GSS Security Talk

【2025 叡揚資安趨勢講堂】

馬上報名

2025 叡揚資安趨勢講堂

遇入 2025 年下半年，企業正面臨前所未有的資安壓力與挑戰。AI 與雲端加速創新，同時也擴大了攻擊面與風險鏈，法規要求日趨嚴格，資安不再只是技術議題，而是企業治理的核心。從程式語言選擇到基礎架構遷移，從開發流程到威脅監控，每一環節都必須重新檢視與強化。我們將推出一系列線上研討會，帶您掌握資安趨勢與應變策略，協助企業在風險中找出轉型契機，建構更具韌性的資安體系。

議程場次

2025 / 八月場

線上研討會

美國網路安全暨基礎設施安全局（CISA）點名產品常見的安全問題：您中了幾個？

8/5(二) at 13:30－14:30

CISA 近期更新了『Product Security Bad Practices』報告，特別點名以 C/C++ 等語言開發的產品所帶來的記憶體安全嚴峻風險。然而，C/C++ 並非『不安全』，而是以其極致性能和靈活性，在關鍵系統開發中扮演無可取代的角色。

本場講堂將深入解析 C/C++ 記憶體安全問題的本質、常見弱點及其開發與修補建議。我們將探討如何有效規避 CISA 所警示的『Bad Practices』，為團隊建立"Starting Left"的基因，幫助企業實踐"Secure by Design"的承諾！

- CISA 『Product Security Bad Practices』Ver.2 更新重點剖析
- C/C++ 記憶體安全風險
- 記憶體安全問題的防禦策略
- 從預防「Bad Practices」到實踐「Secure by Design」

線上研討會

如何解決 JDK 移轉的潛藏成本？企業轉移 JDK 風險與實務

8/7(四) at 13:30－14:30

您是否有換過 JDK 卻碰到奇怪的問題導致置換失敗？越來越多企業開始考慮轉向開源版本的 OpenJDK。然而，這個轉換並不只是換一套 JDK 而已。它牽涉到法規遵循、相容性、效能、安全性與維運成本等層面。本場講堂將深入解析企業進行 OpenJDK 置換的關鍵挑戰與實務建議，協助您掌握替換過程中需要注意的風險與解法。

- 為什麼大家在討論 JDK 置換？
- 選擇 JDK 的建議要點
- JDK 技術挑戰與相容性
- 成功案例分享與轉換建議

線上研討會

2025 雲端資安新趨勢：生成式 AI 應用與風險

8/19(二) at 13:30－14:30

自 2023 年以來，生成式 AI 蓬勃發展。由於生成式 AI 所需的龐大運算資源與高度複雜的技術架構，越來越多企業選擇在雲端平台上部署 AI 模型與應用。然而，在享受彈性與效能的同時，企業也面臨前所未有的資安挑戰。

究竟該如何在雲端環境中安全、可控地使用生成式 AI 呢？本場講堂將帶您深入了解生成式 AI 應用的安全架構、潛在風險、攻擊路徑，以及企業如何透過現代雲端資安解決方案，如 CNAPP、AI-SPM、攻擊路徑分析等技術，有效守護 AI 資產與敏感資料。

- Orca Security 介紹
- Gen AI Security：OWASP Top 10 for LLM Applications
- AI Security Solutions Landscape
- AI-SPM 與關鍵建議

線上研討會

企業資安：透過威脅情報、行為分析洞察駭客攻擊

8/21(四) at 13:30－14:30

在這個數位時代，企業面臨的資安威脅日益嚴峻，駭客攻擊手法不斷翻新，讓資訊安全成為企業存續的關鍵挑戰。想像一下，我們就像《我的英雄學院》中的英雄們，必須時刻洞察敵人的動向，提前預知他們的攻擊計畫，才能在關鍵時刻做出防禦與反擊。就像《怪獸 8 號》的主角卡夫卡，擁有雙重身份，既是威脅也是守護者，我們也必須學會利用駭客的技術和戰術力量，化被動為主動，將威脅轉化為防護的利器。而《一拳超人》中埼玉那一擊必殺的迅速反應，更提醒我們在面對攻擊時，必須果斷且高效地啟動防禦機制，確保企業資訊安全無虞。本場講堂，我們將從這些英雄動漫的故事中汲取靈感，探討如何結合先進的威脅情報、行為分析與自動化防禦，打造企業的資安英雄，迎接未來更複雜的資安戰役。

- 入侵分析鑽石模型
- 暗網工具分享
- 看動漫學資安

線上研討會

AI 時代下的資安挑戰與應對：從合規到風險，如何掌握 AI 應用安全

8/26(二) at 13:30－14:30

生成式 AI 工具正快速滲透企業內部流程，當這些工具開始牽涉敏感資料、決策自動化甚至模型再訓練時，我們的資安策略是否跟得上？本場講堂將從「AI 實際應用」出發，揭示可能帶來的業務風險，並解析最新合規框架下企業應管理的面向。最後，我們也將介紹企業該如何落實治理，從模型透明度、輸入污染防範到合規報告產出。

- 現實中的 AI 應用案例
- 組織風險與業務衝擊
- 企業應關注的治理面向與法規趨勢
- 現有可行的治理手段

線上研討會

行動應用成為新端點風險，企業需邁向自動化檢測新時代

8/28(四) at 13:30－14:30

隨著行動應用成為主要的服務介面，App 本身即是新的「攻擊面」。傳統以程式碼掃描或人工滲透為主的安全測試方式，已難以應對現今快速交付、跨團隊協作、多版本同時運營的情境。

本場講堂將介紹如何透過黑箱自動化測試方案，全面的靜態 (SAST)、動態 (DAST)、互動式 (IAST)分析，快速洞察應用程式中潛藏的安全風險、誤設配置與資料外洩行為，即使無需原始碼，也能有效提升 App 的防禦成熟度。

- 探討行動 App 的風險演進
- 傳統 App 測試方法的盲區
- 自動化測試的技術與效益

2025 / 九月場

線上研討會

2025 最新 App 資安趨勢與挑戰，企業該如何應對？

9/2(二) at 13:30－14:30

隨著 App 攻擊趨勢日益嚴峻，企業必須掌握最新的資安威脅與防護措施。本場講堂將分享最新資安資訊，協助企業掌握第一手的資安趨勢，並且參照目前 App 防護的最佳安全策略，採取措施來保護應用程式的安全與穩定。

- 資安趨勢分享
- 安全防護策略

報名資訊

- **講堂時間**：2025/8/5-2025/9/2，共 7 場，以各議程時間為主。
- **報名期間**：2025/7/1-2025/8/18 12:00
  - 請留意每場次最晚報名期限為前一天 12:00
- **報名流程**：
  - 於報名頁中勾選欲參與之議題
  - 報名後主辦單位將進行審核，若報名成功將會收到報名成功之信件通知
  - 各場次將於當日寄出會議連結，議程開始前十分鐘開放進入線上會議室，敬請留意信件
- **講堂形式**：線上研討會（Webinar）
- **活動備註**：
  - 任何問題歡迎來信洽詢：mktsecurity@gss.com.tw
  - 叡揚資訊保有活動及議程變更之權利。

馬上報名

GSS 叡揚資訊
台灣資訊軟體業領導廠商．雲端 SaaS 服務業界先驅．助力企業守護數位資產
台北德惠｜創富研發中心｜高雄研發中心
海外據點：上海　營業範圍：兩岸三地、日本
Tel：(02)2586-7890｜service@gss.com.tw