

Cymetrics

敏捷及彈性化的資安評估SaaS



Cymetrics



- 關於 OneDegree/Cymetrics
- Cymetrics 資安評估服務介紹

關於 OneDegree



Cymetrics

OneDegree Hong Kong – 透過全數位化保險平臺提供保戶流暢的保險產品體驗

OneDegree Global (SG) – 提供 B2B 企業服務，包括 **保險核心系統 (IXT)** 和 資安 **SaaS (Cymetrics)**。

數位化保險產品
香港純網路保險牌照



OneDegree Hong Kong



資安 SaaS



保險核心系統



OneDegree Global (SG)

獎項與認可



2019 Fintech 100
H2 Ventures & KPMG



ICT StartUp Bronze Award
The Hong Kong ICT Awards 2019
Software & App



ISO/IEC 27001:2013 Certified



Hong Kong Rising Star
2019 Deloitte Hong Kong Technology
Fast Program



Platinum Award of InsurTech
IFTA Fintech Achievement Award 2018

OneDegree 完成B1輪融資，邁向亞洲保險科技領導者 (2021.8.30)

OneDegree 完成2800萬美元 B1 輪融資



2021年8月30日週一 上午11:42 · 2 分鐘文章



<匯港通訊> 保險科技公司之一 OneDegree 今天宣佈完成
伐成為亞洲新世代保險科技領導者。

完成此輪融資後,集團累計獲得逾7000萬美元融資,反映於
新資金將用於投資新技術、產品開發及 B2C 和 B2B 的業

該集團計劃在未來12個月繼續增聘人手,支援亞洲業務發展
同時,集團也在持續加強亞太區和歐洲的戰略夥伴關係,目
洲的全球保險科技公司。



經濟 15:03 2021年08月30日 [縮短網址](#)

0 1 1

香港唯一一家線上寵物保險公司OneDegree30日發佈消息稱,在最新一輪融資中籌
得2800萬美元。公司聯合創始人表示,此次成功融資表明,投資者對香港的數字保
險初創企業仍有信心。

Ref : <https://hk.sports.yahoo.com/news/onedegree-%E5%AE%8C%E6%88%902800%E8%90%AC%E7%BE%8E%E5%85%83-b1-%E8%BC%AA%E8%9E%8D%E8%B3%87-034225488.html>

OneDegree 集團具備金融、研發、資安人才，其中 B2B 保險核心系統 IXT 已被港台的客戶所採用，如：康健人壽、第一保，期望能協助亞洲金融產業進行科技賦能。

OneDegree Global攜手康健人壽 打造保險數位生態圈

12:23 2021/01/27 | 工商 | 陳碧芬



全新推出 醫療+還本

- ✓ 住院一天最高5,000元
- ✓ 重大傷害失能200萬元
- ✓ 滿期還本 保障多更多

全新推出 醫療+還本

- ✓ 住院一天最高5,000元
- ✓ 重大傷害失能200萬元
- ✓ 滿期還本 保障多更多

財經熱門新聞

CIO Taiwan

活動 影音 趨勢分析 CIO IT經理人雜誌 CSO精選 電子報 下載 聯繫我們

首頁 > 供應品視野

OneDegree雙軌併進 搶攻金融、資安商機

2021-05-05 分類: 供應品視野 閱讀時間: 3 mins read



OneDegree 共同創辦人梁德源(左)、資安負責人呂亦儒(右)



Cigna Taiwan selects IXT to empower digital and ecosystem growth

"We've chosen OneDegree Global as they have a deep understanding of the modern-day consumer's needs. Cigna Taiwan has knowledge of the local insurance market, while OneDegree Global contributes to the partnership its innovative solutions and experiences in other Asian markets."



Tim Shields

GM and CEO of
Cigna Taiwan



First Insurance Chooses IXT to accelerate digital transformation

"We selected OneDegree Global to be our partner in this digital transformation journey not only because of their proven core insurance solutions, but also because of their team's experience and dedication in helping clients unlock their potential."



