迎向人培2.0
建構國家級資安攻防演練平台介紹

CSTI 資安科技研究所
CyberSecurity Technology Institute

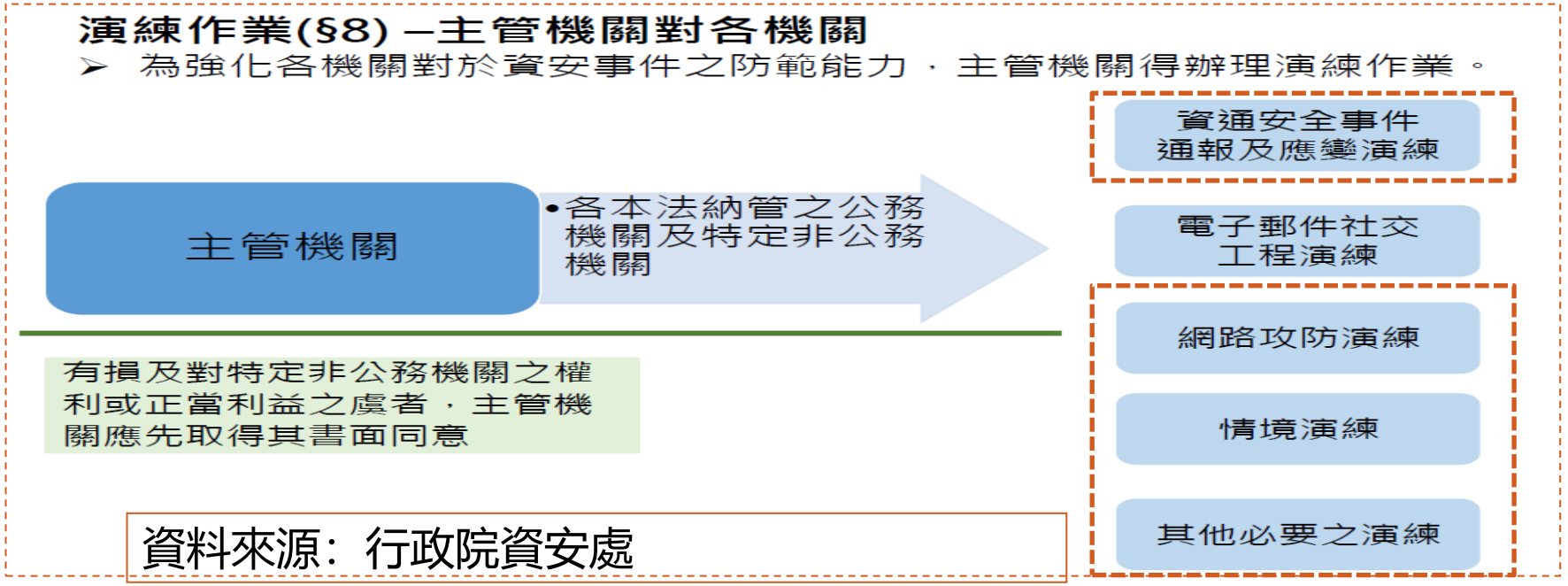
RANGE SEED
智慧技術人才培育中心

Dec.2018

前言~三讀過後，迫在眼前的灰犀牛?

資安處於2017年盤點統計，各部會及八大CII資安人才缺口達千餘人。
層出不窮的金融資安事件，金融業資安人才需求升高，六成業者開出職缺。

在上述需求缺口中，政府及產業尤其重視資安從業人員的攻防演練!



