數聯資安股份有限公司

Information Security Service Digital United, Inc.

為何世界需要 IPS -

混亂的網路時代 需要真正的英雄!

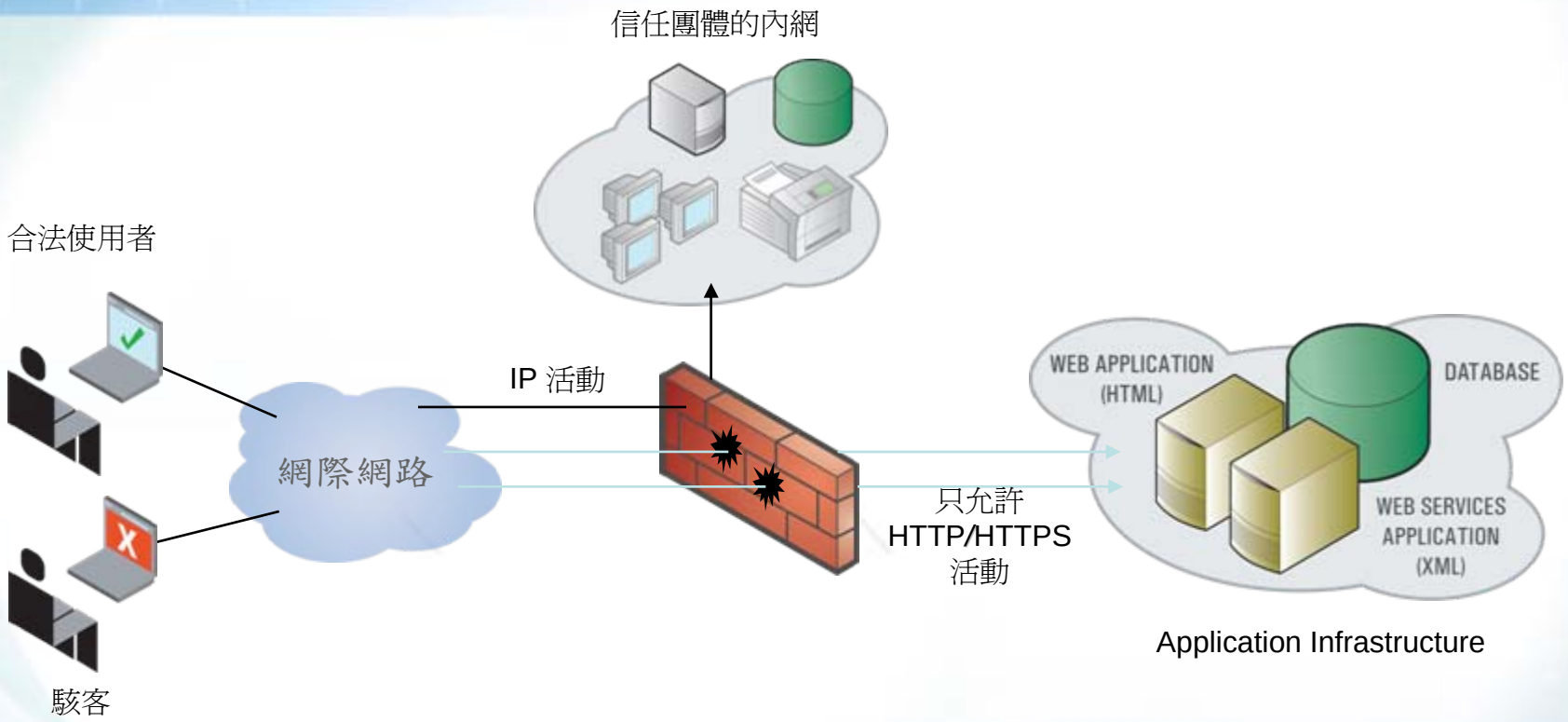
大綱

Information
Security Service
Digital United

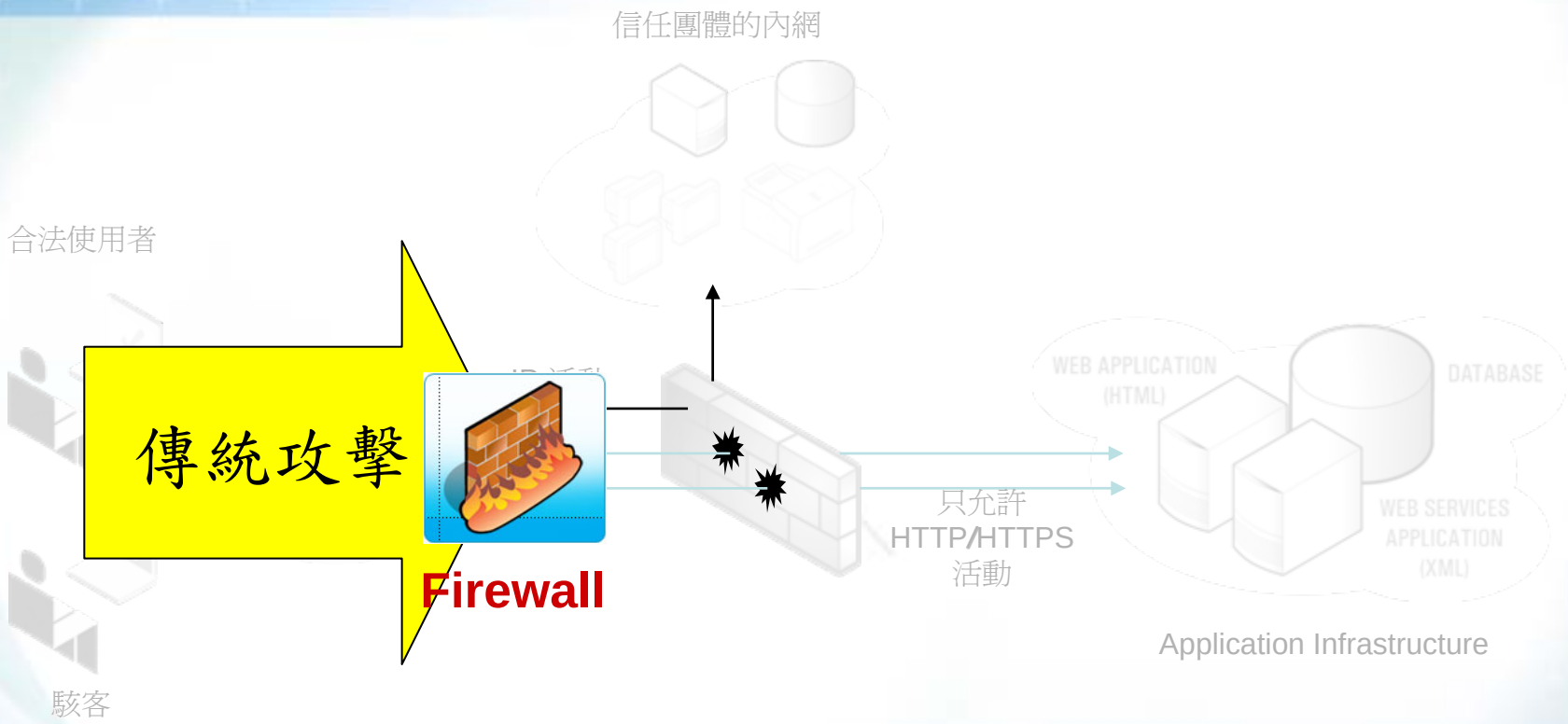
- 傳統防禦架構
- 企業對IPS的期望
- 異常偵測技術的利用
- IPS 的管理態度
- 資安防護的未來

