摔不壞的雞蛋籃

雲端網站集中化的保障

雲端雞蛋籃

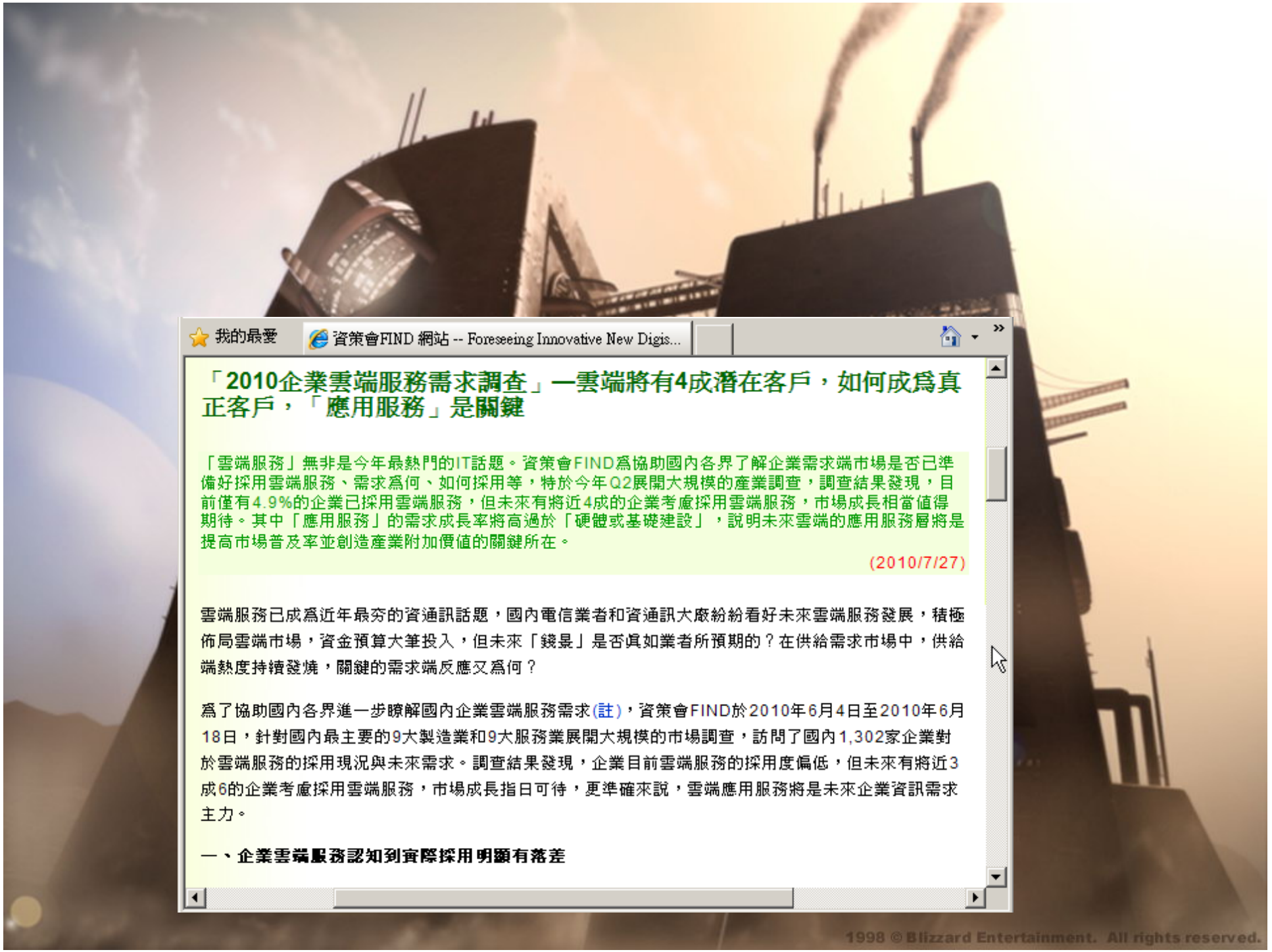
進出兩面擋

防火又防洪

多工靠專家


雲端雞蛋籃

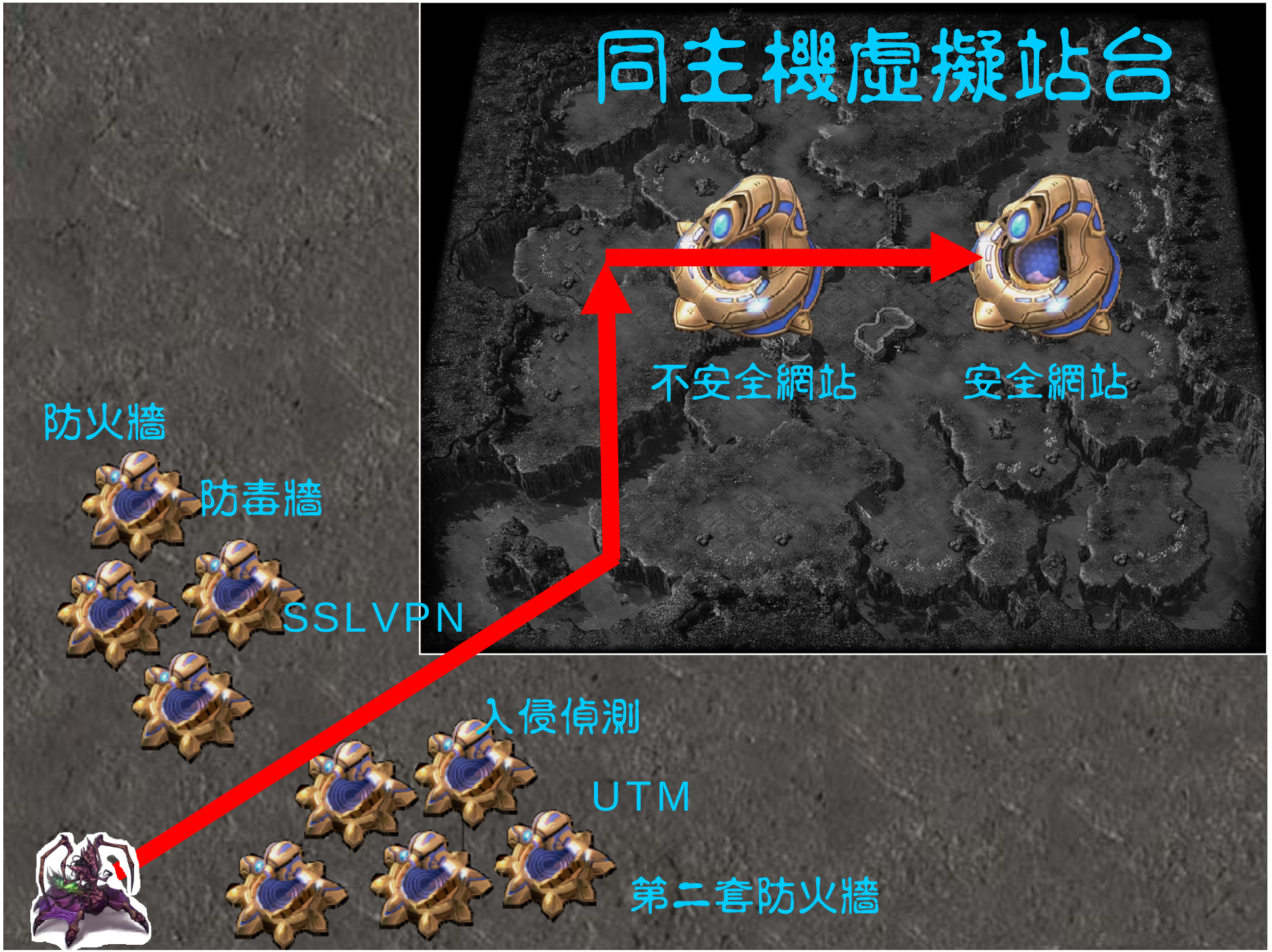

基礎架構服務化(IaaS)
主機代管再擴大
Amazon EC2
虛擬機
私有雲
1998 © Blizzard Entertainment. All rights reserved.

