



# 從電子商務資安事件 來看通報與應變聯防之作為

資策會資安所 林耕宇  
2018.10.03



# 簡報大綱



- 電子商務新型態資安威脅趨勢
- 建立智慧情資與通報聯防機制
- 落實電子商務資安事件處理建議



- **電子商務新型態資安威脅趨勢**
- 建立智慧情資與通報聯防機制
- 落實電子商務資安事件處理建議

# 史上最慘，2億eBay用戶個資恐外流

eBay網站的用戶資料庫遭駭客入侵,eBay資料庫中那些沒有經過加密的姓名、電話、地址和生日資訊，很容易成為駭客發動社交攻擊誘騙民眾的資訊

文/ 王宏仁 | 2014-05-23 發表

讚 5 萬 按讚加入iThome粉絲團

讚 0 分享

G+



5月21日，全球上億eBay用戶紛紛收到了一封令人擔憂的更換密碼通知，eBay只是輕描淡寫地說明內部發生了某種資安或維護問題，因而要求用戶儘快更換登入密碼，就連eBay旗下跨國線上支付服務PayPal的網站上，都貼出eBay緊急呼籲用戶更換密碼的公告。eBay沒有說明太多細節，但這個突如其來的舉動，已引起眾人議論紛紛，不少媒體也紛紛推測eBay出大事了。



# 對比國際，台灣電子商務資安亦面臨威脅



## 台灣電商企業，大多是中小企業為主，資安資源少

中小企業由於預算與人力有限，無法投入多餘資源來導入資安解決方案。

### 電商資安威脅日益嚴重



- 電商賣場網站為求快速上架，一般程式設計完成，**未進行完整測試各種資安風險**
- **防護機制或防火牆未做好**，少一道資安程序，即成為駭客攻擊程式弱點，輕鬆盜取消費者個資。
- **駭客侵入網站竊取個資**，再把個資販賣給詐騙情團。