資料來源：行政院資安處

Case：自我衡量

APT： 進階持續性滲透攻擊

Ransomware： 勒索軟體

Case：自我衡量

APT： 進階持續性滲透攻擊

Ransomware： 勒索軟體

Case Study

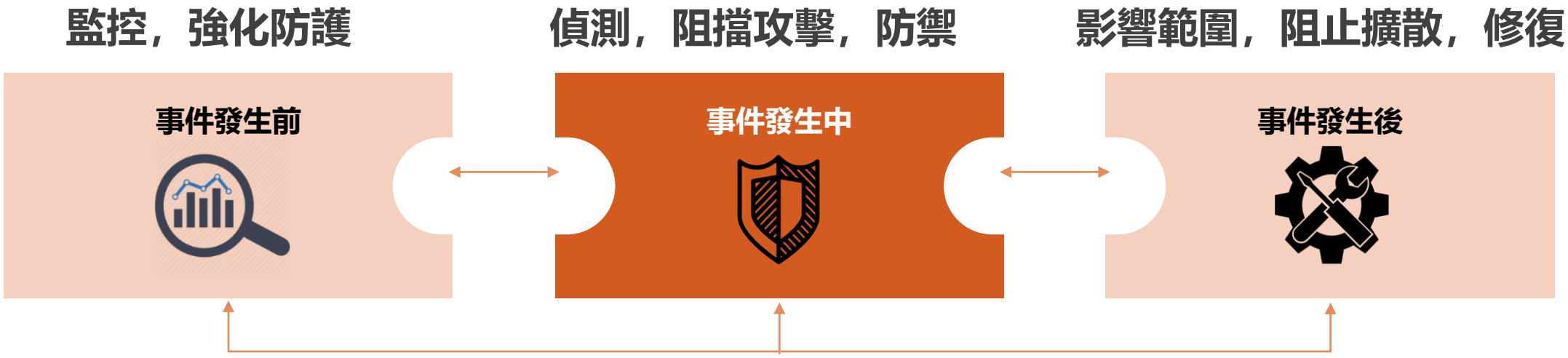
你是個社群網站的網路管理主管，今天你和往常一樣送小孩上學然後九點準時進公司，和平時一樣是個輕鬆愉快的日子。當你打開電腦你發覺開機速度有點不一樣，但你不在意，畢竟公司所配的電腦本來就不是最新的，你利用了開機的空擋時間為自己泡杯咖啡，但當你再次看向你的電腦螢幕時，已經沒心情喝下那杯咖啡了。

電腦螢幕上出現了一個紅色的大鎖，正當你還沒反應過來時，辦公桌的電話突然響起，總經理打給你說他的電腦上也出現了一個紅色的大鎖而且完全不能操作，要你立刻過去，你急忙地掛上電話正要開辦公室門時，你的組員突然衝進來，說業務部的電腦全中了勒索病毒，接著陸陸續續的災情傳到你的耳中，法務部、技術部、開發部...幾乎沒有一個地方沒有災情傳出。

你想辦法要理解事情是如何發生的，但辦公室的電話、手機、報告讓你無法專心的思考，災害持續在擴大。但你不知道更糟的事情在後頭，董事長突然打電話給你，說他在新聞上看到公司客戶的個資出現在新聞媒體上，這時你已經知道該是遞辭呈的時候了...

