簡暴的 OWASP Threat Dragon 威脅建模實作

林家瑋 (Ray Lin)
2025/06

林家瑋 (Ray Lin), ray.lin@ifus.tw

- **全球首批 GCR首位 AWS Security Hero**
- **iFUS System Consultants Ltd. – 資安長(CISO)**
- **DataBrushing.ai (QSP) – 數位長(CDO)**
- **長宏專案(PM-ABC) – PMI授權培訓講師 (PMP/PMI-ACP)**
- **全智網科技(AI Network) – ISC2授權講師 / AWS授權講師**
- **巨匠電腦 – 資安課程合作講師**
- **ISC2 Taipei Chapter – 理事 / 媒體公關委員會 主委　　| PMI Taiwan獎項辦公室(PTGA) – 執行長**
- **DevSecOps Taiwan – 社長**
- **登豐數位、鑑智實相、捷虹資訊、德慎精算、睿峯管顧 – 顧問 / 講師**
- **曾服務於美商、日商、台商、新創、上市櫃、跨國集團等不同型態的公司**
- **擔任過CEO、COO、CISO、CDO、產品主管、IT主管、業務主管、資深SI工程師與資深PG**
- **曾獲台灣發明家創意獎、PMI-TW優良志工獎與績優執行理監事、翻譯出版7本知名敏捷書籍，並取得超過40張國際證照**

威脅建模步驟

1. 定義工作範圍：確認威脅建模範疇，包括外部依賴、進入點、離開點、資產與信任邊界等。使用資料流圖(DFD, Data Flow Diagram)來視覺化系統的資料流和處理節點，這有助於識別系統的潛在弱點
2. 辨識威脅：分類威脅，並根據嚴重性或發生機率對威脅進行排序
   - OWASP Top 10：有助於識別當前最普遍的Web應用安全風險
   - STRIDE：由微軟提出的威脅分類模型，每個元素對應一種安全風險
   - DREAD：用於評估威脅嚴重性的模型
3. 擬定對策與緩解方法：規劃和實施適當的風險緩解措施(ATMA)
4. 評估工作成果：對進行的威脅建模活動、發現的威脅以及實施的控制措施進行評估，並進行後續的驗證和審核，以確保安全措施的有效性

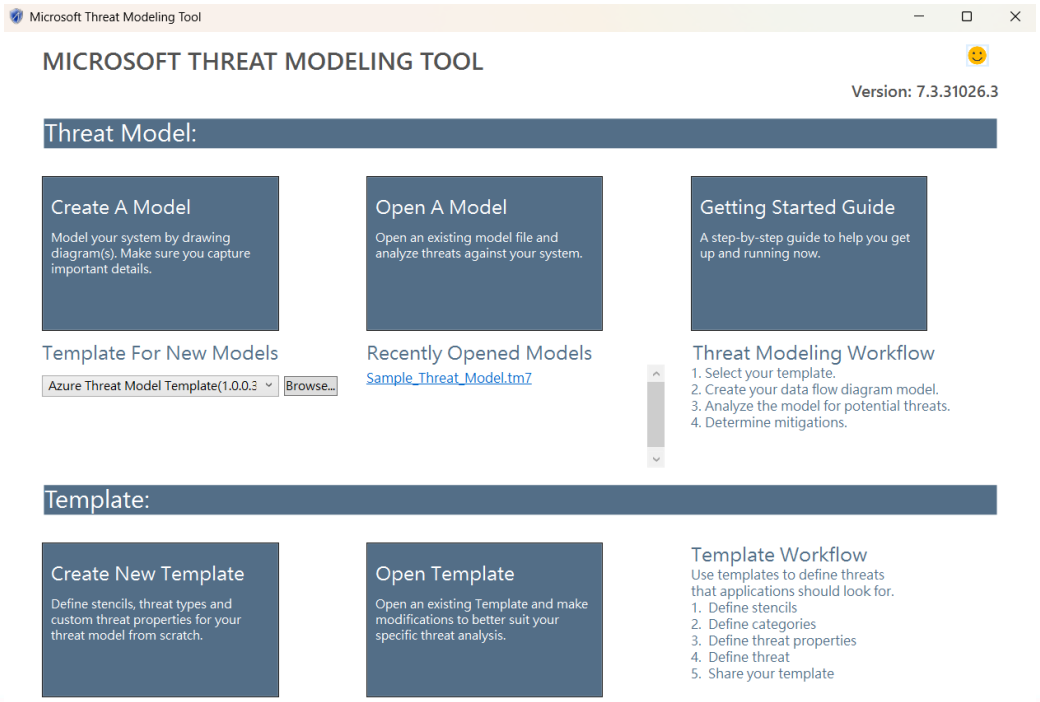
STRIDE

- STRIDE是由微軟提出的威脅分類模型，幫助開發人員系統性地識別潛在威脅。通常與資料流圖(DFD)結合使用，適合於系統設計階段進行

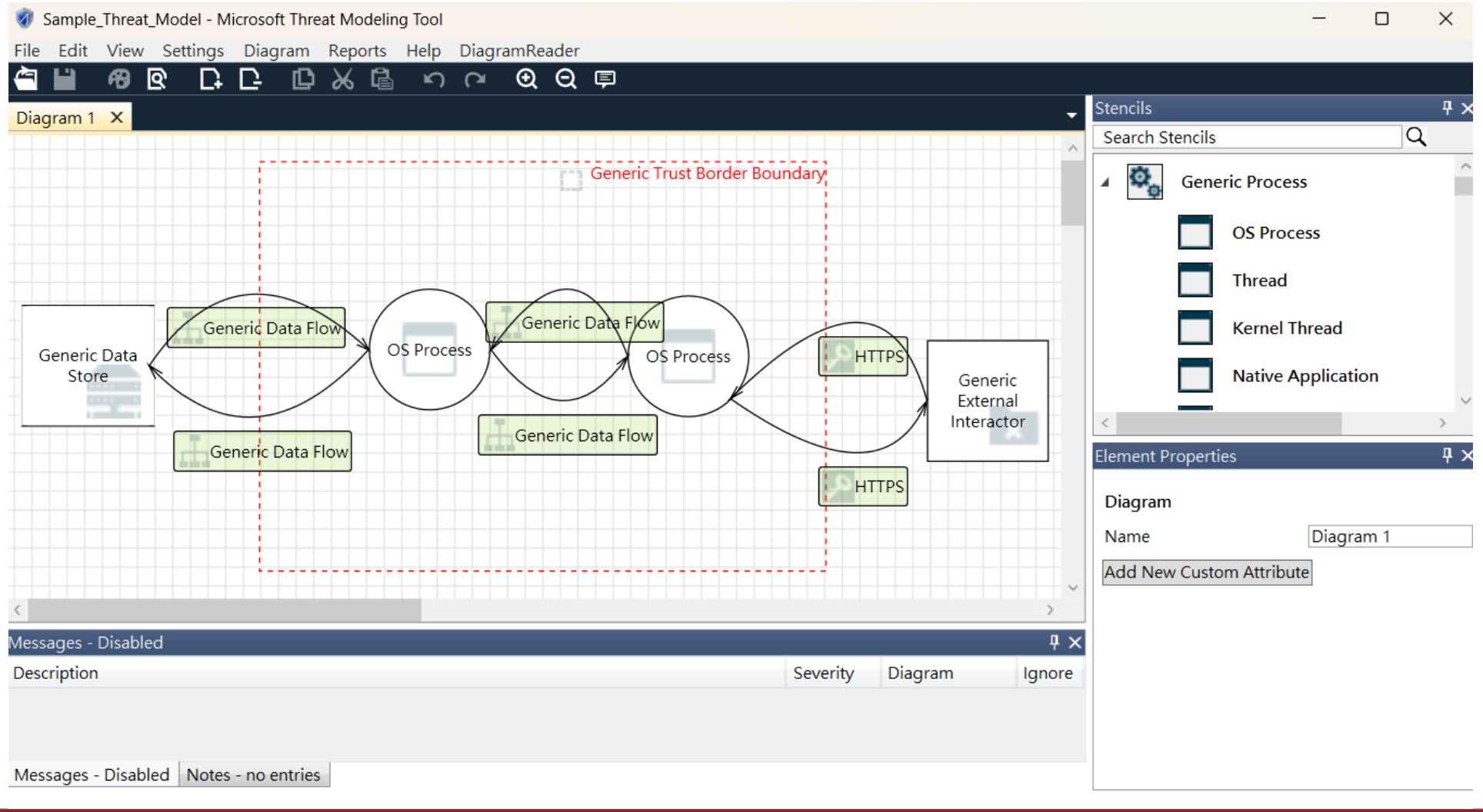
威脅類型	說明	安全風險
偽冒(**S**poofing)	攻擊者假冒他人或設備身分	真實性
竄改(**T**ampering)	未經授權地修改資料	完整性
否認(**R**epudiation)	使用者或系統拒絕承認其行為	不可否認性
資訊揭露(**I**nformation Disclosure)	敏感資訊被未授權存取或公開	機密性
阻斷服務(**D**enial of Service)	使系統無法運作或SLA降低	可用性
特權提升(**E**levation of Privilege)	利用系統漏洞提升權限	以上全部資安問題

