微軟 最佳安全實務

羅廷儀: 微軟資深產品行銷經理

people ready

最佳安全實務

- 2007 ~ 2008 資安趨勢回顧
- 資訊安全策略與微軟最佳實踐
- 資安常見問題與建議改進方法

美國大選 候選人陣營 電腦被駭

2候選人陣營 電腦被駭〔編譯鄭寺音 / 綜合七日外電報導〕

美國「新聞週刊」六日報導，美國大選期間，兩位總統候選人陣營的電腦系統都曾遭到手法熟練的駭客侵入，並被竊走「大量檔案」；專家認為，這應該是中國或俄羅斯為竊取情報進行的網路攻擊行動。

新聞週刊指出，民主黨陣營今夏發現電腦中毒，後來聯邦調查局（ＦＢＩ）密勤局到訪，才知道所謂的病毒其實是駭客入侵。懷疑是中國或俄羅斯搞的鬼。

報導指出：「聯邦調查局與白宮官員告訴歐巴瑪陣營，他們相信有個外國團體或組織企圖蒐集兩方陣營的政策議題演進情報。這些資訊在與下一任政府談判時可能有用。」

ＦＢＩ告訴歐巴瑪陣營，共和黨麥肯陣營的電腦也遭駭客入侵，並向歐巴瑪保證此舉並非他的政敵所為，不過他們的電腦系統已有「大量檔案」遭竊取。歐巴瑪的科技專家後來猜測，駭客應該是俄羅斯或中國人。