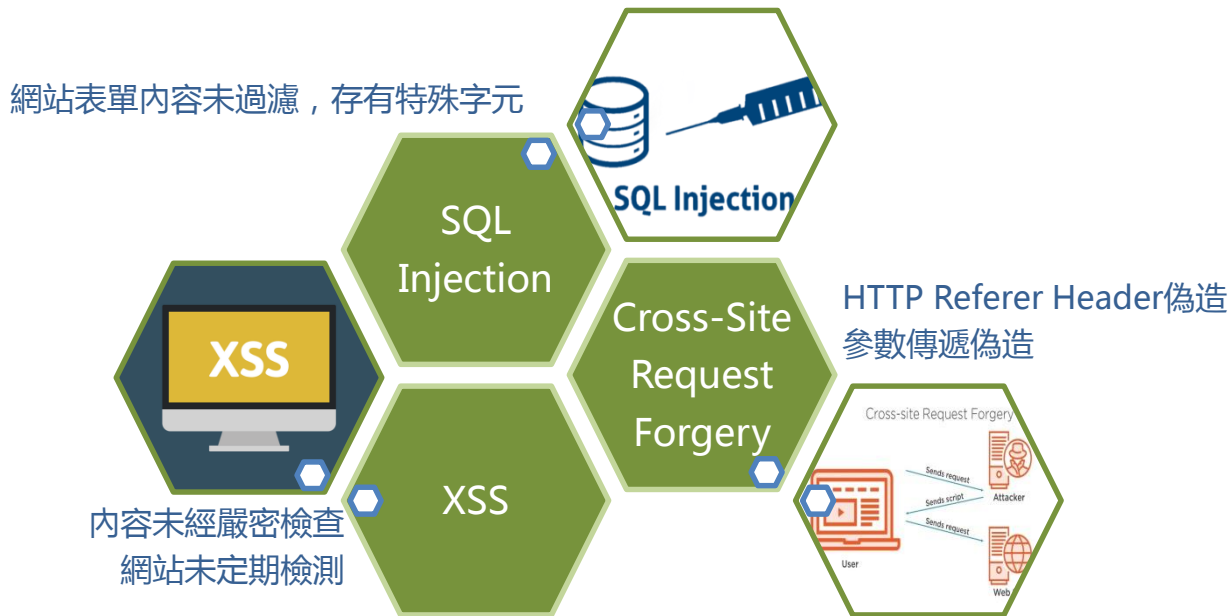
### 電商企業資安所面臨困難



- 組織人力精簡，員工多身兼數職
- 資訊人員缺乏足夠資安資訊，無法提供完整資安防護
- 企業資安應變多成為救火，所發生過的資安事件頻頻再現



# 台灣電子商務資安風險



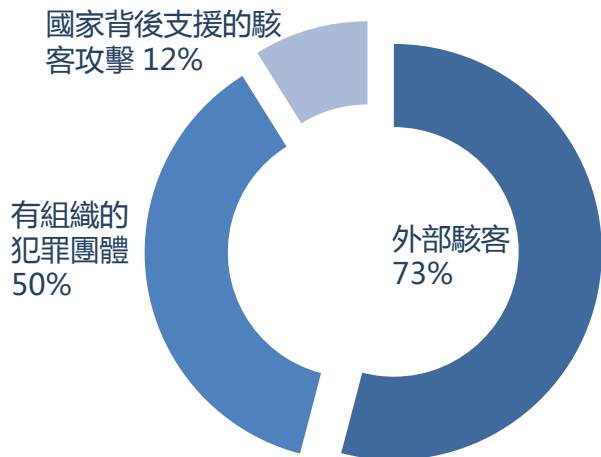
**此外，沒有安全開發應用系統的習慣，亦是導致資安事件原因**  
在設計時未考慮資訊安全因素；忽略異動管理、設定管理、存取控制、軟體測試；未能持續PDCA



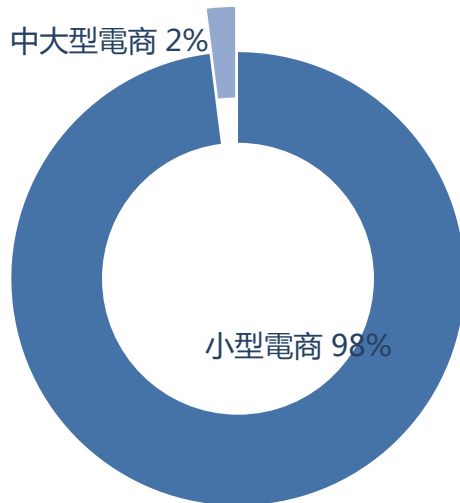
# 台灣電子商務資安事件分析



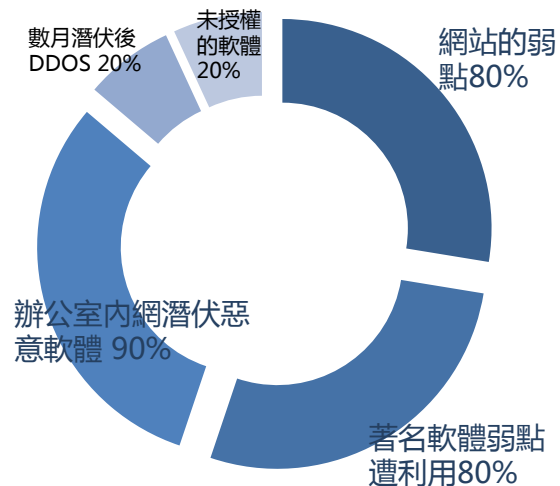
## 主導攻擊者



## 受駭者



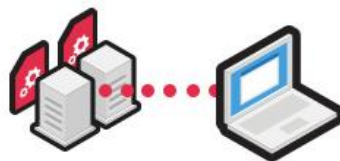
## 利用弱點



資料來源：2018 Data Breach Investigations Report ,, Verizon Enterprise Solution



# 資安攻擊四大階段



## 階段一: 感染

- 利用網站漏洞，上傳 webshell
- 下載惡意程式
- APT郵件、社交工程郵件、釣魚郵件
- 各式的注入攻擊(Cross-site, SQLi...)

