

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



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檔案含有的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/ 林妍濤 | 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

W 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。

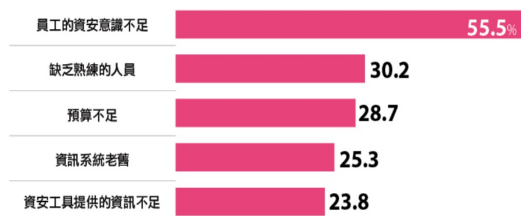


資安事件回應及處理面臨挑戰



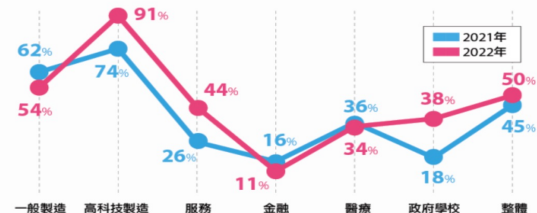
為何企業難以抵抗資安攻擊 (2023 資安弱點排名)

5 成多企業員工資安意識不足，3 成企業缺乏資安老手



2022 年各產業遭駭指數

高科技製造業去年災情嚴重，超過 10 個月處於遭駭狀態



說明：百分比為該產業平均遭駭天數除以365天，來代表該產業一整年有多少比例的時間處於被駭或尚未復原的資安脆弱狀態，百分比越高代表資安體質越不健康。

資料來源：2023 iThome CIO大調查，2023年5月



資安意識及
應變能力不足

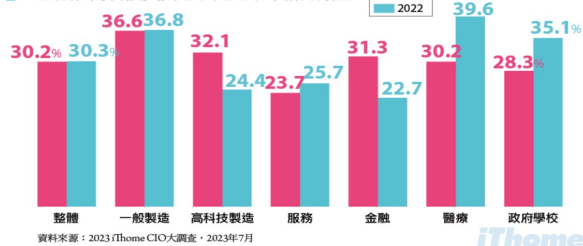
人才培訓需求

資安事件
回應處理

資安人力不足

資安老手不足成為擋不住網攻的弱點

金融和高科技資安老手問題今年格外嚴重

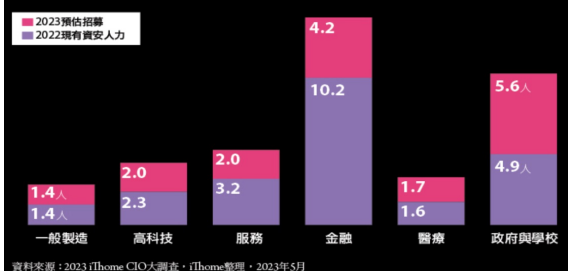


資料來源：2023 iThome CIO大調查，2023年7月



各產業平均現有資安人力與招募數量

金融資安人才需求數量依然最多，政府與學校的人才缺口增幅擴大



資料來源：2023 iThome CIO大調查，iThome整理，2023年5月

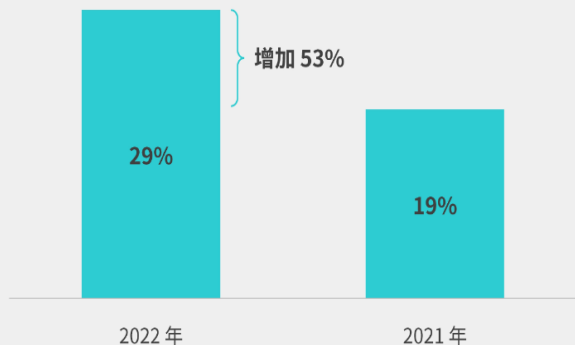
資料來源：www.ithome.com.tw/article/156839

資安人才缺口導致安全威脅加劇



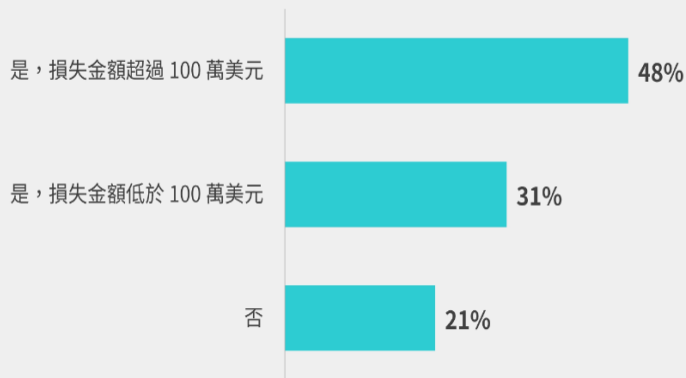
Fortinet《2023年資安技能落差報告》揭露因資安技能落差及資安人才缺口，2022年遭到入侵5次以上的企業組織數量攀升超過五成（53%），近半數企業曾蒙受100萬美元以上經濟損失。

在過去一年內，發生 5 次 (含) 以上網路入侵事件的企業組織數量



FORTINET

在過去一年內，是否曾經因資安漏洞而蒙受經濟損失 (如：罰款、收入減少等)



FORTINET

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**。

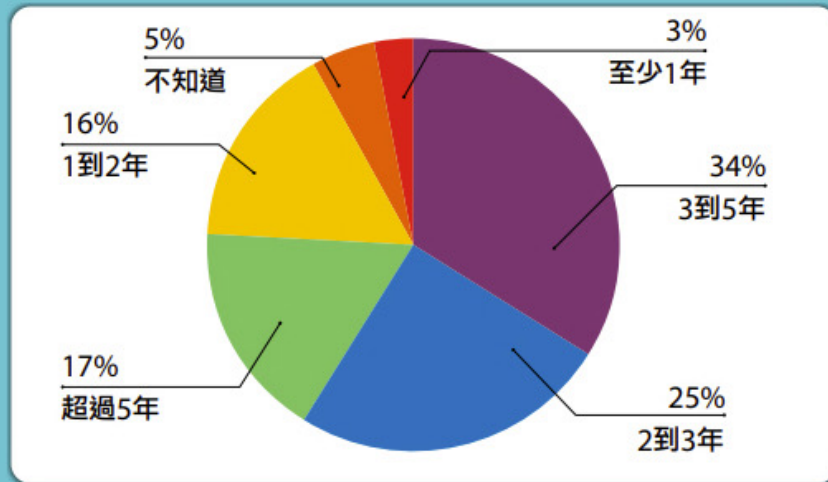
面對資安人才缺口，企業的因應作法：

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。

一位資安人員需要多少時間才能變得熟練？



資料來源：Enterprise Strategy Group (ESG)、資訊系統安全協會 (ISSA) The Life and Times of Cybersecurity Professionals 2021報告，iThome整理，2023年