Edward Lee

VP of First
Insurance



OneDegree Hong Kong selects IXT as end-to-end core platform to empower digital business

"We have deployed IXT core insurance technology since business launch. Its open and scalable cloud platform supports us to provide breakthrough innovations in products and services, and we have achieved 50x monthly sales growth."



Alvin Kwok

GM of OneDegree
Hong Kong

2021 資安大會，Cymetrics 首次於台灣市場亮相

首次被邀請於2021 資安大會分享及展會曝光Cymetrics品牌

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 臺灣資安大會 搜尋

新聞

【臺灣資安大會直擊】因應重大網攻發生頻率增加，專家建議資安風險評估每一周至少要做一次

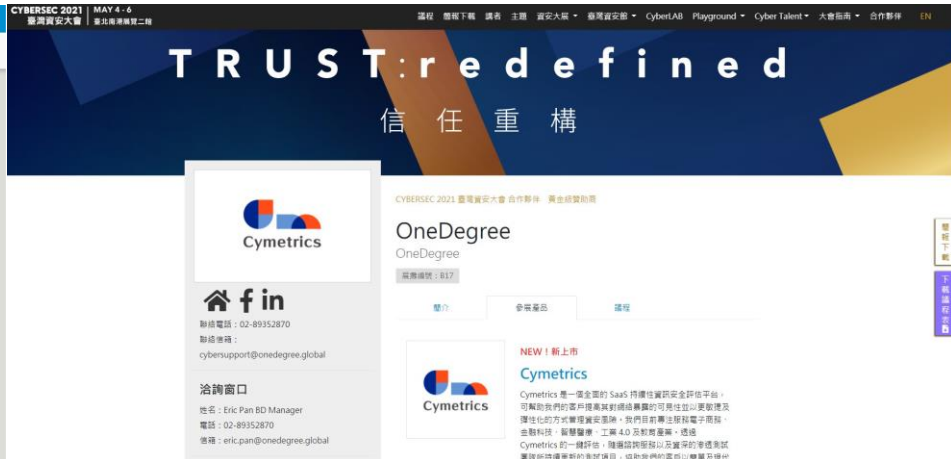
OneDegree資安負責人的周彥儒在資安大會上，分享當前最流行的駭客網路攻擊模式，並且建議企業以較低成本的SaaS安全檢測服務，頻繁地進行風險和弱點評估

文/ 李建興 | 2021-05-05 發表

讚 65 篇 按讚加入iThome粉絲團 讚 337 分享



為因應越來越頻繁的重大攻擊事件，曾任花旗銀行資安官，現在是OneDegree資安負責人的周彥儒，在資安大會的演講中建議企業，應該要全面進行風險評估、弱



金融行業等級資安團隊

資安團隊協助 OneDegree HK 的寵物險平台從產品設計流程開始導入資安架構，並通過香港保監局資安稽核，並取得純網路保險牌照。

- Cymetrics團隊成員來自於 台大資安相關實驗室、資策會資安所、台灣知名電信資安顧問團隊
- 具備多張資安證照 CEH, CISSP, CCSP
- 國際CTF(駭客攻防搶旗賽) 全球 84名