## 階段二: 持續 (維持被感染狀態)

- Rootkit
- Bootkit(開機較作業系統更早載入)
- 修改registry
- 註冊成service

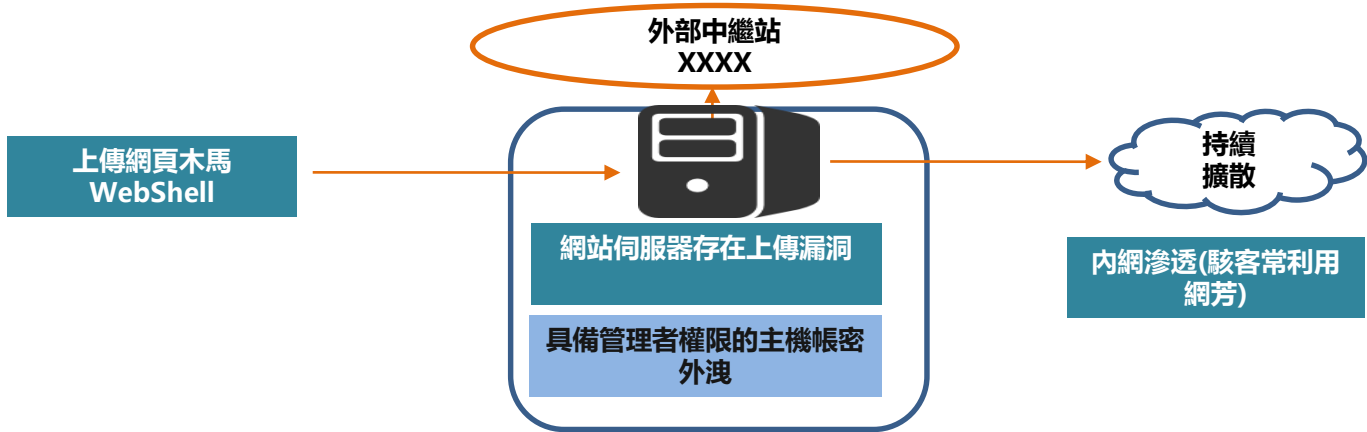
## 階段三: 報到

- 至中繼站下載真正的惡意程式
- 至中繼站回報受害電腦資訊
- 至中繼站接受要執行的指令
- 通常會設proxy、加密或架tunnel

## 階段四: 控制

- 盜取受害電腦資訊
- 利用側錄工具盜取帳號密碼或信用卡
- 進行企業內部擴散或是個人之親朋好友社交工程
- 發動DDoS攻擊

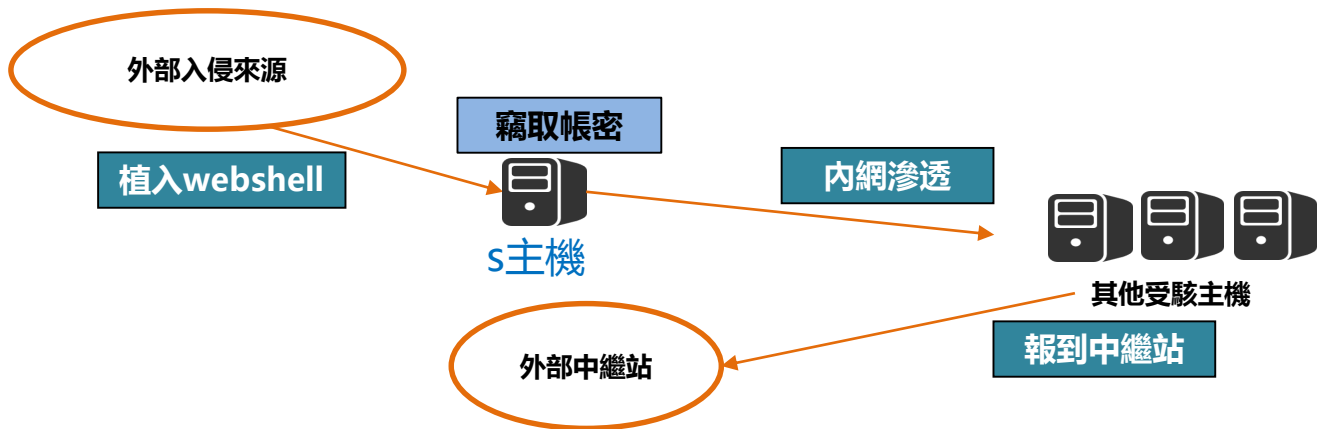




- 網站伺服器使用Apache Struts2 Framework，因Struts2的default.properties設定中，選擇預設載入之套件(Jakarta)存在弱點(CVE-2017-5638)，讓駭客遠端執行shell指令及上傳網頁木馬
- 具備管理者權限的主機帳密外洩
  - ✓ 主機管理者權限帳號存在**弱密碼**，在駭客內網滲透時易被暴力破解
  - ✓ 存在**特殊帳號**且具管理者權限可登入其它主機(例如**備份帳號**)
  - ✓ 駭客植入惡意程式(存在鍵盤側錄程式、密碼竊取工具)