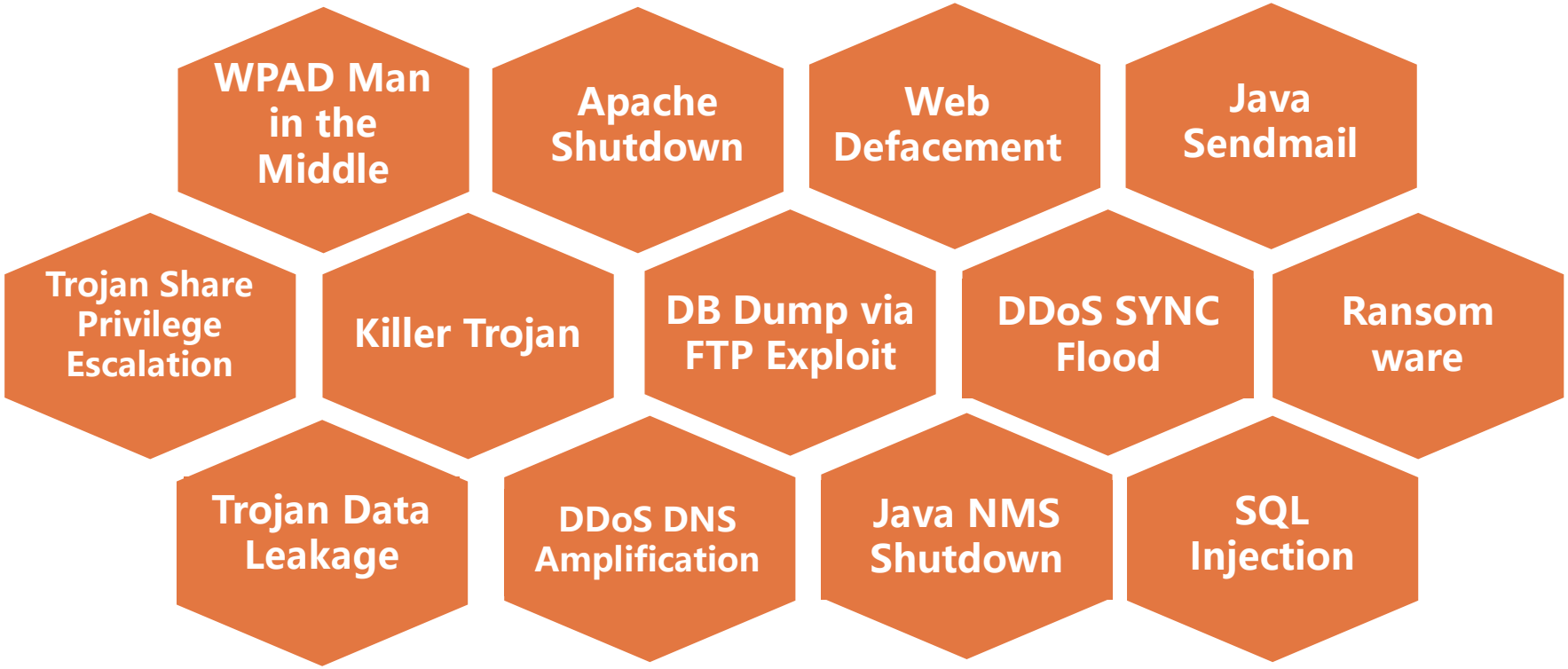
國家級資安攻防演練平台與服務

透過資策會資安所RangeSeed智慧人才培訓中心獨家建置之東京奧運唯一指定使用的國際軍事與商業兩用等級之攻防演練平台(Cyberbit Range)，甫以資安所自行編撰之先備知識，強化資安專業人才事件前、事件中到事件後的完整防禦能力。



