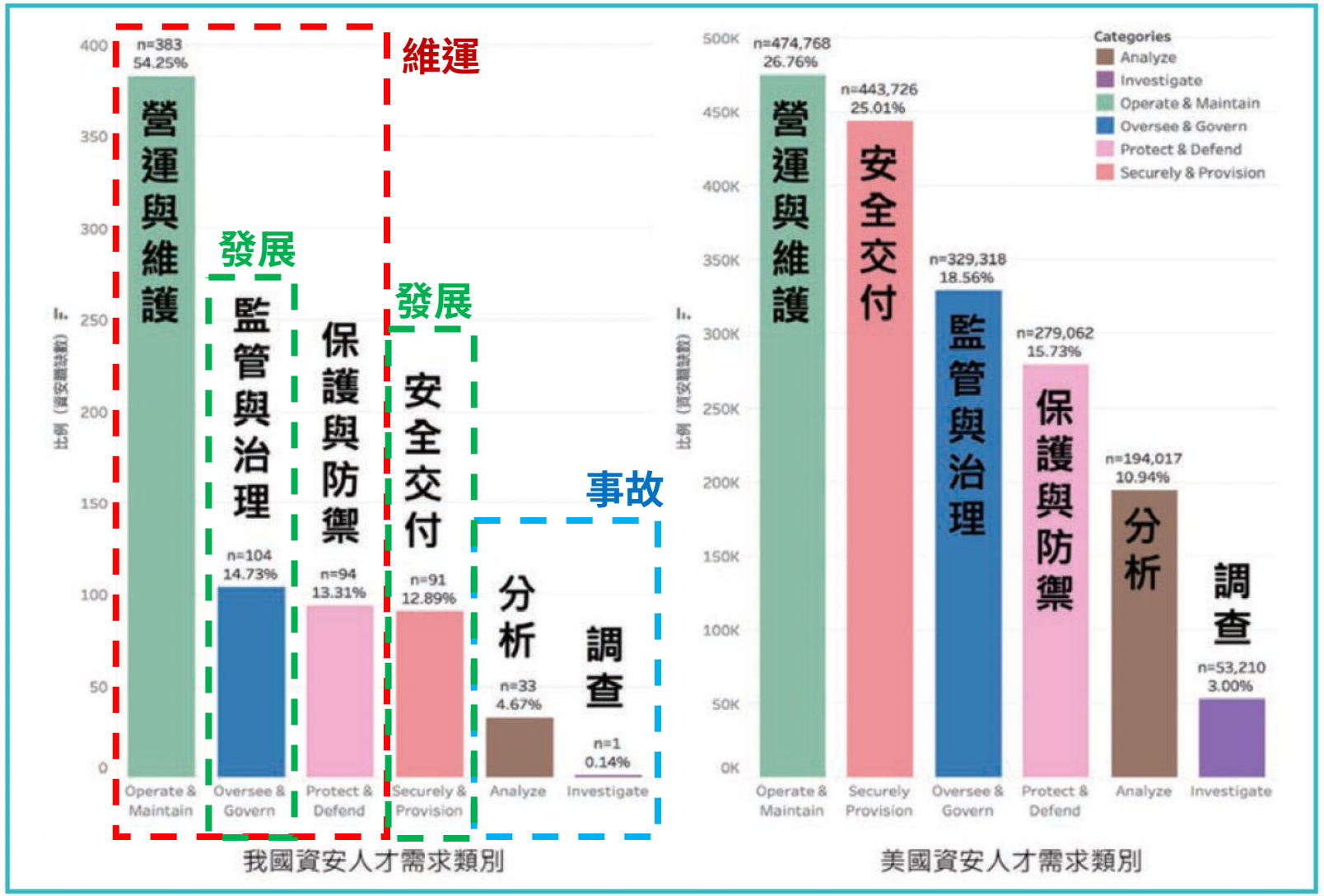
打造資安人才的試鍊場

蔡一郎

SHIELD EXTREME

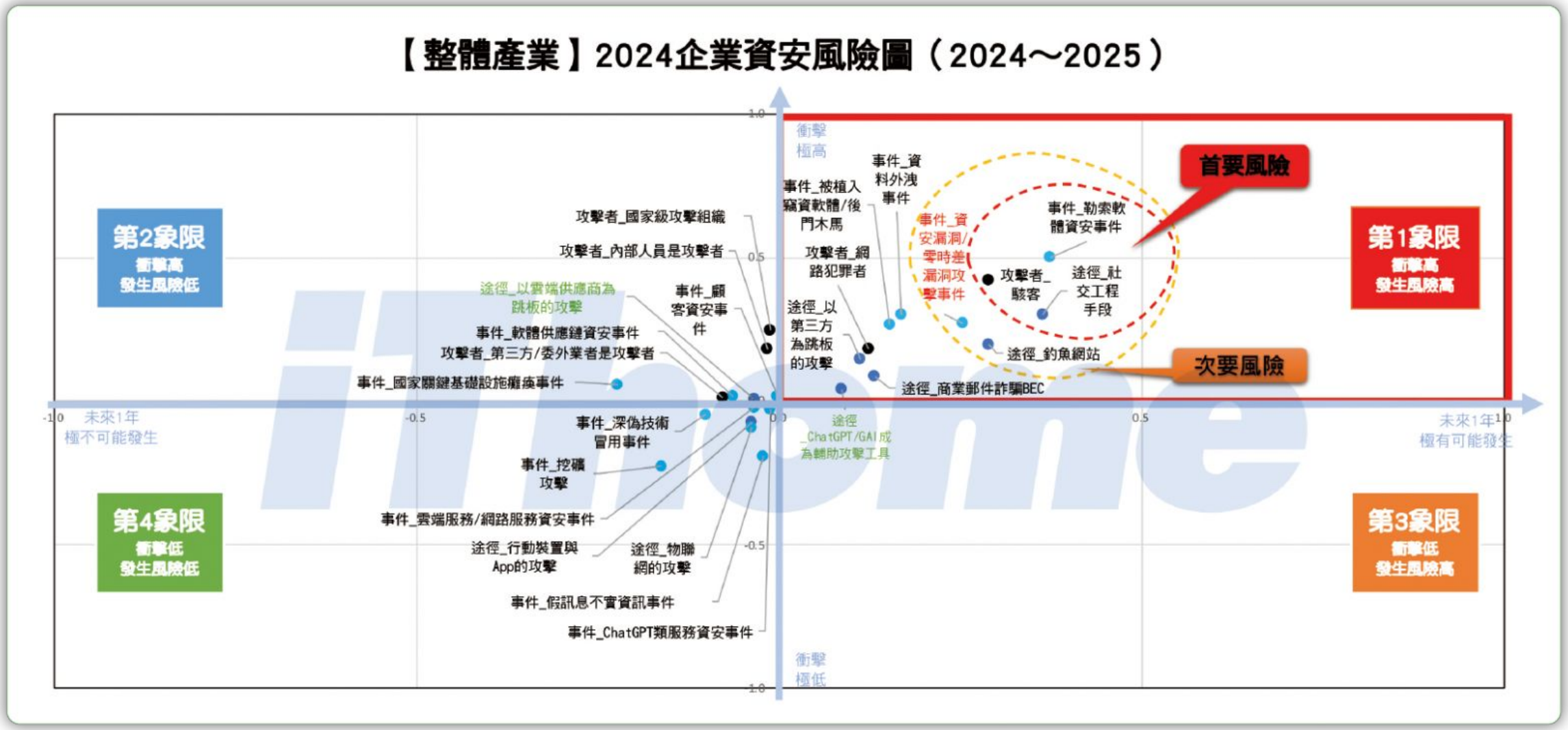
元盾資安
Meta Shield Security

資安人才現況與需求



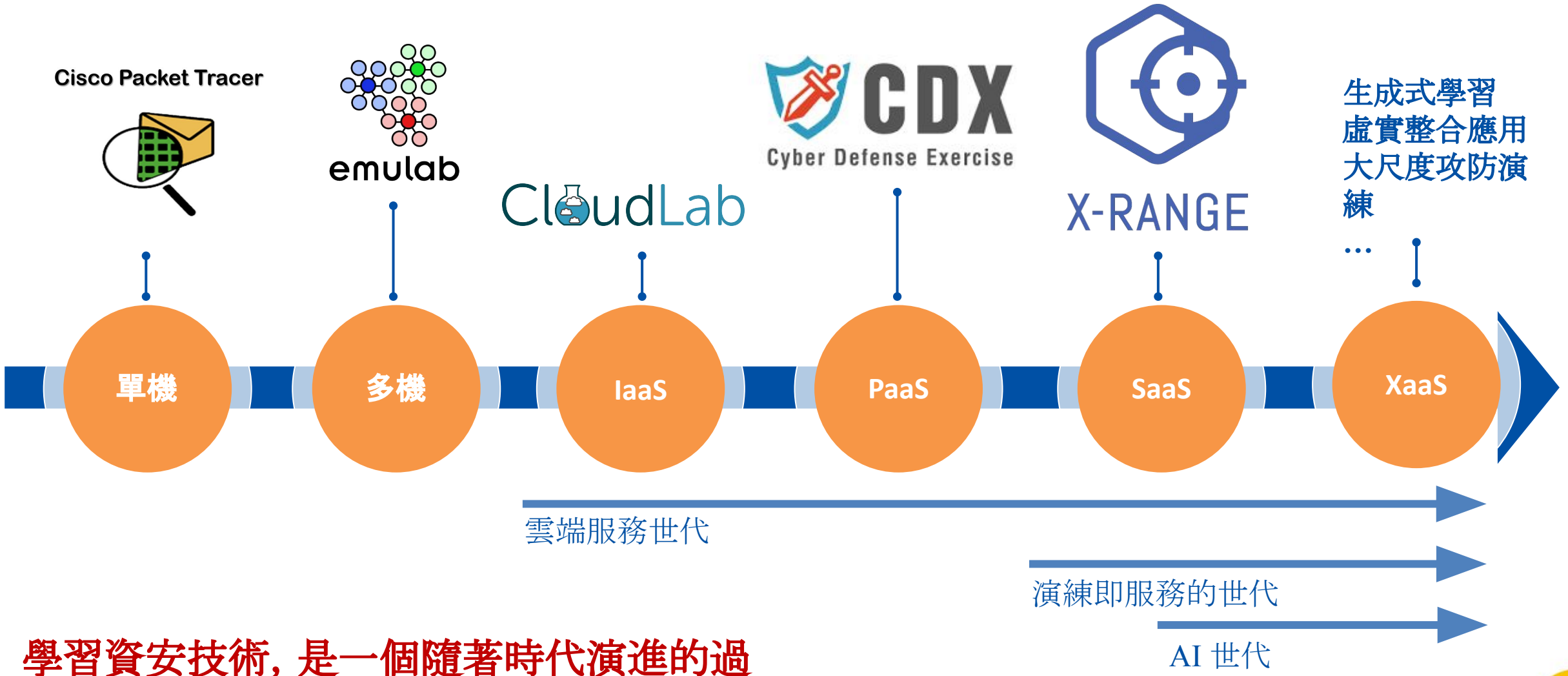
- 台灣 1 年遭駭 7420 萬次，全球之冠
- 台灣遭駭次數為各國平均值 2.7 倍、網路勒索全球第 4 多
- 資安人才缺口，企業維運類資安人才為大宗
- 資安設備買越多，資安維運越吃力
- 資安人力重實戰，資安防護設備無法取代
- 資安人才養成刻不容緩

普遍面臨的資安風險與困境



資料來源：2024 iThome CIO大調查，2024年4月

參與過的資安人才試鍊場發展



學習資安技術，是一個隨著時代演進的過程！

SHIELDXTREME

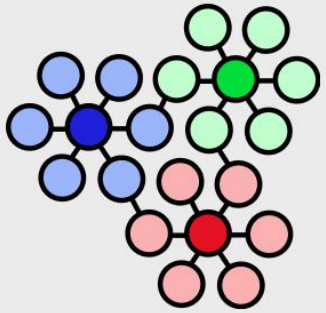
發展歷史與回憶…

一趟前往 Salt Lake City 取經的故事, 開 啟了台灣第一代的網路資安實驗平台。

emulab

A time- and space-shared platform for research, education, and development in distributed systems and networks. Emulab's primary goals are ease of use, control, and realism, achieved through consistent use of virtualization and abstraction.

Request an Account



Emulab is a network testbed, giving researchers a wide range of environments in which to develop, debug, and evaluate their systems. The name Emulab refers both to a **facility** and to a **software system**. The primary Emulab installation is run by the Flux Group, part of the School of Computing at the University of Utah. There are also installations of the Emulab software at more than two dozen sites around the world, ranging from testbeds with a handful of nodes up to testbeds with hundreds of nodes. Emulab is widely used by computer science researchers in the fields of networking and distributed systems. It is also designed to support education, and has been used to teach classes in those fields.

- Emulab Wiki
- How to Get Started
- Acceptable Use Policy
- Administrative Policies
- Security Policies
- Hardware Overview of the Utah cluster
- What happened to the old Emulab?