兩陣營聘請安全公司防堵之後，駭客入侵行動宣告瓦解。聯邦調查局已針對此事展開調查。

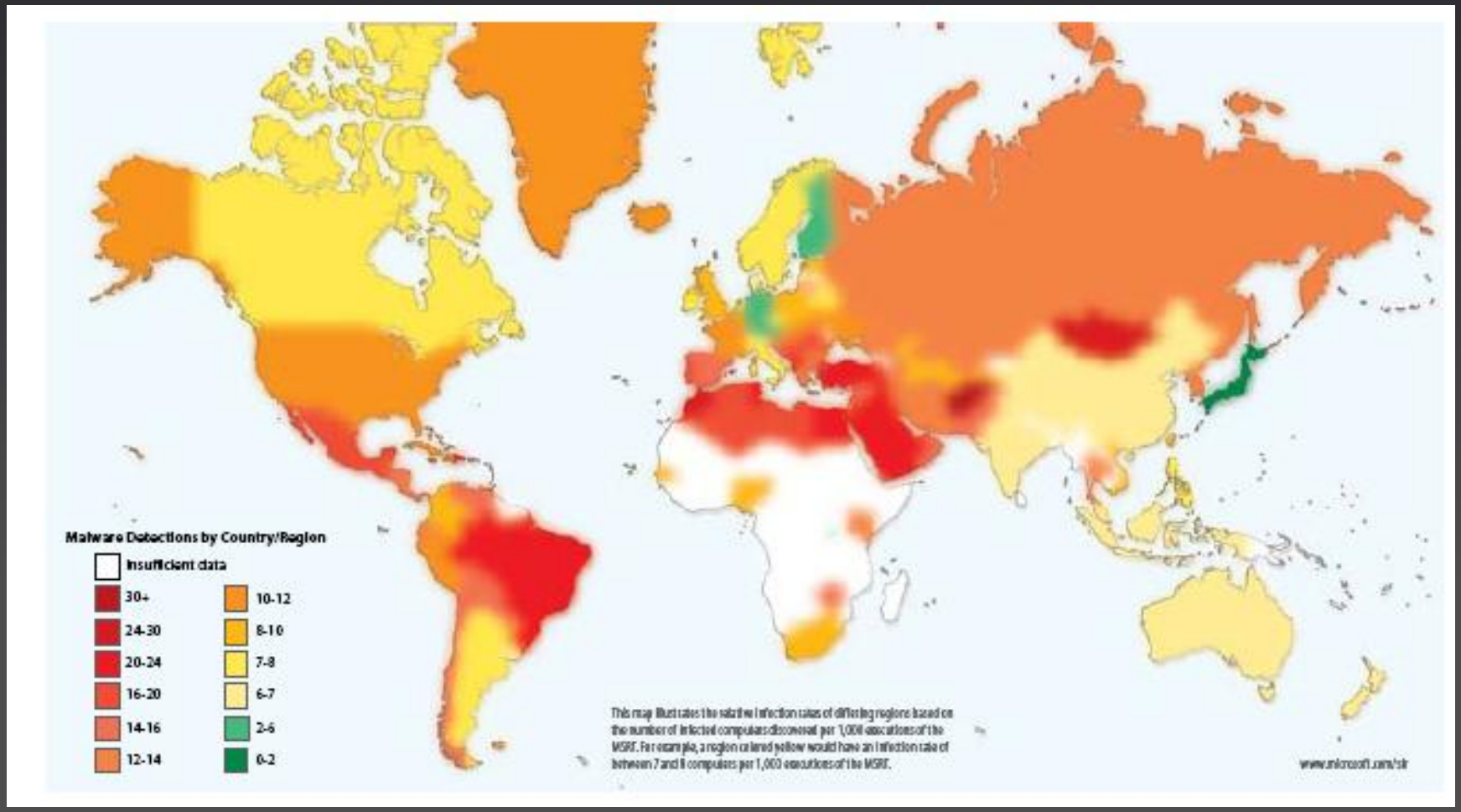
隱私權：Privacy

- 個人資料保護法預計將修正通過，除了擴大保護對象，並訂有每筆資料外洩罰金，2009年實現法規遵循與落實企業社會責任對企業而言將益形重要。

2009年資訊軟體重要議題, MIC

資安威脅區域的分佈

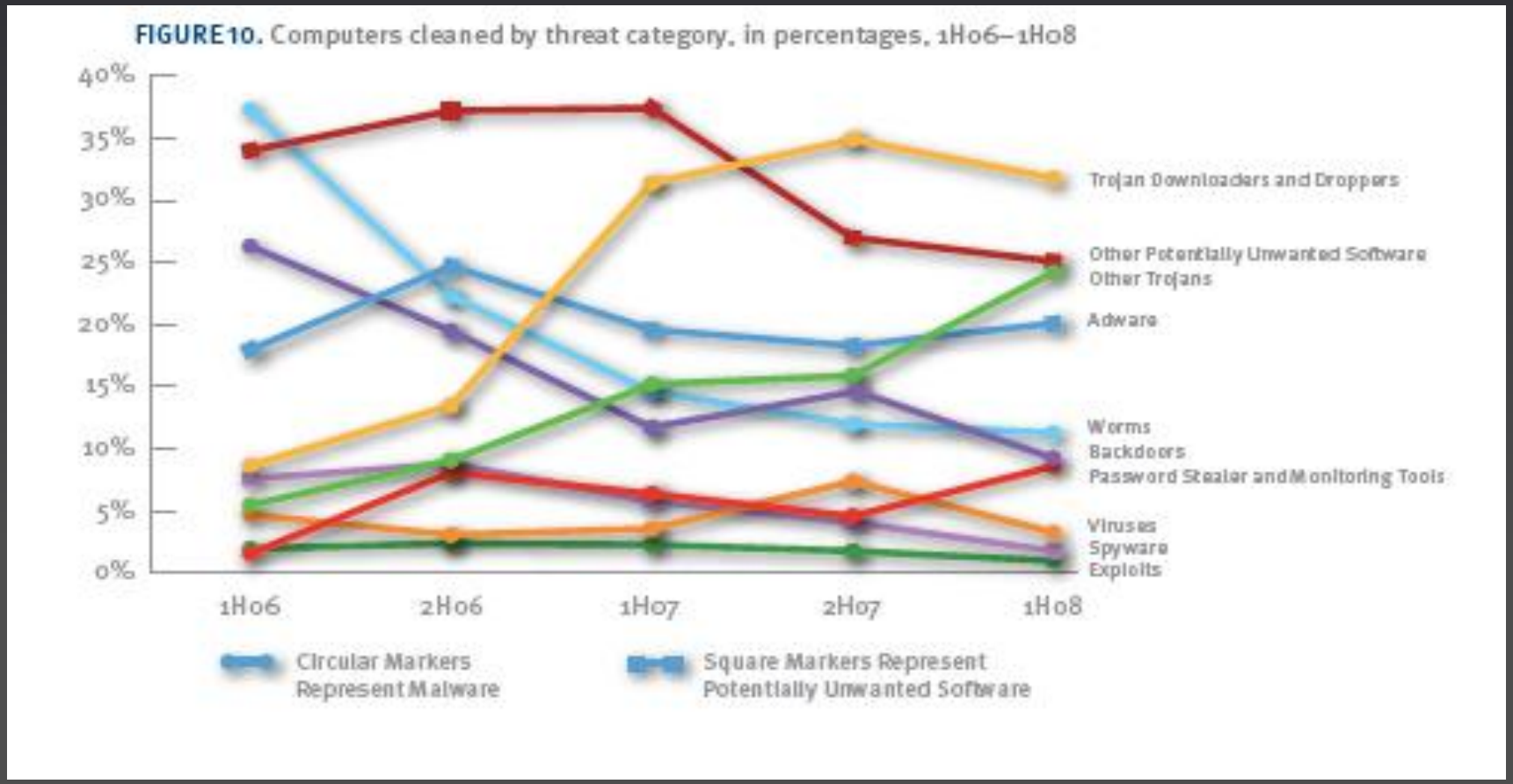
- 發展中國家被惡意程式入侵的機率高於已開發國家



Reported by the Malicious Software Removal Tool (MSRT). 2008

資安威脅趨勢的改變

- 2006 上半年到2008上半年， 木馬程式，不明程式下載為成長最快的項目。
- 病毒，間諜程式逐年下降的趨勢。



微軟2008 Security Advisor Report.

