數聯資安
Information Security Service Digital United

運用雲端數位靶場平台精實資安人員防護戰技經驗分享

產品發展暨顧問處

資深協理 恭俊偉 Kelvin

遠傳FET 遠傳電信關係企業

AGENDA 議程

01 資安威脅與人才缺口造成的風險

02 資安專業人才與技能發展

03 藍隊演訓實際執行經驗分享

01

資安威脅與人才缺口造成的風險

企業遭駭客組織攻擊頻傳

新聞

Okta支援案件管理系統遭駭客入侵，股價大跌11%

駭客利用Okta外洩憑證存取該公司的支援案件管理系統，取得Okta用戶之一的Cloudflare上傳給Okta的HAR檔案，再利用HAR檔含有的Okta令牌資訊入侵Cloudflare內部的Okta實例

文/ 陳曉莉 | 2023-10-23 發

新聞 iThome

LockBit宣稱駭入波音並竊走機密

使用勒索軟體LockBit的駭客組織宣稱利用不知名的零時差漏洞攻擊波音公司並取得內部資料，而波音在安全研究業者VX Underground揭發這起攻擊事件當下，還不確定內部系統是否遭駭

文/ 林妍溱 | 2023-10-31 發表

新聞 iThome

Rackspace證實遭勒索軟體攻擊

Rackspace宣稱勒索軟體災情僅波及該公司旗下代管Exchange業務，資安專家則認為駭客是利用I
ProxyNotShell系列漏洞對Rackspace發動攻擊

雲端服務業者Rackspace因2022年勒索軟體攻擊事故損失5百萬美元

世界新聞網 | 2.9k 人追蹤 ☆ 追蹤

yahoo! 新聞

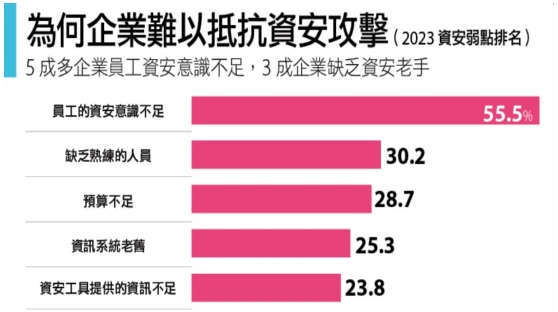
創辦人：Rackspace將從市場消失

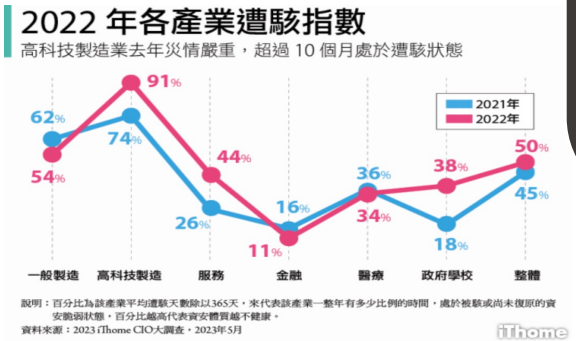
世界日報
2023年1月11日

聖安東尼奧快報報導，德州頗負盛名的雲端計算(cloud computing)科技公司Rackspace，創辦人之一的Richard Yoo(見圖，LinkedIn)本周向媒體表示，公司正在呈拋物線式的墜落，不久後會從市場上消失。

