大數據公司ISO27001導入分享

功典資訊
陳柏霖 Action Chen
0930718943
Action_Chen@migocorp.com

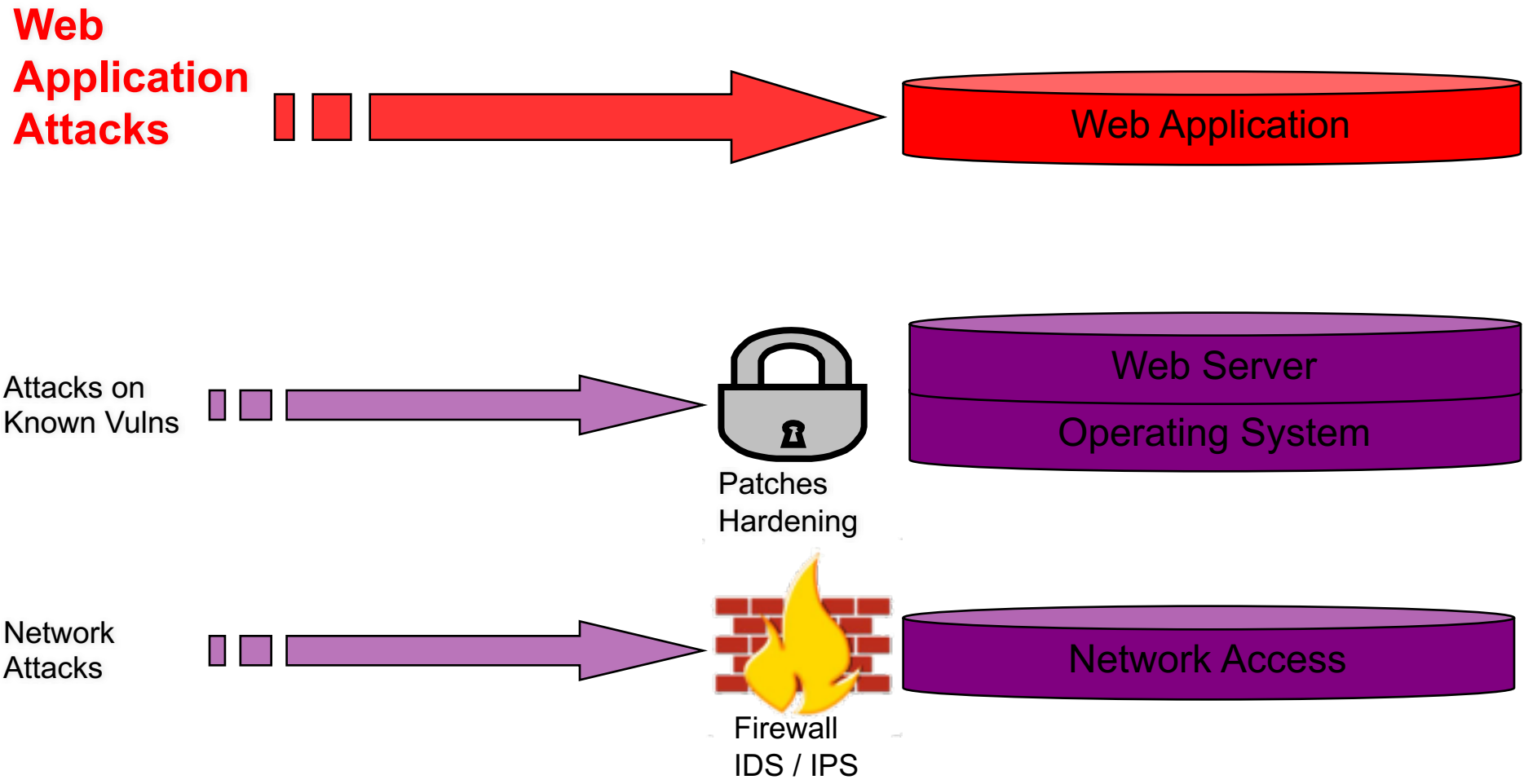
陳柏霖 講師簡介

- ISO27001主導稽核員認證、PMP、IT Project+專案管理認證、PBA商業分析師認證
- 現任功典資訊(Migo)資深系統架構師
- 資策會安全程式系統分析設計課程講師
- 專長：
  - 大數據系統架構設計維運
  - 服務水準協定(SLA)設計維運
  - 資訊安全、滲透測試、安全程式設計
  - DevOps

