115 年第 2 期資安防護實戰產業資安菁英班課程（臺南場）

課程計畫

一、 目的

為因應現代化網路環境中高度複雜與多變之資安威脅，協助各領域中的產業資安人員提升防護應變能力，爰規劃辦理「資安防護實戰產業資安菁英班課程」，聚焦於資安防禦技術之實務應用與演練。

台南場課程專為資安從業人員打造，涵蓋惡意程式分析、Windows 逆向工程與 AI 輔助威脅獵捕三大實戰主題。

課程一以逆向工程、編譯器原理與攻擊行動脈絡為核心，帶領入門分析師建立正確的樣本分析心法，學會運用第一線工具拆解惡意程式，產出具說服力的分析報告。課程二聚焦 Windows 系統逆向技藝，透過 30 個以上貼近實戰的挑戰關卡，涵蓋 REvil、加殼、反調試、.NET、Shellcode 等當前主流攻擊手法，培養學員獨當一面的實戰能力。課程三則從企業藍隊威脅獵捕痛點出發，教授如何運用機器學習進行特徵工程與異常偵測，並結合 LLM 自動生成 Sigma 規則，強化整體偵測工程流程。

二、 主辦/執行單位

- 主辦單位：數位發展部資通安全署
- 執行單位：社團法人台灣駭客協會

三、 課程日期與時間

本期課程共 4 天，日期分別為 115/09/12（六）－09/13（日）、115/09/19（六）－09/20（日）。

•第一天：115 年 9 月 12 日（六）

課程主題	解構野外惡意程式隨開即用的瑞士刀
報到時間	08:50-09:20
開幕式(含參訓須知等)	09:20-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

•第二天：115 年 9 月 13 日（日）

課程主題	Windows 分析核心戰略—從真實攻擊掌握完備逆向技法
報到時間	09:00-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

•第三天：115 年 9 月 19 日（六）

課程主題	透過 AI 驅動的威脅獵捕技術：從異常探索到 Sigma 規則生成
報到時間	09:00-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

•第四天：115 年 9 月 20 日（日）

課程主題	分組競賽
報到時間	09:00-09:30
分組與開賽說明	09:30-10:00
競賽時間(上午)	10:00-12:30
午休時間	12:30-14:00

競賽時間(下午)	14:00-16:00
計算分數、貴賓報到	16:00-16:30
頒獎典禮	16:30-17:00

四、 課程地點

國立成功大學電機系館令洋廳（701 臺南市東區大學里大學路 1 號），實際地點仍以開課通知為準。

五、 課程及講師資訊

➢ 課程一

課程名稱	**〈解構野外惡意程式隨開即用的瑞士刀〉**
課程講師	馬聖豪（Sheng-Hao Ma）
講師簡介	馬聖豪（@aaaddress1）現任 TXOne Networks Inc.產品資安事件應變暨威脅研究團隊 Team Lead。 專注並熱愛於逆向工程與威脅分析，擁有逾 15 年實務經驗。研究領域涵蓋符號執行、人工智慧與機器學習（AI/ML）、自然語言處理（NLP）、編譯器實作、作業系統原理等。 曾任於多場國際級研討會擔任講者與培訓講師，包括 Black Hat USA/MEA、DEFCON、CODE BLUE、S4、SECTOR、HITB、VXCON、HITCON、AVTOKYO、ROOTCON 等。榮獲台灣最大資安展 CYBERSEC 之 Hall of Fame Speaker 資安大會講師名人堂殊榮。 他目前亦為 HITCON 審稿委員、並著有全球中英雙語資安書籍《Windows APT Warfare：惡意程式前線戰術指南》，致力於推動實戰導向的威脅研究與技術知識傳承。

