC)

University Malaya



Unique Benefit(s)

Operation

Automated

Manual, Advanced

Custom Reporting

Custom
Vulnerability Tag
and Test

Coverage

Web Server

Database Server

Application Server

Feature(s)

Web/web svcs scan

Site Crawler

Reporter

Vulnerability editor

Customization option

advanced penetration testing

HTTP editor

HTTP sniffer

HTTP Fuzzer

Blind SQL Injector

Authentication Tester

Target Finder

Compare Result

Command Line Support

AcuSensor Technology



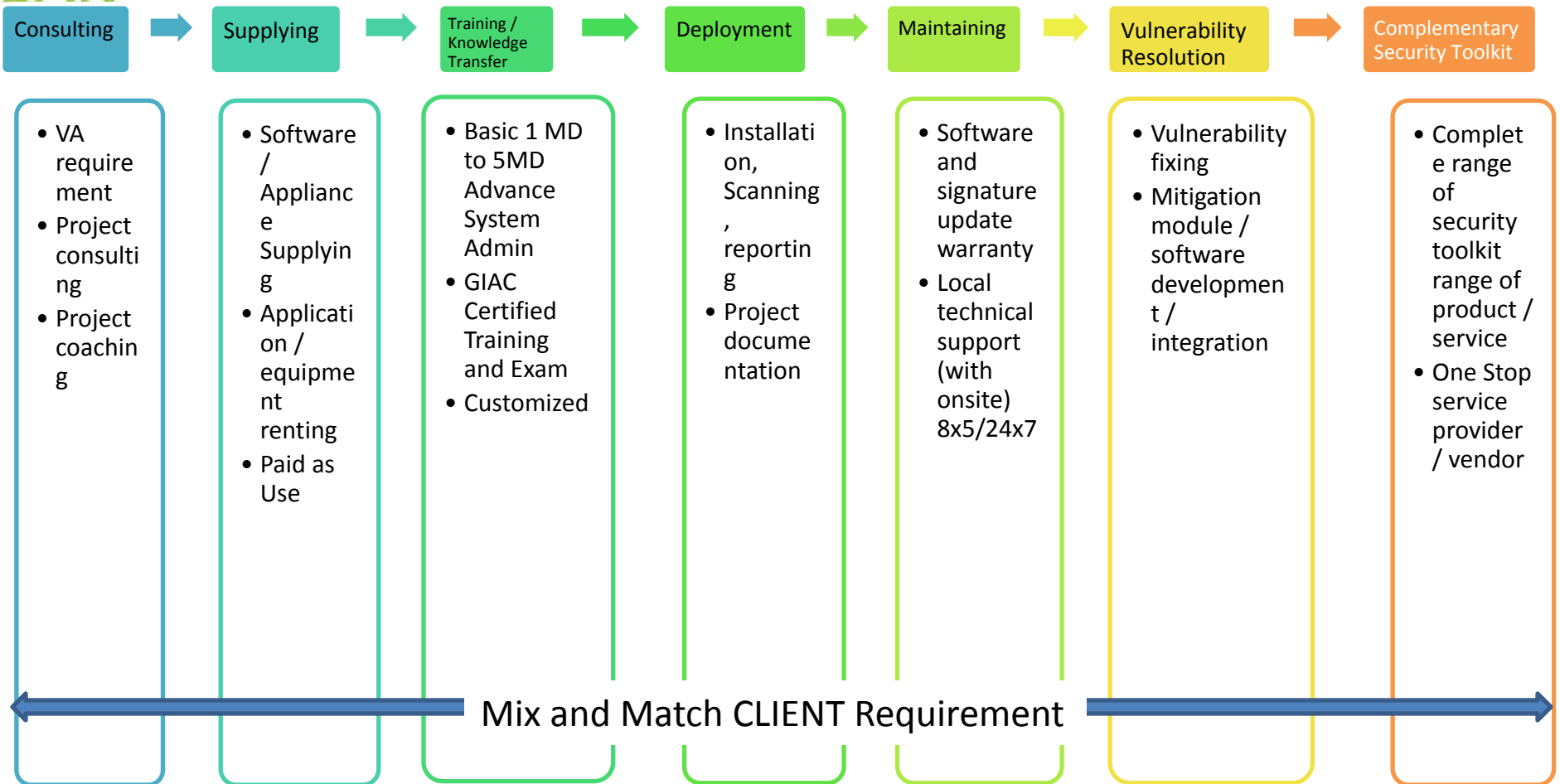
E-SPIN

Unique Benefit(s)

Quick Video Demo



E-SPIN WVS Complete Solution Unique Value Proposition





Transfer of Technology Option

Skill Nature	Transfer Group	Extent of Skill	How it is transferred
Technology Training	<ul style="list-style-type: none"> • Technical Staff • End user technical group 	<ul style="list-style-type: none"> • Basic Web / Application Security Training 	<ul style="list-style-type: none"> • Formal Courses – 1 Day Basic System Administration Training
Application Training	<ul style="list-style-type: none"> • Security Assurance Analyst / Security Admin • End user 	<ul style="list-style-type: none"> • Operation of the application 	<ul style="list-style-type: none"> • Formal Courses – 5 Day Advanced hand on system administration training
Independent and Global Certified Training and Exam	Training for In house domain expert/consultant	Independent and Global recognize GIAC complete range of training and testing	Subscribe for E-SPIN GIAC certified training + certified testing
Project Consulting and Coaching	<ul style="list-style-type: none"> • Real job in hand joint exercise to transfer real skill set by “learned” it first hand 	<ul style="list-style-type: none"> • first hand experience on carry out real job and duties from scanning, configuration, reporting, interpretation, to vulnerability fixing and mitigation solution framework, to really execute vulnerability fixing / mitigation module development, fix production vulnerability 	<ul style="list-style-type: none"> • Participating in the real job in hand, learn by doing and observe how it is performing Subscribe for consulting service with vulnerability fixing outsourcing for 30 Man Day