大綱

- 大數據公司面對的資訊安全威脅
- ISO27001導入經驗分享
- 大數據資訊系統開發的資安落實及方法工具應用實例
  - Threat Modeling
  - DevOps

大數據公司面對的資訊安全威脅



大數據公司面對的資訊安全威脅

Gartner Research

Publication Date: 1 December 2005 ID Number: G00127407

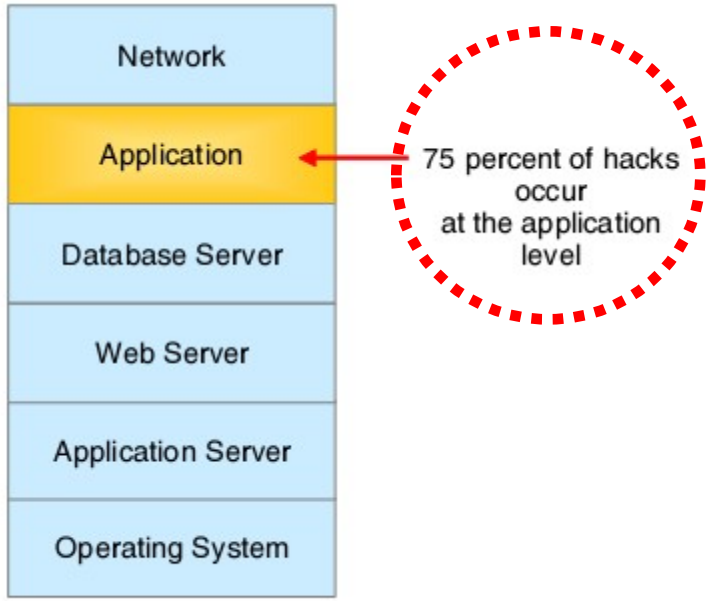
Now Is the Time for Security at the Application Level

Theresa Lanowitz

Applications must be available, useful, reliable, scalable and, now more than ever, secure. Therefore, build security directly into the application life cycle to reduce costs and significantly increase application security.

Security is many things to many people ...

- Network Layer
- ID Theft
- Physical
- Administrative
- Patches
- Infrastructure
- Denial-of-Service Attacks
- Hacks
- Worms and Viruses
- Terrorism (Cyber or Physical)



Source: Gartner (November 2005)

應用程式層的潛在威脅-密碼破解

- 如果攻擊者無法建立匿名連線到伺服器，他們就會嘗試建立一個已驗證的連線，並藉此提高權限，例如：**安全性不足的密碼原則、系統使用的是預設帳戶名稱、Session Hijacking攻擊**。