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



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
策劃類	資安長 (Chief Information Security Officer)	<ul style="list-style-type: none"> 制定資安政策 資安治理架構與評估 資安監督與管理 資安資源配置 	有	監督與治理
	資安架構師 (Security Architect)	<ul style="list-style-type: none"> 系統安全架構 網路安全架構 	有	安全交付
	資安系統規劃師 (Systems Requirement Planner)	<ul style="list-style-type: none"> 系統安全架構 網路與系統建置規劃 	相對應類別	安全交付
管理類	資安風險管理師 (Cybersecurity Risk Manager)	<ul style="list-style-type: none"> 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
	資安法規師 (Cybersecurity Legal Policy & Compliance Officer)	<ul style="list-style-type: none"> 資安法規標準與課別 個人資料保護法 	有	監督與治理
	資安稽核師 (Cybersecurity Auditor)	<ul style="list-style-type: none"> 資安法規標準與課別 	有	監督與治理
教育類	資安教育員 (Cybersecurity Educator)	<ul style="list-style-type: none"> 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	監督與治理
	資安顧問師 (Cybersecurity Consultant)	<ul style="list-style-type: none"> 網路安全/作業系統/資料庫管理與防護 資安風險評鑑 	相對應類別	監督與治理
	資安專案經理 (Cybersecurity Project Manager)	<ul style="list-style-type: none"> 資安管理制度規劃建置 資安專案支援與管理 	相對應類別	監督與治理
技術類	資安檢測工程師 (Cybersecurity Tester)	<ul style="list-style-type: none"> 系統建置與網路 系統安全檢測 	相對應類別	安全交付
	資安研究員 (Cybersecurity Researcher)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 資訊系統開發、程式撰寫 	有※	安全交付
	資安系統維護員 (Systems Administrator)	<ul style="list-style-type: none"> 身分認證與存取控制 惡意程式分析與阻斷 網路安全與備份 	相對應類別	維護與維護
	資安網路防禦工程師 (Cyber Defense Analyst)	<ul style="list-style-type: none"> 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 	相對應類別	保護與防禦
	滲透測試工程師 (Penetration Tester)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 資安事件偵察 資安事件分析與修補 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)	<ul style="list-style-type: none"> 產品與系統之威脅建模、風險評估 逆向工程 	相對應類別	保護與防禦、分析
	威脅分析工程師 (Threat Analyst)	<ul style="list-style-type: none"> 威脅情報分析處理 弱點異常深層分析 	有	分析
	資安鑑識工程師 (Cyber Defense Forensics Analyst)	<ul style="list-style-type: none"> 數位鑑識蒐證 		調查

資料來源：國防資通安全中心研究，iThome報導，2023年9月。備註：對應資安工程師 (Cybersecurity Engineer) 註：資安法規、資產管理、資訊系統、資安顧問、資安專案經理、資安研究員、資安產品開發工程師、資安專案、隱私專職。

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

資安人才類別框架

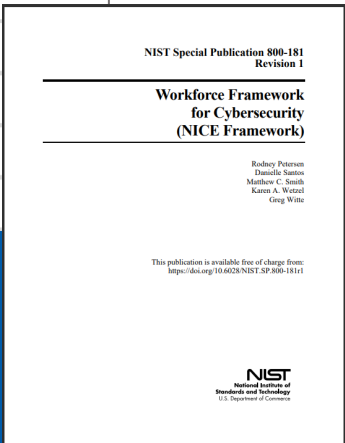
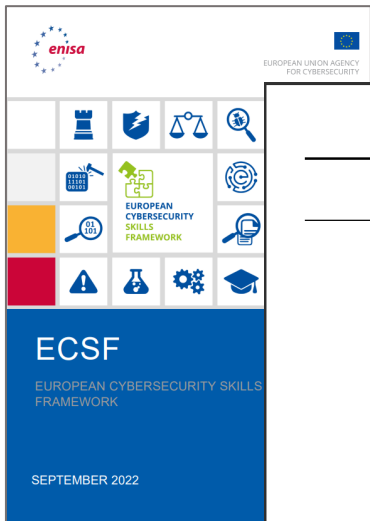