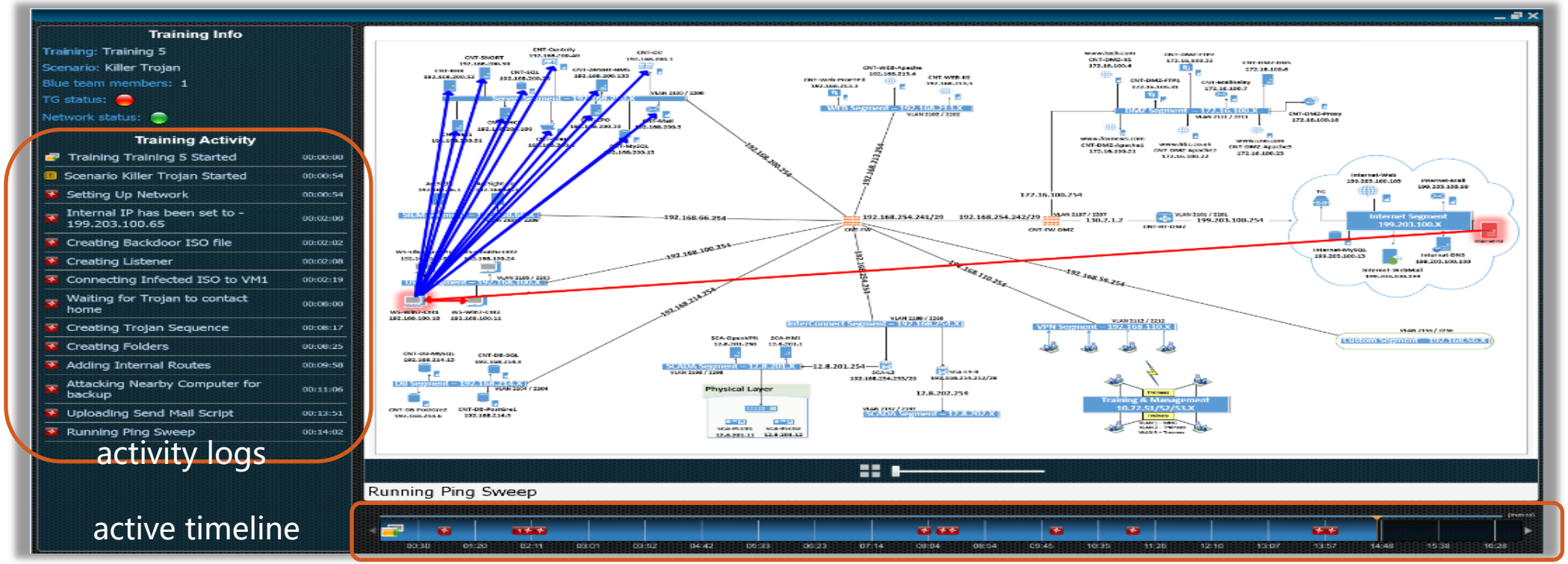
特色1~13類、逾百項攻擊演練場景

提供高度擬真環境訓練體驗、自動進行重複情境式訓練、並可模擬各種網路環境及真實封包傳輸，同時可透過原廠更新或自行研發新的SCENARIO場景。



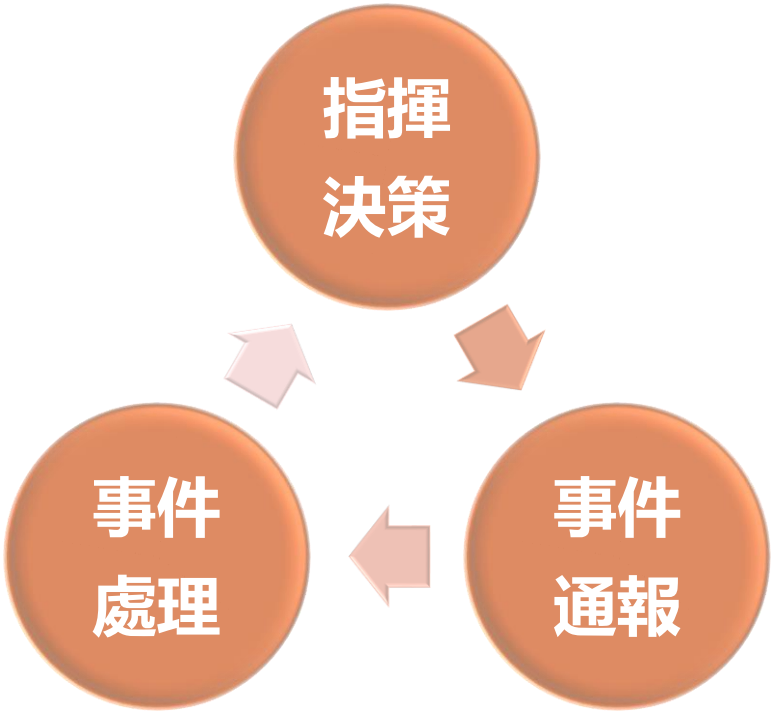
特色2~360° 拓樸圖提供高度擬真

Observer 可透過持續的箭頭移動，觀察攻擊的持續變化，並詳細描述攻擊期間的移動流程。



