出國報告（出國類別：其它）

國防部赴日參加「國際網路安全防護年會-國際資安會議藍色代碼CODE BLUE」公務出國報告

服務機關：國防部參謀本部通信電子資訊參謀次長室

姓名職稱：李玉璞參謀官

派赴國家：日本

出國期間：113年11月12日至11月16日

出國報告審核表

出國報告名稱：國防部赴美參加「國際網路安全防護年會-國際資安會議 CODE BLUE」		
出國人姓名 （2 人以上，以 1 人為代表）	**職稱**	**服務單位**
李玉璞	上校參謀	國防部參謀本部通信電子資訊參謀次長室
出國類別	☐考察 ☐進修 ☐研究 ☐實習 ☑其他 國際會議 （例如國際會議、國際比賽、業務接洽等）	
出國期間：113 年 11 月 12 日至 113 年 11 月 16 日		**報告繳交日期：**113 年 12 月 20 日

出國人員自我檢核	計畫主辦機關審核	審　　核　　項　　目
☑	☑	1.依限繳交返國報告
☑	☑	2.格式完整（本文必須具備「目的」、「過程」、「心得及建議事項」）
☑	☑	3.無抄襲相關資料
☑	☑	4.內容充實完備
☑	☑	5.建議具參考價值
☑	☑	6.送本機關參考或研辦
☑	☑	7.送上級機關參考
☐	☐	8.退回補正，原因：
☐	☐	（1）不符原核定出國計畫
☐	☐	（2）以外文撰寫或僅以所蒐集外文資料為內容
☐	☐	（3）內容空洞簡略或未涵蓋規定要項
☐	☐	（4）抄襲相關資料之全部或部分內容
☐	☐	（5）引用其他資料未註明資料來源
☐	☐	（6）電子檔案未依格式辦理
☐	☐	（7）未於資訊網登錄提要資料及傳送返國報告電子檔
☑	☑	9.本報告除上傳至返國報告資訊網外，將採行之公開發表：
☐	☐	（1）辦理本機關返國報告座談會（說明會），與同仁進行知識分享。
☐	☐	（2）於本機關業務會報提出報告
☑	☑	（3）其他 **本案為行政院數位發展部「數位產業國際合作與輸出拓展及資安演訓先導計畫」之項目，於計畫執行完畢後將提供數位發展部辦理運用。**
☐	☐	10.其他處理意見及方式：

出國人簽章（2 人以上，得以 1 人為代表）	**計畫主辦機關審核人**	**一級單位主管簽章**	**機關首長或其授權人員簽章**

摘　要

本次訪團屬國科會計畫案，係遵行政院國家科學技術發展基金管理會 113 年 6 月 28 日「數位產業國際合作與輸出拓展及資安演訓先導計畫」政策指導辦理，赴美國參加 11 月 12 至 16 日「國際網路安全防護年會-國際資安會議藍色代碼(CODE BLUE)」，本部由參謀官李玉璞等 5 員與會，依職務範圍參加 17 類議程，汲取先進國家網通安全科技新知，並掌握其應對網駭威脅作業技巧及資安事件應處方法，以精進國軍資安防護管理運作機制與應變處置能力。

目　　次

國防部赴美參加「國際網路安全防護年會-東亞區國際資安會議藍色代碼CODE BLUE)」公務出國報告

壹、依據：

依數位發展部資通安全署 113 年 6 月 28 日資安稽核字第 1134000279 號函「行政院國家科學技術發展基金管理會之數位產業國際合作與輸出拓展及資安演訓先導計畫」辦理。

貳、目的：

本部藉參與「國際網路安全防護年會」，汲取先進國家網通安全科技新知，並掌握其應對網駭威脅作業技巧及資安事件應處方法，以精進國軍資安防護管理運作機制與應變處置能力。

參、活動概要：

一、 任務編組及訪團行程：

(一)任務編組：

本次研討會由通次室資戰處參謀官李玉璞等 5 員前往。領隊分配成員負責之議題類別，於行前蒐整及研讀議程相關資料，研討會期間各自負責議題記錄及資料整理，返國後共同完成報告撰擬。

(二)訪團行程：

自 113 年 11 月 12 日上午出發前往日本東京,後於 11 月 14 日至 11 月 15 日 Bellesalle 高田馬場(住友不動產新宿花園塔 B2/1F) 參與東亞區國際資安會議 CODE BLUE，於 11 月 16 日出發返國，實際行程計 6 日(含航程)。

二、 活動說明：

(一)東亞區藍色代碼(CODE BLUE)

在過去的多年來，CODE BLUE 國際安全會議為全球資安人才提供了一個高水準的交流平台，讓專家學者分享最新的研究成果，並促進各界深入合作，共同應對日益嚴峻的資安挑戰。隨著全球網路攻擊手法的多樣化與複雜化，持續關注資安的未來發展趨勢，已成為業界和學界的共同目標，以確保資安策略能有效應對不斷變化的威脅。

參與 2024 年 CODE BLUE 的主要目的是深入了解最新的攻擊向量與防禦技術，並透過專家演講及實作課程掌握資安行業的最前沿技術。此外，CODE BLUE 也是一個不可多得的交流機會，與來自全球的資安專業人士建立連結，交換實戰經驗，並探索新興的資安工具與技術解決方案。這些寶貴的學習與合作將有助於提升自身的專業能力，並為未來的安全挑戰做好準備。

三、 議程概述：

(一)CODE BLUE 議程重點：(議程表如附錄 1)

1. 人工智慧用於形式化驗證；AI 的形式驗證：

講者主要談論了兩個主題，是關於人工智慧如何應用於形式驗證，以及形式驗證如何反過來提升人工智慧的安全性及可靠性；並介紹「安全」和「資安」在英文中的區別，點出隨著 AI 系統的日益強大，兩者界線逐漸模糊，在議程中提出無人機作業系統的案例說明，以驗證如何確保軟體安全；進一步介紹了 AI 如何自動化形式驗證的過程，並以 GPD4 和 DeepSeed Prover 為例，說明 AI 在自動化軟體和數學證明方面的進展，也強調，雖然 AI 自動生成程式碼可

能帶來資安風險，但透過 AI 生成並驗證程式碼，可以確保軟體的正確性和安全性。

講者所提出的安全(Safety)與資安(Security)的差異:在英文中，「安全」和「資安」是兩個不同的概念。安全指的是保護系統免於意外或錯誤，而資安則是指保護系統免於惡意攻擊;舉例來說,如果無人機因為程式錯誤而墜毀，這是安全問題；但若無人機被駭客入侵並操控，這就是資安問題。

AI 如何自動化形式驗證；講者分享了兩套 AI 系統，AI 在自動化形式驗證方面展現出巨大潛力，例如 GPT-4 在未經特殊訓練下能自動完成 SEL4 微核心程式碼中 15.8%至 51.8%的證明，而 DeepSeed Prover 更在 14 個月內將數學證明的自動完成率從不到 30%提升至超過 60%，顯示 AI 可大幅縮短驗證時間並提高軟體和硬體的可靠性。

AI 自動生成程式碼的潛在風險；軟體的正確性建立在硬體正確運作的基礎上。如果硬體本身存在缺陷，那麼即使軟體經過嚴格驗證,也無法保證系統的安全性。演講者以 CPU 設計驗證為例，說明形式驗證如何確保硬體的正確性。

2. **操控 Edge Copilot：**

雖然 Copilot 的設計目標是安全可靠，但講者發現 Bing 搜尋引擎擁有過於寬鬆的 API 訪問權限，例如可直接訪問 Chrome 瀏覽器的 Split Tab 和 NTP（新分頁）API。這些 API 原本不應被 Bing 搜尋引擎直接訪問，因為可能被攻擊者用於繞過彈出視窗攔截器或將惡意程式碼注入 Copilot，從而執行惡意操作，對系統安全構成潛在威脅。

Copilot 在處理與網頁內容相關的使用者查詢時，會將網頁內容傳送至 AI 伺服器，儘管其聲稱在使用者詢問與網頁

無關的問題時不會儲存對話紀錄，但實際上仍可能因判斷失誤導致內容洩露。這是因為 Copilot 使用 AI 模型來判定查詢是否與網頁相關，而該模型的判斷可能不準確，導致網頁內容被意外傳輸至伺服器，進而引發隱私風險。

Copilot 在更新網頁標題時，未對接收到的標題資訊進行適當過濾，這是 Web 開發中常見的錯誤，可能被攻擊者利用注入 HTML 標籤以操控網頁內容。講者指出，攻擊者可以藉此注入帶有 allow 屬性的標籤，並結合 Bing 搜尋引擎中的 XSS 漏洞和 Copilot 的許可權委派機制，在使用者不知情的情況下存取其攝影機和麥克風，對使用者隱私和安全構成重大威脅。

Copilot 中存在一個特殊的 API 端點，雖然本身沒有特殊許可權，但可以被任何網站嵌入。講者發現，攻擊者可利用此端點執行命令並與 Copilot 的後端伺服器通訊，甚至通過端點中的 Search Memory 功能獲取使用者的歷史對話紀錄。此外，攻擊者還可以透過巧妙設計的 prompt，將敏感資訊嵌入到 markdown 格式的圖片或連結中，誘導使用者點擊，進一步洩露資訊，對使用者隱私和安全構成威脅。將安全性高的系統與安全性低的系統整合在一起，並不能保證整體系統的安全性。在軟體開發過程中，必須重視基本的安全原則，並對所有程式碼進行嚴格的審查和測試，才能有效防範安全漏洞。此外，針對 AI 驅動功能的獨特安全風險，需要設計和實施專門的緩解措施，才能確保使用者資料和隱私的安全。

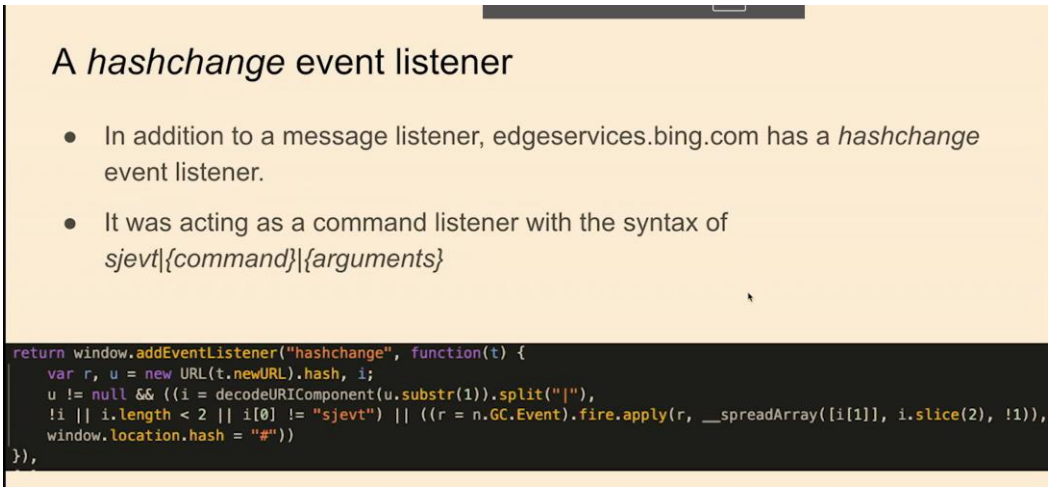


圖 1 Hashchange 事件監聽器的功能和程式碼

講者補充說明了三種網頁安全機制，分別是 CSP（Content Security Policy）、Trusted Types 和 Origin Isolation。CSP 可讓網站管理員控制資源和程式碼的來源，例如圖片、腳本和框架，以降低外部攻擊風險；Trusted Types 是一種瀏覽器 API，能幫助開發人員防止跨站腳本(XSS)攻擊，僅允許受信任的內容注入網頁；Origin Isolation 則是一種瀏覽器安全機制，可將不同來源的網頁內容隔離到不同的處理程序中，防止相互攻擊，進一步強化網頁安全性。這些機制為開發者提供了更完善的防禦工具，應對各種常見的安全威脅。