Microsoft Threat Modeling Tool

- Microsoft開發的威脅建模工具，使用STRIDE與DFD建立視覺化的威脅模型
  - 官網：https://learn.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool
  - 下載安裝檔：https://aka.ms/threatmodelingtool



Microsoft Threat Modeling Tool



Sample

OWASP Threat Dragon

- OWASP開源的威脅建模工具，支援多種威脅模型與DFD，可用於建立視覺化的威脅模型
  - 官網：https://owasp.org/www-project-threat-dragon
  - 操作說明：https://www.threatdragon.com/docs
  - Demo website：https://www.threatdragon.com/#/
  - 下載安裝檔：https://github.com/OWASP/threat-dragon/releases

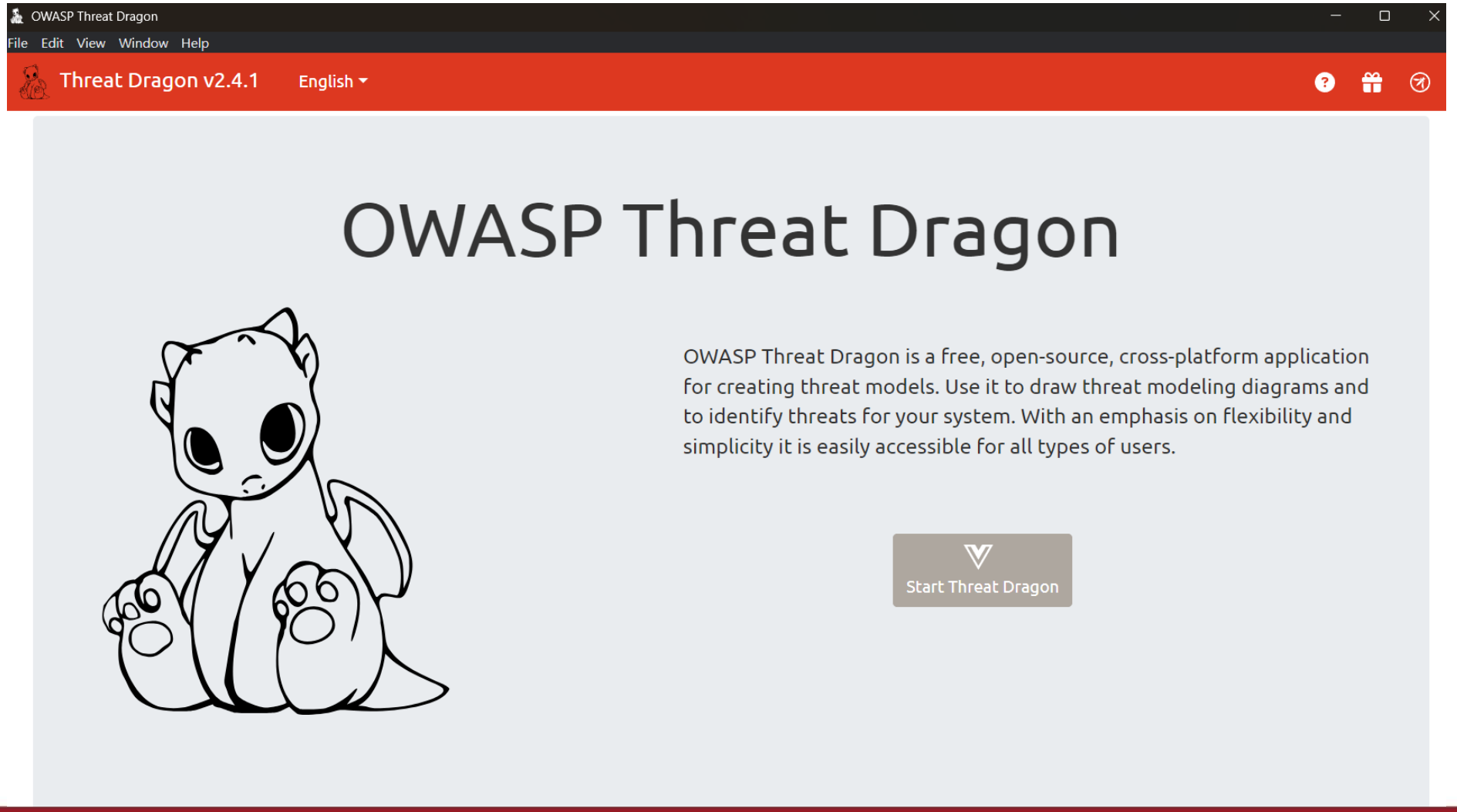
Example

下載安裝檔

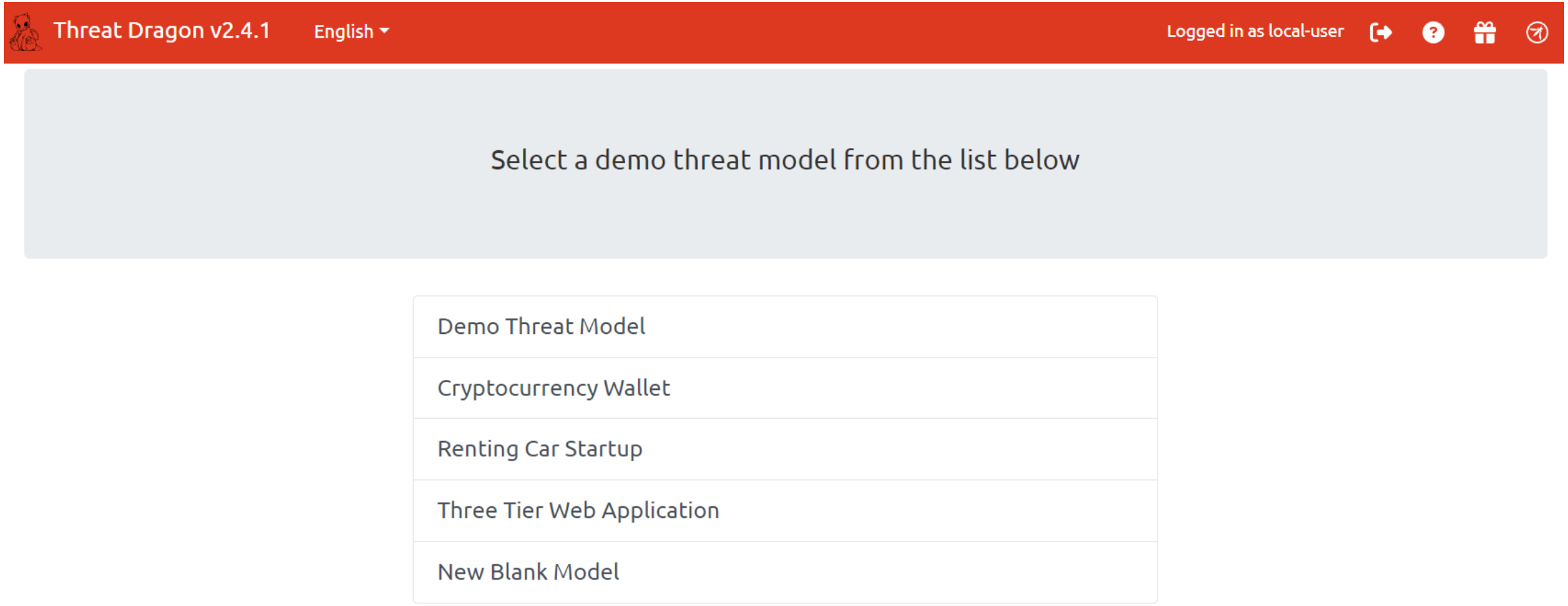
Desktop version

Platform	File	SHA512
Windows NSIS installer	Threat-Dragon-ng-Setup-2.4.1.exe	checksum.yml
MacOS installer x86	Threat-Dragon-ng-2.4.1.dmg	checksum-mac.yml
MacOS installer ARM64	Threat-Dragon-ng-2.4.1-arm64.dmg	checksum-mac-arm64.yml
Linux AppImage	Threat-Dragon-ng-2.4.1.AppImage	checksum-linux.yml
Debian package, AMD64	threat-dragon_2.4.1_amd64.deb	
Redhat package manager, X86 64 bit	threat-dragon-2.4.1.x86_64.rpm	
Linux Snap	direct from Snapcraft	

啟動畫面



多種參考範本



可建立多種威脅模型

Editing: Threat Model

Title

Threat Model

Owner

Ray Lin

Reviewer

RuRu

High level system description

Threat Model for Demo

Contributors

Yui × Start typing to add a contributor

Diagrams

STRIDE	New STRIDE diagram	New STRIDE diagram description	× Remove
CIA	New CIA diagram	New CIA diagram description	× Remove
Generic	New generic diagram	New generic diagram description	× Remove

+ Add a new diagram...