資安院參考歐盟ECSF及美國NICE，從規劃、實施、運維、改進的循環，再依據產業需求額外增加7類，讓編制更完整。

12

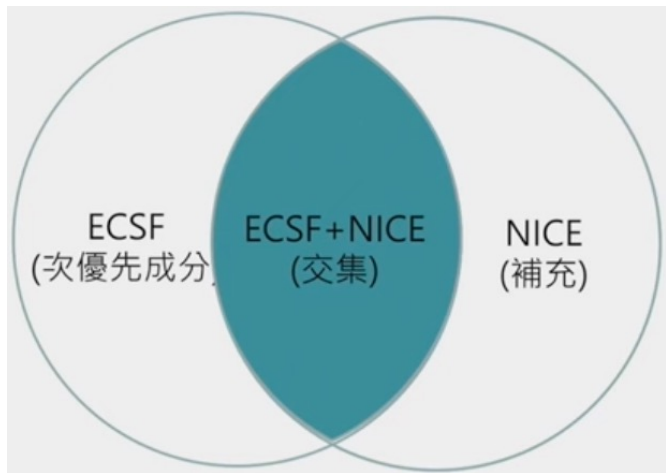
+

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)	Task ID	Description	Knowledge (知識)	KSA ID
	T0168	Perform hash comparison against established database.		
	T0169	Perform cybersecurity testing of developed applications and services.		
	T0170	Perform initial, forensically sound collection of images and data for analysis and mitigation/remediation on enterprise systems.		
	T0171	Perform integrated quality assurance testing for security fixes on enterprise systems.		
	T0172	Perform real-time forensic analysis (e.g., using Helix in cloud environments).		
	T0173	Perform timeline analysis.		
	T0174	Perform needs analysis to determine opportunities for new solutions.		
	T0175	Perform real-time cyber defense incident handling (e.g., forensics, correlation and tracking, threat analysis, and direct system response) for deployable Incident Response Teams (IRTs).		
	T0176	Perform secure programming and identify potential flaws in code.		
	T0177	Perform vulnerability analysis.		
	T0178	Perform vulnerability scanning.		
	T0179	Perform vulnerability testing.		
	T0180	Perform vulnerability validation.		
	T0181	Perform vulnerability verification.		
	T0182	Perform vulnerability reporting.		
	T0183	Perform vulnerability remediation.		
	T0184	Perform vulnerability assessment.		
	T0185	Perform vulnerability management.		
	T0186	Perform vulnerability scanning.		
	T0187	Perform vulnerability testing.		
	T0188	Perform vulnerability validation.		
	T0189	Perform vulnerability verification.		
	T0190	Perform vulnerability reporting.		
	T0191	Perform vulnerability remediation.		
	T0192	Perform vulnerability assessment.		
	T0193	Perform vulnerability management.		
	T0194	Perform vulnerability scanning.		
	T0195	Perform vulnerability testing.		
	T0196	Perform vulnerability validation.		
	T0197	Perform vulnerability verification.		
	T0198	Perform vulnerability reporting.		
	T0199	Perform vulnerability remediation.		
	T0200	Perform vulnerability assessment.		
	T0201	Perform vulnerability management.		
	T0202	Perform vulnerability scanning.		
	T0203	Perform vulnerability testing.		
	T0204	Perform vulnerability validation.		
	T0205	Perform vulnerability verification.		
	T0206	Perform vulnerability reporting.		
	T0207	Perform vulnerability remediation.		
	T0208	Perform vulnerability assessment.		
	T0209	Perform vulnerability management.		
	T0210	Perform vulnerability scanning.		
	T0211	Perform vulnerability testing.		
	T0212	Perform vulnerability validation.		
	T0213	Perform vulnerability verification.		
	T0214	Perform vulnerability reporting.		
	T0215	Perform vulnerability remediation.		
	T0216	Perform vulnerability assessment.		
	T0217	Perform vulnerability management.		
	T0218	Perform vulnerability scanning.		
	T0219	Perform vulnerability testing.		
	T0220	Perform vulnerability validation.		
	T0221	Perform vulnerability verification.		
	T0222	Perform vulnerability reporting.		
	T0223	Perform vulnerability remediation.		
	T0224	Perform vulnerability assessment.		
	T0225	Perform vulnerability management.		
	T0226	Perform vulnerability scanning.		
	T0227	Perform vulnerability testing.		
	T0228	Perform vulnerability validation.		
	T0229	Perform vulnerability verification.		
	T0230	Perform vulnerability reporting.		
	T0231	Perform vulnerability remediation.		
	T0232	Perform vulnerability assessment.		
	T0233	Perform vulnerability management.		
	T0234	Perform vulnerability scanning.		
	T0235	Perform vulnerability testing.		
	T0236	Perform vulnerability validation.		
	T0237	Perform vulnerability verification.		
	T0238	Perform vulnerability reporting.		
	T0239	Perform vulnerability remediation.		
	T0240	Perform vulnerability assessment.		
	T0241	Perform vulnerability management.		
	T0242	Perform vulnerability scanning.		
	T0243	Perform vulnerability testing.		
	T0244	Perform vulnerability validation.		
	T0245	Perform vulnerability verification.		
	T0246	Perform vulnerability reporting.		
	T0247	Perform vulnerability remediation.		
	T0248	Perform vulnerability assessment.		
	T0249	Perform vulnerability management.		
	T0250	Perform vulnerability scanning.		
	T0251	Perform vulnerability testing.		
	T0252	Perform vulnerability validation.		
	T0253	Perform vulnerability verification.		
	T0254	Perform vulnerability reporting.		
	T0255	Perform vulnerability remediation.		
	T0256	Perform vulnerability assessment.		
	T0257	Perform vulnerability management.		
	T0258	Perform vulnerability scanning.		
	T0259	Perform vulnerability testing.		
	T0260	Perform vulnerability validation.		
	T0261	Perform vulnerability verification.		
	T0262	Perform vulnerability reporting.		
	T0263	Perform vulnerability remediation.		
	T0264	Perform vulnerability assessment.		
	T0265	Perform vulnerability management.		
	T0266	Perform vulnerability scanning.		
	T0267	Perform vulnerability testing.		
	T0268	Perform vulnerability validation.		
	T0269	Perform vulnerability verification.		
	T0270	Perform vulnerability reporting.		
	T0271	Perform vulnerability remediation.		
	T0272	Perform vulnerability assessment.		
	T0273	Perform vulnerability management.		
	T0274	Perform vulnerability scanning.		
	T0275	Perform vulnerability testing.		
	T0276	Perform vulnerability validation.		
	T0277	Perform vulnerability verification.		
	T0278	Perform vulnerability reporting.		
	T0279	Perform vulnerability remediation.		
	T0280	Perform vulnerability assessment.		
	T0281	Perform vulnerability management.		
	T0282	Perform vulnerability scanning.		
	T0283	Perform vulnerability testing.		
	T0284	Perform vulnerability validation.		
	T0285	Perform vulnerability verification.		
	T0286	Perform vulnerability reporting.		
	T0287	Perform vulnerability remediation.		
	T0288	Perform vulnerability assessment.		
	T0289	Perform vulnerability management.		
	T0290	Perform vulnerability scanning.		
	T0291	Perform vulnerability testing.		
	T0292	Perform vulnerability validation.		
	T0293	Perform vulnerability verification.		
	T0294	Perform vulnerability reporting.		
	T0295	Perform vulnerability remediation.		
	T0296	Perform vulnerability assessment.		
	T0297	Perform vulnerability management.		