資料來源：IThome 資安新聞，Yahoo新聞

資安事件回應及處理面臨挑戰



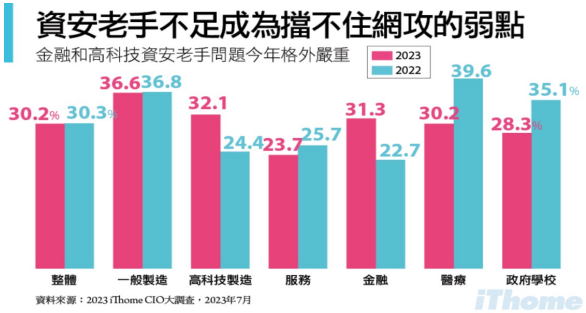


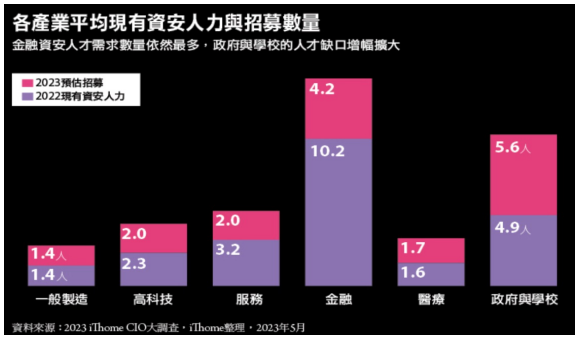
資安意識及應變能力不足

人才培訓需求

資安事件回應處理

資安人力不足

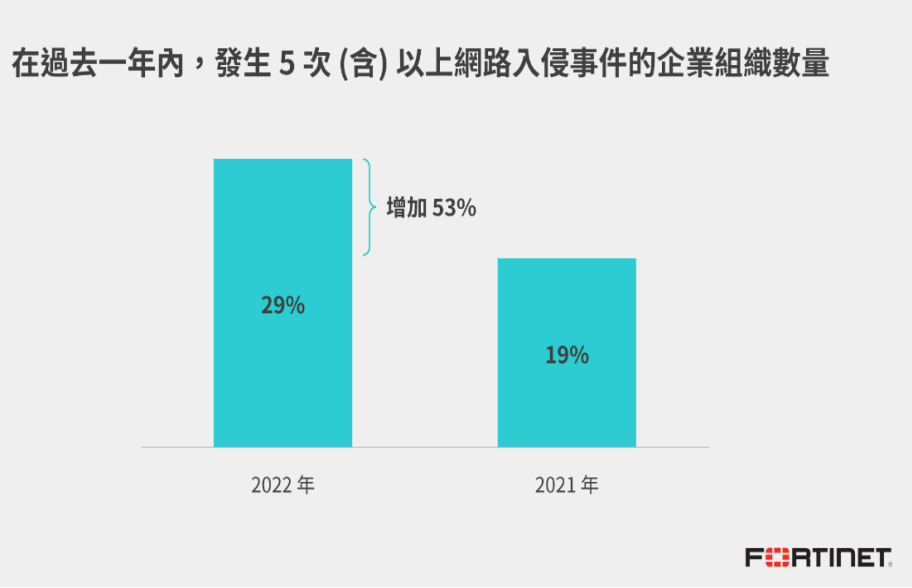


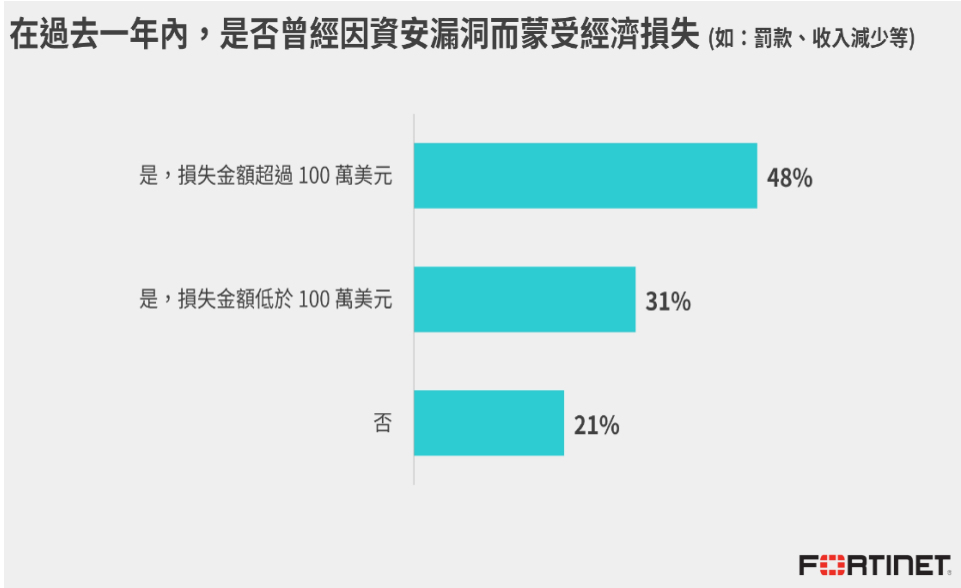


資料來源： www.ithome.com.tw/article/156839

資安人才缺口導致安全威脅加劇

Fortinet《2023年資安技能落差報告》揭露因資安技能落差及資安人才缺口，2022年遭到入侵5次以上的企業組織數量攀升超過五成（53%），近半數企業曾蒙受100萬美元以上經濟損失。





資料來源： Fortinet《2023年資安技能落差報告》

培養熟練的資安人員，平均需約3-5年

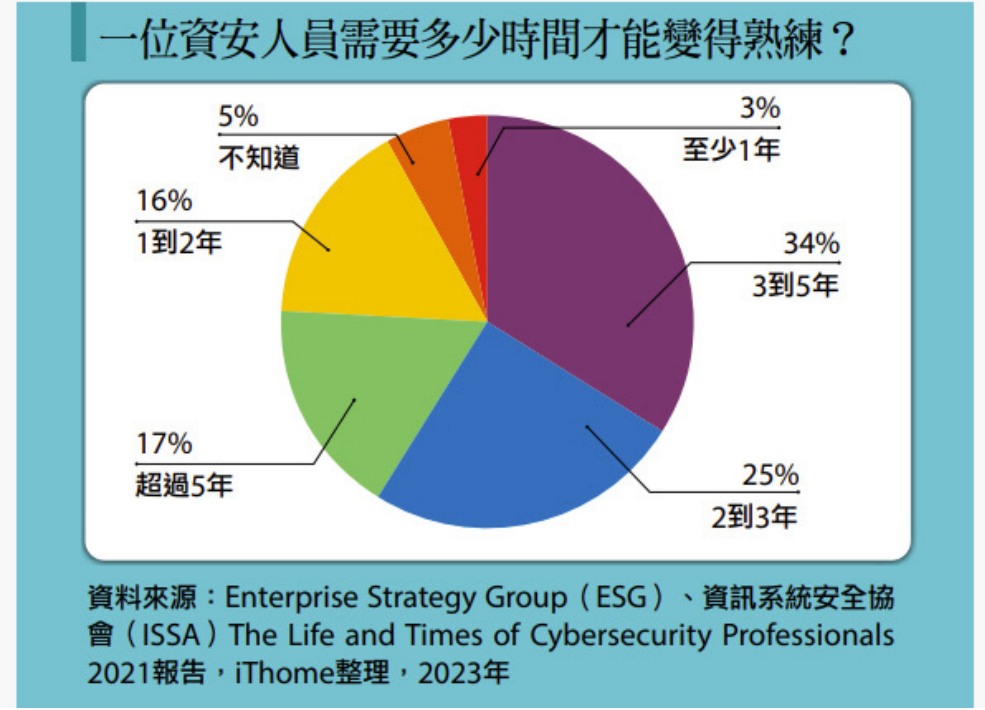
金管會在2021年底修法，明訂上市櫃公司於2023年底前完成設立資安長與資安專責單位。業界預估，在法令推動下，台灣整體產業將有**2萬名以上的資安人才缺口**。

面對資安人才缺口，企業的因應作法：

第一從既有的IT人才訓練成適合的人，速度較快，也可減低時間與成本。

第二跟學校的資訊相關系所或人才培育計畫合作，待學生畢業後，能與企業快速接軌。

第三是直接找資安公司，由於小企業本身的IT人力就不足，更不用說是資安人力。



資料來源：iThome , www.bnext.com.tw/article/67764/cybersecurity-talents-?

02

資安專業人才與技能發展

資安院 資安專業人才分類

新聞

開啟臺灣通用資安職能基準之路， 資安院人培中心積極展開行動

面對臺灣資安人才培育的重要課題，我國行政法人國家資通安全研究院已有推動方向，不僅聚焦基礎資安教育、中階在職培訓、進階專業培養，並將參考國際資安人才技能框架，應對國內普遍規模小且功能全面的資安團隊需求，建構我國資安職能基準，第一年先鎖定資安長與事件分析工程師

文/ 羅正漢 | 2023-06-04 發表

讚 214 分享

建構資安人才培育生態，資安院設四大目標

動機	以需求出發，從基礎、中階、進階、三方面，發展相應培訓量能與評量檢驗，建立我國完整資安人才培育生態			
目標	識別人才缺口（依類別）	打造資安人才職能框架	發展資安培訓綱要與課程	發展評量機制與鑑測指引
行動	● 執行國內人才供給與需求研究 ● 發展通用性資安人才類別	● 參考歐盟ENISA ECSF 12類人才框架，以美國NICE框架充實，發展完整職能參考基準	● 依ENISA ECSF人才框架發展課綱與指南供產官學參考 ● 規畫適合之課程讓公部門人員與產業人才利用	● 依照發展之綱要與課程建立評量制度
資安院預期成果與角色	● 成為長期觀測國內產業人才供需之機構	● 成為長期維護，以及更新國 內資安人才職能標準之機構	● 逐年完成12類角色課綱與指南 ● 四年培養超過400位進階資安人才	● 成為長期維護各類能力評量機制之專責機構