應用程式潛在威脅-輸入驗證

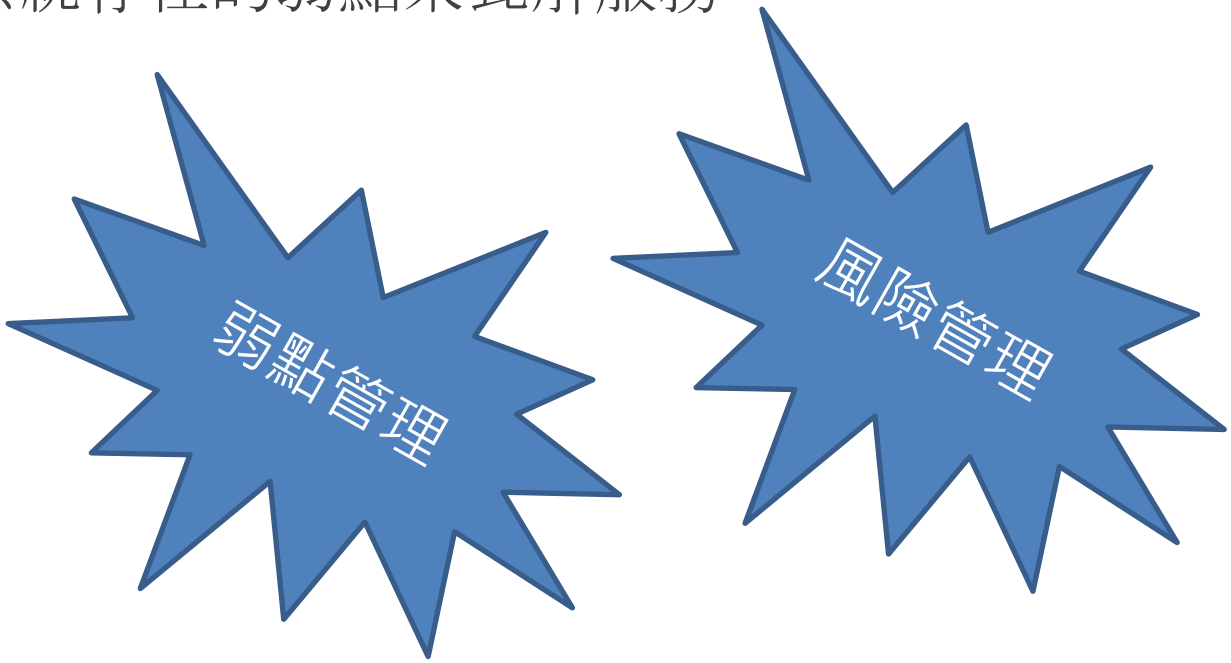
- 如果攻擊者發現應用程式中對輸入資料的類型、長度、格式或範圍，**缺乏黑名單、白名單、正規表示式，或長度限制**等驗證機制，那麼攻擊者就會透過SQL Injection、Cross-Site Scripting等攻擊手段，利用輸入來侵害應用程式。

系統層的潛在威脅-足跡探測

- 足跡探測的例子有**連接埠掃瞄、網路架構掃描、弱點掃描等**，攻擊者可用掃描工具來蒐集點點滴滴有用的系統層級資訊，為更有效的攻擊做準備。足跡探測可能洩露的資訊類型包括帳戶詳細資料、作業系統和其他軟體的版本、伺服器名稱，安全漏洞以及資料庫架構詳細資料等。

網路層的潛在威脅-拒絕服務

- **拒絕服務**有許多方法可以達到瞄準基礎結構中的數個目標。在主機上，攻擊者可以對應用程式使用暴力式 (Brute Force) 攻擊，或者攻擊者可能知道應用程式所在的服務或伺服器作業系統存在的弱點來瓦解服務