Initial exposure and management awareness of the web / application security operation	<ul style="list-style-type: none"> • Technical Support • End user operations personnel • Department Manager • End user operations manager 	<ul style="list-style-type: none"> • Exposure and knowledge in web / application security operation in real-life environment 	<ul style="list-style-type: none"> • Visit sites in Europe



E-SPIN



Vulnerability Management, Security Assessment, Penetration Testing Solution



Solution Complete Portfolio



Application and Web Application Security

- Web Server
- Web Application Server
- Database Server
- Google Hacking
- Cross Site Scripting
- SQL Injection
- Dynamic Source Code Analysis
- Black box hacking
- White box hacking
- Database Security
- Source Code Dynamic and Static Analysis



Exploitation Framework, Development, Library

- Offensive Exploit
- Exploit Research, Development, Testing
- Remote Trojan
- Exploit Library Addon for Network, System, Application, Database, VoIP Security Exploit



Hostile Source Code Reverse Engineering / Malware and Remote Trojan

- Industry de factor hostile decompiler / disassembler to unlock protected binary program into source code
- Remote trojan, keylogger for pc, server activity monitoring include screenshot



Wireless Security Assessment, Penetration Testing

- Wireless Network and Security Audit, Penetration Testing
- Offensive Hacking, then report on the wireless security posture



Network, Server, System Vulnerability Assessment

- Vulnerability Assessment (VA)
- Network Audit
- Server Audit
- System Audit
- Application Audit



Network, Server, System, Application Log Review

- Network Equipment
- Server (Win & Non-Win)
- System & Workstation
- Application Log
- Log Consolidation, Review, Report and Audit