可建立多種威脅模型

Threat Model

Owner:
Ray Lin

Reviewer:
RuRu

Contributors:
Yui

High level system description

Threat Model for Demo

New STRIDE diagram

New CIA diagram

New generic diagram

Edit | Report | Close Model

可匯出報告

Show model diagrams | Show mitigated threats | Show out of scope elements | Show empty elements | Threat Dragon logo | Show element properties

PDF Report | Print | Close

Tue May 13 2025

Threat model report for Threat Model

Owner: Ray Lin

Reviewer: RuRu

Contributors: Yui

Executive Summary

High level system description

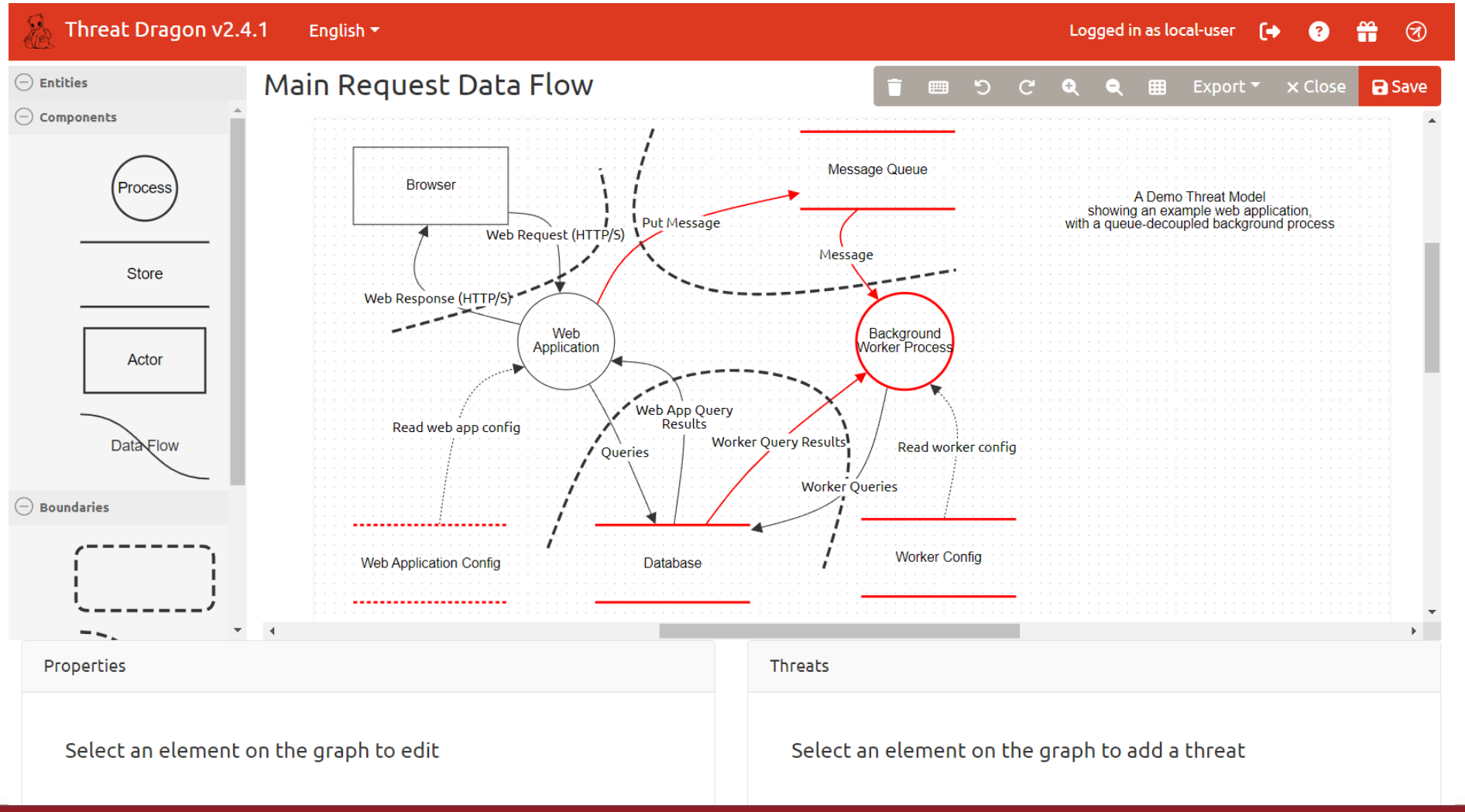
Threat Model for Demo

Summary

Name	Value
Total Threats	0
Total Mitigated	0
Not Mitigated	0
Open / Critical Priority	0
Open / High Priority	0

Sample

實際設計畫面

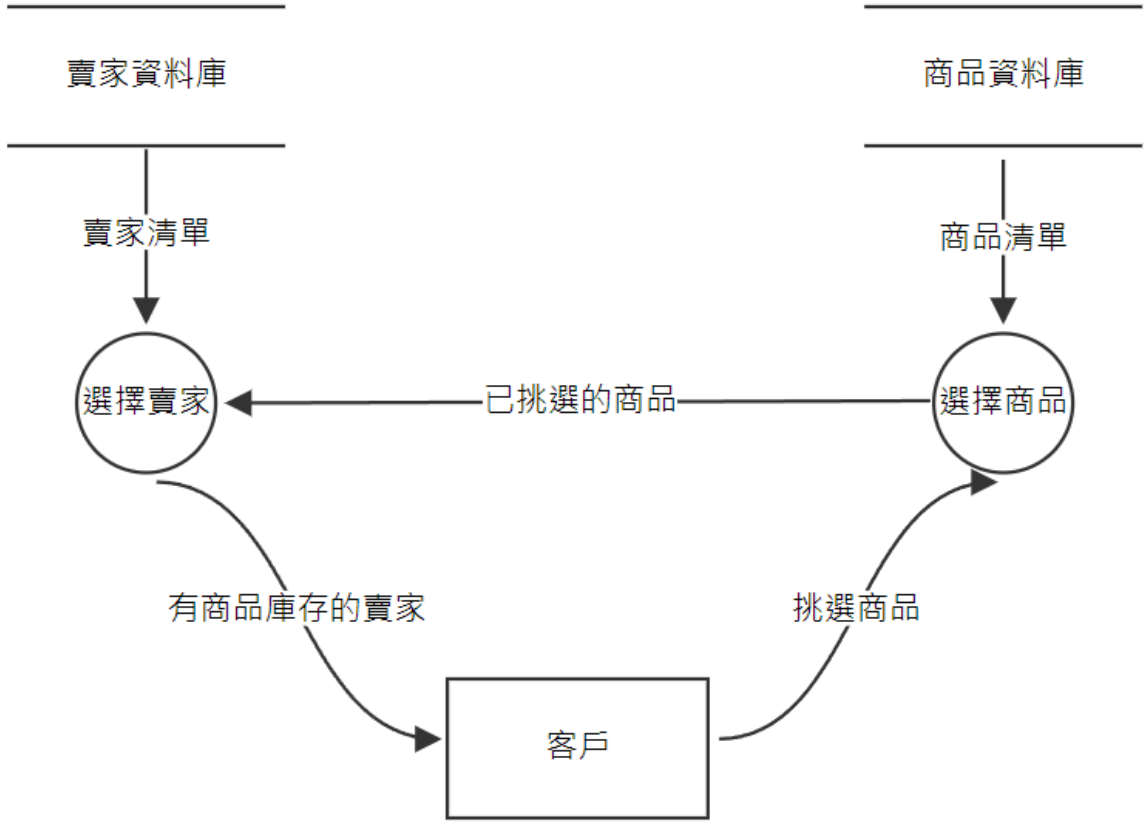


資料流圖(Data Flow Diagram)

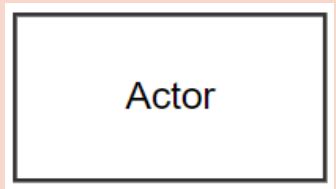
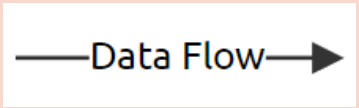
- 資料流程的規劃、各處理單元的動作、並且可以作更深一步的切分

- 資料流圖顯示系統的
  - 輸入
  - 輸出
  - 處理流程(Process)
  - 儲存(Store)