病毒/木馬的潛在威脅脅-任意執行程式碼

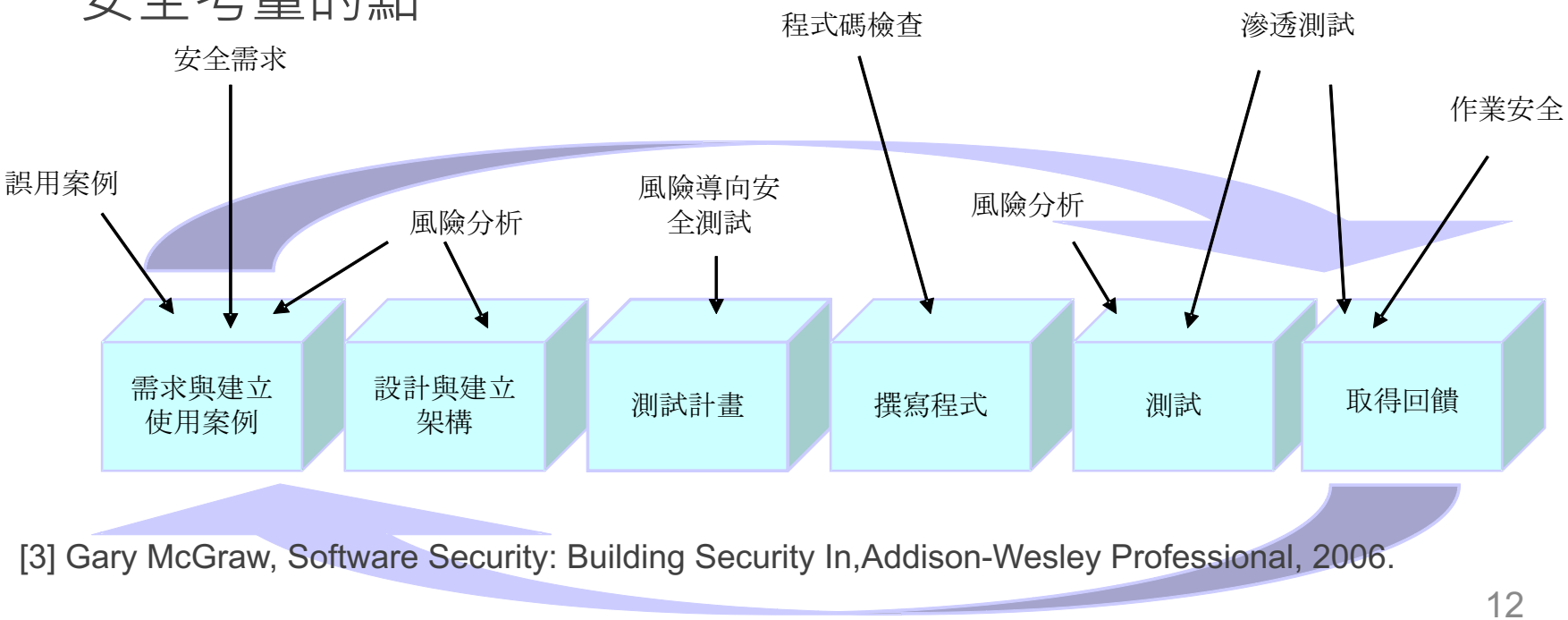
- 如果攻擊者可以在伺服器上執行惡意的程式碼，也就是**病毒或木馬程式**，則該攻擊者可以入侵伺服器資源，或準備進一步的攻擊來對抗下游的系統。如果攻擊者透過伺服器處理序所執行的程式碼權限過高，任意執行程式碼所造成的風險就會增加

全面性的威脅-APT攻擊

- 進階持續性威脅 (Advanced Persistent Threat, APT)，簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。
- **APT攻擊**可能持續幾天，幾週，幾個月，甚至更長的時間。APT攻擊可以從蒐集情報開始，這可能會持續一段時間。它可能包含技術和人員情報蒐集。情報收集工作可以塑造出後期的攻擊，嚴重者可竊取客戶資料，防不勝防。

大數據公司必須因應資訊安全威脅

- 不光是大數據，包括物聯網(IoT)，我們必須從軟體開發生命週期當中便加入資訊安全與隱私的考量。
- McGraw提出在軟體開發生命週期當中，有七個可以加入安全考量的點



[3] Gary McGraw, Software Security: Building Security In,Addison-Wesley Professional, 2006.

大數據公司必須因應資訊安全威脅

- 資訊系統架構設計的安全考量(**OWASP Top 10 弱點分佈**)