Cluster Status

Active Experiments: 40

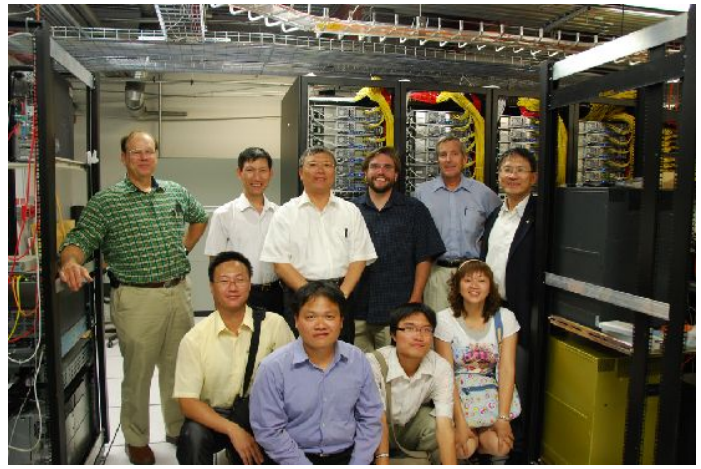
Type	Free	% Inuse
d430	2	99% inuse
d710	67	58% inuse
d820	2	88% inuse
pc3000	108	31%

Activity

Projects	1474
Users	4932
Profiles	2063
Experiments	91481

Looking for the old Emulab frontpage?

https://www.emulab.net/



https://www.testbed.ncku.edu.tw/

國網中心的 CDX

https://cdx.nchc.org.tw/

資安的夥伴 - 微智安聯

- 在地提供即時產品服務
- 提供**雲端**、**地端**與**混合雲**服務模式

01 全球最大資安事件應變組織正式會員

02 全球金融服務資訊分享與分析中心 MSSP會員

03 全公司通過 ISO 27001 資訊安全管理系統認證

04 核心成員皆為國際資安組織會員

05 在地化服務

HN/P

OWASP

CSA cloud security alliance℠

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

FIRST Improving Security Together

- FIRST 匯集來自世界每個國家/地區的事件響應和安全團隊
- **ShieldX PSIRT**為 FIRST 正式會員

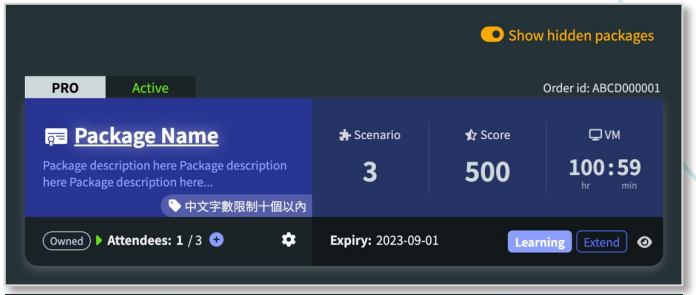
FS-ISAC

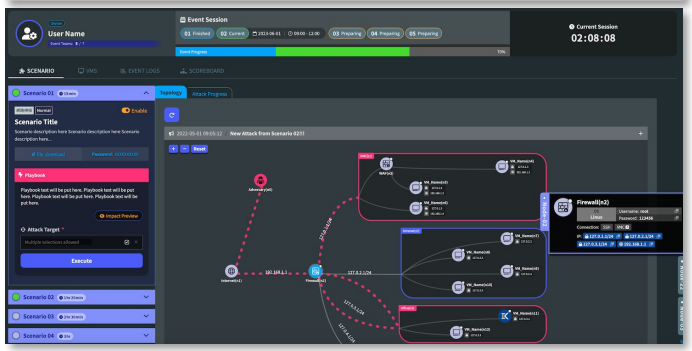
- FS-ISAC 擁有超過 **7,000 家**成員公司
- **Shield eXtreme** 為 **FS-ISAC MSSP**成員, 亦為**國內第一家**在地提供金融威脅情資服務
- 主動收集與分析來自於全球佈署之欺敵網路

微智安聯的產品及服務

X-Range
資安演訓平台

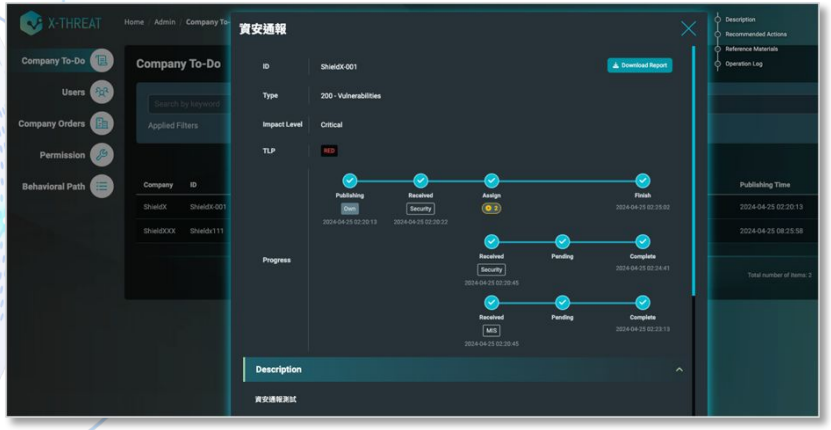
-符合**NICE**、**ECSF**、資安人培框架
-個人紅藍隊資安技術實作
-真實體驗**擬真情境**與環境
-企業網路架構團隊**攻防演練**
-資安人員技能評估與考核





X-Threat
威脅情資管理平台

-符合**ISO 27001:2022** 版本之程序要求:蒐集、分析、溝通與管理
-整合企業資安防護系統,**自動派送**阻擋清單
-支援**ISAC**組織情資管理作業要求與分享機制
-支援國際商用情資,單一訂閱與整合介面



X-Village
資安風險監控平台

-**外部曝險**即時分析與持續監控服務
-企業**弱點及漏洞**掃描與滲透測試
-**企業內部**資安健康狀態檢查服務
-半導體供應鏈**資安評級分數合規改善**服務