基礎防禦架構

基礎安全架構

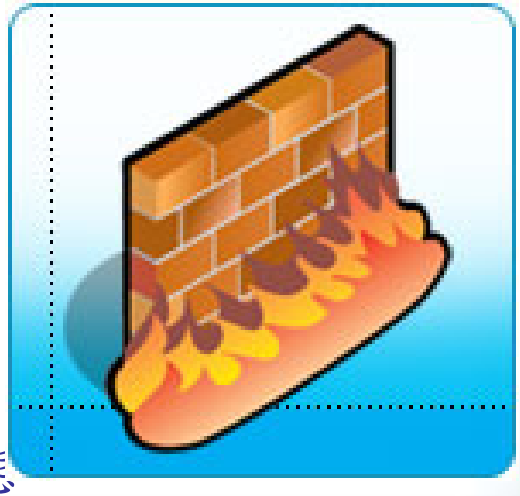

信任團體的內網
合法使用者
IP 活動
網際網路
只允許
HTTP/HTTPS
活動
WEB APPLICATION
(HTML)
DATABASE
WEB SERVICES
APPLICATION
(XML)
Application Infrastructure
駭客

駭客攻擊

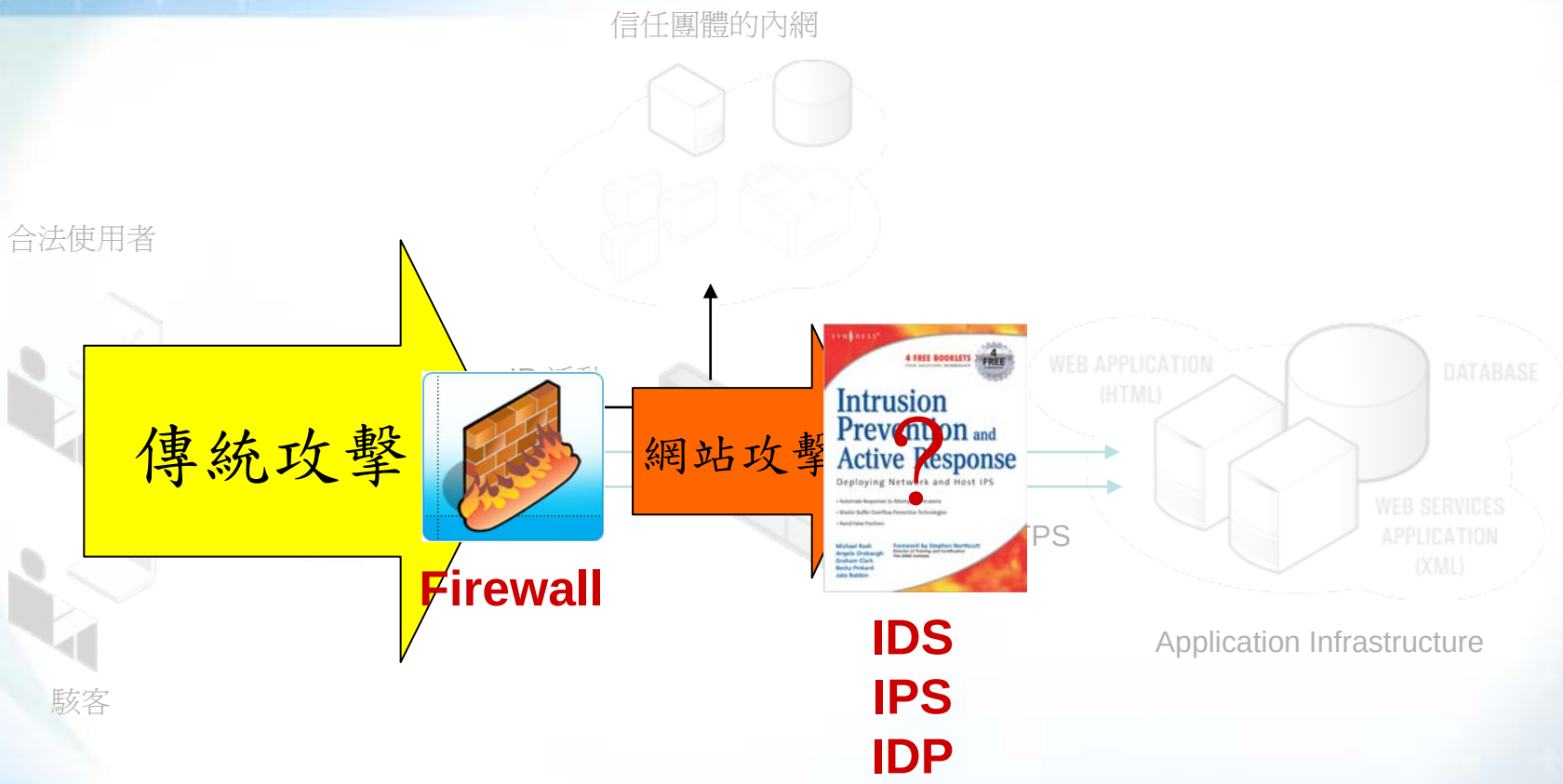

信任團體的內網
合法使用者
傳統攻擊
Firewall
只允許
HTTP/HTTPS
活動
WEB APPLICATION
(HTML)
DATABASE
WEB SERVICES
APPLICATION
(XML)
Application Infrastructure
駭客