資料來源／國家資通安全研究院人才培力中心

我國資安人才類別框架建立，總共19類別 以ENISA ECSF列出的12類為主，並額外增加7類

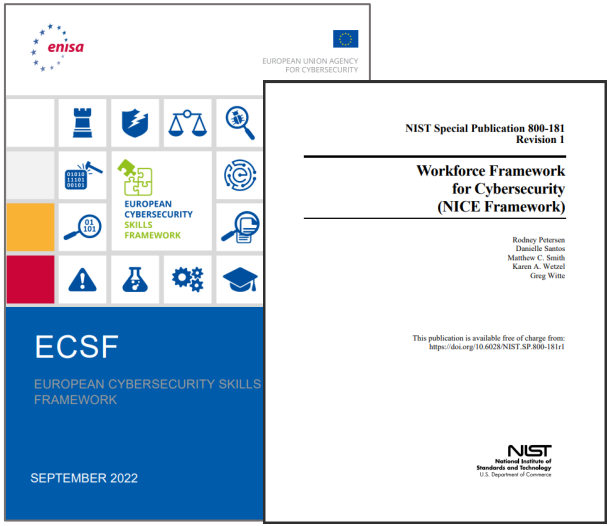
	資安人才類別	核心職能	對應ECSF框架的角色	對應NICE框架的類別
策略類	資安長（Chief Information Security Officer）	● 資安政策制定與規範 ● 資安治理架構與評估 ● 資安監督與管理 ● 資安資源配置	有	監管與治理
管理類	資安架構師（Security Architect）	● 系統安全架構 ● 網路安全架構	有	安全交付
	資安系統規畫師（Systems Requirement Planner）	● 系統安全架構 ● 網路與系統建置規劃	無對應類別	安全交付
	資安風險管理師（Cybersecurity Risk Manager）	● 資產安全等級分類 ● 風險分析與評估 ● 風險處理方式	有	安全交付
	資安法遵師（Cybersecurity Legal, Policy & Compliance Officer）	● 資安法規標準與識別 ● 個人資料保護法	有	監管與治理
	資安稽核師（Cybersecurity Auditor）	● 資安法規標準與識別	有	監管與治理
	資安教育員（Cybersecurity Educator）	● 資安認知宣導與推廣 ● 資安技術傳授與指導 ● 資安教材與資源應用	有	監管與治理
	資安顧問師（Cybersecurity Consultant）	● 網路安全/作業系統/資料庫管理與防護 ● 資安風險評鑑	無對應類別	監管與治理
	資安專案經理（Cybersecurity Project Manager）	● 資安管理制度規劃建置 ● 資安專案支援與管理	無對應類別	監管與治理
技術類	資安檢測工程師（Cybersecurity Tester）	● 系統建置與網路 ● 系統安全檢測	無對應類別	安全交付
	資安研究員（Cybersecurity Researcher）	● 惡意程式、漏洞與攻擊程式深度分析	有	安全交付
	資安產品開發工程師（Information Systems Security Developer）	● 資訊系統開發、程式撰寫	有※	安全交付
	資安系統維運員（Systems Administrator）	● 身分認證與存取控制 ● 日誌收容分析管理 ● 資料安全與備份*	無對應類別	營運與維護
	資安監控防禦工程師（Cyber Defense Analyst）	● 惡意程式防護 ● 網路/系統威脅與攻擊手法與對策 ● 入侵偵測與防禦	無對應類別	保護與防禦
	滲透測試工程師（Penetration Tester）	● 滲透測試與漏洞修補	有	保護與防禦
	資安事件工程師（Cyber Incident Responder）	● 資安事件通報 ● 資安事件分析與修復 ● 緊急應變與持續改善	有	保護與防禦
	漏洞分析工程師（Vulnerability Analyst, Exploitation Analyst）	● 產品與系統之威脅建模/風險評估 ● 反向工程	無對應類別	保護與防禦，分析
	威脅分析工程師（Threat Analyst）	● 威脅情報分析處理 ● 弱點異常深度分析	有	分析
	資安鑑識工程師（Cyber Defense Forensics Analyst）	● 數位鑑識蒐證	有	調查

資料來源：國家資通安全研究院，iThome整理，2023年8月　附註：對應為資安工程師（Cybersecurity Implementer）
註2:資安長為「產業資安」獨有職務；資安顧問師、資安專案經理、資安研究員、資安產品開發工程師是「資安產業」獨有職務。

資料來源：iThome (https://www.ithome.com.tw/news/156621)

資安人才類別框架

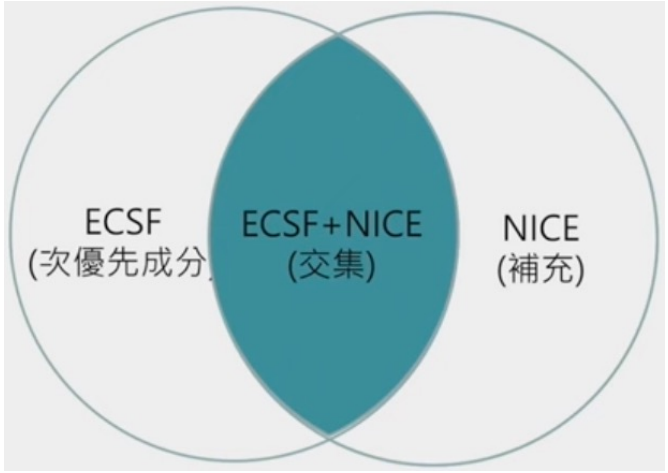
資安院參考歐盟ECSF及美國NICE，**從規劃、實施、運維、改進**的循環，再依據產業需求額外增加7類，讓編制更完整。

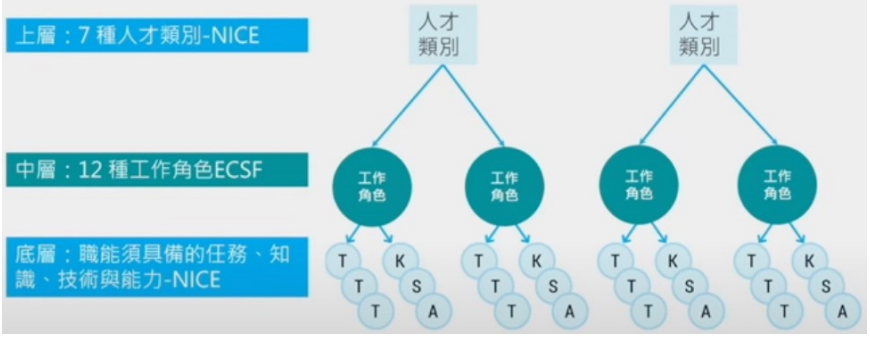


12 + 7

- 資安系統規畫師
- 資安顧問師
- 資安專案經理
- 資安檢測工程師
- 資安系統維運員
- 資安監控防禦工程師
- 漏洞分析工程師

整合NICE及ECSF雙邊知識元素





Work Role（工作角色）

Work Role Name	**Cyber Defense Incident Responder**
Work Role ID	**PR-CIR-001**
Specialty Area	**Incident Response (CIR)**
Category	**Protect and Defend (PR)**
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Abilities	A0121, A0128

Task（任務）

T0168	Perform hash comparison against established database.
T0169	Perform cybersecurity testing of developed applications a
T0170	Perform initial, forensically sound collection of images an mitigation/remediation on enterprise systems.
T0171	Perform integrated quality assurance testing for security f
T0172	Perform real-time forensic analysis (e.g., using Helix in c
T0173	Perform timeline analysis.
T0174	Perform needs analysis to determine opportunities for nev solutions.
T0175	Perform real-time cyber defense incident handling (e.g., f correlation and tracking, threat analysis, and direct systen deployable Incident Response Teams (IRTs).
	Perform secure programming and identify potential flaws

Knowledge（知識）

KSA ID	Description
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
K0171	Knowledge of hardware reverse engineering techniques.
K0172	Knowledge of middleware (e.g., enterprise service bus and message queuing).
K0174	Knowledge of networking protocols.
K0175	Knowledge of software reverse engineering techniques.
K0176	Knowledge of Extensible Markup Language (XML) schemas.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0178	Knowledge of secure software deployment methodologies, tools, and practices.

