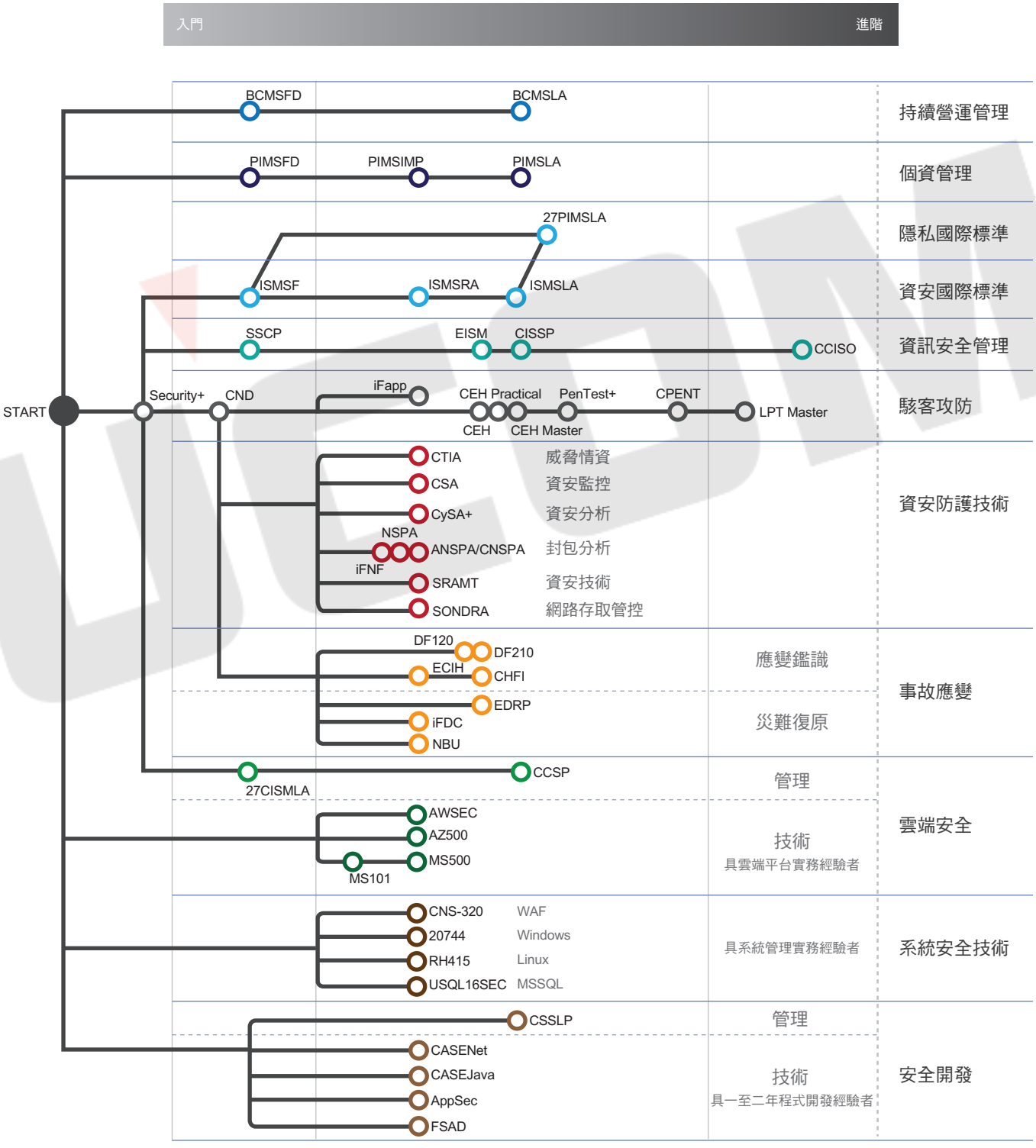
資訊安全專家 課程簡介

UCOM 資安 (ISC)² EC-Council Veritas CompTIA 國際標準 鑒真數位

資安課程 / 證照學習路線圖



資安課程學習全攻略

課程分類	難度	證照	代號	課程名稱	備註
資安入門	初階	CompTIA Security+	Secp	CompTIA Security+國際資訊安全專家認證課程	
資訊安全管理	初中階	SSCP	SSCP	SSCP資安專業人員認證課程	
	中高階	CISSP	CISSP	CISSP資安系統專家認證課程	
	高階	CCISO	CCISO	EC-Council CCISO資安長／EISM 資安經理人認證課程	
資安防護技術	初中階	CND	CND	EC-Council CND網路防禦專家認證課程	
	中階	CTIA	CTIA	EC-Council CTIA威脅情資分析專家認證課程	
	中階	CSA	CSA	EC-Council CSA安全運營中心(SOC)分析師認證課程	
	中階	CySA+	COMPA	CompTIA Cybersecurity Analyst(CySA+)網路資安分析師國際認證班	
	中階	NSPA	NSPA	網路安全封包分析認證課程	
	中階		ANSPA	網路安全封包分析進階實作	
	中階		CNSPA	網路安全封包分析案例探討	
	中階		iFNF	網路鑑識及惡意程式分析	
	中階		SRAMT	資訊安全分析實務-方法、流程與工具	
	中階		SONDRA	安全最佳化-網路設備與遠端存取	
	中階		SECTMK	結合資安技術與管理技巧確保個人資料與營業秘密安全	
	中階	CCP-N	CNS-320	Citrix ADC進階主題-安全、管理和最佳化	
系統安全	中階		20744	Windows Server 2016 資訊安全	
	中階	RHCA	RH415	RHCA認證-Red Hat實體、虛擬及雲端安全	
	中階		USQL16SEC	微軟SQL Server 2016資料庫安全實戰	
駭客攻防	中階		iFApp	智慧型手機APP資安分析	
	中階	CEH	CEH	EC-Council CEH駭客技術專家認證課程	
	中階	CEH Practical	CEHP	CEH大師雙認證實戰考試總複習班	實作考試
	中階	PenTest+	COMPT	CompTIA PenTest+滲透測試和漏洞管理國際認證班	
	中階	CEH Master	CEHM		僅證照、無課程， CEH+CEH Practical=CEH Master
	中高階	CPENT	CPENT	EC-Council CPENT 滲透測試專家認證課程	
	高階	LPT Master	LPT		僅證照、無課程
事故應變	中階	ECIH	ECIH	EC-Council ECIH資安危機處理員認證課程	
	中階		iFDC	資安事件損害控制暨資料復原實務	
	中階	EDRP	EDRP	EC-Council EDRP資安災害復原專家認證課程	