3. 揭代理到核心:從 Windows 核心流出的漏洞

講者首先回顧了近年來駭客攻擊的主要目標，包括 Win32K、CLFS 和 MSK SSRV。他指出，Win32K 由於其複雜性，一直是駭客攻擊的熱門目標，而 CLFS 則是近年來的新興目標，因其複雜的程式碼結構容易產生漏洞。MSK SSRV 則是去年才開始受到關注，但其規模較小，漏洞較容易被發現。

MSK SSRV 的兩個已知漏洞，如下兩點：

●邏輯漏洞:這個漏洞存在於 API 使用過程中，當核心使用

API 映射記憶體位址時，無法正確設定模式存取權限，導致使用者可以提供核心位址並將其映射到使用者空間，進而利用核心空間的二級記憶體進行寫入操作。

●CVE-2023-36802:這個漏洞與檔案物件內部的物件儲存方式有關。當這些物件被使用時,系統不會進行類型檢查，導致類型混淆的發生。

Angel Boy 指出，儘管 MSK SSRV 已經被廣泛研究，但它只是核心串流技術的冰山一角。其他潛在的核心串流元件，例如影音驅動程式，也可能存在漏洞。

他接著說明核心串流的概念，說明當 Windows 系統開啟網路攝影機或音訊裝置時，系統會以串流的方式讀取和寫入數據，例如聲音或影像。Microsoft 使用核心串流框架來處理這些操作，並提供了三種多媒體類別驅動程式模型:埠類別、AVStream 和串流類別。

為了與裝置互動，系統需要列出可用的裝置，並使用裝置名稱或其他識別符號來建立裝置。Microsoft 提供了 SetupAPI 和 CreateFile API 來簡化這個過程。當裝置被開啟時，核心會建立核心串流相關的執行個體，例如核心串流物件，用於封裝硬體功能。其中，KS 篩選器和 KS 針腳是兩個重要的執行個體。KS 篩選器代表裝置的特定功能，例如音訊裝置，它從音訊裝置讀取數據，並透過一系列節點將其傳遞到輸出，最終存入 RAM。KS 針腳則代表 KS 物件的屬性，例如數據格式、音量級別和裝置狀態。

Angel Boy 先生接著說明了如何分析核心串流漏洞，他指出 KS 佇列是核心串流的入口點，負責將 32 位元請求轉換為 64 位元請求。KS 則負責將請求轉發到相應的裝置驅動

程式。

他強調，每個裝置和物件都有其屬性和處理常式，而這些處理常式可能會因為缺乏大小檢查、越界存取和整數溢位等問題而導致漏洞。

Angel Boy 分享了一個他發現的有趣程式碼片段，該片段位於 KS 佇列的入口點，並質疑其安全性。他指出，雖然在一般情況下，由於系統呼叫來自使用者模式，請求模式會被設定為 1，因此這些操作是安全的。但是，他發現了一個新的漏洞類別，稱為"futures first"，它允許攻擊者在核心模式下執行程式碼。

Angel Boy 先生進一步解釋了"futures first"漏洞的原理，指出當使用者應用程式使用 Nt 系統呼叫操作裝置時，核心會將先前的模式設定為使用者模式。然而，如果驅動程式使用 Zw 系統呼叫，則先前的模式會變為核心模式，導致在核心模式下執行程式碼。

他接著介紹了一個名為 KSDEVICE_CONTROL 的 API，該 API 允許攻擊者在核心模式下執行 IOCTL 請求。

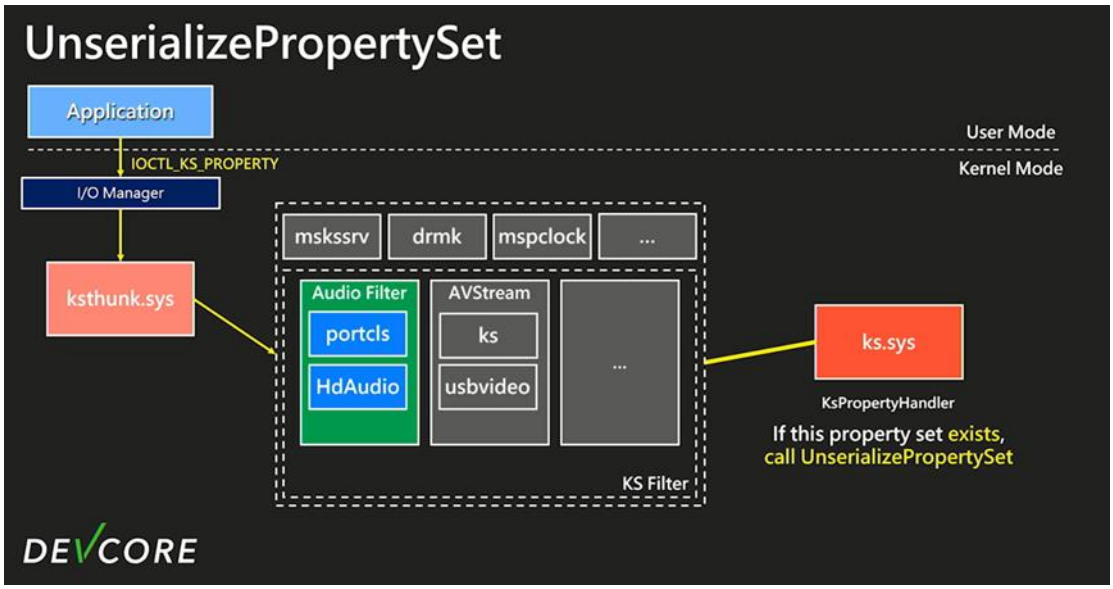


圖 2 UnserializePropertySet 的調用和作用

講者所發現的漏洞分享；反序列化屬性集漏洞，這個漏洞存在於 IOCTL_KS_PROPERTY 處理常式中，當其 Flags 欄位被設置為 KSPROPERTY_TYPE_SERIALIZESET 時，核心會調用 KsPropertyHandler 函式來處理屬性集。攻擊者可以透過構造惡意的屬性集，並利用 IOCTL_KS_PROPERTY 請求將其發送至核心，由於 KsPropertyHandler 函式在處理屬性集時未正確檢查請求模式，導致攻擊者可以藉此漏洞在核心模式下執行程式碼。該漏洞影響範圍廣泛，涵蓋從 Windows7 到 Windows 11 的所有版本，對系統安全構成嚴重威脅。雙重提取漏洞，這個漏洞存在於 KS 屬性處理常式中，核心在處理 KS 屬性時，會將使用者輸入的資料複製到核心緩衝區。攻擊者可以利用競爭條件，在核心執行資料複製的過程中修改使用者輸入的資料，從而控制複製到核心緩衝區的內容。這可能導致核心崩潰或允許攻擊者執行任意程式碼。

4. **破解 PlayStation 5 網路加密：**

物聯網(IoT)設備透過網路傳輸越來越多的敏感資料，因此

加密連線安全至關重要，Aapo 先生指出，物聯網設備透過網路傳輸越來越多的敏感數據，因此加密連線對於保護數據安全至關重要。他介紹了 TLS（傳輸層安全性）協定，它是 HTTPS 中的"S"，用於加密網路數據。TLS 透過交換加密金鑰來確保數據傳輸的安全性，並透過驗證機制防止連線到錯誤的伺服器；並認為 TLS 是一個簡單、有效且經過驗證的技術，被廣泛應用於各種網路服務中。

TLS（傳輸層安全性）是一種廣泛使用的加密協議，可確保網路資料安全。即使您認為自己沒有使用 TLS，您可能也在不知不覺中使用它，因為許多通訊加密協議要麼是 TLS，要麼是基於 TLS，要麼與 TLS 非常相似。

Alo 先生在研究 TLS 的安全性時，回顧了 15 年前 Moxie Marlinspike 在 DEFCON 會議上展示的 TLS 攻擊技術，這些技術揭露了當時 TLS 協議的多個漏洞。儘管這些漏洞在過去的 15 年中已被修復，但 Alo 先生發現，許多物聯網設備仍然受到這些漏洞的影響。他認為，漏洞持續存在的主要原因是缺乏有效的工具來檢測這些漏洞，導致設備開發者無法輕易識別並修補問題。

為了解決這一問題，Aapo 先生開發了一款名為"tlspuffin"的工具。該工具以 Moxie Marlinspike 在 2009 年 DEFCON 會議上展示的 TLS 攻擊技術為基礎，能夠自動測試各種 TLS 漏洞，並嘗試破解加密連線。Aapo 先生利用 tlspuffin 發現了 200 個存在漏洞的應用程式，這些應用涵蓋了 Android、iOS、Windows、Mac，以及各類物聯網設備。令人驚訝的是，其中有一半的漏洞至今仍未修復，顯示出當前開發者對於 TLS 安全性的重視程度仍然不足。

透過這款工具，Aapo 先生還獲得了高達 20 萬美元的漏洞

賞金。他指出，大多數 TLS 漏洞並非源於協議本身，而是由於開發者在使用函式庫時的實作錯誤或不當配置所導致。他強調，TLS 函式庫本身設計完善，通常運作良好，但開發者對其使用方法的理解不足，特別是在處理複雜的安全設定時，容易產生錯誤配置，從而引發漏洞。Aapo 先生的研究不僅突顯了 TLS 漏洞的持續威脅，也提醒了業界必須加強對安全工具的研發與應用，協助開發者更有效地保護其產品和用戶的資料安全。

PS5 加密連線漏洞案例;在開發 tlspuffin 的過程中，Aapo 先生意外發現 PS5 的加密連線存在一個嚴重漏洞。他原本只是想錄製 tlspuffin 的演示影片，卻發現該工具可以解密 PS4 和 PS5 的大部分 TLS 連線，包括帳戶密碼、遊戲數據和作業系統數據。表示，這個漏洞的成因是 PS5 使用的 HTTP 函式庫沒有檢查憑證是否由合法的憑證授權機構(CA)簽發。攻擊者可以利用這個漏洞偽造憑證，並攔截 PS5 的加密連線，且將這個漏洞提交給了 Sony 的漏洞賞金計劃，並獲得了 5 萬美元的獎勵，Sony 在收到報告後快速修復了這個漏洞，並強制所有 PS5 更新到最新版本。

最後，Aapo 先生指出，即使是像 PS5 這樣的大型平台也可能存在安全漏洞。他認為開發者應該重視安全性測試，並使用 tlspuffin 等工具來檢查系統中是否存在已知的 TLS 漏洞，並鼓勵網路安全研究人員和愛好者積極參與 DEFCON 等安全會議，並從中學習最新的攻擊技術和防禦策略。並認為駭客技術並不難學，只要願意花時間研究，任何人都可以成為一名駭客。

5. 語義檢測的全新方法：基於神經符號轉換器的創新模型

講者團隊在 2022 年美國網路安全研討會上提出了一種基

於深度學習的解決方案，專注於識別未知的 API 程式碼。該方法以污點分析為基礎，通過對 API 進行語義分析，結合多種專家規則來實現有效識別。然而，這種方法存在明顯的局限性：需要人類專家編寫大量的規則，而這些規則不僅耗時繁瑣，還容易因覆蓋不足或遺漏而導致錯誤。此外，由於人類能力的限制，難以全面涵蓋所有可能的 API 使用情境，特別是在處理大規模程式碼庫時，效率和精確度會受到顯著影響。

為了解決這些問題，講者團隊提出了一種全新的預測性神經網路模型，基於 Transformer 架構，專為自動化 API 識別而設計。該模型以標準的 LLVM 編譯器引擎為基礎，並結合了團隊此前使用的污點分析技術，能夠通過分析函數的位置和操作所需的符號,自動學習和識別 API 的用法特徵。這種方式不僅克服了人工規則的局限性，還顯著提高了識別未知 API 的效率和準確性。