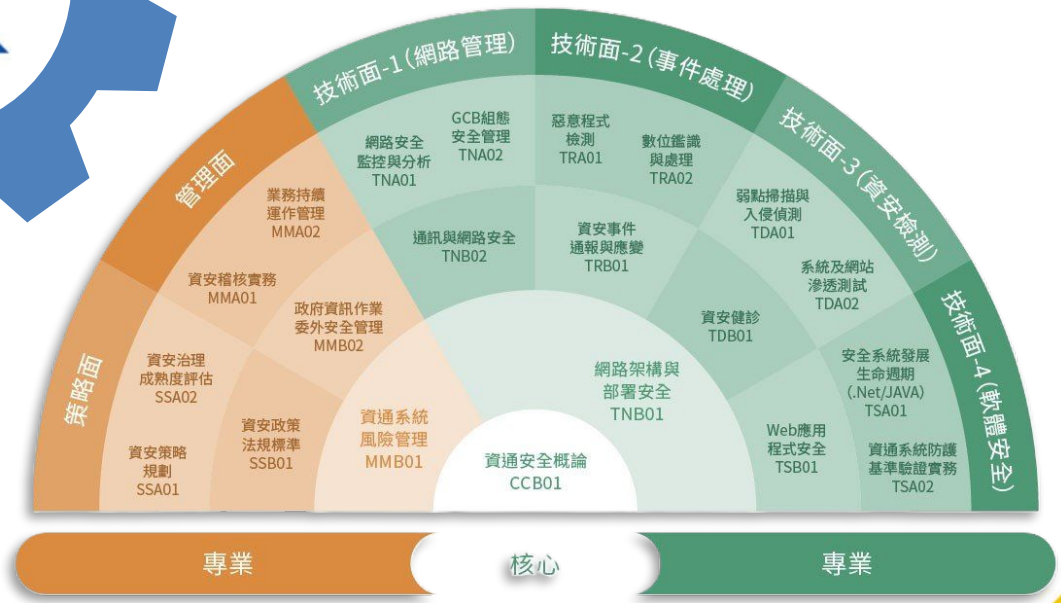
SHIELDXTREME

資安菁英人才育成

- 結合「微智安聯」所發展之資安演訓平台 **X-Lab** ，建立企業資安職能所需 **資安實務技能** 之人才

- 導入「微智安聯」資安威脅情資管理平台 **X-Threat**
- 建立資安威脅預警防禦機制，**強化資安聯防成效**

- 結合「微智安聯」所研發之攻防演練平台 **X-Team**，進行沉侵式攻防演練
- 以 **MITRE ATT&CK** 為技術核心，進行紅藍攻防演訓



X-Range 資安攻防演訓平台

資安攻防演訓

攻擊/防禦技術實作

包含攻擊面向(紅隊)及防禦面向(藍隊)的技術實作與工具應用。

獨立專屬的演訓環境

提供每位使用者或每個團隊獨立的實作環境與網路架構。

企業網路模擬與整合

模擬現實中企業網路的環境與架構，整合商業或開源資安解決方案，打造虛擬化數位靶場。

多樣化演訓情境選擇

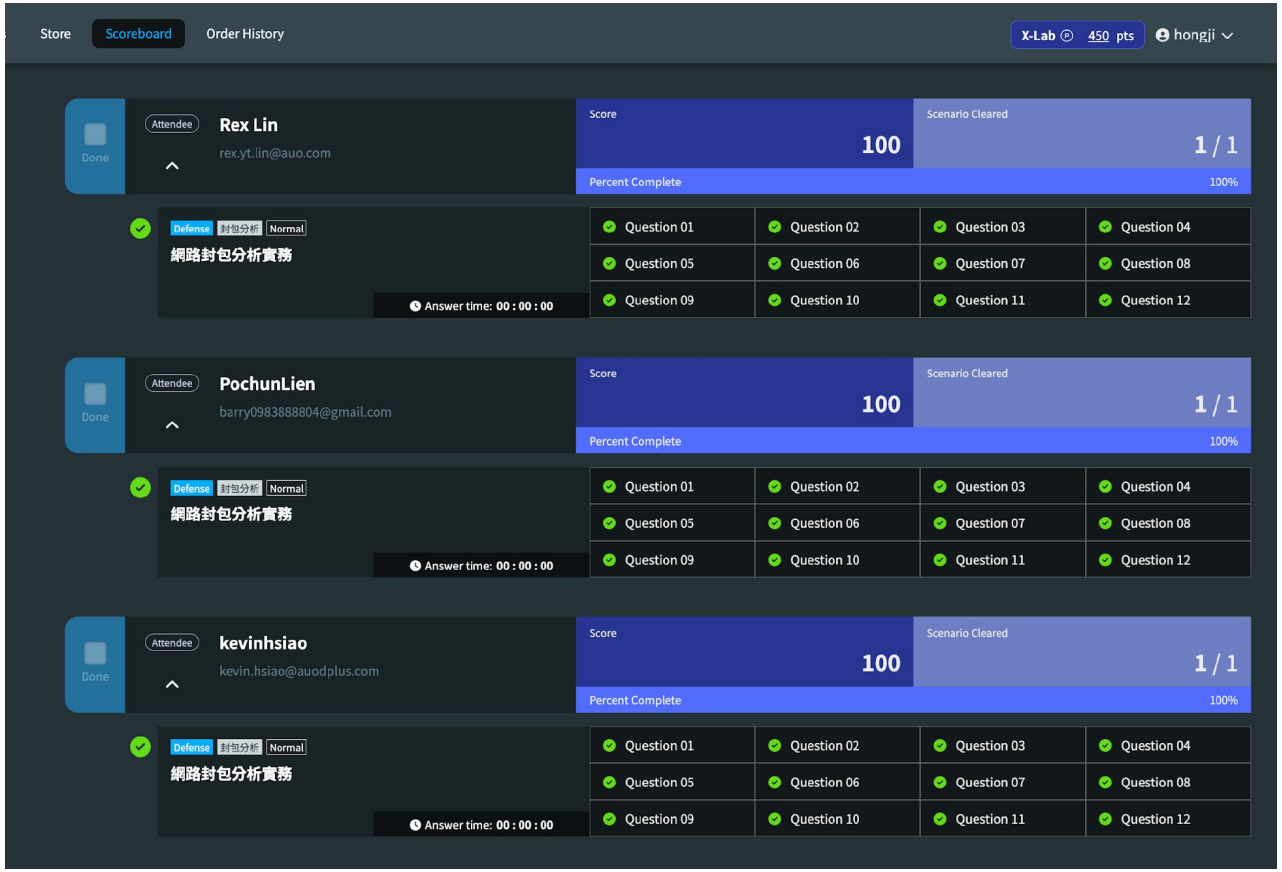