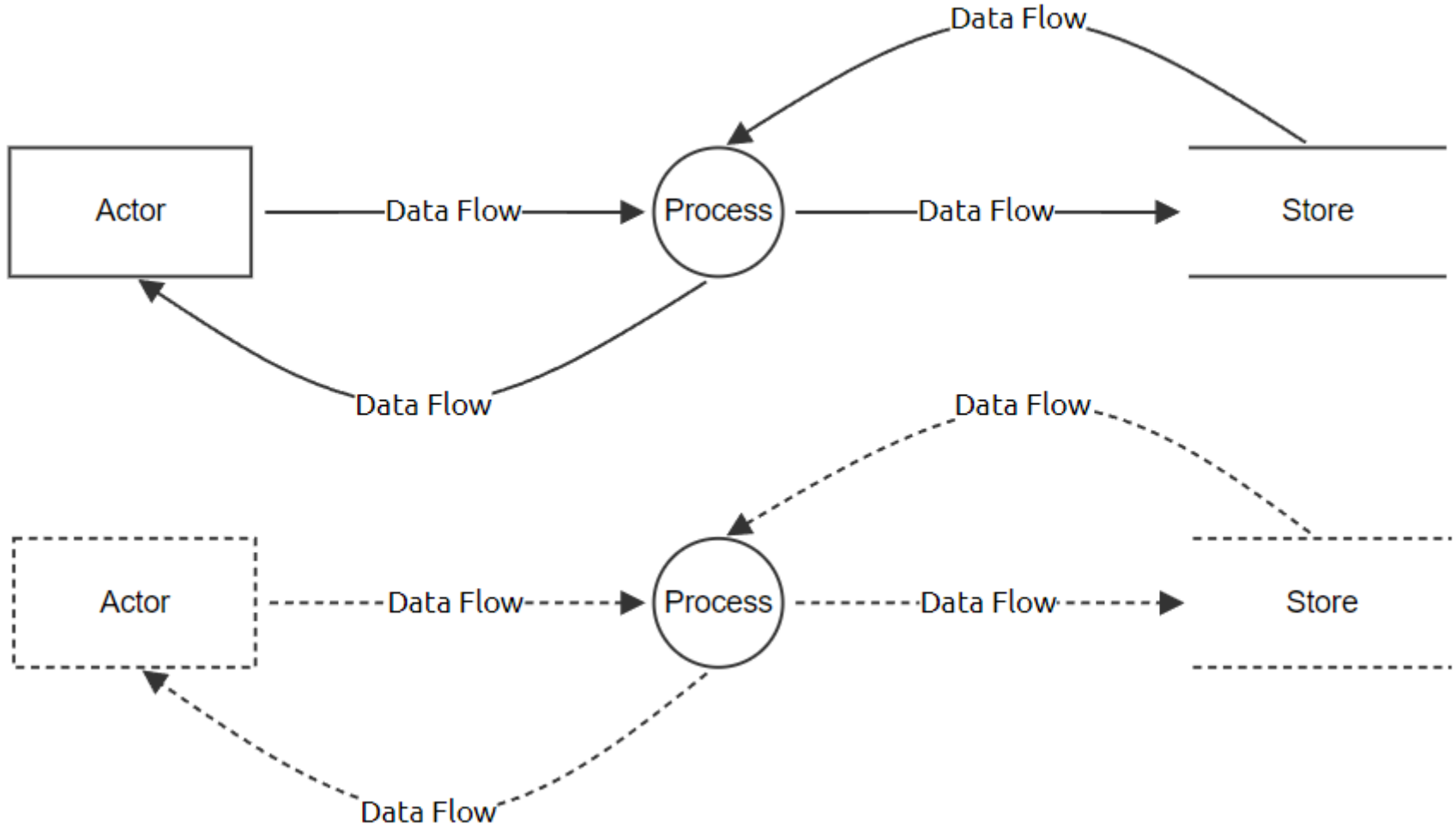
- 可應用在
  - 分析的最後階段
  - 設計的初期開發
  - 實作技術的假設



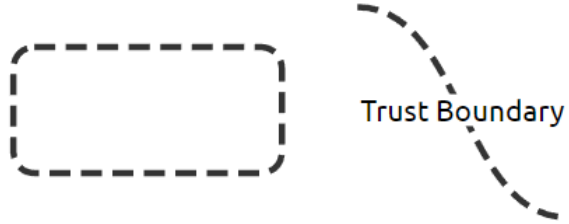
資料流圖(DFD)元素符號

名稱	元素符號	說明
行為者 / 外部實體 Actor / External Entity		跟應用程式互動的行為者或實體，通常在應用程式外部
處理流程 Process		在應用程式控制範圍內流程，執行輸入資料處理轉換成輸出資料的單元
資料流 Data Flow		用來表示處理所需要的輸出和輸入，箭頭代表元件間的資料流向
儲存 Store		資料庫、憑證或Log等儲存資料

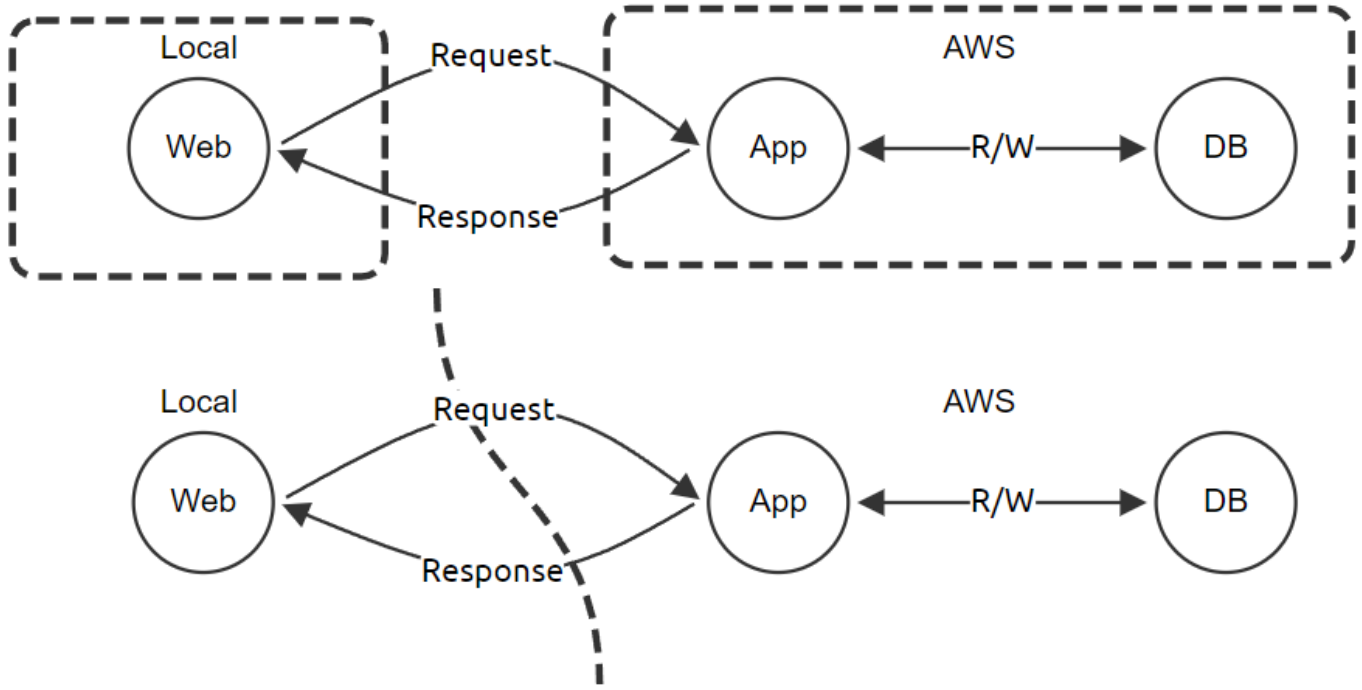
超出範疇(Out of Scope)



信任邊界(Trust Boundary)



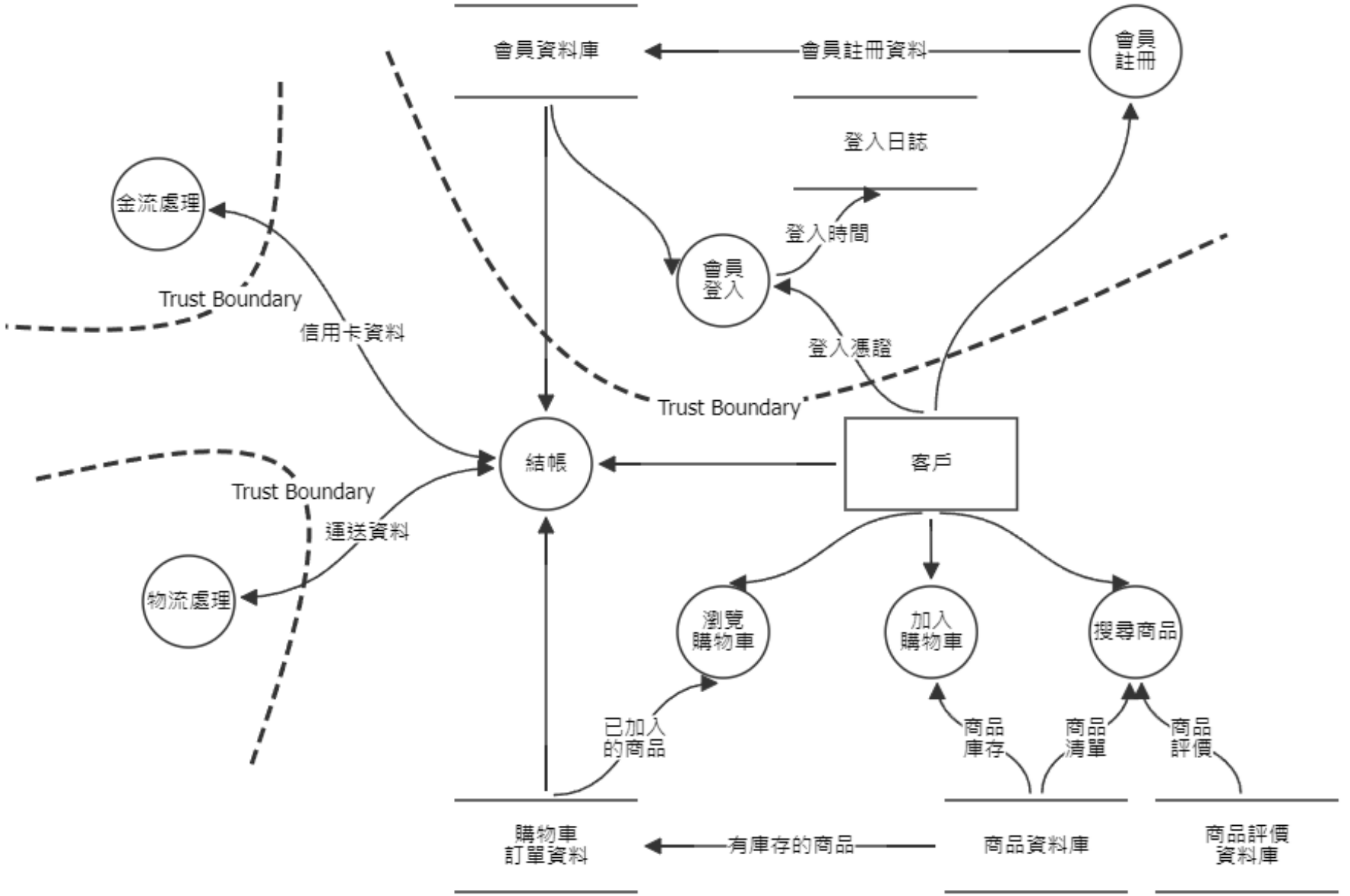
- 信任邊界通常具有以下特色
  - 信任邊界內的使用者或資源具有相同的存取權限或安全需求
  - 跨邊界需驗證，驗證後一定時間內不需重覆驗證