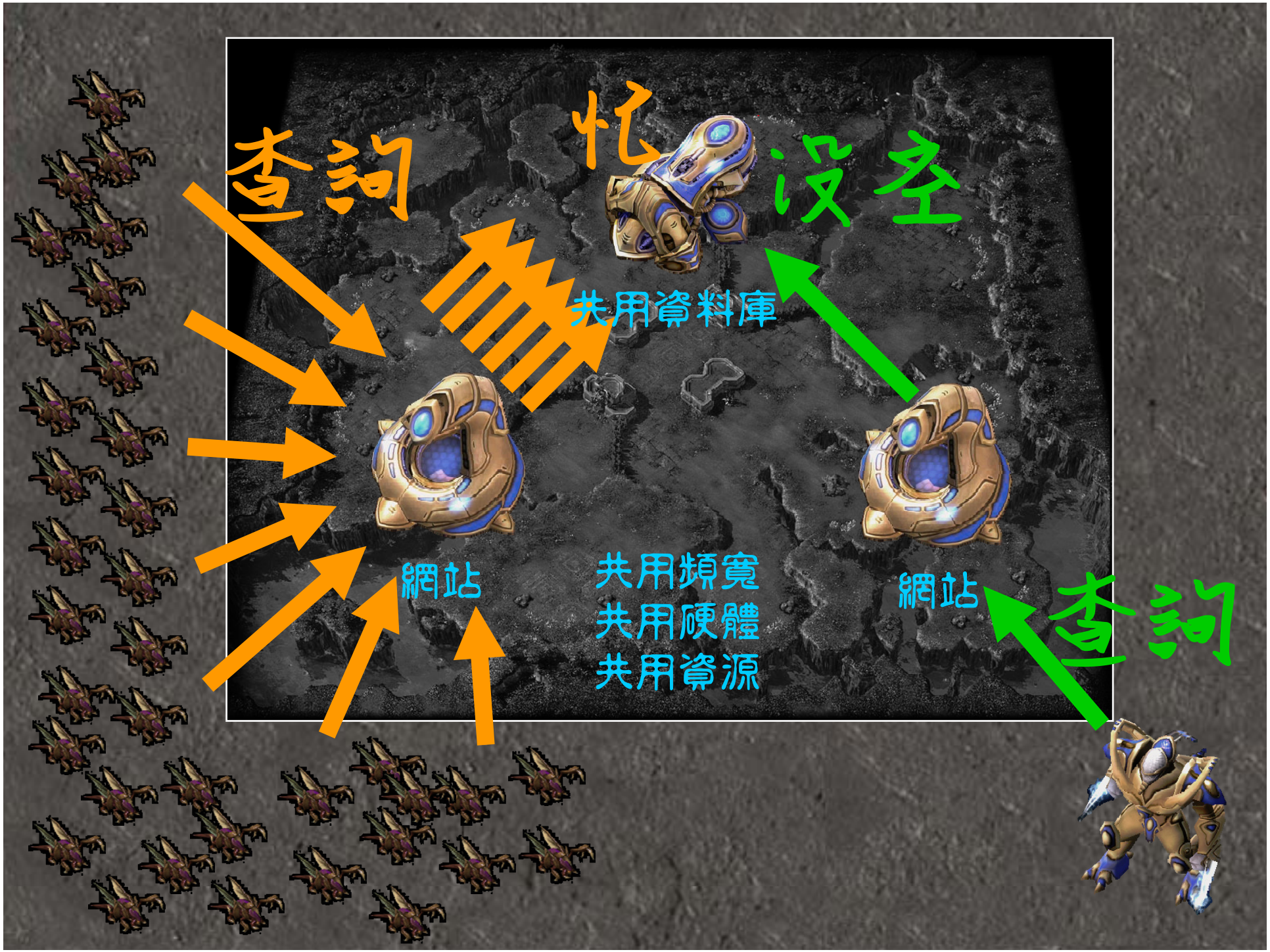

我的最愛
資策會FIND 網站 -- Foreseeing Innovative New Digis...
「2010企業雲端服務需求調查」—雲端將有4成潛在客戶，如何成爲真正客戶，「應用服務」是關鍵
「雲端服務」無非是今年最熱門的IT話題。資策會FIND爲協助國內各界了解企業需求端市場是否已準備好採用雲端服務、需求爲何、如何採用等，特於今年Q2展開大規模的產業調查，調查結果發現，目前僅有4.9%的企業已採用雲端服務，但未來有將近4成的企業考慮採用雲端服務，市場成長相當值得期待。其中「應用服務」的需求成長率將高過於「硬體或基礎建設」，說明未來雲端的應用服務層將是提高市場普及率並創造產業附加價值的關鍵所在。
(2010/7/27)
雲端服務已成爲近年最夯的資通訊話題，國內電信業者和資通訊大廠紛紛看好未來雲端服務發展，積極佈局雲端市場，資金預算大筆投入，但未來「錢景」是否眞如業者所預期的？在供給需求市場中，供給端熱度持續發燒，關鍵的需求端反應又爲何？
爲了協助國內各界進一步瞭解國內企業雲端服務需求(註)，資策會FIND於2010年6月4日至2010年6月18日，針對國內最主要的9大製造業和9大服務業展開大規模的市場調查，訪問了國內1,302家企業對於雲端服務的採用現況與未來需求。調查結果發現，企業目前雲端服務的採用度偏低，但未來有將近3成6的企業考慮採用雲端服務，市場成長指日可待，更準確來說，雲端應用服務將是未來企業資訊需求主力。
一、企業雲端服務認知到實際採用明顯有落差
1998 © Blizzard Entertainment. All rights reserved.


基礎架構服務化(IaaS)
旁注攻擊
代管再擴大
Amazo
流量癱瘓
虛擬
私有雲
1998 © Blizzard Entertainment. All rights reserved.


代管機房
只能攻擊網站
資料庫
郵件主機
AD主機
感染
竊聽
劫持篡改
防火牆
防毒牆
SSLVPN
什麼都可以攻擊
網站
入侵偵測
UTM
第二套防火牆


虛擬環境
更難偵測
V資料庫
V郵件主機
V-AD主機
感染
竊聽
篡改封包
防火牆
防毒牆
SSLVPN
V網站
入侵偵測
UTM
VCenter
第二套防火牆


同主機虛擬站台
不安全網站
安全網站
防火牆
防毒牆
SSLVPN
入侵偵測
UTM
第二套防火牆


查詢
忙
沒空
共用資料庫
網站
共用頻寬
共用硬體
共用資源
網站
查詢

平台服務化(PaaS)

軟體服務化(Saas)