類別涵蓋十種以上的資安主題，提供超過100個演練情境。

實務技能與職能對應

採用國際通用的資安人才職能框架對應學習內容，幫助學習者健全資安職能發展藍圖。

X-Lab 專注於個人資安實作能力提升

- 團隊追蹤每個人的學習歷程

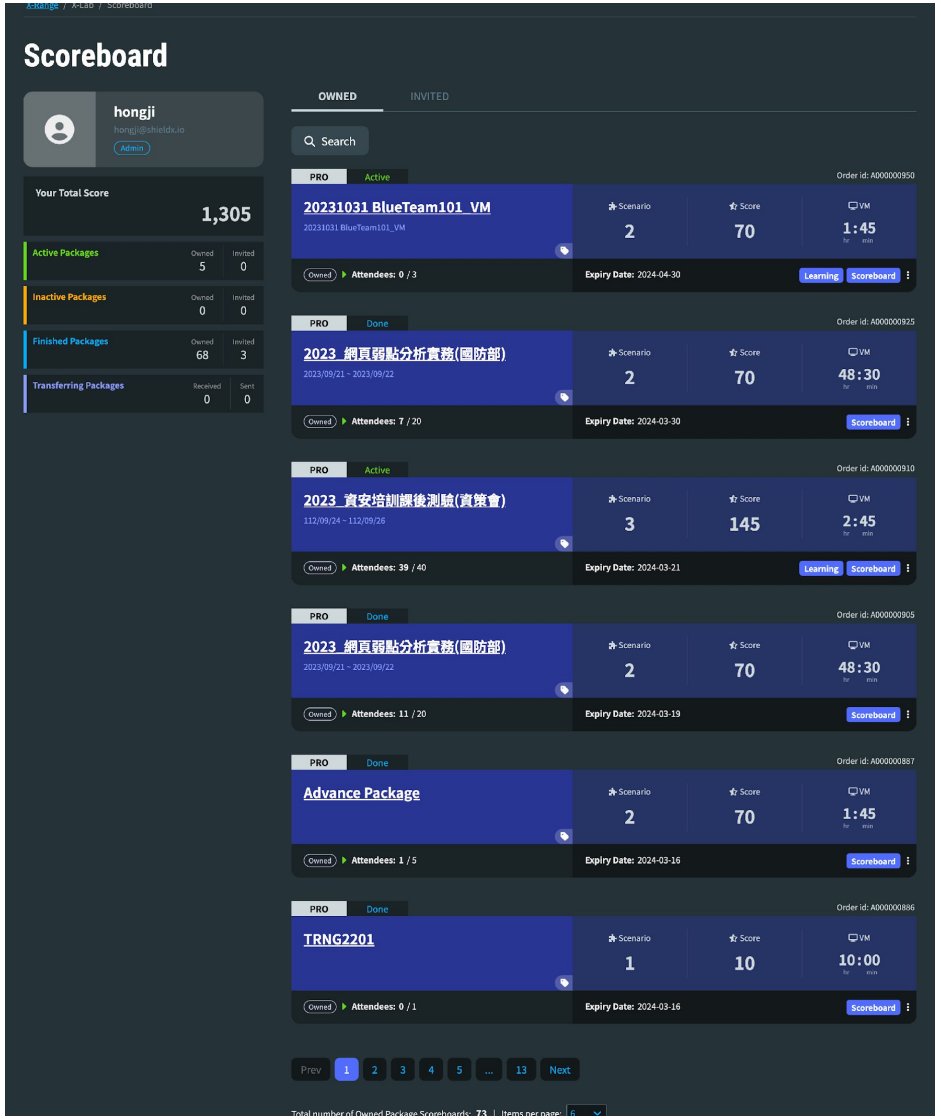


- 提供講師(或管理者)追蹤並管理多位學員(學習者或受測者)歷次練習情形與成績。
- 依照學習成效評估其個人的能力弱點，透過重複學習或加深學習，強化該項技能的肌肉記憶。
- 亦可作為評估人員定期能力考核或應聘考核的參考依據。

X-Lab 專注於個人資安實作能力提升

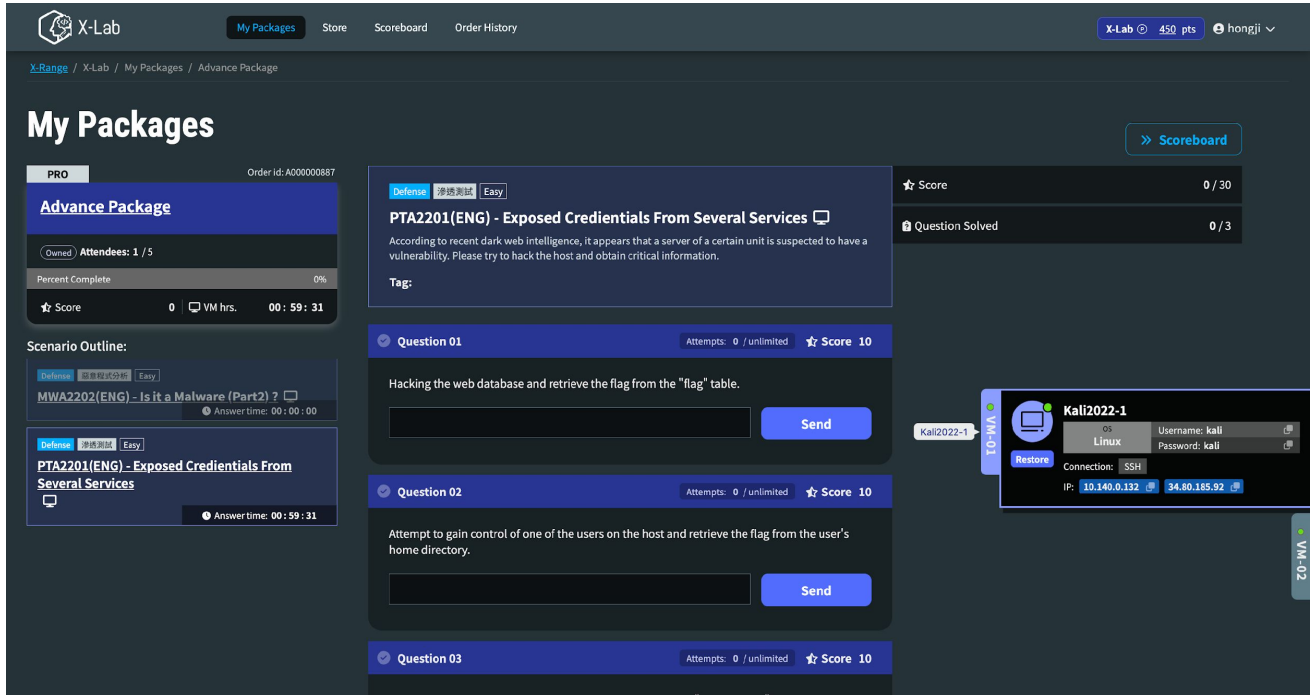
- 個人的學習歷程

  - 學員(學習者或受測者)可於專屬的Scoreboard瀏覽追蹤歷次練習情形與成績。
  - 可依照個人學習成效評估能力弱點，透過重複學習或加深學習，強化該項技能的肌肉記憶。