	中階		NBU	Veritas NetBackup資料保護專業人員認證課程	
	中階		DF120	Opentext-DF120 Encase國際專業鑑識認證課程	
	中高階	EnCE	DF210	Opentext-DF210 Encase國際專業鑑識認證課程	
	中高階	CHFI	CHFI	EC-Council CHFI資安鑑識調查專家認證課程	
安全開發	初階		FSAD	應用程式資安開發基礎課程	技術面
	中階	CASENet	CASENet	EC-Council CASE .NET應用程式安全工程師認證課程	技術面
	中階	CASEJava	CASEJava	EC-Council CASE Java應用程式安全工程師認證課程	技術面
	中階		AppSec	Mobile App Security資訊安全程式實作演練-通訊與資料儲存的安全	技術面
	中高階	CSSLP	CSSLP	CSSLP資安軟體開發專家認證課程	
雲端資安	中階	ISO27017 ISO27018	27CISMLA	雲服務資訊安全管理 (ISO/IEC 27017)與雲服務個人資料保護管理 (ISO/IEC 27018) 主導稽核員訓練課程	管理面
	中階	AWS Certified Security - Specialty	AWSEC	Security Engineering on AWS	技術面
	中階	Microsoft 365 Certified：Enterprise Administrator Expert	MS101	Microsoft 365行動力與安全性	技術面，需通過MS-100及MS-101 2科考試才可取得此認證
	中階	Microsoft 365 Certified：Security Administrator Associate	MS500	Microsoft 365安全管理	技術面
	中階	Microsoft Certified：Azure Security Engineer Associate	AZ500	Microsoft Azure安全性技術	技術面
	中高階	CCSP	CCSP	CCSP雲端資安專家認證	管理面
資安國際標準	初中階		ISMSF	ISO 27001：2013資訊安全管理系統初階訓練課程	
	中階		ISMSRA	ISO 27001：2013資訊安全管理系統風險評鑑課程	
	中高階	ISO27001	ISMSLA	ISO 27001：2013資訊安全管理系統主導稽核員訓練課程	
隱私國際標準	中高階	ISO27701	27PIMSLA	ISO/IEC 27701:2019隱私資訊管理系統主導稽核員訓練課程	ISMS延伸之隱私管理
個資管理	初中階		PIMSFD	個人資料管理系統基礎訓練課程	
	中階		PIMSIMP	個人資料管理系統建置實務課程	
	中高階	BS10012	PIMSLA	個人資料管理系統之稽核員／主導稽核員訓練課程	
持續營運管理	初中階		BCMSFD	營運持續管理系統基礎訓練課程	
	中高階	ISO22301	BCMSLA	營運持續管理系統稽核員／主導稽核員訓練課程	

