Microsoft Azure

Secure DevOps：應用安全原則與實踐

威脅建模

模組概述

- 威脅建模原理
- 威脅建模過程
- 圖解
- 威脅枚舉與優先順序
- 緩解與驗證

Microsoft Azure

威脅建模的原理

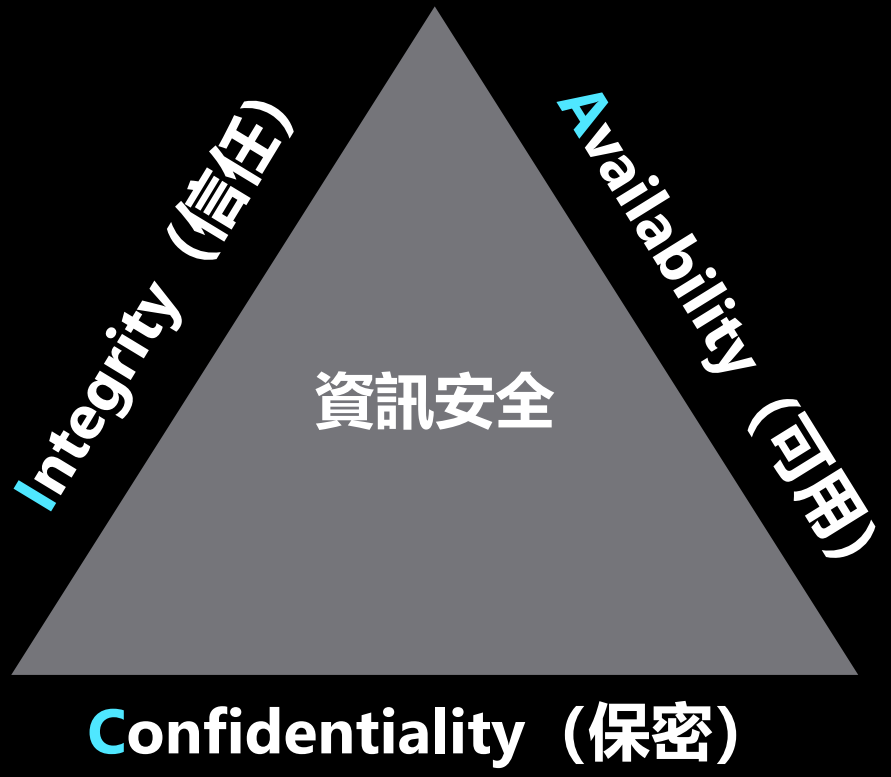
高價值資產與資訊

“如果你用同樣的努力保護回形針和鑽石，很快你會有更多的回形針，而更少的鑽石。”