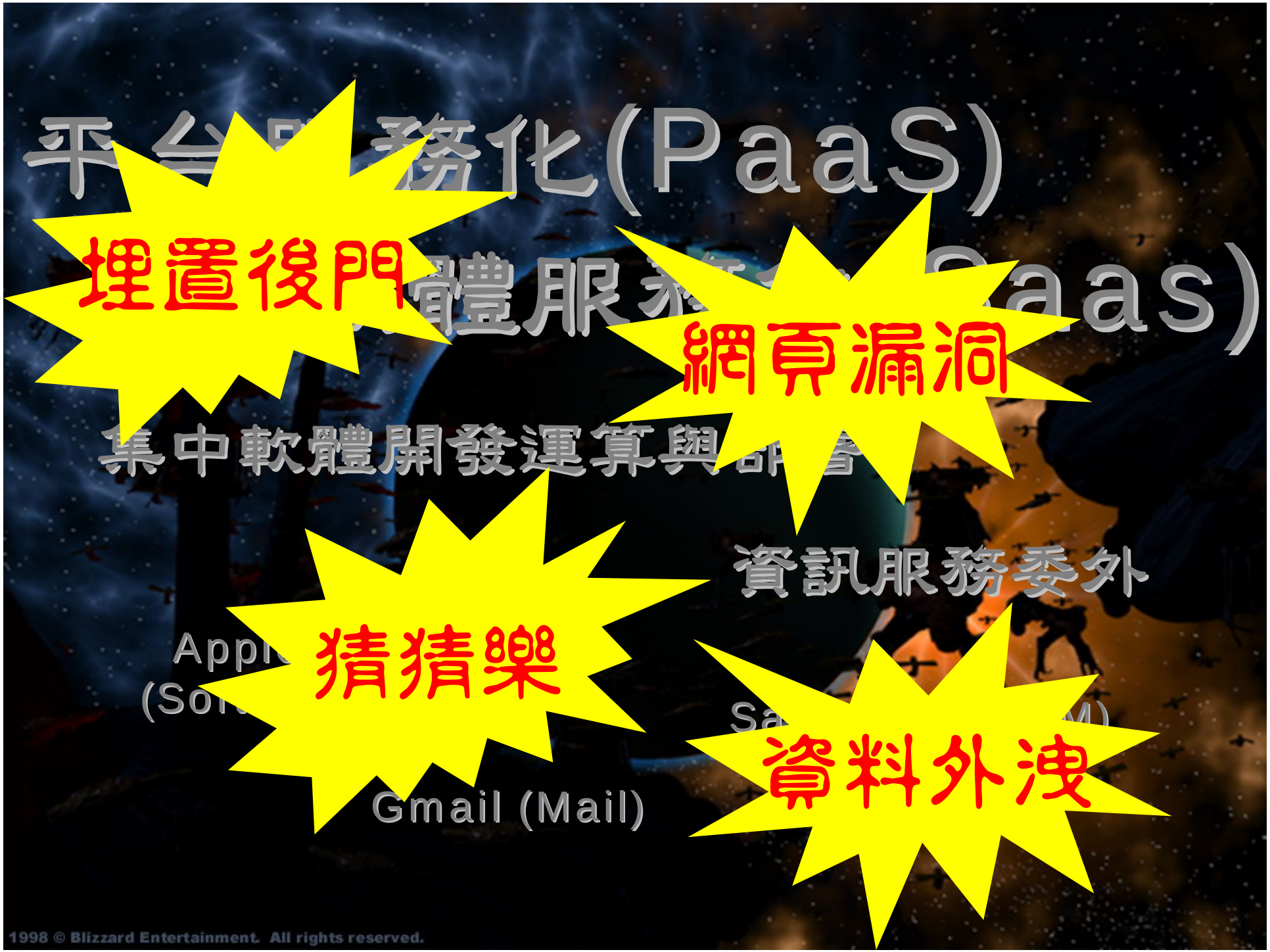
集中軟體開發運算與部署

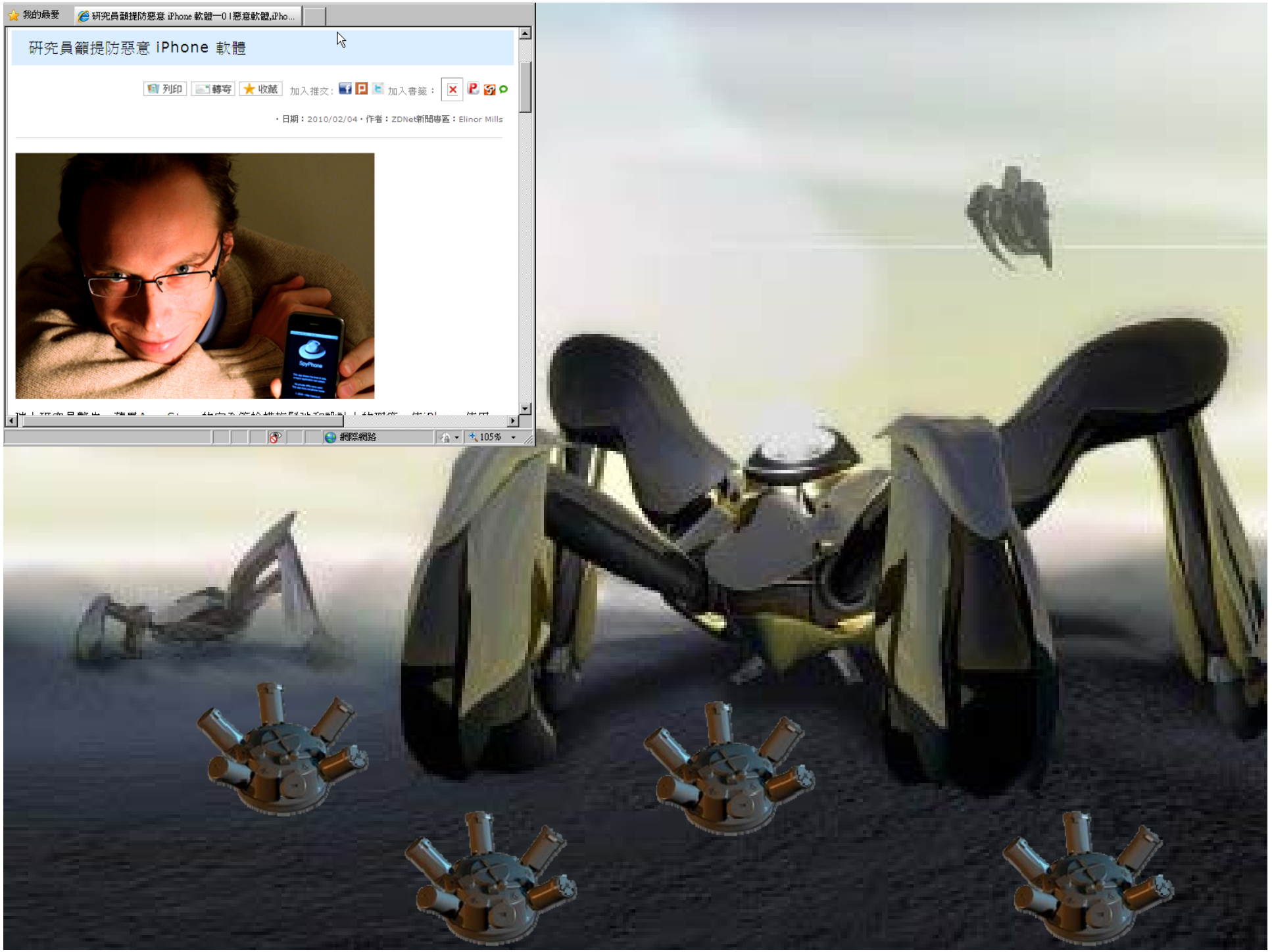
資訊服務委外

Apple Store
(Software/API)

Salesforce(CRM)

Gmail (Mail)


平台服務化(PaaS)
體服務(Saas)
集中軟體開發運算與部署
資訊服務委外
Appl
(Sof
Sa
M)
Gmail (Mail)
埋置後門
網頁漏洞
猜猜樂
資料外洩
1998 © Blizzard Entertainment. All rights reserved.

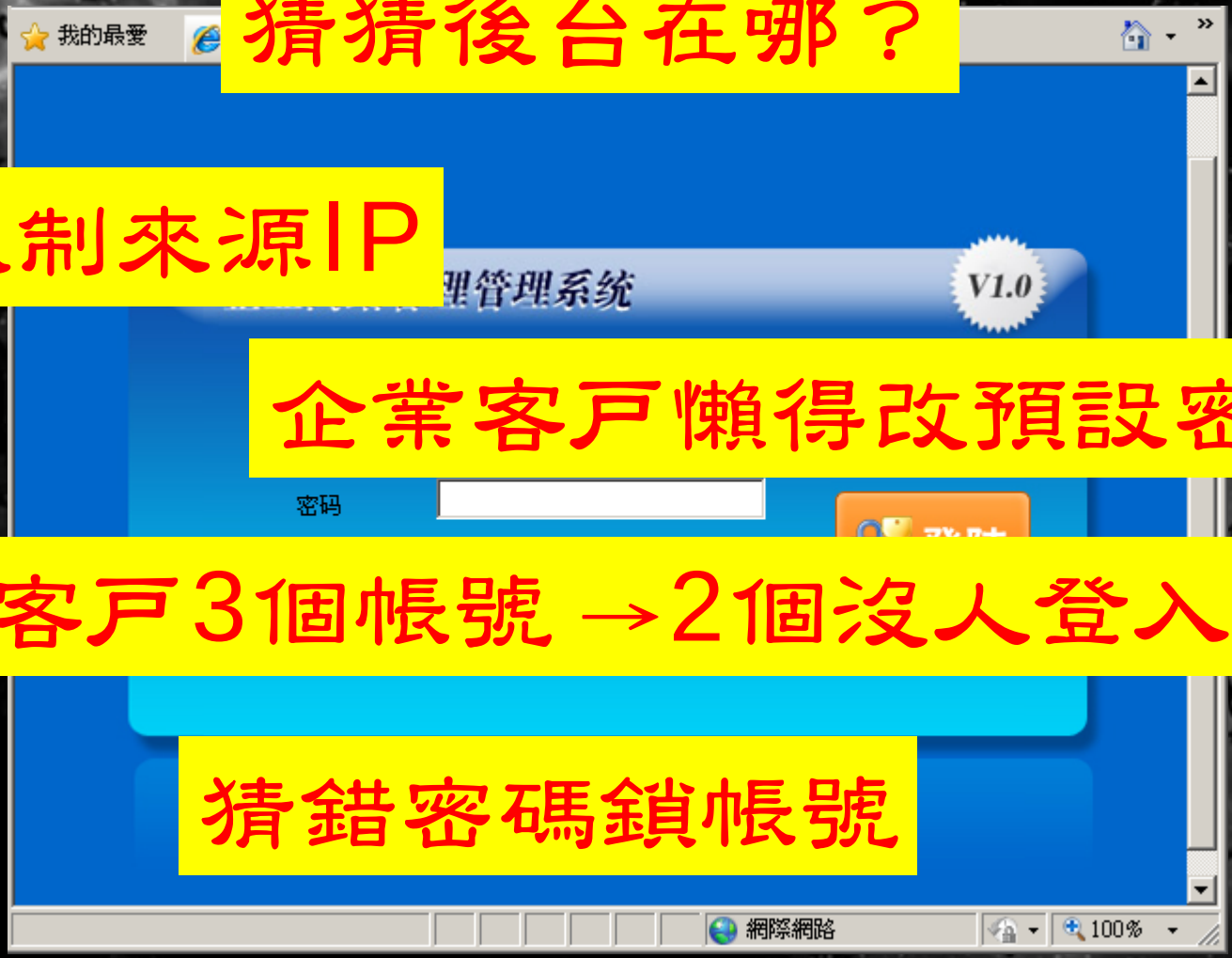

我的最愛
研究員籲提防惡意 iPhone 軟體—0 1惡意軟體,iPho...
研究員籲提防惡意 iPhone 軟體
列印
轉寄
收藏
加入推文：
加入書籤：
・日期：2010/02/04・作者：ZDNet新聞專區：Elinor Mills
網際網路
105%


Injection Flaw(注入)
竊取及修改網站資料庫，或控制網站作業系統
Cross-Site Scripting(跨站腳本攻擊)
竊取客戶的Cookie或Session登入資訊
Broken Authentication and Session Management（認證失效）
身份驗證功能被破解
Insecure Direct Object Reference(物件參照)
OWASP 10大網頁漏洞
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Failure to Restrict URL Access（後台曝露）
管理用網頁未限制存取
Unvalidated Redirects and Forwards（未驗證網頁重新導向）
任意將網頁導至惡意網站
Insecure Cryptographic Storage（資料曝露）
敏感性資料未被加密儲存
Insufficient Transport Layer Protection（傳輸防護不安全）
敏感性資料未被加密傳送
1998 © Blizzard Entertainment. All rights reserved.

