AISHIELD 艾盾資科 X TRAPA

獨家共同開課！
由 Trapa 講師授課

醫療 CODE 網路攻防演練前置模擬教育訓練

攻防實戰學習環境的演練，提供一個類似企業面臨各種網路威脅的真實環境，讓資安人員於攻防演練過程，學習到正確的應對經驗，在演練過程中，會有專家從旁協助，於攻防演練完成後會深入檢討過程之應對技巧有哪些可以改善或做得更好。譬如在面對勒索軟體、進階持續性滲透威脅(APT) 攻擊或阻斷服務式 (DDoS) 攻擊，都需要透過實際情境訓練來提升資安人員之偵防能力，並研擬與實施不同情境下的防禦措施，目標為培育企業資安人員具備充裕的防禦作戰能力。

執行方式

01 透過 APT Group 為基礎的攻擊腳本來做模擬。

02 學員透過系統告警、防火牆等設備的警示紀錄，辨識警示的嚴重性及確認是否被入侵，藉由此過程來培養團隊資安處理的能力。

03 撰寫資安事件報告。

04 講師藉由執行不同的腳本，以不同的攻擊手法訓練學員成為全方位的防禦網路攻擊之人才。

👉 想參與課程？請與我們聯繫報名: contact@aishield.com.tw

科目	時數	預計安排時程
Crazy Hunter	12	11月上旬

課程規劃與大綱說明

課程說明	CrazyHunter 攻擊手法的網路攻擊劇本。攻擊者透過供應鏈攻擊或系統漏洞建立初始據點，使用 WebShell 和開源工具進行內網滲透。利用 AD 漏洞配合 NTLM Relay 取得域控制權後，橫向移動至核心服務系統。攻擊者使用 BYOVD 技術繞過防毒軟體，透過 Microsoft 雲端服務進行 C2 通訊，最終部署客製化勒索軟體加密關鍵系統，威脅公開研究資料以勒索贖金。
課程大綱	1. 真實攻擊事件流程 2. 偵查手段：水平滲透與實務操作 3. Active Directory CS 基礎攻防 4. BYOVD 攻擊手法
課程內容	1. 劇本分析：攻擊情境 2. 劇本分析：防禦情境 3. 事件偵測及遏止規劃 4. 行動要項探討 5. Crazy Hunter攻擊手法分析 6. 權限提升攻擊手法分析(BYOVD) 7. Active Directory CS 攻擊手法說明
Lab練習內容及工具	1. Prince-Ransomware 解密 2. Windows 後門查找與刪除

AISHIELD 艾盾資科

contact@aishield.com.tw

+ 886 - 2 - 25957000

台北市中正區信義路二段 129 號 2 樓