Samsung Project Infinity 團隊：為天下用戶築起網路防護罩

自 Galaxy S24 系列起，三星提供**長達七年的行動安全更新**(註一)。此為目前行動裝置可享的最長安全支援年限，讓消費者透過一次次的更新，更無後顧之憂地使用手機。

置身萬物互聯的新世代，網路威脅無所不在；且亡羊補牢往往為時已晚，網路安全儼然已成為一門重要課題。未來四年的全球網路犯罪損失，預計將從 2024 年的 9.22 兆美元，飆升至 2028 年的 13.82 兆美元(註二)。有鑑於此，使用獲得防護生態圈加持的裝置至關重要 - 例如安全更新。

然而這些安全更新，究竟從何而來？手機為何頻繁地跳出此通知？Samsung Project Infinity 是三星內部成立的專責單位，為三星行動通訊事業部賴以運作的核心。三星新聞中心專訪來自 Samsung Project Infinity 的專家小組，了解這群幕後英雄如何全天候守護 Galaxy 裝置與用戶。

深入探索未知的危險

網路威脅情報(CTI)工作小組是 Samsung Project Infinity 內部的偵察單位，分為紅色(RED)、藍色(BLUE)和紫色 (PURPLE) 三大團隊，旨在走出實驗室環境，辨別現實世界中的危險。RED 和 BLUE 分別負責攻擊和防禦，尋找安全弱點並採取因應措施。PURPLE 則屬於特殊作業單位，在特定的關鍵領域扮演攻防雙重角色。這些團隊策略性地部署於世界各地，包括越南、波蘭、烏克蘭和巴西。

他們暗中行事、秘密出行。唯有收到含有安全修補程式的更新時，方能察覺到他們的存在。

CTI 的職責在於隨時掌握最新風險，偵查潛在的威脅、阻止駭客控制用戶裝置。它們致力阻擋惡意行為，避免駭客販售其所竊取的資料，確保智慧型手機或平板的安全性完全掌控在使用者手中。

該工作小組負責保護 Galaxy 內部基礎架構，守護消費者數據和通行憑證等員工資料；因為任何被駭客竊取的機密資料，都可能遭到販售或盜用，進而引發另一波的攻擊。

為了識別潛在的威脅並採取因應措施，CTI 經常探訪充斥大量安全漏洞、間諜軟體、惡意軟體、勒索軟體、非法工具、企業和客戶機密資訊的交易市集 - 例如深網（Deep Web）和暗網（Dark Web）。

三星電子副總裁暨行動通訊事業部安全團隊負責人 Justin Choi 是 CTI 的掌舵者。Choi 在美國科技產業累積二十餘年的專業經驗，是網路安全領域的權威與道德駭客，他與世界各地的金融和科技巨擘攜手合作，強化安全防護機制。Choi 在識別及緩解零時差威脅方面的專業知識，為開發進階安全措施注入強大動力，守護全球逾十億 Galaxy 使用者。

Choi 指出：「進行安全研究時，我們有時會模擬真實世界的交易。我們密切關注地下論壇和交易市場，監控鎖定針對 Galaxy 裝置的零時差或 N-day 漏洞攻擊，以及可能成為系統滲透破口的任何外洩情報。」

身為一名熟知入侵網路之道、協助識別並解決漏洞的道德駭客 - 或稱為「白帽」駭客，Choi 解釋系統內的任何可疑行為，都能從蛛絲馬跡之中快速追溯攻擊來源。

例如要求的權限過多、異常行為以及來自未知伺服器的網路流量，都可能是潛在違規行為的跡象，此時 CTI 會追蹤這些入侵指標，藉以識別威脅行為者和攻擊目的。

CTI 成員 Ranger（Samsung Project Infinity 員工以別名掩飾真實身份，避免自己成為駭客的目標）談到：「我們一旦發現這些類型的威脅，便與開發人員和業者合作，展開全面封鎖以防止攻擊。為杜絕任何風險事件發生，我們甚至透過私密管道，與其他部門和合作夥伴進行溝通。」