封包過濾式防火牆

- 正面表列式，放行正常行為
- 靜態過濾(Static Packet Filtering)
  - 來源位址(Source IP)、
  - 來源埠號(Source Port)、
  - 目標位址(Destination IP)、
  - 來源埠號(Destination Port)、
  - 允許活動(Action allow/deny)
- 動態過濾(Dynamic Packet Filtering)
  - 除檢查上述參數外，還需記錄並檢查連線狀態

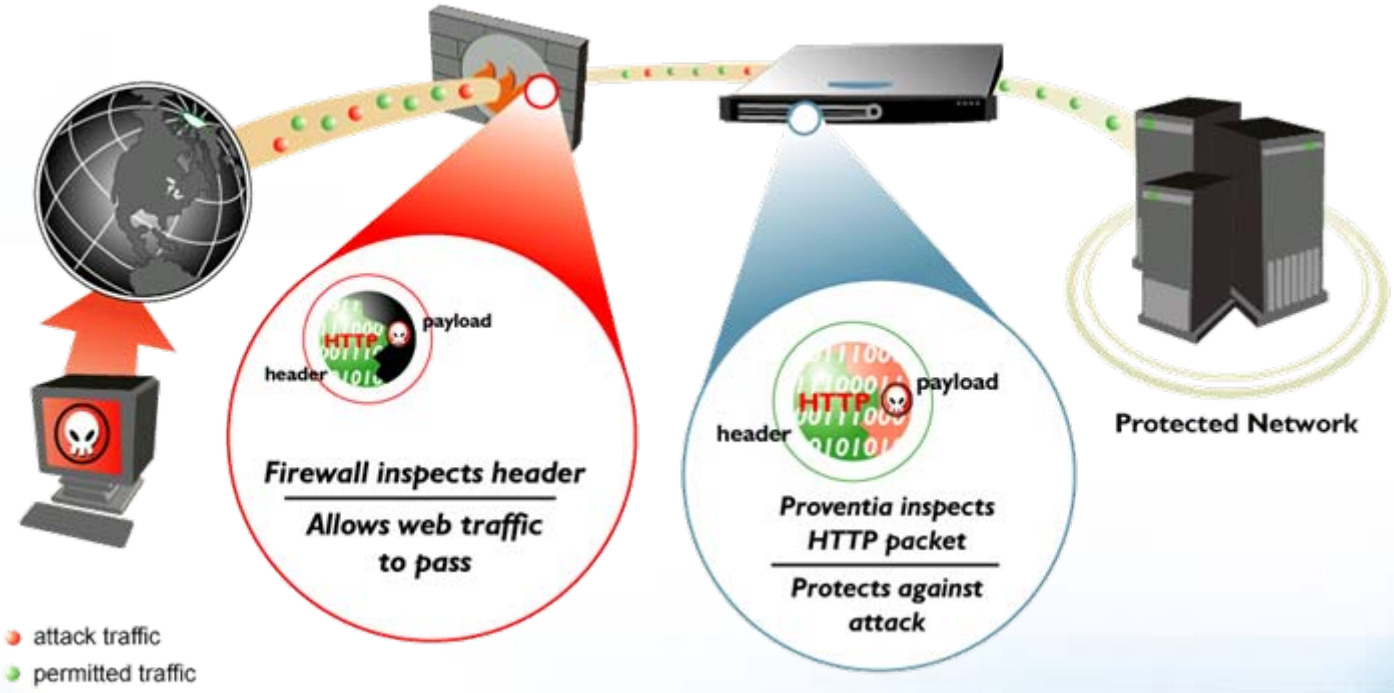


駭客攻擊

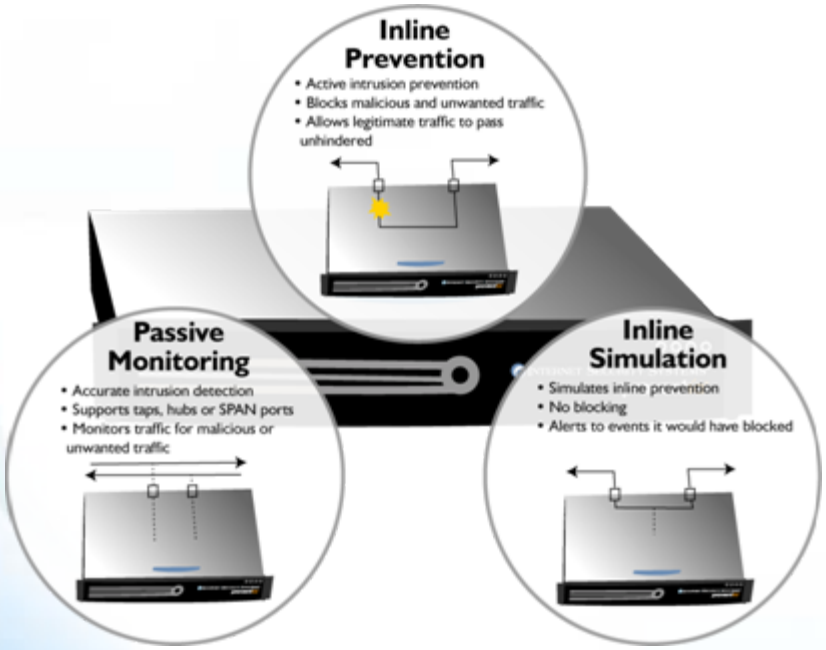


避過Layer 4(IP)層的限制，針對所開啟的埠號進行攻擊

入侵偵測與防禦系統


payload
HTTP
header
Firewall inspects header
Allows web traffic to pass
payload
HTTP
header
Proventia inspects HTTP packet
Protects against attack
Protected Network
attack traffic
permitted traffic