網路犯罪是主要的 財務/法規 威脅的來源

The rapid evolution of computer interconnectivity has had immense cultural and economic benefits. Unfortunately, this evolution has also enabled criminal activity that exploits this interconnectivity for financial gain and other malicious purposes. In a June 2007 report, the U.S Government Accountability Office (GAO) described cybercrime as "having significant economic impacts and a threat to U.S. national security interests. "

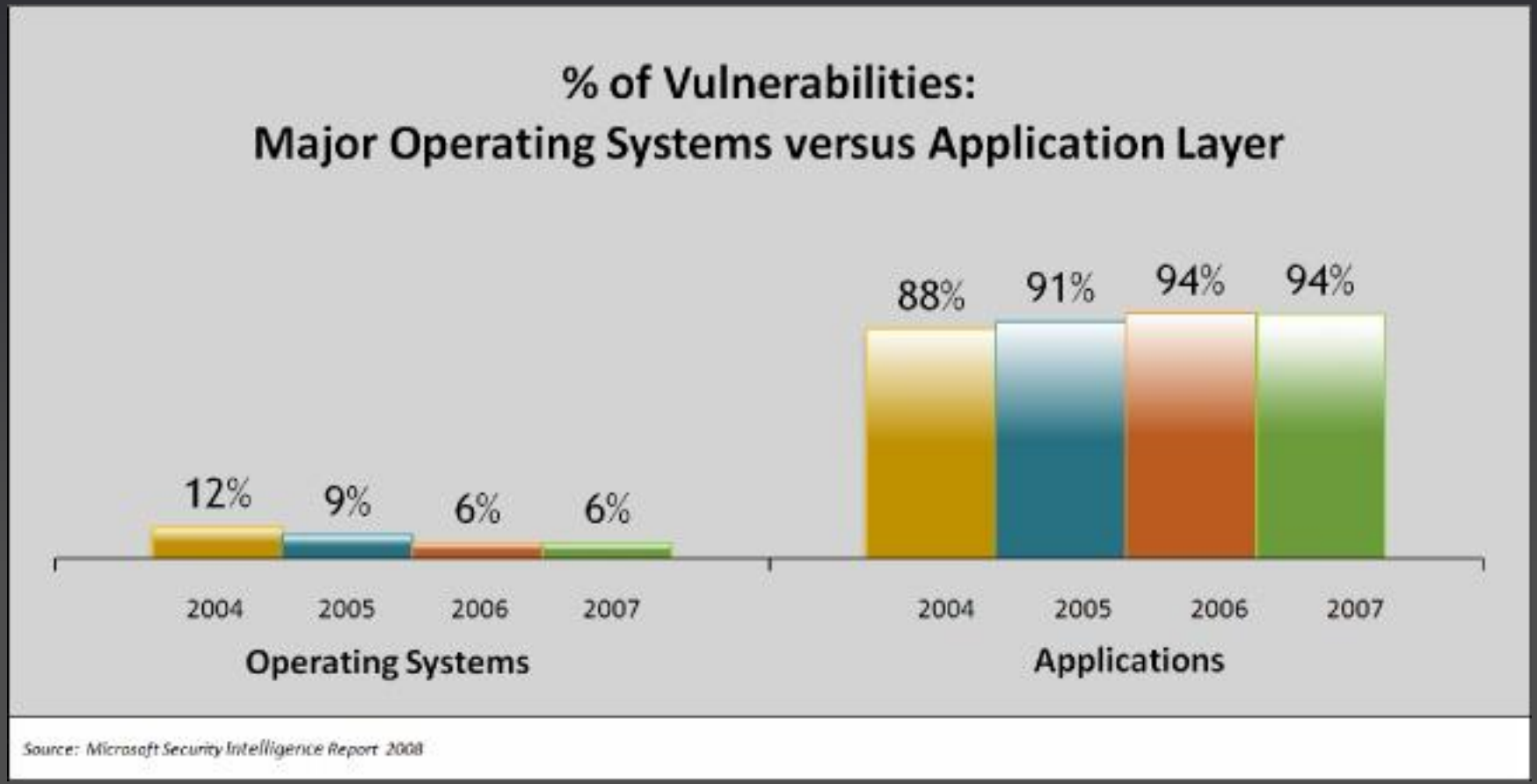
Consider the following sample of data points about cybercrime:

- A 2005 FBI survey estimated annual loss due to computer crime at $67.2 billion for U.S. organizations.
- The estimated losses associated with identity theft in 2006 are $49.3 billion.
- In a 2006 study, the Ponemon Institute, LLC found that the average cost a data breach rose in 2006 to $4.8 million, an increase of 30 percent from the previous year.
- Hacking was responsible for 73 percent of identities compromised during the first six months of 2007 according to the 2007 Symantec Internet Security Threat Report.

CSI 2008 Report

攻擊Application 的機率比OS 高

6% 弱點功擊發生在OS 平台上
同時期， 94%弱點攻擊發生在應用程式的層面。



June 2008 Microsoft Security Intelligence Report

資安產品選擇趨勢的改變

因資安威脅趨勢的改變， 公司組織購買資安產品的項目也因此而調整。

前三名為:

1. NAC/ NAP
2. Application Firewall
3. File Encryption

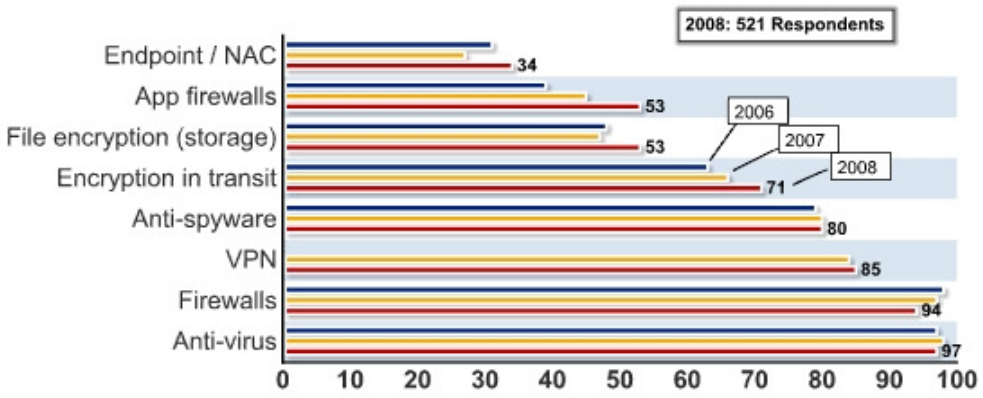
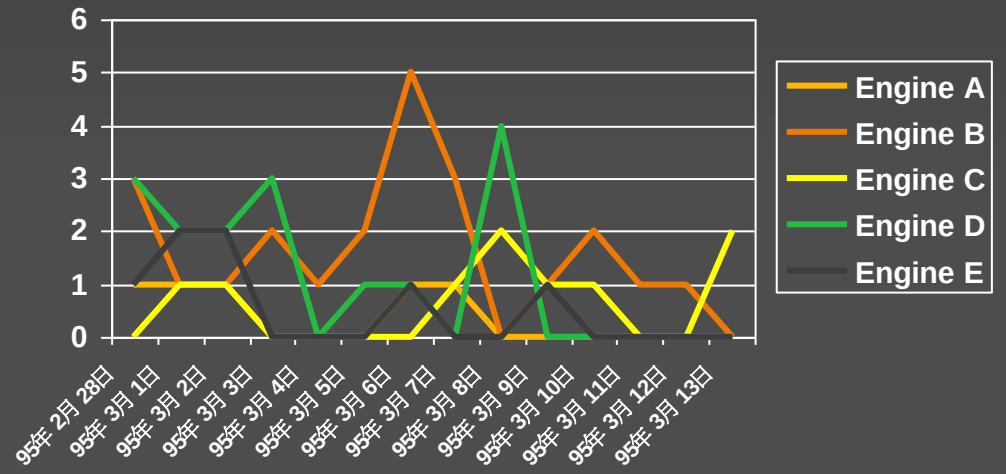


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Exchange 病毒捕捉率

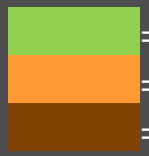
Viruses Caught Only By (excluding body of message viruses)														
	2/28	3/1	3/2	3/3	3/4	3/5	3/6	3/7	3/8	3/9	3/10	3/11	3/12	3/13
Engine A	1	1	1	0	0	0	1	1	0	0	0	0	0	0
Engine B	3	1	1	2	1	2	5	3	0	1	2	1	1	0
Engine C	0	1	1	0	0	0	0	1	2	1	1	0	0	2
Engine D	3	2	2	3	0	1	1	0	4	0	0	0	0	0
Engine E	1	2	2	0	0	0	1	0	0	1	0	0	0	0

- Unique Viruses caught over 14 days
  - Engine A: 5
  - Engine B: 23
  - Engine C: 9
  - Engine D: 16
  - Engine E: 7



多重防禦的重要性

- Rapid response to new threats
- Fail-safe protection through redundancy
- Diversity of antivirus engines and heuristics