CTI 亦研究威脅行為者以破解其行為模式。了解他們的動機和目標，有助於揭示其攻擊手法，並為安全防禦提供見解。

另一名 CTI 成員 Tower 補充：「有時，攻擊是出於經濟或政治動機，有時純粹是為了炫技。」

在威脅成形之前，早一步清除殆盡

雖然即時威脅偵測至關重要，但強大的攻擊安全策略，亦不容忽視。RED 和 BLUE 以軍事實務作為靈感來源，其中紅隊模擬敵方攻擊，藍隊負責建立安全防線，以因應不斷變化的威脅。在三星採取的方法當中，RED 模擬駭客攻擊並設計新的攻擊場景，以辨別潛在的漏洞；BLUE 則開發並部署修補程式，防範這些安全漏洞。

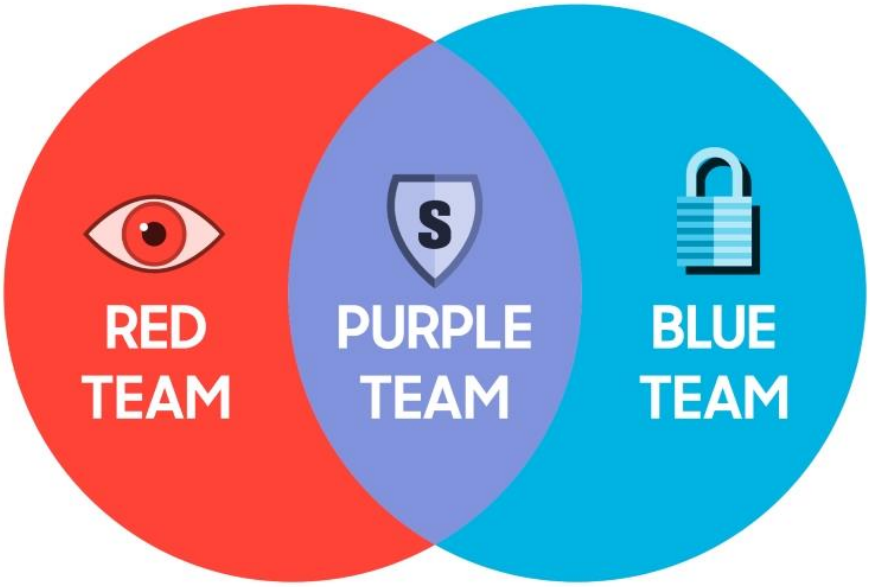
這些團隊專門打擊零時差攻擊，在漏洞遭到利用之前，早一步完成修補，防止未經授權的存取或數據洩漏。2020 年發生的 Pegasus 間諜軟體入侵，使作業系統成為易被攻擊的目標，是著名的數據洩露事件之一。

RED 小組將調查 Galaxy 裝置作為啟動專案的第一步。組員不斷使用和分析 Galaxy 中的新功能，深入研究最近揭露的漏洞，並預想以用戶為對象的潛在安全威脅。該小組進行各種研究，一旦鎖定會對實際 Galaxy 使用者構成任何潛在風險的目標，RED 小組便會開始偵測目標中的零時差漏洞。

RED 成員 Arrowhead 說：「模糊測試是我們執行的其中一項任務。這一項測試會向軟體發送各種意想不到的數據，藉以找出任何隱藏的缺陷。」

諸如程式碼稽核、靜態和動態分析等其他方法，則有助於全盤了解系統的健全與安全性。該團隊考量日常場景中的種種威脅，使 Galaxy 裝置遠離這些風險。

「鬧鐘存在缺陷時，急迫性並不高；但若位置數據出了差錯，可能導致某用戶在不知不覺中，經由其隨身裝置被人一路跟蹤。一旦發現假設性的安全漏洞，我們會立即進行修補，並針對相關型號推出更新。」BLUE 成員 Gate 補充。



