



ArgusHack

Next-Gen Breach & Attack Strategy Platform
(Next-Gen BAS)

在快速變化的資安環境， 企業需要更加靈活的資安量測。

入侵與攻擊模擬 (Breach and Attack Simulation, BAS)，經由 Gartner 解釋，是能夠在有限的風險下提供連續測試，並可用於警告 IT 和業務利益相關者，有關安全狀況方面的現有差距，或驗證安全基礎結構、安全規劃和防禦技術是否按期運行。

BAS 是一種資安驗證的解決方案，存在目的並非要取代既有第三方驗證。透過各項自動化技術為受測環境提供持續性測試，同時提升靈活性與降低成本，補足傳統驗證方案週期間的空隙，達到相輔相成，進而優化整個驗證流程。

企業可藉由 ArgusHack APT 的自動化技術，靈活且低成本的驗證企業資安建設，快速奠定團隊資安量能。而透過 ArgusHack Center，則可進一步配合 Red-Team / PT 服務，使演練測試變得靈活可控，並將珍貴的紅隊資源投入在刀口。

透過 ArgusHack，我們在不同資安建設程度中皆為企業提供了高效的解決方案，伴隨企業在不同的資安階段不斷成長。



ArgusHack

Center 攻擊演練中心

量測資安防護能力 節省資安演練人力

檢驗資安應變能量 持續測試新興威脅

適用情境：Red-Team 後

適用資安成熟度：A、B

持續積累資安能量

73% 降低
資安演練專家需求

160% 縮短
資安量測執行間隔

產品白皮書
white paper



適用週期

高

資安成熟度

低



ArgusHack

APT 先進戰役重現

檢視資安建設不足 熟練資安應變操作

驗證資安規劃成效 提升資安威脅經驗

適用情境：Red-Team 前

適用資安成熟度：B、C、D

高效奠定精實基礎

70% 節省
資安設備驗證時間

300% 提升
資安演練學習成果

產品白皮書
white paper



有關 730、731、732、733 的產品功能規格描述如下內容：

730 - ArgusHack AGH-Premium-APT 菁英戰役重現版一年訂閱授權：

演練平台將透過攜入伺服器進入內部網絡，在隔離的環境中設置多個靶機與攻擊控制器。這些靶機將安裝現有的資安防護軟體，並透過精心設計的劇本，重現駭客使用的未開源工具與攻擊行為，以全面檢驗資安防護的完備性。平台不僅模擬攻擊，更是重現真實戰役，這些演練能直接驗證資安團隊的健全性，強化應變措施，並助力資安團隊之培訓。

731 - ArgusHack AGH-Premium-Center 菁英攻擊演練版一年訂閱授權：

開放式演練平台可在測試區或正式環境中進行高度客製化的攻擊演練。透過介接第三方程式或自行撰寫腳本，能設計專屬的演練劇本，並將測試過的項目與手法儲存為劇本，方便未來的複測使用。這個平台如同即時戰略遊戲，隨時能發動真實且即時的駭客演練，並透過自動化攻擊重放功能，不斷校正，最終呈現企業專屬的資安防護演練報告。

732 - ArgusHack APT 攻擊鏈腳本授權：

APT劇本：模擬APT駭客組織的常用手法，結合FireEye、CrowdStrike、Cisco Talos等知名資安公司的研究與報導，統整出技術特點，製作KILL CHAIN連貫的演練攻擊劇本。

733 - ArgusHack 菁英攻擊演練腳本授權：

蒐集全球各類型駭客集團的攻擊手法，研發演練劇本，並根據演練類型及資安防護標的劃分為對外服務、電子郵件、端點、橫向攻擊、上網與DLP等多個演練面向模組劇本。