Skill（技能）

	Description
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).
S0072	Skill in using scientific rules and methods to solve problems.
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
S0074	Skill in physically disassembling PCs.
S0075	Skill in conducting forensic analyses in multiple operating system mobile device systems).
S0076	Skill in configuring and utilizing software-based computer protecti firewalls, antivirus software, anti-spyware).
S0077	Skill in securing network communications.
S0078	Skill in recognizing and categorizing types of vulnerabilities and as
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-ma external devices, spam filters).
S0080	Skill in performing damage assessments.
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g

Ability（能力）

A0120	Ability to share meaningful insights about the context environment that improve its risk management posture.
A0121	Ability to design incident response for cloud service models.
A0122	Ability to design capabilities to find solutions to less common and more complex system problems.
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
A0124	Ability to establish and maintain automated security control assessments
A0125	Ability to author a privacy disclosure statement based on current laws.
A0126	Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
A0127	Ability to deploy continuous monitoring technologies and tools.
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

資料來源：www.youtube.com/watch?v=7eUcgLCXhg0 , NIST SP800-181 NICE Framework

資安人才技能管理平台

知己 NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

知彼 MITRE ATT&CK™

應變 NIST Incident Response Lifecycle

基於業界標準的網路資安人才

追蹤及更新資安技能及知識基於通用的框架

(ISC)² Security+ CySA+

EC-Council

維持團隊CERTs的能力

在培訓時獲得 CPE 學分

從內建的課程來準備關鍵的認證

自動評估

追蹤團隊基於績效及客觀事實，而非主觀

衡量團隊

比較團隊績效與行業標桿

向董事會展示進度

資安人才技能管理平台

商業級實務演訓模擬
環境與演練情境

依據技術分項進行實機
訓練與測驗

對應MITRE ATT&CK
強化資安分析知識

參考NICE Framework
工作角色提供對應技能
課程

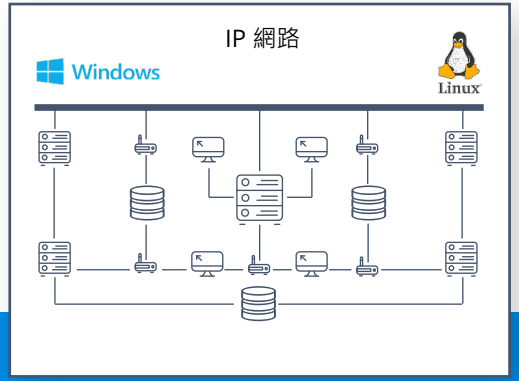
資訊及資安概論 / 基本作業能力 / 標準作業程序

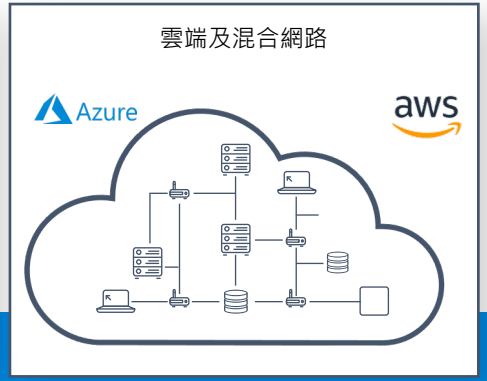
根據NIST 框架

確認資安事故回應能力的評估

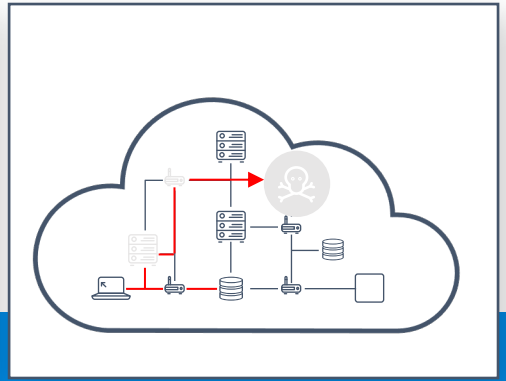
面對不同型態的攻擊預作準備

預先建置的企業等級網路
設計達成最大化的學習影響力





自動攻擊產生器
完整地模擬攻擊鏈



商業的資安工具

splunk> CROWDSTRIKE
paloalto NETWORKS CORTEX XSOAR
f5 Check Point SOFTWARE TECHNOLOGIES LTD
Carbon Black. McAfee
IBM QRadar ArcSight aws
kubernetes Azure docker

由培訓專家設計規劃的實戰演習

Ransomware **Log4J** Phishing investigation Splunk Log Analysis Dragonfly **SOC Analyst Course** **APTs** SSRF Attack
Web defacement TrickBot **Azure Attacks** Secure Development Course Data Exfiltration
Supply Chain Attack **Threat Hunting** with Crowdstrike **Threat Intelligence Course** Coin Mining Attack SSRF Simulation **Network Forensics** **SQL Injection**
AWS Attacks Keylogger DNS Hijacking CompTIA SEC+ Course Kubernetes **PowerShell investigation** Pentesting

