AIS3 課程大綱

課程名稱	資安事件 Case Study；SOC 功能、架構與營運
授課教師	安碁資訊(eDC)資安維運處處長 - 黃瓊瑩
教學目的	SOC（Security Operation Center） 資安防護中心是將不同位置、不同系統中巨量的安全事件進行匯總、過濾、收集和關聯分析，得出全局角度的風險評估結果，並根據此進行回應和處理的綜合安全平臺。Acer eDC 長期從事 SOC 服務，在本課程中分享本身實務經驗，使學員了解與 SOC 資安監控的關聯性。
課程時數	3 小時
課程大綱	● 資安事件剖析 ■ 單點突破實例剖析 ■ 全面控制實例剖析 ● SOC 架構與營運 ■ SOC 資料處理架構介紹 ■ SOC 營運管理介紹

課程名稱	攻擊手法剖析與實作
授課教師	安碁資訊(eDC)經理 - 蔡東霖 安碁資訊(eDC)技術主任 - 陳威安
教學目的	藉由入侵攻擊案例的剖析，搭配上機操作練習常見資安攻擊手法並實機演示。學員依照攻擊手法，進行分組並實際練習及驗證成果。
課程時數	2 小時
課程大綱	● Log 與攻擊活動偵測 ■ Log 種類介紹 ● 實作常見資安攻擊手法及實機演示 ■ Upload / SQL Injection ■ PtT(Pass the ticket attack)實作

課程名稱	SOC 事件分析實務與實作
授課教師	安碁資訊(eDC)經理 - 孫明功
教學目的	實際展示如何應用 SIEM (Security Information & Event Management) 來偵測與預防類似的資安事件發生，使學員理解如何利用 SOC 協助蒐集與分析資安事件，來加強網路攻擊防禦。
課程時數	2 小時
課程大綱	● SOC 事件分析平台功能與應用說明 ● 分組實際練習並驗證成果

課程名稱	Making a security alarm for fun and profit
授課教師	聯發科技術經理、HITCON 戰隊領隊 - 李倫銓(Alan Lee)
教學目的	學完本課程後，學員將理解常見攻擊手法，並撰寫程式從 log 中分析相關攻擊。使用 Linkit connect 7681 開發板連接 MCS (Mediatek Cloud Sandbox)，並運用 API 呼叫 IoT 裝置觸發警告。
課程時數	3 小時
課程大綱	● 從 Log 分析了解攻擊 ● 物聯網應用介紹 ● 做出你的資安警報器 ● Linkit connet 7681 與 MCS ● 運用 MCS API 呼叫 IoT 裝置

課程名稱	The development of CTFs
授課教師	資安研究員、PPP 戰隊隊員 - Tyler Nighswander
教學目的	In the past 6 years there have been several large changes to the CTF scene. For example, the style of problems, the volume and level of competitions, the competitiveness of teams, and the development of tools have all had a large influence on competitions and strategies required to be successful. This course will walk through some history to help put tools and techniques in context with hands on lessons.
課程時數	6 小時
課程大綱	● Introduction to “CTF” ● What is a “CTF”? ● CTF category ● History ● Several challenge ● CTFs Tools ● CTF Meta-Game ● The Future of CTFs

課程名稱	Reverse engineering and malware analysis
授課教師	惡意軟體研究員、PPP 戰隊隊員 - Erye Hernandez
教學目的	讓學員將理解逆向工程基本概念、惡意程式的歷史與種類及惡意程式分析工具介紹及流程，並能夠應用不同種類的逆向工程工具實際演練及練習。
課程時數	6 小時
課程大綱	● Introduction to Malware Analysis ● What is malware? ● History of Malware ● Threat Actors ● Types of Malware ● RE Tools

課程名稱	Binary, Exploitation, Pwning
授課教師	HITCON 戰隊副隊長 - Sean
教學目的	學員將從講師講解 CTF 題目中，理解漏洞的利用方法和實作，如： Stack overflow / Heap overflow，以及一些繞過 DEP/ASLR 等技巧，並能夠實際操作演練。
課程時數	6 小時
課程大綱	● 漏洞的利用方法和實作 ■ Buffer overflow ◆ Stack overflow/Heap overflow ■ Return Oriented Programming ◆ Data Execution Prevention ■ ASLR(Address Space Layout Randomization) ■ Symbol resolving ■ Stack migration ■ GOT Hijacking ◆ Format String Vulnerability ◆ Heap Exploitation

