

# Vulnerability Assessments, Penetration Studies, eDiscovery – Not All The Same

## Core Competencies – C21

**Miguel (Mike) O. Villegas**

CISA, CISSP, GSEC, CEH, PCI QSA, PA-QSA, ASV

Vice President- K3DES LLC

October 14, 2014



# Abstract

We all may have seen and performed vulnerability scanning tools, penetration studies and e-discovery scans but possibly not all three. This session will discuss the difference in nature and use of each. They each have a distinct purpose and are used for security monitoring and compliance. However, they each have their limitations. Another area for discussion is which product solution to implement. There are commercial and open-source solutions that can satisfy a company's needs.

We will discuss how to import, align, and score assets from each type vulnerability scanning tools using a common, shared repository (Log Manager) and triage scoring methodology. We will also discuss workflow and remediations of identified and prioritized vulnerabilities.

The products presented in this session are for informational purposes only and does not reflect an endorsement or recommendation on the part of the presenter. Attendees are advised to perform their own due diligence in selecting the right solution for their institutions.

# Table of Contents

- ❖ [Security Monitoring](#)
- ❖ [Vulnerability Scanners](#)
- ❖ [Penetration Tests](#)
- ❖ [eDiscovery Scanners](#)
- ❖ [Workflow Management](#)
- ❖ [Continuous Monitoring Options](#)

### btn BANK TECHNOLOGY NEWS

## Banks Sue Security Vendor Trustwave After Target Data Breach

by DAVID HEUN

MAR 25, 2014 6:06pm ET

PRINT

EMAIL

REPRINTS

COMMENT

TWITTER

LINKEDIN

The complaint alleges the vulnerabilities in the Target system were "either undetected or ignored by Trustwave," allowing hackers access to millions of card account and personal records.

The suit estimates that the banks will spend about \$172 million reissuing credit and debit cards. Their total losses, including fraudulent charges, could hit \$18 billion, according to the lawsuit.

Plaintiffs Trustmark National Bank and Green Bank N.A. seek class-action status and damages of more



Why Banks Are Failing to Attract Tech Talent

“Target did not face a basic attack. They faced a carefully planned attack which was executed in a very calculated manner. The attack was designed to evade basic controls.

“Target was using advanced techniques which successfully identified hostile activity in their network.”

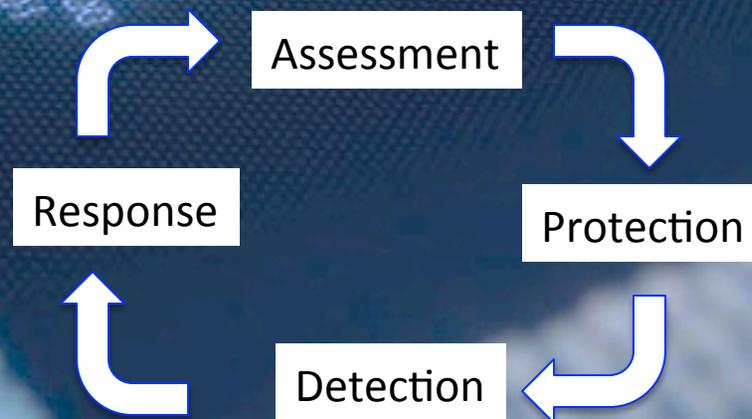
“By Target’s own admission, this was a failure in fully using available security capabilities and controls; without the operational security foundation in place, Target was unprepared to act when presented with advanced information.”

**NTT Group**  
**2014 Global Threat Intelligence Report**

# Information Security

Information Security is the process of maintaining an acceptable level of perceived risk. There are no “silver bullets” to guarantee absolute security but it remains a goal worthy of our attention.

This process revolves around four steps:<sup>1</sup>



<sup>1</sup> *The Tao of Network Security Monitoring*

# Assessment

**Assessment** is preparation for the other three components. It deals with:

- ❖ Policies
- ❖ Procedures
- ❖ Laws
- ❖ Regulations
- ❖ Budgeting
- ❖ Technical evaluation of a company's security posture.

All of these **MUST** be based on perceived (or AKA residual) risk.

<sup>1</sup> *The Tao of Network Security Monitoring*

# Protection

**Protection** is the application of countermeasures to reduce the likelihood of compromise. Another word for this would be *Prevention*.

Protection measures should ALWAYS be based on RISK.

Risk is dependent on:

- ❖ Laws and regulations
- ❖ Value of Asset
- ❖ Cost of Recovery
- ❖ Likelihood of Incidents
- ❖ Reputation Impact
- ❖ Business Impact

<sup>1</sup> *The Tao of Network Security Monitoring*



*Really?*

# Detection

**Detection** is the process of identifying intrusions.

- ❖ **Intrusions** are the policy violations or computer incidents.
- ❖ **Event** is any action that involves a computer system or network.
- ❖ **Incident** is any unlawful, unauthorized, or unacceptable action that involves a computer system or network.

<sup>1</sup> *The Tao of Network Security Monitoring*

# Response

**Response** is the process of validating the fruits of detection and taking steps to remediate intrusions.

Response activities include:

- ❖ Patching
- ❖ Proceeding
- ❖ Pursuing
- ❖ Prosecute

The first two are focused on restoring to original state prior to incident. The latter two are to take legal action against the perpetrator.

<sup>1</sup> *The Tao of Network Security Monitoring*

# PCI DSS 12 Requirements

## Build and Maintain a Secure Network

- ❖ *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
- ❖ *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

## Protect Cardholder Data

- ❖ *Requirement 3:* Protect stored cardholder data
- ❖ *Requirement 4:* Encrypt transmission of cardholder data across open, public networks

## Maintain a Vulnerability Management Program

- ❖ *Requirement 5:* Use and regularly update anti-virus software
- ❖ *Requirement 6:* Develop and maintain secure systems and applications

## Implement Strong Access Control Measures

- ❖ *Requirement 7:* Restrict access to cardholder data by business need-to-know
- ❖ *Requirement 8:* Assign a unique ID to each person with computer access
- ❖ *Requirement 9:* Restrict physical access to cardholder data

## Regularly Monitor and Test Networks

- ❖ *Requirement 10:* Track and monitor all access to network resources and cardholder data
- ❖ *Requirement 11:* Regularly test security systems and processes

## Maintain an Information Security Policy

- ❖ *Requirement 12:* Maintain a policy that addresses information security

# Security Monitoring (PCI) v2.0

Vulnerability Scans	<b>11.2</b> Run internal and external network vulnerability scans at least quarterly and after any significant change in the network
Penetration Tests	<b>11.3</b> Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification
Web Application Vulnerability Scan	<b>6.6</b> For public-facing web applications, ... either... <ul style="list-style-type: none"><li>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes, OR</li></ul> <b>Note:</b> <i>This assessment is not the same as the vulnerability scans performed for Requirement 11.2.</i> <ul style="list-style-type: none"><li>• ... a web-application firewall...</li></ul>
Discovery	<b>3.2</b> Do not store sensitive authentication data after authorization (even if encrypted).