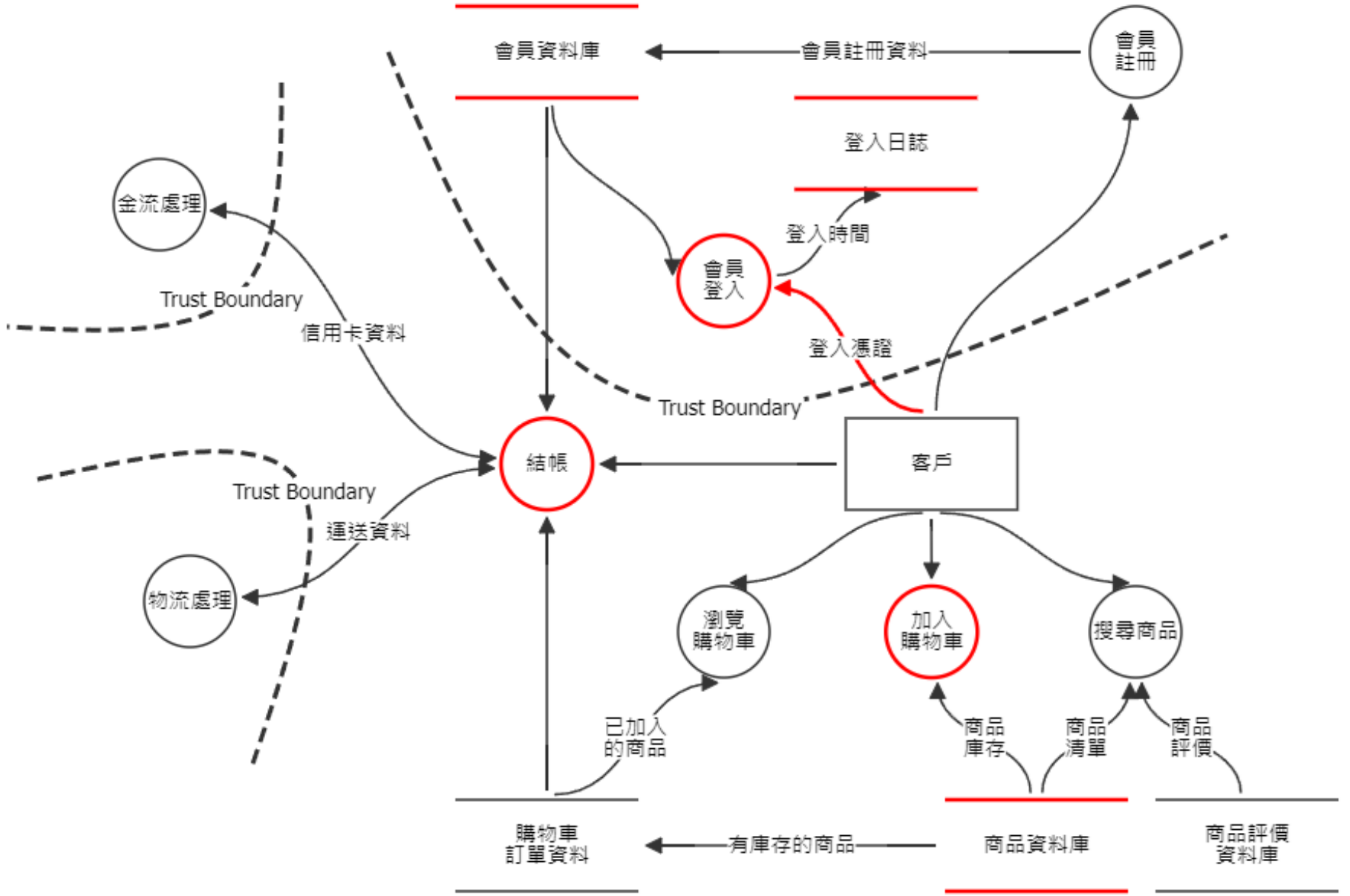
範例一 電商網站

- Ray是一位熱愛網購的上班族，平時忙碌的他，習慣在午休或下班時，透過電商網站快速瀏覽商品、比價、下單並選擇配送方式。網站提供多樣的商品資訊、購物車功能，以及便利的結帳付款流程。小明只要登入會員帳號，網站就會記錄他的購買紀錄、偏好商品和收件地址，讓購物更省時方便
- 功能模組
  - 會員註冊 / 登入，維護會員資料
  - 瀏覽商品、查看庫存與評價
  - 將商品加入購物車
  - 結帳時，串接金流處理（信用卡資訊）、物流處理（配送資訊）
  - 後台資料：包括訂單、庫存、評價等
  - 會員活動、登入日誌紀錄

