資安大偵探

# 福爾摩斯

## 偵察筆記

Holmes

IBM

Holmes

資安大偵探

# 福爾摩斯

偵察筆記

Holmes

「你到底做了什麼，往往無關緊要。
緊要的是，你如何使人相信你做了什麼！」

— 福爾摩斯

如同福爾摩斯畢其生對抗邪惡的莫里亞森教授，IT部門與資安風險的勢不兩立，也是一場漫長且不容懈怠的戰爭！尤其在資訊架構日趨龐雜的企業環境中，再絕頂聰明的您，也無法只憑一己之力孤軍奮戰；您不只要凝聚所有部門主管的資安共識，更要讓他們成為媲美華生的關鍵夥伴。

這本筆記正是協助您把內部阻力化為助力的開始。透過「資訊架構・網路平台・資料庫・電子郵件」四大類別的資安真實事件記錄，您可以更有力地喚起主管們對資安風險的警惕心，說服他們合力杜絕各個營運流程中的資安漏洞。而IBM更將隨時待命出動，以最精良的企業級解決方案傾力相助每位資安大偵探。

資安風險刻不容緩，請您即刻閱讀筆記，凝聚內部共識，建立全面戒備的企業級資安防線！





# Content目錄



Case I
資訊架構

資安大偵探

# 福爾摩斯

## 偵察筆記



### 資訊架構　密室犯罪

## 爆米花詐彈

知名的爆米花專賣店遭詐彈客入侵，善良的女大生在毫無警覺的狀況下，成為詐彈客鎖定的無辜羔羊，平白損失15萬元！誰讓詐彈客輕易混入顧客群中？誰又會成為下個詐彈受害者？福爾摩斯發現，不設防的資訊架構環境，早已成為詐彈客來去自如的密室犯罪溫床……


## 事件本末

一名女大學生聲稱，某知名爆米花店透過客服電話要她提供信用卡號付款，卻因此遭騙損失了15萬元。而且，陸續有消費者表示遭到類似的詐彈攻擊。以獨門研發的10餘種特殊口味，掀起網路團購熱潮的爆米花店，儘管生意搶搶滾，卻毫無資安風險意識。殊不知有心人士早已覬覦該店不斷湧入的消費者個資，利用駭客手法竊取資料，15萬元不過只是詐彈事件的冰山一角！

## 風險影響

消保官強調：「企業對所蒐集之消費者資訊未善盡保護之責，就是違反個人資料保護法，符合民法第184條規定，要負起賠償責任。」除此之外，詐彈效應導致部份網購顧客卻步的無形損失，更是難以估算！





# 福爾摩斯破案技巧

## 迎頭痛擊・IBM資訊架構除駭計策

人紅是非多，網站紅狀況多！倘若企業資訊架構的安全度遠遠落後於知名度，就只能任人宰割。衷心建議資安大偵探們，善用IBM資訊架構除駭計策，讓想佔便宜的不法份子，個個鎩羽而歸！

## 技巧一

### IBM ISS Proventia ESP (Enterprise Security Platform) 企業安全平台

入侵防禦弱點評估諮詢與設計服務以及主動式入侵防禦及弱點保護系統規劃與建置服務。

### 關鍵協助

1. IBM X-Force 是全球頂尖的顧問級安全研發團隊，能夠提供最及時的專業駭客資料庫。
2. 前瞻性防護：最先進的協定分析檢測技術（Stateful Protocol Analysis），同時支援的協定和資料格式超過200種，蠕蟲病毒防護能力、DHCP異常檢測、Web伺服器防護、 Windows活動目錄防護、間諜軟體防護、問題系統定位和隔離掃描檢測。
3. 動態適應阻斷：在不影響網路的前提下，ISS入侵防護設備能夠及時地阻斷攻擊、病毒等非法流量，從而保證營業使用不受損害。
4. 細粒度策略控制，通過政策每個安全事件、連接事件都可以針對防護與記錄行為進行設定。
5. 詳細的日誌審計，證據資料收集將成為企業舉證最佳工具。
6. 卓越的威脅檢測和防護，已經透過第三方公正單位認可的效能與可靠率。
7. 即插即用，靈活部屬。