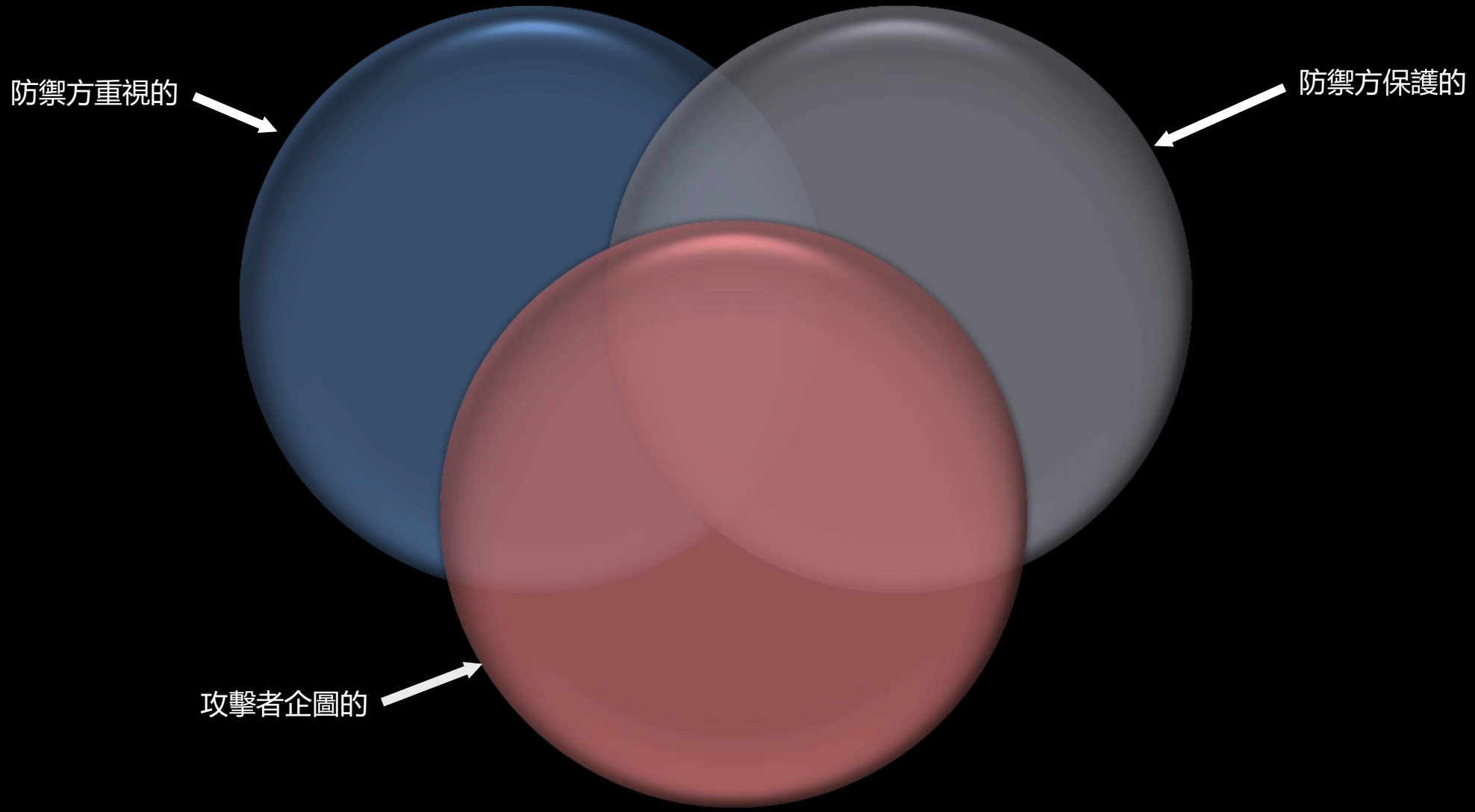
—— 前美國國務卿 Dean Rusk

資訊安全的核心支柱

CIA Triad



安全效能



為什麼我們的安全措施不有效?

資產錯誤分類

- 難以理解的分類
- 錯誤分類的影響巨大

報告不足

- 在異構解決方案中缺乏一致的報告
- 它有效嗎?