入侵偵測與防禦系統



- 原始需求：防駭
- 直接丟棄或阻絕惡意行為
- 利用封包竊聽技術
- 狀態式通訊協定的解碼與分析技術
- 可偵測檢查TCP/IP所有7層的封包內容
- 具有學習機制
- 前身：
  - IDS：只能偵測攻擊
  - IDS-Switch/IDS-Firewall ：與交換器/防火牆整合防禦的過渡方案，不利於防駭，但利於防DoS與L4以下的限速管理

特徵偵測(Signature-Based)

負面表列式，使用模式比對法(Pattern Matching)，將收集到的資訊與特徵資料庫進行比對

防毒、防木馬軟體亦採用類似概念

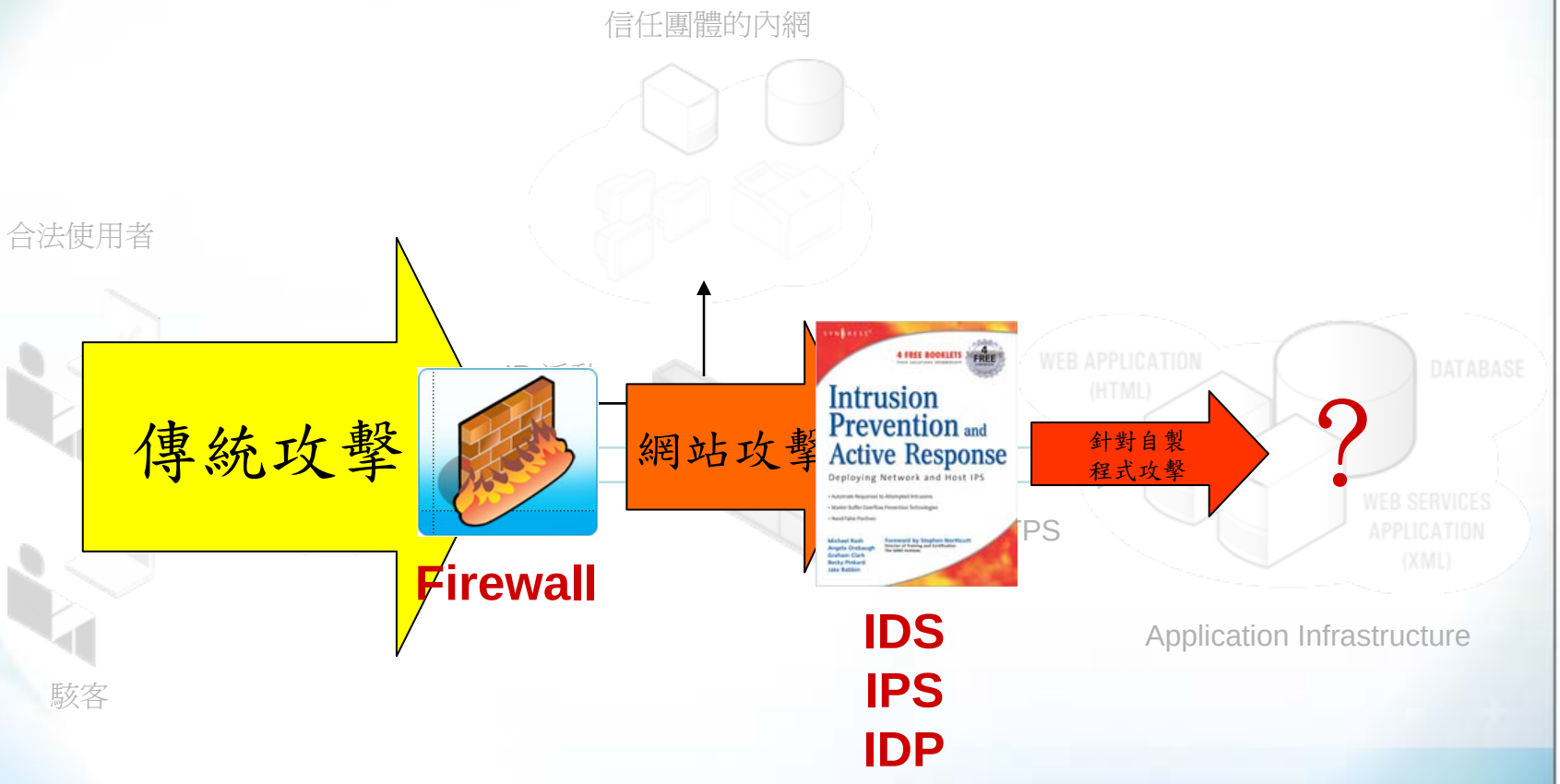
例：

✓ /a.asp?../winnt\system32\cmd.exe
✓ /a.asp?AAAA….AAA%90…cmd.exe

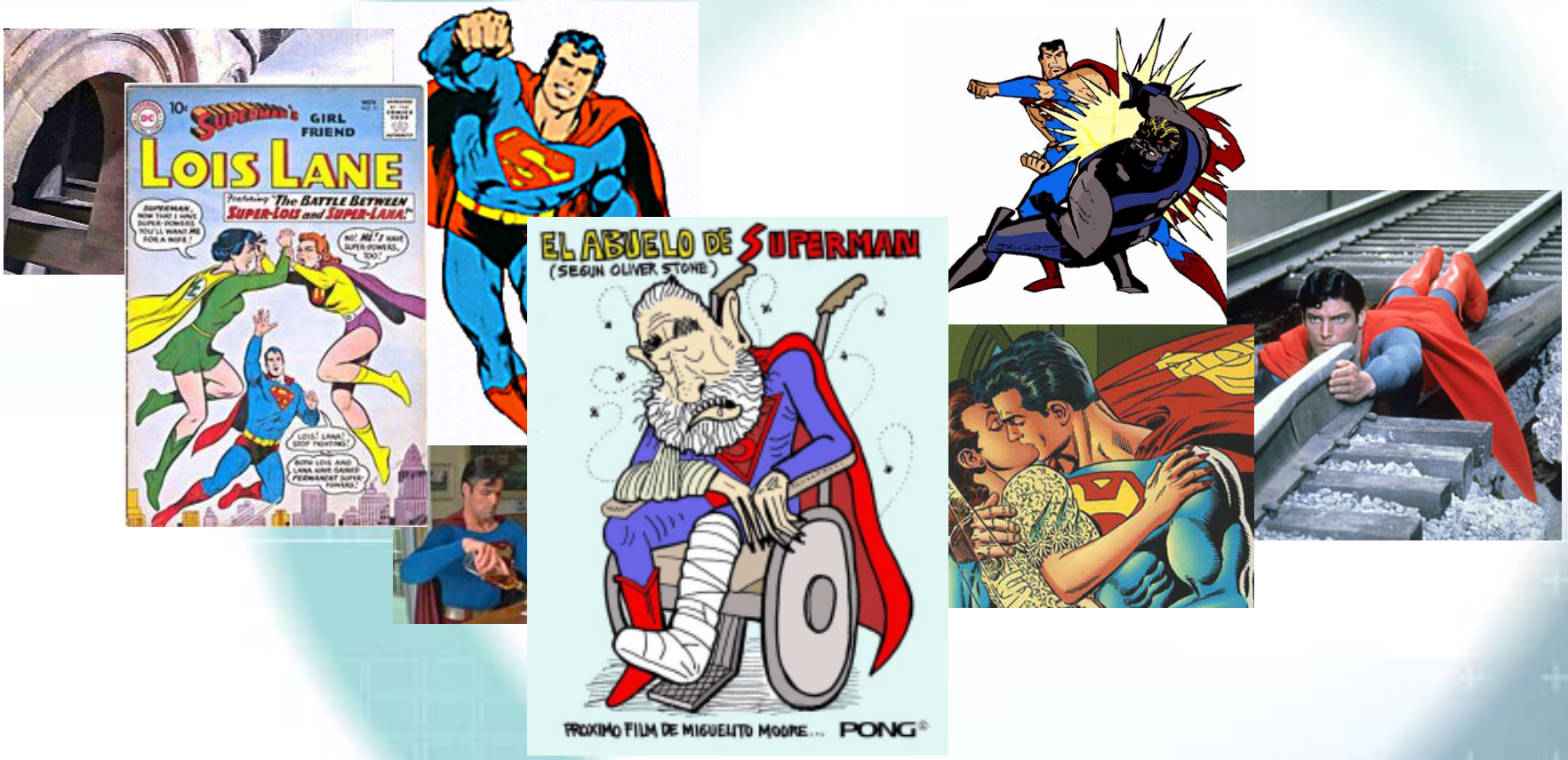
變型：

× /a.asp?..%2Fwinnt%5Csystem32%5Ccmd.exe
× /a.asp?..%255Fwinnt%255Csystem32%255Ccmd.exe
× /a.asp?..%c0%afwinnt%c1%9csystem32%c1%9ccmd.exe
× /a.asp?ABC.....CCC%25..cmd.exe