此外，該模型展現了極大的擴展潛力，可以應用於各種編譯器框架和程式語言環境，進一步推動未知 API 自動化分析技術的發展。講者特別強調，這種方法大幅減少了對人工干預的需求，使得在處理大規模程式碼庫時，能更加快速、準確地識別可能潛藏的 API。這項研究不僅提供了一個高效的解決方案，也為未來在安全性分析和程式碼理解領域的應用奠定了基礎。

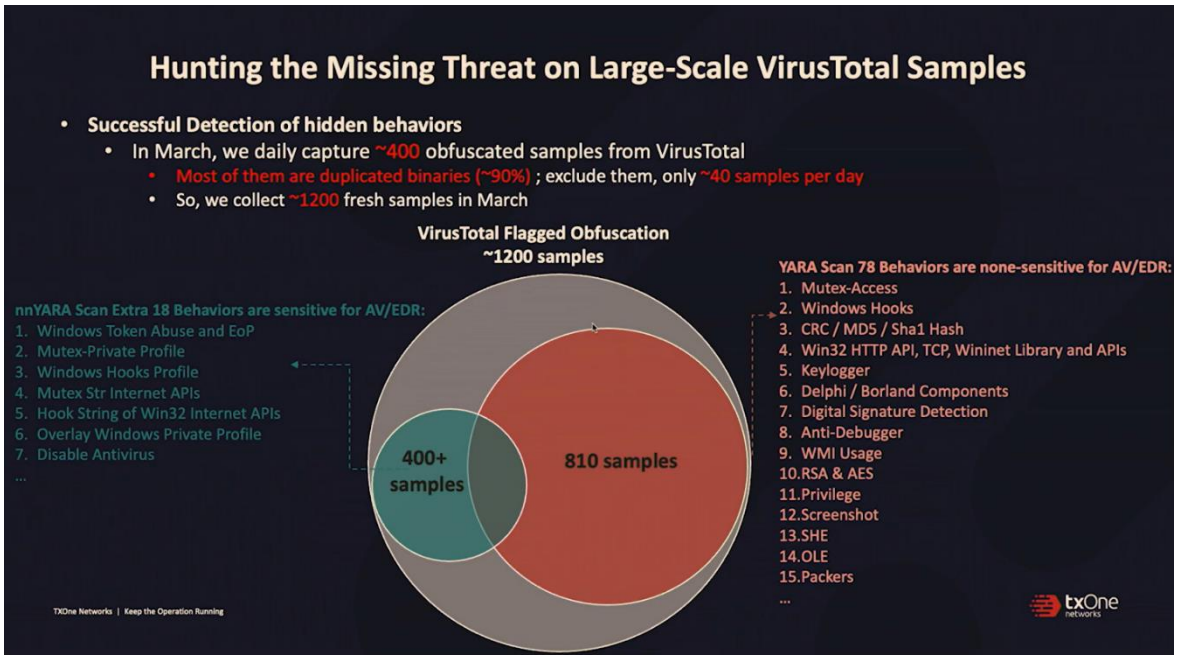


圖 3 在大規模的 VirusTotal 樣本中尋找未被發現的威脅

Sheng-Hao Ma 首先說明了如何使用 Word Embedding 自然語言處理技術來捕捉二進制碼流的語義以及 API 序列的學習。 他們透過自行開發的分析引擎，從二進制碼中提取參數值，並使用 Word Embedding 技術將每個 API 程式碼的語義進行符號化。

然而，由於 64 位元 Windows 系統中的整數值範圍非常大，若要建立一個資料庫來收集每個整數值的向量化語義，資料庫大小將會非常龐大，難以實際應用。 因此，講者團隊從逆向工程的角度出發，考慮整數值的類型，將其分類為人類可讀的字串，例如字串類型、記憶體頁面等，並將其作為 Token ID。

此外，講者團隊還注意到微軟定義了許多具有特定語義的魔術數字，例如代表特定錯誤碼的數字。他們透過識別這些由微軟預定義的魔術數字，將整數值分類為人類可讀的字串。

講者團隊建立了一個基於 MITRE ATT&CK 框架中所有 APT 組織二進制文件的 AI 模型，認為國家級攻擊組織的惡意軟體程式碼質量最高，最能代表真實攻擊案例。經過約 26 小時的訓練，他們開發出一個輕量級的 AI 模型，並成功應用於實際案例分析中。在展示的案例中，惡意軟體採用了高度混淆的加密演算法，傳統基於規則和模式匹配的分析方法難以檢測，但該 AI 模型能通過分析 API 參數值的使用特徵，準確識別出惡意軟體使用了 InternetOpenA API 以及其他相關 API，例如 RegQueryValueExA，展現了其在惡意軟體檢測中的高效性與準確性。

講者團隊使用 Facebook 開發的 Capitan 工具分析 AI 模型的推論過程，以深入了解其判斷邏輯。他們展示了一個後門程式的案例，該程式使用了 RegQueryValueExA API，但缺乏明確的符號名稱。AI 模型透過分析 API 的參數值，判斷該程式可能與 Windows 註冊表相關，並進一步解析其他參數值，最終準確識別出該 API 的功能。這一過程展現了 AI 模型在推論未知程式行為中的精確性和高效性。

為了驗證 AI 模型在大規模惡意軟體分析中的有效性，講者團隊利用 VirusTotal 搜尋所有被標記為惡意軟體的 PE 檔案，並使用 AI 模型分析這些檔案中隱藏的 API 程式碼。他們發現，許多惡意軟體通過隱藏的 API 程式碼來掩蓋其惡意行為，而傳統的分析方法往往難以有效檢測。AI 模型成功揭示了這些隱藏的 API，展現了其在惡意軟體檢測中的優勢與價值。

團隊開發了一個開源工具，可以自動化分析惡意軟體中使用的隱藏 API 程式碼，並公開在 GitHub 上供社群使用。他

們在大規模分析中發現了兩種主要的隱藏技術：

● 反沙盒和反虛擬化技術：惡意軟體會嘗試判斷其是否運行在虛擬機或沙盒環境中，並避免暴露其惡意行為。

● 混合程式設計技術：惡意軟體會同時使用 C#和組合語言程式碼，增加分析難度。

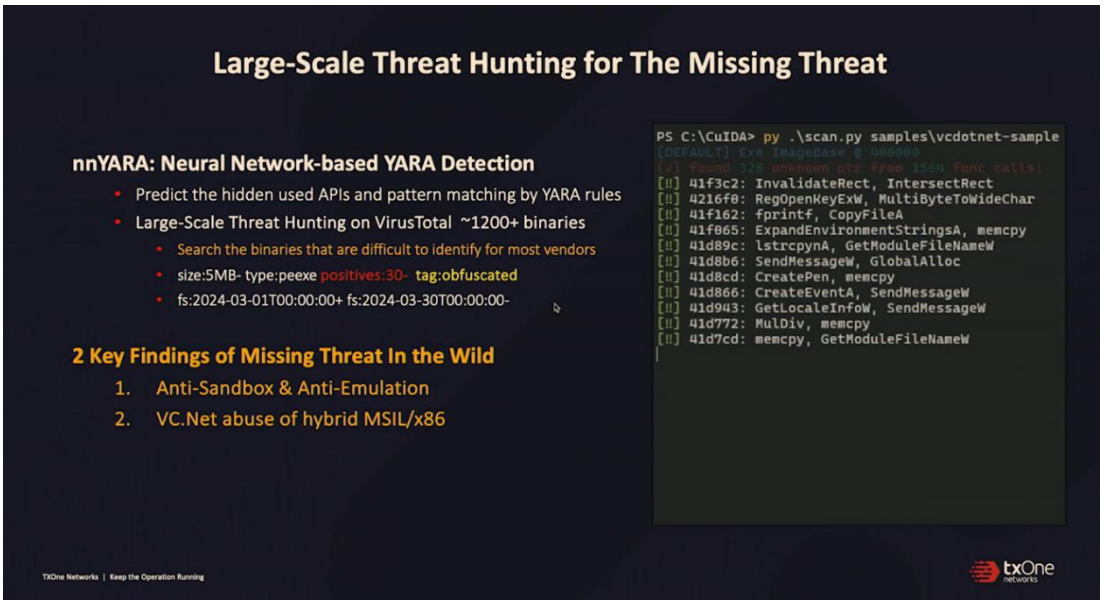


圖 4「Large-Scale Threat Hunting for The Missing Threat」的威脅獵捕流程

講者團隊最後 AI 模型應用於商業封裝器的行為分析，旨在解決現代商業封裝器對惡意軟體分析帶來的挑戰。他們指出，現代商業封裝器的複雜性使得傳統分析方法難以提取純粹的受保護程式碼進行檢測，而 AI 模型能有效彌補這一不足，為惡意軟體分析提供新的解決方案。

傳統的分析方法通常需要進行以下步驟：

● 程序：即使原始程式碼被封裝，它仍然需要解壓縮到进程記憶體中才能執行。

● 尋找原始建構函式：分析人员需要找到原始程式的建構函式，才能訪問程式碼的其他部分。

● 重建導入：Win32 API 是程式與作業系統核心互動的唯一方式，重建導入可以讓分析引擎掃描受保護的 PE 檔案。然而，商業封裝器會盡力隱藏建構函始點，並使用路由函数重定向導入地址欄位，使得分析人員難以重建導入表。

講者的團隊透過 AI 模型，成功分析了使用 VMProtect 封裝的程式，並準確辨識出程式中用到的 API，例如 VirtualAlloc 和 WriteProcessMemory。除此之外，他們還發現，AI 模型能夠辨識 VMProtect 本身的行為，例如它透過 GetModuleFileNameA API 檢查封裝器是否還在執行。因為他們的 AI 模型可以分析封裝程式的使用者定義執行鏈，而許多封裝器在處理堆疊混淆時並不夠完善，因此這種方法應該也能適用於其他商業封裝器，例如 Themida 和 UPX。他們也實際測試了 AI 模型在 Themida 上的分析效果，結果證實該方法確實有效。

講者團隊在執行執行緒和 LLVM 程式碼的污點分析時，面臨一些挑戰，包括「路徑爆炸」問題（分析範圍過大導致計算複雜度過高）、效能瓶頸以及多執行緒協調的困難。此外，即使是當前最先進的反組譯工具，也無法百分之百地分析所有二進制檔案中的程式碼，這意味著仍有部分惡意軟體程式碼可能逃過檢測，無法被完整分析。為了幫助資安領域的藍隊更有效地應對威脅，講者團隊計劃將他們的工具在 GitHub 上開源，希望為更多資安工作者提供有價值的資源，進一步強化防禦能力。

6. 軟體物料清單(SBOM)與安全透明性 – 完整解析其關聯：

現代軟體生態系統複雜且相互關聯，了解軟體成分和潛在漏洞至關重要。演講者 Alan Freeman 強調軟體物料清單(SBOM)的重要性，它就像食品的成分表一樣，列出軟體的組成部分，為軟體供應鏈提供透明度，有助於識別已知漏洞並快速應對新威脅。

以下詳細說明 SBOM 和相關安全措施：

●SBOM 的必要性：

現代軟體通常包含許多第三方組件，這些組件可能存在已知或未知的漏洞。SBOM 有助於開發者了解軟體的組成部分、選擇安全的軟體、並有效地管理漏洞。Alan Freeman 用食品成分表的比喻說明，軟體安全的重要性不亞於食品安全，甚至對社會影響更為深遠。

●SBOM 的應用範圍

SBOM 不僅涵蓋自有軟體，也包括開源程式碼、內部開發模組和二進制文件等各種軟體形式，是整體軟體生態系統安全性的基石。更重要的是，SBOM 不僅是一個好主意，更逐漸成為全球法規和合規要求的一部分：