**請撥0800-016-888按1了解更多破案技巧**

Case I 資訊架構

## 技巧二

### IBM磁碟與磁帶儲存設備

於中心儲存媒體端進行資料加密，保護紀錄企業最核心個資或營運資訊的媒體。

### 關鍵協助

1. 自行加解密：藉由運用創新的加密引擎技術，可在不影響儲存或硬體運行的效能下以原始速度進行加密和解密。
2. 硬碟加密：保護紀錄企業最核心個資或營運資訊的媒體，即使於運送或棄置時遺失或被竊取，仍可確保機敏資料不會被讀取。
3. 自我療癒：藉由備份或複製的時間點資料副本，確保在原始資料遺失時能恢復資料。

**請撥0800-016-888按1了解更多破案技巧**





### 偵察筆記

Case II
網路平台

資安大偵探

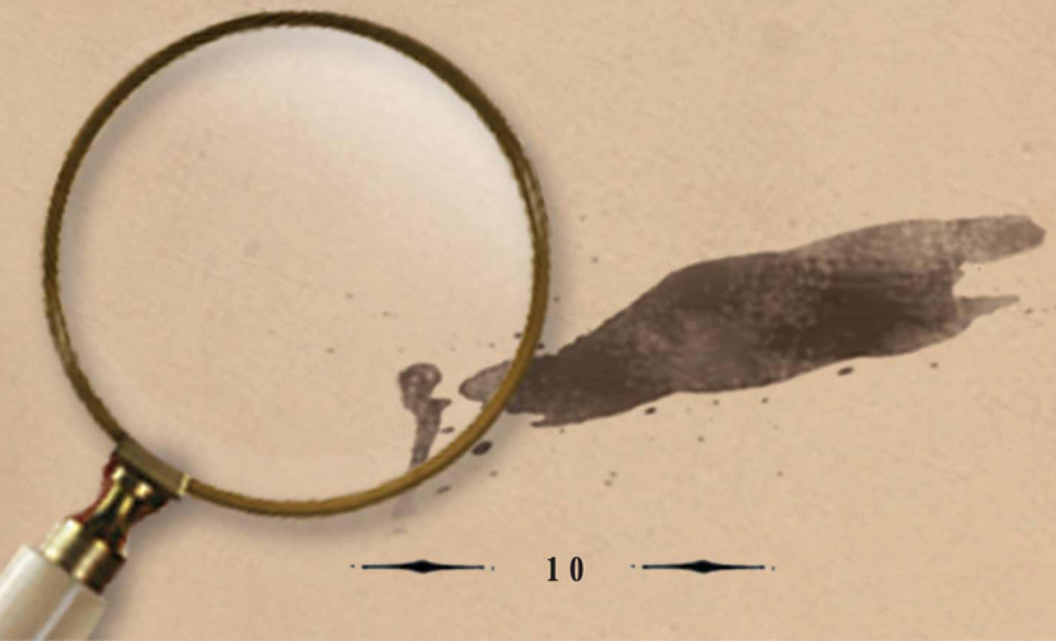
# 福爾摩斯偵察筆記



網路平台　怪盜入侵

## 網路查榜烏龍名冊

見似稀鬆平常的網路查榜，竟然連考生的身分證字號、電話…等個人資料，都可以在榜單中一覽無遺！主辦單位高度懷疑自家網路平台遭駭客入侵，緊急關閉網站程式。福爾摩斯發現，未經安全測試的網路平台，對犯罪高手而言有如進出自家陽台……




