



ACCESS  
INNOVATION  
GROWTH



# AIS Online Tools

Sophia Chen

Manager, Account Information Security

Singapore

August 18, 2005

- Vulnerability Scanning – what is it?
- Scanning Technology Overview
- Step-by-Step Simplified AIS Validation
- Account Management

# What is Vulnerability Scanning?



## ■ Vulnerability scanning

- Automated, remote tool to identify network flaws that be exploited by hackers to gain access to confidential data

## ■ How it works

- Scans via the internet network to test for known vulnerabilities e.g. Microsoft and Lunix published vulnerabilities
- User logs on to ScanAlert Portal to receive report and information to assist in patching flaws

## ■ What is the benefit

- Cheaply, efficiently and regularly identifies security holes hackers may exploit
- Often finds holes IT staff overlook or are not aware of

# Why is regular scanning so important?



- 5 Top Reasons for Account Compromise
  - Ineffective patch management
  - No security scanning
  - Weak network level security
  - SQL injection
  - Lack of real-time security monitoring

**Almost every account compromise could have been prevented if vulnerability scanning had been conducted regularly**

# Visa's online validation tools



## Why?

- To assist Acquirers to easily and efficiently validate their agents compliance
- Provide audit trail and agent track status
- Take advantage of Visa's economies of scale
- Use of experienced specialist scanning providers

## Who?

- ScanAlert ([www.scanalert.com](http://www.scanalert.com))

## When?

- From August 2005

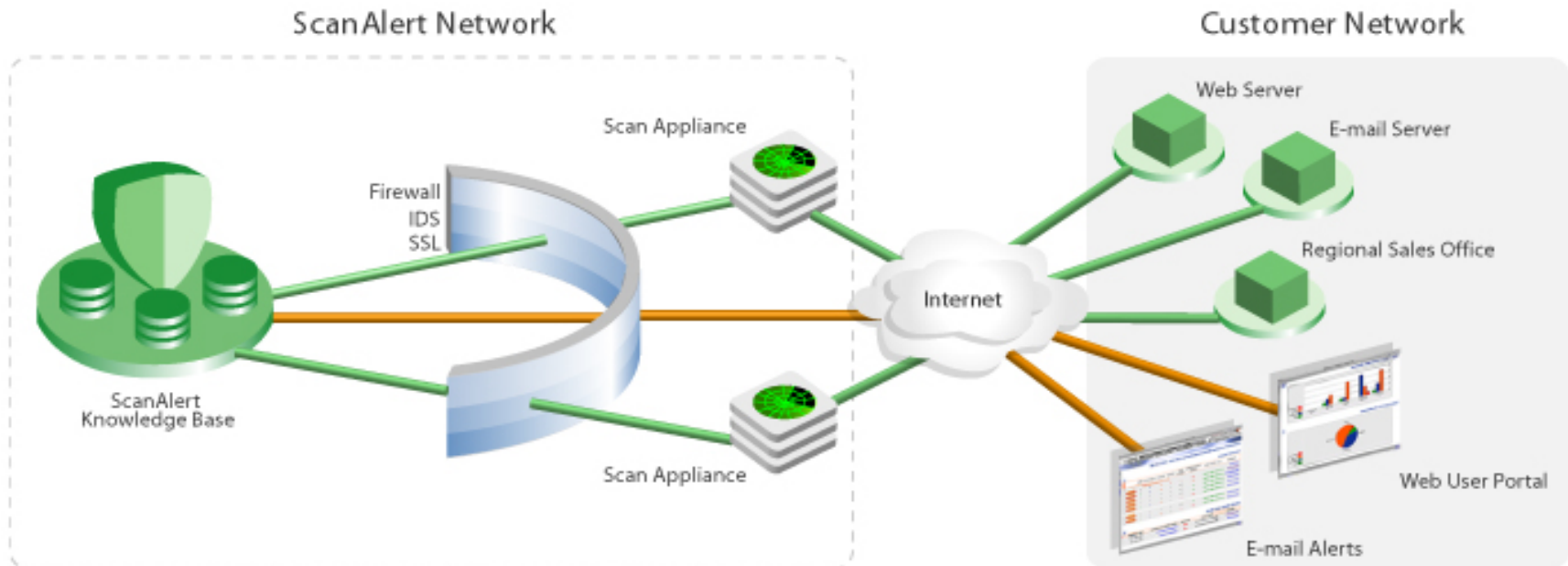
# ScanAlert's Credentials



- Headquartered in California, USA. Asia Pacific offices in Taipei and Sydney
- Over 65,000 websites are protected by ScanAlert
- Vulnerability scanning technology meets FBI/SANS security test and accredited by ALL card schemes
- ScanAlerts customers in Asia and USA



