資安菁英實戰培育課程第三期資訊

課程時間	上午 9 時 30 分至下午 5 時止，中間休息 1.5 小時
課程地點	臺北創新實驗室會議 A 廳 臺北市內湖區洲子街 12 號 2 樓(近捷運港墘站 2 號出口)
報名網址	https://reurl.cc/myp0QM

（一） 藍隊解壓縮 - 從零開始建構企業防禦工事

課程日期	113 年 11 月 2 日（六）、11 月 3 日（日）
先修技能	具備基本 Windows 與 Linux 操作能力即可。
自備工具	VMware Workstation、VMware Fusion (Mac User 請使用非 M1/2 晶片之 Mac)，課程預計提供 3 套 VM（ova），硬碟空間需求 60G 以上，記憶體 16G 以上。

1. 課程介紹：在駭客威脅日益猖獗的今天，企業需要投入大量的時間和資源來應對攻擊與資安事件所帶來的損害。然而，許多企業對於全面的事前防範、事中應對和事後復原策略，甚至所需的資安解決方案的瞭解往往過於單一。為此，本課程以藍隊思維為出發點，深入探討藍隊所需的所有核心概念與技術。

本課程內容涵蓋全面，預計包括藍隊架構與組成、事件應變處理、數位鑑識、惡意程式分析和威脅監控等藍隊日常工作所必備的各項技能。本課程將理論與實作相結合，確保學員能夠在實際工作中應用所學。課程後，學員將掌握藍隊相關的知識與技術，為企業網路安全提供有效的技術能量支持。

2. 講師介紹：

鄭仲倫（Mars Cheng）目前為 TXOne Networks 產品資安事件應變暨威脅研究團隊經理，負責協調產品安全與威脅研究事

宜，同時亦擔任台灣駭客協會常務理事與 HITCONCISO Summit 2024 的總召集人，負責推進與維繫資安社群、企業及政府間的關係。

Mars 在國際資安會議中發表超過 50 場次的演講，這些會議包括 Black Hat USA/Europe/MEA、RSA Conference、DEFCON、CODE BLUE、FIRST、HITB、HITCON、Troopers、NOHAT、SecTor、SINCON、ROOTCON、ICS Cyber Security Conference Asia and USA、CYBERSEC、CLOUDSEC、VXCON 等。同時專注於 ICS/SCADA、企業網絡安全、威脅獵捕及新興資安議題的研究，至今提交了 10 多個 CVE 編號，並於三篇 SCI 期刊中發表與應用密碼學相關之論文。此外，Mars 也曾擔任 HITCON CISO Summit 2023、HITCON PEACE 2022、HITCON2021 的總召集人及 HITCON 2020 的副總召集人。

3. 課程摘要：

(1) 藍隊簡介

- 何謂藍隊？
- 藍隊組成與能力需求概要

(2) 公開來源情報(OSINT)應用分析(Lab)

(3) 資安威脅偵測端點與網路

- 資訊安全監控中心簡介
- 威脅情資應用分析概要
- 威脅偵測策略與分析 (Lab)
- 閘道及應用程式威脅偵測與分析(Lab)
- 端點威脅偵測與分析(Lab)惡意程式加殼分析實戰

(4) 資安事件應變與數位鑑識實務

- 資安事件應變與數位鑑識介紹
- Windows/Linux 實際案例演練(Lab)

(5) 惡意程式分析實務

- 惡意程式分析工具簡介
- 惡意程式分析實戰(Lab)

（二） 雲端保衛戰：藍隊的雲端安全生存指南

課程日期	113 年 11 月 9 日（六）
先修技能	具備基本 Linux 操作能力。
自備工具	VMware Workstation 、VMware Fusion（Mac User 請使用非 M1/2 晶片之 Mac），硬碟空間需求 30G 以上，記憶體 8G 以上。

1. 課程介紹：

雲端安全至關重要。在當前的數位時代，企業和個人越來越依賴雲端技術來儲存和處理數據。這些數據通常包含敏感資訊，因此保障其安全性顯得尤為重要。然而，雲端安全問題的主要原因常常是由於使用者錯誤地使用雲端服務。因此，學習如何正確使用雲端服務並採取適當的安全措施，是所有雲端使用者和管理者應具備的基本知識。

本課程學員將了解雲端攻擊的全貌，並從紅隊的攻擊思路中學習如何預測和防禦潛在威脅。同時，課程將介紹藍隊在雲端安全中的最佳實踐，幫助學員建立穩固的安全措施。課程內容結合 NIST CSF 框架，提供實用的工具和方法，讓學員能夠系統化地強化自身的雲端安全能力。透過實戰演練，學員將學習如何在面對安全事件時快速應變，提升應對能力。此外，課程將介紹雲端安全成熟度模型，指導學員如何通過系統性的強化流程，不斷提升自身的雲端安全成熟度。

透過本課程，學員將全面掌握雲端安全的核心概念和實踐方法，建立起完善的安全策略，以應對各種雲端安全挑戰。

2. 講師介紹：

林殿智（Dange Lin）現為奧義智慧科技的資深資安主任研究員，擔任車載安全研究的 Team Lead，專注於雲端安全、車載安全、機器學習與零信任等領域，除了精通攻擊技術，還熟悉資安管理策略，並持有 CACSP 證照。曾於 Black Hat Europe Arsenal、HITCON、CYBERSEC、MOPCON、ECCWS 等多個研討會發表演講，於 AIS3、NICS 等多場公開授課培訓擔任講師，並且是著名資安教育桌遊《CYBERCANs》的設計者之一。

3. 課程摘要：

(1) 雲端安全概述

- 雲端計算的基本概念
- 雲端安全的重要性和挑戰
- 實戰演練：熟悉雲端環境

(2) 雲端安全常見問題

- 使用者錯誤配置的影響
- 典型的安全漏洞案例分析
- Cloud Security Alliance - Top 11
- 雲端攻擊概念與最新攻擊趨勢

(3) 紅隊攻擊思路

- 雲端攻擊的全貌
- 紅隊如何滲透雲端環境
- 紅隊 Initial Access、Persistence、Privilege Escalation、Exfiltration 等思路

(4) 藍隊防禦策略

- 雲端安全防禦框架與成熟度框架

- 實戰演練：基於 NIST CSF 的防禦實踐和技術演練
- 實戰演練：風險盤點、安全監控和應變措施
- 雲端安全成熟度提升流程

（三） 網路威脅防禦競賽

課程日期	113 年 11 月 10 日（日）

透過國家資通安全研究院內的演練平台，以本次課程所習得之知識技能，進行實戰演練競賽。