# Security Monitoring (PCI) v3.0

Vulnerability Scans	<b>11.2</b> Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
Penetration Tests	<b>11.3.1</b> Perform <i>external</i> penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
Web Application Vulnerability Scan	<b>6.6</b> For public-facing web applications, ... either... <ul style="list-style-type: none"><li>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes, OR</li></ul> <b>Note:</b> <i>This assessment is not the same as the vulnerability scans performed for Requirement 11.2.</i> <ul style="list-style-type: none"><li>•... a web-application firewall...</li></ul>
Discovery	<b>3.2</b> Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

# Security Monitoring

- ❖ Collection
- ❖ Analysis
- ❖ Alerting
- ❖ Escalation

For incidents to detect and respond to intrusions, Intrusion Detection Systems (IDS or IPS) systems provide this level of monitoring. IDS/IPS systems can be at the network level or at the host level (HIDS/HIPS).

But IDS's are reactionary in nature. We need to detect before it happens.

<sup>1</sup> *The Tao of Network Security Monitoring*

# Common Types of Network Attacks

- ❖ **Eavesdropping** - the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic.
- ❖ **Data Modification** - An attacker can modify the data in the packet without the knowledge of the sender or receiver.
- ❖ **Identity Spoofing (IP Address Spoofing)** - An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data.
- ❖ **Password-Based Attacks** - This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

# Common Types of Network Attacks

- ❖ **Denial-of-Service Attack** - prevents normal use of your computer or network by valid users.
- ❖ **Man-in-the-Middle Attack** - attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection
- ❖ **Compromised-Key Attack** - attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack
- ❖ **Sniffer Attack** - application or device to read, monitor, and capture network data exchanges and read network packets.
- ❖ **Application-Layer Attack** - targets application servers by deliberately causing a fault in a server's operating system or applications.

# DDoS

- ❖ Distributed Denial of Service (DDoS) is a denial of service originating from many different source hosts.
- ❖ Historically, there are four different DDoS programs:
  - ❖ Trinoo
  - ❖ Tribe Flood Network (TFN)
  - ❖ TNF2K
  - ❖ Stacheldraht (German for barbed wire)
- ❖ In a DDoS attack, many different “hostile” hosts enlist and direct their attack to a target site.
- ❖ Extremely difficult to trace to a source.
- ❖ Stopping DDoS depends greatly on the updated configuration of firewall and gateway equipment
- ❖ They steal large amounts of bandwidth and crash systems with outside connections

31%

Distributed Denial of Service (DDoS) attacks accounted for 31% of incident response engagements.

NTT Group  
2014 Global Threat Intelligence Report

# Vulnerability Scanning

Scanning Event	Description
Host Discovery	TCP and UDP probes are sent to default ports for common services on each host, such as DNS, TELNET, SMTP, HTTP and SNMP. At least one response, the host is considered "alive."
Port Scanning	All open TCP and UDP ports on target host, configurable.
OS Detection	OS installed through TCP/IP stack fingerprinting, OS fingerprinting on redirected ports
Service Discovery	Uses several discovery methods to identify which service is running on the port
Authentication	Optional, ensure that each host on the network is in compliance with internal security policies
Vulnerability Assessment	Vulnerability tests that are applicable to each target host based on the information gathered for the host



## Common Vulnerabilities and Exposures

*The Standard for Information Security Vulnerability Names*

**New CVE-ID Format as of January 1, 2014 — [learn more](#)**

TOTAL CVEs: [60536](#)

HOME > CVE LIST

### About CVE

Terminology

Documents

FAQs

### CVE List

CVE-ID Syntax Change

About CVE Identifiers

Search CVE

Search NVD

Updates & RSS Feeds

Request a CVE-ID

### CVE In Use

CVE-Compatible Products

NVD for CVE Fix  
Information

CVE Numbering Authorities

### News & Events

Calendar

Free Newsletter

### Community

CVE Editorial Board

## CVE List Main Page

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

**IMPORTANT:** [CVE-ID Syntax Change](#) took effect on January 1, 2014.

### National Vulnerability Database

Full database functionality for the CVE List is provided through MITRE's partnership with the U.S. [National Vulnerability Database \(NVD\)](#).

- [CVE Search on NVD](#)
- [CVE Fix Information](#)
- [CVE SCAP Mappings](#)

### CVE List Master Copy

The master copy of the CVE List is maintained for the community by MITRE on this public CVE Web site.

- [Search Master Copy of CVE](#)
- [Download CVE List](#)
- [View CVE List](#)

You may download the CVE List, copy it, redistribute it, reference it, and analyze it, provided you **do not modify** CVE itself as per our [Terms of Use](#). CVE and NVD are both sponsored by the [office of Cybersecurity and Communications](#) at the [U.S. Department of Homeland Security](#).

### CVE List

[CVE-ID Syntax Change](#)

[CVE Usage of CVRF](#)

[About CVE Identifiers](#)

[Editorial Policies](#)

[Data Sources/Product Coverage](#)

[Reference Key/Maps](#)

[Search Tips](#)

[Updates & RSS Feeds](#)

[Request a CVE Identifier](#)

### ITEMS OF INTEREST

[Terminology](#)

[NVD](#)



<http://cve.mitre.org/cve/index.html>



## Common Vulnerabilities and Exposures

*The Standard for Information Security Vulnerability Names*

**New CVE-ID Format as of January 1, 2014 — [learn more](#)**

TOTAL CVEs: **60686**

HOME > CVE > CVE-2011-0762

### About CVE

- Terminology
- Documents
- FAQs

### CVE List

- CVE-ID Syntax Change
- About CVE Identifiers
- Search CVE
- Search NVD
- Updates & RSS Feeds
- Request a CVE-ID

### CVE In Use

- CVE-Compatible Products
- NVD for CVE Fix Information
- CVE Numbering Authorities

### News & Events

- Calendar
- Free Newsletter

### Community

- CVE Editorial Board
- Sponsor

[Printer-Friendly View](#)

CVE-ID	
<b>CVE-2011-0762</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> <li>• SREASONRES:20110301 vsftpd 2.3.2 remote denial-of-service</li> <li>• URL:<a href="http://securityreason.com/achievement_securityalert/95">http://securityreason.com/achievement_securityalert/95</a></li> <li>• BUGTRAQ:20110301 vsftpd 2.3.2 remote denial-of-service</li> <li>• URL:<a href="http://www.securityfocus.com/archive/1/archive/1/516748/100/0/threaded">http://www.securityfocus.com/archive/1/archive/1/516748/100/0/threaded</a></li> <li>• EXPLOIT-DB:16270</li> <li>• URL:<a href="http://www.exploit-db.com/exploits/16270">http://www.exploit-db.com/exploits/16270</a></li> <li>• MISC:<a href="http://cxib.net/stuff/vspoc232.c">http://cxib.net/stuff/vspoc232.c</a></li> <li>• CONFIRM:<a href="ftp://vsftpd.hearts.org/users/revans/untar/vsftpd-2.3.4/Channel0n">ftp://vsftpd.hearts.org/users/revans/untar/vsftpd-2.3.4/Channel0n</a></li> </ul>	