	T0298	Perform vulnerability scanning.		
	T0299	Perform vulnerability testing.		
	T0300	Perform vulnerability validation.		
	T0301	Perform vulnerability verification.		
	T0302	Perform vulnerability reporting.		
	T0303	Perform vulnerability remediation.		
	T0304	Perform vulnerability assessment.		
	T0305	Perform vulnerability management.		
	T0306	Perform vulnerability scanning.		
	T0307	Perform vulnerability testing.		
	T0308	Perform vulnerability validation.		
	T0309	Perform vulnerability verification.		
	T0310	Perform vulnerability reporting.		
	T0311	Perform vulnerability remediation.		
	T0312	Perform vulnerability assessment.		
	T0313	Perform vulnerability management.		
	T0314	Perform vulnerability scanning.		
	T0315	Perform vulnerability testing.		
	T0316	Perform vulnerability validation.		
	T0317	Perform vulnerability verification.		
	T0318	Perform vulnerability reporting.		
	T0319	Perform vulnerability remediation.		
	T0320	Perform vulnerability assessment.		
	T0321	Perform vulnerability management.		
	T0322	Perform vulnerability scanning.		
	T0323	Perform vulnerability testing.		
	T0324	Perform vulnerability validation.		
	T0325	Perform vulnerability verification.		
	T0326	Perform vulnerability reporting.		
	T0327	Perform vulnerability remediation.		
	T0328	Perform vulnerability assessment.		
	T0329	Perform vulnerability management.		
	T0330	Perform vulnerability scanning.		
	T0331	Perform vulnerability testing.		
	T0332	Perform vulnerability validation.		
	T0333	Perform vulnerability verification.		
	T0334	Perform vulnerability reporting.		
	T0335	Perform vulnerability remediation.		
	T0336	Perform vulnerability assessment.		
	T0337	Perform vulnerability management.		
	T0338	Perform vulnerability scanning.		
	T0339	Perform vulnerability testing.		
	T0340	Perform vulnerability validation.		
	T0341	Perform vulnerability verification.		
	T0342	Perform vulnerability reporting.		
	T0343	Perform vulnerability remediation.		
	T0344	Perform vulnerability assessment.		
	T0345	Perform vulnerability management.		
	T0346	Perform vulnerability scanning.		
	T0347	Perform vulnerability testing.		
	T0348	Perform vulnerability validation.		
	T0349	Perform vulnerability verification.		
	T0350	Perform vulnerability reporting.		
	T0351	Perform vulnerability remediation.		
	T0352	Perform vulnerability assessment.		
	T0353	Perform vulnerability management.		
	T0354	Perform vulnerability scanning.		
	T0355	Perform vulnerability testing.		
	T0356	Perform vulnerability validation.		
	T0357	Perform vulnerability verification.		
	T0358	Perform vulnerability reporting.		
	T0359	Perform vulnerability remediation.		
	T0360	Perform vulnerability assessment.		
	T0361	Perform vulnerability management.		
	T0362	Perform vulnerability scanning.		
	T0363	Perform vulnerability testing.		
	T0364	Perform vulnerability validation.		
	T0365	Perform vulnerability verification.		
	T0366	Perform vulnerability reporting.		
	T0367	Perform vulnerability remediation.		
	T0368	Perform vulnerability assessment.		
	T0369	Perform vulnerability management.		
	T0370	Perform vulnerability scanning.		
	T0371	Perform vulnerability testing.		
	T0372	Perform vulnerability validation.		
	T0373	Perform vulnerability verification.		
	T0374	Perform vulnerability reporting.		
	T0375	Perform vulnerability remediation.		
	T0376	Perform vulnerability assessment.		
	T0377	Perform vulnerability management.		
	T0378	Perform vulnerability scanning.		
	T0379	Perform vulnerability testing.		
	T0380	Perform vulnerability validation.		
	T0381	Perform vulnerability verification.		
	T0382	Perform vulnerability reporting.		
	T0383	Perform vulnerability remediation.		
	T0384	Perform vulnerability assessment.		
	T0385	Perform vulnerability management.		
	T0386	Perform vulnerability scanning.		
	T0387	Perform vulnerability testing.		
	T0388	Perform vulnerability validation.		
	T0389	Perform vulnerability verification.		
	T0390	Perform vulnerability reporting.		
	T0391	Perform vulnerability remediation.		
	T0392	Perform vulnerability assessment.		
	T0393	Perform vulnerability management.		
	T0394	Perform vulnerability scanning.		
	T0395	Perform vulnerability testing.		
	T0396	Perform vulnerability validation.		
	T0397	Perform vulnerability verification.		
	T0398	Perform vulnerability reporting.		
	T0399	Perform vulnerability remediation.		
	T0400	Perform vulnerability assessment.		
	T0401	Perform vulnerability management.		
	T0402	Perform vulnerability scanning.		
	T0403	Perform vulnerability testing.		
	T0404	Perform vulnerability validation.		
	T0405	Perform vulnerability verification.		
	T0406	Perform vulnerability reporting.		
	T0407	Perform vulnerability remediation.		
	T0408	Perform vulnerability assessment.		
	T0409	Perform vulnerability management.		
	T0410	Perform vulnerability scanning.		
	T0411	Perform vulnerability testing.		
	T0412	Perform vulnerability validation.		
	T0413	Perform vulnerability verification.		
	T0414	Perform vulnerability reporting.		
	T0415	Perform vulnerability remediation.		
	T0416	Perform vulnerability assessment.		
	T0417	Perform vulnerability management.		
	T0418	Perform vulnerability scanning.		
	T0419	Perform vulnerability testing.		
	T0420	Perform vulnerability validation.		
	T0421	Perform vulnerability verification.		
	T0422	Perform vulnerability reporting.		
	T0423	Perform vulnerability remediation.		
	T0424	Perform vulnerability assessment.		
	T0425	Perform vulnerability management.		
	T0426	Perform vulnerability scanning.		
	T0427	Perform vulnerability testing.		
	T0428	Perform vulnerability validation.		
	T0429	Perform vulnerability verification.		
	T0430	Perform vulnerability reporting.		
	T0431	Perform vulnerability remediation.		
	T0432	Perform vulnerability assessment.		
	T0433	Perform vulnerability management.		
	T0434	Perform vulnerability scanning.		
	T0435	Perform vulnerability testing.		
	T0436	Perform vulnerability validation.		
	T0437	Perform vulnerability verification.		
	T0438	Perform vulnerability reporting.		
	T0439	Perform vulnerability remediation.		
	T0440	Perform vulnerability assessment.		
	T0441	Perform vulnerability management.		
	T0442	Perform vulnerability scanning.		
	T0443	Perform vulnerability testing.</		