03

藍隊演訓實際執行經驗分享

整個人才培育週期內提升技能

從選人到實戰進行準備

優化
招聘

- **50%** 減少錯誤僱用
- **25%** 更好的人才留任

加速
在職培訓

- **70%** 加速在職的適應期及基於角色定義的學習

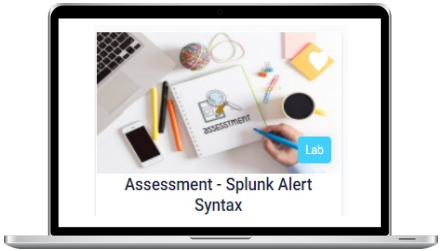
提高
個人技能

- **-30%** 平均修復及每個事件查找分析的時間花費

最大化
資安團隊能力

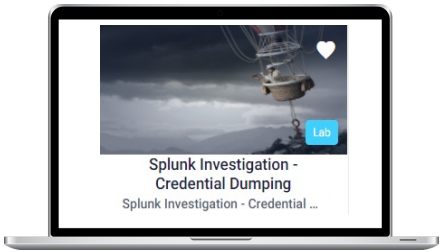
- 改善績效的可視性
- 人才加薪或晉昇的依據

人才篩選實驗室



在職培訓課程

個人技能實驗室



網路靶場實戰操練

實境演訓籌備

主題遴選

講師預習

前備知識彙整 / 課程說明製作

課程資訊發布

課程程序/注意事項

課前/課中說明

執行實境演訓活動

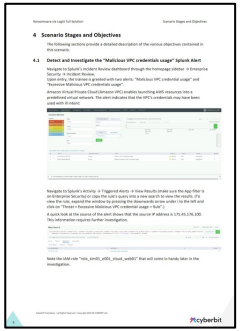
課後說明 / 討論

避免學員卡關

現場督課與協助 / Hint

重點是學習到情境劇本與應對方式

例：Log4j via Ransomware



Take away

人員演訓課程活動規劃

當月份聚焦一項主題情境

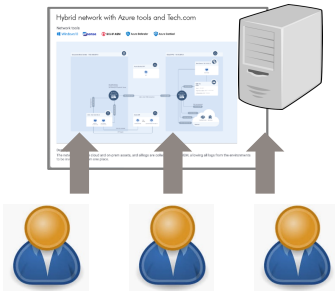
學習活動 | 學習活動 | 學習活動

Exercise #1 | Exercise #2 | Exercise #3

2023/01 | 2023/02 | 2023/03

共同解題

學習活動

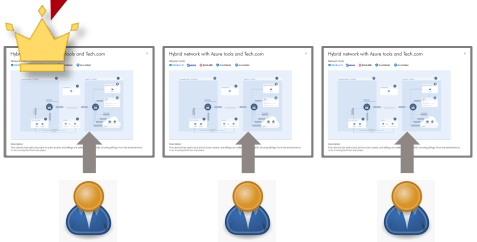


組別1 | 組別2 | 組別3

Winner Award

個人解題

競賽活動



個人1 | 個人2 | 個人3

Competition

競賽月

學習活動 | 學習活動 | 競賽活動 | 學習活動 | 學習活動 | 競賽活動 | 學習活動 | 學習活動 | 競賽活動

Exercise #4 | Exercise #5 | 實境演訓 #6 | Exercise #7 | Exercise #8 | 實境演訓 #9 | Exercise #10 | Exercise #11 | 實境演訓 #12

2023/04 | 2023/05 | 2023/06 | 2023/07 | 2023/08 | 2023/09 | 2023/10 | 2023/11 | 2023/12

搭配主題知識與LAB訓練課程

Spotlight 主題知識

- Introduction to Splunk Enterprise Security
- Basic Searching in Splunk
- Splunk - Rules and Alerts
- Splunk - Advanced Searching
- Splunk - Reporting and Dashboards
- Windows Users and Groups
- Windows CMD Network Commands
- DLLs in Windows
- Windows Filesystem
- Windows Event Log
- Introduction to Linux
- Linux Basic Commands
- Linux File System
- Linux Log Files
- Introduction to SIEM
- False Positives in SIEM
- Secure Shell Protocol (SSH)
- Cisco ASAv Firewall - Overview
- Introduction to Firewalls
- Common Attack Types - Introduction to Password Cracking

相關課程

Lab 實際操作

- Windows Event Log & Sysmon
- Splunk - Investigating Security Events
- Splunk - Web Traffic Analysis
- Working with Linux Commands
- Getting to know the Linux Log Files
- Cisco ASAv Firewall - Build Access Rules
- Cisco ASAv Firewall - Modify Access Rules
- Cisco ASAv Firewall - Device Setup and Management
- Basics of Brute Force

Exercise 實境演訓

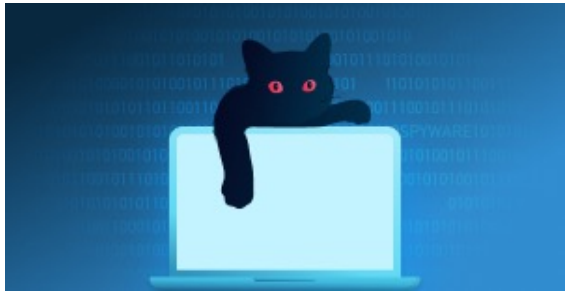
Ex. Log4j via Ransomware

Windows
Mcafee
kiwi
paloalto
splunk
zenoss
cortex

Linux
Apache
Log Analysis
SIEM
SSH
Firewall
brute-force

課程有關關鍵字、工具

實境演訓說明 Advanced Persistent Threat



概觀說明：
模擬資訊系統遭駭客使用APT攻擊手法入侵，參演單位可透過本情境學習如何確認受感染的端末、防止感染擴散、調查入侵與感染路徑、修補潛在的弱點、或強化伺服器的防護措施。

- 7個單元
- 12小時
- 3個Lab
- 4個Life

推薦角色：

- Security Analyst Level / Tier 2 、Tier 3
- Cyber Defense Analyst
- Cyber Defense Incident Responder