DoS for FTP sessions, primarily Linux

CVE List
<a href="#">CVE-ID Syntax Change</a>
<a href="#">CVE Usage of CVRF</a>
<a href="#">About CVE Identifiers</a>
<a href="#">Editorial Policies</a>
<a href="#">Data Sources/Product Coverage</a>
<a href="#">Reference Key/Maps</a>
<a href="#">Search Tips</a>
<a href="#">Updates &amp; RSS Feeds</a>
<a href="#">Request a CVE Identifier</a>
ITEMS OF INTEREST
<a href="#">Terminology</a>
<a href="#">NVD</a>



# Networking Monitoring



- **A detailed analysis of vulnerabilities** found within your IP addresses or domain, classified by High, Medium or Low severity
- **Step-by-step instructions on how to remediate threats**, so you can immediately address the most serious vulnerabilities

## Internal PCI Report

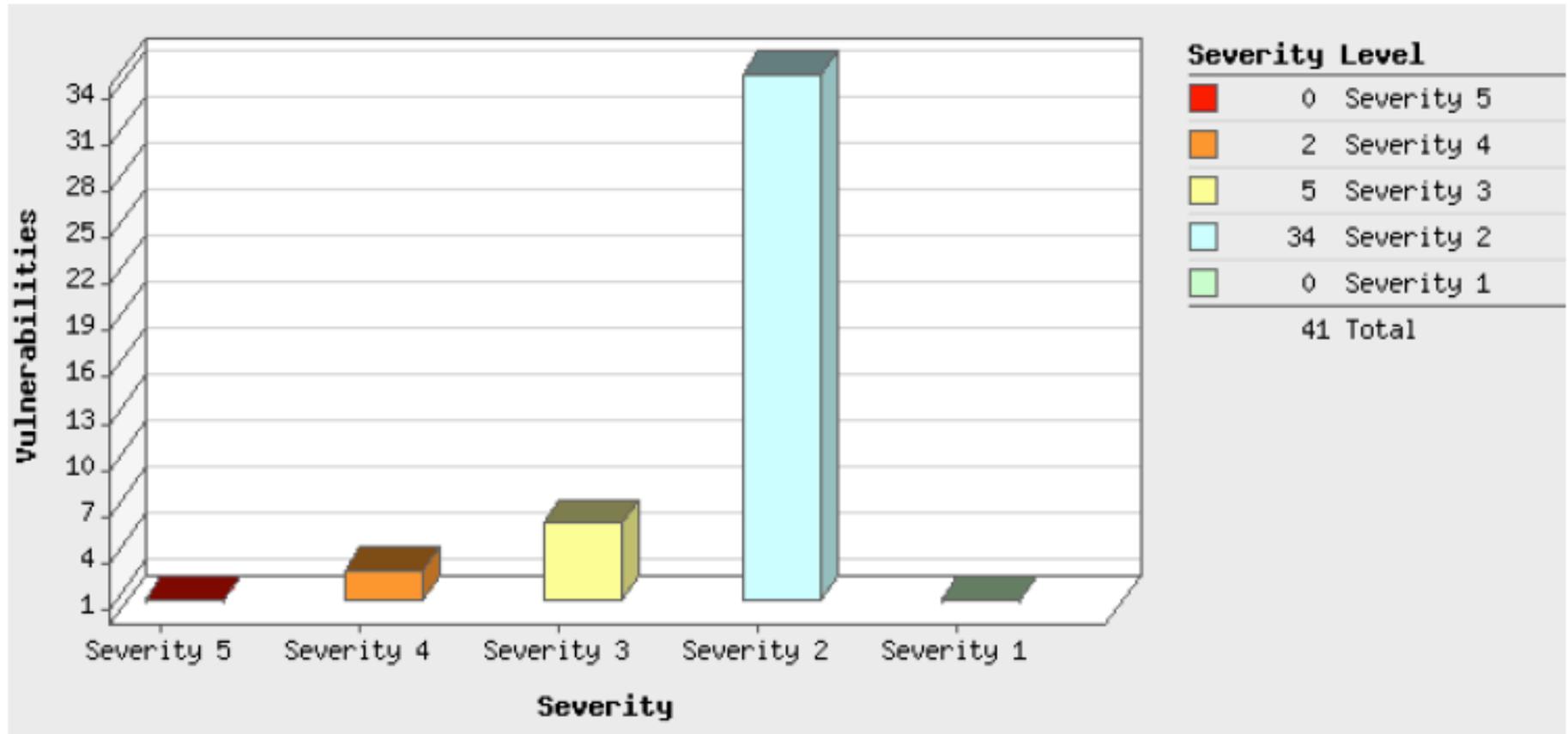
### Summary of Vulnerabilities

Vulnerabilities Total	870	Security Risk (Avg)		2.3
-----------------------	-----	---------------------	---	-----