End to End Professional Service

Warranty, Update, Maintenance Support
•8x5xNBD | 24x7



















Consulting, Coaching
•Project Consulting, Coaching, Implementation

Training, Transfer of Technologies
•Certified | Product Specific

Vulnerability Fixing, Mitigation Module Development
•Development Outsourcing



Solution Complete Portfolio

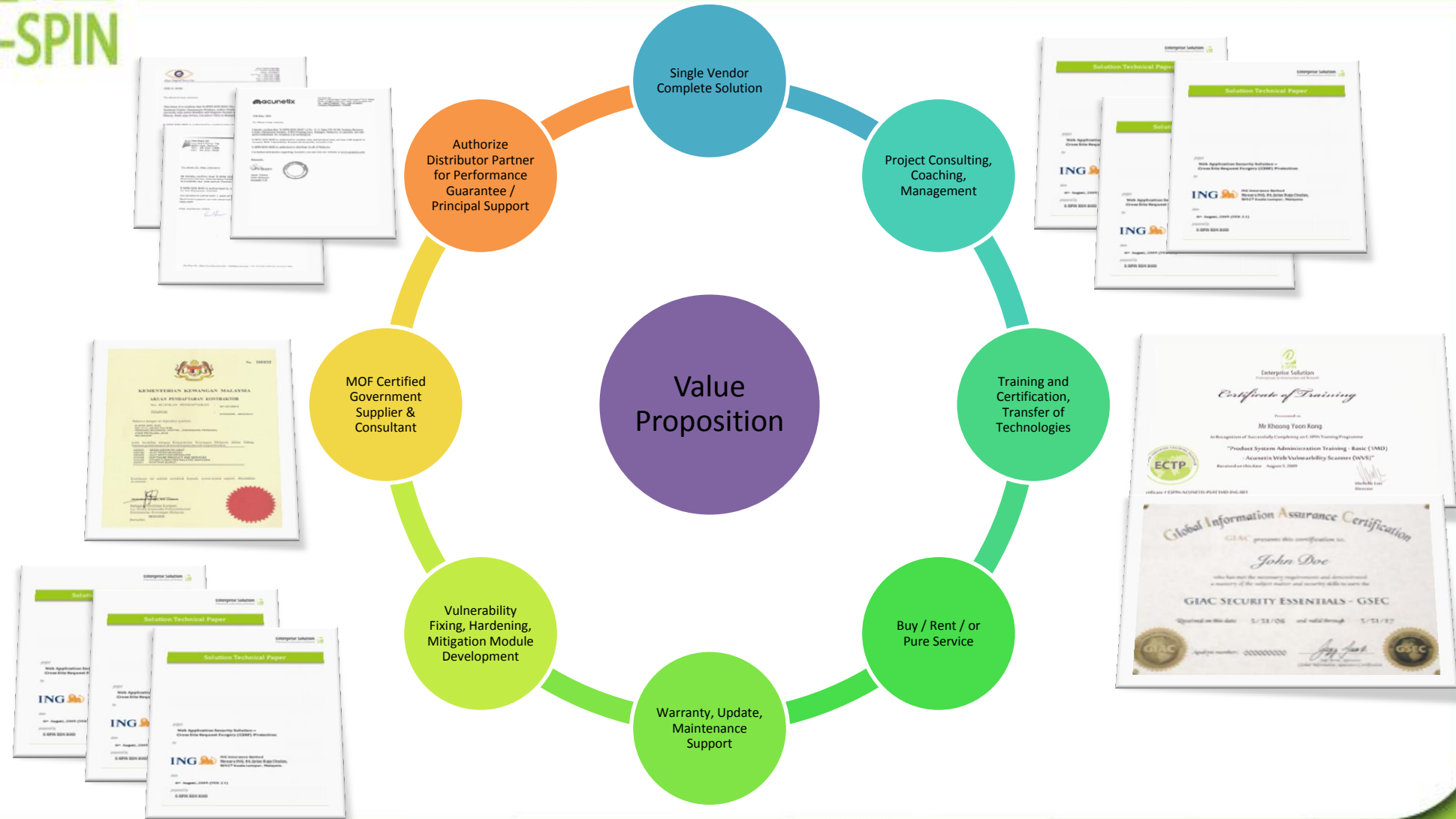
<p>Application, DB, Source Code and Web Application Security</p>  	<p>Exploitation Framework, Development, Library</p>     	<p>Hostile Source Code Reverse Engineering</p>   	<p>Wireless Security Assessment, Penetration Testing</p>   	<p>Network, Server, System Vulnerability Assessment</p>   	<p>Network, Server, System, Application Log Review</p>  
--	---	---	--	---	--

