【專訪】不眠不休邁向全球冠軍之路：
亞特蘭大隊如何完勝人工智慧網路挑戰賽

在全球規模最盛大的 AI 資安攻防競技 - 人工智慧網路挑戰賽（AIxCC）優勝名單揭曉前夕，拉斯維加斯會場一片寂靜，眾人屏息以待，緊張氛圍瀰漫全場。

所有人目不轉睛、緊盯螢幕，等待冠軍得主出爐。當亞特蘭大隊隊徽出現在螢幕上，全場爆出如雷的掌聲與歡呼。匯聚兩年的不懈努力與決心，該團隊精彩完勝世界級對手，抱回四百萬美元的冠軍獎金。

▲亞特蘭大隊勇奪 AI 網路挑戰賽冠軍

三星新聞中心專訪來自三星研究院安全與隱私團隊的 Taesoo Kim 和 Joonun Jang，以及來自 AI 生產力團隊的 Yunjae Choi，帶領讀者回顧激勵人心的冠軍之路。

▲（左起）隸屬三星研究院的 Taesoo Kim、Joonun Jang 和 Yunjae Choi

亞特蘭大隊：由 40 多位頂尖研究人員、工程師和駭客組成的全球聯盟

「人工智慧網路挑戰賽」是美國國防高等計畫研究署（DARPA）主辦的一項全球資安技術競賽。本屆賽事在 Google、Microsoft 和 OpenAI 等科技巨擘贊助下，總獎金高達 2,250 萬美元。亞特蘭大隊的靈魂人物 Taesoo Kim，負責籌組並率領團隊征戰四方。其 40 多位成員橫跨三星研究院、美國喬治亞理工學院（Georgia Tech）、韓國科學技術院（KAIST）、浦項工科大學（POSTECH）及其他世界一流機構，匯聚成一支堅強陣容的資安菁英隊伍。

▲ Taesoo Kim 闡述激勵團隊接受挑戰的動力來源

Kim 身兼美國喬治亞理工學院教授，在獲悉該「人工智慧網路挑戰賽」後，第一時間聯繫多位昔日門下博士生，鼓勵他們加入參賽團隊。這些得意門生在短短的時間內，便成為亞特蘭大隊的核心成員。

在 Kim 的強力號召下，亞特蘭大隊集結來自韓國各地及美國東西岸的菁英。他回憶道：「由於團隊成員分布在世界各地，我們依據每位成員的狀況建立合作框架。韓國當地的一些同仁，甚至在百忙中抽空前往喬治亞理工學院，使團隊成員得以並肩作戰。」

亞特蘭大隊如何在競爭中脫穎而出

「人工智慧網路挑戰賽」是一項以識別和修復大型軟體系統為主題的競賽。其最終目標在於加速開發基於 AI 的資安技術，用以保護交通、能源和醫療照護等關鍵基礎設施。在最後一輪對決中，參賽隊伍的任務是建立一套以 AI 驅動的「網路推理系統（CRS）」，能自動偵測軟體漏洞，並產生安全修補程式。

比賽積分分為「漏洞發現」與「程式修復」兩大部分：團隊若能精準識別特定程式碼當中的弱點，便能獲得發現積分；若能成功修補弱點，便能累積修復積分。簡言之，團隊積分反映其系統能多快偵測組織來源碼當中的漏洞、成功偵測到的漏洞數量、以及漏洞修復的準確性。

▲冠軍獎盃與亞特蘭大隊的優勝積分卡

亞特蘭大隊以壓倒性優勢奪冠，不僅發現為數更多的漏洞，且能更準確地修補漏洞，遙遙領先競爭對手。

Jang 負責監督為偵測 Java 程式漏洞，而開發的大型語言模型（LLM）代理程式，他解釋比賽期間在該代理程式的助攻下，亞特蘭大隊系統成功偵測到更多漏洞。他指出：「團隊成員各以不同方式開發並整合這些代理程式，讓我們得以建構出涵蓋廣泛弱點的系統。」