攻擊趨勢與需求



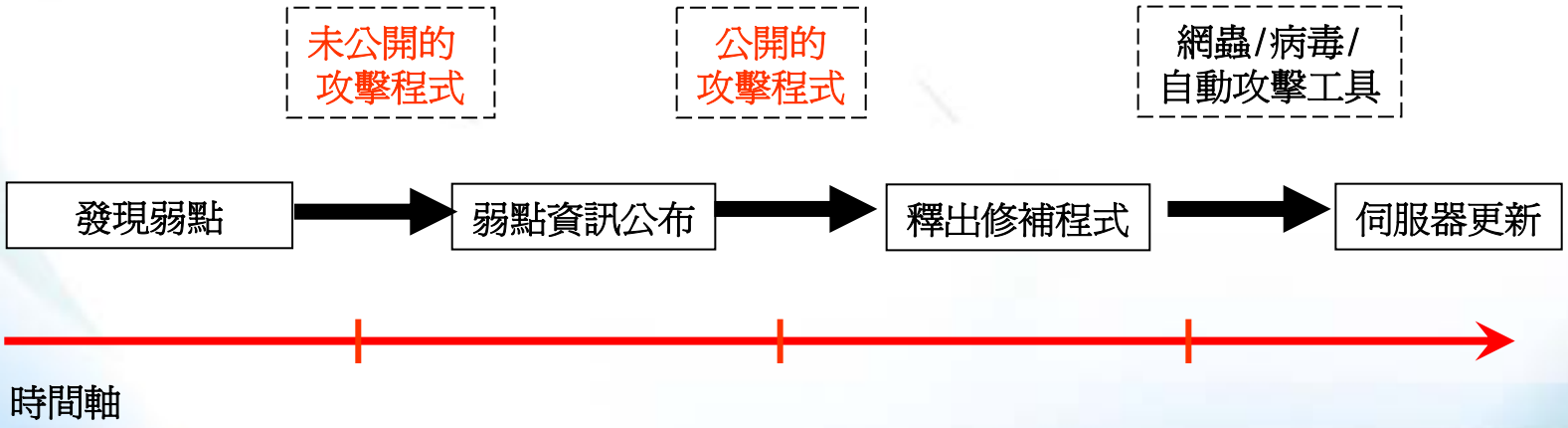
專屬於各網站或自有系統的弱點，並非廣為人知的系統漏洞或攻擊手法


SUPERMAN'S GIRL FRIEND
LOIS LANE
EL ABUELO DE SUPERMAN
(SEGUN OLIVER STONE)
PROXIMO FILM DE MIGUELITO MOORE... PONG

企業對IPS的期望

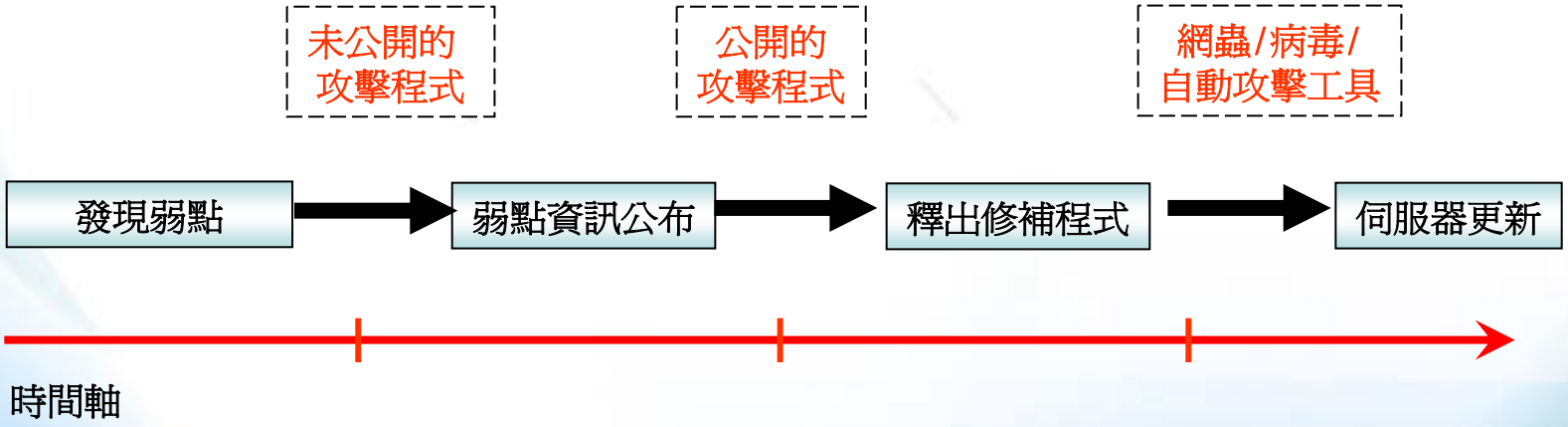
零時差攻擊(0-day Exploit)

- 針對尚未開發修補程式的漏洞，所寫出的攻擊程式



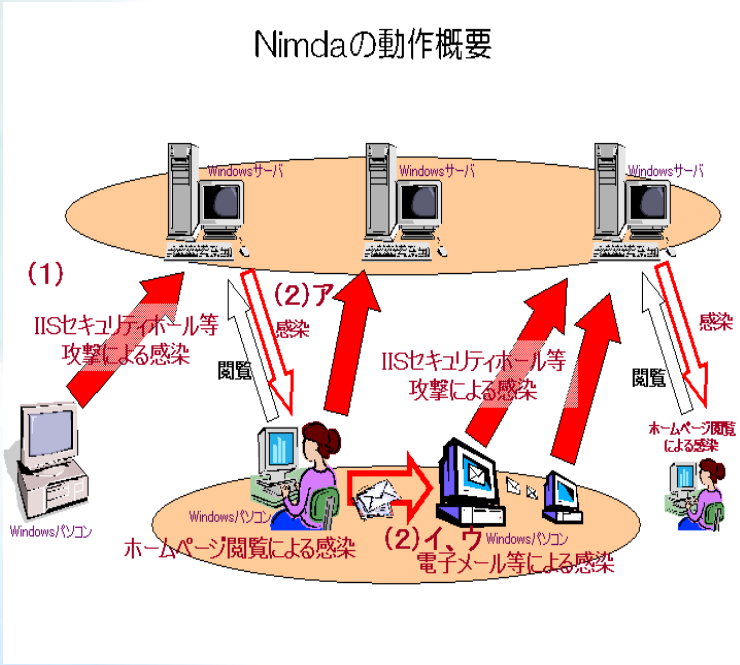
零時差攻擊(0-day Exploit)防禦

- 0-Day 防禦計劃
  - IPS廠商競購漏洞資訊以降低0-Day攻擊程式出現的可能。
  - 雇用更多的駭客和研究員先找出漏洞
- 虛擬修補(Virtual Patch)
  - 特徵偵測：在系統修補前由IPS防禦