猜

猜猜後台在哪？

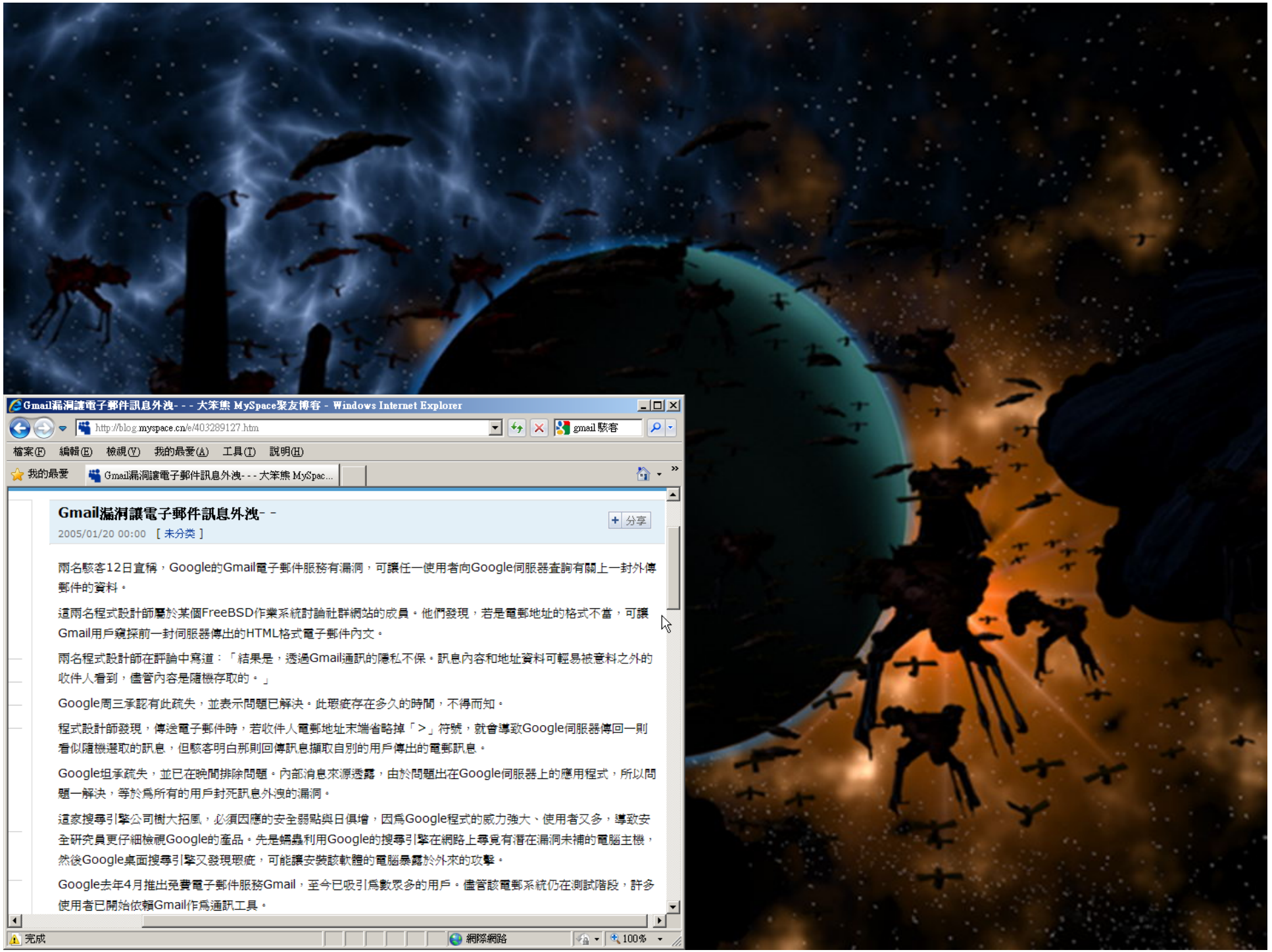
不限制來源IP



企業客戶懶得改預設密碼

每個客戶3個帳號 →2個沒人登入過

猜錯密碼鎖帳號


Gmail漏洞讓電子郵件訊息外洩- - - 大笨熊 MySpace聚友博客 - Windows Internet Explorer
http://blog.myspace.cn/e/403289127.htm
gmail 駭客
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
Gmail漏洞讓電子郵件訊息外洩- - - 大笨熊 MySpac...
Gmail漏洞讓電子郵件訊息外洩- -
分享
2005/01/20 00:00 [未分类]
兩名駭客12日宣稱，Google的Gmail電子郵件服務有漏洞，可讓任一使用者向Google伺服器查詢有關上一封外傳郵件的資料。
這兩名程式設計師屬於某個FreeBSD作業系統討論社群網站的成員。他們發現，若是電郵地址的格式不當，可讓Gmail用戶窺探前一封伺服器傳出的HTML格式電子郵件內文。
兩名程式設計師在評論中寫道：「結果是，透過Gmail通訊的隱私不保。訊息內容和地址資料可輕易被意料之外的收件人看到，儘管內容是隨機存取的。」
Google周三承認有此疏失，並表示問題已解決。此瑕疵存在多久的時間，不得而知。
程式設計師發現，傳送電子郵件時，若收件人電郵地址末端省略掉「>」符號，就會導致Google伺服器傳回一則看似隨機選取的訊息，但駭客明白那則回傳訊息擷取自別的用戶傳出的電郵訊息。
Google坦承疏失，並已在晚間排除問題。內部消息來源透露，由於問題出在Google伺服器上的應用程式，所以問題一解決，等於爲所有的用戶封死訊息外洩的漏洞。
這家搜尋引擎公司樹大招風，必須因應的安全弱點與日俱增，因爲Google程式的威力強大、使用者又多，導致安全研究員更仔細檢視Google的產品。先是蝙蝠利用Google的搜尋引擎在網路上尋覓有潛在漏洞未補的電腦主機，然後Google桌面搜尋引擎又發現瑕疵，可能讓安裝該軟體的電腦暴露於外來的攻擊。
Google去年4月推出免費電子郵件服務Gmail，至今已吸引爲數眾多的用戶。儘管該電郵系統仍在測試階段，許多使用者已開始依賴Gmail作爲通訊工具。
完成
網際網路
100%

雲端廠商要防好？

完全代管
完全負責

系統維運
人力不足

防火牆、IDS/IPS/IDP、系統更新、
SOC監控都到位，還是防不到？

網站開發要寫好？

陳之藩：

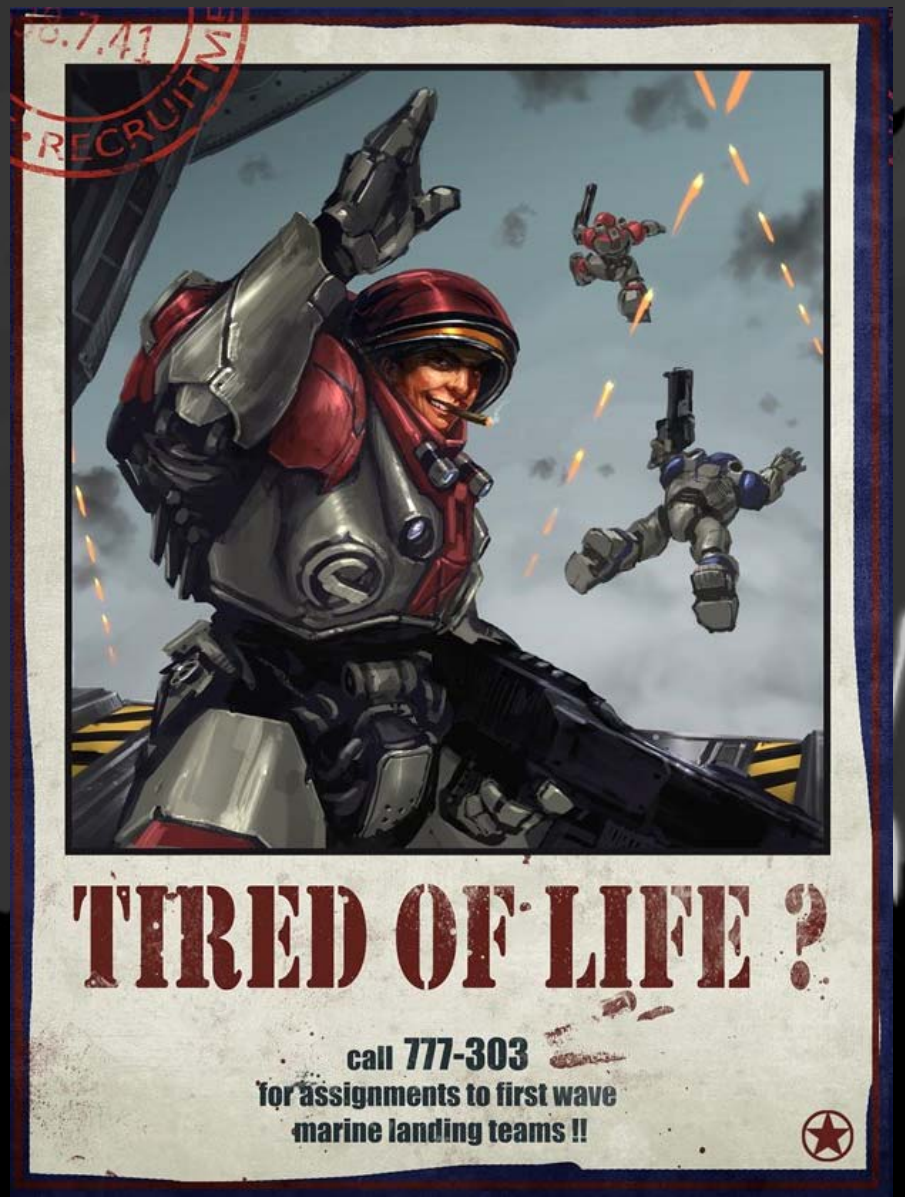
要謝的人太多，

還是**謝天**吧...

程式煩：

要改的程式太多

還是**改天**吧...



