onward SECURITY 安華聯網科技

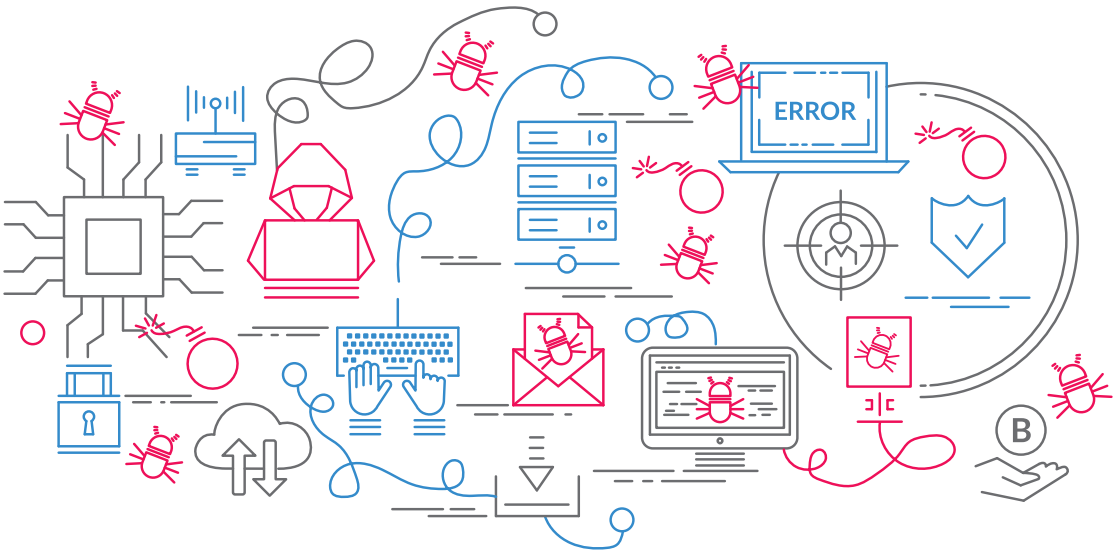
免費諮詢

紅隊演練

安華聯網提供的紅隊演練服務，不只著眼於單一系統的安全防護強度，並且強調企業邊界網路的防護廣度。以情境為導向的演練目標設定，由安華聯網擔任攻擊方(紅隊)的角色，整合情資蒐集、漏洞工具及駭客攻防等技術，驗證企業資安維運團隊(藍隊)對於網路攻擊的偵測與回應能力。

發掘駭客可能的攻擊途徑

- 參考MITRE ATT&CK框架，模擬駭客從網際網路對企業網路發動攻擊。
- 各個攻擊階段所採取的戰術與戰技，嘗試與蒐集到的情資結合，成功侵入對外伺服器。
- 嘗試在企業內部網路橫向移動，直至取得指定目標伺服器的控制權限。
- 將攻擊流程與手法可視化，把演練過程所發動的攻擊行為與現有防護設備的日誌紀錄進行比對，找出資安防護可持續精進的部分。



安華聯網優勢

- 安華聯網為國際組織CREST認可的服務供應商，其人員能力、執行流程及資料保護皆符合國際要求，提供專業且完整的服務。
- 安華聯網團隊成員共發現超過40個以上的零時差安全弱點(CVE)，並在 DerbyCon 及 Code Blue 等國際資安會議發表過資安研究，其漏洞挖掘能力與攻防技術具國際水準。
- 擁有多間金融與科技製造業客戶，執行紅隊演練實績，服務能力與經驗備受肯定。

我需要紅隊演練服務嗎？

已定期執行滲透測試且具備完整資安防護能力的企業，可透過紅隊演練找出在企業邊界網路可能存在的突破點，透過紅隊演練檢視現有資安防護設備與資安事件應變機制是否能如預期發揮作用。

滲透測試

- 是短期評估
- 使用一種攻擊方法
- 旨在識別和利用漏洞
- 企業員工知道要進行滲透測試
- 尋找漏洞是測試人員的核心任務
- 測試目標是事先確定的
- 各個系統獨立進行測試

紅隊演練

- 是長期的評估
- 使用廣泛的攻擊方法
- 旨在測試組織檢測和響應攻擊的能力
- 企業員工通常不知道發生了紅隊演練
- 尋找漏洞是測試人員實現目標的手段之一
- 測試目標不確定且覆蓋多個領域
- 各個系統同時進行測試

為何選擇安華聯網

深度資安檢測技術

- 已發現 40+ 全球首發安全弱點(CVE)
- 已發掘 3000+ 物聯網安全弱點

深耕物聯網產品安全

- 執行 150+ 物聯網產業相關資安專案
- 測試超過 700+ 連網產品安全

全球合規與認驗證能力

- 協助全球 10+ 國家與 300+ 客戶通過認驗證
- 具工控、金融、醫療、車載等產業合規經驗

安華聯網科技

contact@onwardsecurity.com

www.onwardsecurity.com

Website Facebook Linkedin Twitter Youtube