資安主題列表-恆逸教育訓練中心

項次	主題	上課對象	課綱
1	資安通識課程	一般人員	1. 近期資安趨勢與威脅 2. 社交工程與電子郵件安全 3. 社群媒體網站安全 4. 個人資料的安全 5. 勒索病毒最新攻擊手法與防範 6. 智慧型手機安全 7. 安全上網瀏覽的方法 8. 個人電腦保護方法
2	電子郵件社交工程宣導	一般人員	1. 電子郵件社交工程 2. 惡意的電子郵件 3. 電子郵件社交工程類型 4. 電子郵件社交工程之防護 5. 分辨電子郵件的真假
3	資訊安全防護宣導	一般人員	1. 資訊安全無所不在 2. 免費的最貴，網路詐騙無所不在 3. 防範注意老生常談，你都知道了嗎? 4. 人手一機時代下的危機 5. 駭客攻擊思維 6. 你所不知道的網路世界:「暗網」
4	深入淺出聊資安	一般人員	1. 近期資安新聞分享 2. 資訊安全的基本概念 3. 網際網路的安全性 4. 電子郵件的安全性 5. 個人資料的安全性 6. 提升資安意識
5	個資威脅應對之道	一般人員	1. 個人資料面面觀 2. 面對威脅的防護重點 3. 人手一機時代下的危機 4. 連網裝置的安全概觀 5. 常見弱點介紹與實作

資安主題列表-恆逸教育訓練中心

6	資訊安全最新探討	一般人員	1. 近期資安趨勢與威脅 2. 社群媒體網站安全 3. 個人資料安全性 4. 勒索病毒最新攻擊手法與防範 5. USB 病毒攻擊手法與防範 6. 智慧型手機安全 7. 安全上網瀏覽的方法 8. 個人電腦保護方法 9. 帳號密碼的安全設定 10. 密碼不安全其他原因 11. Q&A
7	社群網站駭客手法實務案例	一般人員	1. 社群網站駭客手法實務案例 2. 社群網站網路釣魚的防範 3. 新型態 LINE 社交工程手法 4. LINE 七大安全設定
8	新型態駭客手法-智慧型手機社交工程	一般人員	1. 新型態駭客社交工程手法 2. 智慧型手機安全防治宣導 3. 社群網站駭客手法實務案例 4. 智慧型手機社交工程手法 5. 智慧型手機安全防護 6. 智慧型手機安全重點項目 7. 實用手機 APP 教學
9	Big Data 資訊安全現況與新型態威脅因應		1. 新聞報導國內外駭客成功案例 2. 行動裝置資訊安全與資安防護 3. 雲端個資敏感資料外洩問題 4. 連網裝置資訊安全防範及案例解析

資安主題列表-恆逸教育訓練中心

10	新興科技發展下資訊安全防禦思維 (資訊安全現況及未來發展新型態駭客競賽)	一般人員	1. 資訊安全發展現況 甲、資訊科技發展趨勢 乙、資訊安全發展現況 2. 新興科技威脅趨勢 甲、資訊認知作戰 乙、關鍵基礎設施面臨之威脅 3. 資訊安全應有之防禦思維 甲、技術面 乙、管理面
11	人工智慧與網路安全 (駭客的「終極完美武器」：人工智能大未來)	一般人員	1. 人工智慧發展與應用 甲、人工智慧發展 乙、人工智慧應用場域 2. 人工智慧攻擊手法與案例分享 甲、駭客攻擊手法 乙、案例說明 3. 人工智慧時代應有之思考 甲、網路安全防禦 乙、人工智慧法律責任
12	雲端網路安全	一般人員	1. 雲端系統的運用現況 2. 雲端系統的優缺點 3. 雲端服務的資安攻擊案例 4. CVE 漏洞的修補探討 5. 木馬後門的異常偵測範例
13	個人資訊安全防護	一般人員	1. 電子郵件社交工程 2. 以案例方式，介紹何謂社交工程?並解說社交工程常見手法與防範方式, 與社交工程案例與測試演練。 3. 個人日常的網路安全 4. 介紹臉書與詐騙式購物的網站案例, 同時分析偽冒金融機構的網站案例。 5. 行動裝置的安全防護 6. 介紹常見的手機資安重點防護, 包括有:偽裝通知的惡意程式,竊取資訊的手機 APP,偽裝手機感染病毒網頁,LINE 的假新聞與假帳號 7. 持續性滲透攻擊(APT) 8. 簡介何謂 APT? 分析 APT 攻擊案例並宣導如何防範 APT 攻擊?