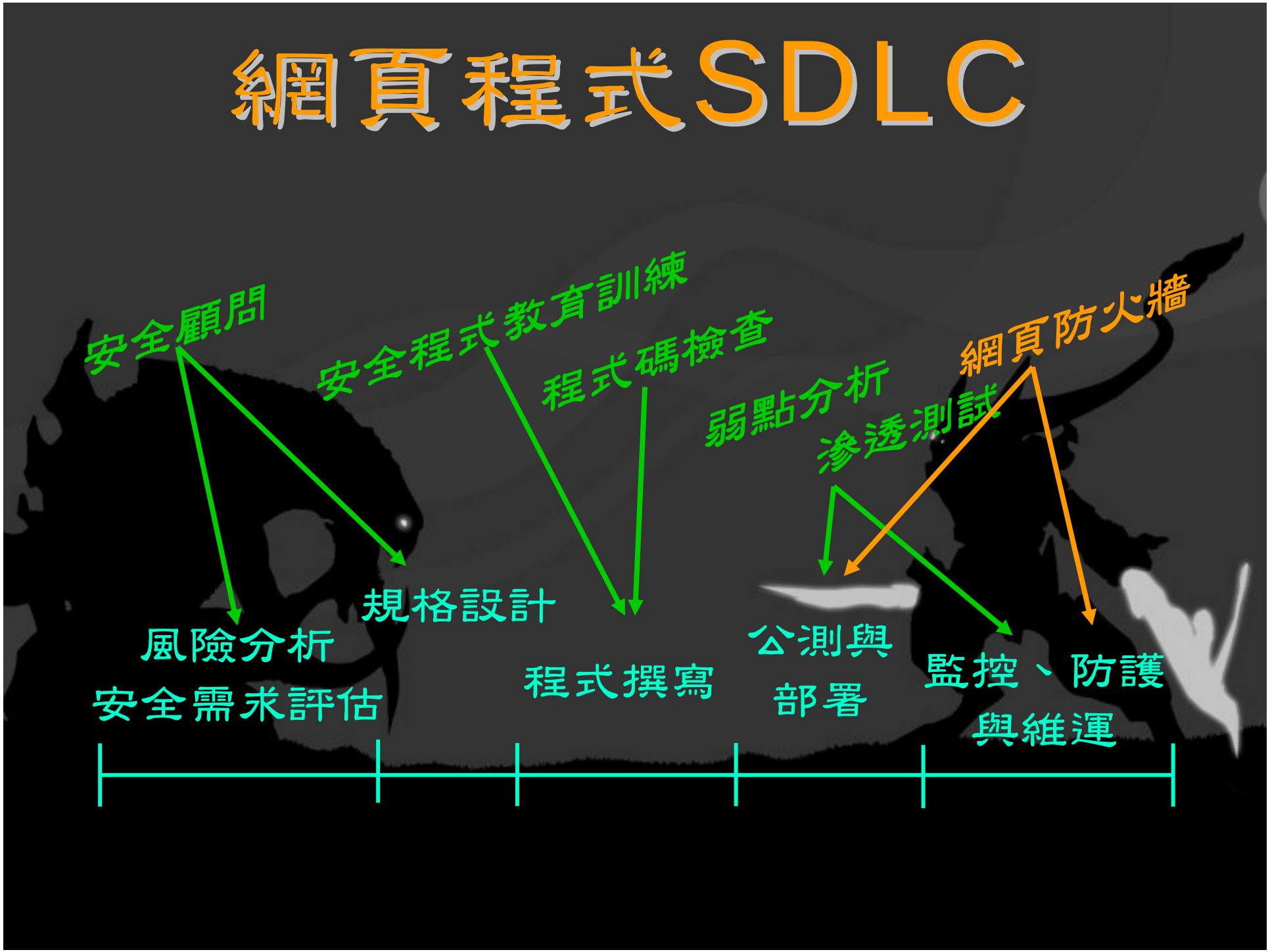
我不懂寫安全程式...

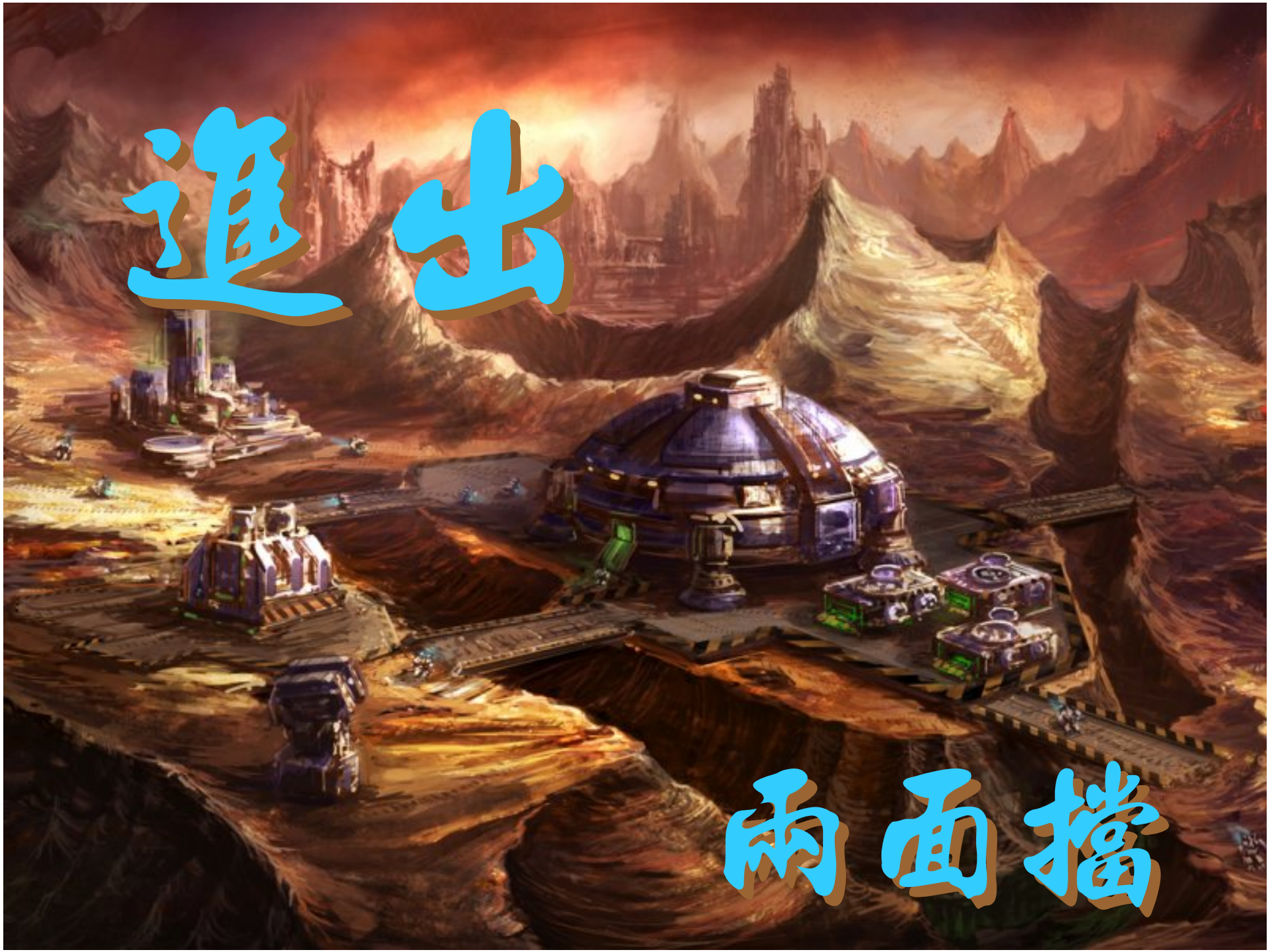
時程来不及啦！

當初程式規格又沒開資安！

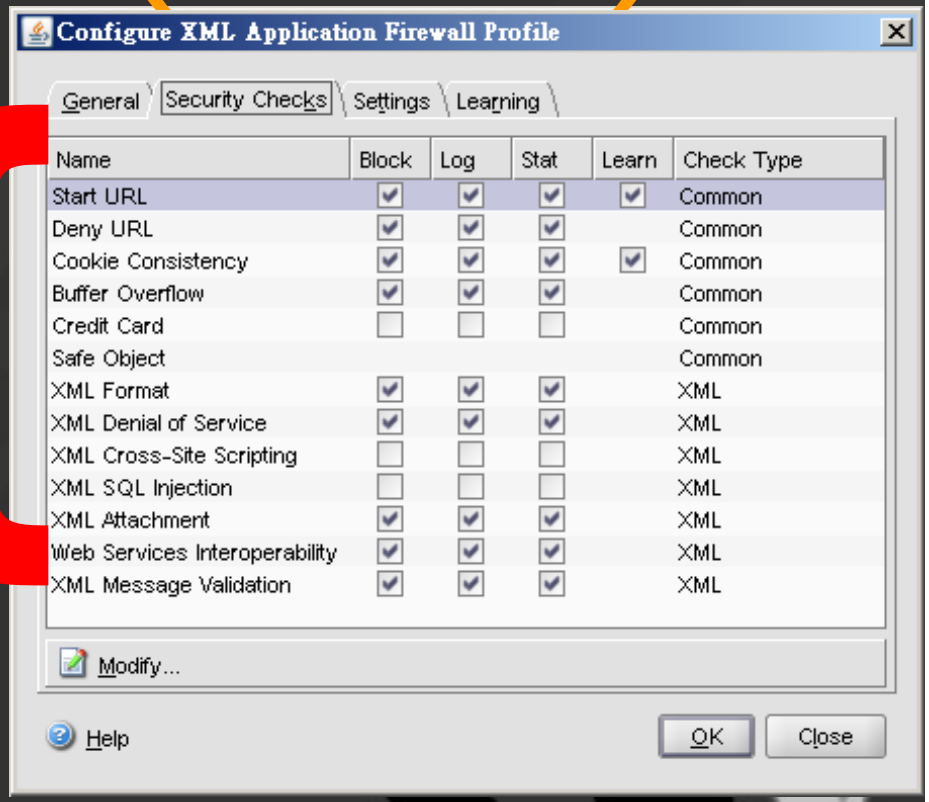
个面漂亮才是王道！

寫那段的早離職啦！


網頁程式SDLC
安全顧問
安全程式教育訓練
程式碼檢查
弱點分析
滲透測試
網頁防火牆
風險分析
安全需求評估
規格設計
程式撰寫
公測與
部署
監控、防護
與維運


進出
兩面擋

網站防火牆(WAF)