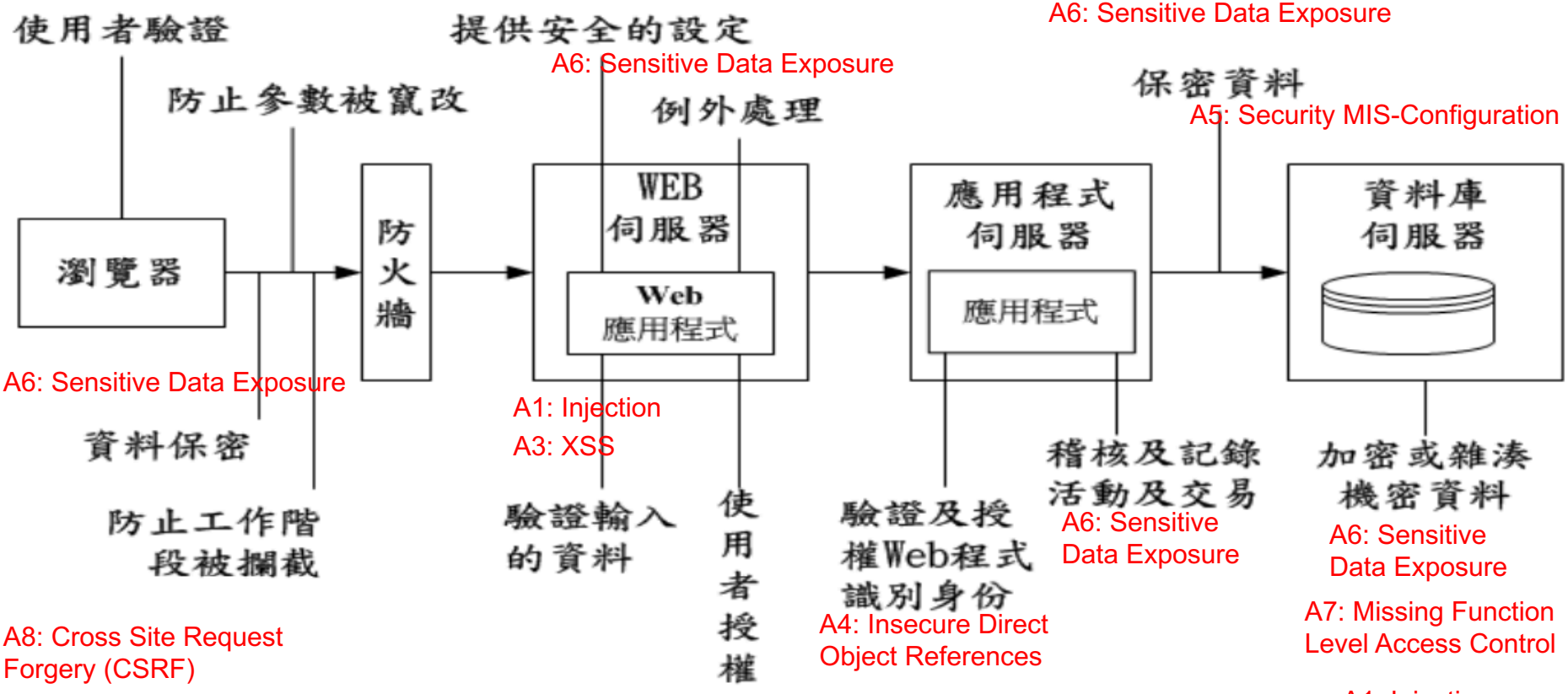
A10: Invalidated Redirects and Forwards

A2: Broken Authentication and Session Management

A9: Using Known Vulnerable Components

A5: Security MIS-Configuration

A6: Sensitive Data Exposure



A6: Sensitive Data Exposure

A1: Injection

A3: XSS

A8: Cross Site Request Forgery (CSRF)

A7: Missing Function Level Access Control

A4: Insecure Direct Object References

A6: Sensitive Data Exposure

A6: Sensitive Data Exposure

A7: Missing Function Level Access Control

A1: Injection

ISO27001導入經驗分享

- 建立安全政策與規劃

A.5 資訊安全政策	A.8 資產管理	
A6 在組織內外的安全考量	A.11 實體與環境安全	A.9 存取控制
A.15 供應商管理	A.12 作業安全	A.10 密碼使用
A.7 人力資源安全	A.16 資訊安全事件管理	A.13 通信安全
A.17 業務永續運作管理	A.18 符合性	A.14 系統開發、取得、維護

ISO27001導入經驗分享

- 以A.16 資訊安全意外事故管理(Information security incident management) 為例
  - A.16.1 管理資安意外事件並做改進：確保能夠用一個一致與有效的方法，建立包括安全事件與安全弱點通報的資訊安全事件管理程式
    - A.16.1.1 責任與程式(Responsibilities and procedures)：應建立相關程式，並定義人員責任，以便在資訊安全意外事件發生時，能夠快速、有效的進行回應
    - A.16.1.2 資訊安全事件報告：應該要透過合適的管道，對於資訊安全事件儘快的報告
    - A.16.1.3 通報資訊安全弱點：員工與約聘雇人員在使用資訊系統時應注意可疑的安全弱點，並進行通報