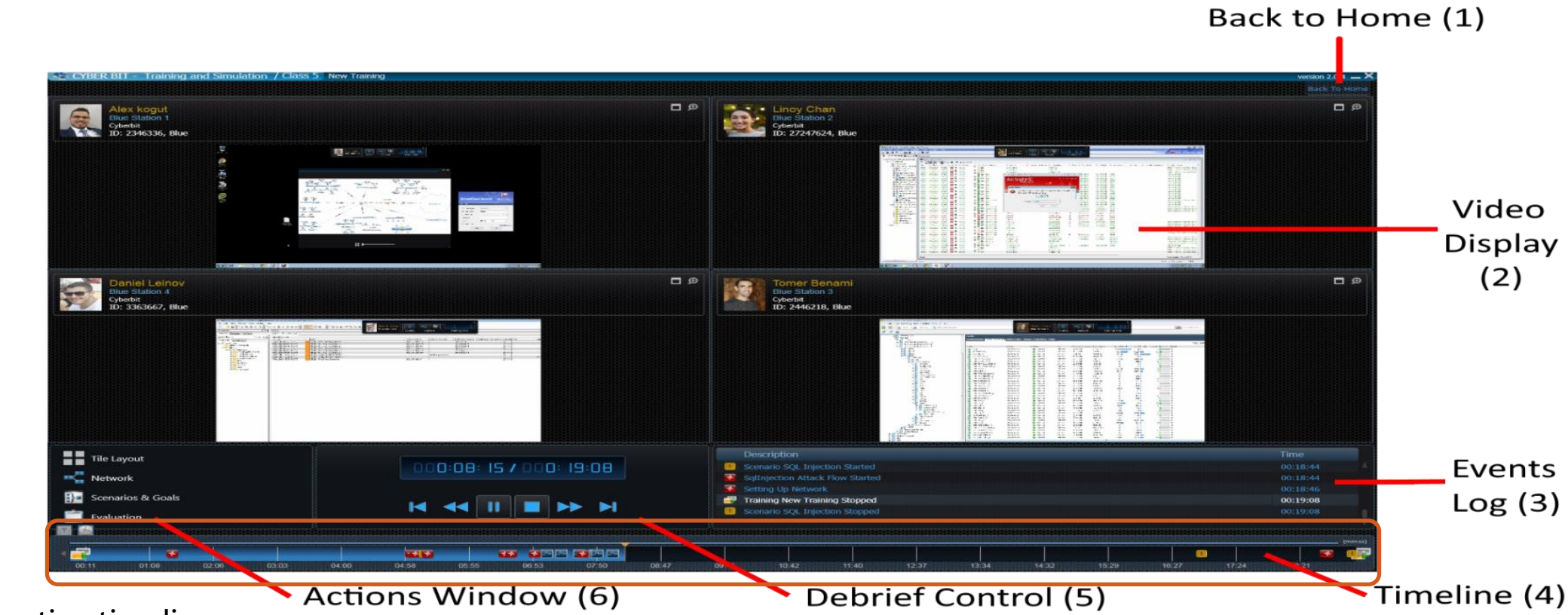
特色3~小班菁英教學，可分組合作或P.K

每班上限8人，學習過程中將學員分為指揮官、通報、處理等角色。
可培養團隊作戰能力或舉辦小組競賽等方式進行。



特色4~縝密的Debriefing

Debriefing (After Action Review) 模式讓 trainer 可透過播放學員演練的紀錄影片，重點總結學員的演練成果與說明未來可強化的地方與技巧。