Case II
網路平台

## 事件本末

一位考生進入某訓練中心網站，點選所參加的技術檢定考試成績，赫然發現除了成績，包括身分證字號…等個資「全都露」，五萬多筆資料無一倖免！承辦單位主管隨即表示並未外洩考生資料，高度懷疑網路平台被駭客入侵，並聲稱中心網站須透過網路防火牆才能進入。然而發現疏失的考生直言指出，這些網站設計不只沒安全防護，甚至連基本的技術都談不上！

## 風險影響

由於網站防火牆安全漏洞，讓立意良善的網路查榜竟成為一本烏龍名冊！試想，若這些個資遭不法集團盜用，後果將不堪設想。而事件導致主辦單位人員清白、考試公信力遭受連帶懷疑，更是嚴重波及企業形象！





# 福爾摩斯破案技巧

## 敵我分明·IBM網路應用程式弱點偵查術

打開網路大門，就要有被駭的心理準備？您的網站驗收有掛”安全保證”嗎？99%的網站應用程式漏洞，其實都來自於開發階段的無心疏忽。衷心建議資安大偵探們，善用IBM網路應用程式弱點偵查術，知己知彼才能百戰百勝，讓居心叵測者不得其門而入！

## 技巧一

### IBM Rational AppScan Web 應用程式零漏洞方案

Rational AppScan為Web應用程式安全性檢測軟體的先驅，市佔率世界第一。協助您擁有全面的應用程式安全管理平台，能為軟體開發過程各階段增添應用掃描與安全診斷功能。

### 關鍵協助

1. 整個軟體開發的生命週期皆可應用。
2. 可簡化發現與修復Web應用系統安全性問題的工作，降低維護資訊安全的成本。
3. 黑箱測試:模擬各種駭客攻擊的手法，以無害的方式去使用運行中的Web應用系統。
4. 白箱測試:分析提供的原始碼，判斷系統是否存在各種安全性問題。
5. 掃描結果報告:全中文化(支援多國語言)，可依不同對象調整產出項目與詳細程度，超過40種遵規標準報告，輕鬆面對法規遵循需求。