(1)美國：政府採購的所有軟體都需要提供 SBOM。

(2)歐盟：歐盟的網路安全法規將涵蓋所有在歐盟銷售的數位產品，SBOM 將成為法規的一部分。

(3)印度：印度證券交易委員會已宣布 SBOM 的重要性。

(4)日本：日本是首批發布 SBOM 指導方針的國家之一，目前已更新至第二版。

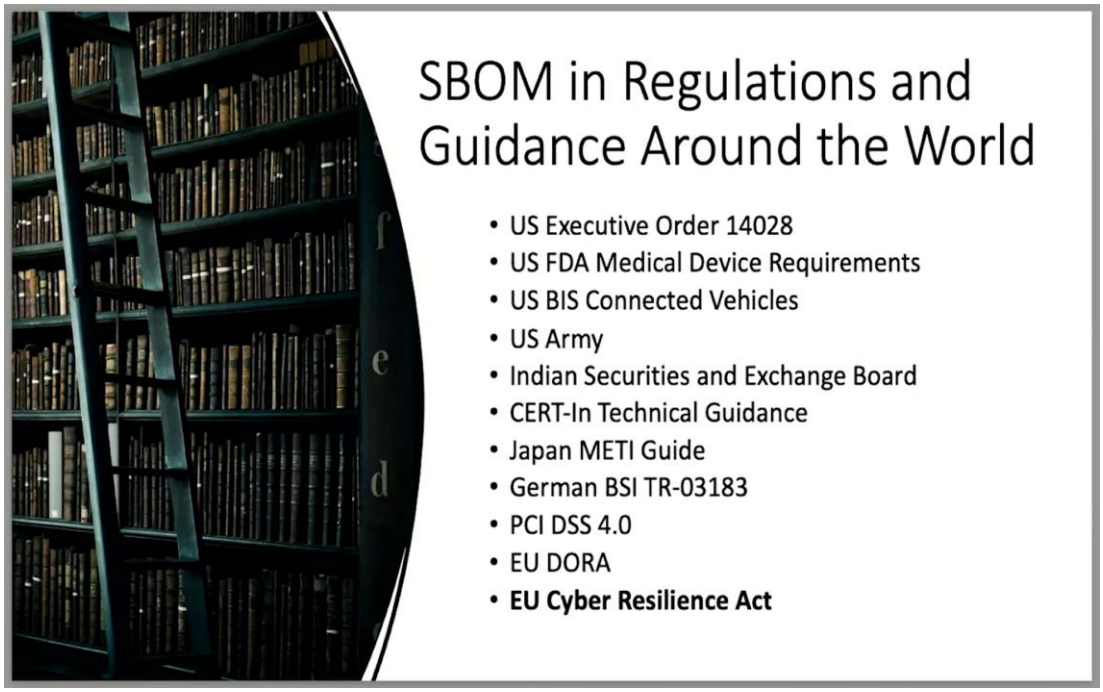


圖 5 SBOM（Software Bill of Materials）在全球各地法規和指導文件中的應用與要求

●SBOM 面臨的挑戰

(1)定義標準化：目前缺乏統一的 SBOM 標準，不同工具生成的SBOM格式可能不同,增加數據交換和分析的難度。Alan Freeman 強調全球協調一致的重要性,並提到 CISA 與各國合作制定共同標準。

(2)數據品質:SBOM 的價值取決於數據的準確性和完整性。一些免費工具可能無法提供完整資訊,而商業工具可能難以滿足特定需求，例如醫療設備的安全需求。

(3)工具可靠性：SBOM 工具質量參差不齊，有些工具無法準確識別所有組件或提供實用資訊。

●軟體識別

準確識別軟體組件是 SBOM 的基礎,但命名和識別符問題可能導致混淆。例如，Windows 10 的不同版本可能使用不同名稱或識別符。Alan Freeman 建議採用多種識別符,如 CPE、

PURL 和哈希值，以提高準確性。

●協調漏洞披露（CVD）

CVD 是一個重要的安全流程，可以幫助組織及時發現和修復漏洞。Alan Freeman 強調，組織應與安全研究人員保持有效溝通，積極回應漏洞報告，而非採取法律威脅等不當行為，從而促進漏洞披露的良性循環。

●漏洞信息質量與 VEX

漏洞信息質量至關重要，例如 CVE 數據庫等漏洞記錄可能存在不完整或不準確的問題。為解決此問題，CISA 推出了 VEX(漏洞可利用性交換）項目，提供更準確且可機讀的漏洞資訊，幫助組織更好地評估風險。

●自動化和模組化

手動創建和分析 SBOM 不僅費時，還容易出錯。自動化工具能幫助更有效地生成、交換和使用 SBOM 數據。同時，模組化設計提高了工具的靈活性與互通性，促進不同工具和數據源之間的整合。

最後 SBOM 和相關安全措施對於構建安全可靠的軟體生態系統至關重要。透過提高軟體供應鏈的透明度、自動化安全流程、加強合作，我們可以更好地應對日益複雜的軟體安全威脅，推動軟體行業向更高效、更安全的方向發展。

7. 濫用舊式鐵路信號系統：

David Meléndez 是一位資深的嵌入式系統研發工程師，擁有超過 12 年的網路安全和硬體駭客經驗，並指出鐵路訊號系統安全議題至關重要，特別是傳統的鐵路訊號系統存在安全漏洞，可能被駭客攻擊，進而造成嚴重事故。因此，他們團隊針對西班牙的鐵路訊號系統進行深入研究，希望找出潛在的風險並提出改善建議。

●鐵路區塊系統介紹

鐵路區塊系統是一項為確保列車運行安全而設計的核心技術。其基本概念是將鐵路軌道劃分為多個區塊，並確保在任意時間內，每個區塊最多僅允許一列列車駛入，從而有效防止列車碰撞的發生。在傳統的區塊系統中，燈號信號被用來管理列車運行：當列車進入某一區塊後，該區塊後方的信號燈會轉為紅色，以阻止其他列車進入，針對區塊系統的具體運作方式，常見的方法包括以下幾種：

(1)計軸器：透過計算經過裝置的車軸數量來確保列車的完整性，從而判斷列車是否已完全離開區塊。

(2)路牌閉塞：司機必須持有代表區塊使用權的路牌才能駛入下一區塊。然而，由於效率和可靠性問題，此方法已逐步被淘汰。

(3)電話閉塞:由車站人員通過電話相互確認列車運行情況，並通知下一站有列車即將抵達。

(4)電子閉塞：以自動化技術進行列車的運行控制，如單線雙向自動閉塞和雙線自動閉塞，顯著提高了效率和安全性。

●西班牙的 ASPA 系統

講者接著介紹了西班牙的 ASPA 系統(Anuncio de Señales y Frenado Automático)，該系統用於提醒司機注意訊號並提供自動煞車功能。ASPA 系統包含兩個主要組成部分：

(1)軌道上的信標 (Beacon):信標會發送特定頻率的訊號，代表不同的燈號訊號(紅、黃、綠等)。

(2)列車上的接收器:接收器會接收信標的訊號，並將其顯示在司機的控制台上。

當列車接近信標時，司機需要確認控制台上顯示的訊號並按下對應的按鈕，否則列車會自動煞車。ASPA 系統有多種版本，包括類比和數位版本，數位版本可以使用更多頻率來傳輸更複雜的訊號。

●ASPA 系統的安全漏洞

ASPA 系統的設計存在顯著的安全漏洞，主要原因在於其軌道上的信標與列車之間的通訊缺乏認證機制。這種缺陷使得攻擊者能夠藉此進行訊號偽造，例如傳送模擬紅燈的訊號，導致列車誤判情況並觸發緊急煞車。

研究人員成功利用線圈和電容器製作了一個偽造的信標，並模擬了 ASPA 系統的訊號。他們進一步分析了信標內部的電路結構，發現其運作基於電感耦合原理，這種技術類似於無線充電的工作方式。這一研究結果突顯了 ASPA 系統在設計層面上的潛在風險，並強調了引入認證機制以提升系統安全性的必要性。

圖 6 簡易偽造信標

●其他國家的類似系統

除了西班牙的 ASPA 系統外，講者也提到了其他國家存在類似的傳統鐵路訊號系統，這些系統也可能存在類似的安全漏洞。

(1)英國的 AWS（Automatic Warning System，自動警報系統）：AWS 系統會在軌道上設置信標，向列車發送警報信號。列車駕駛室內的接收器會接收信標信號，並提醒駕駛注意前方信號或速度限制。

(2)日本的 ATS（Automatic Train Stop，自動列車停止系統）：ATS 系統會在軌道上設置地面設備，當列車超速或闖越紅燈時，會自動啟動列車煞車系統，防止事故發生。

(3)德國的 Indusi（Induktive Zugsicherung，感應式列車控制系統）：Indusi 系統利用軌道上的電纜和列車上的線圈進行感應，向列車發送速度限制和信號信息。當列車超速或未按規定停車時，系統會自動啟動煞車。

這些傳統鐵路訊號系統大多依賴於軌道上的信標和列車上的感應設備來傳輸信息，缺乏現代化的安全機制，例如加密和身份驗證。 因此，攻擊者可能可以利用這些漏洞，偽造信標信號或干擾列車和軌道之間的通信，造成嚴重後果。

最後呼籲相關單位重視傳統鐵路訊號系統的安全性問題，並採取措施加強系統防護。 建議定期檢查信標的運作狀態，並加強對信標的物理保護，防止駭客 tampering。此外，也可以考慮升級現有系統，引入更先進的加密和身份驗證技術，提高系統的安全性。 講者表示他們的團隊將繼續研究其他國家的鐵路訊號系統，並與國際同行分享研究成

果。

8. 入侵 Google：運營與強化內部紅隊的經驗教訓

Stefan Friedli，目前擔任 Google 紅隊技術領導與經理，專注於進攻性安全與威脅模擬，致力於企業基礎設施的漏洞挖掘與防禦強化。自 2003 年起，他便活躍於資訊安全領域，並多次於國際資安會議擔任講者。他亦參與了滲透測試執行標準（PTES）的制定，為資安領域的標準化作出貢獻。近期，他專注於模擬真實攻擊場景，提升大型科技公司的資安防禦能力，同時強調在演練過程中遵循倫理規範與實務應用。

在此次演講中，Stefan Friedli 分享了其建立與運營 Google 內部紅隊的經驗，旨在幫助與會者了解紅隊的價值與運作模式，並提供建立與維護高效紅隊的實用建議。

講者首先闡述了紅隊的定義與目標。他引用美國陸軍對紅隊的定義，指出紅隊的核心價值在於從攻擊者的角度思考問題，挑戰既有假設。在網路安全領域，紅隊的主要目標是模擬真實攻擊者的行為，以測試和評估組織的防禦能力。講者強調，紅隊與滲透測試等其他安全評估方式的不同之處在於，紅隊並非專注於發現漏洞，而是利用漏洞達成特定目標，例如獲取敏感資料或控制關鍵系統。

●紅隊的價值和優勢

Stefan Friedli 強調，紅隊的價值主要體現在以下幾個方面：

(1)提升偵測和回應能力：紅隊演練能有效幫助藍隊測試並優化偵測和回應機制，從而提升應對真實攻擊的效率與速度。

(2)驗證實際風險：透過模擬真實攻擊場景，紅隊能夠驗證潛在風險的實際影響，並向管理層直觀展示安全漏洞可能導致的損害。

(3)促進安全意識提升：紅隊演練不僅讓組織成員了解攻擊者的思維方式與攻擊手法，還能提升整體安全意識，鼓勵主動思考與改進安全措施。

這些價值使得紅隊成為現代資訊安全策略中不可或缺的一環，為組織的防禦能力提供了關鍵支持。

●紅隊演練的關鍵要素

Stefan Friedli 分享了紅隊演練中幾個關鍵要素，為有效模擬攻擊場景提供指導：

(1)明確的目標和模擬對象:紅隊需明確演練的目標及模擬的攻擊者類型,例如國家級駭客、駭客組織或內部員工,並根據這些攻擊者的動機與能力來制定攻擊策略。

(2)真實的攻擊手法：紅隊應採用與真實攻擊者相似的攻擊手法，完整模擬攻擊鏈，包括初始入侵、橫向移動、權限提升及最終目標的達成,從而檢驗防禦機制的實際效能。

(3)詳細的報告和故事敘述：紅隊報告不僅需要記錄技術細節，還需以故事敘述的方式呈現攻擊過程，使非技術人員也能理解攻擊的手法與影響,從而促進針對性安全改進措施的實施。