課程簡介	對於資安從業的入門分析師而言，如何有心法與攻擊行動脈絡的正確推理拆解惡意程式是一項極為困擾的問題。上至豐富的攻擊行動、下至對於做出樣本分析有信心的逆向推理報告確實將所有潛藏的攻擊行為都分析完畢，這些看似基礎但卻實質充滿困難與挑戰而非僅只是逆向工程的技術活。 為解決多數入門分析師上述痛點，本課程內容將結合逆向工程、編譯器原理、與攻擊行動三大領域，引領學員以務實第一線分析人員使用的工具探索並掌握學習野外的樣本分析的必備心法，讓學員能以逆向心法活用各式豐富的社群工具並做出有信心的分析報告與資安調查。
課程摘要	◦ IDA、Yara/Capa 靜態逆向分析與實務 ◦ Names,ProximityView,ControlFlowGraph(Tab&LinePrefixes) ◦ FunctionBasic:Import,Export,Bounds,Format,Refs, StackFrames(3+Lab) ◦ DataStructure:Integers,Array,Ansi,Unicode,Headers (2Lab) ◦ TypeLibraries(CompilerSDKs) ◦ Binary/TextSearching ◦ ModuleRebases(Lab) ◦ 立即數&Macros(Lab) ◦ Patching(Lab)
學員先修技能	具備基本 Windows 操作能力即可
學員自備工具	裝載 Vmware Workstation、Vmware Fusion 的 Intel 晶片電腦設備，課程預計最多提供 1 套 VM（ova），硬碟空間需求 70G 以上，記憶體至少 8G 以上（建議 16G 以上為佳)。

➢ 課程二

課程名稱	**〈Windows 分析核心戰略—從真實攻擊掌握完備逆向技法〉**
課程講師	馬聖豪（Sheng-Hao Ma）
講師簡介	同課程一
課程簡介	Windows 系統為最廣為使用的作業系統而有著最豐沛應用且複雜的設計架構、使得完整掌握 Windows 逆向工程技巧相當困難，本課程也為此規劃了完整逆向技藝將帶 領學員探索 Windows 各項系統實現原理與對應的實務分 析技巧。本課程包含 30+個使研究人員頭痛樣本與當前 正在野外肆虐的惡意程式（如 REVil、加殼、反調試、dotNet、Shellcode 等）使學員能在一道道關卡做中學得能 在業界實戰的分析成就感，無論在分析系統漏洞或者惡意程式能成為獨當一面的即戰力。
課程摘要	◦ Function Basic: Import, Export, Bounds, Format, Refs, Stack Frames ◦ Data Structure: Integers, Array, Ansi, Unicode, Headers ◦ Type Libraries (Compiler SDKs) ◦ (Lab) Module Rebase：DLL-based 側錄型後門 ◦ (Lab) Patching：真實網軍濫用反編譯器問題的混淆樣本 ◦ 現代野外商用紅隊武器分析 (3 Lab） ◦ 在野樣本 Shellcode 分析 (3+ Lab） ◦ 惡意程式脫殼分析實戰 (2 Lab）
學員先修技能	具備基本 Windows 操作能力即可

學員自備工具	裝載 Vmware Workstation、Vmware Fusion 的 Intel 晶片電腦設備，課程預計最多提供 1 套 VM（ova），硬碟空間需求 70G 以上，記憶體至少 8G 以上（建議 16G 以上為佳)

➢ 課程三

課程名稱	**〈透過 AI 驅動的威脅獵捕技術: 從異常探索到 Sigma 規則生〉**
課程講師	黃智威（Jr-Wei Huang）
講師簡介	黃智威（@in0de_16）目前於 TXOne Networks Inc.資安威脅與產品防護中心擔任 Team Lead，負責產品偵測與威脅研究。研究領域涵蓋系統安全、惡意行為獵捕與惡意程式分析，並擁有企業資安產品研發的實務經驗。曾於 HITCON、No Hat、JSAC、CYBERSEC Taiwan 等資安會議擔任講者，分享系統安全、藍隊防禦實務與偵測工程等主題，亦曾在學校與企業擔任授課講師。
課程簡介	在實務企業藍隊進行威脅獵捕時最花時間的往往是在大量紀錄檔中探索可疑的痕跡，從雜亂的行程建立資訊、網路連線與系統事件中找出具備脈絡的證據鏈總是會使分析人員無從下手，然而，隨著 LLM 的發展迅速我們是否能透過機器學習的演算法幫助我們加快偵測獵捕的速度並藉由自動產生的規則讓企業能夠涵蓋到更完整的攻擊鏈。 本課程以機器學習快速篩選端點異常為起點，說明如何以輕量且具判斷力的特徵工程，將原始日誌轉換為可供模型使用的訊號，接著說明現今攻擊者常用