**請撥0800-016-888按1了解更多破案技巧**

Case III 資料庫

資安大偵探

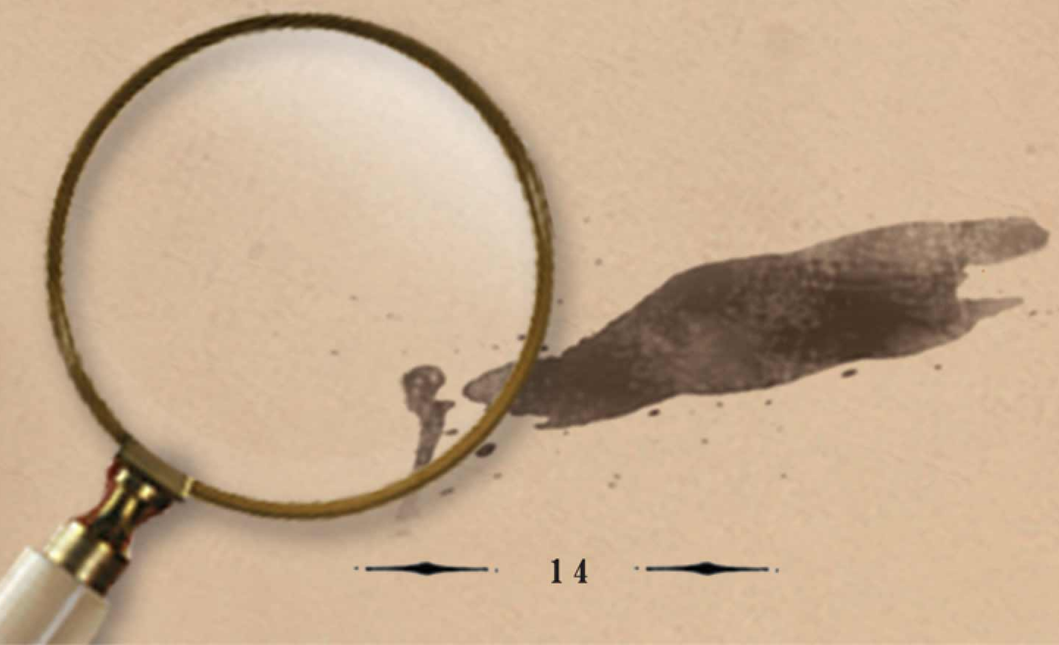
# 福爾摩斯偵察筆記

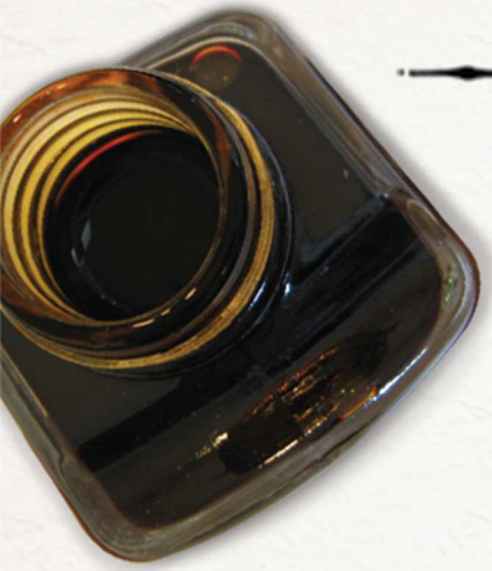


## 資料庫 神祕竊案

## 誰刪了國安情報？

130筆外籍敏感人士身分資料遭到莫名刪除，而且是經由主管權限密碼登入刪除。層層追查下，隸屬主管單位的專員坦承，是自己盜用直屬長官密碼所為。福爾摩斯發現，資料庫最可怕的敵人，往往在它的內部……





Case III 資料庫

## 事件本末

為減輕工作，竟竊取長官密碼，將130筆外籍敏感人士身分資料刪除。這起匪夷所思的資料庫安全事件，印證資安防範最可怕的漏洞，往往在自己內部！雖然當事人辯稱被刪除的只是機場、學校等維安目標資料，且內部稽核機制也已將資料復原。但它所曝露的資安缺陷正警惕我們：不管資料庫有幾道門，只要有鑰匙，它隨時可能被不當人士開啟，為所欲為！

## 風險影響

不管是國家機密或商業機密，一旦遺失或遭竊，輕則影響營運，重則動搖生存根本！事後的緝兇或資料復原只能減少危害程度，把心力和資源及早投入事前的防範與管控，才是上上之策！





# 福爾摩斯破案技巧

## 祕密證人・IBM資料庫活動跟蹤法則

想讓任何非法存取的行徑在第一時間敗露，就必須更早一步掌控他們的行蹤。衷心建議資安大偵探們，善用IBM資料庫活動跟蹤法則，讓任何蠢蠢欲動的企圖，在您眼前原形畢露！

## 技巧一

### IBM Optim Data Privacy 資料管理解決方案

打造出可信賴的架構環境，讓企業能以充分反映資訊價值及保障用戶隱私的方式，安心地把資訊資產用於業務最佳化。

### 關鍵協助

1. 隱私資料保護：提供自動化的資料轉換、變形能力，能夠輕鬆地跨越多個資料庫將企業中涉及的各種個人資訊或保密資訊實施脫密、漂白處理及遮蔽機制。
2. 法規遵循：對不同資料格式亦提供不同遮蔽機制，能夠輕鬆地執行身份刪除(De-Identification)，去個人化(Depersonalize)，匿名化(Anonymize)及身份遮蔽(Masking)並同時保持資料完整性。
3. 法規遵循：支援HIPAA、GLBA、DDP、PIPEDA、Safe Harbour、PCI DSS等隱私權規範。

**請撥0800-016-888按1了解更多破案技巧**


# 技巧二

## IBM InfoSphere Guardium資料庫稽核解決方案

部署集中管理且標準化的控管功能，以便即時維護資料庫安全並加以監視、進行詳細的資料庫審核、將法規遵循的報告自動化、管制資料層級的存取、管理資料庫漏洞，並自動探索機密資料。

