

GSS Security Talk

【2025 叢揚資安趨勢講堂】

[馬上報名](#)

2025 叢揚資安趨勢講堂

【2025 叢揚資安趨勢講堂】隆重登場！全新一年，我們再次聚焦「資安領域最新趨勢、議題與挑戰」，伴隨數位化的進程加速，企業所面臨的網路安全威脅愈加隱匿且多樣，如何有效應對這些挑戰，已成為每個人不可忽視的關鍵課題。

在本系列講堂中，叢揚資安團隊將結合豐富的實務經驗與前瞻洞察，深入剖析網路攻擊的最新趨勢，從多元視角探討有效的應對策略。以協助企業制定防禦策略、分享情報、提升資安意識等技能。期待各位在這場數位攻防戰中，共創一個更加安全的資安藍圖。

叢揚資安趨勢講堂-場次

2025 / 二月場

 線上研討會

從零開始：打造無懈可擊的 SSDLC 實戰指南

2/11(二) at 13:30 – 14:30

在數位轉型過程中，企業導入 Zero Trust 安全架構，以「永不信任，始終驗證」原則管理資源存取，防範內外部威脅。同時，透過 SAST（靜態應用程式安全測試）於開發初期檢測程式碼漏洞，並使用 SCA（軟體成分分析）檢查第三方元件安全，降低供應鏈風險。此外，企業推動資安教育訓練，將資安意識融入文化中，有效構建安全、穩定的開發環境，迎接未來挑戰。

- SSDLC 各階段的重點與實務操作
- 常見的 SSDLC 挑戰與解決方案
- 成功導入 SSDLC 的企業案例及經驗分享

 線上研討會

打破傳統：管理網路可以很 Easy

2/13(四) at 13:30 – 14:30

攻擊已進入 AI 生成時代，傳統的縱深防護已不足以應對新式的網路攻擊。結合傳統縱深防護與新式橫向防護的網路微分段技術，成為企業網路安全的創新解決方案。透過網路微分段，企業可以更精細地管理網路，大幅減少攻擊面，有效提升網路彈性，從單線防護變成全面防護，大幅提升企業的網路防護等級與攻擊變能力。

- 突破傳統：賦予企業網路安全韌性
- 從網路微分段角度配合實際演示說明如何提升網路管理彈性

 線上研討會

從漏洞到勝利：Secure Code Warrior 如何幫助企業掌控生成式 AI 的兩面性

2/18(二) at 13:30 – 14:30

在生成式 AI 加速軟體開發的時代，企業面臨前所未有的資安挑戰與機會。本次線上研討會將深入探討生成式 AI 的兩面性，並聚焦於如何透過 Secure Code Warrior，協助開發團隊化解危機、掌握先機。我們將分享從漏洞到勝利的關鍵策略，助力企業構築堅實的資安堡壘！

- 生成式 AI 與企業資安管理的趨勢與挑戰
- 落實生成式 AI 資安策略的三大步驟

 線上研討會

解析 2024 雲安全風險報告與雲新興 AI 應用與風險

2/20(四) at 13:30 – 14:30

隨著雲端技術與生成式 AI 的快速發展，企業面臨日益複雜的資安挑戰。本次研討會將聚焦 Orca Security 2024 年雲安全風險報告，解析當前及新興風險，並探討生成式 AI 等新技術的資安挑戰與應對策略，協助企業在變動的風險環境中做好防護。

- 2023-2024 年雲安全洞察與未來趨勢
- AI 未來發展與資安風險解析

 線上研討會

從理論到實踐：政府機關的 SBOM 應用與防護策略

2/25(二) at 13:30 – 14:30

在當今數位時代，政府機關正面臨前所未有的資安挑戰。為了確保軟體供應鏈的透明性、安全性與合規性，我們將為您提供全方位的軟體物料清單（SBOM）解決方案，幫助您有效管理軟體風險，應對相關法規要求，並保障資安防護措施的到位。

- SBOM 解密：國際與主管機關關注的核心議題
- 缺少SBOM管理的風險：案例深度剖析
- 從策略到實施：打造全面的 SBOM 管理計劃

 線上研討會

提升 Java 效能的最佳實踐：穩定、高效的全方位策略

2/27(四) at 13:30 – 14:30

本次線上研討會將深入探討 Java 效能最佳實踐，從 JVM 運作原理到代碼優化技巧，結合效能分析工具與實戰案例，講解調整 JVM 參數、優化垃圾回收策略等實用方法。此外，將介紹 Zing JDK 的核心功能與優勢，展示如何實現高效優化、低延遲啟動與穩定運行，協助企業全面提升 Java 應用效能以滿足業務需求。

- Java 效能調整瓶頸的難處
- 效能調整案例分享

2025 / 三月場

 線上研討會

自動化測試的第一步：從手動測試到自動化的轉型之路

3/4(二) at 13:30 – 14:30

在軟體開發快速迭代的時代，手動測試已無法跟上需求變化，且重複性測試不僅耗費大量人力，也難以確保產品品質的穩定性。如何邁出自動化測試的第一步？是許多團隊轉型中的最大挑戰。這次研討會將引導您了解如何逐步實現測試流程的智慧化與自動化，讓測試不再只是重複操作，而是提升產品品質與加速交付的關鍵助力！

- 自動化測試的基本概念與好處
- 從手動測試逐步邁向自動化的實用策略
- 工具介紹：如何透過 CT 實現自動化測試

 線上研討會

應對Desktop & Embedded裝置中的網路安全威脅：從程式碼保護到資料完整性

3/6(四) at 13:30 – 14:30

隨著物聯網和嵌入式設備的廣泛應用，以及桌面應用程式的持續發展，程式碼混淆已成為保護智慧財產權和防止逆向工程的關鍵技術。同時，桌面應用程式和嵌入式設備正面臨日益嚴峻的網路安全威脅，包括程式碼竊取和資料篡改。本次研討會將討論如何透過程式碼混淆、執行時間應用程式自我保護（RASP）和白箱加密等技術，全面提升桌面和嵌入式系統的安全防護能力，重點關注智慧財產權保護、程式碼完整性、資料機密性，以及安全通道的認證與授權機制金鑰保護，幫助開發者建立更安全的系統。

- 資安現況及挑戰
- 該如何全面保護桌面應用程式和嵌入式設備

[馬上報名](#)

報名資訊

• 講堂時間：2025/2/11-2025/3/6，共 8 場，以各議程時間為主。

• 報名期間：2025/1/6-2025/3/5 12:00

◦ 請留意每場次最晚報名期限為前一天 12:00

• 報名流程：

- 於報名頁中勾選擬參與之議題
- 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

◦ 叢揚資訊保有活動及議程變更之權利。