	的混淆技術，探討現階段對於混淆的內容有哪些偵測方法，最後我們將說明從偵測工程的角度該如何讓 LLM 生成出有效的 Sigma 規則並完善整體規則撰寫流程。課程適合企業 SOC 分析師、偵測工程師與威脅研究人員，學員將掌握全新的威脅獵捕方式，期望為企業提供更有效的偵測手法。
課程介紹	◦ Adversary Tactics & Attack Surface Exploration ◦ Practical Real-World Log Analysis (Hands-on Labs) ◦ Large-Scale Windows Log Hunting with ML ◦ Introduction to Anomaly detection ◦ Feature Engineering (Cmdline Tokenization, Parent–child Chain…) ◦ Introduction to event normalize and Model selection ◦ Using and Fine-Tuning Anomaly Detection Models (Hands-on Labs) ◦ Script Obfuscation Techniques (String Concatenation, Char Casting,...) ◦ Introduction to Script De-obfuscation Technique with AI/Non-AI ◦ Hunting Script Obfuscated Content (Hands-on Labs) ◦ From ML Anomalies and TTPs to Sigma YAML with LLMs ◦ False Alert Testing and Refinement ◦ LLM-Driven Sigma Generation (Hands-on Labs)
學員先修技能	具備基本 Windows 相關防禦知識

學員自備工具	VMware Workstation、VMware Fusion（Mac User 請使用非 M1/2 晶片之 Mac）

六、 參訓資格

(一)授課對象為各產業領域之在職資安人員，包含金融、軟體、智慧製造、資安、法人/學校/醫院、特定政府機關及其他綜合產業，屬高階技術實戰培訓。

(二)具中華民國國籍，並擁有資安領域 2 年以上實務經驗。

(三)以企業資安技術人員、資安公司研發人員及其他單位資安技術人員為主要對象，但不限於此範圍。

(四)每一企業(公司)限兩名人員報名。

七、 報名方式

(一)報名期限自即日起至 115 年 8 月 23 日（日）23 時 59 分，請至課程活動報名網站填寫資訊（https://hitcon.kktix.cc/events/elite-industry-course-tainan）。

(二)完成報名後將進行學員遴選，獲正取通知後始得參與課程。主辦單位保有是否錄取學員之權利，錄取結果另以電子郵件通知。

八、 注意事項

(一)課程期間提供午餐。

(二)本課程學員須全程參訓，禁止由他人冒名頂替參與課程。課程上下課時間以講師實際授課情形為準。

(三)如報名錄訓後因故無法參訓，請於開課日前 3 天通知主辦單位，以利安排遞補。

(四)為保障智慧財產與著作權，課程中禁止拍照、錄影及錄音。學員自本課程所取得之課程相關教材，未經主辦單位授權同意，不得任意重製、傳輸、散布等受著作權法規範之行為。

(五)為課程結案需要，課程中將進行拍照紀錄。

(六)課程期間如遇不可抗力因素（如：颱風、水災、地震、疫情等，依行政院人事行政總處或中央疫情指揮中心公告）導致課程停辦或延期，異動資訊以主辦單位公告為準。

(七)為確保參與者之學習品質及達到培訓目的，並避免浪費訓練資源，若出席總時數未達 20 小時，該名學員將於一年內喪失參與數位發展部資通安全署及國家資通安全研究院所有活動之權利。

九、 課程聯絡窗口

(一)數位發展部資通安全署 黃繼民專案分析師

電話：02-2380-8743

E-mail：jiminhuang@acs.gov.tw

(二)社團法人台灣駭客協會秘書處

電話：02-2700-0073

E-mail：info.elite@hitcon.org