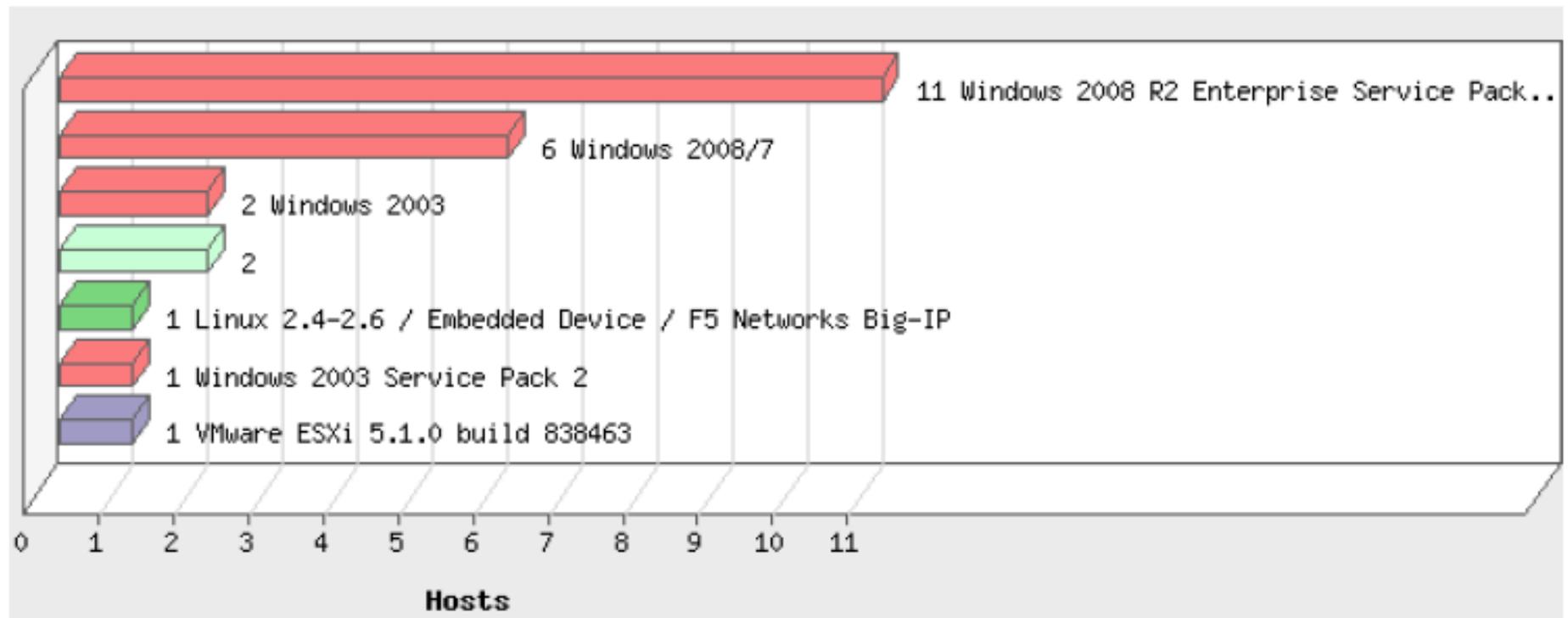
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	2	2	0	4
3	5	30	27	62
2	34	24	78	136
1	0	5	663	668
Total	41	61	768	870

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	11	25	164	200
TCP/IP	3	0	162	165
Information gathering	0	0	140	140
Web server	5	12	79	96
Web Application	2	12	79	93
Total	21	49	624	694

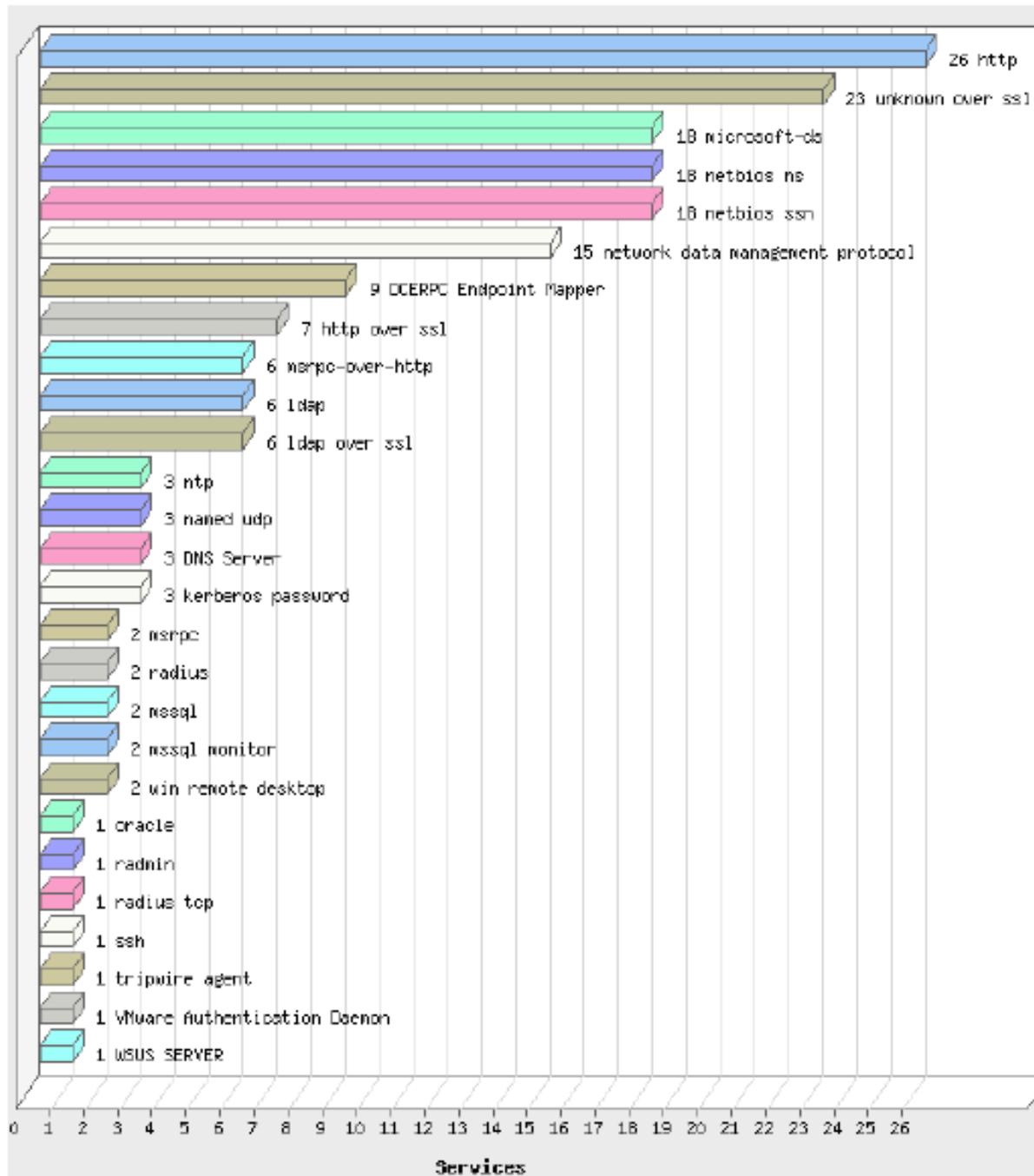
## Vulnerabilities by Severity



## Operating Systems Detected



## Services Detected



**PCI COMPLIANCE STATUS**

PCI Severity:

**MED****VULNERABILITY DETAILS**

CVSS Base Score: **4**  AV:N/AC:H/Au:N/C:P/I:P/A:N  
CVSS Temporal Score: **3.6** E:F/RL:W/RC:C  
Severity: **3**   
Comments: Default ranking

QID: 38139  
Category: General remote services  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Service Modified: 05/09/2012  
User Modified: -  
Edited: No  
PCI Vuln: Yes

**THREAT:**

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular Web servers, mail servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 Protocol (<http://www.schneier.com/paper-ssl.html>)

**IMPACT:**

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

**SOLUTION:**

Disable SSLv2.

# False Positives

- ❖ False Positive - The erroneous identification of a threat or dangerous condition that turns out to be harmless. False positives often occur in IDS and vulnerability scans.
- ❖ False Negative - The erroneous identification of a benign condition that turns out to be harmful.