# Technology Overview



- **Vulnerability Knowledge Base** – updated every 15 min
- **Web Portal and Alert System** – extensive management features
- **Security** – Data center with biometric access & 7/24 onsite security
- **Scanning Support** – unlimited email + business hours phone
- **Multi-Lingual Portal** – English and Chinese

# Key Features



- Non-disruptive and non-invasive scanning
- Follows links embedded in Flash Files on Merchant Site
- Tests for ALL types of SQL Injection vulnerabilities
- Automatically test for Default Password (admin)
- Avoids false positives due to unexpected error page content
- Rate limits scans for low server load
- Caches all requests and results to avoid duplicate requests
- Does not perform dangerous tests that could crash services

<http://www.scanalert.com>

# 3 Steps for AIS Validation



## ■ Step 1 – Self Assessment Questionnaire (SAQ)

- Pre-populated based on answers to wizard
- Displays percentage of pass/fail answers
- Provides sample PCI compliant Security Policy
- Assists in appointment of Data Security Officer
- Form can be saved at any point of time and continue

## ■ Step 2 – Scanning

- Device enrollment
- Scan authorization and launch of scans
- Patching vulnerabilities, rescanning if necessary

## ■ Step 3 – Receive Validation Reports

- SAQ
- Vulnerability scan

Address http://www.scanalert.com

# ScanAlert™

.. CUSTOMER LOGIN .. English

Making the web HACKER SAFE®

We make websites safe from hackers and certify it to their customers

FIND HACKER SAFE SITES

THE SAK

ScanAlert™ HACKER SAFE TESTED 14-AUG

PCI COMPLIANCE CTSP / AIS / SDR

Over 65,000 Web sites use HACKER SAFE® certification to help protect you from identity theft and credit card fraud.

Wouldn't you rather shop at a HACKER SAFE site?

View demo to learn more . . .

**VISA** Visa Asia Pacific AIS validation service

[Click here to sign-up for PCI certification service](#)

- SHOPPERS
- MERCHANTS
- GOVERNMENTS & NON-PROFITS
- PROFESSIONAL SERVICES
- PARTNERS
- TECHNOLOGY
- COMPANY

Copyright 2005 ScanAlert, Inc - HACKER SAFE®    Call 877.302.9965    Terms Of Service    Privacy Policy    Company Info

# Easy Three Step Validation Process



Security Management Console

VISA

Security Account Tools PCI HACKER SAFE Help Logout

[1 Self-Assessment](#) [2 Security Scanning](#) [3 Certificate of Compliance](#)

**Welcome to Visa Asia Pacific's AIS/PCI Compliance Service**

Visa Asia Pacific requires all entities that process, transmit or store credit card data on a network connected in any way to the Internet to be certified to meet the AIS standard within the framework of the Payment Card Industry (PCI) Data Security Standard.

To meet these AIS requirements, you must complete both the annual PCI Self-Assessment Questionnaire (SAQ) and pass quarterly security scanning of your web site(s) and office or store Internet connection(s).

There are three basic steps to validate AIS compliance:

1. Completing and passing the annual security self-assessment questionnaire
2. Completing and passing quarterly security scans of your Internet infrastructure
3. Obtaining a Validation Report

# Step 1: Self Assessment Questionnaire (SAQ)

## Implement Strong Access Control Measures

### Requirement 9: Restrict physical access to cardholder data

	DESCRIPTION	RESPONSE		
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	Yes	No	
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?	Yes	No	N/A
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	Yes	No	
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	Yes	No	
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	Yes	No	
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	Yes	No	
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	Yes	No	