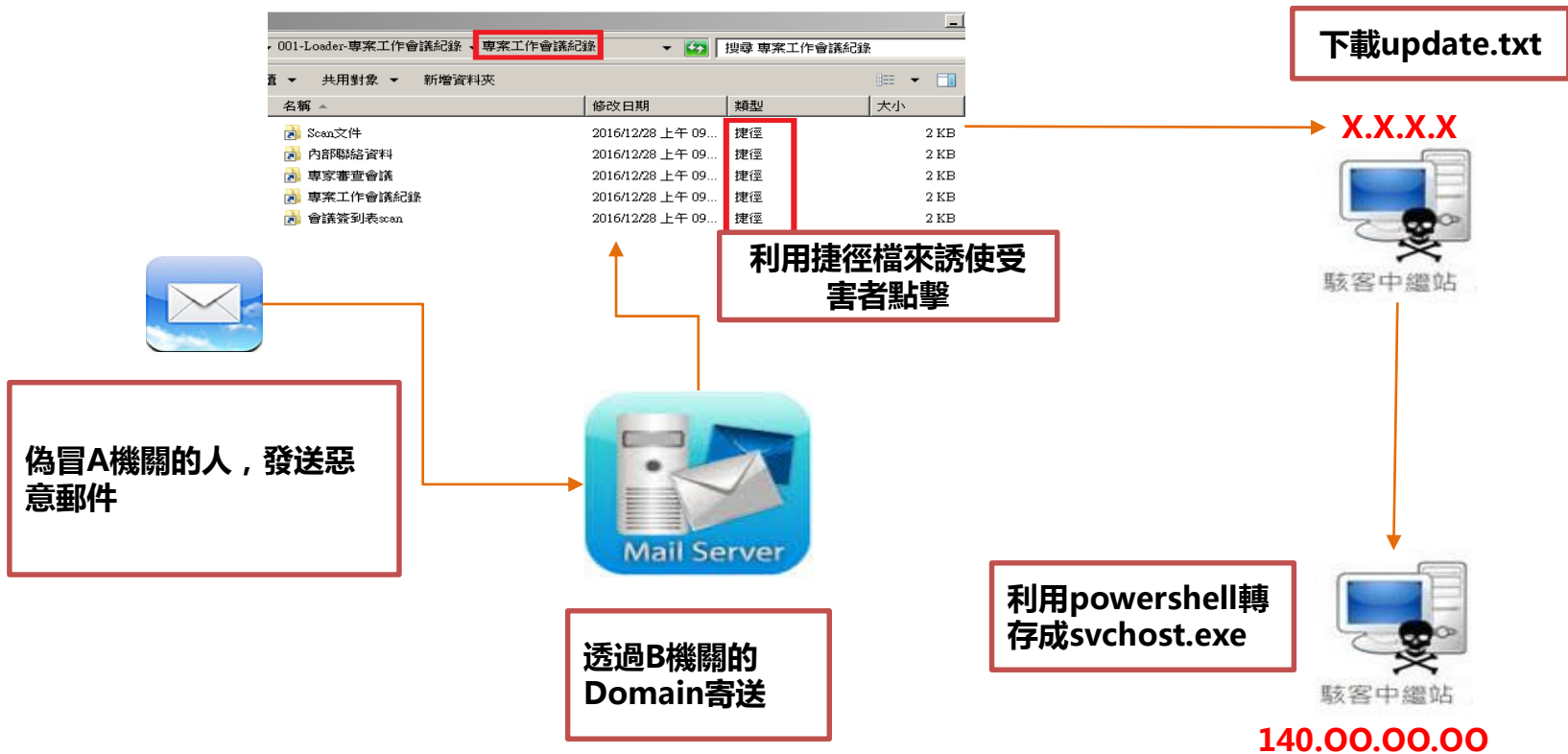
# 常見手法-利用網頁弱點



- 駭客從外網植入webshell
- 駭客由S主機中竊取帳密
  - ✓ 駭客使用密碼竊取工具，取得以下重要帳密
    - 網芳與遠端連線帳號
    - 該單位的系統管理者帳號
- 駭客利用網路芳鄰進行內網滲透
  - ✓ 利用內網防火牆較寬鬆的狀況，使用上述竊取之帳號以網路芳鄰、遠端桌面服務登入其他受駭主機
- 報到駭客中繼站
  - ✓ 駭客陸續植入惡意程式，使受駭主機連線至4個外部中繼站報到