# Penetration Testing

PCI DSS Requirements	Testing Procedures
<p><b>11.3</b> Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:</p>	<p><b>11.3.a</b> Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.</p> <p><b>11.3.b</b> Verify that noted exploitable vulnerabilities were corrected and testing repeated.</p> <p><b>11.3.c</b> Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).</p>
<p><b>11.3.1</b> Network-layer penetration tests</p>	<p><b>11.3.1</b> Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.</p>
<p><b>11.3.2</b> Application-layer penetration tests</p>	<p><b>11.3.2</b> Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.</p>

## PCI DSS v2.0

**11.3 Implement a methodology for penetration testing that includes the following:**

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

**11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following:**

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

**Penetration Testing  
PCI DSS V3.0  
REQUIREMENT AFTER JUNE 30, 2015**

<p><b>11.3.1</b> Perform <i>external</i> penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).</p>	<p><b>11.3.1.a</b> Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:</p> <ul style="list-style-type: none"> <li>• Per the defined methodology</li> <li>• At least annually</li> <li>• After any significant changes to the environment.</li> </ul> <p><b>11.3.1.b</b> Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).</p>
<p><b>11.3.2</b> Perform <i>internal</i> penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).</p>	<p><b>11.3.2.a</b> Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.</p> <ul style="list-style-type: none"> <li>• Per the defined methodology</li> <li>• At least annually</li> <li>• After any significant changes to the environment.</li> </ul> <p><b>11.3.2.b</b> Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).</p>
<p><b>11.3.3</b> Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.</p>	<p><b>11.3.3</b> Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.</p>

# Penetration Testing

**11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

Big Issue: This means a penetration test of the CDE must include the analysis of card data flow in electronic form on any system within the CDE and any connected systems.

**11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems.

**11.3.4.b** Examine the results from the most recent penetration test to verify that penetration testing to verify segmentation controls:

- Is performed at least annually and after any changes to segmentation controls/methods.
- Covers all segmentation controls/methods in use.
- Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

## PCI DSS v3.0

# External Network & Application Penetration Test

External Network and Application Penetration Tests are conducted to help identify vulnerabilities throughout <company's> environment. Assessments are conducted using a Full-disclosure / Non-evasive approach. They include:

1. **Discovery Phase** – Performed host discovery utilizing ping sweeps and limited port scans.
2. **Target Profiling Phase** – Enumerated, grouped, and prioritized services running on active hosts.
3. **Examination Phase** – Performed vulnerability testing utilizing automated and manual techniques.
4. **Risk Validation Phase** – Confirmed vulnerabilities through authorized exploitation attempts.

# Top 20 Critical Security Controls - Version 5

- 1: Inventory of Authorized and Unauthorized Devices
- 2: Inventory of Authorized and Unauthorized Software
- 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Malware Defenses
- 6: Application Software Security
- 7: Wireless Access Control
- 8: Data Recovery Capability
- 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- 11: Limitation and Control of Network Ports, Protocols, and Services
- 12: Controlled Use of Administrative Privileges
- 13: Boundary Defense
- 14: Maintenance, Monitoring, and Analysis of Audit Logs
- 15: Controlled Access Based on the Need to Know
- 16: Account Monitoring and Control
- 17: Data Protection
- 18: Incident Response and Management
- 19: Secure Network Engineering
- 20: Penetration Tests and Red Team Exercises



# OWASP Top 10 - 2013

Top 10 – 2013	
A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query.
A2 - Broken Authentication and Session Management	application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens
A3 – Cross Site Scripting (XSS)	XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	developer exposes a reference to an internal implementation object, such as a file, directory, or database key, attackers can manipulate these references to access unauthorized data.
A5 – Security Modification	for the application, frameworks, application server, web server, database server, and platform.
A6 – Sensitive Data Exposure	web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials.
A7 – Missing Function Level Access Control	access unauthorized or Administrative functions without authentication
A8 – Cross-Site Request Forgery (CSRF)	forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application.
A9 - Using Components with Known Vulnerabilities	applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10 – Unvalidated Redirects and Forwards	web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages.

# Input Validation (Encoding)

## How many ways can you say

**YAHOO!**

- ❖ <http://www.yahoo.com> → ir1.fp.vip.sp2.yahoo.com
- ❖ <http://206.190.36.45> (IP address. Everyone knows it...)
- ❖ <http://0xCEBE242D> (Hex representation)
- ❖ <http://3468567597/> (Decimal representation)
- ❖ <http://0316.0276.044.055> (Octal representation)
- ❖ <http://206.0xbe.044.055> (You can mix them too!)

...what about one? <http://www.google.com/search?hl=en&q=yahoo+page&btnl=>

# Penetration Testing Key Concepts

- ❖ Industry-Based Methodology
- ❖ Scope Reduction Controls
- ❖ Application Layer Penetration Testing
- ❖ Threats and Vulnerabilities Experience Last 12 Months
- ❖ Retention of Penetration Tests and Remediation Results
- ❖ Internal Penetration Test
- ❖ External Penetration Test
- ❖ Qualified Internal Resource
- ❖ Qualified External Resource
- ❖ Exploitable Vulnerability Remediated and Retested
- ❖ Segmentation Controls

