

資安實戰攻防演練中心 (Cyber Range Workshop)



“有看過真正攻擊發生時的樣子嗎？”



簡報目錄

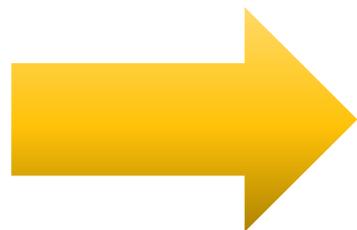
- 實戰攻防演練中心簡介及目標
- 教育訓練平台
- 教學方式及特點
- Q & A

Cyber Range

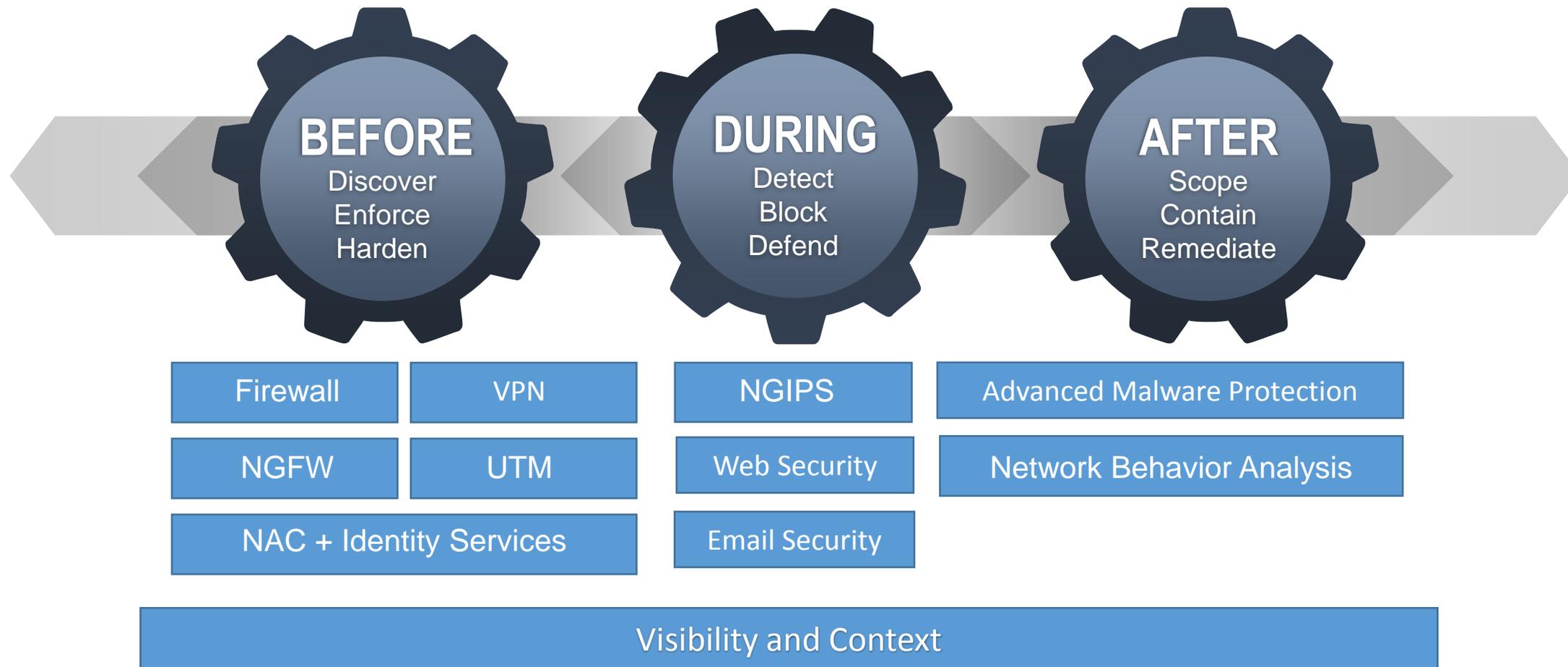
資安實戰攻防演練中心 簡介及目標



資安教育訓練的下一步 – 由紙本進入到實作



課程內容 - 包含攻擊的**事前**、**事中**及**事後**



課程內容 – 資安實戰攻防演練提供

■ 超過 100 種的真實攻擊
情境與組合

■ 整合安全情報資訊 / 惡
意網址及軟體