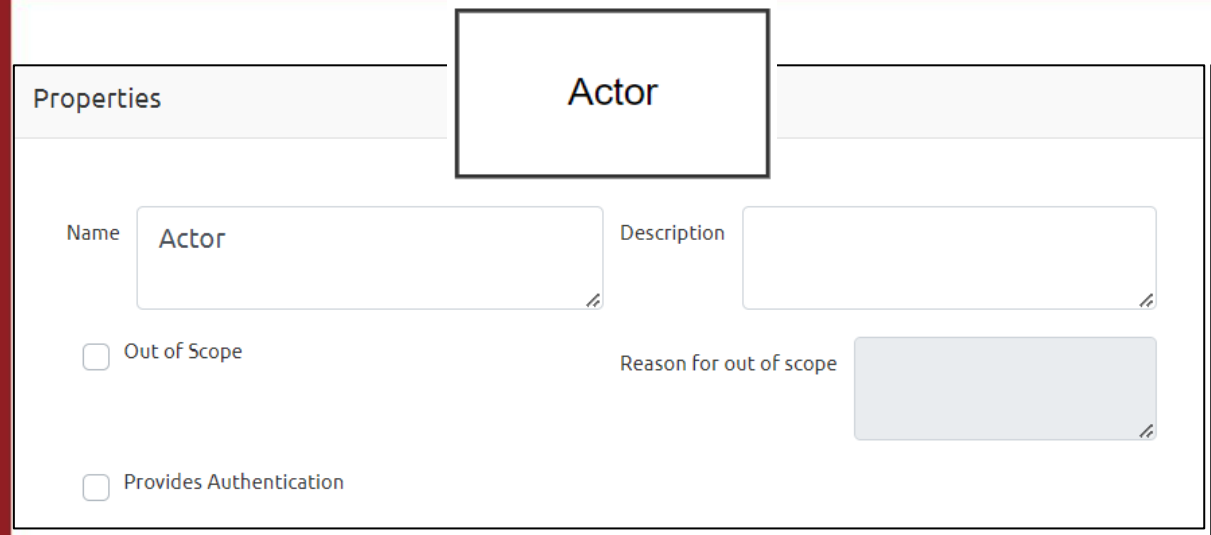
範例一 電商網站

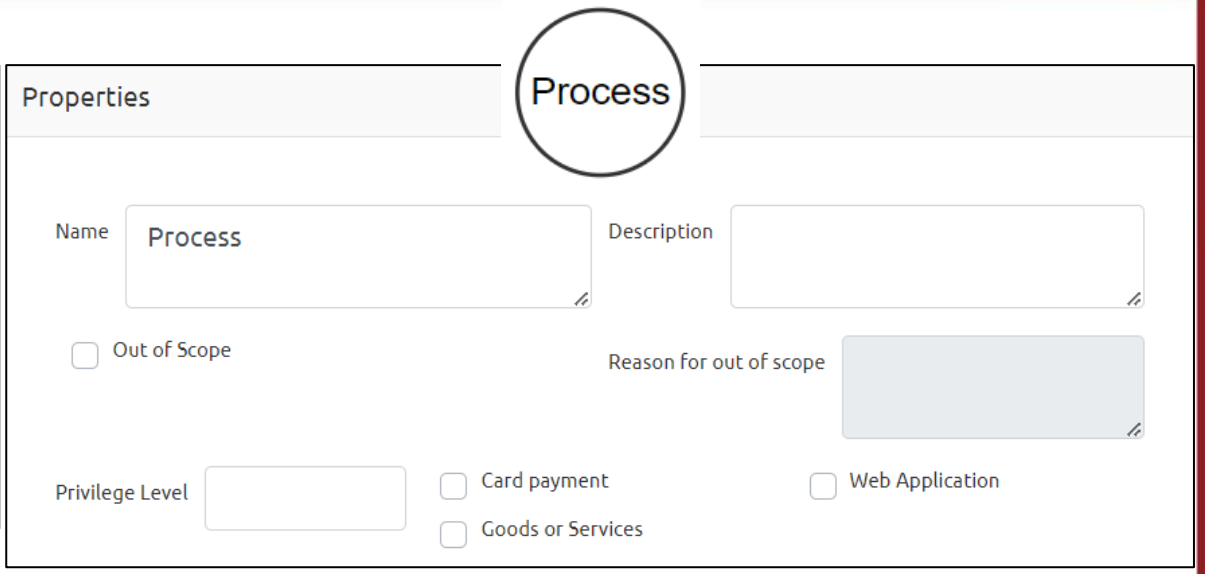


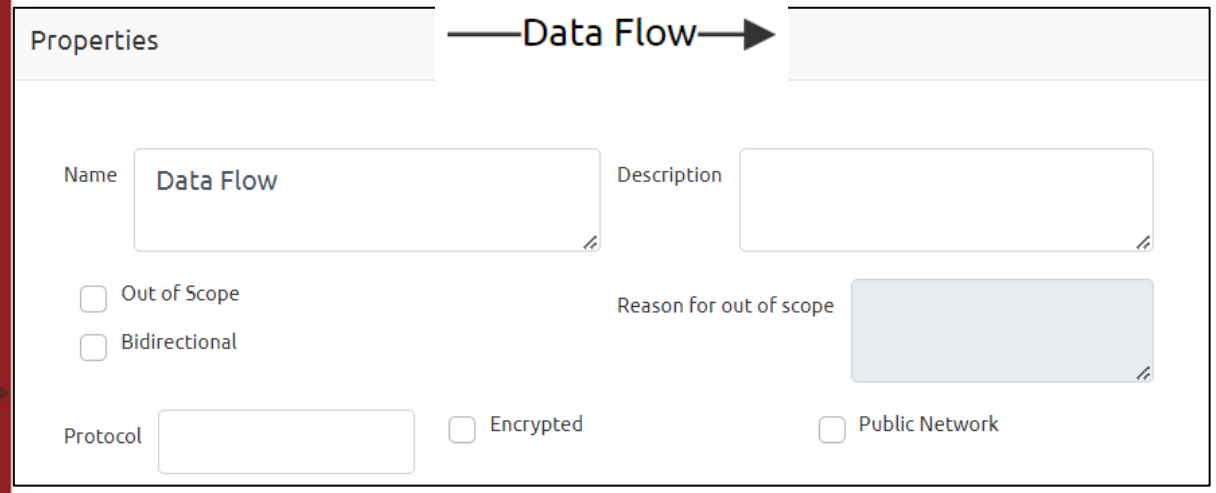
範例一 電商網站 - 加上威脅

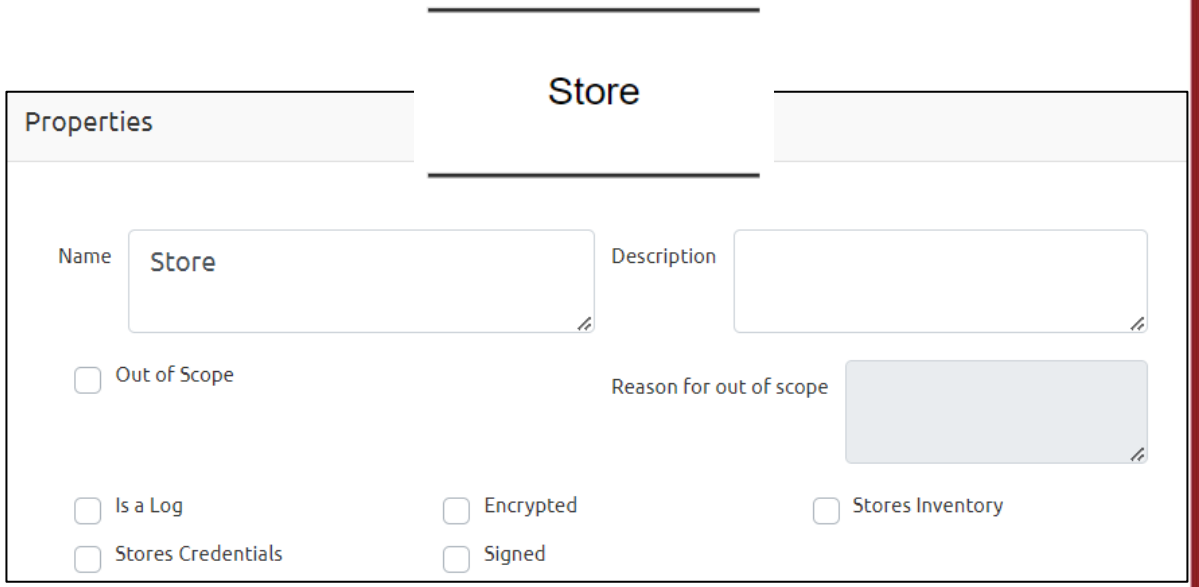


元素特性(Properties)



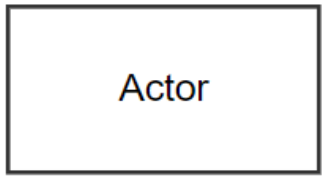




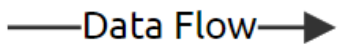


元素特性(Properties)

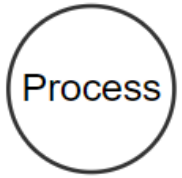
- 行為者(Actor)
  - 是否提供身分驗證(Provides Authentication)



- 資料流(Data flow)
  - 通訊協定(Protocol)
  - 是否加密(Encrypted)
  - 是否經過公有網路(Public Network)

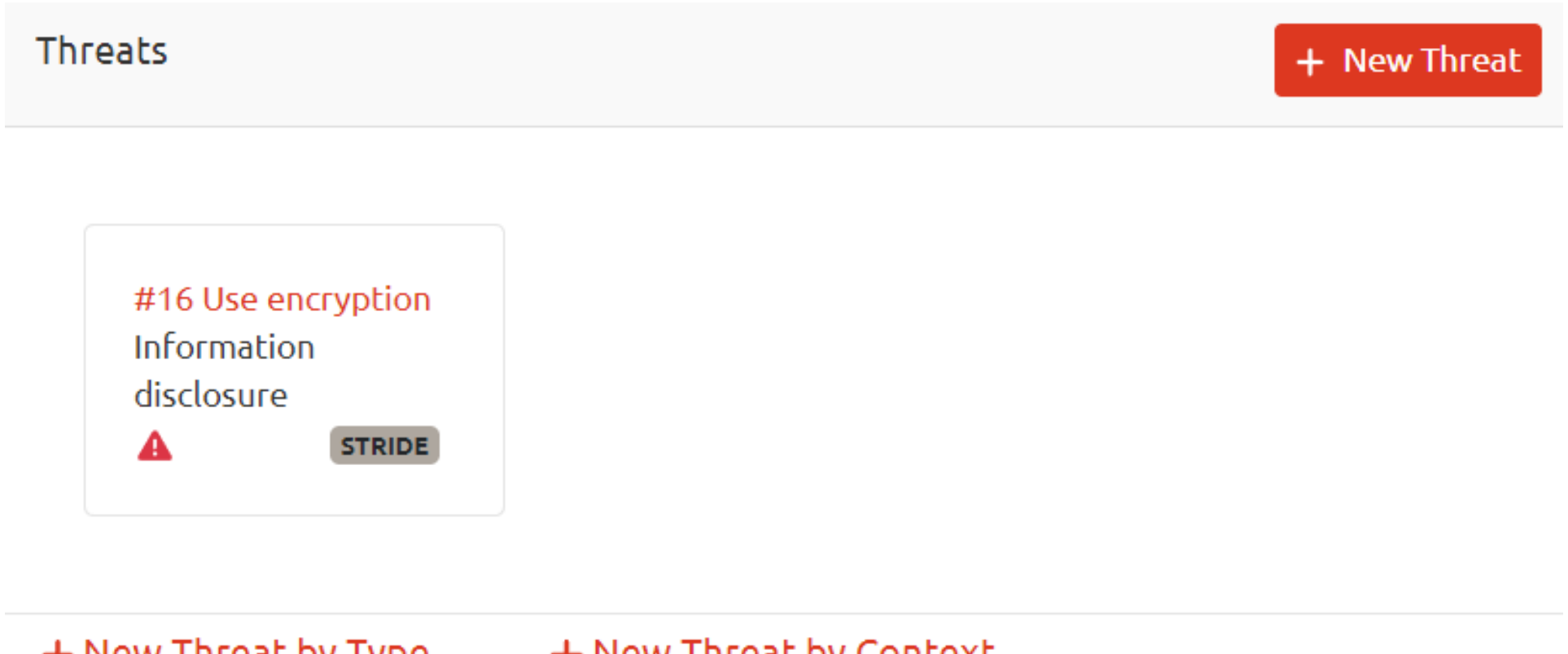


- 處理流程(Process)
  - 特權等級(Privilege Level)
  - 是否涉及信用卡付款(Card payment)
  - 是否提供商品或服務(Goods or Services)
  - 是否為網站應用程式(Web Application)