毋須上百條規則

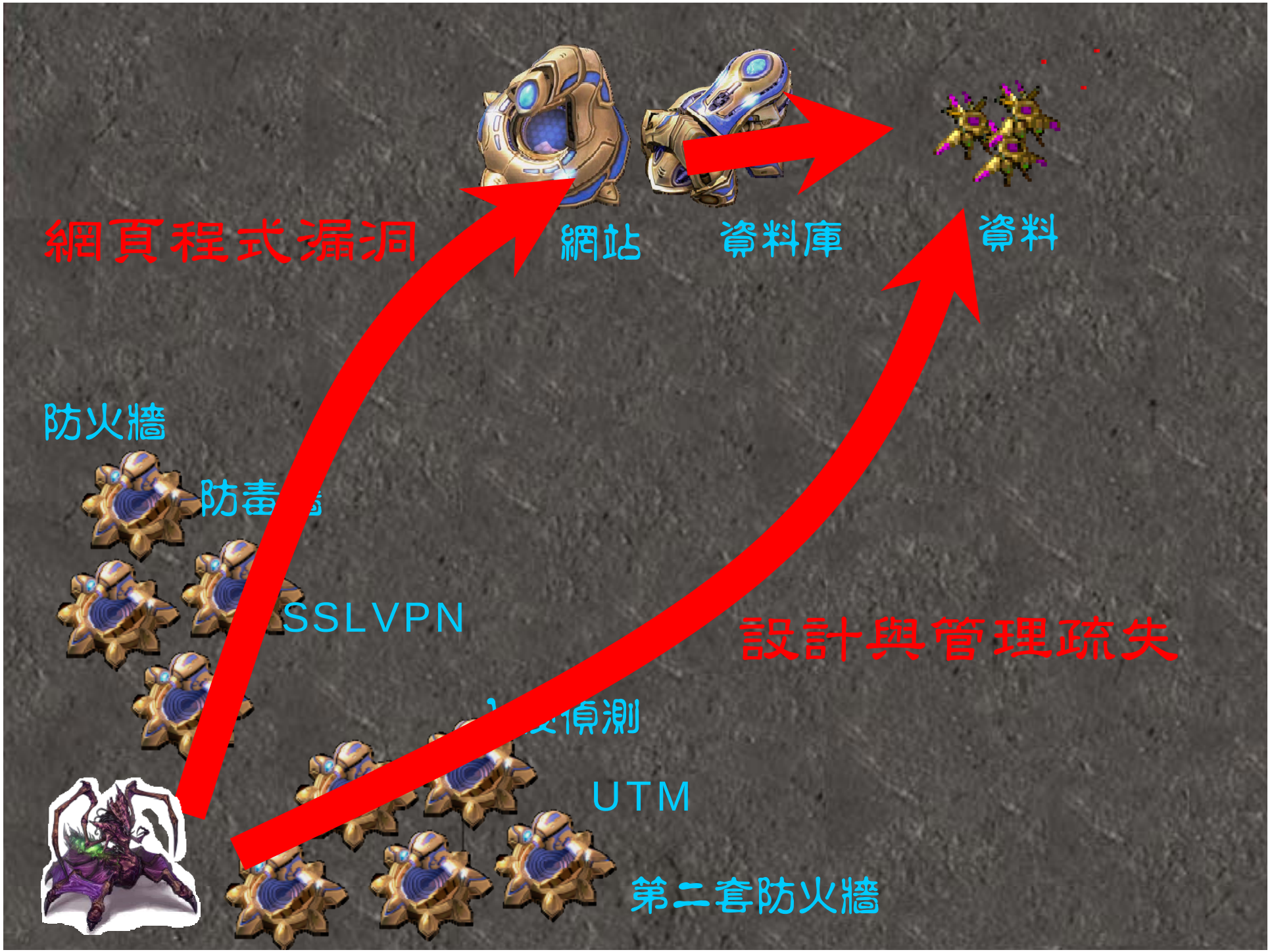
以「行爲」爲基準

毋須更新

正面表列白名單

只開放程式可正常執行的行爲

可防堵零時差攻擊


網頁程式漏洞
網站
資料庫
資料
防火牆
防毒
SSLVPN
偵測
UTM
第二套防火牆
設計與管理疏失


網頁程式漏洞

SQL Injection偷資料

SQL Injection自動化

設計與管理疏失

設計與管理疏失

首頁.htm

新聞頁.htm

訂閱新聞.asp

今日新聞.asp

會員登入.php

下單交易.php

個人資料.doc

會員測試.bak

組織通訊錄.xls

後台管理.asp

補強設計與管理疏失

首頁.htm

新聞頁.htm

訂閱新聞.asp

今日新聞.asp

會員登入.php

下單交易.php

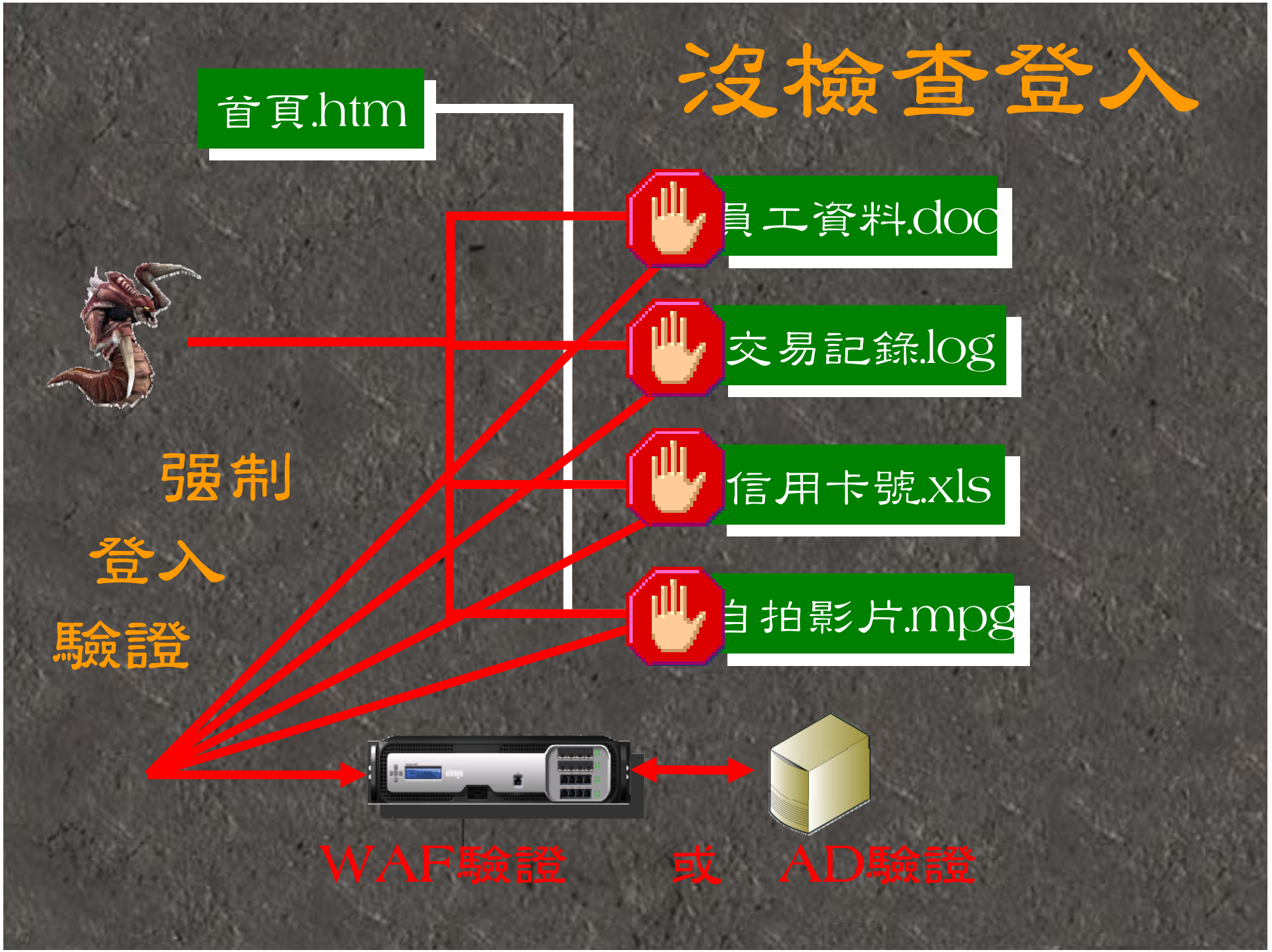
個人資料.doc

會員測試.bak

組織通訊錄.xls

後台管理.asp

程式設計師
不小心放上的
檔案與個資

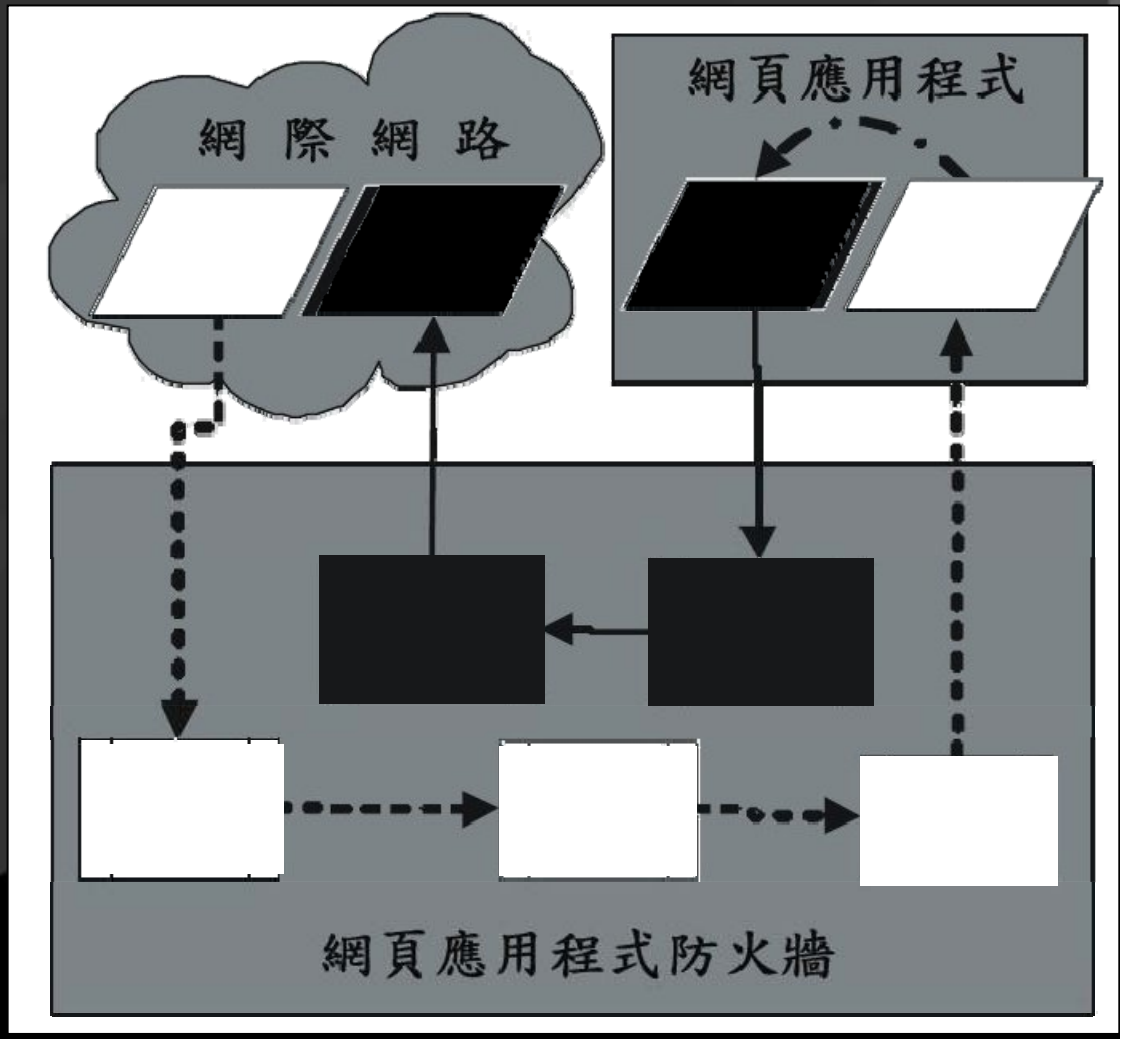

沒檢查登入
首頁.htm
員工資料.doc
交易記錄.log
信用卡號.xls
自拍影片.mpg
強制
登入
驗證
WAF驗證
或
AD驗證


網頁防火牆

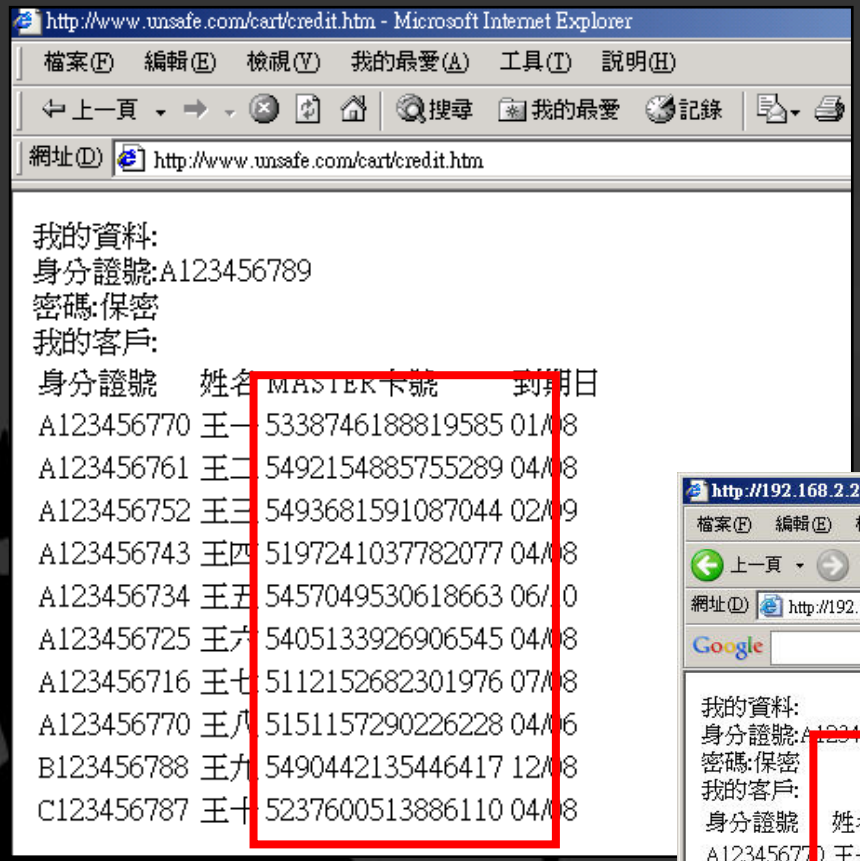
正面表列白名單

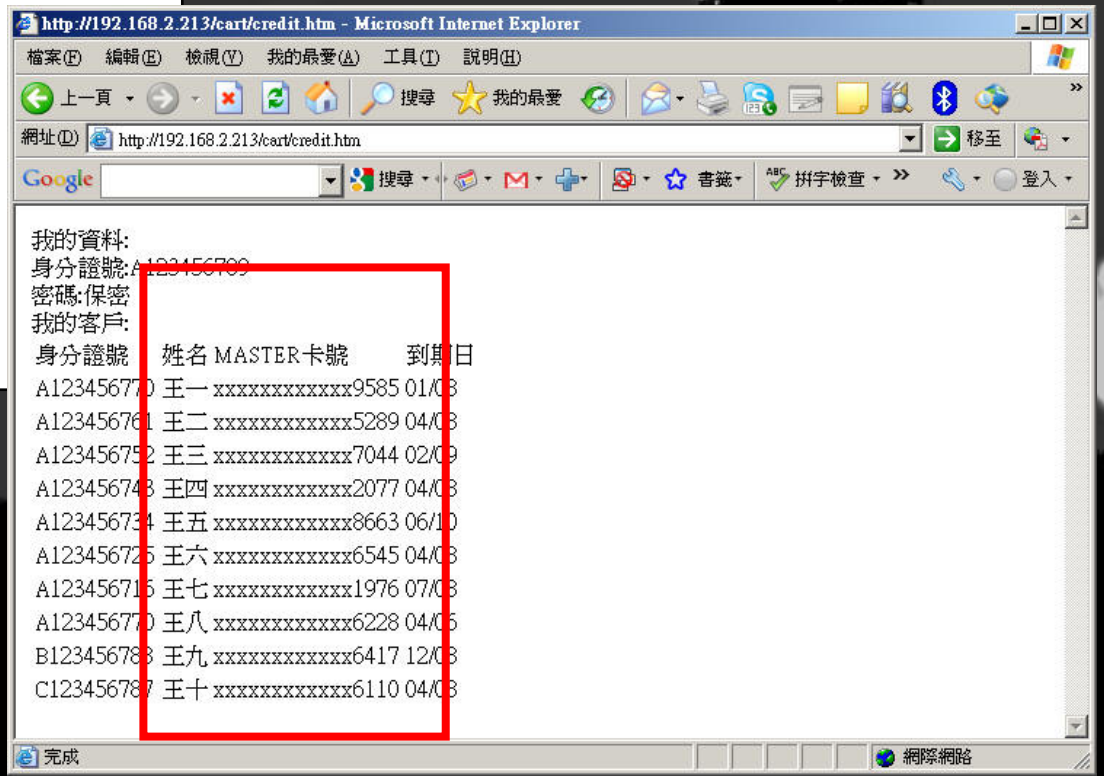
利用正向白名單概念，專門針對網站程式進行防護

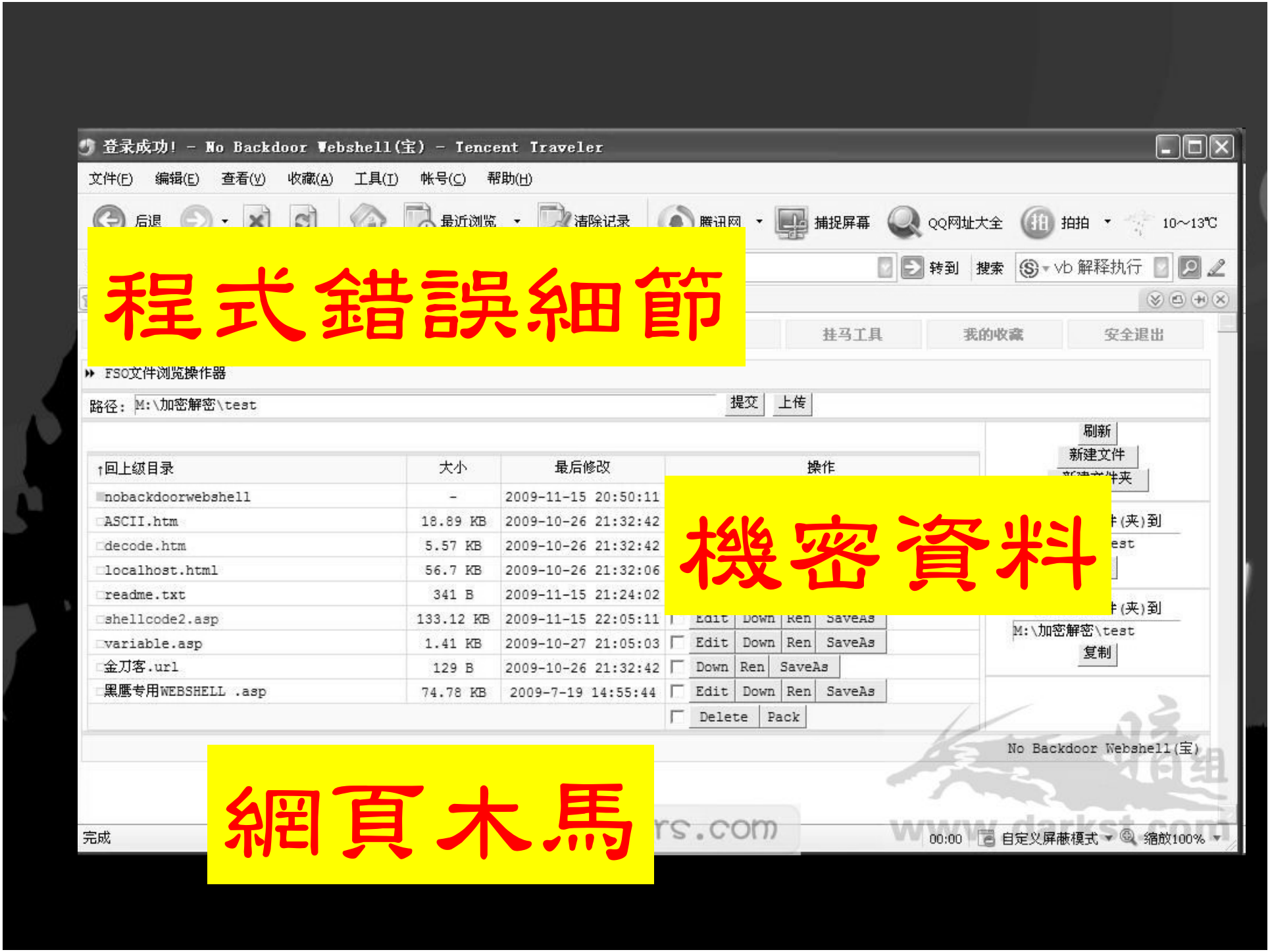
- 遮蔽程式漏洞
- 補强設計/管理疏失
- 强制登入驗證
- 資料外洩預警



機密資料
外洩預警


http://www.unsafe.com/cart/credit.htm - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 記錄
網址(D) http://www.unsafe.com/cart/credit.htm
我的資料:
身分證號:A123456789
密碼:保密
我的客戶:
身分證號 姓名 MASTER卡號 到期日
A123456770 王一 5338746188819585 01/08
A123456761 王二 5492154885755289 04/08