SRAMT 資訊安全分析實務-方法、流程與工具

Information Security Implement-Methadology and Tools

時數：35小時 | 費用：28,000元 | 點數：7點 | 教材：恆逸專用教材

適合對象	1. 想要學習資安實用操作技巧的IT人員 2. 對系統的資安有興趣管理，希望能加強實作技巧的IT人員
預備知識	1. TCP/IP網路通訊協定 2. 已取得微軟Windows MCSA認證、紅帽RHCE認證之工程師，或具備網路基本架構概念者 3. 資訊安全基礎概念
課程內容	1. 評估系統的資訊安全 2. 評估流程與相關工具 3. 列舉與入侵系統的參考步驟 4. 駭客的矛盾對決 5. 探索與測試 6. 常見服務檢測：電子郵件伺服器 7. 常見服務檢測：網站伺服器 8. 常見服務檢測：搭配伺服器加密需求TLS 9. 跡證保存與警報系統 10. 備份與復原 11. 標準化建立系統與弱掃零檢出 12. 相關實作演練
後續推薦課程	CHFI：EC-Council CHFI資安鑑識調查專家認證課程

SECTMK 資通安全法令遵循實務

Cyber Security Law Compliance

時數：14小時 | 費用：20,000元 | 點數：5點 | 教材：恆逸專用教材

適合對象	法務人員、IT人員、資安人員、稽核人員
預備知識	具備基礎資安管理能力
課程內容	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
備註事項	課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT$16,000元
後續推薦課程	CEH：EC-Council CEH駭客技術專家認證課程

DCDSM 資料中心資訊安全管理實務演練課程

Data Center Design and Security Management Training Course

時數：16小時 | 費用：25,000元 | 點數：6.5點 | 教材：CQI/IRCA認證原廠授權教材

適合對象	1. IT部門或資料中心高階領導 2. 參與資料中心設計、規劃、建置、運行與管理人員 3. 資料中心服務提供者 4. IT專業人士
預備知識	1. 具備基礎英文閱讀能力 2. 具備一般電腦文書處理能力 3. 具備資訊技術或資訊安全經驗 4. 具備資料中心工作經驗者佳 5. 具備資訊服務或管理經驗
課程內容	1. 資料中心的分級 2. 資料中心安全需求簡介 3. 資料中心設計的要求介紹 4. 電腦/電信機房之設計規範介紹 5. 電信、自動化與機電控制系統、空調系統架構與要求 6. 資料中心檢測、驗證與認證要求
備註事項	白天班之上課時間為09:00~18:00；參加全程課程者授予「上課證明」
後續推薦課程	CEH：EC-Council CEH駭客技術專家認證課程