Web/Mail Security

SIEM

Firewall / IPS

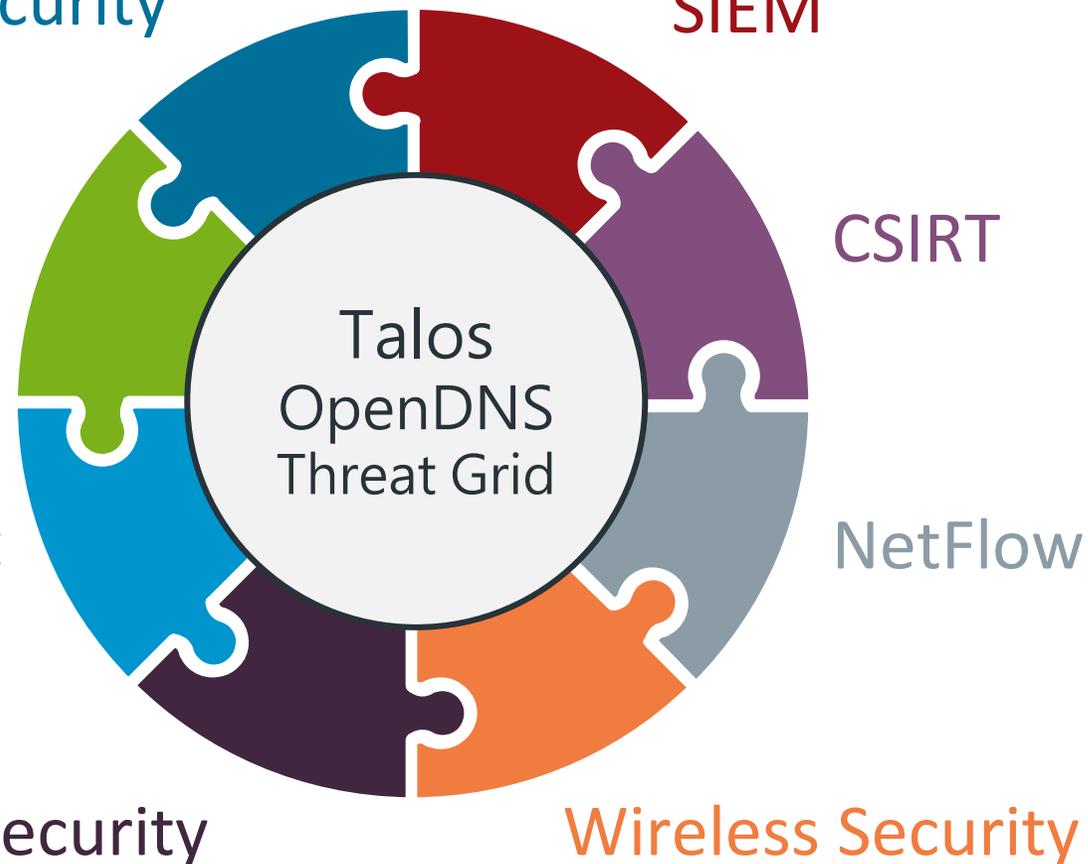
CSIRT

Cyber Threat
Defense

NetFlow

Cloud Security

Wireless Security



實作課程的學習效益

檢視企業防護架構