End to End Professional Service

<p>Warranty, Update, Maintenance Support •8x5xNBD 24x7</p>	<p>Consulting, Coaching •Project Consulting, Coaching, Implementation</p>	<p>Training, Transfer of Technologies •Certified Product Specific</p>	<p>Vulnerability Fixing, Mitigation Module Development •Development Outsourcing</p>
--	---	---	---

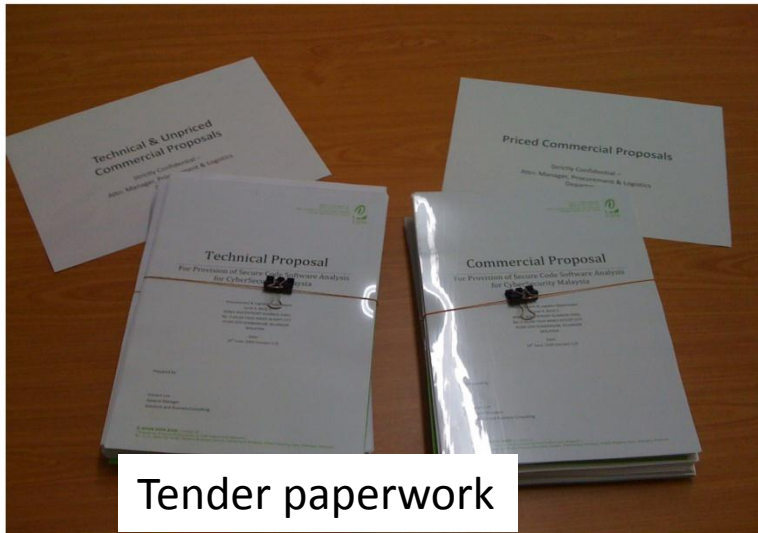


Why Do Business with E-SPIN?

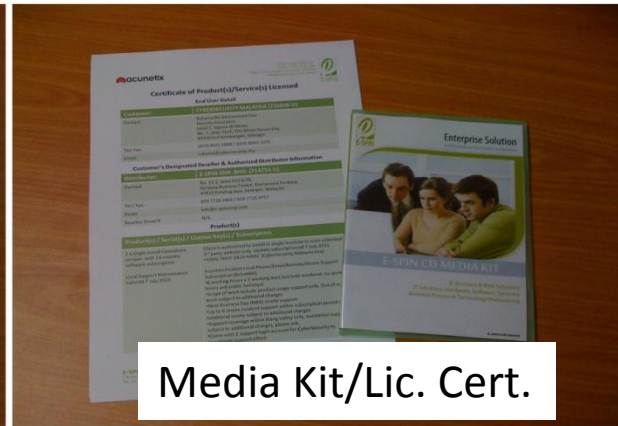




Value Added Service(s)



Tender paperwork



Media Kit/Lic. Cert.



Training Cert.