SONDRA 安全最佳化-網路設備與遠端存取

Security Optimization：Network Device and Remote Access

時數：21小時 | 費用：32,000元 | 點數：8點 | 教材：恆逸專用教材

適合對象	1. 想要學習網路安全實用技術的IT人員 2. 想要了解設備與遠端存取安全作業標準的資安管理員	3. 需要管理交換器、路由器、遠端桌面、遠端存取安全的IT人員
預備知識	1. 了解網路架構、並具備 Cisco IOS 基本操作能力 2. 孰悉 Windows 與 Linux 系統、網路基本管理	3. 網路安全基本概念
課程內容	1. 網路安全，縱深防禦(defense-in-depth) 2. 管理與實作二層交換器安全基準線 3. 運用與實作 802.1X 4. 管理與實作路由器安全基準線 5. 使用 Playbook 集中管理網路設備安全 6. 管理與實作 VPN Tunnel 安全	7. 管理與實作 Linux SSH Tunnel 安全 8. 管理與實作遠端桌面(RDP)安全 9. 使用遠端桌面閘道(RDS GATEWAY)，強化遠端桌面安全 10. 強化遠端管理(ssh)安全 11. 集中管理設備驗證、授權與稽核
後續推薦課程	SRAMT：資訊安全分析實務-方法、流程與工具	

獨家課程 網路安全封包分析認證

NSPA 網路安全封包分析認證課程

Network Security of Packet Analysis Course

時數：21小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

適合對象	1. 具備TCP/IP網路技術概念者 2. 企業網路之管理人員	3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	已完成以下課程所具備技術能力 NINS：網路基礎架構與網路服務	
課程內容	1. 網路封包分析的基本知識與常用技巧 2. 常見網路服務FTP、Telnet、SSH、SMTP、POP3、IMAP封包行為分析 3. 常見HTTP、HTTPS之正常與異常封包行為分析 4. 網路芳鄰(CIFS/SMB/NAS)之正常與異常封包行為分析	5. ODBC、MS-SQL、MySQL、PostgreSQL、Oracle資料庫之封包行為分析 6. 惡意程式(Malware)、跳板主機與駭客攻擊封包行為分析 7. 網路異常與駭客攻擊的案例分析
備註事項	1. 白天班之上課時間為09:30~17:30 2. 本課程結束後將頒發結業證書 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班 4. 本課程包含一次認證考試，考試時間將於課程第三天下午舉行筆試，考試時間60分鐘，題數33題。 證照寄發：7天知道考試結果，30天後收到中華民國網路封包分析協會(NTPA)寄發的電子證書。 通過標準：滿分100分，測驗及格分數70分即可通過考試，取得網路安全封包分析認證。 5. 課程優惠方案：早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT$19,200元	
後續推薦課程	ANSPA：網路安全封包分析進階實作	

ANSPA 網路安全封包分析進階實作

Network Security of Packet Analysis – Practice Course

時數：21小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

適合對象	1. NSPA Class C認證人員 2. 企業網路之管理人員	3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	TCP/IP網路通訊協定 資訊安全基礎概念 NSPA：網路安全封包分析認證(Class C) NINS：網路基礎架構與網路服務	
課程內容	1. 網路安全封包分析-常見木馬程式實例 包括有：網路資安基本檢測方式、判斷網路異常通訊方式、正常網路封包的分析(實作)、惡意程式攻擊實作與封包分析(Emotet, TrickBot, AgentTesla, HawkEye, QuasarRAT, NjRAT, RevengeRAT, NanoCore, Maria, Lucifer等等)、封包分析技巧的學習評量與討論(實作題5題、木馬程式部分) 2. 網路安全封包分析-常見加密勒索實例 包括有：加密勒索的運作與偵測、加密勒索的案例研析、加密勒索攻擊實作與封包分析(Loocipher, WannaCry, GandCrab, Maze, Sodinokibi, Daharma, Nemty, GlobleImposter)的分析、封包分析技巧的學習評量與討論(實作題5題、加密勒索部分) 3. 網路安全封包分析-常見IDS/IPS與手機封包實例 包括有、APT組織的探討與案例、駭客攻擊的策略與戰術、多重複合式攻擊的案例、IDS/IPS偵測規則與Wireshark的規則轉換、手機封包的分析方式、平板手機的封包分析實作(正常iPhone手機, 正常HTC手機, 正常三星手機, 正常 Asus 手機, 其他手機封包, :Android 惡意 APP 封包分析)、封包分析技巧的學習評量與討論(實作題2題、手機部分)	
備註事項	1. 白天班之上課時間為09:30~17:30 2. 參加全程課程者授予「上課證明」 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班 4. 課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT$19,200元	
後續推薦課程	CNSPA：網路安全封包分析案例探討	