透過實際的演練來 *對比目前企業的環境架構* 完備程度，達成事件發生前可偵測、警示及發生時可阻斷

經驗學習

由實作的經驗中學習為企業 *建立適合的管理流程與機制*，並且一併建立適當的回饋機制以修正相對應的管理流程及機制

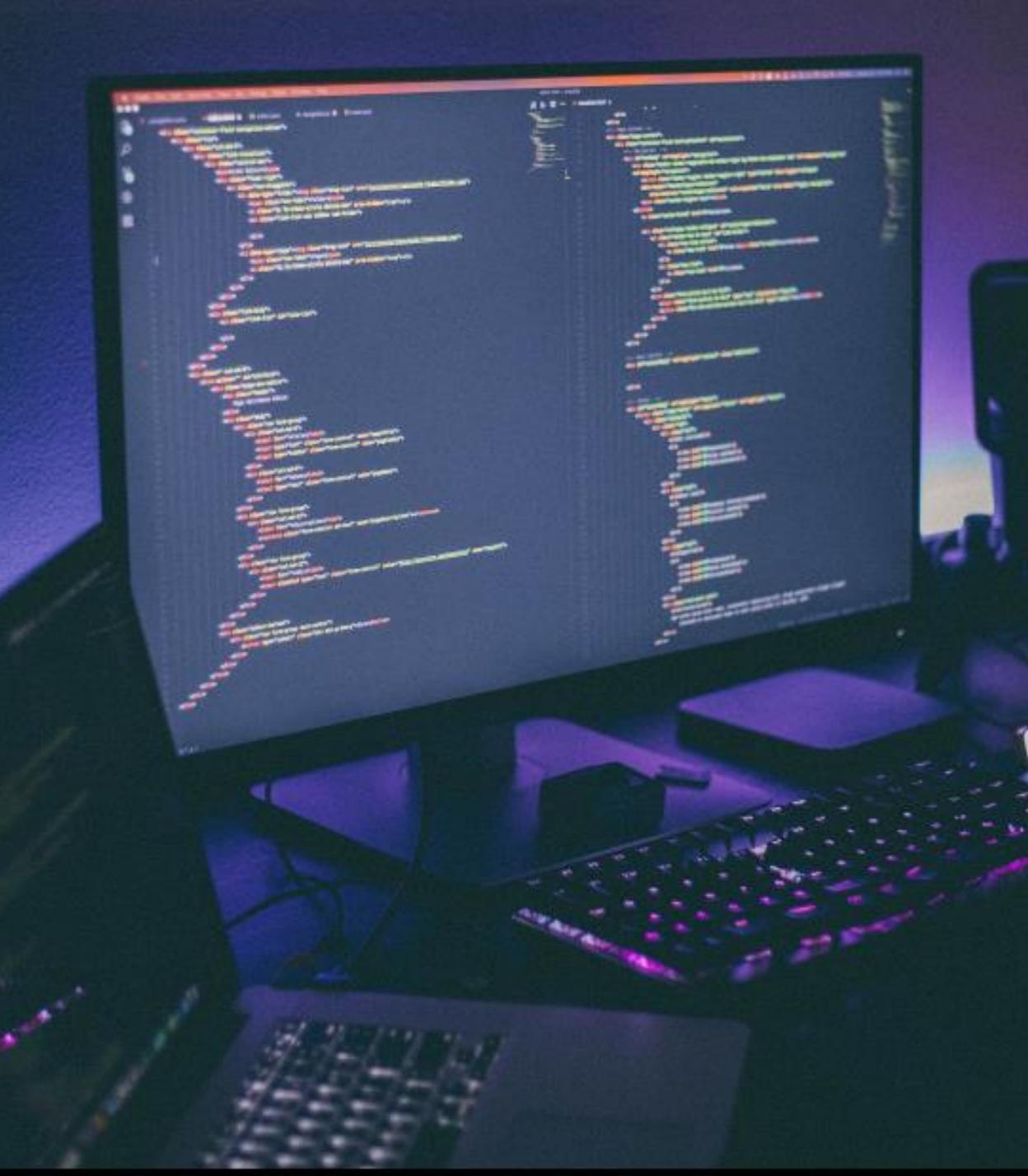


提高對異常的警覺