Stanley Chou

- 現任：OneDegree 資安長/Cymetrics產品負責人
- 經歷：
 - 花旗銀行資安官
 - 勤業眾信資深顧問

Cymetrics 資安評估方案介紹

長期且持續的審視資安防禦策略



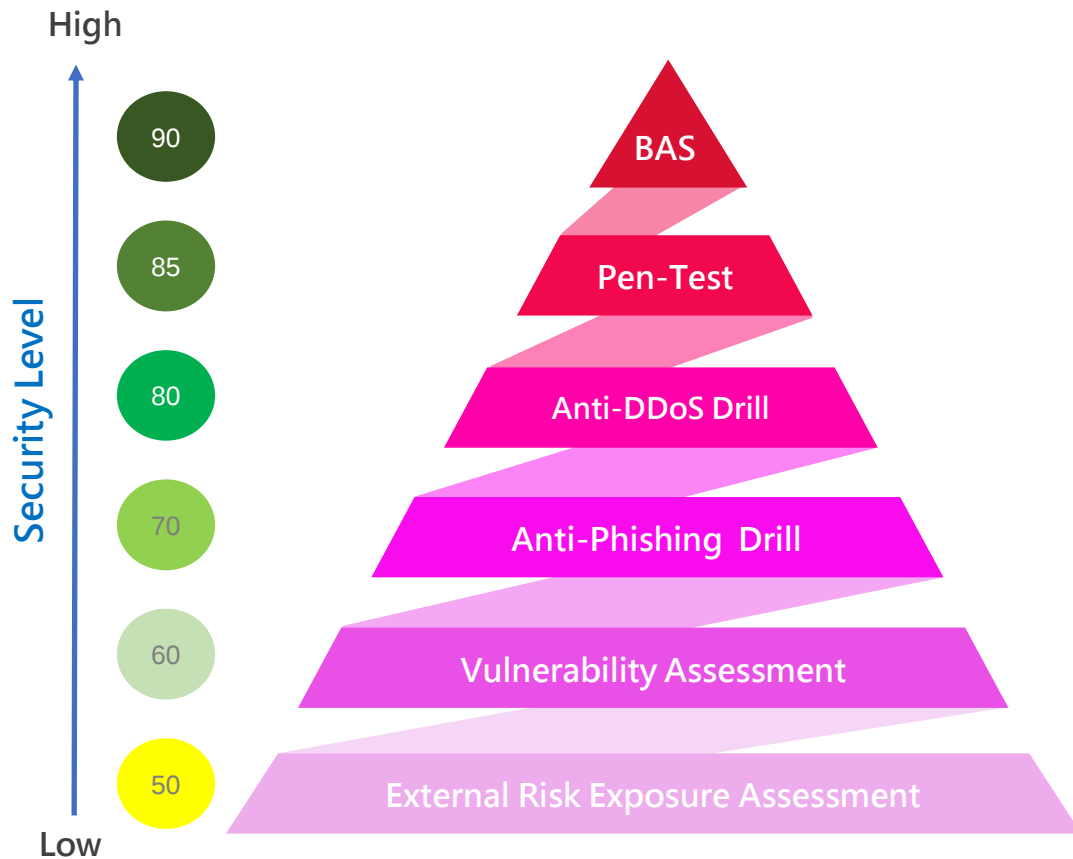
Cymetrics

Cyber Defense Matrix (CDM矩陣)