X-Lab 專注於個人資安實作能力提升

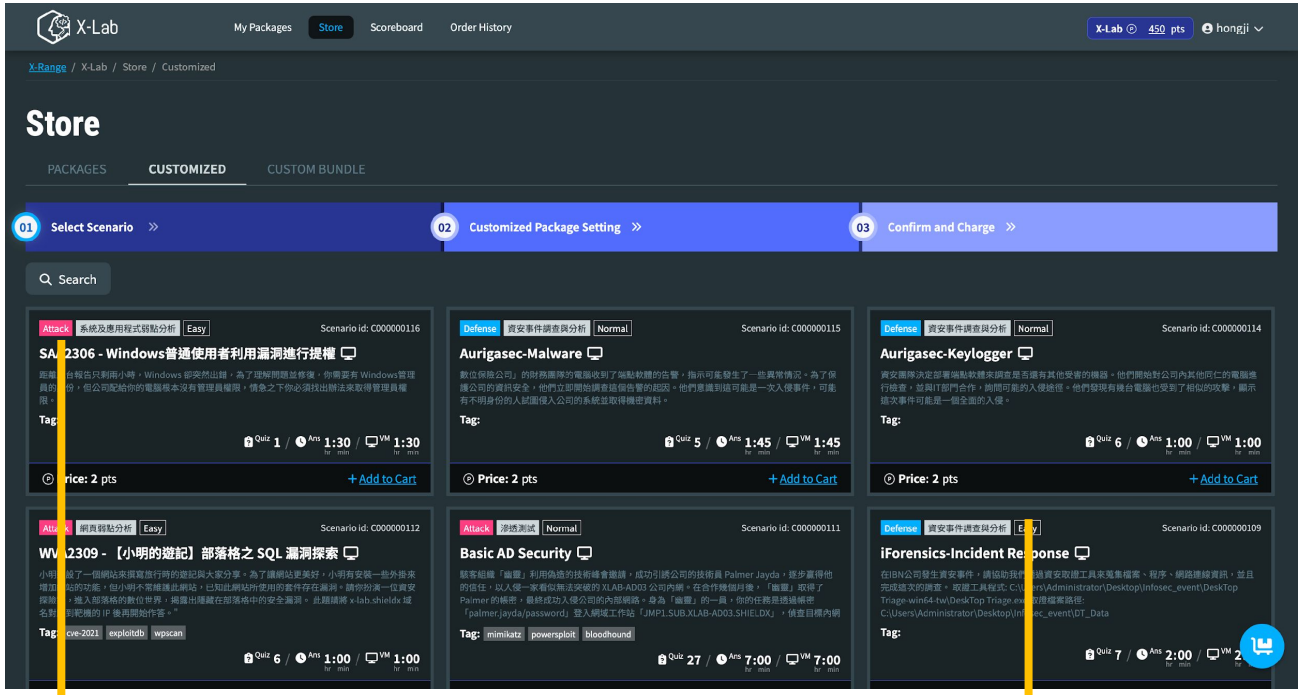
- 專屬專人使用練習環境



- 個人化的練習環境與情境。
- 實作練習虛擬機或靶機，均為個人專屬，不與他人共用。
- 無須安裝任何工具，僅需透過瀏覽器即可完成功能開啟及問題分析作業。
- 全雲端化系統架構，不用擔心資源不足的情形。

X-Lab 的多樣化與豐富性

- 情境主題多樣化，多元選擇合適的訓練主題



依照「攻」、「防」選擇主題

依照「難易度」挑選練習情境

- 商城模式，可挑選多種主題情境。
- 依照「攻」「防」不同主題分類。
- 依照「難易度」分類提供挑選參考。
- 具備打包模式，選擇複合式主題類型，一次滿足多種情境練習需求。
- 打包後情境可提供多人使用，作為評估的練習或考題依據。
- 每季更換最新情境主題供選擇。

課程建議

*建議1日課程選擇1個主題

課程名稱	課程大綱	時數	演練情境搭配
惡意程式分析	有使用端點保護軟體EDR以及進階的系統工具如 Sysinternals Suite、IDA Pro等分析工具進行惡意軟體分析和檢測。了解惡意程式行為和防禦方法。	6小時	惡意程式分析
封包分析	具備使用如Wireshark、TCPDump 等封包分析工具，進行資安事件封包 分析的豐富經驗。深入理解網路封包原理，能 夠迅速識別異常流量模式和潛在的安全威脅，	6小時	封包分析
網頁弱點分析	熟悉網頁應用程式安全，包括了解常見的網頁應用程式漏洞（如跨站 腳本攻擊、跨站偽造請求等）和防禦方法。有使用和設定網頁應用程式防火牆（WAF）的經驗。有進行程式碼審 查和使用自動化安全掃描工具的經驗。	6小時	網頁弱點分析 網頁應用程式碼分析
資安事件分析	有利用網路流量分析工具和日誌管理系統進行深入的網頁伺服器事件分析和調 查經驗。瞭解網站安全相關攻擊手法如 SQL注入、跨站腳本和跨站點請求偽造（CSRF）等原理	6小時	惡意程式分析 資安事件調 查與分析 威脅情資分析
資安健診	具有基本的網路協議（如 TCP/IP）以及操作系統的基本知識，且使用網路封包分析經驗如 wireshark以及Sysinternals Suite等工具分析經驗。	6小時	封包分析 惡意程式分析
應用程式介面安全	熟悉網頁安全及 API基礎知識，包括了解常見的網頁應用程式漏洞（如注入攻擊、認證失效等）和防禦方法。具備開發相關經驗及資安掃描工具使用經驗尤佳。	6小時	網頁弱點分析

X-Team 演練平台之應用

X-Team **企業擬真平台**，虛擬化企業內各種 IT 元件, 包含:

- 網路層防護:防火牆、IPS、WAF、Proxy
- 應用層系統:Web Server、DB Server、AD Server、SIEM…
- 系統層:Windows Srever / PC、Linux Server…
- 端點資安防護:EDR、AntiVirus…

演練情境：資安漏洞攻擊事件

演練說明

演練聚焦在正在攻擊或是已經被駭客入侵的主機，在演練過程當中需要進行事件的調查與分析，分析駭客攻擊的前、中、後，過程當中須從事件主機當中，找出有攻擊者來源、駭客所植入受害主機的惡意程式進行解析，並且建立IoC入侵指標以避免災害擴大。
此演練為主要為針對CVE編號所導致的入侵事件，考驗藍隊是否在演練中對透過受害主機完成分析，找出入侵根因。

時間：90分鐘

難易度

演練內容

- 識別受害主機攻擊手法與漏洞
- 識別駭客攻擊前的行為及工具
- 分析駭客攻擊成功後的攻擊軌跡
- 建立IoC入侵指標

MITRE ATT&CK™

策略	技術
偵察	T1591
資源開發	
初步訪問	T1190
執行	T1059、T1053
持續性	T1547
權限提升	T1068、T1548
防禦迴避	
憑證存取	T1110
探索	T1046, T1083
橫向移動	
收集	T1074
命令與控制	
外洩	T1567
影響	