  - 異常偵測：由行為面進行防範？



防毒、防蠕蟲

- 透過郵件與網頁下載後門與病毒程式
- 網蟲透過網路散佈
- 特徵偵測：
  - 可偵測利用安全漏洞的網蟲
  - 可偵測具有掃瞄行為的網蟲
  - 針對所有網蟲與病毒寫偵測碼?(AV困境)
  - 利用網路分享散佈的網蟲？
  - 只作破壞（例：亂列印）的網蟲？
  - 包含反彈式木馬的網蟲？



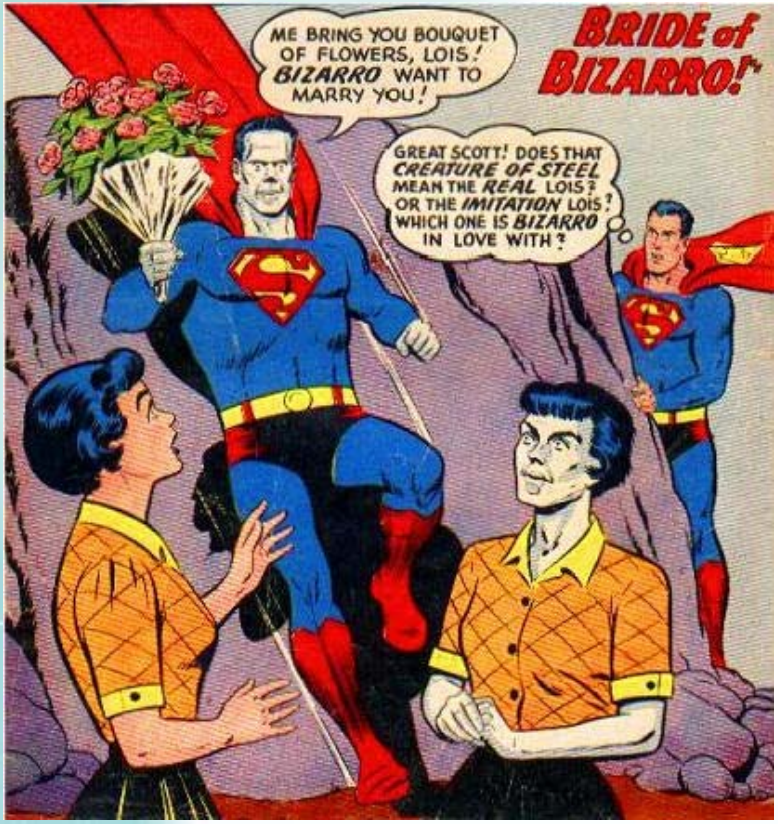
人員行為稽核和控管

- 非必要網站
- 內部的file/FTP server？
- 點對點軟體(P2P) ？
- 使用盜版軟體或媒體？

- 即時通訊軟體(IM) ？
  - 軟體版本不斷更新：MSN, Skype…
  - 難以分析的特殊協定：Skype
- 稽核？監控？阻擋？控管？

客製化政策

- 偵測使用者密碼太短？
- 偵測網頁是否洩露個人機密？
- 偵測機密文件的傳輸？
- 偵測特定文字或信件內容？
- 偵測程式碼的上傳？
- 解析自有應用協定？
- 針對自有應用程式的攻擊？