=低於 5 個小時
= 5~24 個小時之間
=超過 24 小時

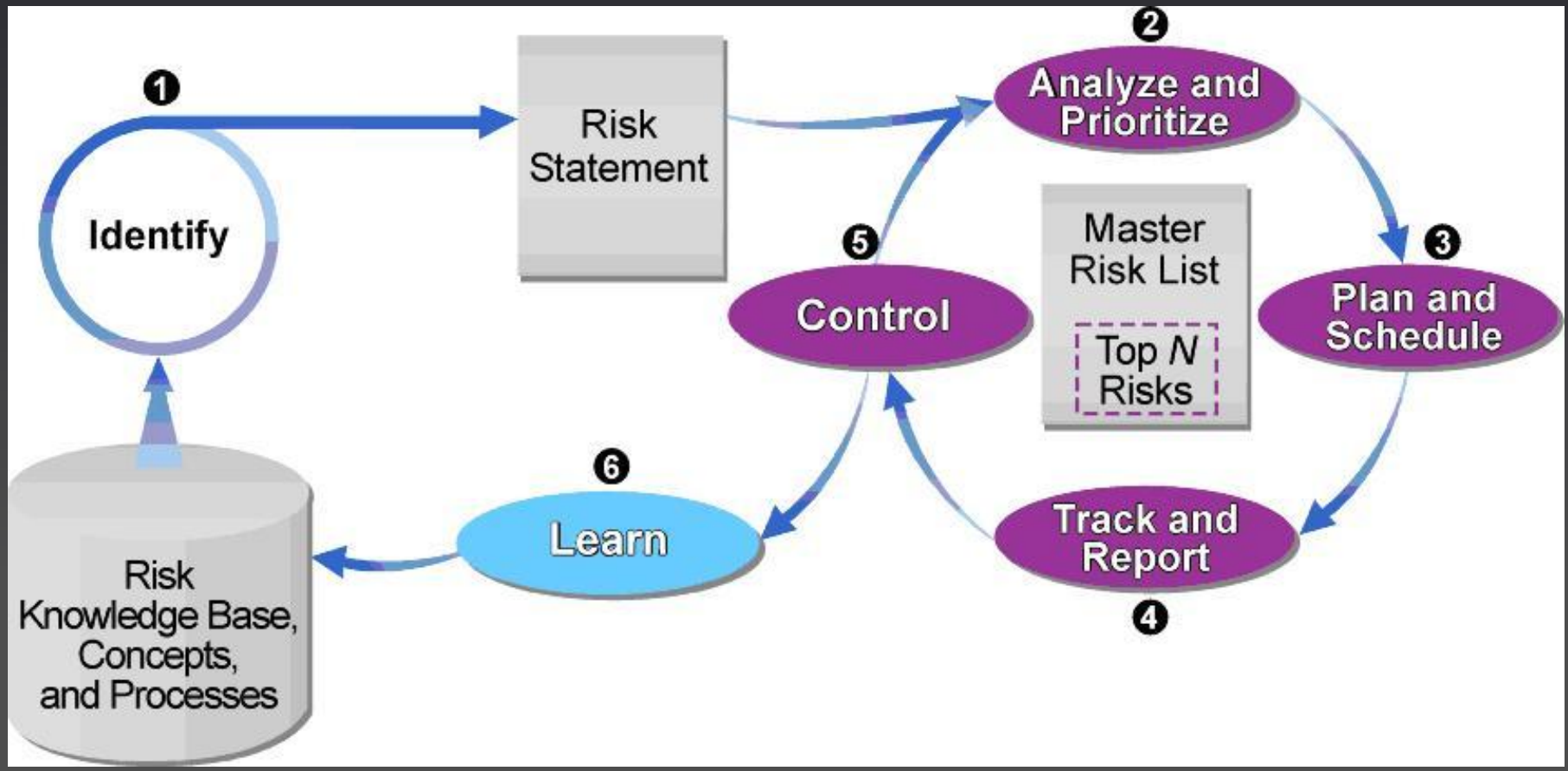
		Response time[1] (in hours)					
		The Microsoft multiple-engine solution			Other single-engine solutions		
WildList Number	Malware Name	Forefront Set 1	Forefront Set 2	Forefront Set 3	Vendor A*	Vendor B*	Vendor C*
01/08	agent_itw14.ex_	0.00	0.00	0.00	0.00	268.65	65.33
01/08	autorun_itw180.ex_	0.00	0.00	0.00	1023.47	0.00	1123.98
01/08	autorun_itw92.ex_	0.00	0.00	0.00	275.67	0.00	731.43
01/08	ircbot_itw227.ex_	0.00	0.00	0.00	1083.70	640.45	557.53
01/08	ircbot_itw236.ex_	0.00	0.00	0.00	0.00	711.47	1148.27
01/08	ircbot_itw238.ex_	0.00	0.00	0.00	563.13	521.73	452.13
01/08	ircbot_itw295.ex_	0.00	0.00	0.00	40.08	226.02	37.32
01/08	ircbot_itw301.ex_	387.98	387.98	404.13	558.98	678.73	514.55
01/08	ircbot_itw305.ex_	387.98	387.98	404.13	484.80	485.77	487.38
01/08	ircbot_itw308.ex_	0.42	0.42	0.42	101.02	12.03	2.10
01/08	ircbot_itw314.ex_	0.00	0.00	0.00	808.48	355.20	802.03
01/08	ircbot_itw317.ex_	0.00	0.00	0.00	12.45	506.28	6.57
01/08	pushbot_itw2.ex_	0.00	0.00	0.00	0.00	700.27	696.17
01/08	rbot_itw2555.ex_	0.00	0.00	0.00	1083.70	0.00	1082.28
01/08	rbot_itw2579.ex_	0.00	0.00	0.00	386.60	306.83	422.27
01/08	rbot_itw2582.ex_	0.00	0.00	0.00	1117.85	0.00	138.83
01/08	rbot_itw2583.ex_	0.00	0.00	0.00	1112.17	3.67	1110.75
01/08	sdbot_itw2584.ex_	0.00	0.00	0.00	961.78	344.62	795.35
01/08	sdbot_itw2596.ex_	0.00	0.00	0.00	301.77	415.20	89.50
01/08	sdbot_itw2636.ex_	0.00	0.00	0.00	0.00	247.47	699.33
02/08	autorun_itw245.ex_	0.00	0.00	0.00	1321.35	0.00	1025.30
02/08	ircbot_itw318.ex_	0.00	0.00	0.00	100.02	619.72	223.42
02/08	ircbot_itw320.ex_	0.00	0.00	0.00	157.67	120.12	669.15
02/08	ircbot_itw336.ex_	0.00	0.00	0.00	181.08	811.67	17.47
02/08	ircbot_itw337.ex_	0.00	0.00	0.00	701.95	901.80	54.68
02/08	ircbot_itw338.ex_	0.00	0.00	0.00	97.73	763.30	81.02
02/08	rcbot_itw342.ex_	0.00	0.00	0.00	1360.62	78.92	260.15