演練情境：勒索軟體攻擊

演練說明

此次演練聚焦於勒索軟體攻擊，模擬同仁電腦因釣魚電子郵件或駭客利用漏洞攻擊，導致單一台或多台電腦的資料被加密。學員需針對勒索軟體的行為進行深入解析，嘗試找到解密金鑰，並設法恢復被加密的資料。演練過程中，
此演練學員將學習如何有效識別勒索軟體的加密邏輯，對勒索軟體惡意行為完成分析，最後嘗試進行資料復原動作。

時間：60分鐘

難易度

演練內容

- 勒索軟體的行為分析與感染路徑追蹤
- 解密金鑰的尋找與分析技術
- 建立針對勒索軟體攻擊的防禦與應變措施
- 建立入侵偵測指標

MITRE ATT&CK™

策略	技術
偵察	
資源開發	
初步訪問	T1566 、T1190
執行	T1204
持續性	
權限提升	
防禦迴避	T1055、T1027、T1562
憑證存取	
探索	T1046
橫向移動	
收集	
命令與控制	
外洩	
影響	T1486

演練情境：社交工程攻擊

演練說明

此次演練聚焦於社交工程攻擊手法所引發的駭客入侵，藍隊需對釣魚電子郵件、不明連結等可疑行為進行深入分析。過程中，學員需對已感染的系統進行詳細檢查，評估是否遭駭客獲取存取控制權，並進一步確認是否導致機密資料的外洩風險。
此次演練將強化藍隊在應對社交工程攻擊中的威脅分析、系統調查。

時間：90分鐘

難易度

演練內容

- 識別社交工程攻擊手法
- 分析駭客組織
- 惡意程式行為分析
- 與資料外洩分析
- 建立入侵偵測指標

MITRE ATT&CK™

策略	技術
偵察	
資源開發	
初步訪問	T1566
執行	T1203、T1053、T1204
持續性	
權限提升	
防禦迴避	T1055、T1562
憑證存取	T1056、T1003、T1552
探索	
橫向移動	
收集	
命令與控制	
外洩	
影響	

演練情境：資料外洩事件

演練說明

演練聚焦於資料外洩事件，專注於模擬攻擊者利用網頁相關漏洞進行攻擊。攻擊者可能透過常見的網頁應用漏洞，如SQL注入、檔案上傳或網頁篡改等手法，非法存取並竊取系統中的敏感資料。此次演練旨在加強藍隊對此類攻擊手法的應對能力。

時間：60分鐘

難易度

演練內容

- 資料外洩手法分析
- 漏洞攻行為分析
- 惡意程式程式敏感資料存取行為分析
- 網路行為進行分析
- 清除網頁後門程式
- 建立入侵偵測指標

MITRE ATT&CK™

策略	技術
偵察	T1595
資源開發	
初步訪問	T1190、T1133
執行	T1059、T1203
持續性	
權限提升	
防禦迴避	
憑證存取	T1110、T1557
探索	T1040
橫向移動	
收集	T1560 、T1119、T1056
命令與控制	
外洩	T1567
影響	

演練情境：內部威脅

演練說明

次演練聚焦於內部威脅，模擬攻擊者如何利用內部常用服務發動滲透攻擊及傳播惡意程式。演練的核心是惡意程式行為的解析，可能涉及模擬使用者感染無檔案攻擊、文件型攻擊或後門程式等不同類型的惡意行為。攻擊過程中還可能搭配DLL劫持(DLL Hijacking)、迴避技術(Evasion)等手法，使駭客能夠取得主機控制權，進一步操控系統。

時間: 90 分鐘

難易度

演練內容

- 內部威脅手法研判
- 惡意程式行為分析
- 惡意程式迴避技術應對
- 建立入侵偵測指標

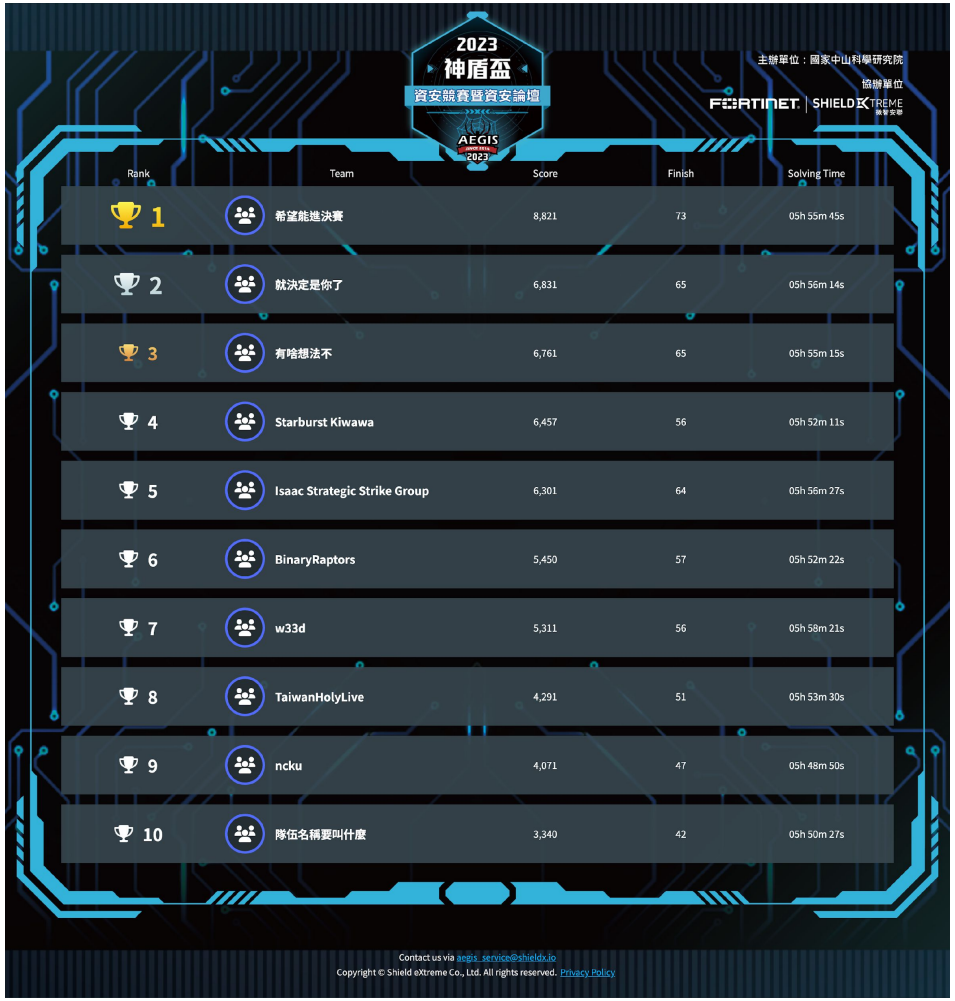
MITRE ATT&CK™

策略	技術
偵察	
資源開發	
初步訪問	
執行	T1059 T10534
持續性	T1547、T1574、T1503
權限提升	
防禦迴避	T1574、T1112、T1055、T1014 、T1562
憑證存取	T1056、T1003、T1552
探索	
橫向移動	
收集	T1560、T1119、T1074
命令與控制	T1071、T1132、T1572
外洩	
影響	

