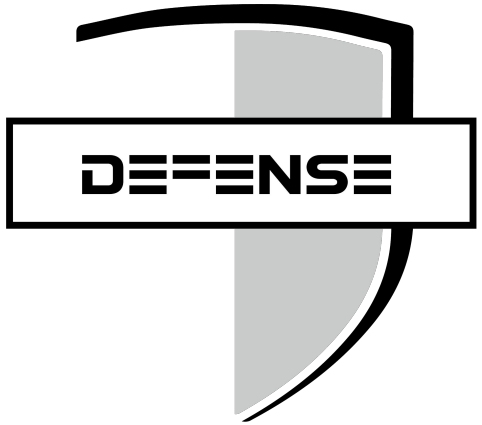


HITCON DEFENSE 2018

企業資安攻防大賽

指導單位:經濟部　主辦單位:台灣駭客協會/經濟部工業局　執行單位:台灣駭客協會/工研院

活動目的

HITCON Pacific 2018 以「Transforming:Cybersecurity and Resilience」為主題，聚焦於各式強韌性資安技術、安防措施等可加強企業關鍵系統的議題上，以期能協助企業與政府縮短資安事件造成的各層面影響。事實上，這幾年來，政府對於金融、國防、交通等關鍵基礎設施特別加強資安等級及規範，也相繼成立情資分享中心(ISAC)，讓防護體系更為完備。此外，對於政府對於資安人材培育及專業課程規劃，也漸有成效。今年，HITCON 預計在 12 月 14 日，舉辦 HITCON DEFENSE「企業資安攻防大賽」，此大賽將模擬企業所遇到的資安威脅，包含駭客入侵、蠕蟲擴散、資料外洩等情況，讓參賽隊伍在有限時間 內，利用自身能力和經驗，搭配各項資安設備，來解決問題，甚至更進一步，把解決後的問題，分享給其它隊伍，發揮情資分享精神。

此活動不僅將資安人材延伸到企業資安團隊，更可讓企業著重於面對資安威脅的解決能力，結合政府對於情資分享的重視，打造更健全及強韌的企業安全環境。

活動特色

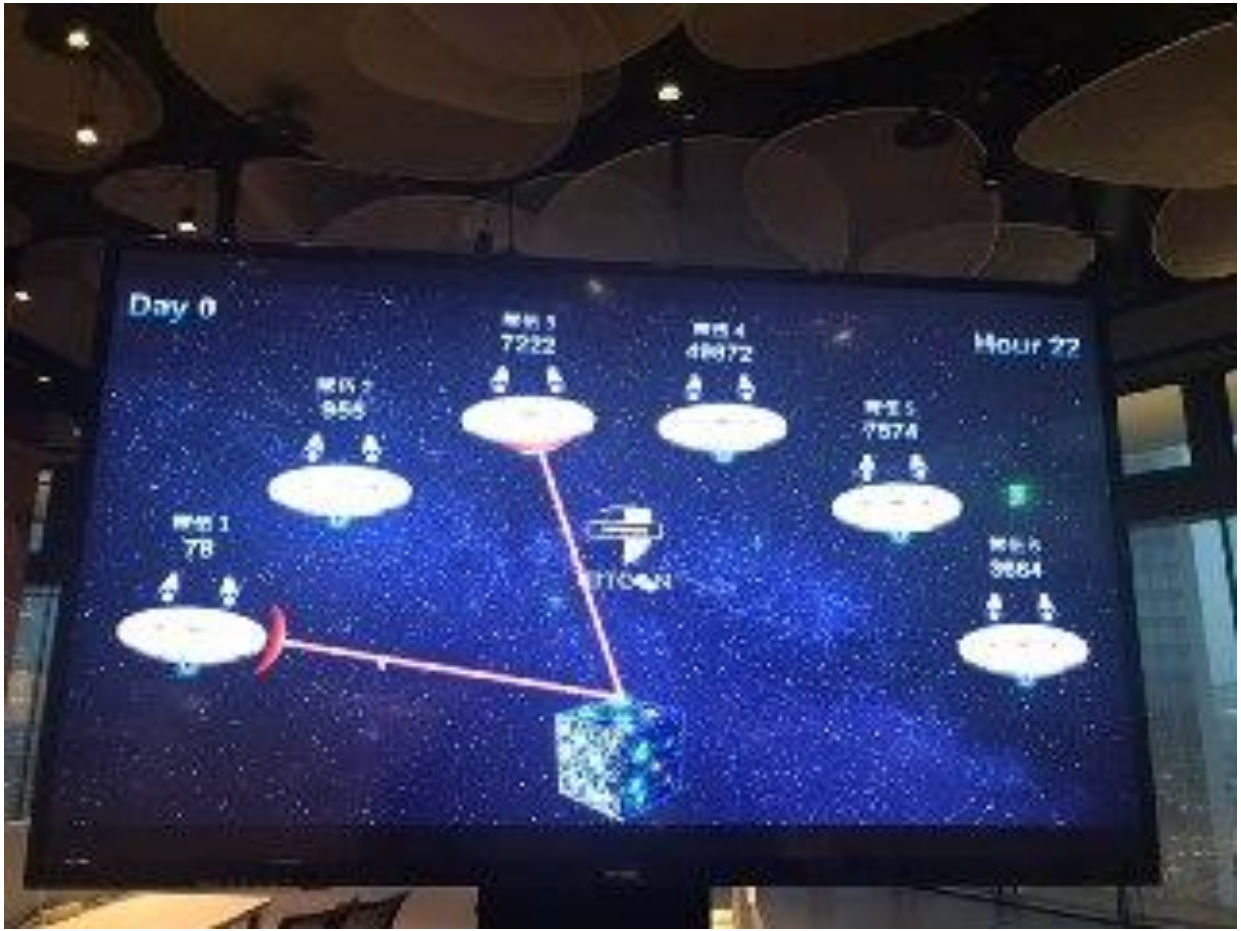
- 每一隊伍都是一個小型企業的 IT/資安 團隊
- 每一隊伍擁有完整的資安及網路設備，價值共超過三千萬新台幣
- 題目類型都是企業實際發生之案例，充滿各項挑戰，能充份發揮團隊能力
- 讓每一隊能了解維持企業網路及網站正常運作，可帶來企業實質營收
- 能讓參賽隊伍了解情資分享之重要性及精神