技能需求：

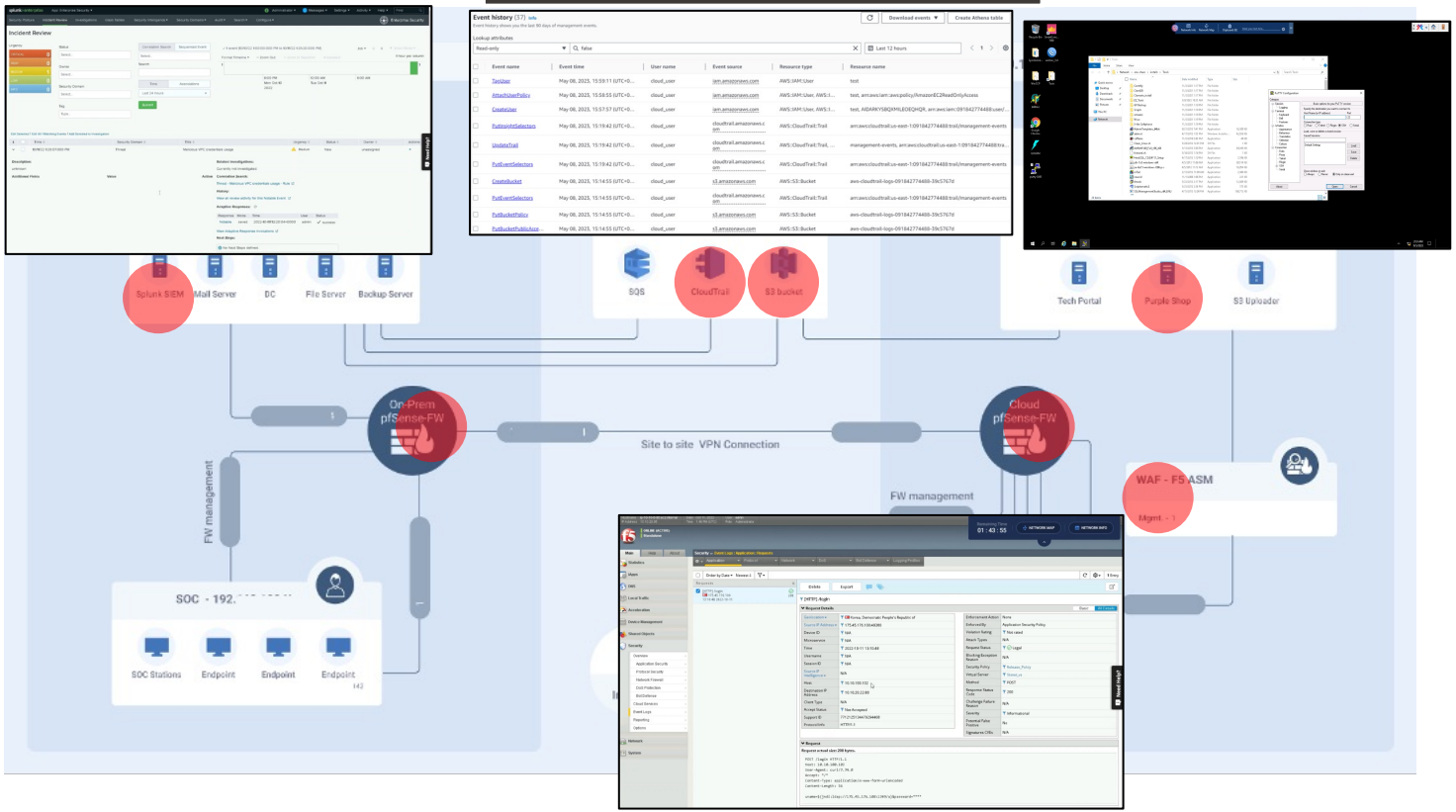
- 熟悉 Windows 日誌管理
- 熟悉 PowerShell 功能和命令
- 具有安全資訊和事件管理 （SIEM） 工作經驗
- 使用防火牆的經驗
- 熟悉 Windows 活動目錄

學習目標：

- 了解如何偵測和防止Ticket和類似的 Kerberos 攻擊
- 練習 Windows 日誌記錄研究和基本取證
- 練習先進的橫向移動調查技術
- 獲得資料外洩事件的實務經驗
- 獲得 Active Directory 結構和取證的實務經驗
- 獲得應對鍵盤記錄器威脅的實務經驗
- 獲得網域控制器 (DC) 管理工具的實務經驗
- 獲得 IIS 管理工具的實務經驗

實境演訓 – Log4j via Ransomware - Team1

Team-1 完成時間：1h:45m



Windows 10

pfsense

splunk>

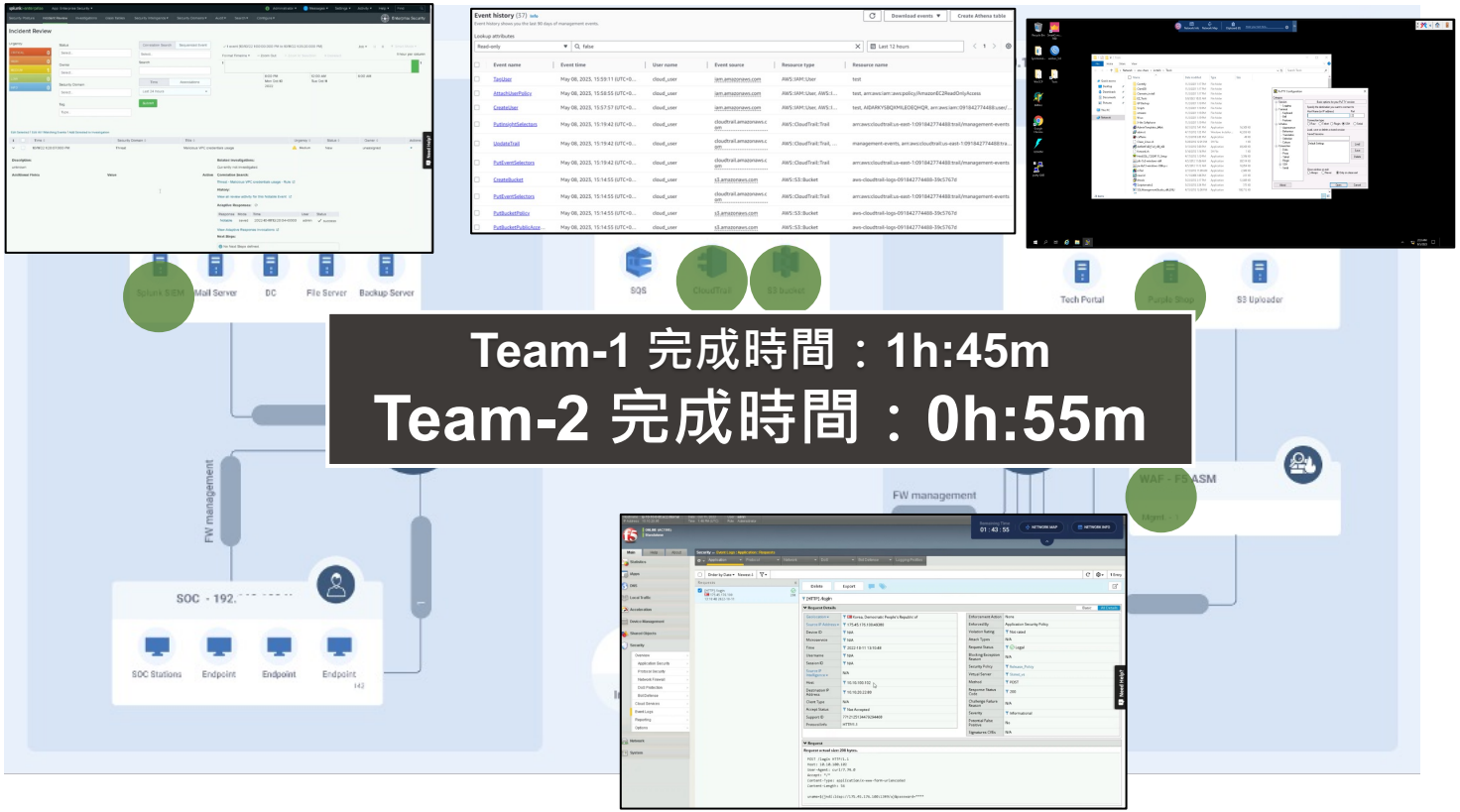
amazon SQS

amazon S3

amazon CloudTrail

BIG-IP ASM

實境演訓 – Log4j via Ransomware – Team2



Windows 10

pfsense

splunk>

amazon SQS

amazon S3

amazon CloudTrail

BIG-IP ASM

實境演訓分析講評

目標取證：
✓通過防火牆日誌查找埠掃描
✓在SIEM中發現相關服務被停止
✓在網路中找到攻擊服務的主機
✓找到已感染主機下載的惡意pdf檔
✓檢測到伺服器首頁被替換
　❑發現惡意檔案的源頭
　❑檢測到伺服器首頁index.html被修改
✓檢測到串改伺服器首頁的外部地址