A123456752 王三 5493681591087044 02/09
A123456743 王四 5197241037782077 04/08
A123456734 王五 5457049530618663 06/10
A123456725 王六 5405133926906545 04/08
A123456716 王七 5112152682301976 07/08
A123456770 王八 5151157290226228 04/06
B123456788 王九 5490442135446417 12/08
C123456787 王十 5237600513886110 04/08


http://192.168.2.213/cart/credit.htm - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://192.168.2.213/cart/credit.htm
移至
Google 搜尋 書籤 拼字檢查 登入
我的資料:
密碼:保密
我的客戶:
身分證號 姓名 MASTER卡號 到期日
王一 xxxxxxxxxxxx9585
王二 xxxxxxxxxxxx5289
王三 xxxxxxxxxxxx7044
王四 xxxxxxxxxxxx2077
王五 xxxxxxxxxxxx8663
王六 xxxxxxxxxxxx6545
王七 xxxxxxxxxxxx1976
王八 xxxxxxxxxxxx6228
王九 xxxxxxxxxxxx6417
王十 xxxxxxxxxxxx6110
完成
網際網路


登录成功! - No Backdoor Webshell(宝) - Tencent Traveler
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帐号(C) 帮助(H)
后退
最近浏览
清除记录
腾讯网
捕捉屏幕
QQ网址大全
拍拍
10~13℃
转到
搜索
vb 解释执行
程式錯誤細節
挂马工具
我的收藏
安全退出
FSO文件浏览操作器
路径: M:\加密解密\test
提交
上传
刷新
新建文件
回上级目录
大小
最后修改
操作
nobackdoorwebshell - 2009-11-15 20:50:11
ASCII.htm 18.89 KB 2009-10-26 21:32:42
decode.htm 5.57 KB 2009-10-26 21:32:42
localhost.html 56.7 KB 2009-10-26 21:32:06