* Includes beta signatures
** 0.00 denotes proactive detection

[1] Source: AV-Test.org 2008 (www.av-test.org)

people ready

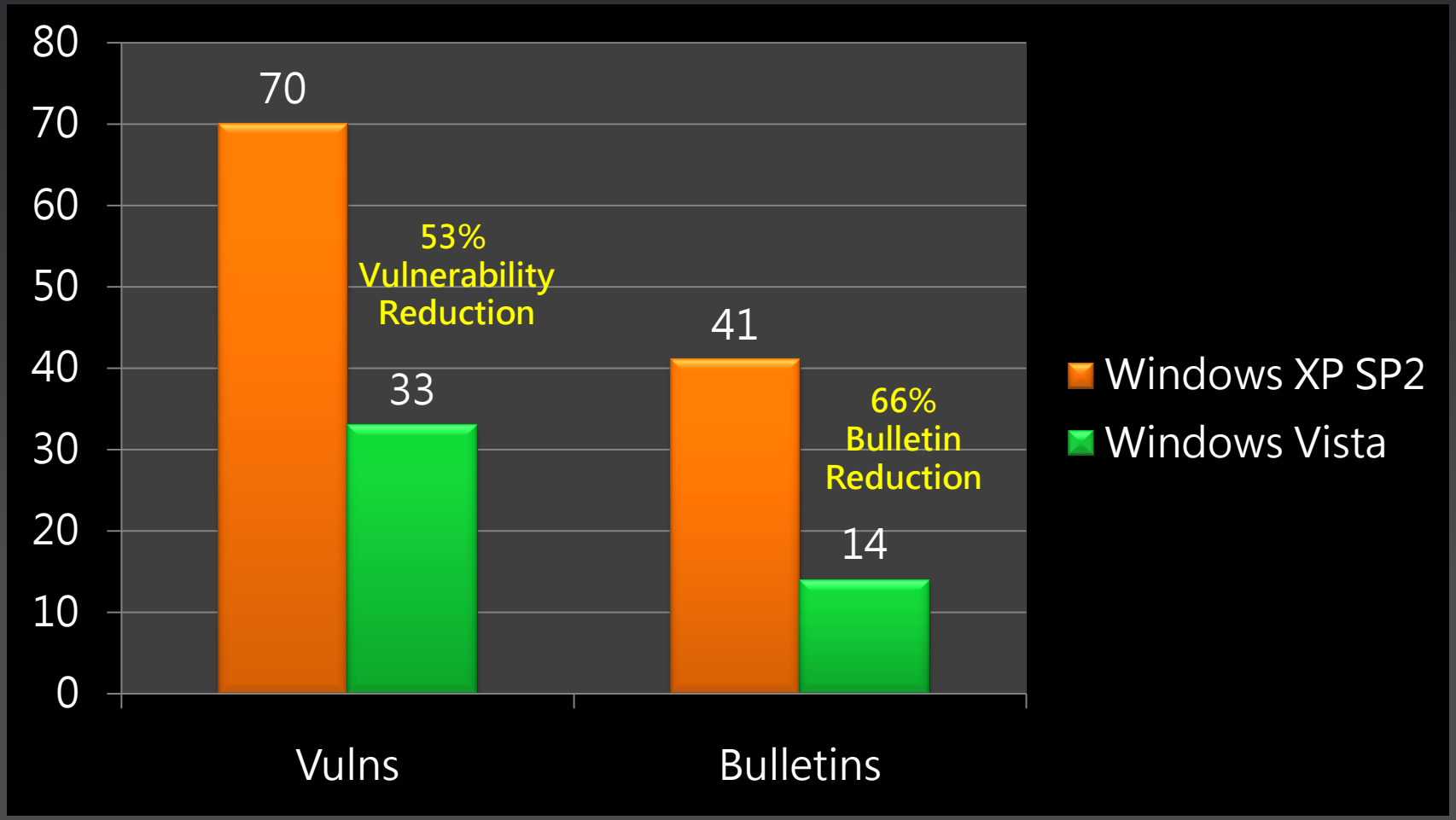
資安風險控管:
Information Lifecycle Management



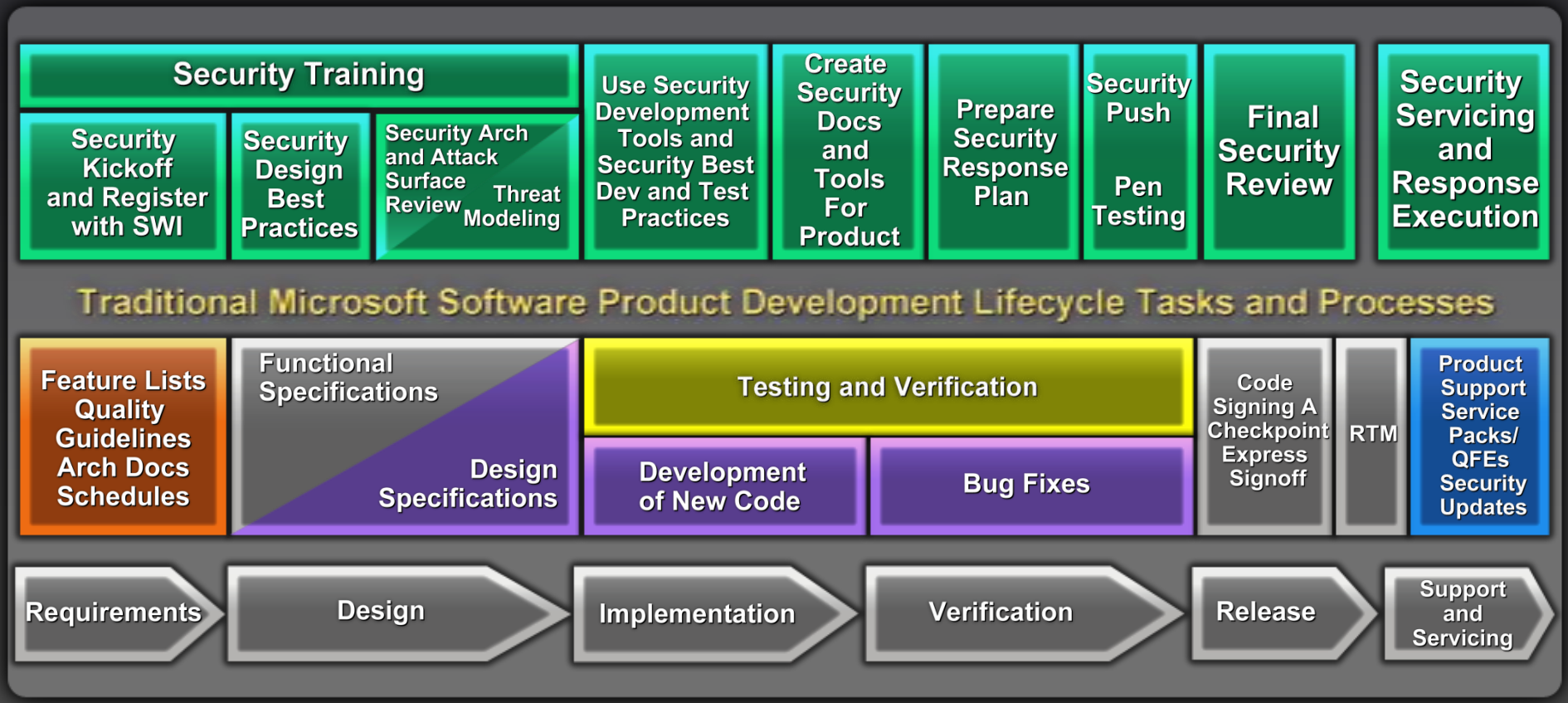
What *IS* the SDL?