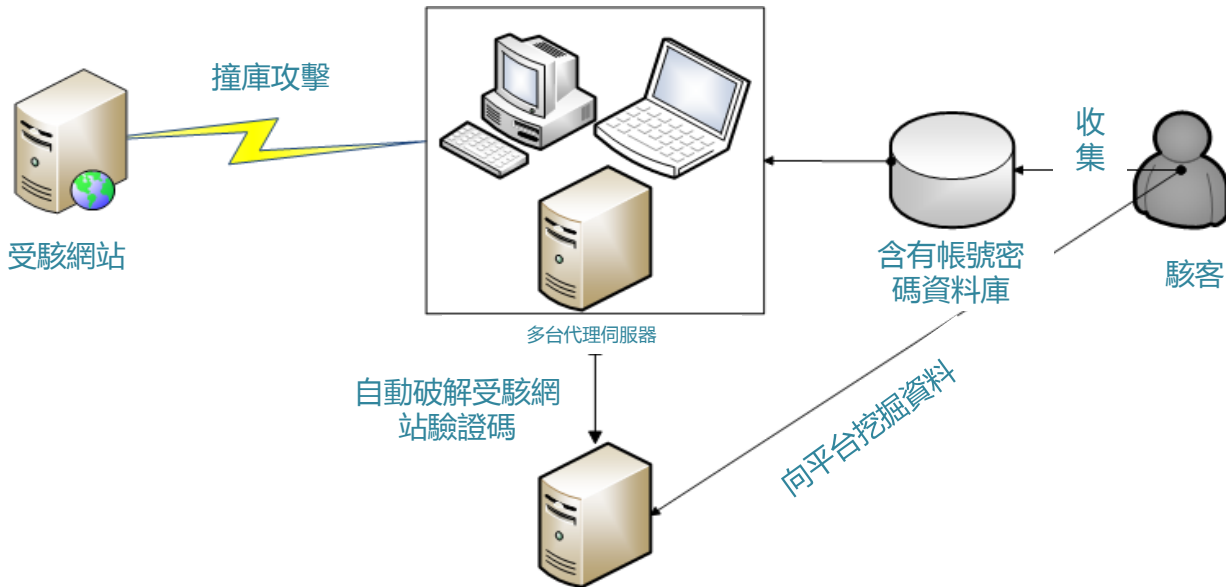


# 常見手法- APT郵件攻擊





# 常見手法-撞庫攻擊



- 撞庫攻擊不需要特殊的攻擊樣式，容易繞過WAF，因為完全合法，只利用弱密碼的特點，次數多了，每天都有收穫。
- 撞庫攻擊並不是暴力破解密碼
- 張公喝酒李翁醉。

# 下一波威脅-POS與加密貨幣已遭受連環攻擊

- 國際駭客組織Lazarus Group之子組織Bluenoroff針對韓國研發之POS，發佈惡意程式以竊取客戶上網付款卡片資訊，目前已發現有近千個受害客戶。受竊之用戶資料亦被利用為第二波攻擊加密貨幣企業之資料。
- 該手法係利用已附加於Microsoft Office文件之macro, javascript 與 CHM (微軟HTML幫助集)惡意檔案來入侵目標伺服器。

被竊取且利用為攻擊加密貨幣企業之客戶資料樣本



항목	내용
동일권 가맹점	129000TC
시장 점유율	80~70%
2017년 1월 거래액	300 million USD
일일 거래액	3300 million USD
동일권 시장	70 million USD
연간 수익	1000 million USD

시각	2016	2015	2014
시장 점유율	수익 구조 확립	서비스 안정화	블록체인 인식화
공격적 마케팅			블록체인 가맹점 강화
2017년 1월 실적			블록체인 금융 서비스 도입
신규서비스 개발			블록체인 서비스 개발
			비트코인 결제 도입