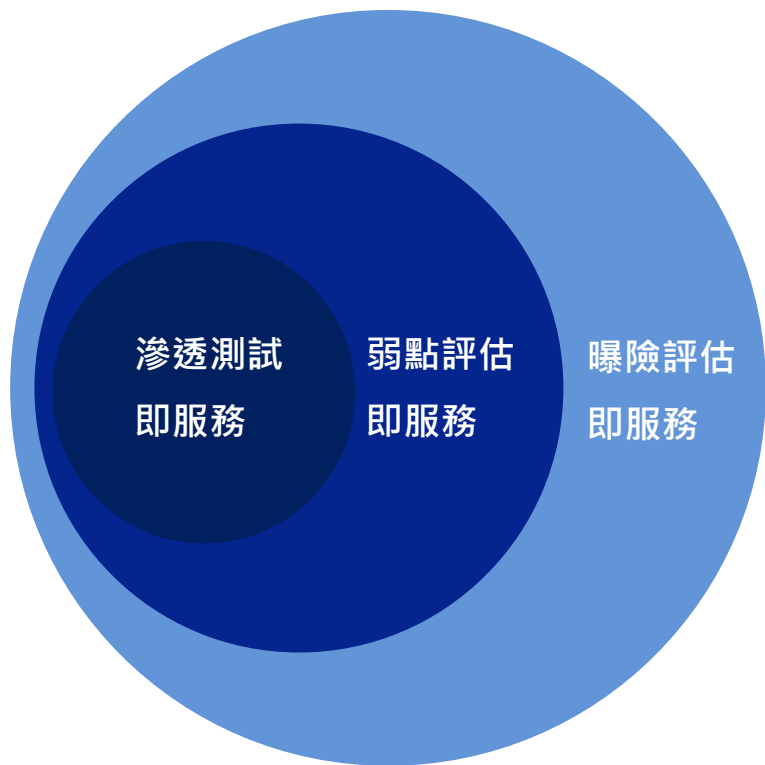


	Identify 識別	Protect 保護	Detect 偵測	Respond 應變	Recover 復原
Endpoint 終端設備		Antivirus	IPS/IDS		
Application 應用程式	VA	WAF	Security Health Check	EDR/MDR	SOAR
Network 網路	PT/BAS	DAM		SIEM/SOC	Digital Forensic
Data 數據	Phishing		Anti-DDoS	Training	
User 使用者					

Enhance cyber security awareness by Red Team services



由外而內、由廣而深，持續性資安量化及合規評級



Level 1 : 曝險評估即服務

透過蒐集及分析資安情報，客戶可先從了解自己及供應鏈的資安曝險開始進行資安管理。

Level 2 : 弱點評估即服務

持續性的評估，早於駭客一步做好漏洞管理，降低 OWASP TOP 10、CWE 及 CVE 中的風險

Level 3 : 滲透測試即服務

線上預約資安工程師進行滲透測試，找出“未知”漏洞來測試資安縱深防禦的有效性。



Level 1：曝險評估即服務(EAS) – 非侵入式資安曝險評估報告

- 非侵入性，不影響日常營運
- 被動式蒐整及分析資安情資與網路足跡
- 進一步瞭解合作夥伴、供應商資安曝險及評級

MITRE
ATT&CK™

CVE™



Cyber Score Cymetrics 透過安全情資服務提供即時曝險圖 (EAS)，輔助評估曝險圖 (SAS)，並評估組織脆弱性 (PTM)，全面性的揭露組織客戶在資安曝險層面上的曝險程度。我們的服務會持續蒐集其法進行資安評估，協助客戶提供外企業資安安全情資及風險的可視性，更進一步協助客戶以最佳的方式管理其資安曝險提升資安程度。

C+

客戶 Client
offices355
受測日期 Date
2021 / May / 3

資安評級
Cymetrics 資安評級由最高至最低為 A、B、C、D、E、F、G 七個等級，評級圖中不同之等級及顏色代表不同之資安曝險程度。資安評級可協助企業資安曝險程度之風險管理，進行內部安全提升及工作參考。

A- 網路服務
External Service

● 遠端控制 Remote Control ● 資料庫 Database ● 應用服務 Remote Service ● 黑名单 Blacklist
• 建議參考曝險監控報告細部後，依據評級提升建議優先進行曝險改善。

B+ 網站
Web Application

● 網頁伺服器 Web Server ● 網頁應用 Web Application ● 憑證 Certificate ● 網域 Domain
• 建議參考曝險監控報告細部後，依據評級提升建議優先進行曝險改善。

A- 電子郵件
Email

● 郵件服務 Email Service ● DMARC Domain Authentication ● SPF Sender Policy Framework
• 建議參考曝險監控報告細部後，依據評級提升建議優先進行曝險改善。