●與其他團隊的合作

紅隊演練的成功仰賴於與組織內部其他團隊的緊密合作。講者特別強調了幾個關鍵合作夥伴的重要性：

(1)藍隊：紅隊和藍隊應建立互信關係，即時共享活動日誌和資訊，共同提升組織的整體防禦能力。透過密切合作，藍隊可以從紅隊的攻擊手法中學習並改進防禦策略，而紅隊也能從藍隊的回饋中了解自身攻擊的有效性並調整策略。雙方應避免將彼此視為對立關係，而是將彼此視為共同提升組織安全的夥伴。

(2)安全倡導者：安全倡導者熟悉不同部門的安全需求和挑戰，可以協助紅隊了解目標系統的特性和潛在風險，並在演練後協助推廣紅隊的成果和建議。他們可以扮演橋樑的角色，促進紅隊與其他團隊之間的溝通和合作。

(3)威脅情報團隊：威脅情報團隊可以提供真實攻擊者的情報，例如攻擊手法、目標和動機，幫助紅隊設計更貼近實際的演練場景。藉由參考真實攻擊案例，紅隊可以模擬更具威脅性的攻擊行為，並測試組織應對真實威脅的能力。

(4)法務團隊： 紅隊在進行演練時，可能需要進行一些具有法律風險的操作，例如模擬網路釣魚攻擊或入侵系統。因此，紅隊需要與法務團隊合作，確保演練符合相關法律法規，並在必要時取得相關許可。

紅隊與其他團隊的合作不僅能提升演練的效率和效益，更能促進組織內部的安全意識和文化。透過共同努力，組織可以建立更強健的安全防禦體系，有效抵禦日益複雜的網路威脅。

●建立和維護高效紅隊

紅隊的組成應該多元化，網聚擁有不同背景和技能的成員。

這樣的團隊組成有助於模擬各種攻擊者，例如國家級駭客、激進份子或心懷不滿的員工，並確保演練的多樣性和創新性。

其次，明確的規則和界限至關重要。紅隊需要事先制定明確的規則，包括可測試的系統、禁止的操作等，並與管理層達成共識，以避免演練過程中出現不必要的風險或爭議。例如，Google 的紅隊絕不會訪問真實用戶數據，而是使用測試帳戶來模擬攻擊。

持續學習和成長是紅隊保持技術優勢的關鍵。紅隊成員需要不斷學習新的攻擊技術和防禦措施，並積極參與安全社群，與同行交流經驗和知識。由於資訊安全領域的快速發展，紅隊必須不斷更新知識和技能，才能有效地模擬真實世界的攻擊者。

此外，關注團隊成員的身心健康也至關重要。紅隊工作壓力大，長時間模擬攻擊者的行為和思維模式容易造成成員倦怠。因此，領導者需要關注團隊成員的健康，鼓勵合理的工作時間和休息時間，並建立積極的團隊文化，營造相互支持和鼓勵的氛圍。鼓勵成員在演練之間從事工具開發和研究等低壓力的工作，也有助於緩解壓力並促進團隊的長期發展。

紅隊演練的最終目的是提升組織的整體安全防禦能力，而不是單純地找出漏洞或指責其他團隊的錯誤。 紅隊應主動與其他團隊合作，例如藍隊、安全倡導者、威脅情報團隊和法務團隊，分享資訊、資源和專業知識，共同提升組織的安全防禦能力。更重要的是，紅隊應鼓勵組織成員將紅隊的思維方式應用到日常工作中，主動思考潛在的安全風

險，並採取措施降低風險。透過這種合作和意識提升，組織才能建立更強健的安全防禦體系，有效抵禦日益複雜的網路威脅。

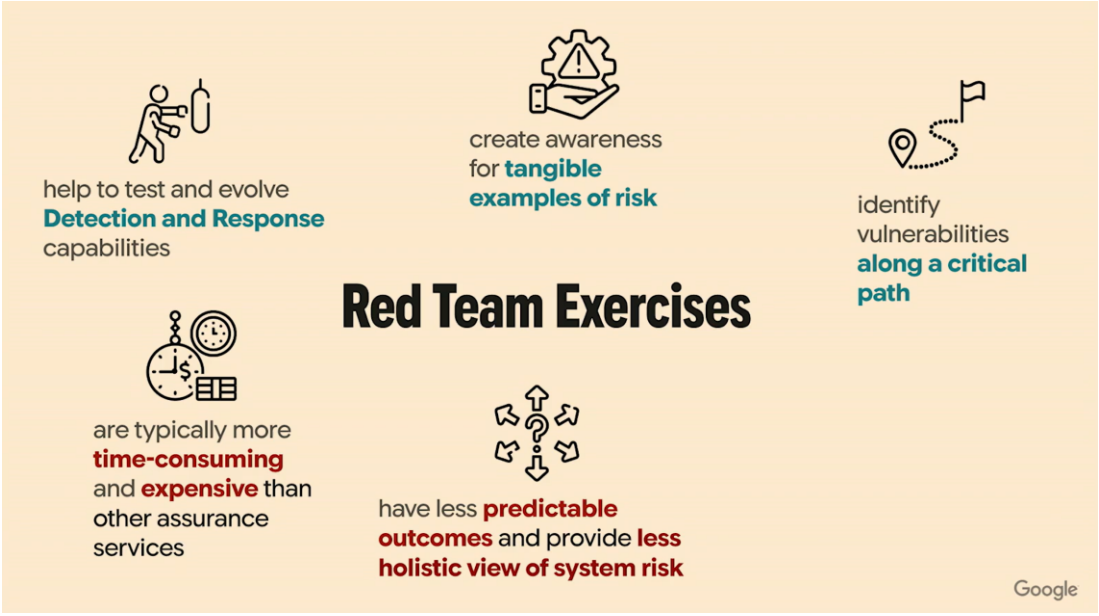


圖 7 攻紅隊演練（Red Team Exercises）的角色、優點與挑戰

9. BlackTech 的子域名濫用是否已經“進化”？

谷口剛與大杉孝太郎是日本資安領域的知名專家，分別專注於惡意軟體分析與鑑識調查，以及網路安全策略與防禦技術的研究。谷口剛自 2012 年起，便針對日本關鍵產業的網路攻擊進行深入研究，並在國際資安會議上分享其在網路釣魚攻擊與進階持續性威脅（APT）方面的見解。大杉孝太郎則專注於企業資安實務和跨國聯防，致力於提升企業在 AI 時代下的資安防護能力，並多次於國際論壇上發表演講。

講者指出，近年來雖然許多資安廠商針對 BlackTech 的攻擊手法與惡意軟體發表了研究報告，但對該組織在 DNS 領域的活動卻少有深入分析。為此，他們的研究團隊對 BlackTech 的 DNS 活動進行了詳細調查，發現該組織採用

了具有高度威脅性的獨特手法。此次研討會旨在分享這些最新研究成果，幫助資安社群更全面了解 BlackTech 的攻擊策略，進一步提升防禦能力。

此外，講者介紹了 BlackTech 的背景。作為一個來自中國的網路間諜組織,BlackTech 主要針對東亞國家進行攻擊，尤其是日本。日本警方和美國政府機構近期皆警告，BlackTech 通過攻擊海外子公司滲透日本企業總部，對日本的網路安全構成了嚴重威脅。

●BlackTech 惡意軟體分析：以 ReVulnPrint 為例

BlackTech 使用多種惡意軟體進行攻擊，其中一款名為 ReVulnPrint(又稱 Waterbear)。該軟體自 2009 年開始活躍，並不斷演進。2019 年，趨勢科技發現 ReVulnPrint 開始使用 API 鉤取技術。2020 年，TeamT5 發表了針對 ReVulnPrint 的深度分析報告。2021 年，Unit 42 公開了 ReVulnPrint 的內部結構。2022 年，ReVulnPrint 進化為 DeuterBear，並開始使用 HTTPS 加密通訊，使得分析難度大幅提升。

ReVulnPrint 主要由三個模組組成：Loader、Downloader 和 RAT。其中，Downloader 模組使用了多種程式碼混淆技術，例如動態解密函數和使用 BWI 指令隱藏重要資訊，使得逆向工程分析變得非常困難。此外，ReVulnPrint 還使用了自定義的挑戰-回應機制，利用已棄用的 RC4 加密演算法來區分真正的 C2 伺服器和偽造的伺服器。

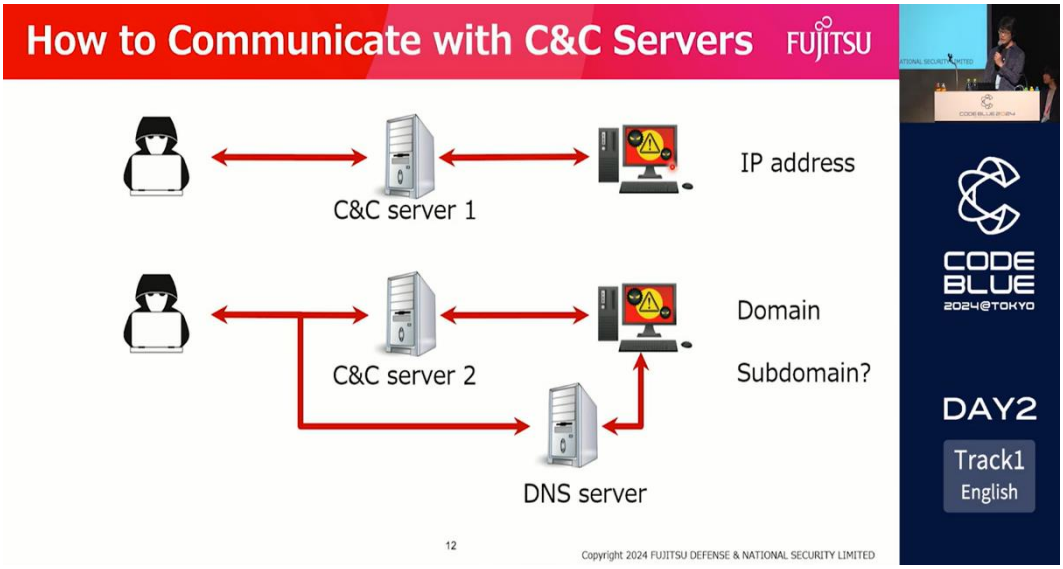


圖 8 C&C（Command and Control）伺服器進行通訊的運作方式

●BlackTech 的 DNS 攻擊手法分析

講者團隊針對 BlackTech 的 DNS 攻擊手法進行了深入分析，並採用了兩種主要方法：

(1)時間軸分析(時間軸變化偵測)：團隊追蹤了 BlackTech 攻擊手法隨時間的演變，觀察其策略和技術的變化趨勢。

(2)不同駭客組織的攻擊手法比較分析(群組間差異偵測)：團隊比較了 BlackTech 與其他 APT 駭客組織的攻擊手法差異，藉此識別 BlackTech 獨特的攻擊模式和策略。

綜合評估： 講者團隊將「時間軸變化偵測」和「群組間差異偵測」兩種方法結合，以更全面地了解 BlackTech 攻擊手法的演進趨勢。他們首先分析了 TeamT5 的威脅情報報告，並提取了 2022 年 1 月至 2024 年 3 月期間的 IOC（攻擊指標）。根據 IOC 分析結果，講者團隊發現 BlackTech 主要攻擊目標為台灣，但日本也可能成為未來的攻擊目標。

在分析 BlackTech 如何與 C&C 伺服器通訊後，講者團隊發現 BlackTech 主要利用 DNS 來隱藏 C&C 伺服器的 IP 位址，並使用子網域來規避偵測。講者團隊將 BlackTech 的子網域攻擊手法分為三種類型：