Agreement



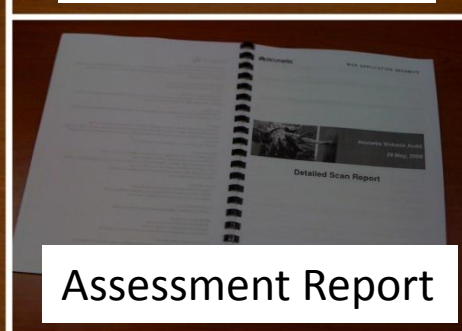
Technical Proposal



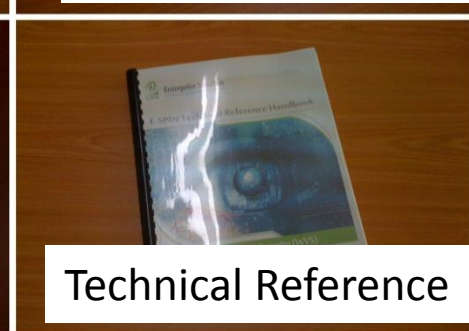
Training Handout



Vulnerability Fixing



Assessment Report



Technical Reference



Propose Business and Service arrangement with Client/Partner

Distribution
& Trading

Equip. &
App. Renting

Service
Outsourcing

Certified /
Training

Project
Independent
Consultant /
Sub Con





Consultancy, Training, Certification and Support



System
Deployment



Development /
Customization



Technology
Consultancy



Special Project
Custom Training



Certification /
Exam



Coaching /
Solution
Architect



Onsite Advanced
Training



Offsite Technical
Training



E-SPIN

Thank You & Open Discussion



Vulnerability Management, Security Assessment, Penetration Testing Solution

E-SPIN Value Added Services

Professional Qualification | Skill Certification

Product In Depth Training

Vulnerability Fixing | Mitigation Module Development

System Hardening | Patching

Project Consulting | Solutions Development

Local Technical Support (phone | email | remote | onsite)

Single Sourcing Hardware | Software | Service

Security Assessment Outsourcing | Subcontracting

Extended Security Assessment

Penetration Testing

Intrusion Analysis

Incident handling

System Admin.

Security Mgmt.

Security Audit

Secure Development

Forensics Analysis

Core Security Assessment

Web App (Web, App, Db. Server).

Network /Server & System

Database In Depth

Packet / Wireless/ Log

Malware Analysis/ Reverse Engineering

Exploitation Testing & Research



Case SPRM

(3rd Party /Independent Network/Application/Database/Server Security Audit)

E-SPIN Customer Case Study SPRM (MACC)

Network, System and Application internal and External Penetration Testing, Security Assessment, Vulnerability Management, Training, Maintenance Support

Background Information
Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) SPRM (or Malaysia Anti Corruption Commission MACC) is Malaysia Anti Corruption authority operate multi branches and multi site nation wide operation.

Solutions Benefits

- Immediate cost saving by capable to automate intranet and portal application security and vulnerability scanning, auditing, penetration testing, reporting to free up importance manpower to focus on interpreting, enforcing and implementing the vulnerability fixes and patches before hackers exploits.
- Outsourced penetration tests, system supply, training and maintenance for E-SPIN to leverage E-SPIN core competences build up internal staff strengths on penetration testing, security assessment, and vulnerabilities management.

Solution Overview
The packaged solution include 2 times pre- and post penetration testing (with reports) for each of the applications, supply the systems with installation, training and maintenance support.

Solution Architecture
Single package solution run in three (3) phases that design and develop to address client business IT and operation requirements and deliver better technologies, process, people skillset, knowledge and ability, full empowering support service from consulting, coaching, product system administration training and maintenance support.

© E-SPIN SDN BHD ALL RIGHT RESERVED

- Engaged E-SPIN to deliver 3rd party in depth network/application/database/server security audit
- Line of Business Anti Corruption System (KRIS) within Network
- Public Facing Portal and Web Application (sprm.gov.my)
- Report on the vulnerability and security posture
- Recommendation of the vulnerability fixing / mitigation
- Supply the system with three (3) years maintenance contract
- Class of 5 man days system administration training for 1 class (10 pax)



Case PizzaHut (3rd Party /Independent Network/Application/Database/Server Security Audit)

Web Anti Defacement and Auto Recovery, External Penetration Testing Solution Show Case



Pizzahut Malaysia invested in E-SPIN's Anti Defacement and Penetration Testing to protect E-Commerce Applications.