# Tools for Pen Testing

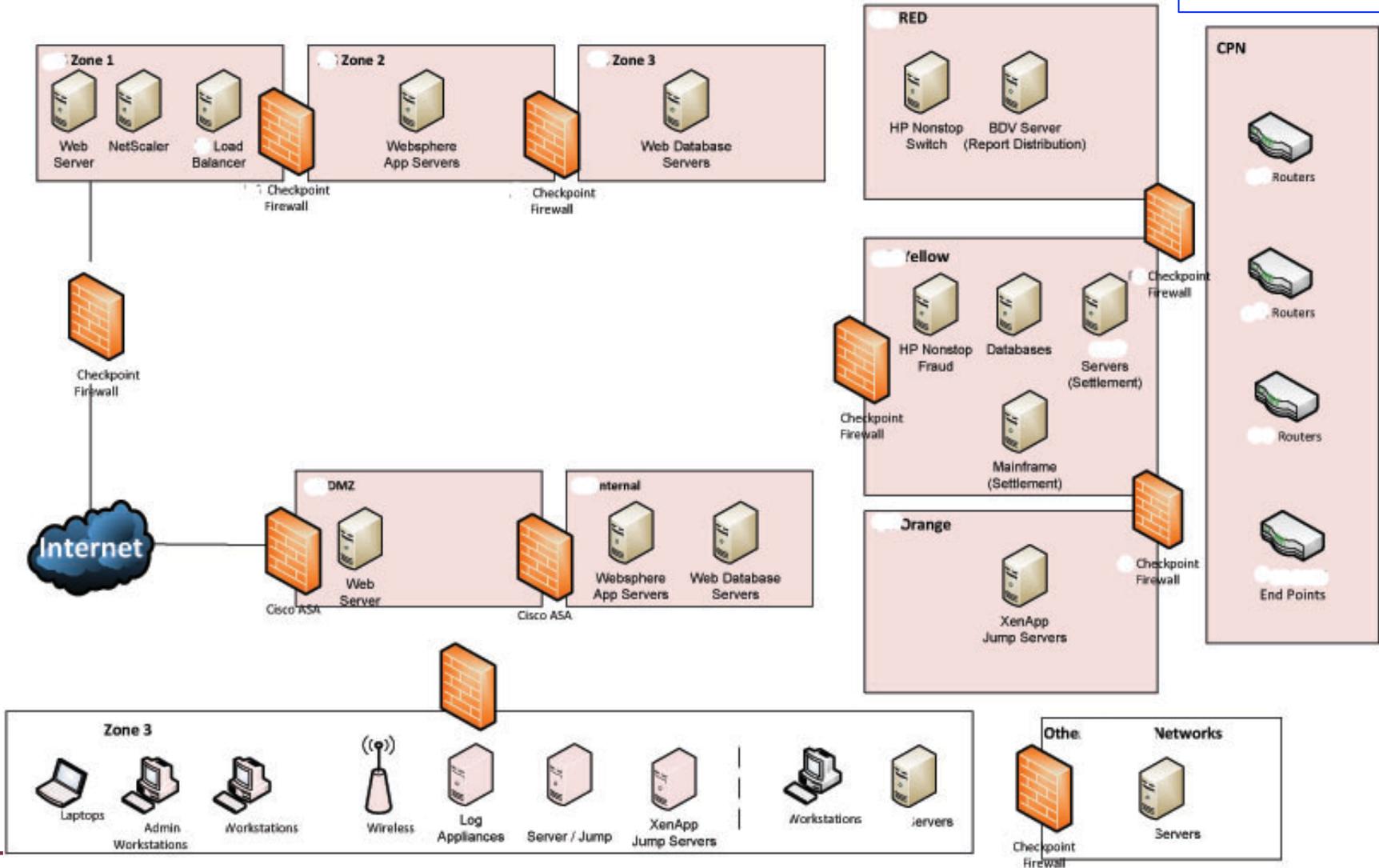
- ❖ **BackTrack Linux 5 R2/R3** – attacker machine
- ❖ **Nmap Network Scanner** – used to identify ports and services on target system
- ❖ **Metasploit Framework** – used for exploiting, generating the payload, establishing a session with target system
- ❖ **Others...**

# Segmentation

Network Diagram Sample (Redacted)

## Infrastructure

In Scope      Not In Scope



# Segmentation Issues

- ❖ Cardholder Data (CHD) must exclusively be stored, processed or transmitted through the Cardholder Environment (CDE)
- ❖ You have to prove this by:
  - ❖ Clearly defining the In-Scope Segments
  - ❖ Demonstrate that CHD does not exist in Not-In-Scope segments
  - ❖ Prove that the use of firewalls, ACLs and proxies segment CDE from untrusted segments
  - ❖ All communication lines to CDE is protected or encrypted using dedicated leased lines, SSLv3, VPN w/IPSEC, strong encryption (AES-256), and/or 2-factor authentication
- ❖ Biggest issue is PCI DSS v3.0 is that now it needs to be pen tested

# eDiscovery

- ❖ eDiscovery tools are used for several reasons:
  - ❖ Legal e-discovery
  - ❖ HIPAA/PCI/PII e-discovery
  - ❖ Digital Forensics
  - ❖ Security Monitoring
- ❖ Lawyers and e-discovery practitioners, in particular, struggle with the rights, restrictions and reality involved in employees' use of social media

# Magic Quadrant on eDiscovery



## Upper Right Quadrant

- Kroll Ontrack
- FTI Technology
- kCura
- AccessData
- HP Autonomy
- Symantec
- Recommind
- Exterro
- Guidance Software

# Data Discovery Tools

❖ Used to scan for Cardholder Data (CHD)

❖ Examples:

❖ Card Recon

❖ iScan

❖ ICVERIFY

❖ Spider Crawlers

**3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).

**3.4.c** Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.

**3.4.d** Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.

# Sample Spider Scan

START				
State File: C:\Documents and Settings\jasonsu\Local Settings\Application Data\Spider\State\spider-<hostname>-20131204-17.ss3				
Hostname: <hostname>				
Username: <username>				
Last Scan Date: 12/4/2013 5:52:50 PM				
Comments:				
FILE	HIT TYPE	TOTAL HITS	ACTION	DATE
C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\about_arithmetic_operators.help.txt	Credit Card Number	1	Marked as false positive	12/5/13 13:46
C:\WINDOWS\system32\WindowsPowerShell\v1.0\about_arithmetic_operators.help.txt	Credit Card Number	1	Marked as false positive	12/5/13 13:46
END				