特色5~有效的學員訓後評量

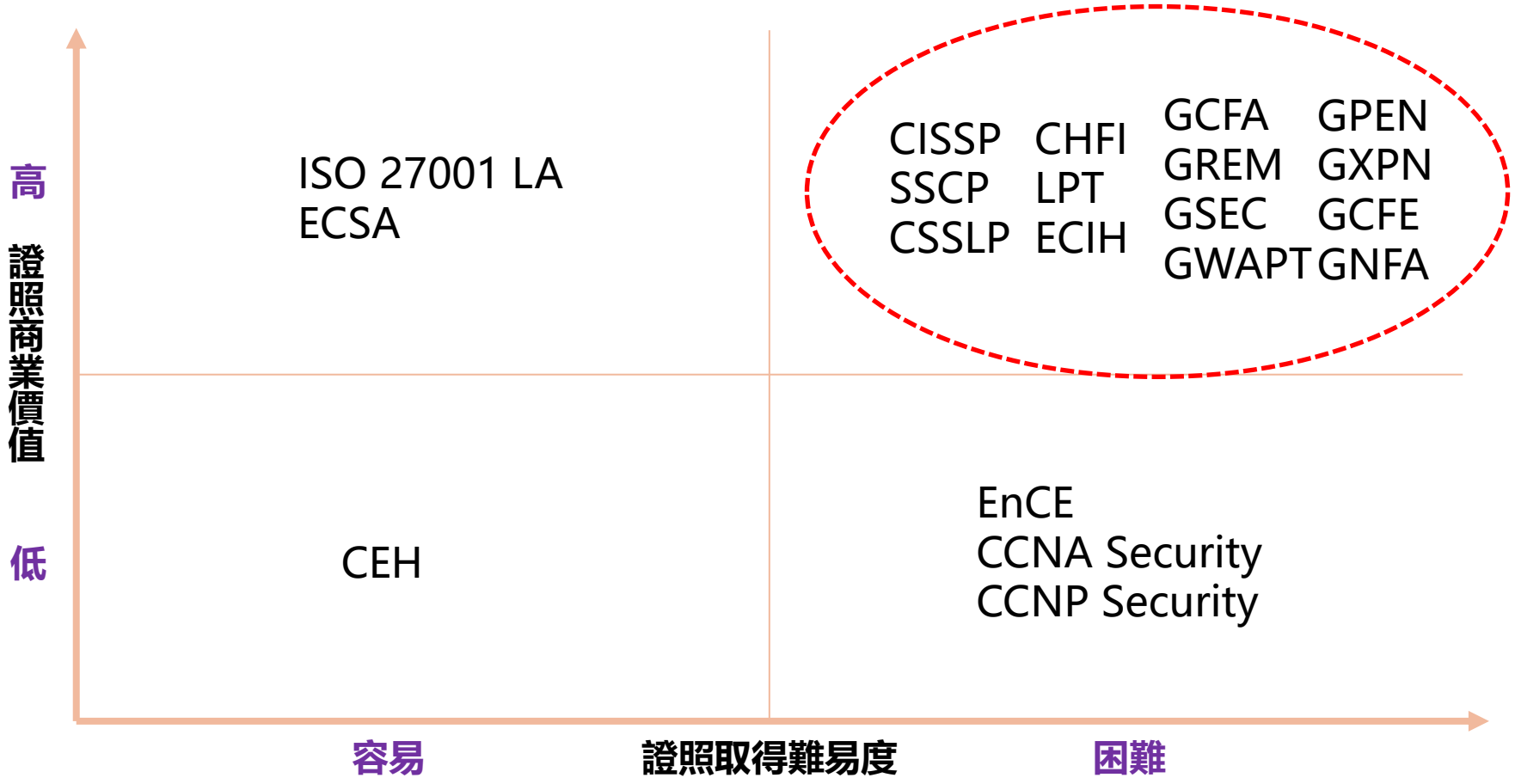
學員訓後將提供每學員客製化之成效評量報告，分為個人分數(知識、技能、領導能力等三面向共18項指標)與團隊分數(系統自動產生)，以做為未來強化能力之參考。