- A set of design, development, testing and post-release security and privacy-related software process improvements
- The goal is to improve security and privacy by:
  - » Reducing the number of vulnerabilities in shipping software
  - » Reducing the severity of remaining vulnerabilities
- SDL works!

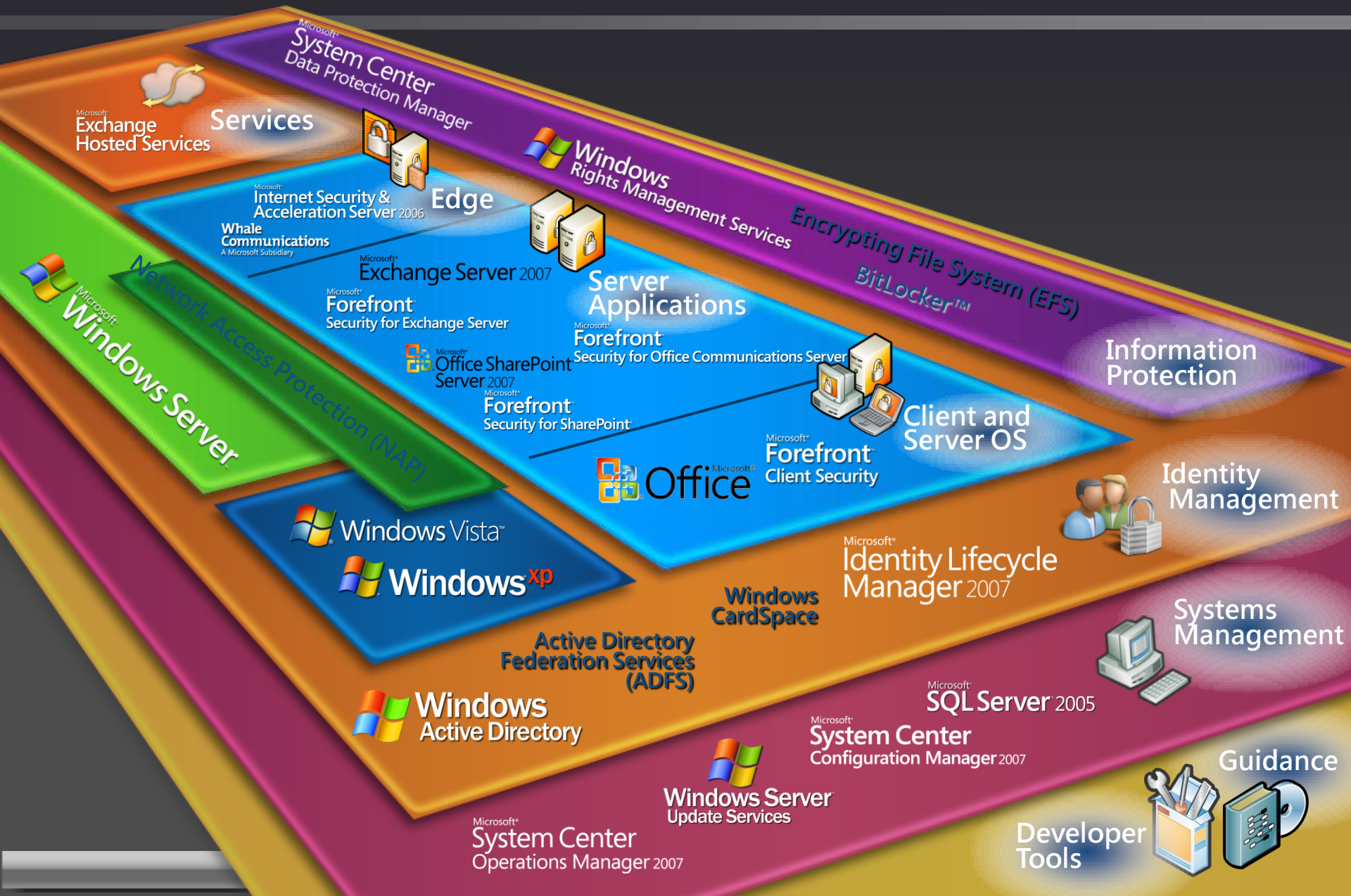
SDL Works!