資料來源：Bluenoroff Targets Korean PoS software and Cryptocurrency businesses, Kaspersky Intelligence portal, Jan, 2018



- 電子商務新型態資安威脅趨勢
- **建立智慧情資與通報聯防機制**
- 落實電子商務資安事件處理建議



# 情資是聯防第一步



SECBUZZER



LOGIN

## API

透過SecBuzzer API服務,協助您使用我們的情資平台進行客製化搜尋與分析,獲得包含軟體漏洞、惡意程式、與惡意網域在內的資安情資,用以擴充您的情資資料庫。



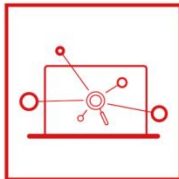
Update 2018 Jan. 23 14:01

Saturday



## VAS Service

Secbuzzer 提供自動化的網頁弱點掃描,輸入您的網站位址即可協助您檢視網站安全性,並且提供您完整的檢驗報告,協助您強化網站的資安防護。



Update 2018 Mar. 01 06:26

Thursday



## Emerging Topic

Secbuzzer 蒐羅全球資安專家在國際網路上的討論與分享,即時提供您熱門的資安議題、相關新聞事件、與威脅解決方案。透過 Secbuzzer 讓您掌握未來趨勢與資安脈動。



Update 2018 Apr. 19 08:23

Thursday



## Customized Threat Intelligence

SecBuzzer 提供客製化的威脅情資,透過簡單的步驟即可追蹤任何你感興趣的議題,深入了解資安專家的看法以及更多相關的資訊,自訂屬於您個人的情資頻道來了解全球資安威脅。