資安人才技能管理平台



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



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



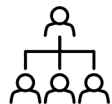
自動評估

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

Lateral movement

Overview

While infiltrating an organization or any other network, after the initial entry point, the attacker or malware will attempt to spread itself and create a stronger foothold in the system. The techniques used during this phase are a part of what is professionally called "lateral movement".

The goal of lateral movement is to reach either sensitive data in the infiltrated organization or to reach a "kill switch" in order to cripple a said organization. In this exercise, the trainee will gain hands-on experience on the Carbon Black EDR management system while investigating the malicious activity.

Courses

- Carbon Black - Analysis with EDR
- Carbon Black - Analysts with EDR
- Command & Scripting Interpreter (T1059)
- CompTIA CySA+ Preparation
- CompTIA CySA+ Preparation
- Cybersecurity Tier-2 Analyst
- Cybersecurity Tier-3 Researcher
- Masquerading (T1036)

Roles

- Security Analyst Level / Tier 3
- Cyber Graduates
- NICE Cyber Defense Analyst (Forensic Computer Analyst, Cyber Security)

NICE KSA&T

Knowledge (5)

- K0005 - Knowledge of cyber threats and vulnerabilities.
- K0042 - Knowledge of incident response and handling methodologies.
- K0046 - Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- K0070 - Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- K0110 - Knowledge of adversarial tactics, techniques, and procedures.

Skills (1)

- S0054 - Skill in using incident handling methodologies.

Abilities (2)

- A0010 - Ability to analyze malware.
- A0128 - Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Tasks (2)

- T0166 - Perform event correlation using information gathered from an observed attack.
- T0258 - Provide timely detection, identification, and alerting of possible events from benign activities.

Recommended Skill Set

對應MITRE ATTACK
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



Debrief: Share-Lock Ransomware, 399962

Debrief

學習報告

Share-Lock Ransomware - Osaka | Summary

BT

AB

TM

Total Score: **50** / 100

Mission: **50** / 82

Quiz: **0** / 18

Training Time: **4hr / 4hr**

Difficulty Level: **Advanced**

Configuration: Guided Training, Crisis Simulation

總分

花費時間

Mission

Score Distribution By Milestones

Response: 0/32

Score: **50/82**

Detection &...: 50/50

Completed Tasks: **5 / 8**

- Detection & Analysis: 5/5
- Response: 0/3

各項績效評分

- 偵測搜查能力
- 事件回應能力
- 資安防禦能力

Discussion Questions

Submitted Answers: **2 / 28**

Quiz - Soc Room

Answers: **0** / **2**

Achievements

(ISC) CPE: **0**

MITRE ATT&CK® Techniques: **26**

Help

Hints: **0 / 8**

Solution Brief: **Opened at: 01:35**

MITRE ATT&CK

感測器在練習期間
即時監控過程及成就

Timeline

Filters: Attack Flow, Achievements, Escalation, Note, SIEM, Help

00:00 Training 'Ransomware - 399962' Started

00:00 Scenario Ransomware Started

00:00 Attack flow Execution: Setting Up Network

00:00 Attack flow Execution: Internal IP Has Been Set to - 199.203.100.77

00:00 Attack flow Execution: Sending Infected E-mail to User082@services.dom fro...

00:00 Attack flow Execution: Sending Infected E-mail to User067@services.dom fro...

00:00 Attack flow Execution: [Status]

學習歷程

- 攻擊事件流程
- 事件處理紀錄

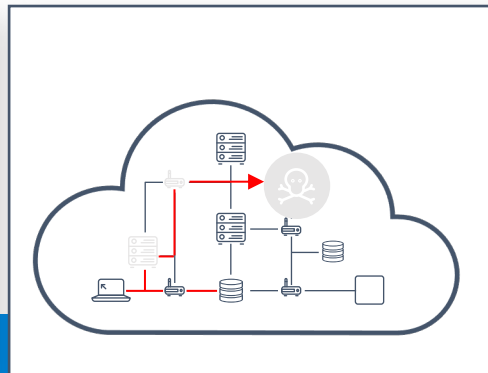
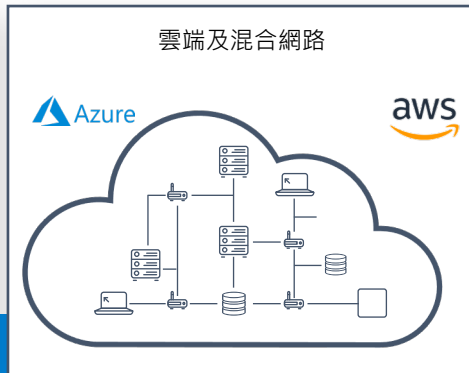
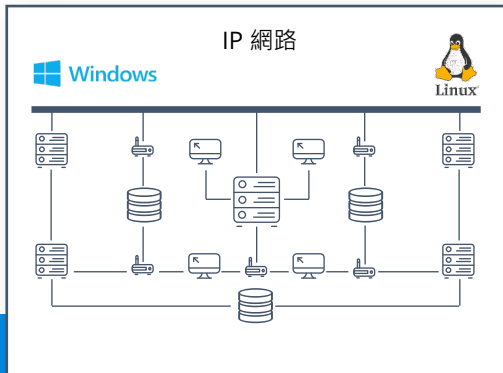
面對不同型態的攻擊預作準備