# Data Loss Prevention



websense®

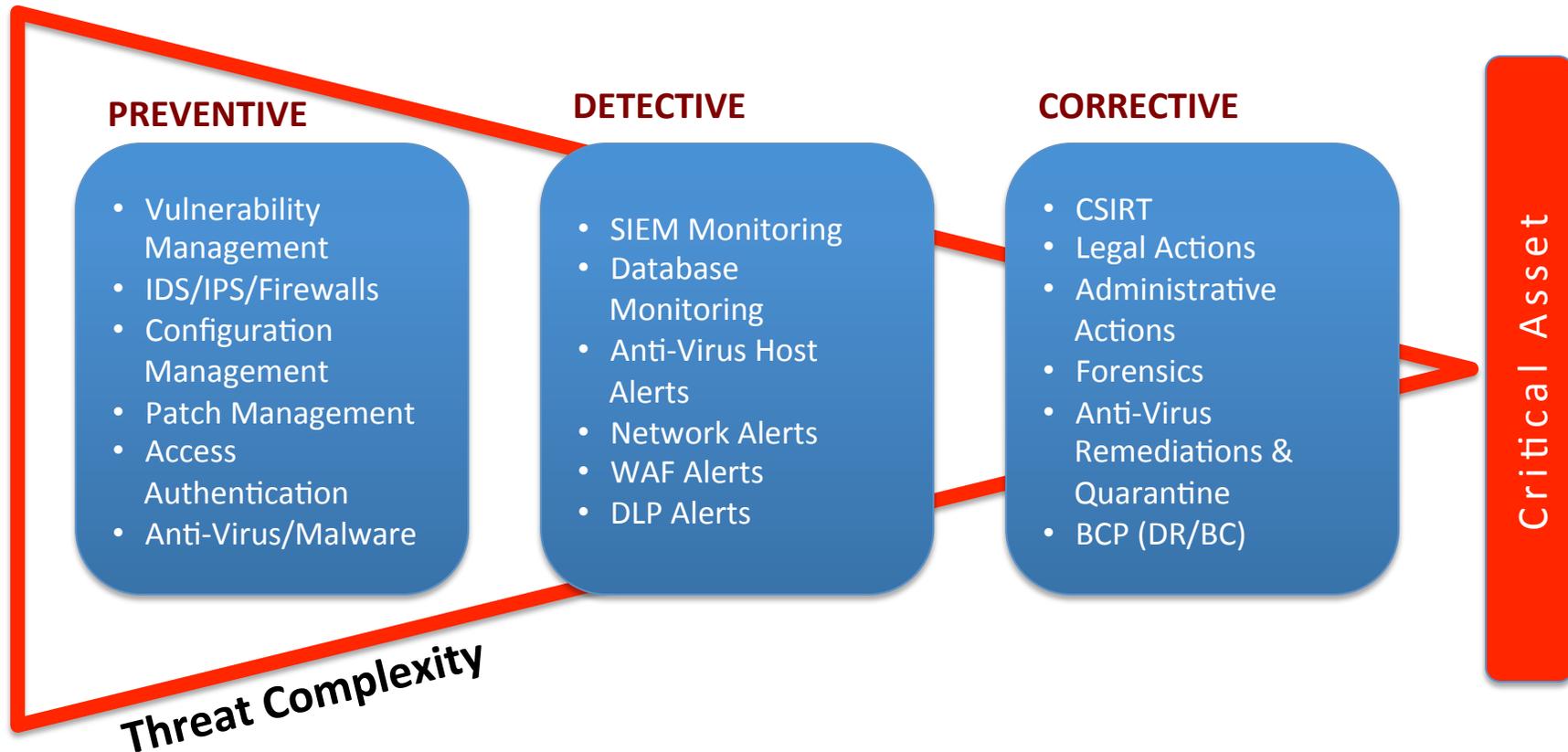
**DLPWorks.com**  
Code Green Networks Authorized Reseller



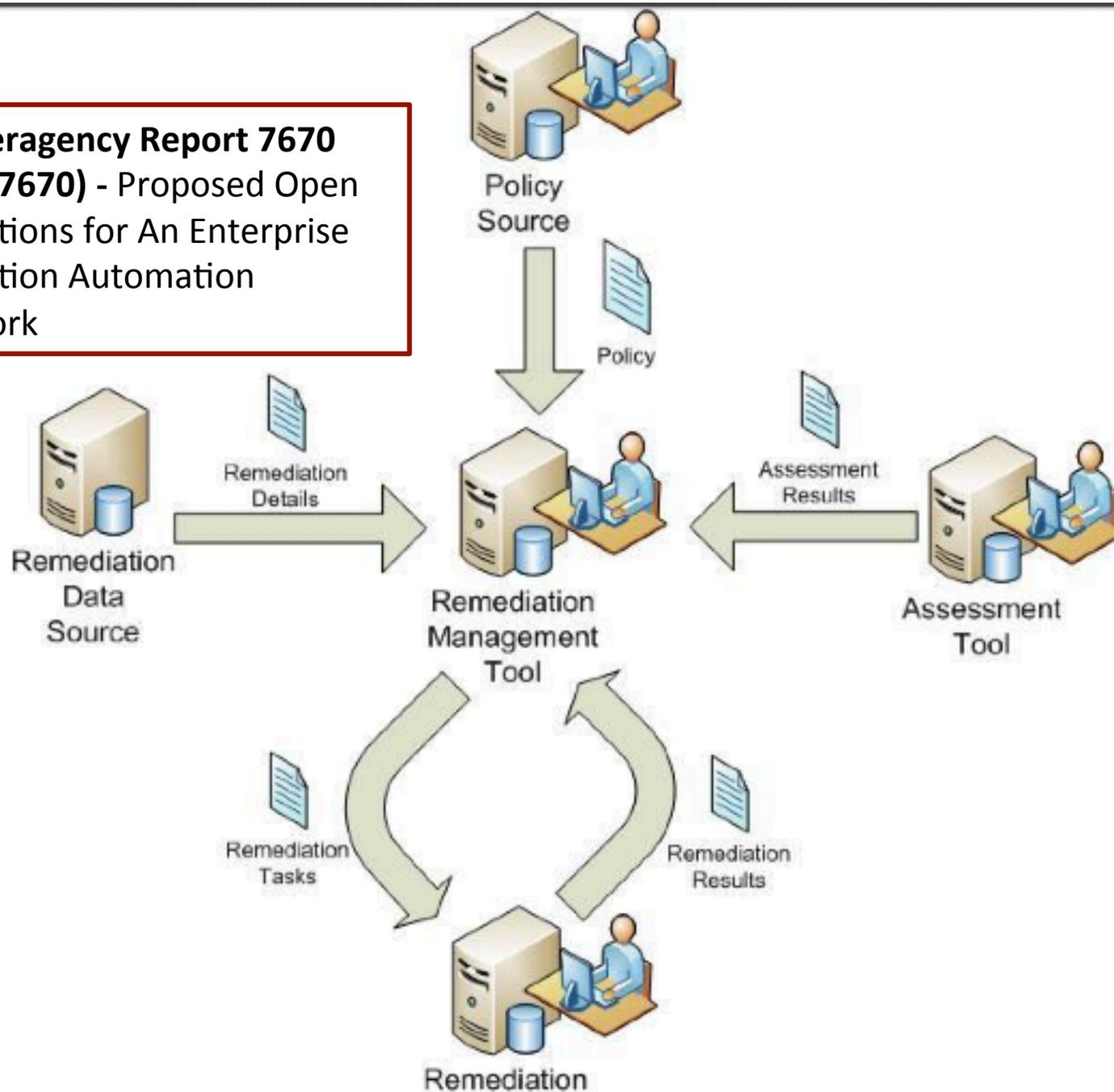
opendlp

- Detect, block or control the usage of (for example, saving, printing or forwarding) specific content based on established rules or policies.
- Monitor network traffic for, at a minimum, e-mail traffic and other channels/ protocols (HTTP, IM, FTP) and analyze across multiple channels, in a single product and using a single management interface.
- End-Point / Network / Discovery

# Workflow Management



**NIST Interagency Report 7670  
(NIST IR-7670) - Proposed Open  
Specifications for An Enterprise  
Remediation Automation  
Framework**