Update 2018 Feb. 02 01:45

Friday



## Threat Alert

搭載自主研发的自動化情資探索技術,Secbuzzer 為您收集並彙整新興的軟體漏洞與資安威脅議題,藉由電子郵件定期發送相關資訊,讓您隨時接收第一手情資。



Update 2018 Apr. 03 06:23

Tuesday





# Situation Room可以學習自我感知



為使用者建立  
獨一無二的模  
組，並進行使  
用者行為異常  
偵測



自動學習設  
立連線白名  
單，有效偵  
測異常連線

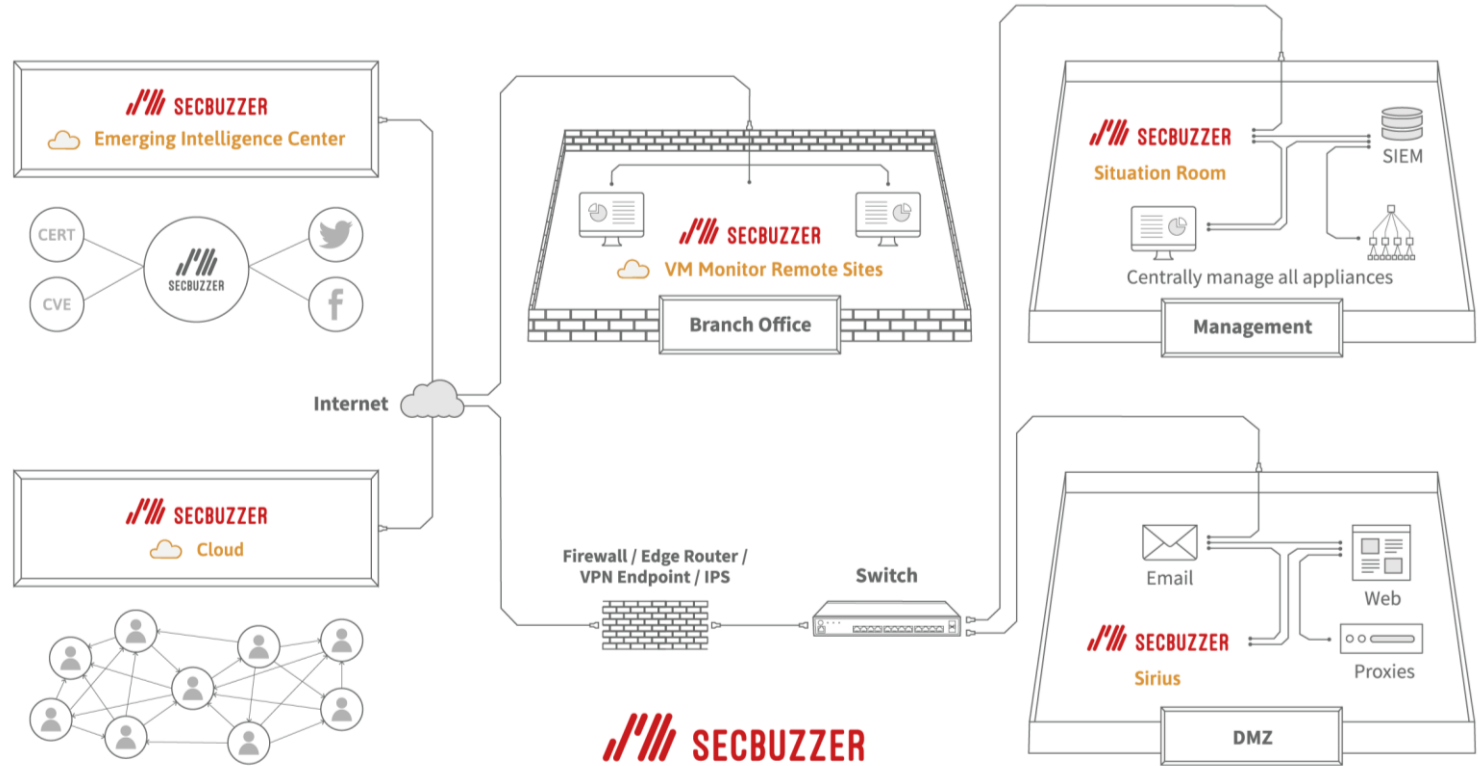
使用AI技術快  
速有效追蹤無  
檔案攻擊







# 從情資通報串連到事件中的偵測防禦

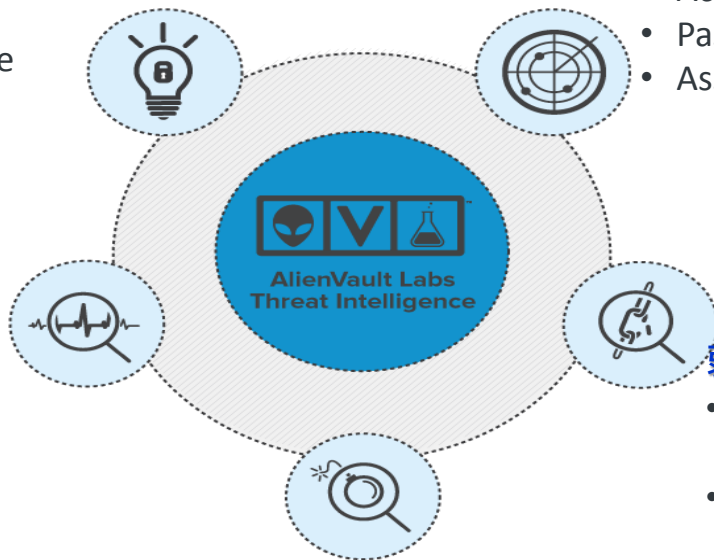


## SIEM

- Log Collection
- Event Correlation
- Incident Response

## 網路行為監控

- Netflow Analysis
- Service Availability Monitoring



## 資產盤點

- Active Network Scanning / 自動
- Passive Network Scanning / 被動
- Asset Inventory / 資產清單