Background Information

Pizzahut Restaurant is an established global pizza fast food chain store. Malaysia operation is implementing e-commerce web application for online tracking and delivery system. Client is concern on hacking and defacement attack and require anti defacement and auto recovery system for non-stop protection and external penetration testing and advisory service to understand overall security posture against hacking.

Solution Overview

The proposed solution consist of anti defacement and auto recovery system deliver non-stop protection against defacement and hacking attack on the server application, Internet and web application security penetration test and firewall audit, security consulting service.

Solution Architecture

The proposed solution consists of international grade anti defacement and auto recovery system against unauthorized change in the portal content and application scripts. It will monitor the protect content in 24x7 non-stop manner for any defacement and content hacking attempts. Regardless of whatever attack attempt, it will roll back into original content. It is scalable system solutions can cater for multi server and one-to-many content update and publishing workflow environment. The packaged inclusive of software licensing, installation and software annual email / phone / onsite maintenance support subscription service.

External penetration test and firewall audit is use to provide 3rd party objective factual data and information gather. The deliverable include the report, interpretation of the report founding, and advisory on next step action to enhance overall security posture on the client Internet and web security operation.

Solution Benefits

- Immediate achieve the non-stop 24x7 protection against website portal, web application files and data unauthorized change. It offloading system administrator to perform more critical knowledge work and let the system perform routine monitoring and recovery.
- Firewall and Network Security can not prevent web application hacking and defacement due to port 80 (web) and port 443 (https) is always open for access.
- The solution complementing existing network security by lockdown original content against unauthorized changes.
- Prevent against corporate reputation damage and risk due to successful hacking and defacement incident and post damage lost.
- External penetration and firewall test let the client have the overall understanding on own security posture and determine what to do next.

© E-SPIN Sdn Bhd All Right Reserved

- Engaged E-SPIN to deliver 3rd party in depth network/application/database/server security audit
- Line of Business Pizza Online Order Credit Card / Ebusiness Facility
- Public Facing Portal and Web Application
- Report on the vulnerability and security posture
- Recommendation of the vulnerability fixing / mitigation
- Supply the Anti Defacement system with maintenance contract



Case Hong Leong Network/Server Security, Assets Inventory & Patch Management)

Network Vulnerability Scanning, Patch Management & Software Auditing Solution Show Case

HLA Implement E-SPIN's Network Vulnerability Scanning, Patching and Auditing solution on network server and client.

Background Information
Hong Leong Assurance Bhd is part of Hong Leong Group business. It business in General Insurance and Life Insurance.

Previously their IT Security unit is using open source and experimental tool for network vulnerability scanning, patch management, and software auditing for the vulnerability assessment and reporting purpose. It is highly inefficient and ineffective due to intensive manual operation required. All the party involved take note that it is much better to implement automate and integrate network vulnerability scanner, patch manager and software auditing software for the operation to generate standard and consistent report that is easy to compare across the time period and prevent human error being in the scan, patch and audit process.

Solution Overview
Proposed solution include integrated Network Security Scanner that provide network vulnerability scanning, patch management and software auditing functionality required and subscribed for ongoing software update subscription and local product phone and email support service as a total solution package.

Solution Architecture
The proposed solution was use to check client network for possible security vulnerabilities by scanning client entire network for missing security patches, service packs, open shares, open ports, unused user accounts and more. With this information (displayed in customizable graphical report), client used to easily lock down network against hackers.

It also use to manually deploy missing service packs and patches and custom / 3rd party software and patches in application and OS network-wide and perform patch auto-download and patch rollback. Furthermore, it was use to perform network and software auditing and management reporting and compliance purpose.