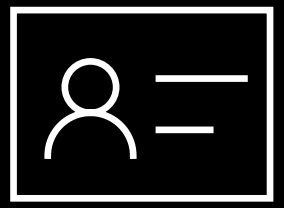
未執行的政策和控制措施

- 依賴使用者
- 工具與政策不一致且缺乏自動化
- 工具降低生產力，用戶繞過流程

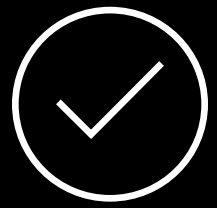
影響成本很少被認識到

- 應用分類和保護需要時間、金錢和資源。
- 對單條記錄與匯總記錄的丟失缺乏理解。

良好系統的特性

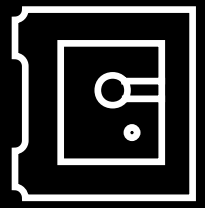


Authentication（認證）

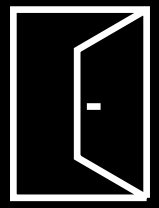


Integrity（誠信）

Nonrepudiation（不可篡改）



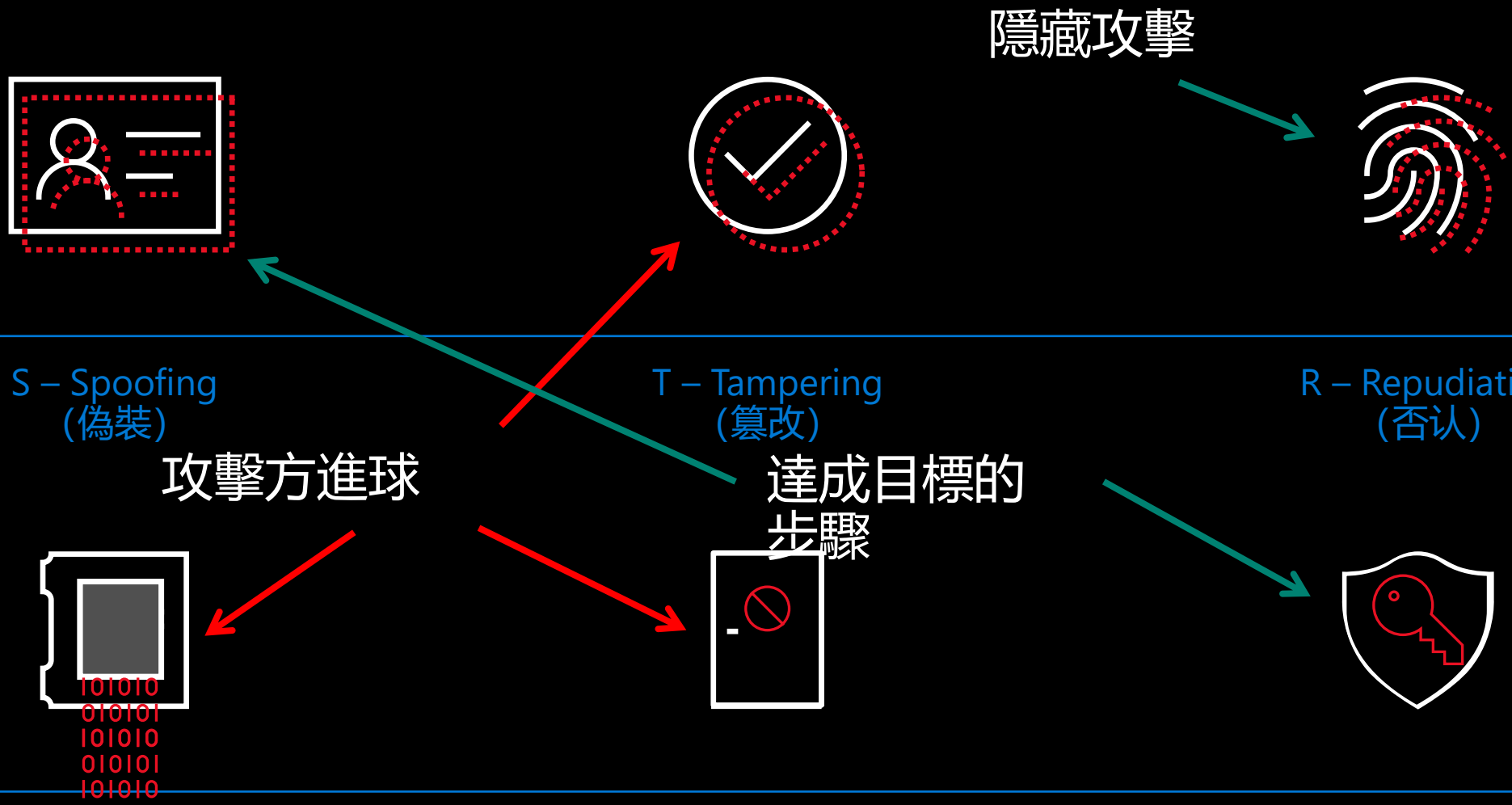
Confidentiality（保密性）



Availability（可用性）

Authorization（授權）

糟糕系統的特性：STRIDE



威脅建模

“如果我們雙手被綁在身後（其實並沒有），只能做一件事來提升軟體安全…… 我們會每天做威脅建模。”