### 關鍵協助

1. 非侵入性：持續即時監控所有資料庫行動，但不需改變資料庫或應用程式配置，也幾乎不會影響效能表現。
2. DBMS獨立性，支援多種資料庫及應用系統。
3. 可達到細緻精密的策略與監控如：who，what，when，how。
4. 在評估階段找出資料庫弱點，在運行階段提供即時警示及阻絕。
5. 可提供全面的活動監控：包含遠端及本機的存取。
6. 職權分立：審核資料儲存於多個不同的實體或虛擬裝置中，內部人員或是駭客無法藉由篡改審核日誌資料來遮掩不法情事。

**請撥0800-016-888按1了解更多破案技巧**





## 偵察筆記

Case IV
電子郵件

資安大偵探

# 福爾摩斯

## 偵察筆記



### 電子郵件　攔截偷窺

## 內線交易密謀案

就在重大營運消息即將對外披露前夕，一場密謀已久的內線交易事件，也在暗中悄悄進行。全公司只有5個人知道這項營運消息，誰才是真正的主謀者？福爾摩斯發現，當他們藉著電子郵件互相聯絡時，所有重大資訊早已被第6個人悉數掌握……


## 事件本末

傳說中，飯店女侍因為偷聽大老闆們的聚餐談話，而在股市上一夕致富。時至今日，企業核心人物就算守口如瓶，別忘了電子郵件會幫你洩露更多祕密！再機密的郵件都免不了透過公共網路，內部資安漏洞更是讓有心人有太多可乘之機。你以為只有少數人參與機密，卻被暗處的藏鏡人悉數掌握。當郵件按出傳送之際，小心在另一個收件匣裡，有人正攔截偷窺著你所有的機密！

## 風險影響

失去對資訊的掌控權，就代表失去贏得商機的主控優勢。更甚者，可能爆發內線交易、惡意攻擊、形象受損…種種難以預料的危機。小小的電子郵件，爆炸起來的威力絕對不容你小覷！



# 福爾摩斯破案技巧

## 天羅地網・IBM電子郵件全面過濾法

上古世紀的木馬屠城記，到今天都還在不斷重演；披著郵件外衣的狼，隨時等著狠狠咬企業一口！衷心建議資安大偵探們，善用IBM電子郵件全面過濾法，把郵件永遠放在對的位置！

## 技巧一

### IBM Lotus Protector for Mail Encryption

### 郵件系統安全加密機制

業界首見與僅見的網路垃圾郵件過濾器，保護資料，減輕遵規負擔。

### 關鍵協助

1. 可封鎖99%以上的已知垃圾郵件。
2. 即時檢查並擊退可疑郵件。
3. 每15分鐘進行保護更新。
4. 擁有950億個且數目不斷增加的已識別垃圾郵件來源。
5. 全面掌控入埠與離埠內容。
6. 即時的多層防毒保護。

**請撥0800-016-888按1了解更多破案技巧**

## 偵察筆記



Holmes

偵察筆記

Holmes

## 偵察筆記



Holmes

偵察筆記

Holmes

Holmes

# 2011年曆

## January 1

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| 31 | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

## February 2

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | | | | | | |

## March 3

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 31 | | | |

## April 4

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

## May 5

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| 30 | 31 | | | | | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |

## June 6

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | | | |

Holmes

Holmes

# 2011年曆

## July 7

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

## August 8

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | | | | |

## September 9

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | | |

## October 10

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| 31 | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

## November 11

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | | | | |

## December 12

| 一 | 二 | 三 | 四 | 五 | 六 | 日 |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | |

Holmes

Holmes

**披上風衣化身資安大偵探**

**請撥0800-016-888按1了解更多破案技巧**

Holmes

TW1AN01D

台灣國際商業機器股份有限公司 台北市110松仁路7號3樓
IBM市場行銷處0800-016-888按1 www.ibm.com/tw