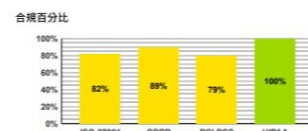
D 帳號密碼
Credential

● 網路串流 Credential Leakage
• 建議參考曝險監控報告細部後，依據評級提升建議優先進行曝險改善。

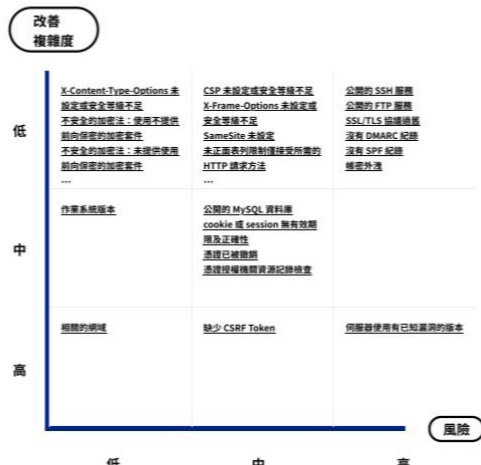
Cymetrics 資安評級之計算，係將曝險程度之曝險圖及風險圖與客戶在曝險圖 (網域活動紀錄與客戶之程度) 綜合考量後，逐項曝險圖及風險圖之曝險圖及客戶在曝險圖中曝險圖時不同會有變化，因此曝險圖之曝險圖與客戶在曝險圖之評級會不同。

Compliance

合規分數



Cymetrics 合規分數之計算，係將客戶曝險圖之曝險圖及風險圖與客戶在曝險圖 (網域活動紀錄與客戶之程度) 綜合考量後，逐項曝險圖及風險圖之曝險圖與客戶在曝險圖中曝險圖時不同會有變化，因此曝險圖之曝險圖與客戶在曝險圖之評級會不同。



本資安評級提升象限圖，依據風險及改善複雜度兩個維度提供客戶作為資安評級提升優先順序之參考，可從右上（風險高且改善複雜度低）的項目開始，逐步往左下（風險低且改善複雜度高）的項目改善或進行風險轉移。公司亦可依自身風險預算，針對左下象限之項目選擇風險接受。

Cymetrics



Level 1 : 曝險評估即服務(EAS) – 檢測項目



客戶 Client
OD 有限公司

受測日期 Date
2021 / Jul / 21

本報告測試之子網域

www.example.com

資安評級

系統性歸納由 MITRE 提出的 ATT&CK 資安框架及 NIAC 美國國家基礎建設諮詢委員會公開的 CVSS 通用漏洞評分系統，並根據實時風險情資調整評級權重，將各面向風險區間由高至低分為 A、B、C、D、F，5大級別

A B C D F

A

網路服務

External Service



遠端控制

Remote Control



資料庫

Database



應用服務

Remote Service



黑名單

Blacklist

B

網站

Web Application



網頁伺服器

Web Server



網頁應用

Web Application



憑證

Certificate



網域

Domain

B

電子郵件

Email



郵件服務

Email Service



DMARC

Domain Authentication



SPF

Sender Policy Framework

A+

帳號密碼

Credential



網路曝險

Credential Leakage

Level 1 : 曝險評估即服務(EAS) – 檢測項目 Cont'd (1/2)

網路服務 (External Service)

- 遠端控制：檢測遠端控制 (SSH, RDP, VNC) 的 port 有沒有開啟
- 資料庫：檢測資料庫服務 (MySQL, MSSQL...) 的 port 有沒有開啟
- 應用服務：常見服務像是 SMB, FTP 的 port 有沒有開，以及作業系統版本
- 黑名單：查看 IP 是否被列為黑名單

網站 (Web Application)

- 網頁伺服器：查看伺服器版本是否洩漏、CSP、X-Frame-Options 這些 header 有沒有設定
- 網頁應用：檢查 HTTP/HTTPS 是否混用以及是否缺少 CSRF token
- 憑證：檢查憑證版本以及使用的演算法是否有問題
- 網域：是否有相似的網域或是子網域劫持的問題

Level 1：曝險評估即服務(EAS) – 檢測項目 Cont'd (2/2)

電子郵件 (Email)

