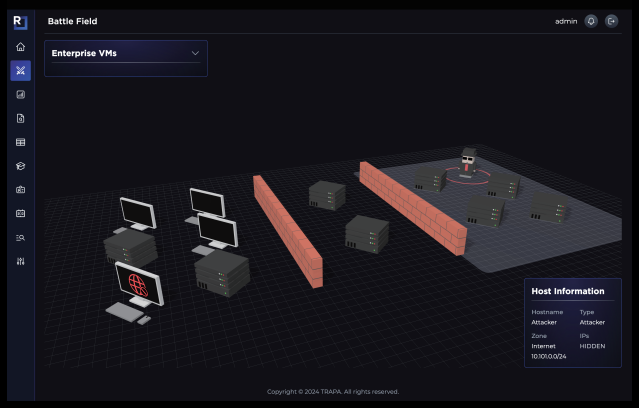
PRODUCT

TRAPA CYBER RANGE™

BLUE TEAM EXERCISES

網路威脅實戰演練，完整精進團隊應變能量。



演練場景

APT29

劇本難度:中
MITRE ATT&CK Techniques : 19+
NICE KSA : 19+

主要演練內容包含

Windows Active Directory 滲透
系統環境探測
透過內建合法機制橫向移動
規避及停用監控機制
無檔案後門埋入
多種檔案滅證手法

實戰強化調查能力

模擬資源有限的 SOC 單位進行攻防演練，協助資安人員演練如何評估事件嚴重性與安排調查順序。利用有限資源最大化調查成效，縮短實戰反應時間。

整合國際資安標準

結合國際標準 MITRE ATT&CK 與 NIST NICE 框架，明確標示演練題目相應的攻擊技術，使資安人員能進行系統性的訓練，掌握符合行業標準的知識與經驗。

深度掌握攻擊全貌

組織完整 APT 族群攻擊鏈，模擬真實攻擊行動始末。透過若干線索逐步拼湊攻擊者行為，幫助企業資安人員建構威脅事件全貌框架，藉以迅速掌握威脅事件全貌。

量化團隊演練成效

根據演練過程的即時表現，將團隊與個別成員演練成果以資訊面板量化呈現，幫助企業了解 SOC 團隊真實能力情況，以利進一步擬定訓練策略與運用方針。

TRAPA CYBER RANGE™ 能夠幫助企業

✓ 檢驗訓練成效

以針對性訓練評估藍隊實力，制定策略有效增強整體戰力。

✓ 實戰攻防演練

擬真實戰環境，實際體驗經典 APT 的完整行動與攻擊技術。

✓ 強化應變能量

拓展全方面事件應變經驗，有效緩解潛在風險及防禦破口。