資安主題列表-恆逸教育訓練中心

			9. Q&A 結論
14	網路攻擊案例與資訊安全	一般人員	1. IoT 安全威脅與風險管理 2. 智慧手機安全防護 3. 勒索攻擊與資料備份 4. 遠距辦公與視訊安全 5. Q&A
15	預見未來-人工智慧對決駭客競賽	一般人員	1. AI 智能家電安全性 2. AI 智能住宅安全性 3. AI 車聯網安全性 4. AI 進行網路犯罪（以子之矛、攻子之盾） 5. AI 攻擊手法，插入噪音就能破壞語音辨識系統
16	駭客入侵實戰-網路探測	資訊人員	1. 網路探測 2. 資訊蒐集 3. 弱點掃描 4. NMAP 實務 5. 弱點利用 6. 密碼破解
17	撞庫攻擊與帳號保護	資訊人員	1. 常見社交工程攻擊方式 2. 憑證填充攻擊(撞庫攻擊)原理 3. 密碼潑撒攻擊原理 4. 撞庫攻擊探討與剖析 5. 撞庫攻擊的政策與防護(攻擊端) 6. 撞庫攻擊的政策與防護(使用者端) 7. 實際操作示範 8. 撞庫攻擊 FAQ 常見問答
18	加密勒索攻擊與檔案保護	一般人員 資訊人員	1. 勒索攻擊原理與認識 2. 加密勒索攻擊序列 3. 加密勒索案列與剖析 4. 資料檔案保護的策略 5. 加密勒索的暗網活動 6. 加密勒索攻擊的政策與防護

資安主題列表-恆逸教育訓練中心

19	密碼破解與設定安全的認知	一般人員 資訊人員	1. 帳號密碼的安全設定 2. 密碼的破解方式 3. 密碼不安全其他原因 4. 密碼事件的範例-SolarWinds 5. FBIG 密碼、Apple-ID 的外洩探討 6. 駭客猜測密碼的範例-Binary Tree 7. 資料庫儲存密碼的建議
20	數位鑑識概論	一般人員 資訊人員	1. 數位鑑識概念 甲、數位鑑識定義 乙、數位證據 2. 數位鑑識原則與程序 甲、數位鑑識原則 乙、數位鑑識程序 3. 數位鑑識實務 甲、數位鑑識實務案例 乙、數位鑑識技術運用
21	元宇宙發展概論（未來世界:元宇宙(萬物無網)	一般人員	1. 元宇宙概念 甲、何謂元宇宙 乙、元宇宙之運作 2. 元宇宙之技術與應用 甲、技術運用 乙、應用場域 3. 元宇宙之挑戰 甲、資訊安全 4. 法律規範
22	元宇宙與 NFT 安全簡介	一般人員 資訊人員	1. 元宇宙簡介 2. 元宇宙的資安風險 3. 元宇宙新的資安攻擊媒介與資安挑戰 4. NFT 簡介 5. NFT Ecosystem 生態系統的安全問題 6. NFT 的漏洞與安全問題 7. 常見的 NFT 騙局以及安全建議 8. 加密貨幣簡介 9. 加密貨幣的安全標準 10. 如何保護數位資產 11. 加密貨幣安全保護措施

資安主題列表-恆逸教育訓練中心

23	網路威脅與滲透測試	資訊人員	1. 近期資安新聞與駭客分類與事件 2. 滲透測試簡介 3. 資訊蒐集方法 4. 掃描工具介紹 5. 網路安全風險與標準介紹 6. 面對威脅的防護重點
24	滲透測試教學	資訊人員	1. 滲透測試簡介 2. 資訊蒐集 3. 弱點掃描 4. 弱點利用 5. 網頁安全 6. 報告撰寫
25	資通系統委外開發安全重點	資訊人員	一、SSDLC 程式開發安全 ➢ SSDLC 安全的系統開發生命周期實務操作 ➢ 資訊系統委外安全管理 ➢ 規格安全要求、實作安全要求、安全測試 二、資訊系統委外開發資安需求 ➢ 程式語言開發者重點事項 ➢ 密碼儲存系統重點事項 ➢ 案例分析 1: 美國 SolarWinds 資安事件 ➢ 案例分析 2: American Bank Systems 資安事件 三、結論與討論 ➢ 從攻擊者的觀點看資訊安全 ➢ 他山之石, 如何攻錯
26	系統與網站弱點掃描	資訊人員	1. 弱點定義與評估基準 2. 系統弱點掃描分析 3. OWASP TOP 10 比較 4. 網站弱點掃描分析 5. 如何強化系統與網站安全