專家中的專家

PURPLE 身兼攻擊與防禦角色，確保重要區域的安全性 - 亦即 Galaxy 裝置的關鍵功能。顧名思義，PURPLE 兼具 RED 和 BLUE 二者技能，但對於行動裝置內建的安全機制，卻有著更深一層的了解，使其成為箇中佼佼者。

PURPLE 成員 Sphinx 分享：「三星與外部安全研究人員合作，共同發現安全漏洞，而我們對 Galaxy 系統更瞭若指掌，因此我們能更有效率地鎖定潛在弱點。」

另一位 PURPLE 成員 Oracle 補充：「當你愈了解系統，愈能妥善防護它。」

有時，PURPLE 需處理其他人無法解決的問題，包括提出新的安全規範、設計和功能。不過，這不僅關乎使 Galaxy 裝置和 Samsung Knox 安全平台維持良好狀態，三星亦根據晶片組和網路供應商的要求，為其提供相關建議和解決方案。

三星穩坐硬體龍頭寶座，此地位意味著三星不僅有能力擴大安全創新，還能加惠其安全供應鏈。因此，Galaxy 正為新世代晶片的安全性做出貢獻。

此工作背後的動機，有時無關乎科技，這點可能令人感到意外。PURPLE 成員以保護消費者安全為己任，發掘和解決安全漏洞，使其產生一種自豪和滿足感。

Oracle 繼續補充：「使用 Galaxy 裝置的人，不僅只有我而已，還包括我的家人和朋友。所以，確保使用安全性，已成為團隊的使命！」

團隊的進入門檻很高，單有精湛的技術並不足夠。欲成為團隊的一員，亦須展現崇高的品格，因為團隊發現的任何安全漏洞，都可能被不肖人士趁機牟利。

Choi 指出：「團員須堅忍不拔，品性端正。除了責任感，亦須將使用者的利益，置於個人利益之上。」

Sphinx 補充道：「身為科技早鳥，具備掌握趨勢的深厚涵養，亦是有利的加分項。」

防護體系

CTI、RED、BLUE 和 PURPLE 是 Galaxy 資安策略的重要組成，但 Samsung Project Infinity 亦同時採行諸多措施，包括三星行動安全獎勵計劃，藉由與資安社群的廣泛合作，進一步審查 Galaxy 的防禦力。

今年，三星頒布高達 100 萬美元的獎勵金推行計劃，鼓勵各路高手找出 Galaxy 裝置最嚴峻的攻擊場景 - 創下三星安全計畫史上最高的獎金紀錄。

Choi 提到：「在網路攻擊手法日益精進的世界，鼓勵資安社群加入行列，合力識別潛在的漏洞尤為重要。」

三星長期以來與數百家夥伴合作，包括電信業者、服務供應商、晶片組供應商等，此合作模式是促成這一切的關鍵。Samsung Project Infinity 積極與夥伴及廣泛的社群攜手合作，揪出安全威脅並開發修補程式，確保三星實施各項舉措並承擔企業責任，以強化自身的不足之處。

Choi 補充：「三星人才濟濟，專家陣容強大，但這並不表示三星拒絕與外界合作。借助眾人的敏銳目光，資安漏洞將無所遁形，有助於提升使用者安全。」

現在，得知手機跳出的通知，來自於守護用戶安全的盡責團隊，
您是否還會一如既往地忽視它？

每一條通知，都象徵著三星為維護顧客的資料安全堅持不懈的努力。

下次看到更新通知時，請別躊躇猶豫。只需輕觸「安裝」選項，便能繼續安心悠遊網路，因為有一個完整團隊為您全力戒備。

註一：三星 Galaxy 裝置安全更新版本的釋出時間與供應性，可能因市場、網路供應商及 / 或型號而異。
註二：資料來源 Statista Market Insight「Cybercrime Expected To Skyrocket in Coming Years」統計圖表 Chart: Cybercrime Expected To Skyrocket in Coming Years | Statista。