Solution Benefits

- * Replace manual and open source network security vulnerability scanner, and replace with scanner that capable to not just scanning and report vulnerabilities, and capable to deploy patches on demand and conduct software auditing for the internal auditing operation.
- * Network security scanning, patching and auditing process automation. The propose solution allow automate and schedule scanning to save administrators significant of the time by automate routine security scanning, patching and auditing operation with minimal human intervention.
- * Deliver security benefits. It provides up-to-date vulnerabilities database, patch and service pack in single solution.

© E-SPIN SDN BHD ALL RIGHT RESERVED

- Engaged E-SPIN to deliver network/server security assessment system, incorporate assets inventory and patch management functionality
- Perform internal network audit, assessment
- Report on the vulnerability and security posture
- Recommendation of the vulnerability fixing / mitigation
- Supply the system with the ongoing system update and maintenance contract



Case ING Insurance

Web/Application/Database/Network/Server Security' Vulnerability Fixing, Training & Maintenance)

E-SPIN customer case study ING Insurance

Web Application Security and Vulnerability Scanning, Audit and Reporting, Process Integration and Automation, Training and Knowledge Transfer, Risk Mitigation Fixing Module Development, Operation Consulting, Project Coaching, Software and Technical Support.

ING
Your future. Made easier™

Background Information
ING Insurance is the worldwide financial and insurance multinational corporation (MNC) operates globally. In Malaysia it operates various insurance, financial and investment services.

Due to business IT quality assurance and process improvement initiative, client seek for end to end web application software quality control and assurance solution that capable to automate and integrate into their existing workflow process and minimize exploitable vulnerabilities before hackers does.

Solution Overview
Proposed solution include leading web sites and web application security and vulnerability scanning, auditing and reporting system licenses for unlimited internal IP scanning and reporting, software warranty and ongoing vulnerability signature update subscription, project deployment, product system administration training and knowledge transfer, operation consulting, project coaching, process integration and automation, local technical support and maintenance subscription as single package solution to resolve current technology, risk compliance and process improvement challenges.

Solution Architecture
Single package solution that design and develop to address client business IT and operation requirements and deliver better technologies, process, policy and procedures, people skillset, knowledge and ability, full empowering support services from consulting, coaching, custom built risk mitigation and fixing module software development, product system administration training and knowledge transfer, to process integration and automation.

Solution Benefits

- Immediate cost saving by capable to automate website web application security and vulnerability scanning, auditing and reporting to free up importance manpower to focus on interpreting, enforcing and implementing the vulnerability fixes and patches before hackers exploits it and bringing tangible damage against client reputation.
- Existing business IT and software development process integration and automation to streamline web application testing and debugging cycle to ensure less vulnerable, hackable and secure web application roll out to the production.
- Ensure always access to latest software version and technology in the fraction of the total software ownership cost to enjoy latest features and functionality, ongoing update on vulnerability signature and patterns.
- Perform mission critical and sensitive internal web application security test and ongoing check, report and distribute vulnerabilities to be fix and get it done without 3rd party involvement and use it to validate 3rd party web application penetration test report.

- Engaged E-SPIN to deliver web/application/database/network/server security assessment system, incorporate into ebusiness Software Development Life Cycle (SDLC) for Quality Assurance, Product Security Audit
- Outsourced vulnerability fixing and mitigation module development
- Training and project live system coaching
- Supply the system with the ongoing system update and maintenance contract



E-SPIN Threat and Vulnerability Management Solutions

Threat Analysis

Intrusion Monitoring

Malware Detection

Content Filtering

Classify threat based on probability and potential damage

Vulnerability Identification

Compliance Testing

Vulnerability Scanning

Operations Availability Analysis

Uncovering weaknesses before they can be exploited

Vulnerability Management

Baseline Development

Incident Response Team

Asset Inventory and Classification

Event Correlation

Reporting

Developing and maintaining an on-going process

Remediation

Asset and Patch Management

Classification of Threats

Incident Response

Isolating and resolving asset security issues once identified