(1)合法服務濫用：BlackTech 會利用合法的動態 DNS 服務來建立子網域，例如 DynDNS，這種手法讓 BlackTech 可以快速且頻繁地更改 C&C 伺服器的 IP 位址，增加追蹤和封鎖的難度。

(2)子網域操作：BlackTech 利用子網域字串和大量註冊父網域來隱藏 C&C 伺服器。這種手法可以讓攻擊者建立大量的子網域，並將其分散到不同的父網域之下，使得防禦者難以追蹤和封鎖所有惡意子網域。子網域操作又可細分為兩種手法：

(2.1)字串操作：BlackTech 使用與目標組織相關的字串來建立子網域，例如 JPCERT 或 KRCERT。這種手法可以讓攻擊者偽裝成合法的組織或服務，降低被偵測的機率。

(2.2)父網域大量註冊：BlackTech 註冊大量父網域，並在每個父網域下建立多個子網域，以增加攻擊複雜度。這種手法可以讓攻擊者建立一個龐大的子網域網路，並將惡意流量分散到不同的子網域，增加防禦者分析和追蹤的難度。

(3)父網域操作：BlackTech 利用長期休眠的網域或偽造網域來隱藏 C&C 伺服器。這種手法可以讓攻擊者利用看似正常的網域來隱藏惡意活動，降低被偵測的風險。父網域操作又可細分為兩種手法：

(3.1)策略性網域：BlackTech 註冊網域後，會使其休眠一段時間，例如兩年，以避開偵測系統對新註冊網域的警覺。這種手法可以讓惡意網域看起來更像是合法的網域，降低被安全系統標記為可疑的風險。

(3.2)偽造網域:BlackTech 使用偽造的網域來建立子網域，並將子網域指向惡意伺服器，而原網域則保持休眠狀態。這種手法可以讓攻擊者利用看似正常的父網域來掩護惡意子網域，增加防禦者識別攻擊的難度。

透過以上三種類型的子網域攻擊手法，BlackTech 可以有效地隱藏 C&C 伺服器的真實位置，並規避傳統安全防禦機制的偵測。防禦者需要了解 BlackTech 的攻擊手法，並採取相應的措施來防禦其攻擊。

講者團隊針對 BlackTech 的偽造網域攻擊手法提出了一種名為「額外主動式 DNS(AADNS)」的防禦措施。AADNS 的原理是在客戶端查詢子網域時，同時向 DNS 伺服器發送一個針對父網域的查詢。如果父網域沒有回應，則表示該子網域可能使用了偽造網域。

講者團隊分析了 BlackTech 在 Amazon、Google 等知名服務的網域下建立子網域的案例。他們發現 BlackTech 將子網域指向惡意伺服器，但網域仍然指向合法的服務，藉此混淆視聽。AADNS 防禦措施無法有效偵測這種攻擊手法。講者團隊建議使用被動式 DNS 資料庫來分析過去的解析記錄，並結合 IP 位址地理位置資訊來判斷父網域是否可疑。

●時間軸變化偵測分析結果

講者團隊分析了 BlackTech 在 2018 年至 2023 年期間的攻

擊手法演變。他們發現BlackTech在2019年開始註冊網域，並在2023年開始大量使用父網域來建立子網域。

●群組間差異偵測分析結果

講者團隊比較了 BlackTech 與其他 APT 駭客組織的攻擊手法差異。他們發現 BlackTech 積極利用父網域進行多目標攻擊，而其他 APT 駭客組織則較少使用這種手法。

●BlackTech子網域攻擊手法演進結論

講者團隊認為 BlackTech 的子網域攻擊手法確實有所演進，但這種演進並非為了規避偵測，而是為了更有效率地建立攻擊基礎設施。BlackTech 透過策略性網域熟成和偽造網域等手法，建立了大量具有高度隱蔽性的子網域，並利用知名服務的網域來混淆視聽。

10. PkgFuzz 專案：針對開源軟體的又一持續模糊測試工具

近年來，開源軟體(OSS)的應用日益普及，但其安全性卻成為一大隱憂。儘管Google推出了OSS-Fuzz 等模糊測試平台，但其門檻較高，許多小型 OSS 專案難以參與，導致其安全性難以得到保障。為了解決此問題，川古屋雄平、塩地英太郎和大月優翔三位資安專家組成的講者團隊，致力於開發一套更易於使用的模糊測試系統Package Fuzz，讓更多 OSS 專案受益於模糊測試技術，提升整體軟體安全性。

Package Fuzz的運作原理是利用軟體包(Package) 中的資訊來自動化模糊測試流程。該系統分為三個階段：

(1)套件分析：在取得軟體包後，進行建置並監控整個過程，以收集執行檔、命令列參數和測試輸入檔案等相關資訊。

同時，在建置選項中加入模糊測試所需的編譯器選項，以生成適用於模糊測試的程式版本，為後續的測試與分析提供基礎。

(2)模糊測試：進行短時間的模糊測試，篩選出無法運作或不易發現漏洞的套件。對於通過初步篩選的套件，進一步執行長時間的模糊測試，使用 AFL++ 和 libfuzzer 等工具以進行深入測試，提升漏洞挖掘的精確性與效率。

(3)損毀處理:在模糊測試過程中，對產生的損毀進行分類，排除已知問題或不相關的損毀，並評估其是否具有可利用性。接著，根據影響程度對潛在漏洞進行優先排序，最後驗證這些損毀是否能在原始套件中重現，以確保分析結果的準確性與實用性。

模糊測試是一種自動化的軟體安全測試技術，透過向目標程式輸入大量隨機或變異的資料來嘗試引發程式崩潰，以發現潛在漏洞。這一技術自 1990 年首次提出，至今已發展超過 35 年，成為軟體安全研究的重要領域。Google 的 OSS-Fuzz 是一個知名的大規模開源軟體模糊測試平台，利用 Google 雲端運算資源，為參與專案提供持續性模糊測試服務。儘管 OSS-Fuzz 自 2023 年 8 月以來已協助修復超過 36,000 個漏洞，但其參與門檻較高，對資源有限的小型開源專案來說是一大挑戰。

為降低模糊測試的門檻，講者團隊開發了 Package Fuzz 系統。該系統利用軟體套件中的資訊自動化模糊測試流程，包含三個主要階段：套件分析、模糊測試與崩潰分析。在套件分析階段，Package Fuzz 自動下載軟體套件並提取建

置腳本、測試程式與輸入檔案等資料；在模糊測試階段，使用 AFL++和 LibFuzzer 等工具進行深入測試；在崩潰分析階段，則採用 C-CRASH 工具對崩潰進行分類與排序，幫助開發者優先處理高風險漏洞。

講者團隊使用 Debian 23.10 作業系統中的 265 個軟體套件進行實測，共執行 606 次模糊測試，發現約 65,000 個程式崩潰，其中約 1,200 個被歸類為獨特類型。結果顯示，64.5%的套件至少發現一個程式崩潰，24.5%的套件至少發現一個可能導致漏洞的程式崩潰，而最常見的原因為記憶體讀寫錯誤（記憶體讀取錯誤佔 54%，寫入錯誤佔 21%）。雖然 Package Fuz 的程式碼覆蓋率略低於 OSS-Fuzz，但漏洞發現率相近，並成功發現 5 個可被利用的漏洞，已向相關機構報告。

此外，Package Fuzz 還計畫進一步提升自動化程度，包括自動生成測試工具與整合根本原因分析工具，以幫助開發者更快定位漏洞位置。講者團隊希望透過 Package Fuzz 的開發與應用，降低模糊測試的技術門檻，讓更多開源專案能參與其中，共同提升軟體安全性。

補充說明，基於生成式預訓練模型的 AI 技術，如 ChatGPT 和 Copilot 365，展現了人工智慧在資訊科技領域的廣泛應用。這些工具雖然與 Package Fuzz 的研究方向不同，但都反映出 AI 在協助資料處理、回答問題與知識統整方面的潛力，進一步推動資訊科技的創新與發展。

(二)TRAPA Cyber Range™ 訓練平台：

在本次活動中，來自於台灣的菱鏡股份有限公司(TRAPA

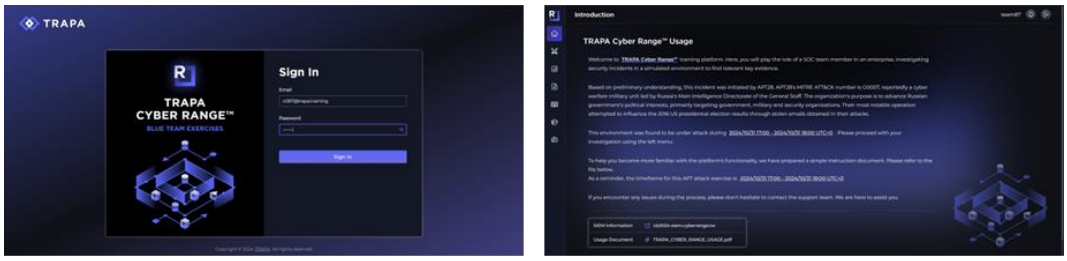
Security)使用該公司 TRAPA Cyber Range™訓練平台舉辦了一場 Cyber Range Excise 的體驗活動，如圖 9 所示，該平台主要以網路安全事件回應的藍隊演習為中心，該場體驗活動主要模擬對企業的網路攻擊，活動參與人員須扮演企業安全作業中心(Security Operation Center, SOC)團隊成員的角色，透過分析大量的威脅警報資料和系統日誌來追蹤攻擊者的蹤跡，並找出相關的關鍵證據，以對網路攻擊事件做出正確的回應，從而增強企業針對網路安全威脅的防禦能力。

圖 9、TRAPA Cyber Range Excise 活動說明

在活動體驗所開放的腳本是模擬由 APT28 所發動的網路安全事件、編號 G0007 的 MITRE ATT&CK。該組織被認為是由俄羅斯總參謀部主情報局(Russia's Main Intelligence Directorate of the General Staff)所領導的一個網路戰軍事單位，其目的是促進俄羅斯政府的政治利益，主要攻擊目標包括政府機構、軍事和安全組織。該組織最著名的一次攻擊行動是試圖通過竊取的電子郵件影響 2016 年美國總統選舉的結果。活動體驗所開放的腳本中要求體驗者調查在 2024/10/31 17:00 至 2024/10/31 18:00 (UTC+0)期間所發現的攻擊作為，並逐一回答每一個題組中所需要的攻擊資訊與線索，藉此讓參與人員體驗 TRAPA Cyber Range™訓練平台的各項功能與操作介面，並藉題組安排來

循序漸進了解資安鑑識人員應有的作為與流程。每一個參加體驗的人員可以拿到一張登入 TRAPA Cyber Range™訓練平台專屬的帳號與密碼，如圖 10 所示，登入頁面及進入平台後的首頁則如圖圖 11 所示。

圖 10、提供參賽人員登入 TRAPA Cyber Range™之網址與帳號密碼

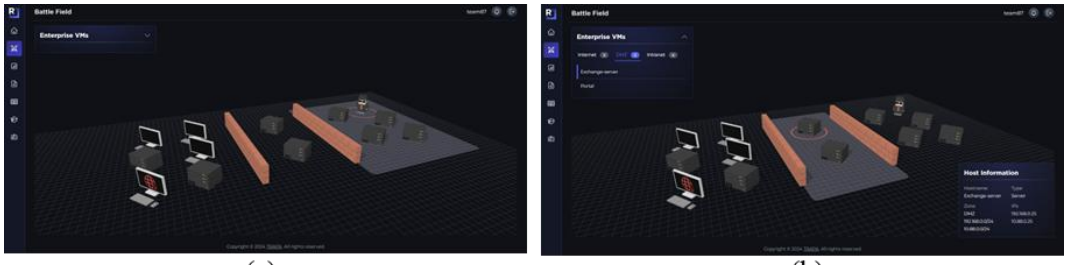


(a) (b)