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



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

Supply Chain Attack

Threat Hunting with CrowdStrike

Web defacement

TrickBot

Azure Attacks

Secure Development Course

Data Exfiltration

AWS Attacks

Keylogger

DNS Hijacking

Threat Intelligence Course

CompTIA SEC+ Course

Coin Mining Attack

Kubernetes

SSRF Simulation

PowerShell investigation

Network Forensics

Pentesting

SQL Injection

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



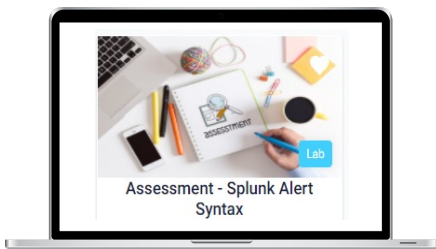
- -30% 平均修復及每個事件
查找分析的時間花費

最大化
資安團隊能力

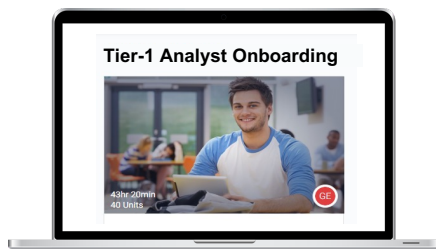


- 改善績效的可視性
- 人才加薪或晉昇的依據

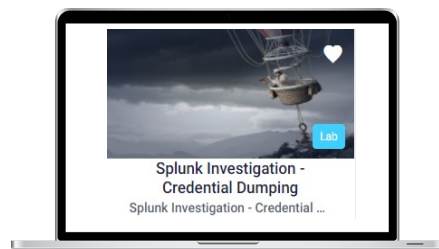
人才篩選實驗室



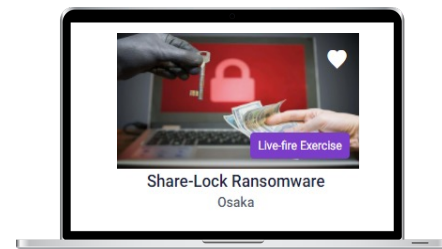
在職培訓課程



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

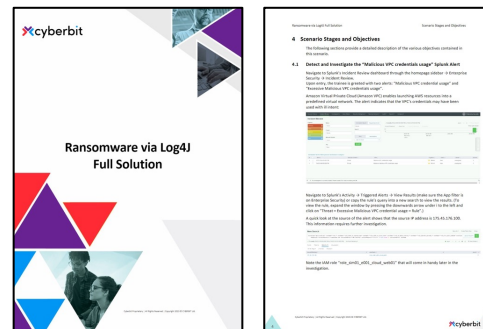
課前/課中說明

執行實境演訓活動

課後說明 / 討論

例：Log4j via Ransomware

Name	Trainee	Type	Difficulty Level	Score	Mode	Booked By	ID	Status	Completion
Ransomware via Log4j	Lei Li	Hands-on	Intermediate	100	Self-paced	Robert Hu	533463	Completed	Nov 9 2023
Topic: Rides and Alerts	Robert Hu	Self-paced	Easy	-	Self-paced	Robert Hu	-	Completed	Nov 9 2023