ISO27001導入經驗分享

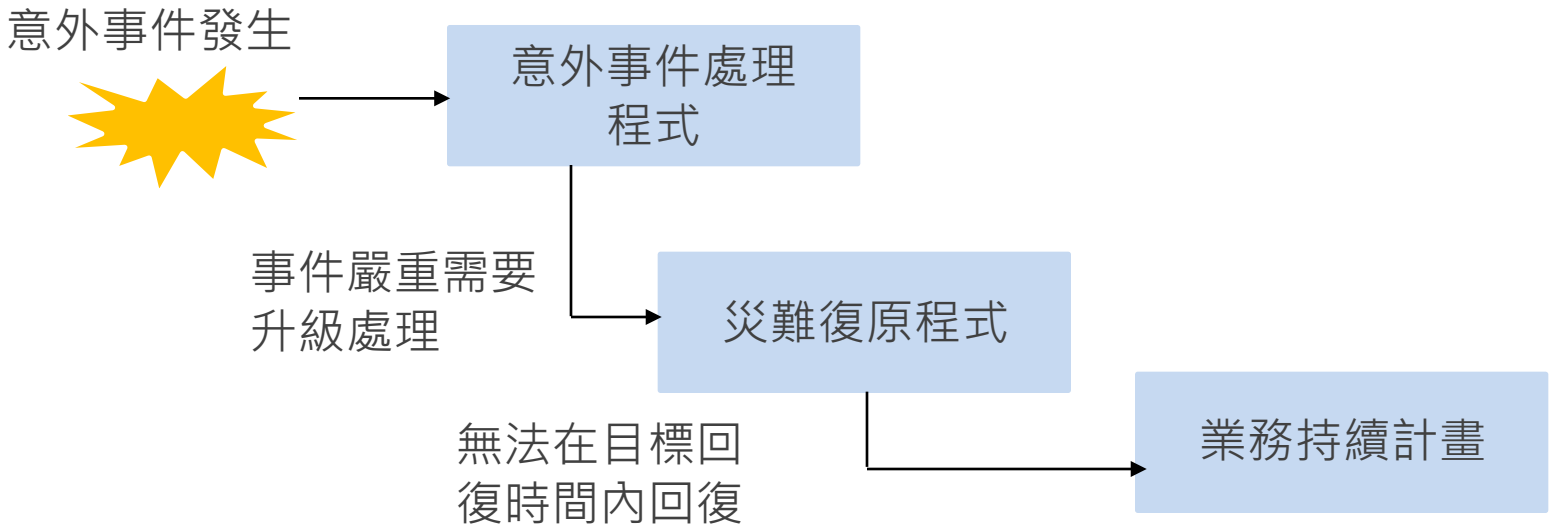
- A.16.1.4 對收到的資訊安全事件進行評估，以便判斷是否該被歸類為資訊安全意外事件
- A.16.1.5 對於資訊安全意外事件的回應：應該依照現前訂定的書面化程式，去對資訊安全意外事件去進行回應
- A.16.1.6 從資訊安全意外事件中學習：應該透過對於資訊安全意外事件與解決方案的的分析去獲得經驗，從而減少未來發生類似事件的可能性，並降低可能的衝擊。
- A.16.1.7 證據的收集：應該建立對於證據的識別、收集、萃取、保存程式。以便在需要時可做為證據而使用。

ISO27001導入經驗分享

- 事故與事件相關，A.12.4 記錄與監控(Logging and Monitoring)：需記錄事件，產生證據，以利追蹤根因
  - A.12.4.1 事件記錄(Event logging)：記錄包括使用者活動、例外事件、錯誤、資訊安全事件等的事件，並妥善保存與定期檢視
  - A.12.4.2 對於記錄資訊的保護：應該建立足夠的保護機制，確保記錄資訊不會被竄改或受到未經授權的存取
  - A.12.4.3 管理者與系統維運者的動作記錄：應該要保存系統管理者與系統維運者行為的記錄，此記錄應同樣的被保護與定期審查
  - A.12.4.4 對時(Clock synchronization)：相關系統的時間應對單一時間來源進行對時，以便事件發生時能夠追蹤軌跡