ME BRING YOU BOUQUET OF FLOWERS, LOIS! BIZARRO WANT TO MARRY YOU!
BRIDE of BIZARRO!
GREAT SCOTT! DOES THAT CREATURE OF STEEL MEAN THE REAL LOIS? OR THE IMITATION LOIS? WHICH ONE IS BIZARRO IN LOVE WITH?

異常偵測技術的利用

異常偵測(Anomaly-Based)

- 也稱為Statistical-Based、Profile-Based
- 利用IDS或監控工具觀察並列明正常與異常行為
- 利用統計模式或專家系統概念，定義異常行為基準線(Baseline, Profile)
  - Traffic Based
  - Protocol Based
  - Behavior Based
  - Etc…

異常偵測範例

- 偵測網路活動量、信件數量等網路行為的異常
  - 阻絕服務攻擊(Dos)?
  - 大量網路掃瞄(Scan)?
  - 郵件炸彈(Mail Bomb)?
  - 大量網路登入失敗？

異常偵測範例

- 偵測應用程式行為的異常
  - 例：信件中附檔含有雙檔名(gif.exe, tar.gz)？
  - 例：附信名與格式不符(cutegif為執行檔)？
  - 例：所傳送的執行檔使用UPX加殼保護？
  - 例：意圖遠端傳送程式(exe, com, bat, pif…)？
  - 例：程式自行呼叫 Outlook 寄送信件？
  - 例：網址目標與連結不符？

異常偵測範例

- 偵測使用行為的異常
  - 例：使用80埠號但未使用HTTP協定(後門、IM、P2P)
  - 例：輸入密碼小於8
  - 例：在網址列含有<script>、cmd.exe等字串
  - 例：在網址列含有xp_cmdshell字串
  - 例：連接後台網站http://target/admin/login.asp

異常偵測範例

- 偵測回應內容的異常
  - 網頁回應裏包含身分證號與信用卡號
  - 網頁被換
  - 網頁內具有<iframe>語法
  - 網頁回應裏敏感錯誤訊息
  - Windows Shell Banner
  - 阻擋敏感性字眼的洩露
    - Microsoft OLE DB Provider for ODBC Drivers 錯誤'80040e14' [Microsoft][ODBC SQL Server Driver][SQL Server]
    - Hacked By…
    - Personal Email

IPS 的管理態度

業務的廣告用語

- IPS 初始設定完之後就可自行作業，只有在網路架構變動時才需要調整

  -- 以前是賣防火牆的業務

- IPS 只要設定好自動更新，隨時更新特徵碼就不用害怕了

  -- 以前是賣防毒產品的業務

- IPS 設定簡易，架設容易，安裝完後就大功告成，不會擔心被入侵了

  -- 以前是賣網路設備的業務

真正的需求？

- 你需要：
  - 防駭？
  - 零時差攻擊(0-day Exploit)防禦？
  - 防毒、防蠕蟲？
  - 人員行為稽核和控管？
  - 客製化政策？
- 思考：
  - 是為了符合規定購買資安產品？
  - 如何切合我的環境？
  - 如何展現防護績效？

IPS需要

- 了解自有的網路、應用程式、使用者環境
- 定義正常狀態，進行偵測政策的初始調整
- 隨時觀察以分析事故與自身風險的狀況
- 調整偵測政策以因應企業營運現況
- IPS的永續運作與維護政策
- IPS的分析結果與事故處理流程

資安防護的未來

IPS強化的未來趨勢

- Attack Mitigation Systems(AMS)
- Application-based Firewall(加密)
- Proxy / Reverse Proxy
- Personal oriented protection HW/SW
- OS Bulit-in Security
- Unified Threat Management (UTM)
- Security Information Management (SIM)
- Security Operation Center

強化正面防守

負面表列

- 阻擋惡意的網頁要求
- 設定較為簡易
- 保證50%的網頁安全
- 只能針對明顯惡意行為，無法阻擋正常網頁要求中的惡用活動
- 無法偵測使用者或管理者設定上的問題

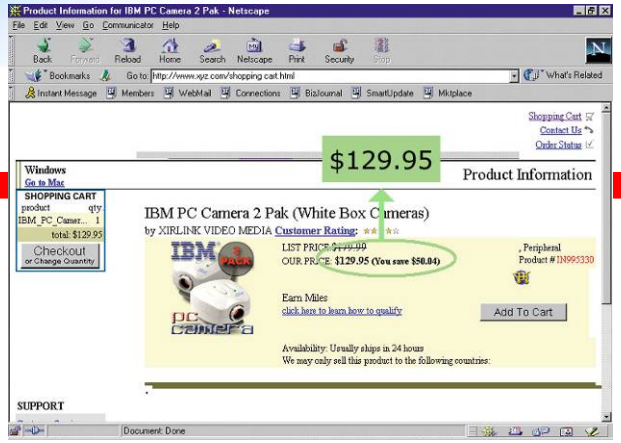
結合正面表列

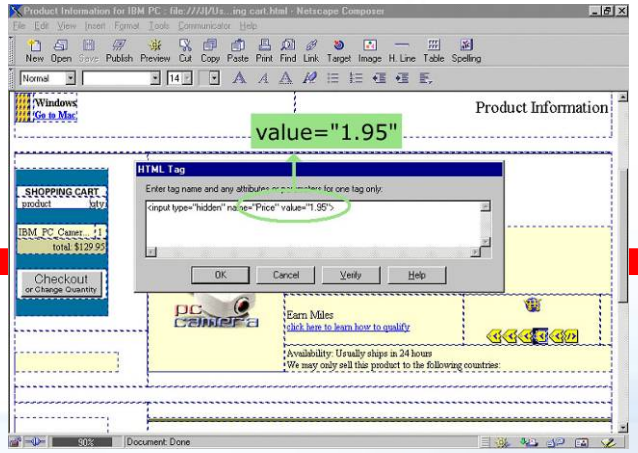
- 防火牆與入侵偵測概念的混合應用，正面決定可提供的資源清單
  - 例：只允許表列的網址作為網站進入點：
    允許： http://www.target.com/index.htm
    不允許：http://www.target.com/admin/index.htm
- 毋需針對不同伺服器撰寫多種攻擊特徵
- 毋需經常性維護與更新
- 針對各使用者介面客製化，提供較多偵測功能與調整彈性
- 確保99%的網頁安全