分析並處理攻擊：
✓重啟SIEM的服務
✓清理受感染的主機
✓將攻擊者IP列入黑名單
✓恢復伺服器的主頁

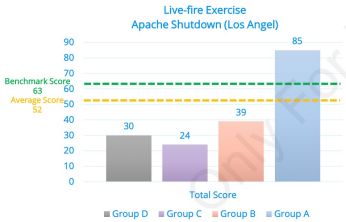
預防以後再受此類攻擊
✓阻止外網訪問伺服器的SSH埠
✓更改被洩露的密碼
✓不允許使用遠端工具的憑證緩存功能
✓將SIEM的重要服務進行監控

SIEM關閉攻擊取證步驟

1. 設置攻擊者「外網」位址，199.203.100.69
2. 對企業的邊界路由器發起SSH暴力攻擊，成功得到登錄憑證 → 6 打開防火牆日誌，查找攻擊者IP的記錄，發現很多ssh到路由器的記錄。
3. 準備shell反彈木馬檔，嵌入Vayyata使用者協議說明pdf中，替換路由器主頁index.html → 5 登錄Vyatta系統，發現主頁被替換
4. 使用者User055打開邊界路由器主頁，由於缺乏安全意識，保存並運行了惡意的說明pdf → 2 登錄SIEM伺服器，發現近期有192.168.100.10登錄，進而需要在Win7-CNT1上進行取證，發現異常PDF檔，得到攻擊者IP 199.203.100.69。
5. 反彈到Shell中並獲得許可權，遍歷機器中安裝的軟體，找到WinSCP並且得到SIEM的存儲的登錄憑證。 → 4 Win7-CNT1得到Plink, VyattaLicenseAgreement.pdf，cmd相關
6. 通過WinSCP中Putty程式，SSH到SIEM伺服器，關閉Qradar中關鍵的hostcontext服務，導致SIEM功能失效 → 1 經過講師提醒或者SOC日常工作，發現SIEM平台異常，不能正常工作。此處開始取證調查。
7. 在用戶機器上執行伺服器端多次的埠掃描，掩蓋或者迷惑安全人員。 → 3 重啟SIEM服務，可以看到很多Win7-CNT1到伺服器段的埠掃碼事件。

Live-fire Exercise 實戰演練結果

種類	參與人員	平均分數	基準
團隊演練(Apache Shutdown)	4 個團隊	52	63



Live-Fire Exercise 講師評論

- Los Angeles (Apache Shutdown)實戰演練

種類	參與人員	平均分數	基準
團隊演練(Apache Shutdown)	4 個團隊	52	63

- 講師評論
  - **團隊表現－四個團隊**
    - 團隊A，超過平均分數和基準分數，離滿分僅有15分差距；
    - 團隊B/C/D，未達到平均分數；
  - NIST IR**流程階段表現**
    - **偵測與分析**（60%）
      - 團隊A/B/C有進行本階段任務，但團隊D未進行本階段任務；
      - 團隊B/C在本階段得分較低，需要在實做知識/技能等方面加強；
    - **回應**（30%）
      - 團隊A/D有進行本階段任務，但團隊B/C未進行本階段任務；
      - 團隊D在本階段有較高得分，但是在第一個偵測與分析階段未完成任何任務，需要在IR流程上加強；此外團隊D完成本階段實做后，由於刪除了惡意Payload,破壞了環境，已無法在進行準確的攻擊溯源；
  - **預防**（10%）
    - 團隊B/D有進行本階段任務，但團隊A/C未進行本階段任務；
    - 所有團隊在預防階段表現一般，可能與未完成完整的偵測與分析和回應階段有關；
    - 需要提高偵測與分析和回應階段的效率，要通過提高知識/技能等實現。