ISO27001導入經驗分享

- 事故矯正階段的安全考量
  - 建立意外事件處理程序，以減小意外發生時所造成的損失
  - 如需進入法律程式，需考慮數位證據的取得與保存
  - 意外事件處理程式應結合相關的災難復原與業務永續程式
  - 事件發生後要進行檢討以便建立矯正措施，並且確保矯正措施的落實



ISO27001導入經驗分享

- 再以客戶提供的資料報廢階段的安全考量為例
  - 針對存放或處理敏感資訊的裝置，或是可用以存取敏感資訊的金鑰，建立報廢程序。
  - ISO 27001:2013年的相關控制建議：
    - A.8.3.2 儲存媒體的報廢(Disposal of media)：應該依照建立的程式去對儲存媒體進行報廢
    - A.11.2.7 對於裝置的報廢或再利用(Secure disposal or reuse of equipment Control)：在裝置被報廢或再利用前，應該要確定其儲存媒體當中的敏感資料與授權軟體已被刪除
  - 這是大數據公司客戶最重視的議題之一，重要性與個資欄位加密及客戶資料不落地相當。

大數據資訊系統開發的資安落實及方法工具應用實例：Threat Modeling

- 步驟 1. 描述系統架構與識別資產
- 步驟 2. 運用資料流程圖掌握威脅
- 步驟 3. 拆分系統元件
- 步驟 4. 識別威脅項目並進行評估與回應

[6] CSA Mobile Working Group, Security Guidance for Early Adopters of the Internet of Things (IoT) , 2015.

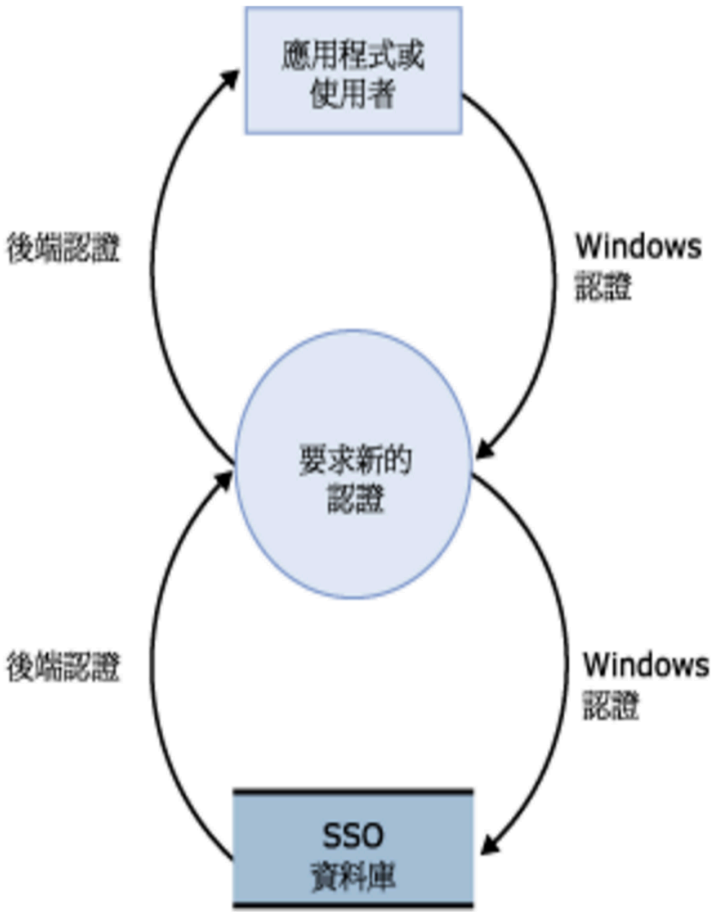
大數據資訊系統開發的資安落實及方法工具應用實例：Threat Modeling

- **1. 描述系統架構與識別資產**
  - 資產識別：包括資產的機密性、完整性與可用性。
  - 掌控應用架構
    - 網路圖：瞭解資產的實體位置、網路位置、傳輸媒介
    - 資料流程圖：識別重要資料，包含資料儲存位置、傳輸流程、系統邊界等，以及資料流程。
  - 建立安全政策
    - 一般性安全政策。
    - 特別針對大數據或物聯網應用的安全政策。