- 儲存(Store)
  - 是否為日誌(Is a Log)
  - 是否儲存憑證(Stores Credentials)
  - 是否加密(Encrypted)
  - 是否簽章(Signed)
  - 是否儲存庫存資訊(Stores Inventory)

威脅(Threats)

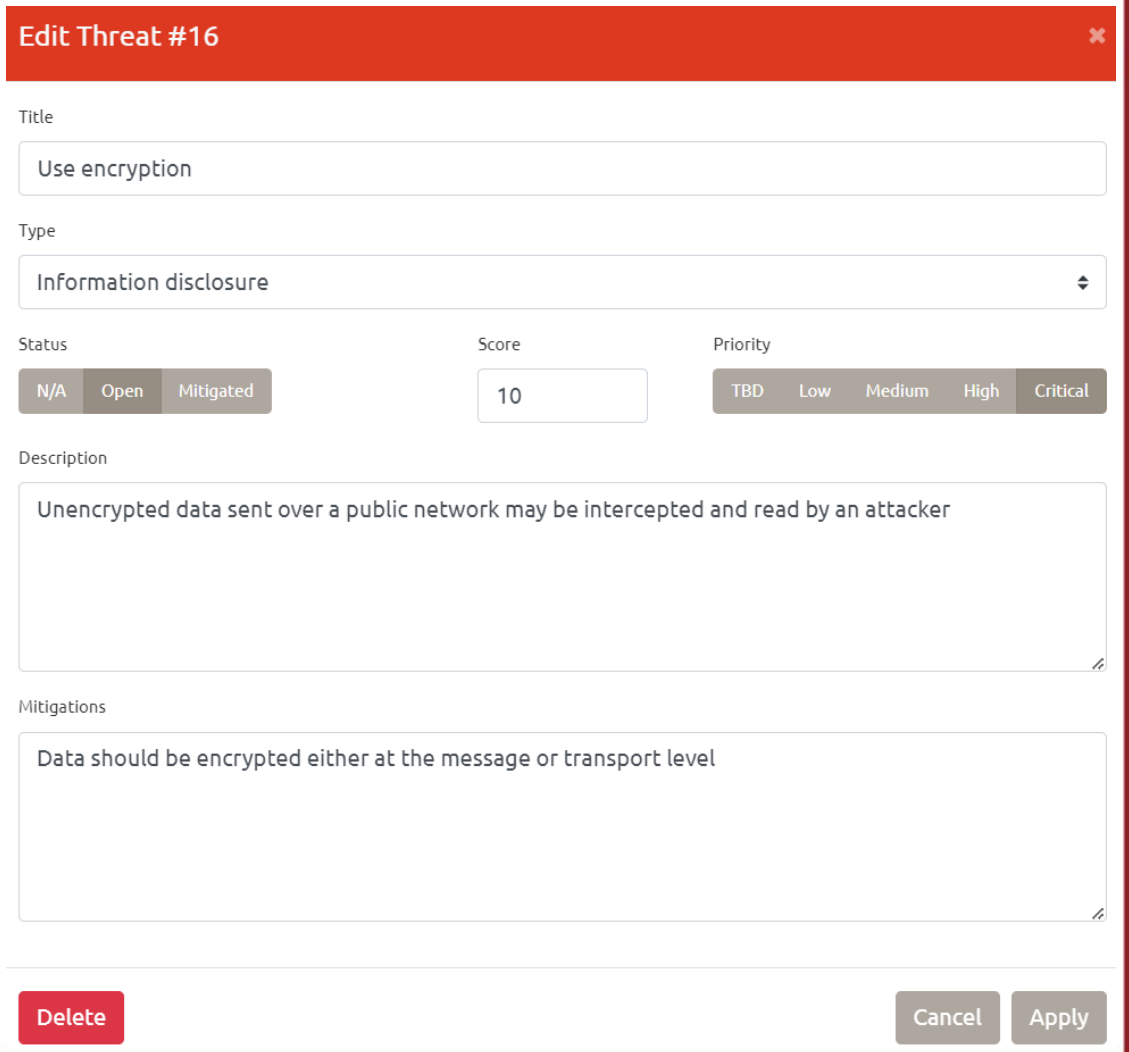


DFD元素對應STRIDE威脅

	偽冒 (Spoofing)	竄改資料 (Tampering)	否認 (Repudiation)	資訊揭露 (Information Disclosure)	阻斷服務 (Denial of Service)	特權提升 (Elevation of Privilege)
行為者(Actor)	V		V			
處理流程(Process)	V	V	V	V	V	V
資料流(Data flow)		V		V	V	
儲存(Store)		V	V	V	V	

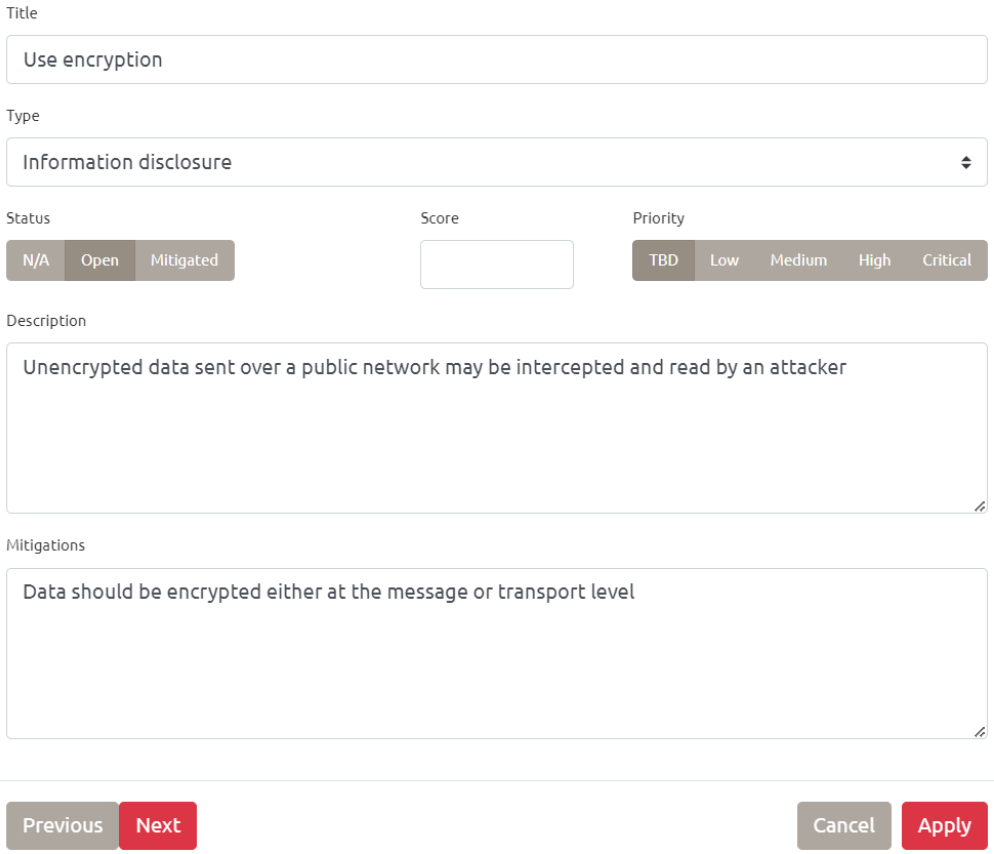
New Threat by Type

- 名稱(Title)
- 類型(Type)：例如STRIDE、CIA
- 狀態(Status)：開放或已緩解
- 分數(Score)：可自訂或用DREAD分數
- 優先度(Priority)：依照嚴重性排序處理
- 說明(Description)
- 緩解(Mitigations)：ATMA風險處置