個人知識能力評估	★~★★★★★
網絡拓樸圖與架構	
主機架構	
應用程式漏洞與特性	
惡意程式	
資訊安全防護	
漏洞修補與復原	

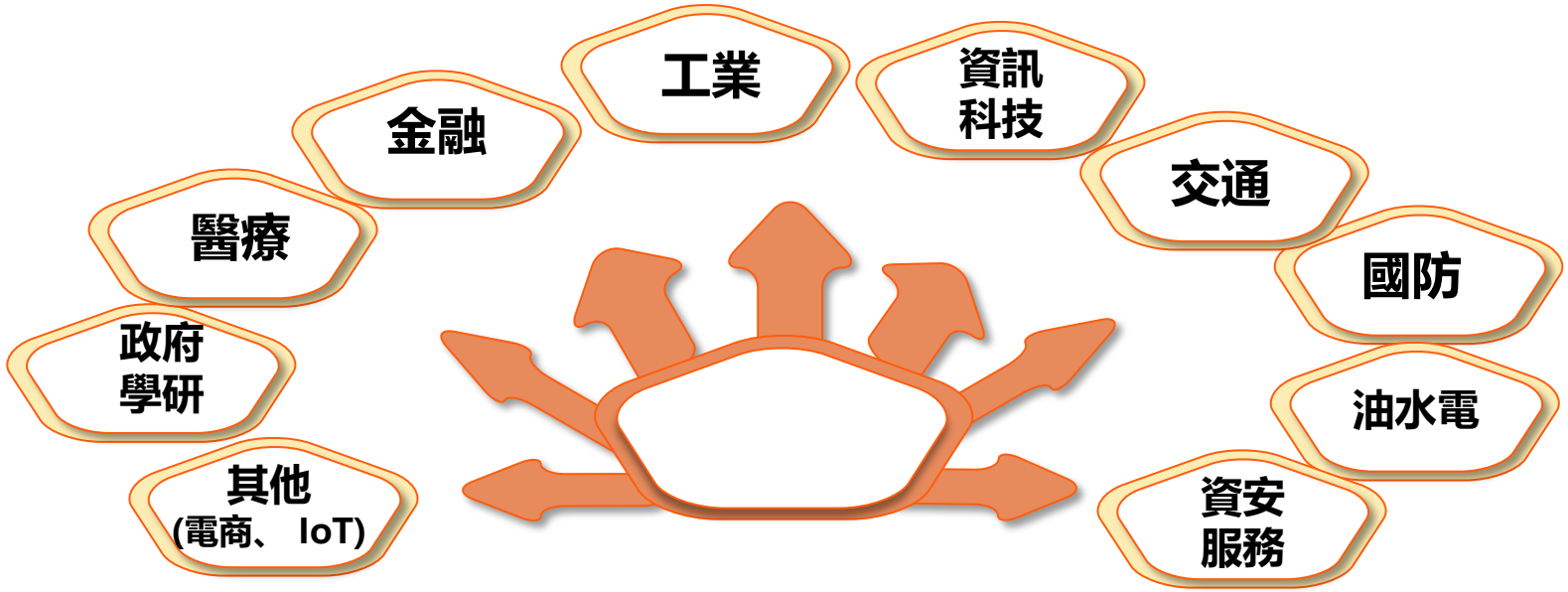
個人技術能力評估	★~★★★★★
網路跡象分析	
系統日誌熟悉度	
系統語法熟悉度	
程式語言熟悉度	
惡意威脅與行為分析	
漏洞修補與復原	