大數據資訊系統開發的資安落實及方法工具應用實例：Threat Modeling

2. 運用資料流程圖掌握威脅

圖 2 企業單一登入實例的 DFD



1.使用者或應用程式以 Windows 認證登入。

2.企業單一登入使用 Windows 認證來要求後端網路的認證。

3.企業單一登入將 Windows 認證對應到 SSO 資料庫中儲存的後端認證。

4.企業單一登入會擷取後端認證，然後使用它們將使用者或應用程式連接到後端網路。

大數據資訊系統開發的資安落實及方法工具應用實例：Threat Modeling

- **3. 拆分目標系統元件，分別繪製資料流程圖**
  - 可依系統分，或依主要資訊資產分，繪製各系統或資訊資產的資料流程圖。
  - Demo

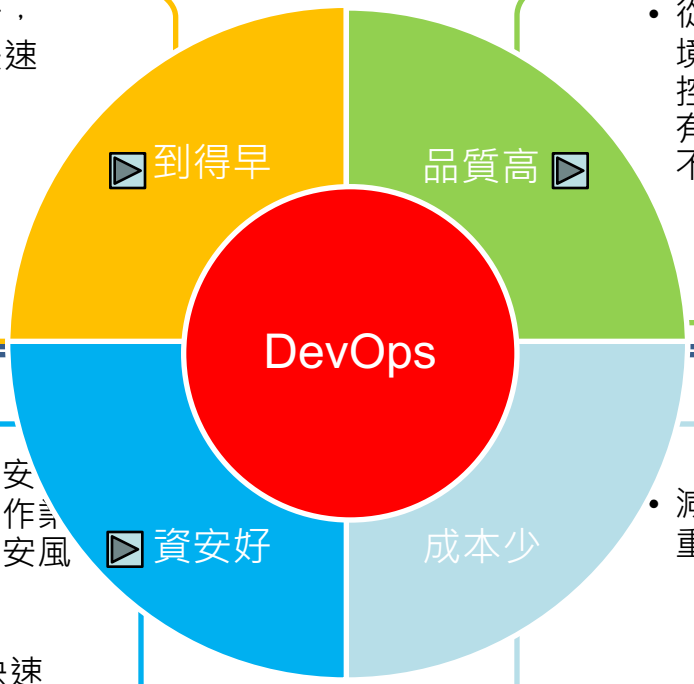
大數據資訊系統開發的資安落實及方法工具應用實例：Threat Modeling

- **4. 識別威脅項目並進行評估與回應**
  - 可參考STRIDE模型並做擴充，評估威脅項目：
    - 偽裝使用者或裝置識別碼(Spoofing Identity)
    - 資料竄改(Tampering with Data)
    - 否認(Repudiation)
    - 資訊外洩(Information Disclosure)
    - 阻斷服務(Denial of Service)
    - 提高權限(Elevation of Privilege)
  - Demo

大數據資訊系統開發的資安落實及方法工具應用實例：DevOps

- 快速自動化佈署，一日可多次發行，到得早，快速交付，快速改善，快速變現。

- 從開發環境、測試環境到正式環境，任何發行或變更都進行版本控制、自動功能測試、自動佈署，有效減少失誤、人為疏失、測試不足等問題，品質自然高。



- 減少人工作業，可降低來自內部資安攻擊，並減少資安漏洞，特別在變更作業時，最容易發生人為疏失，造成資安風險。
- 可確保業務的持續性(Business Continuity)，系統Downtime時可快速回復備份、備援版本，減少可用性造成的衝擊。

- 減少人力需求，減少人為錯誤的重工，成本自然少。