課程名稱	各種 reversing 實例經驗談
授課教師	趨勢科技 RD – Dark Luo
教學目的	藉由實例讓學員學習 reversing，接著講解 wargame 解題技巧，分析 windows 裡的 undocument API 並加以利用,，解析 malware protocol 並還原通訊資料，實際帶著學員一同解題。
課程時數	6 小時
課程大綱	● Reversing 實例：Make your life easier! ■ How to bypass program registration? ■ How to avoid the NAG window? ■ How to hack a game? ■ 破解鍵盤加密晶片機制 ● DLL Hijacking 型惡意分析&提取 Shellcode 並編寫 Loader ● 編寫 IDC Script 輔助分析惡意程式 ● 惡意程式分析 & 封包解密

課程名稱	網頁應用程式安全
授課教師	戴夫寇爾執行長、HITCON 社群總召 – 翁浩正(Allen Own)
教學目的	隨著服務規模與複雜度的提升，暴露在外的風險也相對提高，因此網頁應用程式安全日趨重要，將於課程介紹 OWASP Top 10 的重要性，透過實際演練讓學員了解、改善網頁應用程式與服務的安全性，也充分了解在軟體安全風險的情況下做出決策。
課程時數	6 小時
課程大綱	● 資安概論 ● 正確防禦者的思維與駭客的思維 ● 駭客攻擊流程 ● 資安事件處理步驟 ● OWASP Top 10 ● Man-In-The-Middle Attack ● Metasploit + BeEF

課程名稱	Exploring decoys and honeypots
授課教師	中央研究院資安研究員 – Fyodor Yarochkin
教學目的	This talk will walk attendees through common methodologies of building and deploying decoys and honeypot networks as well as will discuss a number of case studies of incidents identified on honeypot networks.
課程時數	3 小時
課程大綱	● Introduction ● Darknet at Academia Sinica ● Tools of trade ● Case studies ● Detecting client attacks

課程名稱	資料科學家未曾公開之資安研究事件簿
授課教師	中央研究院資訊科學所研究員 – 陳昇瑋
教學目的	在網路安全研究中，無法預期黑客的攻擊行為，而必須從大量資料中發現及解決各種已發生或將發生可能危害使用者資料安全及隱私的行為。學員將從這場研究中，了解 data-driven network security research 及實際的研究案例，從中理解真實資料的統計分析可以幫助解決什麼樣的安全問題。
課程時數	3 小時
課程大綱	● Introduction to data science ● Data collection ● Introduction to R ● Unsubscription Prediction ● 實際研究案例： ■ Game Bots ■ 未知號碼電話該不該接？ ■ 有沒有人在偷用你的臉書？ ■ 釣魚網頁偵測 ■ 以資料分析幫助設計外觀裝備

課程名稱	Automatic exploit generation
授課教師	交通大學資訊技術服務中心教授 – 黃世昆
教學目的	Software failures 中常見的類型為 software crash，這種類型的 failures 特徵在於軟體測試、可靠性及質量保證，而非網路安全。透過構建 symbolic failures 模型研究 software crash 的行為，並自動生成通過 symbolic 模型的操作軟體攻擊，帶著學員了解對軟體品質的網路安全威脅。
課程時數	3 小時
課程大綱	● AEG history ● Introduction to CRAX ● Method ● Implementstion ● Result ● ROP Chain ● TRITON

課程名稱	行動軟體(APP)安全檢測
授課教師	國家資通安全會報技術服務中心組長 – 陳培德
教學目的	在目前新興的行動軟體檢測上，學員會了解實務的操作方法與風險評估，實際針對 Google Play/App Store/MS Marketplace 上的 APP 軟體檢測操作，瞭解實際各 APP 市集架上常見的 APP 弱點，並討論如何預防與避免。透過交互討論思考，建立未來可行的創新的應用服務。
課程時數	3 小時
課程大綱	● 行動終端安全風險 ● 行動軟體(APP)安全性議題 ● 行動軟體(APP)安全檢測框架 ● 檢測工具及流程 ● 檢測結果摘要 ● 行動裝置(APP)強化重點

課程名稱	APT 攻守地圖與惡意程式家族
授課教師	臺灣威瑞特總經理 – 吳明蔚(Benson Wu)
教學目的	APT 攻擊者往往都會透過長時間且持續性的潛伏及監控，而在本課程學員將了解 APT 攻擊及可能遭受攻擊的對象、攻擊者的攻擊手法，且該如何偵測攻擊。接著分析惡意程式家族，讓學員理解其特點。
課程時數	3 小時
課程大綱	● 什麼是 APT (Advanced Persistent Threat)？ ● 受攻擊對象 ● 攻擊的手法 ● 如何偵測攻擊 ● 惡意程式家族介紹 ● 案例分享