麥可·霍華德
高級首席網路安全架構師
Microsoft 公司

威脅建模

威脅建模是一個理解系統安全威脅、確定這些威脅風險並建立適當緩解措施的過程。

- ✓ 讓你的安全目標浮現出來
- ✓ 提升意識
- ✓ 降低剩餘風險
- ✓ 讓你與組織風險政策保持一致

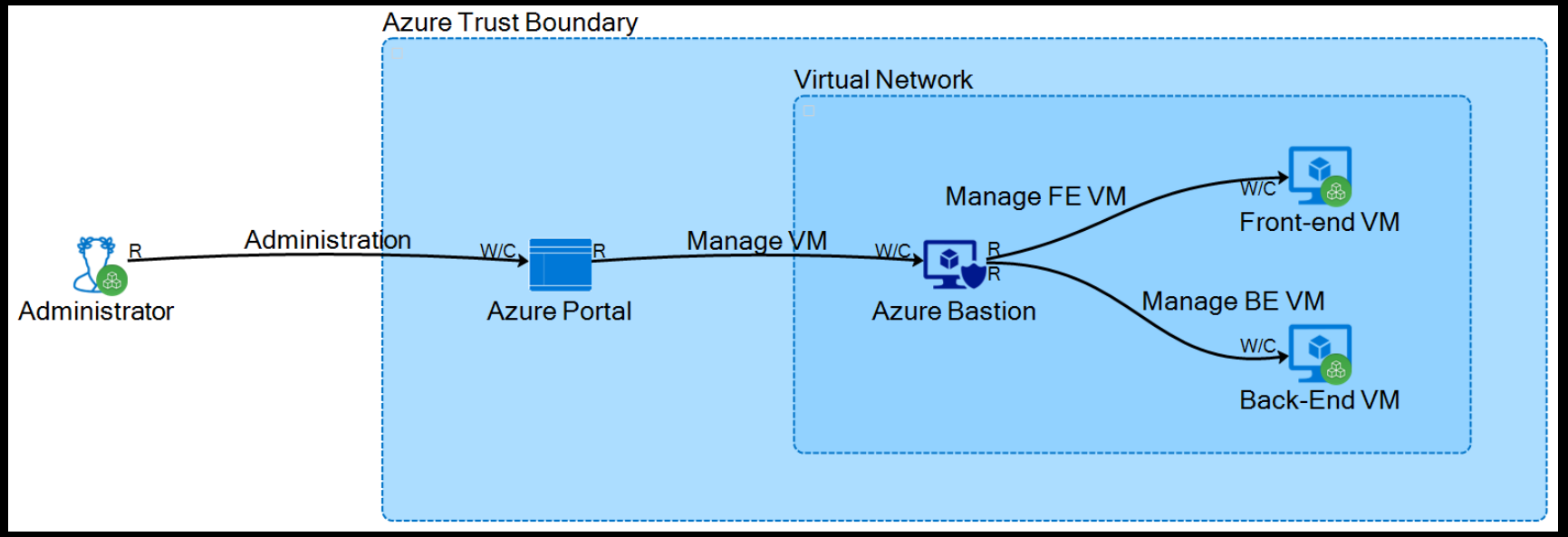
Microsoft Azure

威脅建模過程

理解解決方案

理解解決方案 | 識別風險 | 識別緩解措施 | 測試緩解措施 | 實施緩解措施 | 選擇緩解措施 | 管理剩餘風險

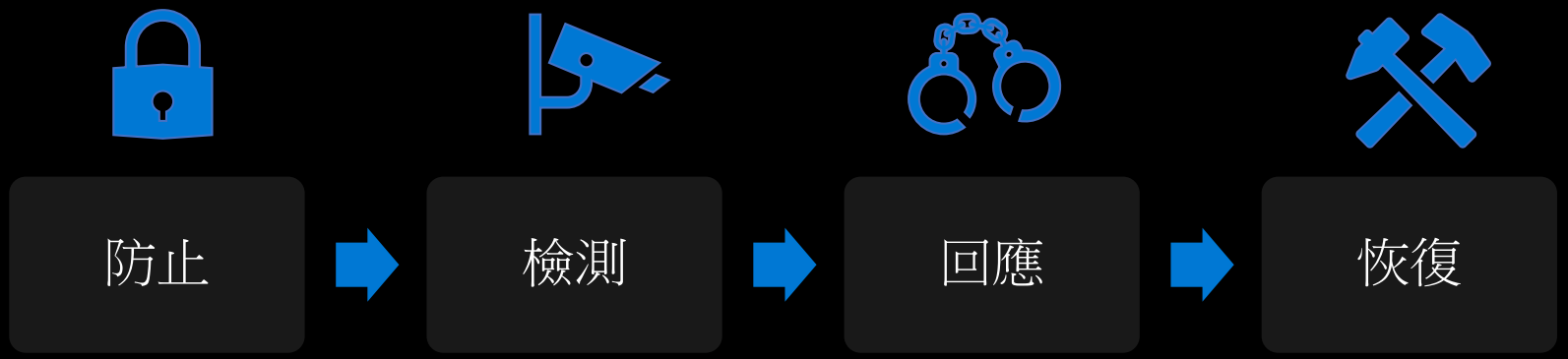
- ✓ 審查檔
- ✓ 訪談架構師和團隊
- ✓ 深化對關鍵主題的瞭解