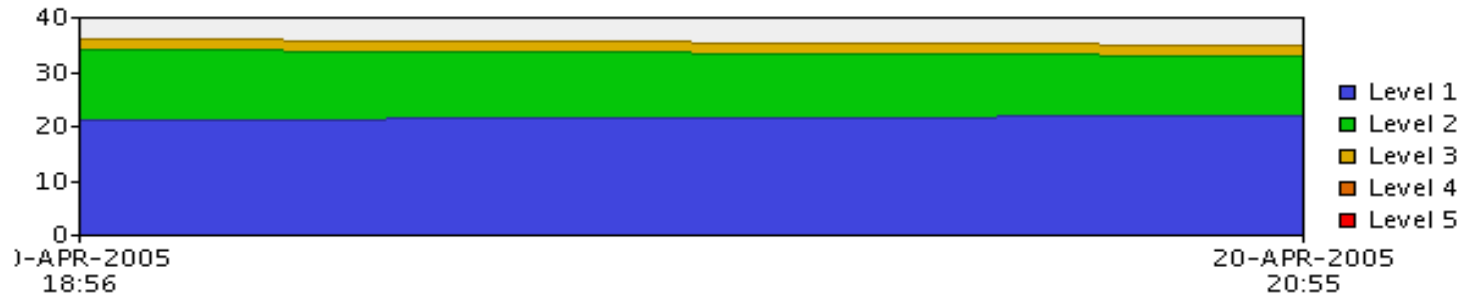
# Step 2: Security Scanning (report)



[Overview](#) [Vulnerabilities](#) [Web site](#) [History](#) [Edit](#)

## Recent Audits

Vulnerabilities Per Audit



[Audit Now](#)

## Open Ports

Port	Protocol	Typical Service	Service
1	tcp	tcpmux	tcpmux
21	tcp	ftp	220 You will be disconnected after 15 minutes of inactivity.
22	tcp	ssh	SSH-1.99-OpenSSH_3.6.1p2
25	tcp	smtp	220-husky.switchfusion.net ESMTP Exim 4.43 #1 Wed, 20 Apr 2005 21:14:12 -0500
53	tcp	domain	domain
53	udp	domain	ISC BIND 9.2.2
80	tcp	http	Apache/1.3.33 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.3.9 FrontPag

# Step 2: Scanning Report



## Report Overview

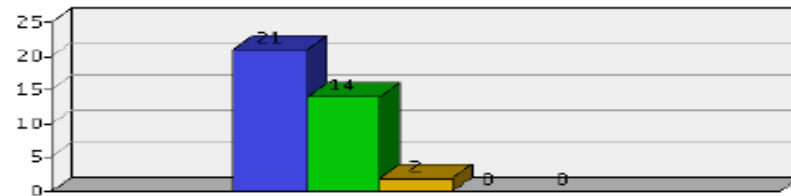
Customer Name	Visa Asia Pacific
Date Generated	20-APR-2005 19:25
Report Type	Security - By Device
Devices	1
Device Groups	0
Vulnerabilities	23

## Report Contents

- Vulnerabilities By Severity
- Vulnerabilities By Category
- Device Overview
- Services Detected
- All Vulnerabilities Found
- Device Detail
- Appendix

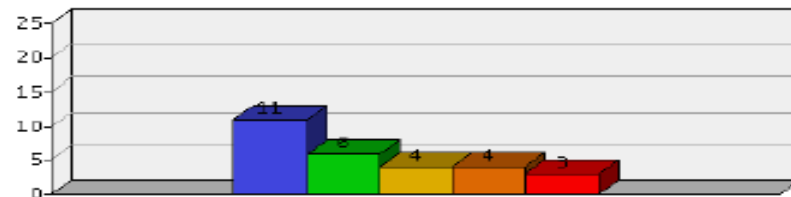
## Vulnerabilities By Severity

Severity	Count
5 Urgent	0
4 Critical	0
3 High	2
2 Medium	14
1 Low	21



## Vulnerabilities By Category (Top 5)

Category	Count
11 Web Server	11
6 Email	6
4 Apache	4
4 Other	4
3 Remote System Management	3



# Members' Reporting Portal



- Provides validation and compliance status of merchants and IPSPs – SAQ and scan
- Merchant or IPSP details
- Last Scan Date: accounts whose scans are more than 3 months past current date are highlighted
- Pass / Fail result
- SAQ date: the last date form was completely answered
- SAQ percentage: percentage of correct answers

- ScanAlert's Scanning Technology Overview
  - Acts as “Super Hacker” to find security holes
  - Safely scans over 65,000 web sites each day
  - Non-invasive and non-disruptive
- Step-by-Step Simplified AIS Validation
  - Self-Assessment “Wizard” simplifies form completion
  - Extensive online support tools
  - Help desk and email support if required
- Account Management
  - Easy portfolio risk management with online reports

**VISA**