80
70
60
50
40
30
20
10
0
70
53%
Vulnerability
Reduction
33
41
66%
Bulletin
Reduction
14
Vulns
Bulletins
Windows XP SP2
Windows Vista

Security Development Lifecycle



全盤性的資安架構


Microsoft System Center Data Protection Manager
Windows Rights Management Services
Encrypting File System (EFS)
BitLocker™
Information Protection
Microsoft Exchange Hosted Services
Services
Edge
Microsoft Internet Security & Acceleration Server 2006
Whale Communications
A Microsoft Subsidiary
Microsoft Exchange Server 2007
Microsoft Forefront Security for Exchange Server
Server Applications
Microsoft Forefront Security for Office Communications Server
Microsoft Office SharePoint Server 2007
Microsoft Forefront Security for SharePoint
Microsoft Windows Server
Network Access Protection (NAP)
Office Microsoft
Microsoft Forefront Client Security
Client and Server OS
Identity Management
Windows Vista
Windows xp
Microsoft Identity Lifecycle Manager 2007
Windows CardSpace
Systems Management
Active Directory Federation Services (ADFS)
Windows Active Directory
Microsoft SQL Server 2005
Microsoft System Center Configuration Manager 2007
Guidance
Windows Server Update Services
Developer Tools
Microsoft System Center Operations Manager 2007

2000 資訊安全策略: 資安十大法則

1. 若他人能說服你在你的電腦上執行程式, 則這台電腦將不再屬於你.
2. 若他人能改變你的作業系統配置, 則這台電腦將不再屬於你.
3. 若他人能無限制實體上存取你的電腦, 則這台電腦將不再屬於你.
4. 若你允許他人上傳程式到你的網站, 則這個網站將不再屬於你.
5. 使用弱的密碼只是糟蹋其他強固的防護

資訊安全策略:資安十大法則 (續)

6. 只有當管理者是可信賴時, 電腦才會是安全的
7. Encrypted data is only as secure as the decryption key
8. 過期的掃毒軟體只比沒有掃毒軟體好一點點罷了
9. 不管是在現實生活或網站上, 完全匿名是不切實際的做法
10. 技術不是萬靈藥

2008 重新思考安全性的十大不變法則

- 倘若不肖份子能夠說服使用者執行程式，第1 條法則點出的不是軟體的弱點，而是人性的弱點！關鍵就在「您能不能拒絕誘惑」這一詞。法則的重點是，身為電腦操作員的您，必須為您在該部電腦上執行的軟體負責。如果您安裝了惡意驅動程式或惡意視訊轉碼器，就等於把這部電腦的控制權拱手交給歹徒！

因此除了確保使用者沒有執行系統管理員工作的權限之外，使用者教育也是非常重要的一環。所以，雖然說目前第 1 條法則仍然適用，不過可能得稍微修改一下您電腦的定義。

更改作業系統配，電腦將不在屬於你？

- 作業系統的定義？
- 作業系統已經隨著運算需求的發展而改變複雜化。

更改作業系統中從未用過的一部分，並不會入侵您的電腦，而且作業系統中從未用過的部分可多著呢。

每個 IT 組織必須擁有的 4 項安全性技術

- 風險管理儀表板
  - » SCOM 2007 end to end 監控系統
- 防惡意程式
  - » Vista Defender+ Forefront Security
- 網路異常偵測
  - » 防火牆, 防毒牆(ISA + Web Monitor)
- 目標建構管理
  - » 良好的 資安系統應該自動掃描網路，確定新系統適當部署，並驗證已建立的系統保持符合規範。

Microsoft Security Center Of Excellence(SCO)

1. 存取內部資料前前做好身分認證及資產分類。
   - ✓ Before: IT 部門間各管各的
   - ✓ Now : V-Team

2. 建立資產擁有者管理制度。
   - ✓ Before: system administrator或是電腦維修人員
   - ✓ Now: Business Group 也需要被納入電腦資產管理所有人。

3. 清楚界定基本資安系統需求的建立的健全與完整。
4. 設立的資安法規是可被執行與評估。
5. 確實的執行法規

免費資源分享

Review Guidance

SDL:

» http://msdn.microsoft.com/en-us/security/cc448177.aspx

Resources and Training

» http://msdn.microsoft.com/en-us/security/cc448120.aspx

» http://www.microsoft.com/technet/security/map/default.mspx

<include industry specific guidance>

Learn from MSIT Showcase: (how Microsoft does Security)

- http://www.microsoft.com/technet/itshowcase/default.mspx

Register for Important Security Updates & Newsletters:

» http://www.microsoft.com/security/bulletins/alerts.mspx

Bedankt

谢谢您

Thank You!

Grazie

Danke

Merci

謝謝您

Takk

Obrigado

Gracias

Microsoft®

Your potential. Our passion.™