中介防禦機制

- 程式面：
  - 修改原始程式碼
  - 外掛檢查用程式碼
- 軟體面：
  - 使用Web Code Review 軟體
  - URLScan(Microsoft IIS)
  - mod_security(Apache)
- 硬體面：
  - 網頁式防火牆(Web Application Firewall)
  - 反向式代理伺服器(Reverse Proxy)


Make GahooYoogle your home page
Add GahooYoogle to your Favorites
GAHOOYOOGLE
Search Google & Yahoo at the same time.
Web Images Videos News Shopping Directory Answers Blogs
GahooYoogle it!
Advertisement: Get paid for surfing the web.
Why to use GahooYoogle?
Try the easiest search yet.
Save your time, get more results in less time.
Your search will be faster and more reliable.
How to remember the name and spelling of GahooYoogle?
A little "poem", you will never forget GahooYoogle:
Write Yahoo then Google
Make the Y and G Toggle
Never forget GahooYoogle


Product Information for IBM PC Camera 2 Pak - Netscape
$129.95
Product Information
IBM PC Camera 2 Pak (White Box Cameras)
Add To Cart
SUPPORT


value="1.95"
Product Information
HTML Tag
OK
Cancel
Verify
Help
Checkout

轉址

http://www.gov.tw/moa

http://www.gov.tw/mob

http://www.gov.tw/moc

http://moa.gov.tw/

http://mob.gov.tw

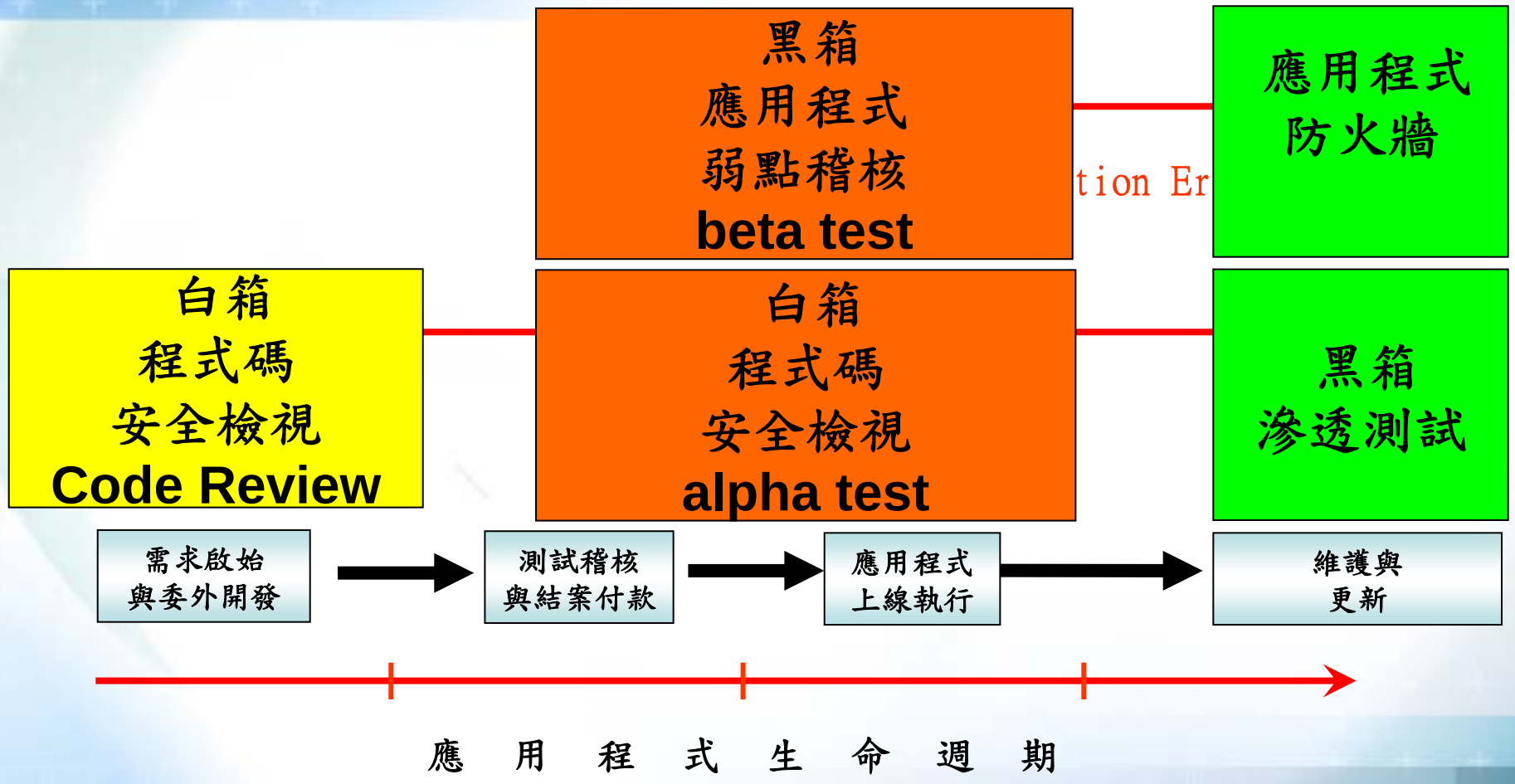
http://moc.gov.tw

http://www.gov.tw

網頁式防火牆

防黑長城？

事後丸誠可貴，小雨衣更可靠



問題與討論