New Threat by Context

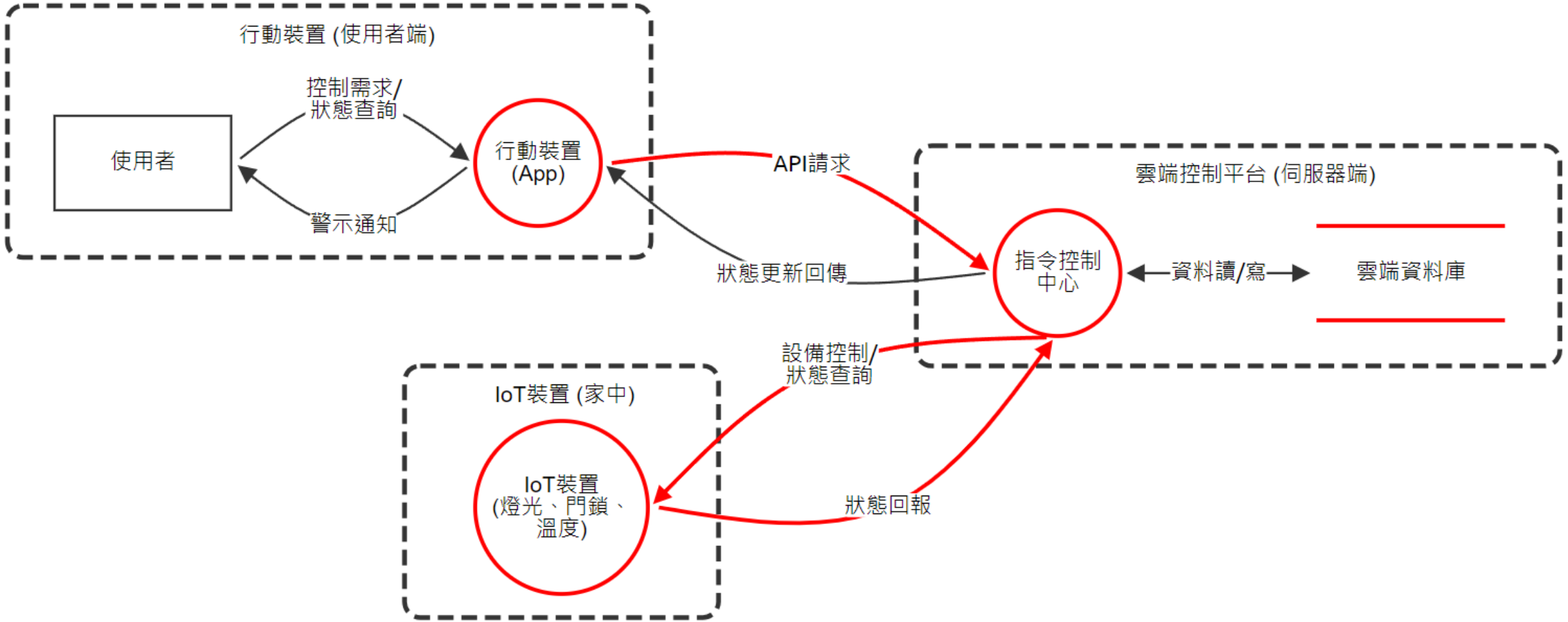
- 威脅情境主要來自OWASP Automated Threats to Web Applications



範例二 智慧家居遠端管理

- Ray平時早出晚歸家中沒人，他在上下班途中想確認家中門鎖是否已鎖好，或在回家前開啟冷氣與燈光。他使用一款App（iOS / Android）來查看家中裝置狀態與遠端操作。App需要與雲端控制平台進行互動，平台再將命令送至家中IoT裝置
- 功能模組
  - 使用者透過手機App連接雲端平台
  - 雲端平台與IoT裝置互動（開關燈、調整溫度等）
  - IoT裝置（家中燈光、門鎖、溫度控制）

範例二 智慧家居遠端管理

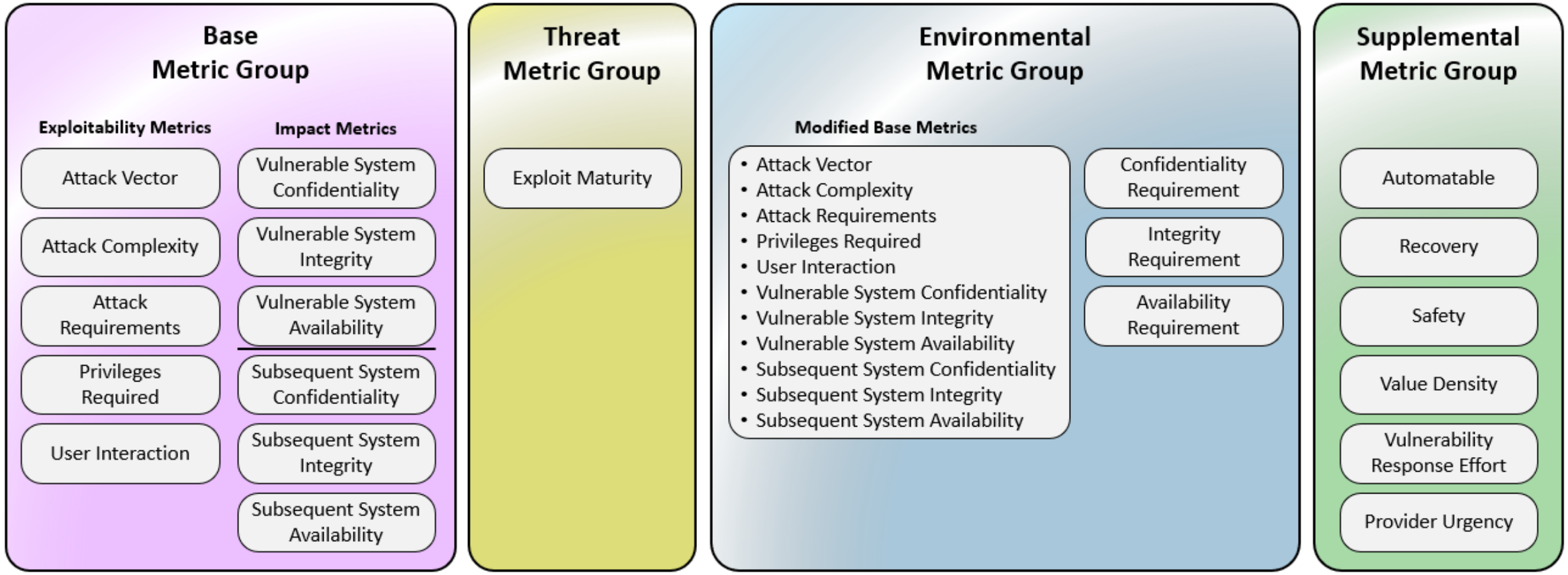


威脅建模分數訂定

通用漏洞評分系統(CVSS)

- 通用漏洞評分系統(CVSS, Common Vulnerability Scoring System)是一套全球廣泛使用的資訊安全漏洞嚴重性評估標準，它提供一致且可量化的方式，協助組織評估處理漏洞的優先順序
- CVSS主要目的是衡量資訊系統中漏洞的嚴重程度，並以0 ~ 10的分數表示
  - 0.0：無風險
  - 0.1 ~ 3.9：低(Low)
  - 4.0 ~ 6.9：中(Medium)
  - 7.0 ~ 8.9：高(High)
  - 9.0 ~ 10.0：嚴重(Critical)
- CVSS計算機：https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator

通用漏洞評分系統(CVSS)



Source: https://www.first.org/cvss/v4-0/specification-document

DREAD

DREAD	說明
損害(Damage)	評估一個安全漏洞被利用後可能對系統或資料造成的損害程度
可再現性(Reproducibility)	評估攻擊者是否能夠輕易且一致地重現攻擊
可利用性(Exploitability)	評估利用該漏洞的難易度，需多少技術能力或條件以成功利用漏洞
受影響使用者(Affected Users)	評估一旦漏洞被利用，有多少使用者會受到影響
可發現性(Discoverability)	評估發現該漏洞的難易度，需多少知識和工具才能識別出此缺陷

STRIDE + DREAD

威脅類型	安全風險	說明	損害 (Damage)	可再現性 (Reproducibility)	可利用性 (Exploitability)	受影響使用者 (Affected Users)	可發現性 (Discoverability)	風險分數	緩解措施
偽冒 (Spoofing)	真實性	攻擊者假冒他人或設備身分	8	7	6	9	8	38 (高)	
竄改資料 (Tampering)	完整性	未經授權地修改資料	9	6	7	8	7	37 (高)	
否認 (Repudiation)	不可否認性	使用者或系統拒絕承認其行為	7	5	5	7	6	30 (中)	
資訊揭露 (Information Disclosure)	機密性	敏感資訊被未授權存取或公開	8	6	6	9	8	37 (高)	
阻斷服務 (Denial of Service)	可用性	使系統無法運作或SLA降低	9	7	8	9	7	40 (高)	
特權提升 (Elevation of Privilege)	以上全部資安問題	利用系統漏洞提升權限	9	5	7	8	7	36 (高)	

DREAD風險分數排序建議

- 直接使用
  - 0：無風險
  - 1 ~ 19：低(Low)
  - 20 ~ 34：中(Medium)
  - 35 ~ 44：高(High)
  - 44 ~ 50：嚴重(Critical)
- 取平均(參考CVSS v4.0)
  - 0.0：無風險
  - 0.1 ~ 3.9：低(Low)
  - 4.0 ~ 6.9：中(Medium)
  - 7.0 ~ 8.9：高(High)
  - 9.0 ~ 10.0：嚴重(Critical)

DevSecOps Taiwan

林家瑋|大Ray@DevSecOps社長

DevSecOps Taiwan (2000+)

https://bit.ly/AG3_DevSecOps

- 每個月免費線上分享
  - 每月固定一場 👉 1~2小時分享
  - 不定期快閃 👉 0.5~1小時分享
- 社群分享主題與交流方向
  1. Agile / Waterfall / Hybrid
  2. DevSecOps (DevOps + Security)
  3. AI + Security
  4. Cybersecurity
  5. Cloud Security (AWS / Azure / GCP)
  6. 從零開始的跨雲生活系列

歡迎加我好友

Email: ray.lin@ifus.tw