CNSPA 網路安全封包分析案例探討

Network Security of Packet Analysis-Case Study

時數：21小時 | 費用：32,000元 | 點數：8點 | 教材：專用教材

CNSPA

適合對象	1. NSPA Class C 認證人員 2. 企業網路之管理人員 3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	1. TCP/IP網路通訊協定 2. 資訊安全基礎概念 3. NSPA：網路安全封包分析認證(Class C) 4. NINS：網路基礎架構與網路服務
課程內容	1. 網路安全封包分析-國際資安案例之Cobalt Strike Beacon案例 包括有：實際案例解說、Cobalt Strike 介紹、Beacon用途、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: Cobalt Strike Beacon部分) 2. 網路安全封包分析-國際資安案例之DoppelPaymer案例 包括有：實際案例解說(Hyndai-KIA, Foxconn, Compal, A123 Systems, Mitsubishi Polysilicon)、Doppel Paymer 介紹、Mimikatz用途、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: Doppel Paymer部分) 3. 網路安全封包分析-國際資安案例之GlobeImposter案例 包括有：實際案例解說(醫療院所)、GlobeImposter 介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題:GlobeImposter部分) 4. 網路安全封包分析-國際資安案例之 Solar Wind供應鏈案例 包括有： Solar Wind 介紹、軟體系統供應鏈案例分析、American Bank System案例分析、Solar Wind之惡意樣本程式、學習評量與討論 5. 網路安全封包分析-國際資安案例之WastedLocker, LockBit, MountLocker案例 包括有：實際案例解說(Garmin與其他受駭廠商)、WastedLocker 介紹、LockBit介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: LockBit, MountLocker部分) 6. 網路安全封包分析-國際資安案例之Insider Offensive 案例 包括有：實際案例解說(CPC、FEIB)、ARP Scan 介紹、C#-Powershell介紹、svchost介紹、SWIFT/Bitsran介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題2題: svchost部分，封包題2題: Bitsran部分)
備註事項	1. 白天班之上課時間為09:30~17:30 2. 參加全程課程者授予「上課證明」 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班 4. 課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價NT$25,600元
後續推薦課程	ANSPA：網路安全封包分析進階實作

2022新課

FSAD 應用程式資安開發基礎課程

Fundamentals of Secure Application Development

時數：21小時 | 費用：24,000元 | 點數：6點 | 教材：恆逸專用教材

FSAD

適合對象	1. 對網路安全有興趣者 2. 對應用程式安全性有興趣，希望能加強資安實作技巧的IT人員 3. 有志成為安全分析師、滲透測試人員、道德駭客或安全顧問等專業人員
預備知識	1. Windows及Linux作業系統基礎操作 2. 網路基礎概念 3. 程式設計基礎概念
課程內容	1. 使用SQL Map 進行SQL 資料隱碼攻擊(SQLi) 2. 跨網站指令碼(XSS) 3. 跨網站偽造要求(CSRF) 4. 伺服器側請求偽造(SSRF) 5. HTTP Session 攻擊與防護 6. 身份驗證繞過漏洞(Authentication Bypass Vulnerability) 7. 帳戶枚舉(Web App Enumeration) 8. 目錄瀏覽暴力攻擊(Directory Browsing/Brute forcing) 9. LFI與RFI 10. 任意文件上傳與下載(Arbitrary File Upload & Download) 11. 檔案篡改(File Tampering) 12. 安全配置錯誤(Security Misconfigurations) 13. 字典攻擊(Dictionary Attack) 14. 特權升級(Privilege Escalation) 15. 使用 Kali Linux 進行網路應用滲透測試(Penetration Testing) 16. 使用DirBuster滲透測試工具進行漏洞偵查 17. 使用Metasploit套件進行弱點測試 18. 使用Legion 及 Nmap網絡滲透工具 19. 使用Google Search查找出現過的漏洞、名單與密碼表等弱點資訊 20. 檢視exploit-db漏洞利用資料庫 21. 使用Nikto Web掃描工具進行全面性Web伺服器檢測
後續推薦課程	SRAMT：資訊安全分析實務-方法、流程與工具