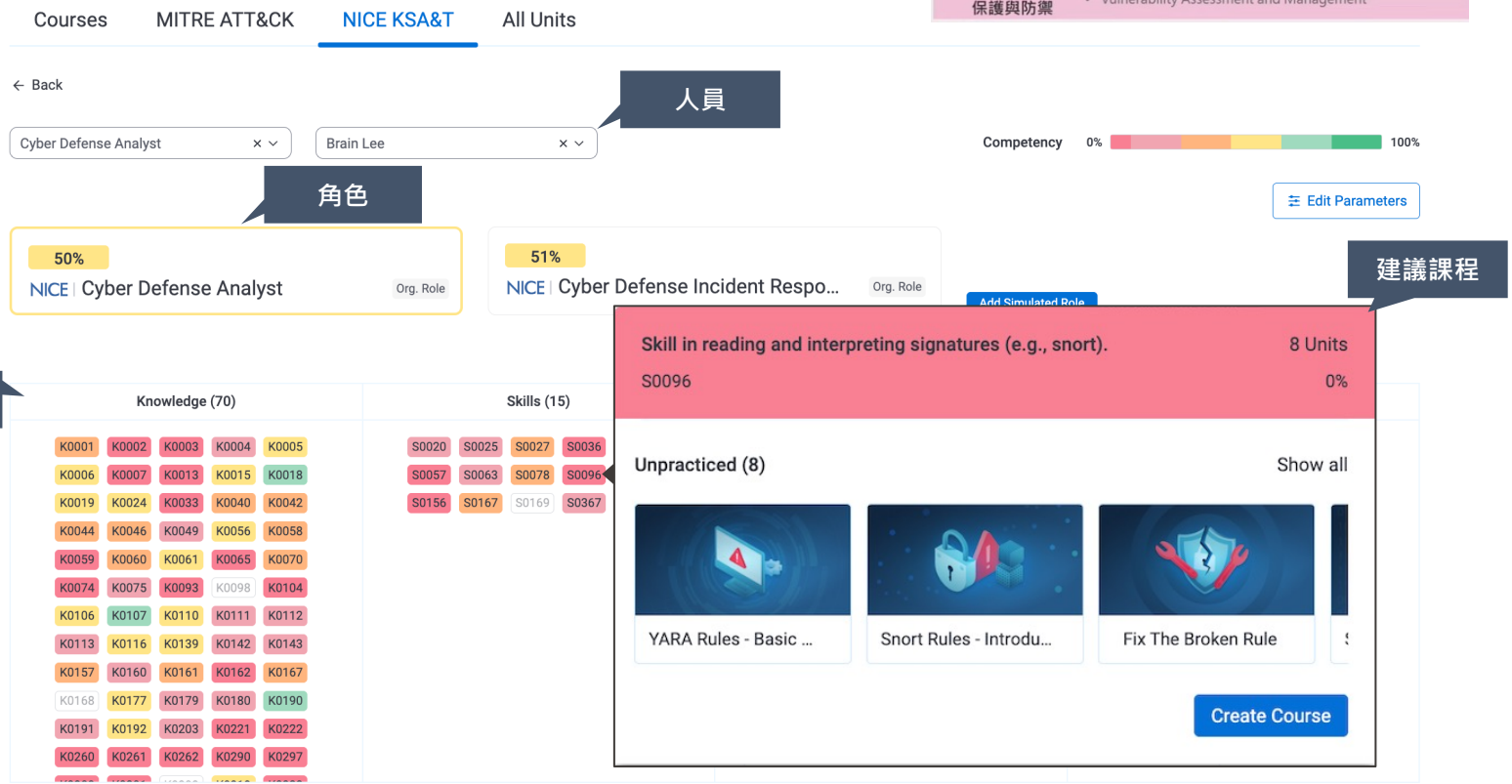
實境演訓後續精進建議

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Protect & Defend 保護與防禦

辨識、分析、減緩內部資訊系統與網路威脅

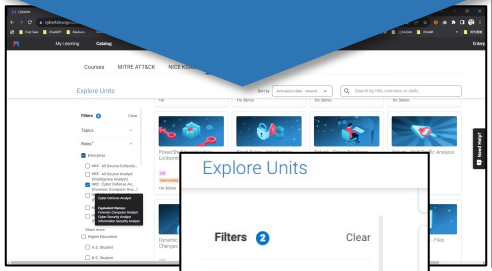
- Cyber Defense Analysis
- Cyber Defense Infrastructure Support
- Incident Response
- Vulnerability Assessment and Management

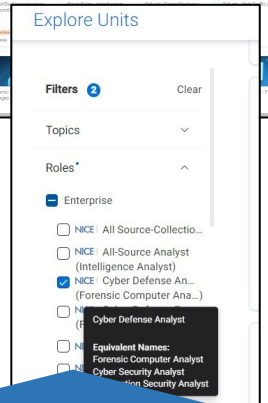


Based on NIST NICE Framework

實境演訓活動剪影

技術知識、Lab實作課程及商業實務模擬演訓





對應NICE工作角色篩選對應課程項目

技術知識學習

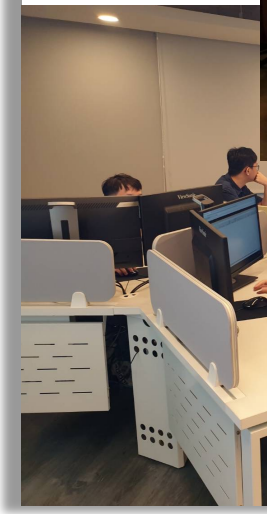
Lab 實機技術學習

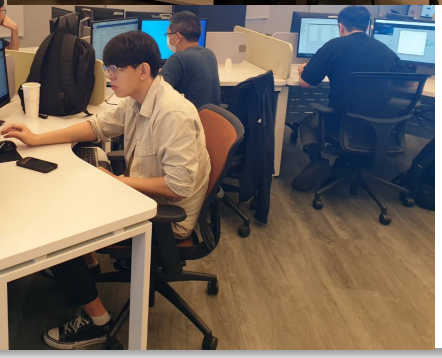
實機團體演練

團體演練成果分析

支援及參與各項資安攻防演練活動競賽

參與金融研訓院攻防演練活動，運用數位靶場教學平台協助教學及演練活動





支援教育部先進資通安全人才培育計畫，以數位靶場教學平台辦理資安防護解題解題教學與競賽活動

參與演訓活動學員回饋意見

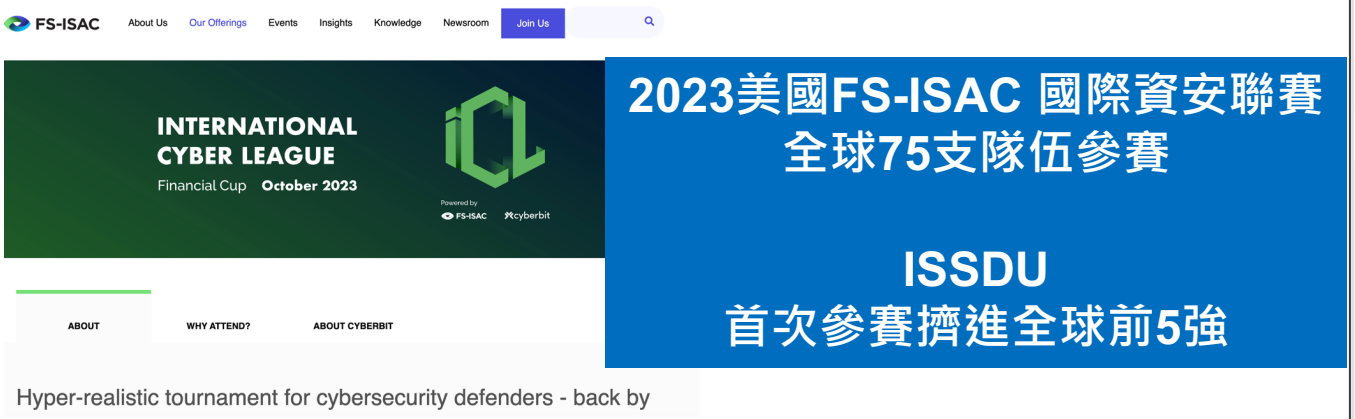
- 了解**攻擊手法與過程**
- 對於事件發生時**問題查找的方向**及觀念
- 學習到事件發生時，**事件追蹤與處理**
- 實用多元及很有**臨場感**
- 模擬**實戰演練**，加速經驗累積
- 面對資安異況，**學會研判方向**
- 由攻防演練學習到**如何分析資安事件**
- 透過實務了解**如何查找線索**
- 對於資安**事件調查**有進一步的了解
- 可在**安全的環境學習**如何處理惡意程式和資安鑑識
- ……

- ✓ 體驗擬真攻擊
- ✓ 學習查找方向
- ✓ 累積實戰經驗

經驗分享結語

公司內部全年實施成效

- ✓ 訓練超過 **70** 位以上的藍隊成員
- ✓ 演練超過 **15** 種實際攻擊場景
- ✓ 各類角色技能學習時數超過 **10,000** 小時
- ✓ 平均縮短約 **30%** 事件查找及分析的時間
- ✓ 各演練帳號使用活躍度的超過 **80%** 以上



2023美國FS-ISAC 國際資安聯賽
全球75支隊伍參賽

ISSDU
首次參賽擠進全球前5強

THANK YOU

感 謝 您 的 聆 聽

www.issdu.com.tw

數聯資安

Information Security Service Digital United