readme.txt 341 B 2009-11-15 21:24:02
shellcode2.asp 133.12 KB 2009-11-15 22:05:11 Edit Down Ren SaveAs
variable.asp 1.41 KB 2009-10-27 21:05:03 Edit Down Ren SaveAs
金刀客.url 129 B 2009-10-26 21:32:42 Down Ren SaveAs
黑鹰专用WEBSHELL .asp 74.78 KB 2009-7-19 14:55:44 Edit Down Ren SaveAs
Delete Pack
機密資料
M:\加密解密\test
复制
No Backdoor Webshell(宝)
網頁木馬
完成
00:00
自定义屏蔽模式
缩放100%


3039
1289
199/200
防火
又防洪

SYN COOKIE / PROXY

HTTP DDoS

會員登入.php

商品搜尋.asp

暴力猜測密碼

資料庫效能低落

商品搜尋.asp

CC攻擊 - Proxy

CC攻擊 - iframe

連線洪水

HTTP DDoS – WAF對策

會員登入.php

商品搜尋.asp

暴力猜測密碼

限制來源IP登入頻率

資料庫效能低落

限制查詢目標頁頻率

商品搜尋.asp

CC攻擊 - Proxy

查Forwardee頻率

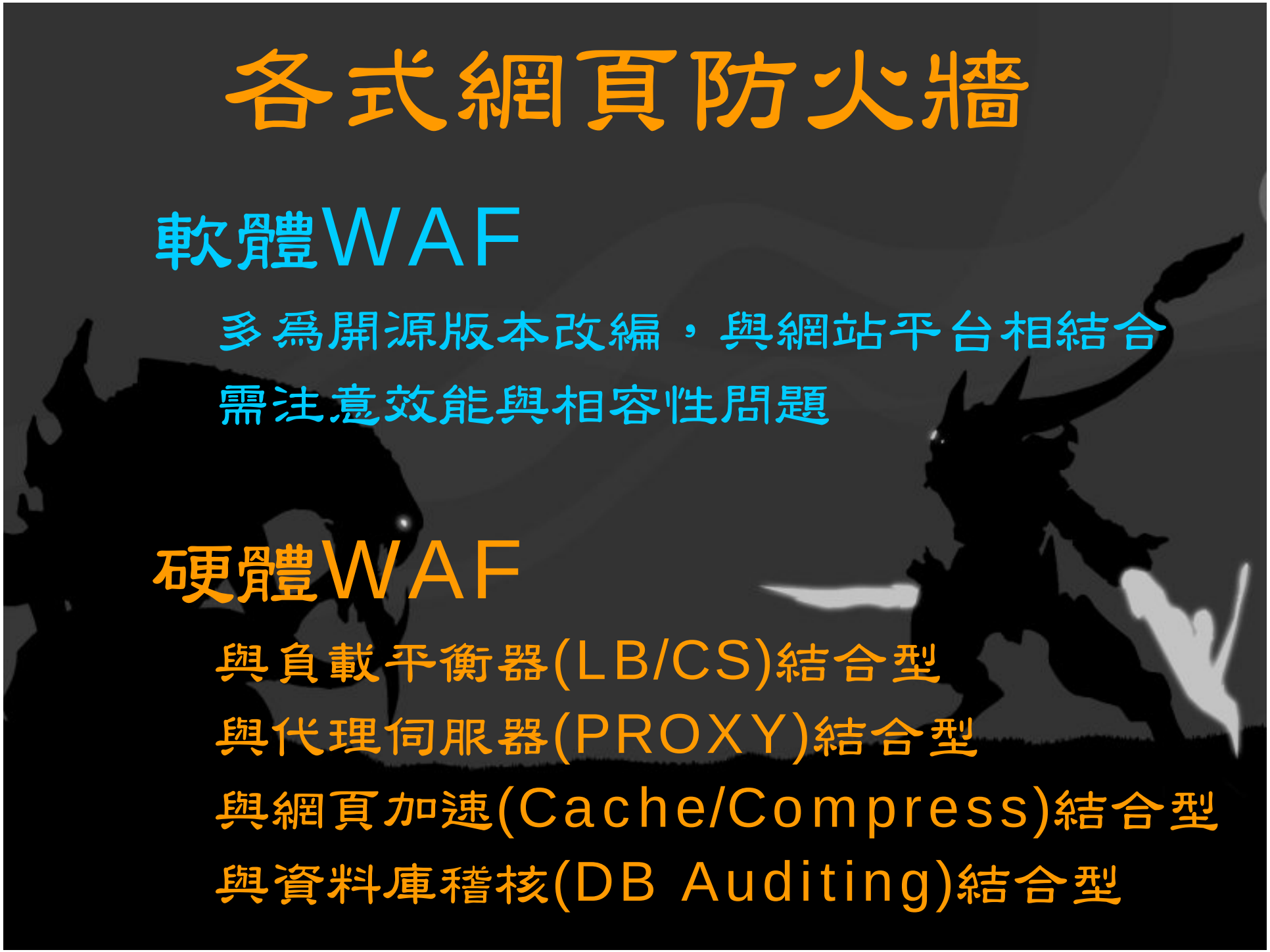
CC攻擊 - iframe

查Referer頻率

連線洪水

HTTP DDoS –JS法


多工兼專家


各式網頁防火牆
軟體WAF
多為開源版本改編，與網站平台相結合
需注意效能與相容性問題
硬體WAF
與負載平衡器(LB/CS)結合型
與代理伺服器(PROXY)結合型
與網頁加速(Cache/Compress)結合型
與資料庫稽核(DB Auditing)結合型

成功因素還是在人

管理者

熟知各種網管原理，排除架構面問題

具備AP開發能力，協助開發者修正程式

熟知各種網頁攻擊手法，了解邏輯面問題

資管與AP間的協調

長官與資安政策支持

lucifer.yang 小老鼠 sti.com.tw

- 網頁防火牆
- 資料庫稽核
- 資料防洩
- 資安解決方案規劃
- 資安服務
  - 滲透測試
  - 弱點掃瞄
  - 緊急應變
  - 程式碼檢測
  - 資安強化SOP手冊

ピピピ
問題？