- 郵件服務：檢查是否有公開的 IMAP, POP3, SMTP 服務
- DMARC：透過 DNS record 檢查 DMARC 是否設置，幫助讓發信端和收信端雙方可確認對方身分，可用於防止詐騙和網路釣魚
- SPF：透過 DNS record 檢查 SPF 是否設置，幫助收信方確認寄信方宣稱之來源是否為合法位置，可與 DKIM 及 DMARC 共同用於防止詐騙和網路釣魚

帳號密碼 (Credential)

- 網路曝險：透過 HIBP 查詢是否有帳密外洩，以及在公開的地方 (GitHub, S3, Azure blob...) 是否找得到外洩的檔案

Level 2：弱點評估即服務(VAS) – 弱點掃描SaaS

- 隨時可啟動檢測，彈性高
- 檢測紀錄可隨時存取閱讀(包含PDF及Excel)
- 自動產出檢測報表，並附帶漏洞改善建議



Level 2 : 弱點評估即服務(VAS) – 弱點掃描SaaS

- 攻擊模式更新快速 (平均每月更新)
- 平均 3-6 小時內產出弱點檢測報告
- 支援中、英文雙語報告



資訊安全健診摘要說明

靶站 (下稱 "公司") 委任 ONEDEGREE GLOBAL (SG) PTE. LTD. (下稱 "OneDegree") 執行資訊安全健診 (含弱點掃描暨滲透測試)。本委任之目的為辨識公司資訊安全曝險並量化資安評級。OneDegree 特此聲明本次資安健診已完成, 並彙整資訊安全健診結果如下。

日期: 2021/03/04

範圍:

網域	高風險	中風險	低風險
https://www.offices355.com/☹	4	9	9

問題彙總:

風險等級	問題
高風險	Remote OS Command Injection
高風險	缺少 CSRF Token
高風險	跨域腳本攻擊
高風險	路徑遍尋
中風險	XSLT Injection
中風險	不安全的 HTTP 方法: Trace
中風險	標頭配置錯誤: CSP 任意加載
中風險	標頭配置錯誤: 缺少 CSP
中風險	標頭配置錯誤: 缺少 X-Frame-Options
中風險	目錄瀏覽
中風險	相對路徑混淆
中風險	逆向 Tabnabbing
中風險	錯誤信息揭露
低風險	偵錯信息揭露