圖 11、TRAPA Cyber Range™之(a)登入頁面與(b)首頁

當登入 TRAPA Cyber Range™訓練平台後，左方有幾個會需要使用到的功能圖示，分別是戰場(Battlefield)、安全事件監控中心(SOC Room)以及儀錶板(Dashboard)，戰場選項頁面主要藉由圖視化界面的方式，將網際網路(Internet)、非交戰區(Demilitarized Zone, DMZ)以及內部網路(Intranet)的機器以不同圖示來進行呈現，如圖 12 (a)所示，使用者可透過點擊圖示之方式了解每一台機器的內部資訊，包含設備類型與 IP 等，圖 12 (b)即為點擊非交戰

區中一台 Exchange-Server 所呈現之資訊。



(a) (b)

圖 12、Battlefield 之(a)圖示化全貌與(b) DMZ 其中一台 Exchange-Server 之資訊

其次，安全事件監控中心頁面顯示的則是任務（題組）清單、以及各題組每一次答題之結果，如圖 13 所示，該畫面左半邊會顯示各題組名稱、答題結果、以及完成解題時間。當點擊各題組名稱時，如未完成答題之題組，則會顯示題目資訊描述(Investigate Action)、提示(Notice)、以及須輸入答案之欄位；已完成答題之題組則會顯示該題組所得分數、題目細節(Action Detail)、調查員評論(Investigator comment)、所提交答案之資訊(Submitted Information)。安全事件監控中心畫面右半邊則顯示每一次送出答題結果之 ticket，綠色為答題正確之 ticket；紅色則為答題錯誤之 ticket，若點擊答題錯誤之 ticket，會顯示該題組答錯欄位之提示。而答題所得之總成績則會在圖 14 (a)的儀錶板中顯示，並同時顯示其他參賽隊伍之成績變化時間軸，如圖 14 (b)所示。

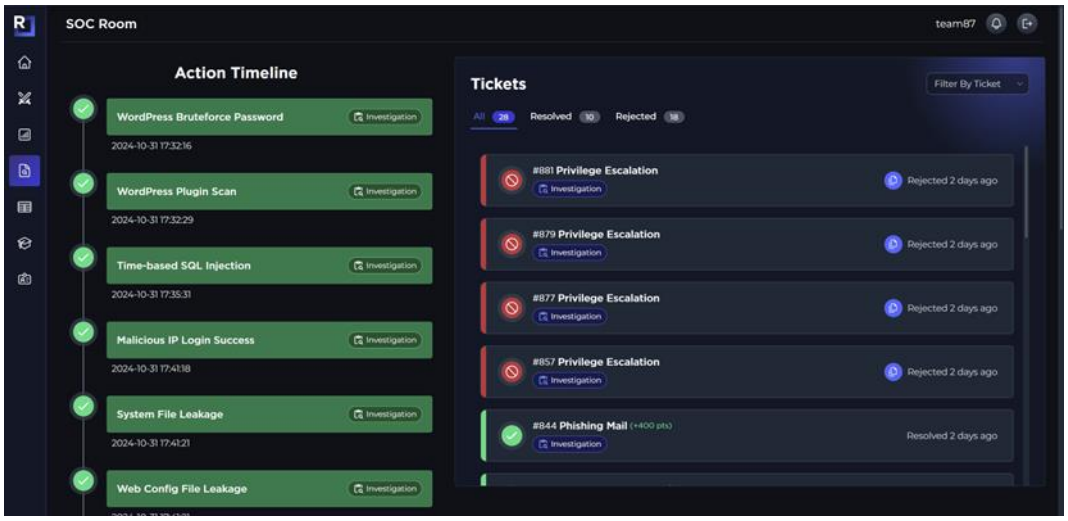


圖 13、SOC 各題組資訊以及答題結果所得到之 tickets

(a) (b)

圖 14、Dashboard 之(a)答題所得之總成績及(b)各參賽隊伍得分時間軸資訊

除了 TRAPA Cyber Range™訓練平台各選單頁面外，解題所需要之各項線索，則需要登入另外一個 Splunk 安全資訊與事件管理(Security Information and Event Management, SIEM)平台進一步查詢系統紀錄進行判斷與分析，登入頁面如圖 15 所示。因解題時限關係，無法針對每一個題組所找到之線索頁面進行記錄，因此僅將 Splunk SIME 各 log 頁面進行截圖，包含 Firewall Status、Mail Log from Snort、Snort Log、Web Access、Windows Event Viewer、以及 Windows Host Monitor 等 log 頁面，如圖 16 (a)至(f)所示。

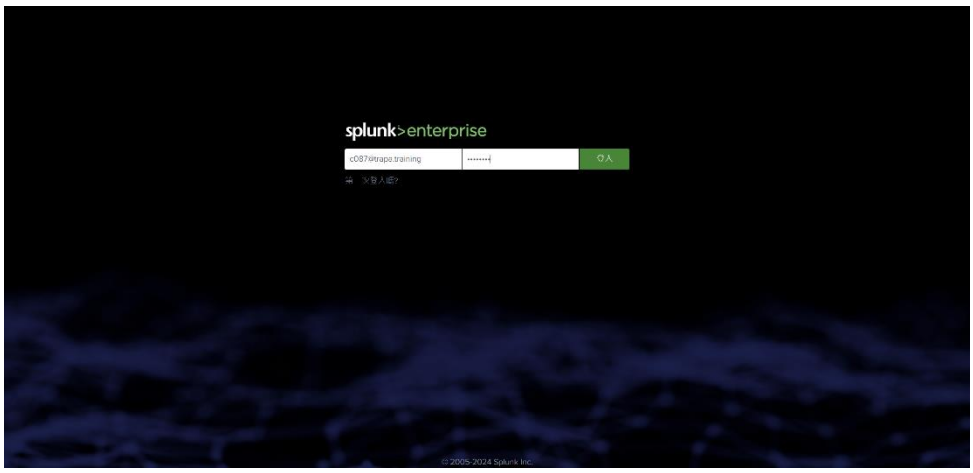


圖 15、Splunk SIEM 登入頁面

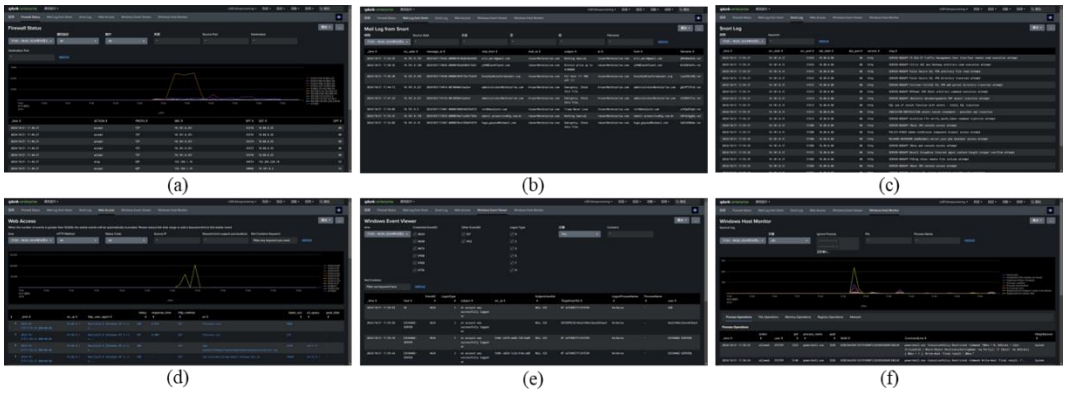


圖 16、Splunk SIEM 之(a) Firewall Status、(b) Mail Log from Snort、(c) Snort Log、(d) Web Access、(e) Windows Event Viewer、以及(f) Windows Host Monitor 頁面

Exercise 將解題情境區分為 13 個題組，各題組編號、主題、以及該題組分數(僅已完成解題之題目會顯示分數)分述如下：

1. Ticket #516 - WordPress 暴力破解密碼(WordPress Bruteforce Password)，+100 pts。
2. Ticket #538 - WordPress 擴充套件掃描(WordPress Plugin Scan)，+100 pts。
3. Ticket #549 - 基於時間的 SQL 注入攻擊(Time-based SQL Injection)，+300 pts。

4. Ticket #561 - 惡意 IP 登入成功(Malicious IP Login Success)，+100 pts。
5. Ticket #610 - 系統檔案洩漏(System File Leakage)，+50 pts。
6. Ticket #618 - 網站配置檔案洩漏(Web Config File Leakage)，+50 pts。
7. Ticket #685 - 上傳 Webshell (Upload Webshell)，+200 pts。
8. Ticket #688 - 資料庫洩漏(Database Leakage)，+50 pts。
9. Ticket #784 - DMZ 至內部網路的網路掃描(DMZ-Intranet Network Scan)，+100 pts。
10. Ticket #844 - 網路釣魚郵件(Phishing Mail)，+400 pts。
11. T1068 - 特權提升(Privilege Escalation)，未完成。
12. T1003.001 - HR-1 憑證轉儲(HR-1 Credential Dump)，未完成。
13. T1550.002 - 橫向移動-傳遞雜湊值(Lateral Movement - Pass the Hash)，未完成。

上述題組之題目細節分述如下：

1. WordPress 暴力破解密碼(WordPress Bruteforce Password)

- 行動描述：有一個 IP 嘗試登入管理頁面，請找出該 IP。
- SIEM 相關儀表板：Web Access。
- 行動細節：已確認有一個 IP 位址嘗試使用常見密碼登入 admin 帳號。
- 調查員評論：通常網路上充滿了這類的登入機器人，如果沒有後續行動，您無需特別注意它們。

- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.22
  - 攻擊開始時間：2024-10-31T17:32:16
  - 攻擊對象 URI：/wp-login.php
  - 攻擊嘗試使用之使用者帳號：admin
  - 上述題組原始說明內容如圖 17 所示。

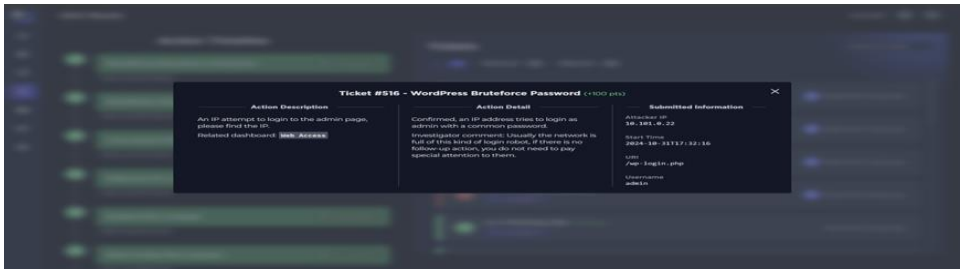


圖 17、WordPress 暴力破解密碼(WordPress Bruteforce Password)題組內容

2. WordPress 擴充套件掃描(WordPress Plugin Scan)

- 行動描述:有一個 IP 嘗試列舉 WordPress 擴充套件之路徑，請找出該 IP。
- 提示：SIEM 可能對顯示的日誌數量有上限。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，有一個 IP 位址嘗試在 Portal 上列舉 WordPress 擴充套件。
- 調查員評論：如果攻擊者發現感興趣的內容，可能會採取進一步行動。請密切監控該來源 IP 的後續行為。順帶一提，通常 SIEM 或日誌檢視工具對顯示的事件數量會有上限。在調查時，需注意避免因一次搜尋過多事件而遺漏重要資訊。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231

- 攻擊開始時間：2024-10-31T17:32:29
- 使用者代理（User Agent）：Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- 上述題組原始說明內容如圖 18 所示。

圖 18、WordPress 擴充套件掃描(WordPress Plugin Scan)題組內容

3. 基於時間的 SQL 注入攻擊(Time-based SQL Injection)