學習 *檢測網路封包或行為* 的異常、分析 event 及 log 資訊，並判斷是否為攻擊行為

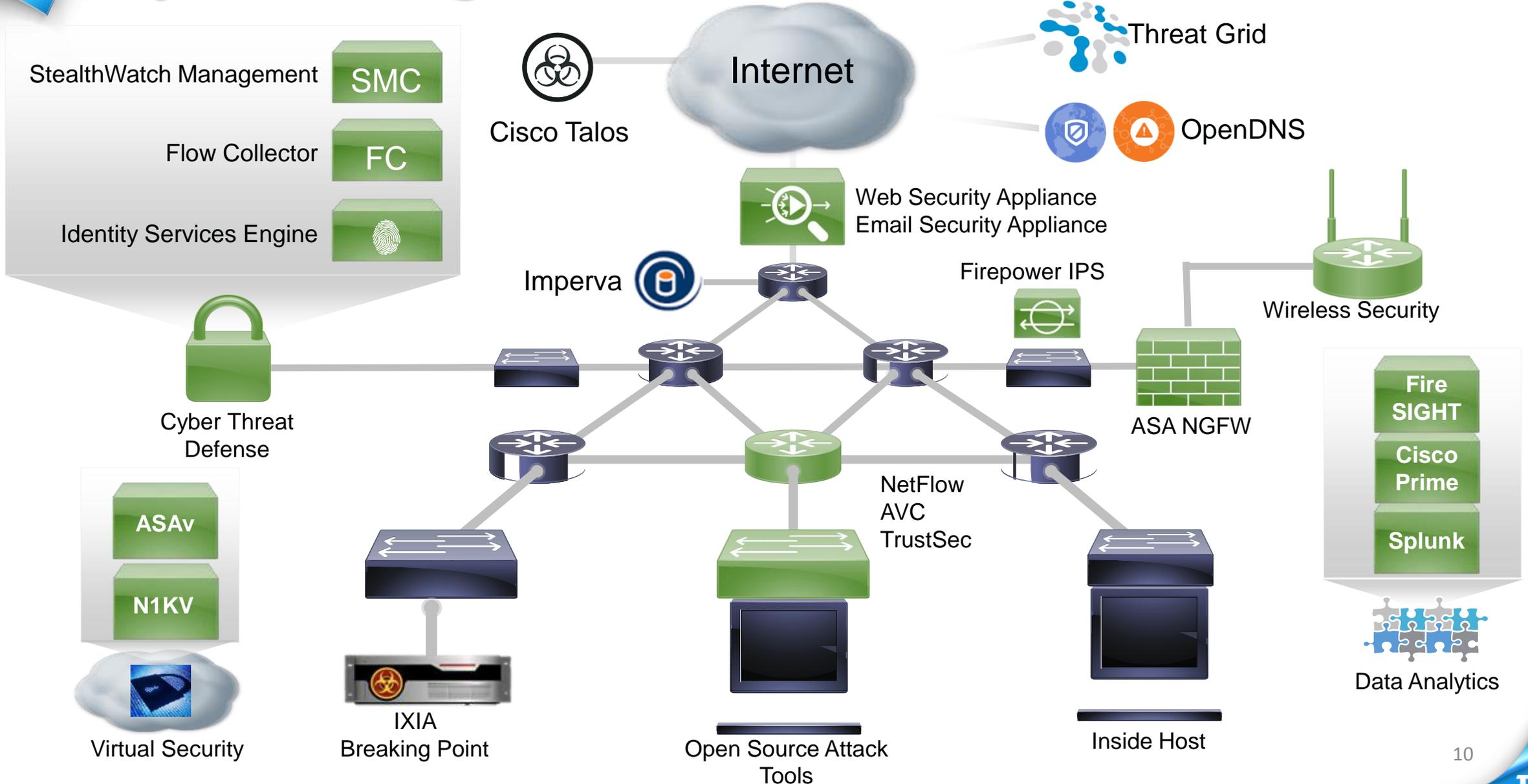
鑑往知來

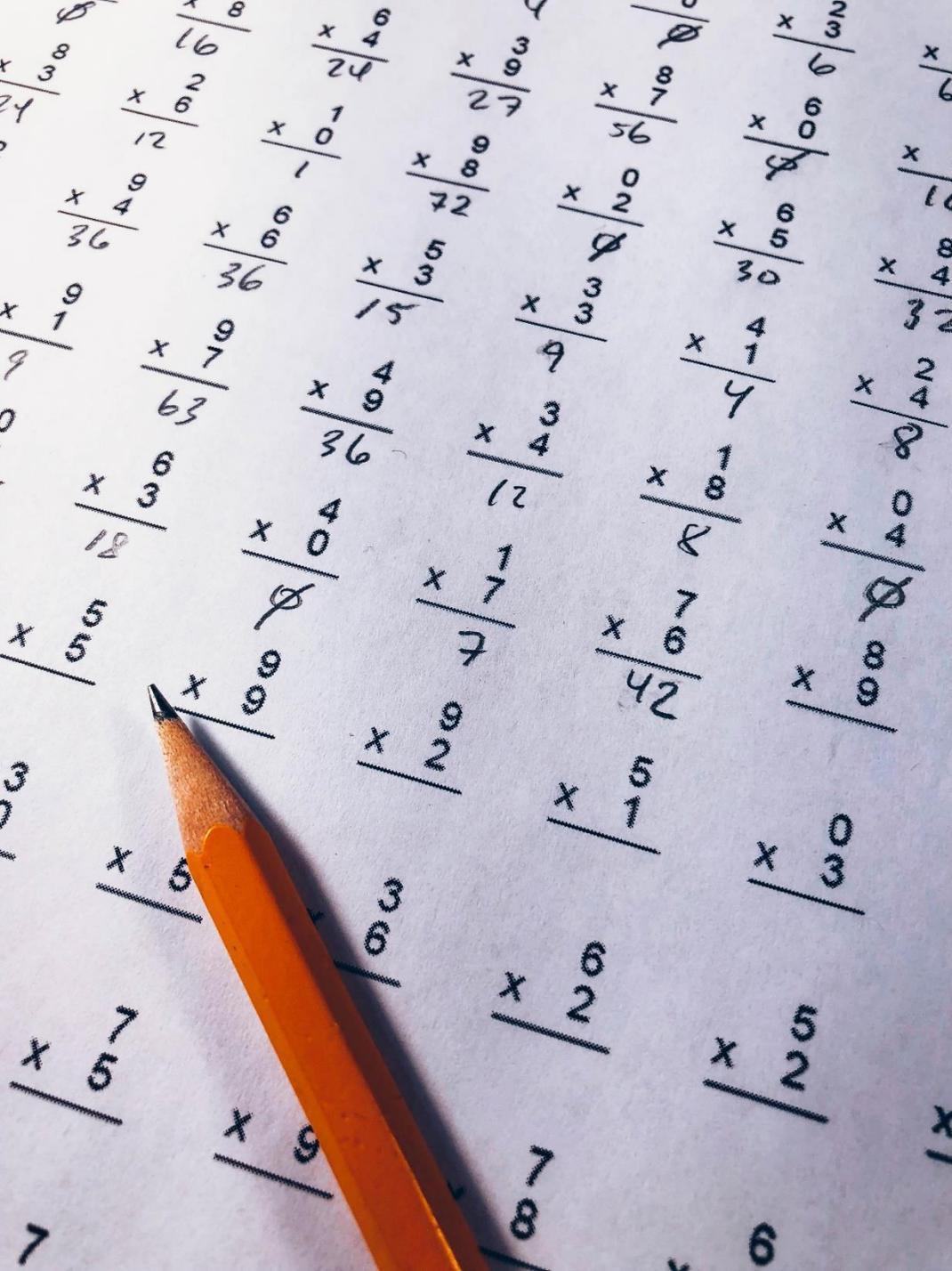
檢視 *是否曾經歷過相同或類似的攻擊*、當時處理的程序是否適當且處理的結果是否合乎組織的預期