Level 3 : 滲透測試即服務(PTS) – 測試方法論

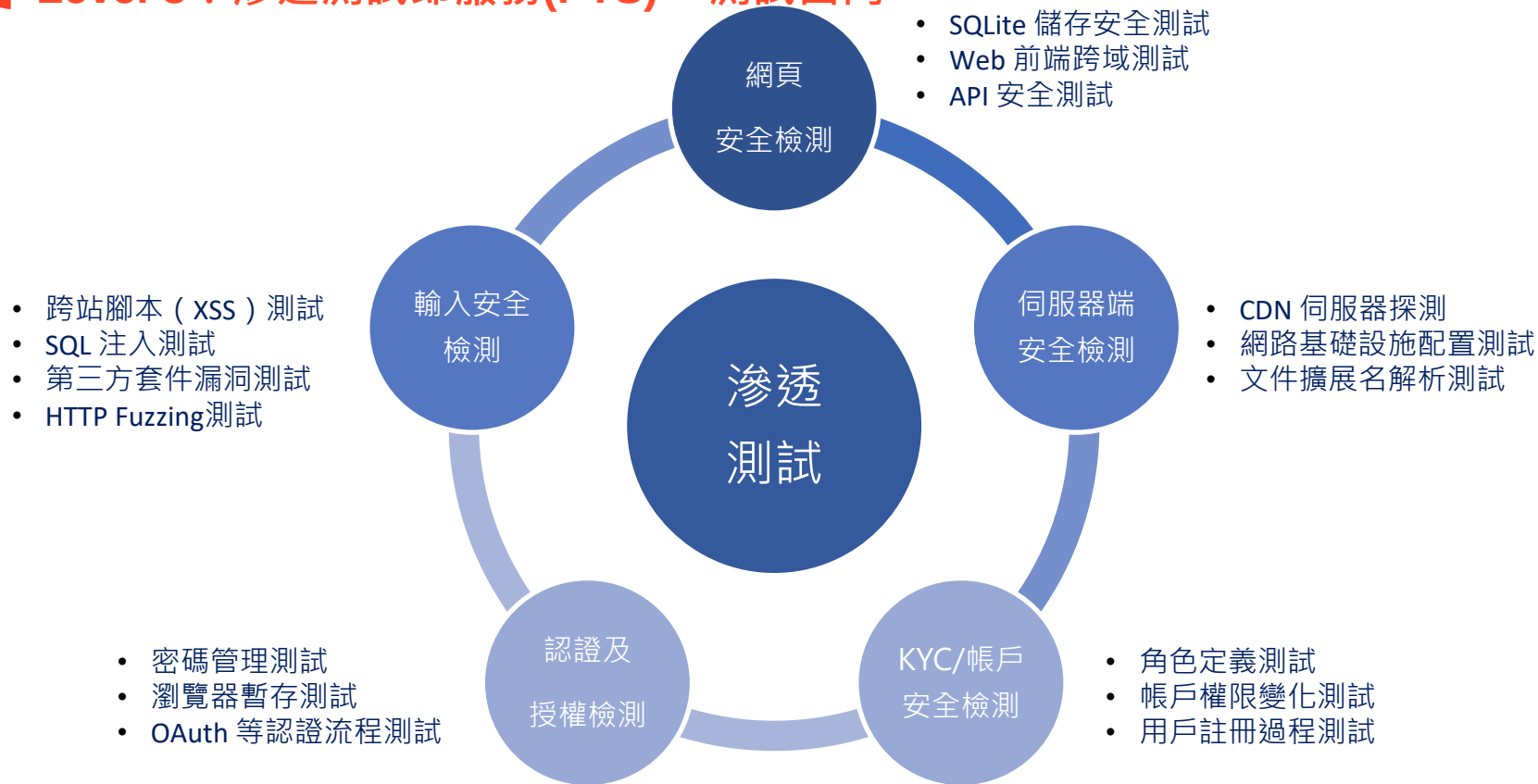
- OSSTMM by ISECOM The Open Source Security Testing Methodology Manual
- OSSTMM 以資安圖 (Security Map) 描述資安測試環境
- 六群測試模組互相重疊

- The Information System Security Assessment Framework (ISSAF) By Open Information System Security Group



- OWASP (Open Web Application Security Project)
- OWASP Testing Guide
- OWASP Top 10 網站應用程式攻擊
- Regional Intelligence
- 國家資通技術服務中心滲透測試規範
- 行政院國家資通安全會報
- Reginal CERT (Community Emergency Response Team)

Level 3 : 滲透測試即服務(PTS) – 測試面向



Level 3：滲透測試即服務(PTS) – 目的與效益

Purpose

- 找出系統架構或程式設計上 (Design) 的安全弱點
- 驗證潛在性 (Potential) 的安全弱點，包括組態、權限、密碼等之設定與管理問題
- 尋找服務被中斷 (DoS) 的可能，並預先調整防禦策略
- 透過第三方執行攻擊與顧問判斷風險可能造成的危害範圍
- 演練攻擊發生時，可能造成的損害以及應變措施是否有效

Benefit

- 釐清漏洞對企業的影響程度，也能使企業依據風險影響程度及改善複雜度判定出風險優先修復等級，使業者在攻擊來臨前預演並高效的移除風險。
- 檢視現行資安服務與產品是否能有效應變

會員 個資保護

- 國際知名血糖機品牌
- 線上教育平台

專案/客戶 規格要求

- 雲端HR平台
- 金融業第三方服務供應商(TSP)
- 全台最大速食業者

法規合規 需求

- 企業網路貸款平台
- 網路保險服務

聯繫我們

Joyce Hsiao

joyce.hsiao@cymetrics.io



Cymetrics