競賽方式(模擬資安團隊剛空降到某企業)

- 每隊 3~5 位，可攜帶筆電
- 提供每隊若干雲端主機服務，以及實體主機若干台
- 提供每隊數台桌機，並已模擬小型企業內部網路環境
- 每十分鐘，主辦方紅隊會嘗試入侵各隊，可能攻擊雲端服務或企業內部網路
- 每隊要在競賽限時內，將各種攻擊利用網路或資安設備，進行分析和阻擋
- 不得關閉外部服務或內部主機，也不可讓外部服務中斷
- 情資分享模式:
  - 每隊有兩次機會，可利用分數，與主辦方換得攻擊的情資，但僅可以換到已有隊伍分享的情資
  - 當解決任一道題目後，每隊可將此情資提供給主辦方，可額外獲得分數獎勵以及 30 分鐘的免戰，免戰期內，主辦方紅隊將停止攻擊該隊

計分方式

- 每隊需保護各自的伺服器，並確保服務不中斷
- 模擬真實時間，現時一分鐘等於比賽的1小時
- 伺服器營運會依照競賽時間產出不同分數
- 只要伺服器服務不中斷，每組分數就會依時間累積
- 伺服器的服務存在漏洞，每隔一段時間，主辦方紅隊會試著入侵，若被入侵成功則會被扣分，直到扣完分數為止
- 每隊的內部網路可能存在間諜或木馬軟體，若被主辦方紅隊盜取內部資料成功，也會持續扣分
- 競賽結束後，依累積分數，分發名次


Day 0
Hour 22
7222
7574
78
9864


Day 25
Hour 04
38
9572
7211
6850


WARNING: BIOCHEM ATTACK
BANDWIDTH
ENERGY
RPI CLIENT

klicKklacK

可立可資安

BORG

企業資安讀書會

aws


NETSCOUT
Arbor


PANDUIT
infrastructure for a connected world


EMC


GAIA
Information Technology


Hauman
豪 勉 科 技

TEAMT5

Persistent Cyber Threat Hunters

Pulse Secure®

力麗科技股份有限公司

LEALEA TECHNOLOGY CO.,LTD.

中國文化大學 資訊中心

中國文化大學推廣教育部

SCHOOL OF CONTINUING EDUCATION
CHINESE CULTURE UNIVERSITY