## 弱點掃描

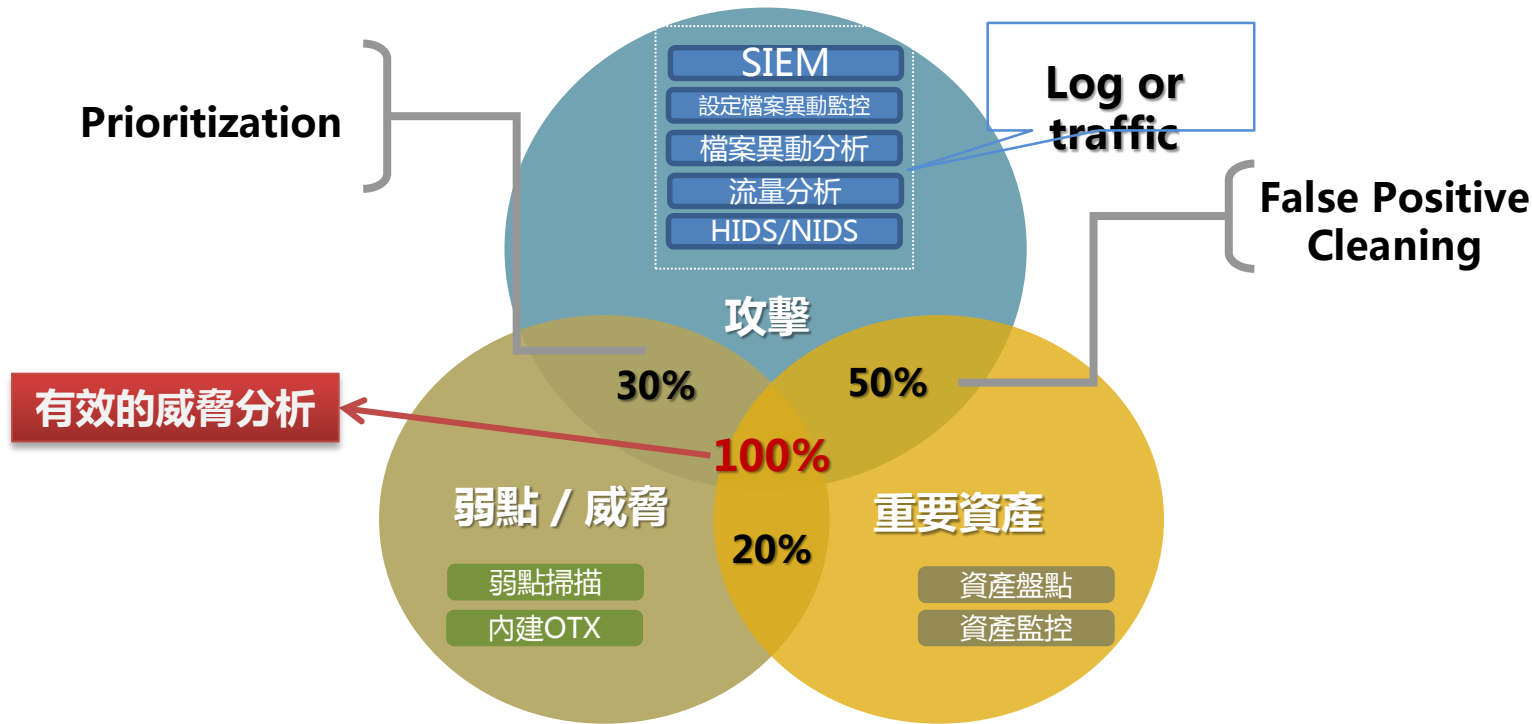
- Continuous Vulnerability Monitoring (持續性弱點監控)
- Authenticated / Unauthenticated Active Scanning

## 入侵偵測

- Network IDS(網路型入侵偵測)
- Host IDS(主機端入侵偵測)
- File Integrity Monitoring (檔案完整性監控)



# 建構關聯分析模組



參考資料：竣盟與本會合作項目



- 電子商務新型態資安威脅趨勢
- 建立智慧情資與通報聯防機制
- **落實電子商務資安事件處理建議**



# 落實電商資安事件處理建議



- 適時清空線上資料庫
- 前台與後台的分離
- 限制弱密碼的使用
- 密碼定期變更，長度比複雜度更重要
- 千萬不要使用非法軟體
- 勿留存歷史購物紀錄

政策 & 管理

情資 & 通報

- 善用**EC-CERT**等政府資源
- 參與SECBUZZER情資分享
- 事件通報形成聯防體系
- 軟體、設備等資產盤點

- 透過鑑識了解入侵根因
- 進行矯正與強化
- 更新網路以及應用程式白名單

鑑識 & 杜絕

應變 & 處理

- 接觸訂單資料電腦與其他網路隔離
- 網站登入檢查增加captcha 驗證，增加攻擊難度
- 人員攻防演練
- 定期資安健診(弱掃、源碼、滲透、紅隊演練)



# 感謝聆聽 敬請指教

---



服務網站：[ec-cert.org.tw](http://ec-cert.org.tw)  
服務專線：6607-2056  
服務信箱：[service@ec-cert.org.tw](mailto:service@ec-cert.org.tw)