識別緩解措施

理解解決方案 | 識別風險 | 識別緩解措施 | 測試緩解措施 | 實施緩解措施 | 部分緩解措施 | 管理剩餘風險

- ✓ 確定標準緩解措施
- ✓ 尋找替代方案，控制多樣性
- ✓ 定義路線圖



有效威脅建模會議

會議前制定威脅模型草案
- 利用會議進行討論

先看 DFD 的攻略

識別最有趣的元素
- 資產（如果你發現的話）
- 入口/信任邊界

針對這些元素逐項分析 STRIDE

跨元素/反覆出現的威脅
- 考慮庫，重新設計

Microsoft Azure

圖表

隔離與信任邊界

所有通信必須跨越信任邊界
- 沒有秘密通信路徑或數據傳輸

信任邊界定義了什麼是可信的政策
- 例如，機場安檢

在邊界處提 STRIDE 問題

Spoofing（欺騙）

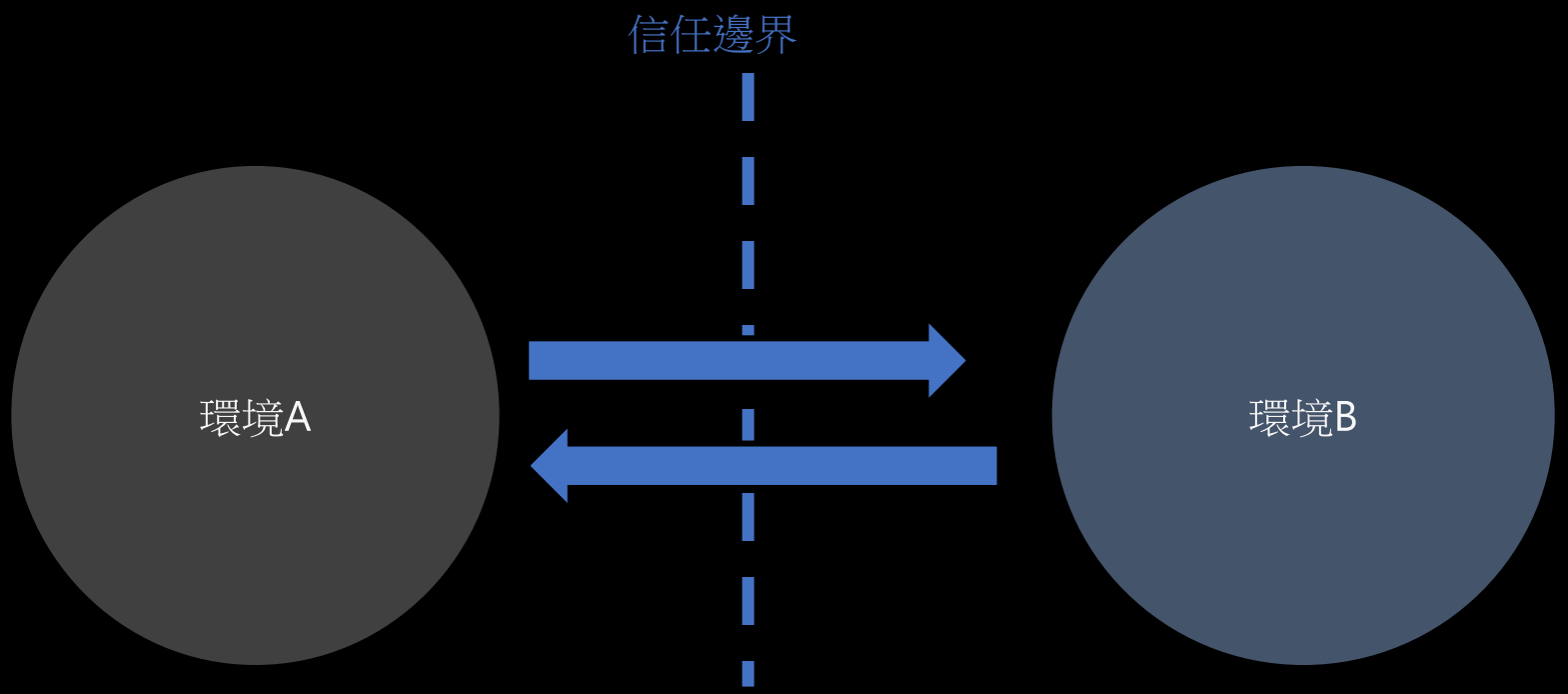
Tampering（篡改）

Repudiation（否认）

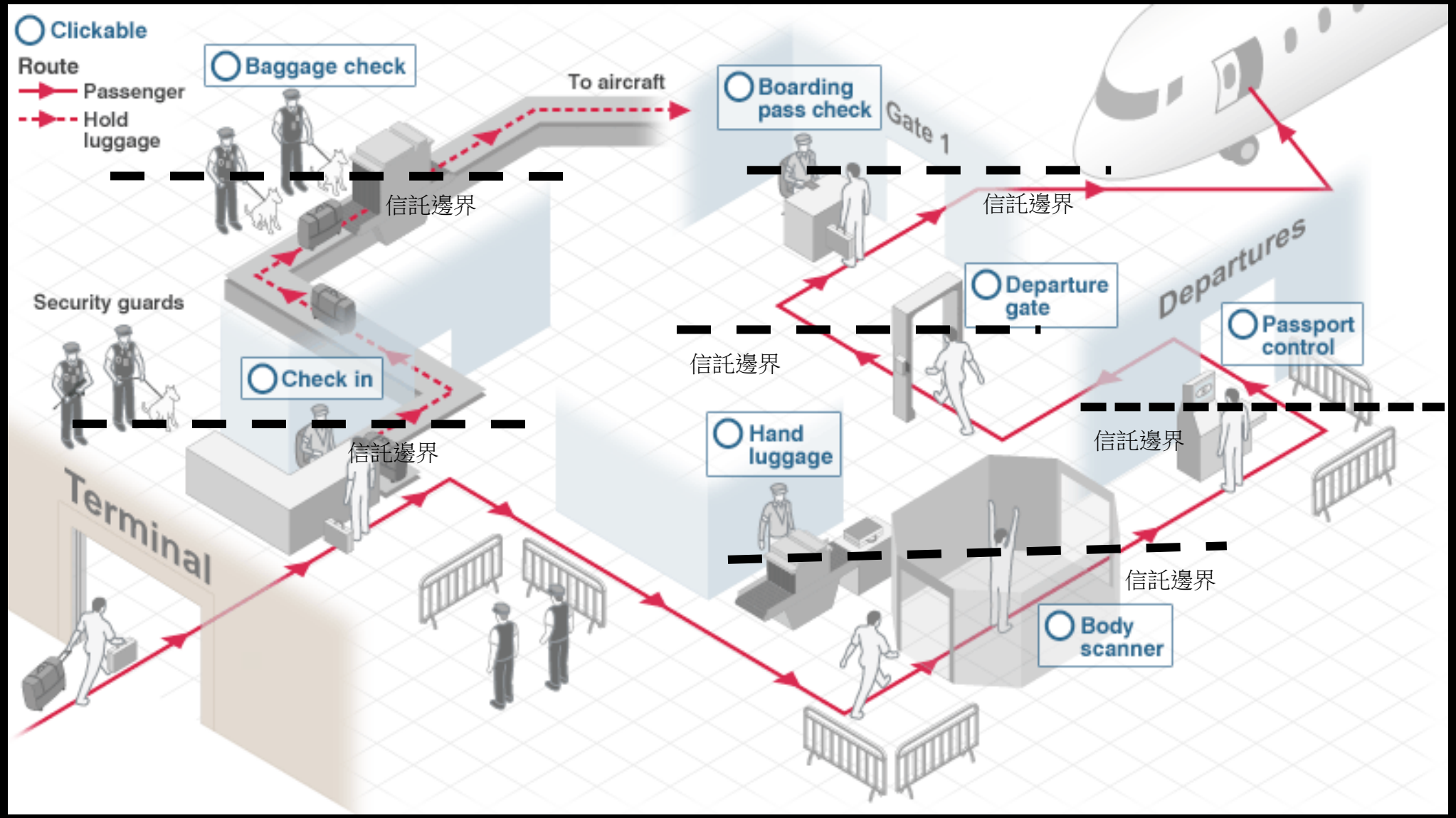
Information Disclosure（信息披露）

Denial of Service（拒绝服务）

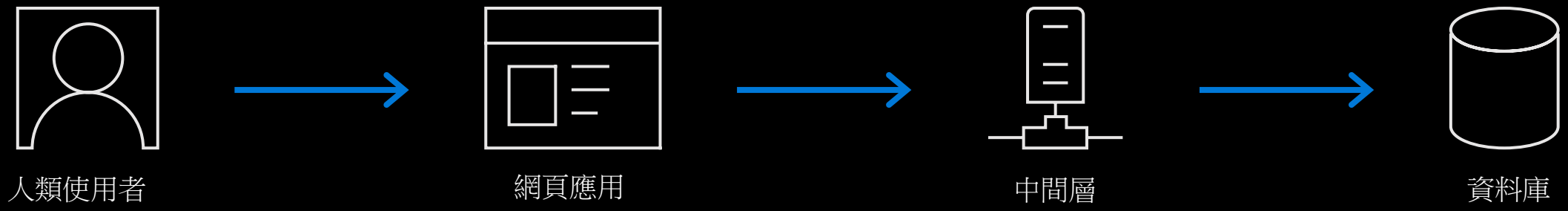
Elevation of Privilege（權限提升）



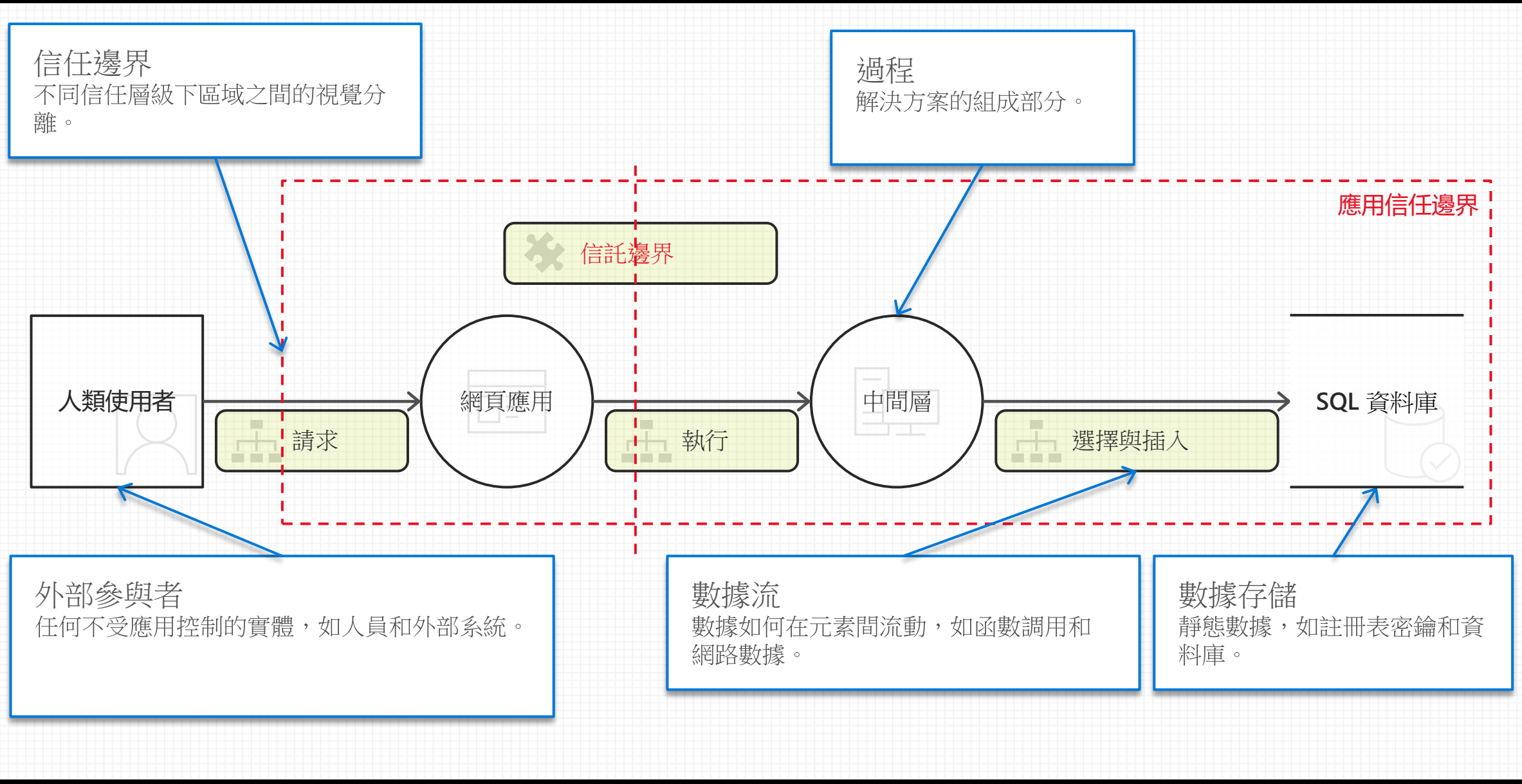
機場示例


Clickable
Route
Passenger
Hold luggage
Baggage check
To aircraft
Boarding pass check
Gate 1
信託邊界
信託邊界
Departures
Departure gate
Passport control
Security guards
Check in
信託邊界
信託邊界
Hand luggage
信託邊界
Terminal
Body scanner

威脅建模示例



威脅建模示例圖示


信任邊界
不同信任層級下區域之間的視覺分離。
過程
解決方案的組成部分。
應用信任邊界
信託邊界
人類使用者
請求
網頁應用
執行
中間層
選擇與插入
SQL 資料庫
外部參與者
任何不受應用控制的實體，如人員和外部系統。
數據流
數據如何在元素間流動，如函數調用和網路數據。
數據存儲
靜態數據，如註冊表密鑰和資料庫。