教育訓練平台

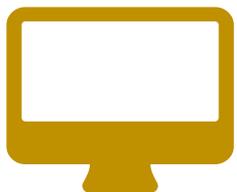
Cyber Range 實作環境含完整的企業架構





教學方式及特點

以學員最佳的學習效果為出發點



一人一機

確保每位學員皆能完整操作所有實作個案



低師生比

兩位講師及兩位助教同時教學，師生比最多 1:6，以維持最佳的教學品質



走動式教學

隨時與學員保持最佳的互動性



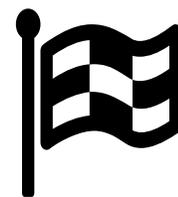
75% 為實作課程

概要說明各種攻擊情境及原理，以實作為課程重點



分組合作

兩人一組、共同討論



解題競賽

以學員間的互相競爭來提升及加強學習效果

課程大綱 – 三日正式課程

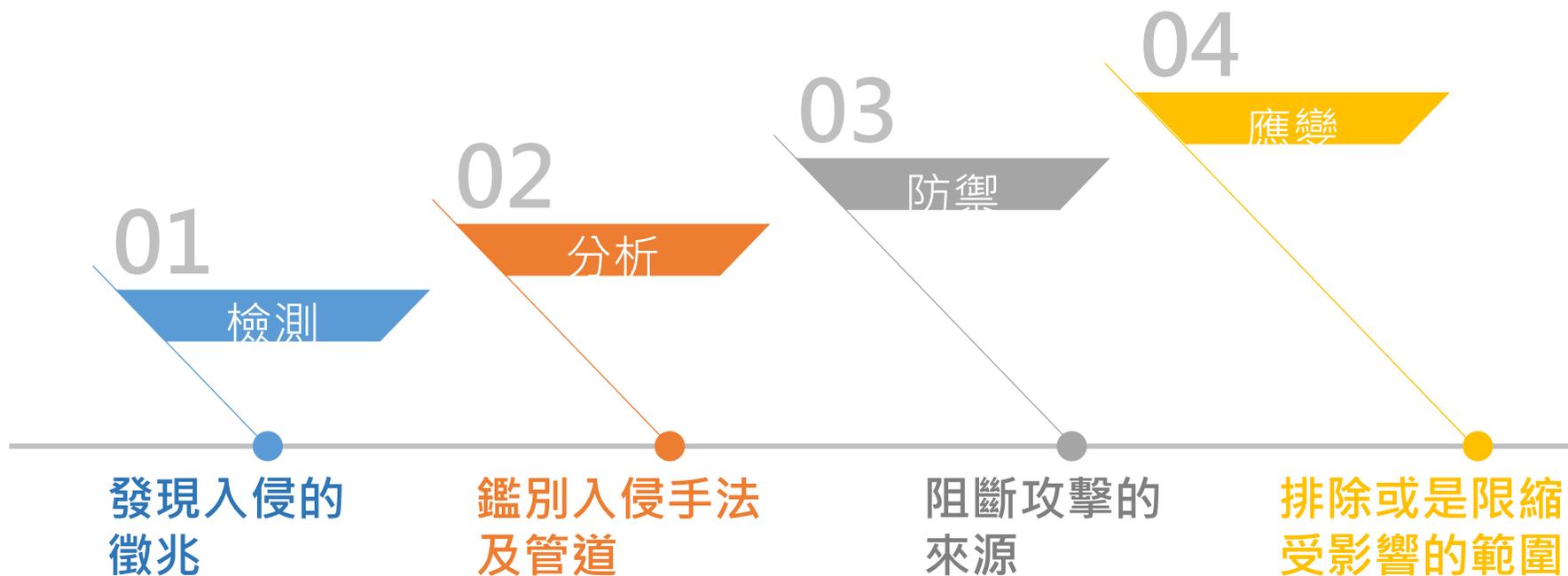
日期	內容
Day 1 上午	Cyber Range架構簡介及情境演示 電腦安全事件應變小組(Computer Security Incident Response Team, CSIRT)實務介紹
Day 1 下午	安全性資訊與事件管理(Security Information and Event Management, SIEM)概述 實戰演練：初階攻擊與防禦、含背景流量之混和式攻擊
Day 2 上午	防火牆(Firewall)及入侵防禦系統(IPS)簡介 實戰演練：5個相關攻擊情境
Day 2 下午	入侵技術簡介 網頁及電子郵件安全 實戰演練：5個相關攻擊情境
Day 3 上午	網路威脅防禦簡介 實戰演練：5個相關攻擊情境
Day 3 下午	無線網路安全 實戰演練：物聯網設備攻擊及應變 實戰演練：含背景流量之混合式攻擊 實戰競賽：藍隊(防禦方)競技

**75% 的
課程皆為
實作體驗**

完整學習資安事件處理的程序

■ 超過 100 種的真實攻擊
情境與組合

■ 整合安全情報資訊 / 惡
意網址及軟體



企業級資安實戰攻防演練中心



資安實戰攻防演練中心 官網 cybersecurity.com.tw/

如欲瞭解更多實戰攻防演練中心相關訊息，請洽
協志聯合科技 盧小姐 (02)55625463 Sunny.Lu@tisnet.com.tw
大同世界科技 黃小姐 (02)55625627 Linda.Huang@etatumg.com



Q&A



TISNet
協志聯合科技
www.tisnet.com.tw