個人領導能力評估	★~★★★★★
凝聚組員意見達成共識	
問題與解決方案分析	
計畫與組織	
判斷力	
達成情境目標	
團隊分工與領導	

特色6~演練內容有助國際證照接軌



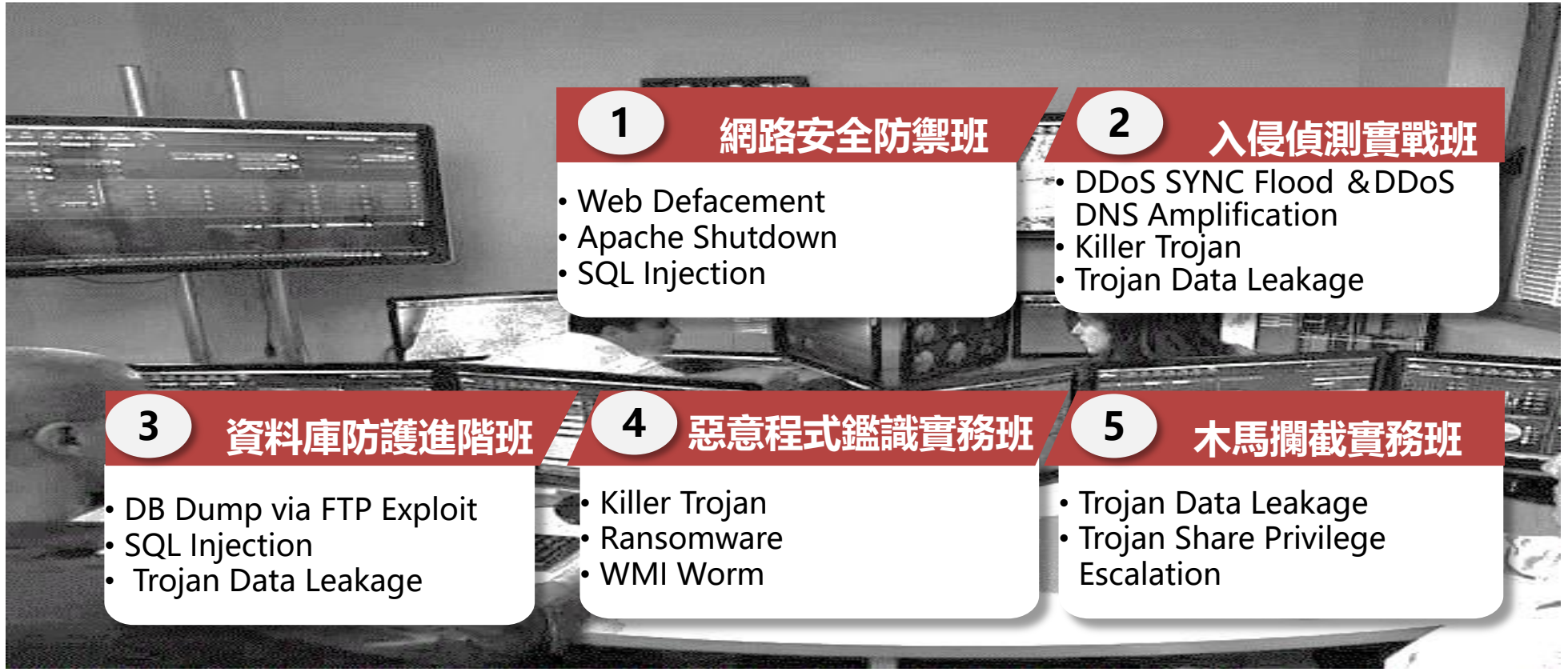
本課程適合對象



- 資訊安全專家
- 資訊技術專家
- 軟體開發人員
- IT/OT/網管人員
- SOC人員
- CERT團隊
- 資安服務人員
- 資安研究人員
- 資訊/資料分析人員

適合台灣環境之專家班課程設計

3天(演練2~3大類場景)，4~8人小班制，可企業包班，可課程客製。



「5大專班內容介紹

課程名稱	演練情境一	演練情境二	演練情境三	課程效益
網路安全防禦班	Web Defacement	Apache Shutdown	SQL Injection	• 識別駭客如何利用暴力破解網站密碼，從日誌分析中找出遭受攻擊的網頁 • 學習事件分析技巧及網站入侵事件檢測
入侵偵測實戰班	DDoS SYNC Flood & DDoS DNS Amplification	Killer Trojan	Trojan Data Leakage	• 學習網路流量狀態的分析，了解駭客如何透過DDoS癱瘓伺服器 • 教授伺服器的網路架構及作業系統和資料庫日誌之分析，強化SSH Client及系統管理工具應用 • 增強事件分析的實戰練習並有效執行入侵檢測
資料庫防護進階班	DB Dump via FTP Exploit	SQL Injection	Trojan Data Leakage	• 識別駭客如何利用網頁的架構漏洞，插入SQL指令來攻擊網站資料庫或伺服器 • 教授網站系統和資料庫日誌分析，加強伺服器之防護 • 學習使用網路管理工具了解日誌和事件分析工具，實時監測威脅
惡意程式鑑識實務班	Killer Trojan	Ransomware	WMI Worm	• 學習及分析駭客惡意程式攻擊之手法，鑑識受木馬入侵的主機，以阻止病毒擴散 • 學習透過分析系統日誌，強化用戶端Outlook系統及防火牆管理工具的使用 • 透過系統管理政策部署的概念，讓學員將概念延伸至本身熟悉的工具，執行入侵檢測分析
木馬攔截實務班	Trojan Data Leakage	Trojan Share Privilege Escalation	-----	• 識別駭客如何利用木馬程式或Windows腳本程式攻擊手法 • 增強學員對於郵件系統、資料庫及防火牆等工具的使用實務技巧及木馬病毒防護 • 學習透過分析日誌了解駭客的攻擊邏輯

新挑戰 新思維 新契機!

RANGE SEED
智慧技術人才培育中心

https://rangeseed.com

資策會資安所 邱之崧
(02)6607-8973
0935-870-755
tony@iii.org.tw