資安主題列表-恆逸教育訓練中心

27	網路目標對象情蒐 情蒐與足跡偵查	資訊人員	1. 情蒐與足跡偵查 2. 資訊蒐集 3. Google hacking 4. GHDB 5. 相關工具、網站介紹 6. 什麼是暗網
28	網路服務探勘與資源介紹（實作）	資訊人員	1. 虛擬機基本操作介紹 2. 網路服務檢測工具資源介紹 3. TCP/IP、UDP 工作原理解析 4. 網路服務探測及識別手法 5. 網路弱點掃描分析 6. 網路安全防禦
29	從滲透測試看駭客攻擊	資訊人員	1. 駭客練兵場 2. 駭客攻擊思維 3. 弱點定義&評估基準 4. OWASP TOP 10 5. 網站弱點掃描工具 6. 利用 HTTP 通訊協定強化網站安全
30	駭客技術分析	資訊人員	1. 認識與了解資訊安全與道德駭客相關議題 2. 使用各種駭客手法檢測電腦系統、網路、網站、手機、無線網路、物聯網及雲端環境安全 3. 認識與檢測惡意程式 4. 透過社交工程攻擊評估組織人員安全意識
31	內部資安攻擊的實務案例與因應技巧	一般人員 資訊人員	1. APT, 內部攻擊與外部攻擊 2. 內部網路攻擊的異常徵兆 3. 檢視內部攻擊的基本技巧 4. 處理內部攻擊的因應步驟 5. 真實案例探討(將依時數討論案例數量) Case 1: 金融機構內部網路異常 Case 2: 貿易公司 Windows 系統異常 Case 3: 科技公司主機活動異常 Case 4: 醫療院所主機網路異常 Case 5: 教育大學內部網路異常 Case 6: 製造工廠主機網路異常 6. 結論與 QA

資安主題列表-恆逸教育訓練中心

32	惡意程式探討	資訊人員	1. 惡意行為攻擊趨勢 瞭解惡意程式的基本分類，並且觀察電腦程式的運作方式，藉此可以進一步了解惡意程式運作執行的時候，電腦呈現的症狀。 2. 惡意程式分析方法介紹 惡意程式的運作，隨著目標不同而有所改變。但是，在理想狀況下，惡意程式的組成架構，可以增加其攻擊破壞能力。 3. 惡意程式 案例探討 根據真實案例，討論惡意程式的運作，與其攻擊破壞能力。網路的攻擊與防衛，是一體兩面。越能瞭解惡意程式就越能防護電腦網路安全。 4. 惡意程式的行為分析 在虛擬機與沙箱環境，分析常見的惡意程式的執行過程，瞭解惡意程式本身的關鍵要素，與預防之道。 5. Downloader 與加密勒索 探討惡意程式，家族與加密勒索家族相關影響，並進一步瞭解其因應處理的步驟
33	資通安全法令遵循實務	一般人員 資訊人員	1. 資通安全現況 2. 資通安全事故案例研析 3. 資通安全法律規範 - 刑法妨害電腦使用罪章 4. 資通安全法律規範 - 個人資料保護法 5. 資通安全法律規範 - 資通安全管理法 6. 資通安全技術面應用 7. 資通安全管理面設計 8. 資通安全法令遵循執行策略與方法
34	SQL Server 資料庫安全實戰	資訊人員	1. SQL Server 安全總體架構簡介 2. SQL Server 維繫安全的工具 3. 應用程式存取資料庫

資安主題列表-恆逸教育訓練中心

			4. 服務帳戶之安全設定 5. 加密 SQL Server 的連線 6. 驗證模式 7. 授權的要項 8. 稽核(Audit) 9. 資料的加解密 10. 其他安全性相關設定 11. 應用程式安全性
35	Web 應用程式安全課程	資訊人員	●OWASP TOP10 2021 A01:2021 – 權限控制失效 (Broken Access Control)的弱點描述及防禦 A02:2021 – 加密機制失效 (Cryptographic Failures)的弱點描述及防禦 A03:2021 – 注入式(隱碼)(Injection)的弱點描述及防禦 A04:2021 – 不安全設計 (Insecure Design)的弱點描述及防禦 A05:2021 – 安全設定缺陷 (Security Misconfiguration)的弱點描述及防禦 A06:2021 – 易受攻擊和已淘汰的組件 (Vulnerable and Outdated Components)的弱點描述及防禦 A07:2021 – 認證及驗證機制失效 (Identification and Authentication Failures)的弱點描述及防禦 A08:2021 – 軟體及資料完整性失效 (Software and Data Integrity Failures)的弱點描述及防禦 A09:2021 – 資安記錄及監控失效 (Security Logging and Monitoring Failures)的弱點描述及防禦 A10:2021 – 伺服端請求偽造 (Server-Side Request Forgery ;SSRF)的弱點描述及防禦