實績案例-中科院神盾盃資安競賽

- 提供初賽攻防及決賽攻防二階段比賽平台
- 情境包含「網頁安全」、「社交工程」、「異常網路行為」內容等情境題目
- 初賽：每組隊伍5人，共40組隊伍，採用線上方式進行，
- 決賽：每組隊伍5人，共計10組隊伍。，採實體到場方式進行。

實績案例-中科院神盾盃資安競賽



實績案例-離島盃資安競賽(金門大學&澎湖科技大學)

實績案例-資安署「資安工作坊」

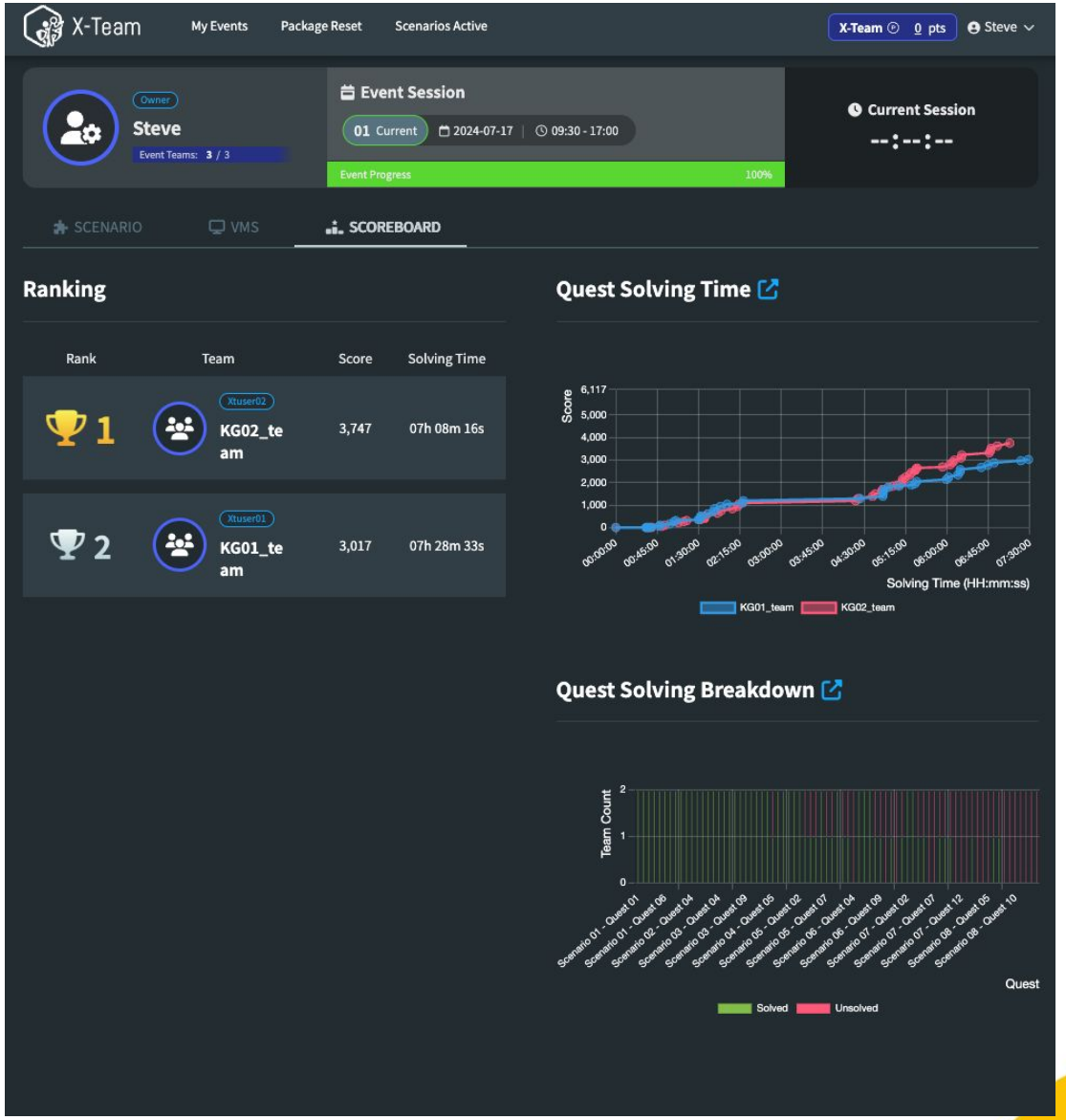
- 本案資安工作坊之目的，為培訓資安專責人員所需技術面或管理面資安技能需求，透過資安事件及模擬練習環境提升學員實務資安攻防原理。
- 情境包含「網頁安全」及「社交工程」內容等情境題目。
- 每組隊伍3人，共計10組隊伍，採實體到場方式進行。

實績案例-ＯＯ金控攻防演練

- 為提升ＯＯ金控資安事件之自我應變能力及資訊安全體系維運核心團隊，委請安排執行資安事故調查挑戰賽，得以自立因應各種資安威脅攻擊事件。
- 因應SOC L1/L2同仁參與今年度的專業職能教育訓練，確保同仁能將教育訓練中所學的知識及工具運用於實際環境上。
- 每組隊伍3～4人，共計3組隊伍，採實體到場方式進行。

實績案例-ＯＯ銀行攻防演練

- 為提升ＯＯ銀行資安專責人員所需技術面或管理面資安技能需求，透過資安事件及模擬練習環境提升學員資安攻防原理。
- 情境包含「資料外洩事件」、「內部威脅」及「資安漏洞攻擊」內容等情境題目。
- 每組隊伍3～4人，共計2組隊伍，採實體到場方式進行。



期待與我們一同 啟航

進入沉浸式資安學習的領域

資安人才的試鍊場


元盾資安 X 微智安聯
SHIELD XTREME
即時修補
Patch
主動警戒
Alert
PADDA
主動式防護
藍隊演練專家
X-RANGE
智能演練
AIPT
持續防護
Detection
主動誘捕
Deception
X-RANGE
資安攻防演訓平台

- **Hackers are everywhere, all the time!**

Are you READY ?

Welcome to Shieldx.io

SHIELDEXTREME

元盾資安
Meta Shield Security