▲ Joonun Jang 闡述亞特蘭大隊為偵測 Java 程式漏洞而開發的 LLM 代理程式

Choi 負責開發能在漏洞發現的同時，隨即自動修補漏洞的 AI 代理程式。他指出：「由於 AI 是提供給所有參與者的通用工具，因此真正的技術優勢，取決於如何高效運用 AI。團隊面臨的關鍵性挑戰，是打造能針對新發現的漏洞，而靈活因應的 AI 代理程式。」

▲ Yunjae Choi 闡述亞特蘭大隊為自動修補漏洞而開發的 AI 代理程式

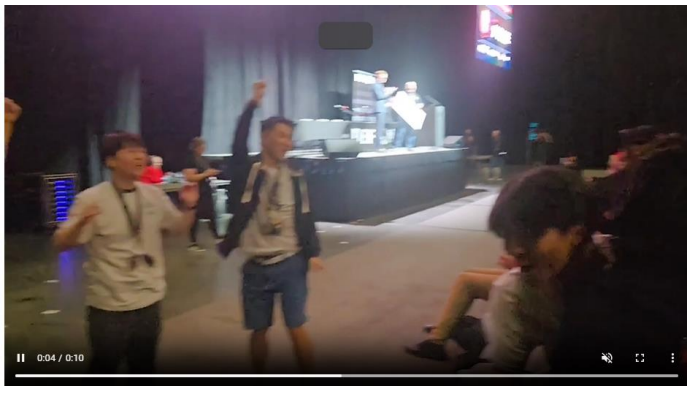
度秒如年的等待

決賽當天，晉級的七支隊伍齊聚拉斯維加斯，等待最終成績揭曉 - 參賽兩年的心血成果。作為全球規模最盛大的網路安全競賽，該賽事匯聚來自全球各地的頂尖隊伍，緊張與期待之情溢於言表。直至揭曉第三名、第二名得獎主，亞特蘭大隊仍遲遲未被唱名。

「鑑於眾多優秀隊伍參賽角逐，若能躋身前三強，已稱得上是一項豐功偉業。所以在冠軍揭曉之前，我一方面感到憂心，一方面抱持謹慎樂觀的態度。」

最終，當亞特蘭大隊隊徽躍上螢幕、確認奪冠的那一刻，台下頓時歡聲雷動。Choi 說：「原以為這只是個奢望，意識到我們真的奪下冠軍時，整個團隊欣喜若狂。」

Kim 回憶道：「兩年的備賽時間，短得如一閃而過的電光，而等待成績揭曉的一小時，卻有如一世紀般漫長。」



▲亞特蘭大隊被宣布奪下 2025 AI 網路挑戰賽冠軍的光榮時刻

他補充：「就在截件日期前夕，我們赫然發現先前提交的系統，雖然進度超前，但卻存在一個嚴重錯誤，每每回想這段經歷，我仍感到激動不已。我們瘋狂地工作到最後一刻。為解決問題，我甚至不得不在凌晨 5

點叫醒整個團隊。光是回想，就令我不寒而慄。」

▲（左起）Taesoo Kim、Yunjae Choi 和 Joonun Jang

三星對 AI 資安擘畫的未來願景

隨著摘下 AI 網路挑戰賽冠軍榮銜，三星再次彰顯其在 AI 資安領域的技術領先地位，及獨步全球的競爭優勢。展望未來，三星將持續精進新世代 AI 資安解決方案，進一步提升自主識別和解決漏洞的能力。

Kim 在受訪時表示：「三星的 AI 資安技術已被廣泛應用於強化產品和服務防護，包括 Galaxy 裝置和 AI 智慧顯示器。透過持續性的開源貢獻，以及積極的社區參與，鞏固我們在 AI 資安領域的全球領先地位。」