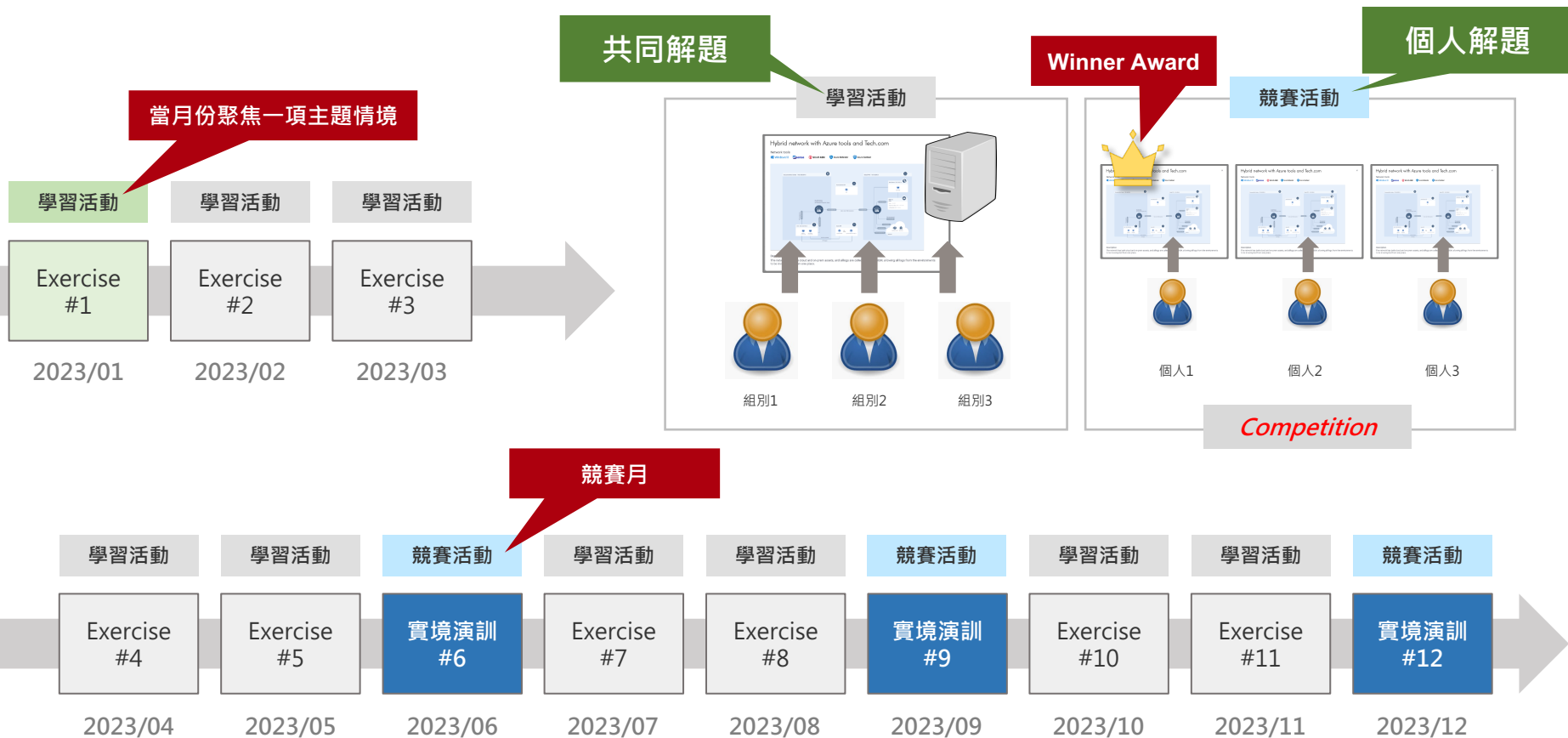
避免學員卡關

現場督課與協助 / Hint

重點是學習到情境劇本與應對方式

Take away

人員演訓課程活動規劃



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 ASA 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 ASA Firewall - Build Access Rules
- Cisco ASA Firewall - Modify Access Rules
- Cisco ASA 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

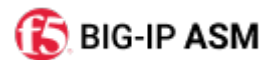
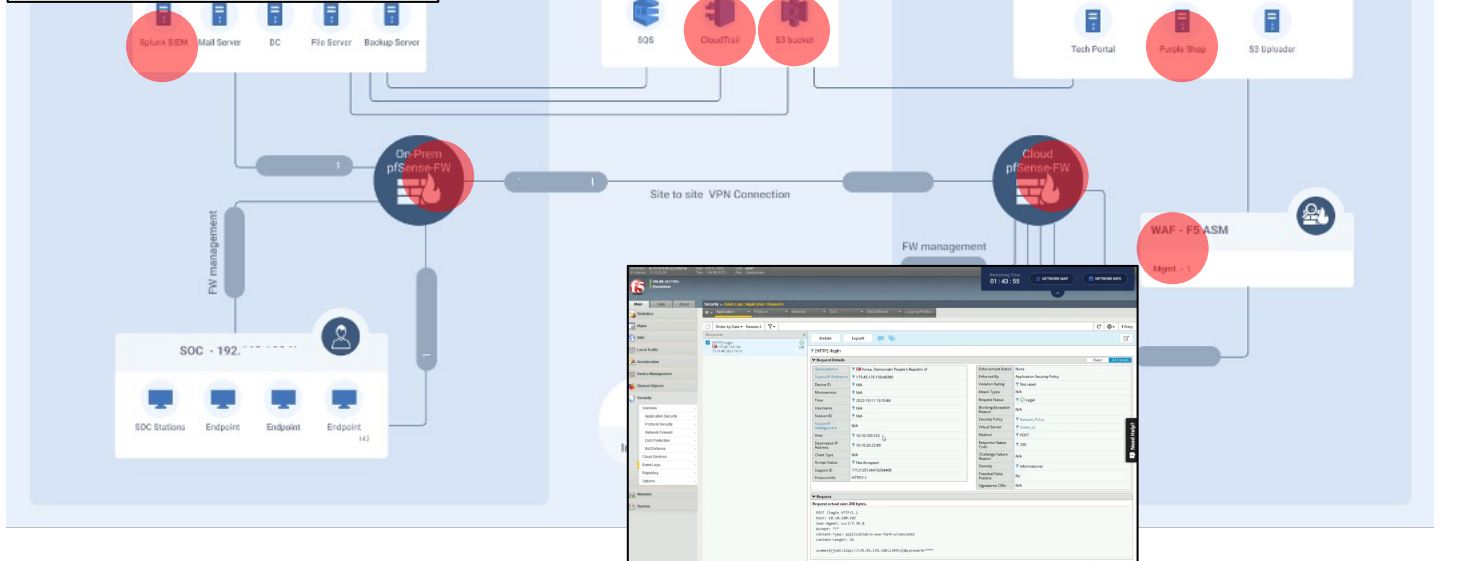
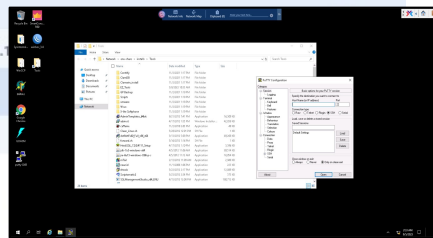
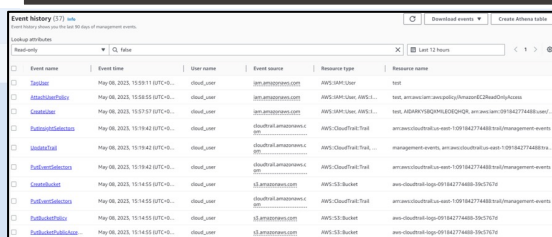
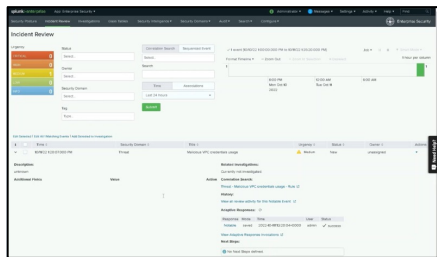
學習目標：