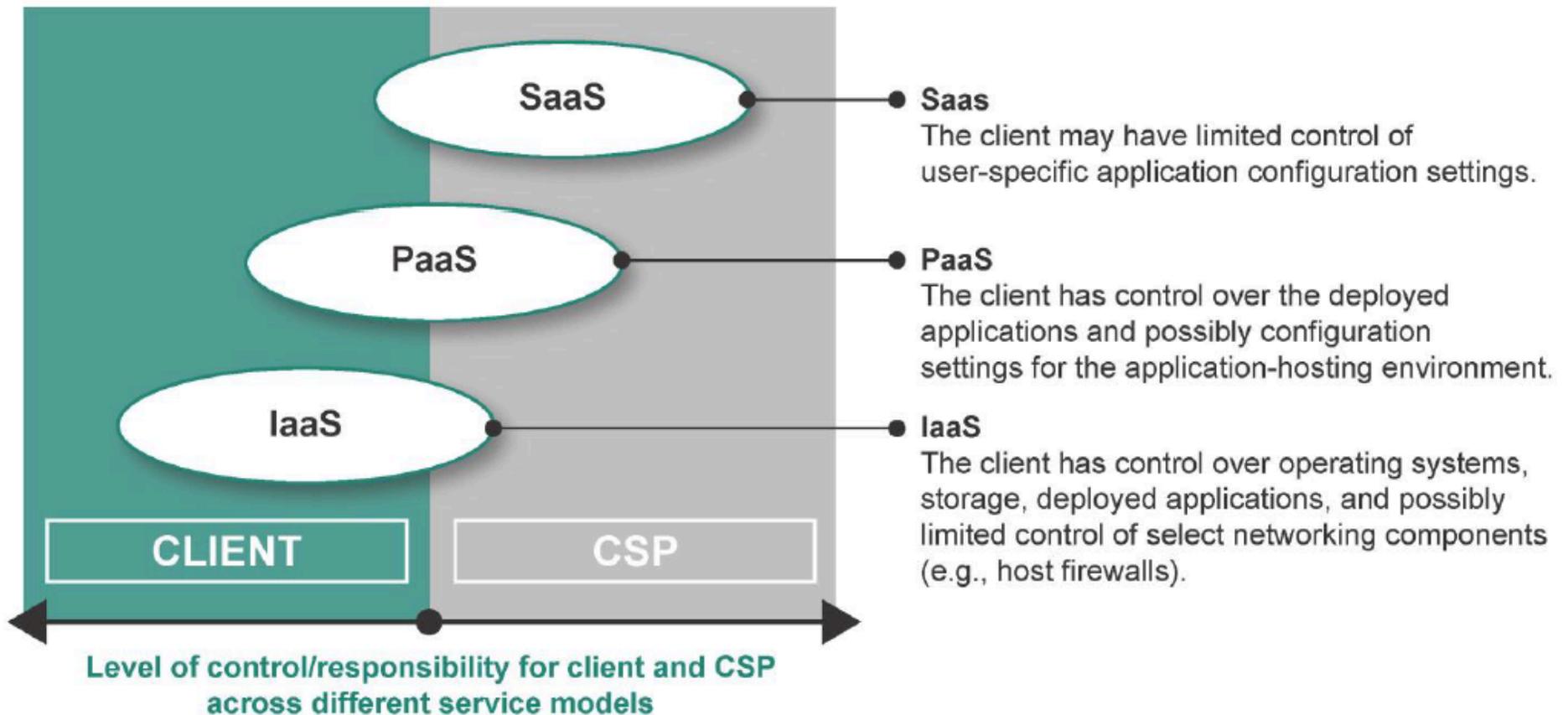
# NIST IR-7670 Workflow

Remediation Policy Source	Public or private repository for remediation policy documents
Remediation Policy	Set of remediation policy directives for computing assets. These directives may specify target platforms, parameter values, and a reference to a common remediation identifier. Remediation policies may define configuration settings that are to be applied, vulnerabilities to be remedied, and patches that must be applied. Such policies can be established at the enterprise level and may be tailored to meet the local operational needs of organizational elements or business units.
Remediation Management Tool	Tool responsible for evaluating assessment results, remediation policy, and remediation details to produce specific remediation tasking instructions for remediation tools.
Remediation Data Source	Public or private repository for detailed remediation information
Remediation Tool	Tool responsible for apply individual remediations to specified assets.
Remediation Details	Publicly or privately held data that identifies the vulnerability or misconfiguration a remediation addresses, any prerequisites for performing the remediation and post-application instructions.
Assessment Results	Describes the vulnerabilities or misconfigurations discovered by an assessment or scanning tool and the metadata regarding how and when the assessment was performed (e.g., date & time of the scan, tool used, scan operator).
Remediation Tasks	Remediation instructions specifying which remediations are to be applied, when they are to be applied, and under what conditions.
Remediation Results	The outcome of attempted remediation tasks on particular assets.

# Managed Services

- ❖ When considering managed service providers it is critical to understand which of their service offerings have been validated as HIPAA, PCI DSS, GLBA, FISMA compliant.
- ❖ Do not rely on an SSAE-16 unless you know what the CPA auditors tested. Many times they use the SSAE-16 as validation that they are regulation or PCI compliant.
- ❖ Obtain, in writing, whether they will provide or allow vulnerability scanning, penetration testing or discovery services on behalf of client.
- ❖ Ensure that the services they provide do not compromise security if your data is shared or housed in the same environment as other company data.

# Cloud Computing Security Role/Responsibility



# Tools for Continuous Monitoring

- ❖ Security Incident & Event Monitoring (SIEM)
- ❖ File Integrity Monitoring (FIM)
- ❖ Intrusion Detection and Prevention Systems (IDS/IPS)
- ❖ Web Application Firewalls (WAFs)
- ❖ Firewalls (numerous)
- ❖ Database Monitoring
- ❖ Two-Factor Authentication
- ❖ Encryption

# Security Information & Event Monitor (SIEM)

## COMMERCIAL



## OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

# File Integrity Monitoring

## COMMERCIAL



## OPEN SOURCE

TRIPWIRE



**AIDE**

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

# IDS/IPS

## COMMERCIAL



## OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

# Web Application Firewalls

## COMMERCIAL



## OPEN SOURCE



ESAPI Web Application Firewall (ESAPI WAF)



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current attack vendors

# Database Monitoring

## COMMERCIAL



## OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

# Two-Factor Authentication

➤ Multi-factor authentication (also Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors

- **Something I know**
- **Something I have**
- **Something I am**



- RSA SecurID



PhoneFactor offers instant integration with a wide range of applications, including all leading remote access VPN solutions, single sign-on systems, cloud applications, online banking, and websites as well as custom applications. PhoneFactor also integrates with Active Directory and LDAP servers for centralized user management.

# Summary

- ❖ **Security Monitoring**
- ❖ **Vulnerability Scanners**
- ❖ **Penetration Tests**
- ❖ **eDiscovery Scanners**
- ❖ **Workflow Management**
- ❖ **Continuous Monitoring Options**

## BIO

**Miguel (Mike) O. Villegas** is a Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/IEC 27001:2005 program. Mike was previously Director of Information Security at Newegg, Inc. for five years.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC and CEH. He is also a QSA, PA-QSA and ASV as VP for K3DES.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 18 years.