Cisco Cyber Range Service （數位靶場實戰服務）

服務概觀

由於安全威脅越來越複雜，攻擊行為的針對性和持久性愈來愈明顯，不斷為組織及企業的業務營運帶來更多的挑戰及威脅。而安全設備和安全軟體並不足以阻止最先進的攻擊。安全防禦需要實際的防禦技術經驗，並由訓練有素的資訊安全人員，擁有專業技術檢測能力及防禦技術。針對可能性侵害行為以先知著見的高度防禦技術，制止可能性的危害。

思科 Cisco Cyber Range Service（數位靶場實戰服務），幫助組織及企業內的安全人員建立必要的防禦技能和實戰經驗協助打擊安全威脅。基於現實條件 Cisco Cyber Range Service（數位靶場實戰服務）提供一種合成攻擊及防禦的實際環境，讓參與人員發揮兩者的作用（攻擊者和防禦者），以了解脆弱性及威脅性的最新方法和利用先進的工具和技術，以減輕和阻擋威脅。

Cisco Cyber Range Service(數位靶場實戰服務)提供：

- 真實的攻擊防禦環境與經驗，搭配防禦技術和複雜的攻擊內容，包括持續性滲透威脅（Advanced Persistent Threat, APT）。
- 在部署成熟及完整的安全保護模式下，進行各種攻擊及防禦演練程序。
- 採用領先業界的工具和技術，真實的模擬安全技術防禦手段及技巧。
- 強調參與人員團隊精神和分工合作，專注核心技術，且提昇安全技術及技能。

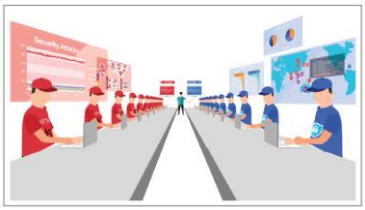
服務說明

Cisco Cyber Range Service（數位靶場實戰服務）是一個防禦實戰的演練平台，是學習及體驗線上攻擊及防禦實戰的智慧型系統。如同飛行模擬器中，飛行員學會如何處理複雜的飛航系統及不同的飛行狀況。Cisco Cyber Range Service（數位靶場實戰服務）是安全人員實戰的最佳環境。

Cisco Cyber Range Service(數位靶場實戰服務)，是一種網路世界威脅砂坑（Send Pit）環境中的網路模擬。一個典型企業的安全管理，包含保護技術、人員技能、安全流程及機敏資料，但擁有的技術環境只能著手於現實環境上的妥協。思科為企業建立相關環境，協助客戶狀大及增強相關安全管理技能。

服務資源

Cisco Cyber Range Service（數位靶場實戰服務）由以下部分組成：



- 綜合 15 種以上的安全解決方案（SIEM、Big Data、CSIRT、Cloud Security、Wireless Security、Web Security、Mail Security、NetFlow、Cyber Threat Defense、FW / IPS 等）。
- 超過 100 種不同的攻擊手法及劇本，超過 100 種實際應用。
- 每月不斷更新最新的攻擊和威脅情況。
- 每天資料總流量超過 5GB。
- 安全情報資料（Security Intelligence）超過 10,000 筆以上。
- 惡意網址及軟體（Malwares）超過 1 億筆。

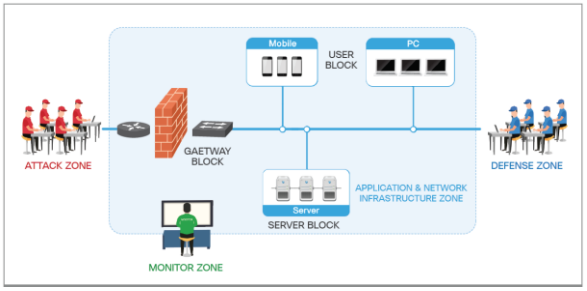
環境特色

思科 Cisco Cyber Range Service（數位靶場實戰服務）網路環境特色：

- 建置於組織及企業安全運作之實務模型，彙集人員、流程和技術在相對應的威脅場景。
- 專注於威脅的焦點，及防禦能力的驅動力，並注入思科雲端技術與安全情報資料

（Intelligence security services）及相關防禦管理工具。

- 使用虛擬環境，世界上任何地方都可以進行。
- 模擬完整的網際網路及企業網路，含伺服器、應用程式、安全設備及安全軟體，圖一為 Cisco Cyber Range Service（數位靶場實戰服務）網路環境圖：



圖一：Cisco Cyber Range Service 環境圖

服務規格

Cyber Range Service（數位靶場實戰服務）模擬基礎設施服務和攻擊防禦的實務環境，演練標準規格如表一：

Infrastructure	Attacks	Visibility and Control
• Wired, wireless, and remote access • Network and routing • Client simulator • Server simulator • Application simulator • Traffic generation	• Day 0 Attack/New threats • DDoS • Network reconnaissance • Application attacks • Data Loss • Computer malware • Mobile device malware • Wireless Attacks • Evasion techniques • Botnet simulation • Open source attack tools • Virtual Network Attacks	• Global Threat Intelligence(Cloud) • Firewall & IDS/IPS • Signature based Detection • Behaviour based Detection • Data Loss Prevention • Web & email Security • Application Visibility & Control • Wireless Security • Identity & access management • Security and event management • Event correlation • Packet Capture and Analysis • Virtual Network Security • TrustSec-SGT • Software Defined Network

表一：Cisco Cyber Range Service 服務規格表

- 安全管理團隊（Security Operation Center）人員的養成及演練。
- 安全分析技術人員的訓練。
- 降低潛在威脅的專屬能力。
- 模擬新的威脅手法（zero day）或訂定制止威脅手段的策略和技巧。