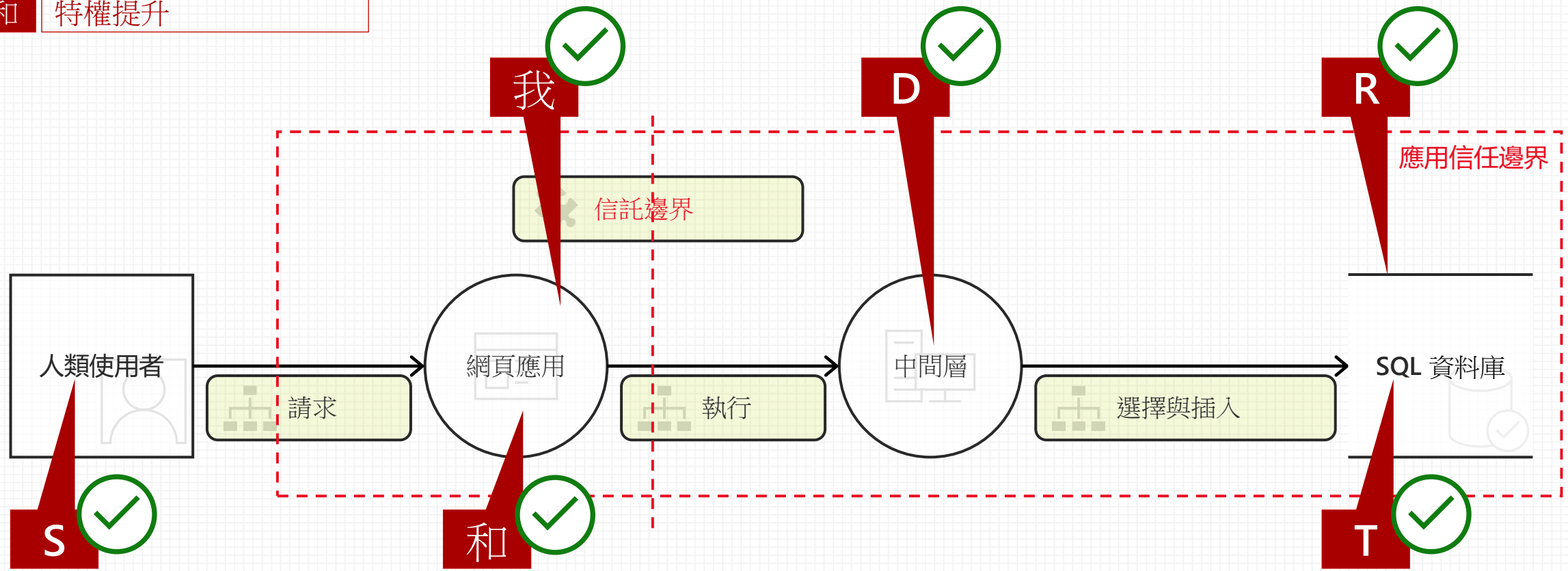
威脅識別

專家：
頭腦風暴和其他非正式方法。

專家與非專家
使用 STRIDE 威脅類型。
基於 Microsoft 安全回應中心（MSRC）的問題和常見漏洞與暴露（CVE）（詳見 http://cve.mitre.org）。

威脅建模示例圖示

S	欺騙
T	篡改
R	否認
我	資訊披露
D	拒絕服務
和	特權提升



按元素識別 STRIDE 威脅

元素	S	T	R	我	D	和
 外部實體	✓		✓			
 過程	✓	✓	✓	✓	✓	✓
 數據存儲	!	✓	!	✓	✓	✓
 數據流		✓		✓	✓	

✓ Threat

! Depends on store

常見的錯誤

缺失的參與者

它們代表最高風險，威脅模型必須包含所有這些因素。

例如：“*誰會閱讀審計資料庫？*”

缺失的數據來源

如果應用消耗數據，數據應該來自某個地方。

例如：“*預填充資料庫使用的源碼是什麼？*”

缺失的數據處理器

沒有邏輯幫助，數據無法在資料庫間流動。

例如：“*Jobs 或 ETL 流程是用某個 SSIS 軟體構建的嗎？*”

實用的 STRIDE

按流程
- 偽造任何端點; 來源和目的地（包括重放攻擊）
- 在傳輸過程中和/或通過惡意輸入進行篡改和信息洩露
- 任何參與者的抵賴（取決於信任級別）
- 拒絕服務——物理上的或來自源端，目的端很少發生
- 通過惡意輸入或來自先前行為的資訊提升許可權（圖形思維）

過程
- 終端用戶設備上的直接篡改和信息洩露
- 由於RBAC薄弱導致的篡改和信息洩露
- 通過疏忽的錯誤處理導致的拒絕服務和信息洩露
- 機密處理和加密

數據存儲
- 篡改和信息洩露
- 由於資源耗盡導致的拒絕服務
- 由於弱認證授權（ACLs，RBAC）導致的許可權提升
- 由於注入攻擊導致的許可權提升

干擾

不必擔心這些威脅（除非你專門建模它們）

- 計算機感染了惡意軟體（惡意程式）。
- 有人拆除了硬碟並進行篡改
- 管理員正在攻擊使用者
- 一個使用者正在攻擊自己

如何優先處理威脅

先做簡單的修復。
«Bug Bar» 方法
CVSS – 對某些行業 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
DREAD（風險 = 損害 + 可重複性 + 可利用性 + 受影響使用者 + 可發現性）
«Delphi Oracle» 方法

漏洞門檻是適用於整個軟體開發專案的品質關卡，用於定義安全漏洞的嚴重性閾值。

漏洞門檻一旦設定，就不應放寬。

Microsoft Azure

緩解與驗證

緩解已識別的威脅

緩解措施（按偏好排序）

- 重新設計
- 標準緩解措施
- 自行設計的、非行業標準的自創緩解措施（你不是專家）

商業決策

- 在政策範圍內轉移風險
- 在政策範圍內接受剩餘風險

識別外部責任。

標準緩解措施示例

威脅	標準緩解範例	
欺騙	多因素認證（MFA） 數字簽名	消息認證碼 OpenID Connect
篡改	ACLs 數字簽名	消息認證碼
否認	強認證	安全日誌與審計
資訊披露	加密	ACLs、RBAC
拒絕服務	ACLs 配額	高可用性設計
特權提升	ACLs Group或角色成員	輸入驗證

確定外部責任

例子：

- Microsoft 的 Azure Services。
- 第三方軟體即服務（SaaS）解決方案

可以合理假設的（也許）：

- 安全實施和測試
- 定期針對已知漏洞進行補丁

不能輕易假設的事：

- 安全配置

驗證威脅和緩解措施的品質

好的威脅描述

- 攻擊
- 背景
- 影響

良好的緩解措施

- 與威脅關聯
- 描述緩解措施
- 提交漏洞或工作項。

通過提交漏洞或工作項，使這些威脅變得可執行/可落地！

謝謝！