- 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



實境演訓 – Log4j via Ransomware – Team2



Event name	Event time	User name	Event source	Resource type	Resource name
SignIn	May 09, 2025, 10:38:11 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test
awscloudtraillogs	May 09, 2025, 10:55:55 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:57:57 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1
awscloudtraillogs	May 09, 2025, 10:59:42 (UTC+8)	cloud_user	aws-logs-001-us-east-1	AWS CloudTrail Trail	test-awscloudtraillogs-aws-logs-001-us-east-1

Team-1 完成時間 : 1h:45m
Team-2 完成時間 : 0h:55m



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

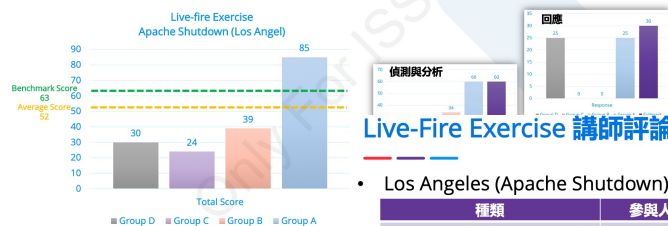
- ✓ 阻止外網訪問伺服器的SSH埠
- ✓ 更改被洩露的密碼
- ✓ 不允許使用遠端工具的憑證緩存功能
- ✓ 將SIEM的重要服務進行監控

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Vayyatta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
 - 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。
4. 使用者User055打開邊界路由器主頁, 由於缺乏安全意識, 保存並進行了惡意的說明pdf
 - 2 → Win7-CNT1得到Plink, VyattaLicenseAgreement.pdf, cmd相關
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 → 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。
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 → 重啟SIEM服務, 可以看到很多Win7-CNT1到伺服器段的埠掃描事件。
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。

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完成本階段實做後, 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;

NICE MITRE ATT&CK NIST IR流程階段表現

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

Courses MITRE ATT&CK **NICE KSA&T** All Units

← Back

Cyber Defense Analyst x

Brain Lee x

人員

Competency 0% 100%

Edit Parameters

角色

50%

NICE | Cyber Defense Analyst

Org. Role

51%

NICE | Cyber Defense Incident Respo...

Org. Role

建議課程

提升方向

Knowledge (70)

Skills (15)

K0001	K0002	K0003	K0004	K0005
K0006	K0007	K0013	K0015	K0018
K0019	K0024	K0033	K0040	K0042
K0044	K0046	K0049	K0056	K0058
K0059	K0060	K0061	K0065	K0070
K0074	K0075	K0093	K0098	K0104
K0106	K0107	K0110	K0111	K0112
K0113	K0116	K0139	K0142	K0143
K0157	K0160	K0161	K0162	K0167
K0168	K0177	K0179	K0180	K0190
K0191	K0192	K0203	K0221	K0222
K0260	K0261	K0262	K0290	K0297

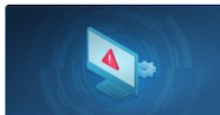
S0020	S0025	S0027	S0036
S0057	S0063	S0078	S0096
S0156	S0167	S0169	S0367

Skill in reading and interpreting signatures (e.g., snort). 8 Units

S0096 0%

Unpracticed (8)

Show all



YARA Rules - Basic ...



Snort Rules - Introdu...



Fix The Broken Rule

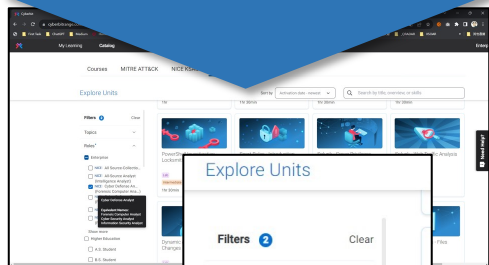
Create Course

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



Explore Units

Filters 2 Clear

Topics

Roles

- Enterprise
 - NICE - All Source-Collectio...
 - NICE - All-Source Analyst (Intelligence Analyst)
 - NICE - Cyber Defense An... (Forensic Computer Ana...)
 - NICE - Cyber Defense Analyst
 - NICE - Forensic Computer Analyst
 - NICE - Cyber Security Analyst
 - NICE - Information Security Analyst

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

Summary

Congratulations! You have reached the final phase of this session. Your achievements are detailed below and will be available for review in My Achievements.

Item	Score	Out of	Difficulty Level	Configuration
Final Score	96	100	Medium	Self-Training
Mission	66	100	Medium	Self-Training
Quiz	30	100	Medium	Self-Training

Mission

Score Distribution by Milestone

Completed Tasks

- Introduction & Analysis
- Response

Score: 66/70

Unit Steps:

- About This Unit
- Virtual Network
- Mission
- Quiz
- Summary

Complete Session

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



ISIP CAMP
教育部先進資通安全實務人才培育計畫

金融資安 Mentor 實務教學

8.24~8.25 全天

精誠資訊恆逸台北中心
(105台北市松山區復興北路99號14樓)

8/24活動內容

09:00-10:00	金融資安威脅
14:00-14:10	台灣資安主管聯盟論壇 與談人： 富邦金控副總經理暨資安長 蘇清偉 永豐銀行副總經理暨資安處副處長 高大宇 元大證券資安主管 陳松春
12:00-13:00	午休
14:30-15:30	金融攻防平台實機操作 SIEM資安監控平台操作介紹 資安事件應處工具介紹 攻防演練平台操作說明

8/25活動內容

09:00-12:00	資安攻防演練-情境一
15:50-17:00	情境一-檢討交流
12:30-13:30	午休
13:30-16:30	資安攻防演練-情境二
16:30-17:00	情境二-檢討交流



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

FS-ISAC About Us Our Offerings Events Insights Knowledge Newsroom Join Us



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

Hyper-realistic tournament for cybersecurity defenders - back by



THANK YOU

感謝您的聆聽

www.issdu.com.tw