- 行動描述：有一個 IP 大量發送 POST 請求到相同的 URI，導致異常的回應時間。請找出該 IP。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，有一個 IP 嘗試從 MySQL 的使用者表中導出 admin 的雜湊值。
- 調查員評論：一旦雜湊值洩漏，我們必須假設該憑證已經遭到洩漏，此帳號的每次登入行為都必須被仔細檢查。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - 攻擊對象資料表名稱：wp_users
  - 攻擊對象 URI：/wp-login.php
  - 上述題組內容如圖 19 所示。

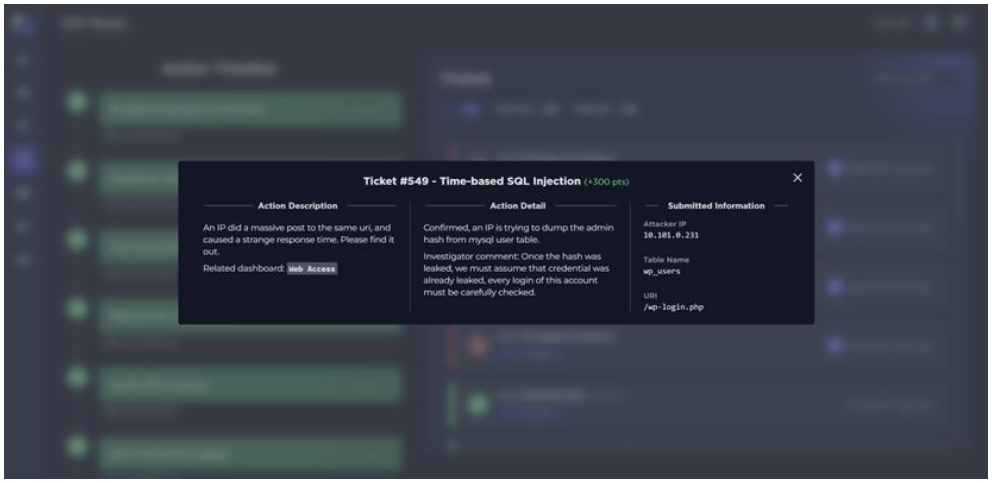


圖 19、基於時間的 SQL 注入攻擊(Time-based SQL Injection)題組內容

4. 惡意 IP 登入成功(Malicious IP Login Success)

- 行動描述：一個具有攻擊行為的 IP 已成功登入 Portal。請找出遭到入侵的帳號，並提供登入時間以及攻擊者的 IP。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，該惡意 IP 確實使用提供的帳號成功登入。
- 調查員評論：當惡意地址成功登入後，不僅需要確認他是如何獲得密碼的，更重要的是確認他登入後進行了哪些行為。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - 攻擊者登入時間：2024-10-31T17:41:18
  - 攻擊者登入使用之使用者名稱：admin
  - 上述題組原始說明內容如圖 20 所示。

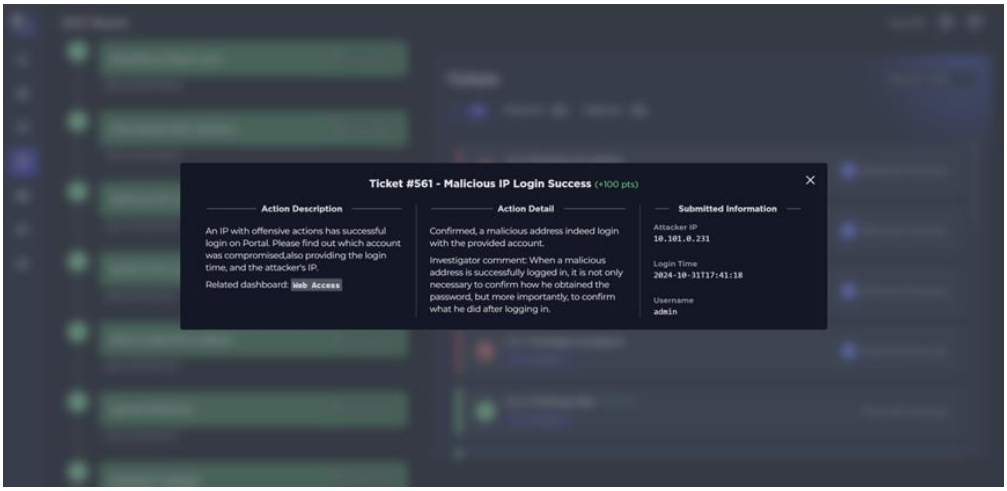


圖 20、惡意 IP 登入成功(Malicious IP Login Success)題組內容

5. 系統檔案洩漏(System File Leakage)

- 行動描述:我們偵測到 Portal 上的一個系統檔案已洩漏，請檢查相關情況。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，攻擊者取得了 www-data 的權限，因此僅有/etc/passwd 的內容被洩漏。
- 調查員評論：攻擊者已將/etc/passwd 帶走。我們已檢查公司內部帳號的登入狀態，未發現可疑的登入記錄。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - 傳輸位元組數(Bytesout)：968
  - 檔案路徑：/etc/passwd
  - 時間：2024-10-31T17:41:21
  - 上述題組原始說明內容如圖 21 所示。

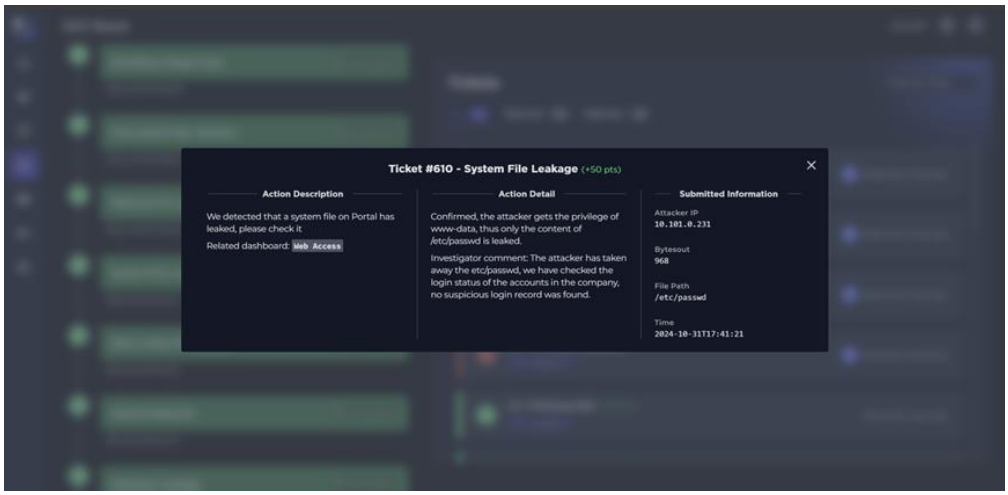


圖 21、系統檔案洩漏(System File Leakage)題組內容

6. 網站配置檔案洩漏(Web Config File Leakage)

- 行動描述:我們偵測到 Portal 上的一個網站配置檔案已洩漏，請檢查相關情況。
- SIEM 相關儀表板：Web Access
- 行動細節:已確認,攻擊者通過Webshell獲取了配置檔案，該檔案包含資料庫密碼。
- 調查員評論：攻擊者已取得資料庫密碼，他接下來會採取什麼行動？
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - 傳輸位元組數(Bytesout)：2041
  - 網站配置洩漏檔案名稱：wp-config.php
  - 檔案洩漏時間：2024-10-31T17:41:21
  - 上述題組原始說明內容如圖 22 所示。

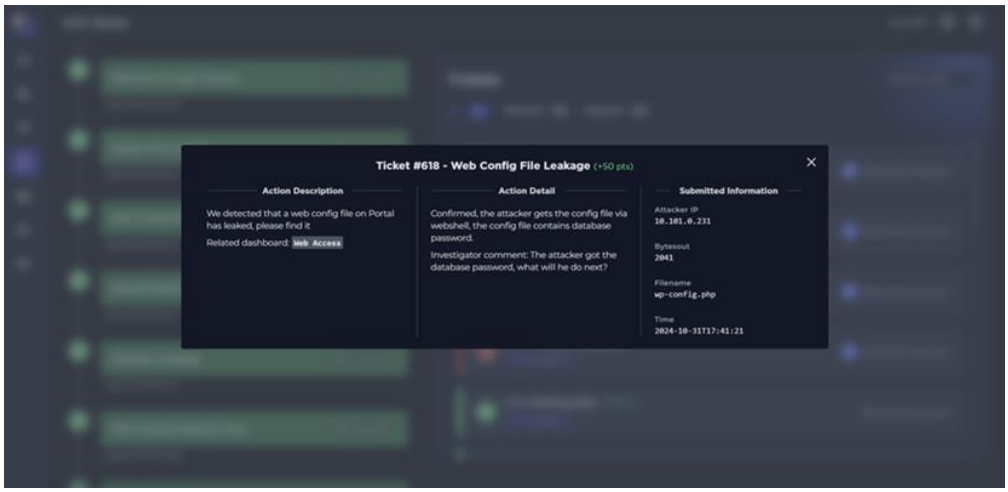


圖 22、網站配置檔案洩漏(Web Config File Leakage)題組內容

7. 上傳 Webshell (Upload Webshell)

- 行動描述：一個具有特權的使用者將一個可疑檔案上傳至 Portal，請調查發生了什麼情況。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，該使用者將一個 Webshell 上傳至 Portal。
- 調查員評論：攻擊者成功取得了 Webshell，此主機已被入侵。接下來，我們必須找到方法確認攻擊者在此主機上進行了哪些操作。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - Webshell 上傳時間：2024-10-31T17:41:21
  - URI：/wp-admin/update.php
  - Webshell 路徑：/wp-content/plugins/VTKYVpYG/VTKYVpYG.php
  - 上述題組原始說明內容如圖 23 所示。

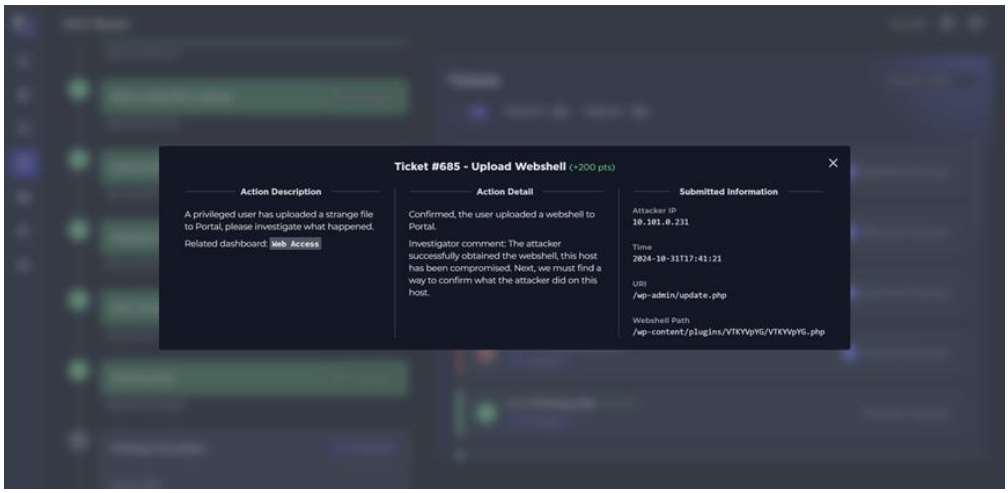


圖 23、上傳 Webshell (Upload Webshell)題組內容

8. 資料庫洩漏(Database Leakage)

- 行動描述:我們偵測到資料庫已遭洩漏,請調查相關情況。
- SIEM 相關儀表板：Web Access
- 行動細節：已確認，攻擊者使用 mysqldump 並通過取得的密碼導出資料庫。
- 調查員評論：攻擊者已取得整個資料庫。幸運的是，資料庫中僅包含 1 個 admin 帳號，且無敏感數據。
- 答題所提交之資訊：
  - 攻擊者 IP：10.101.0.231
  - 資料庫密碼：WORDpress1234!!
  - 檔案名稱：db.dump
  - 時間：2024-10-31T17:41:21
  - 上述題組原始說明內容如圖 24 所示。

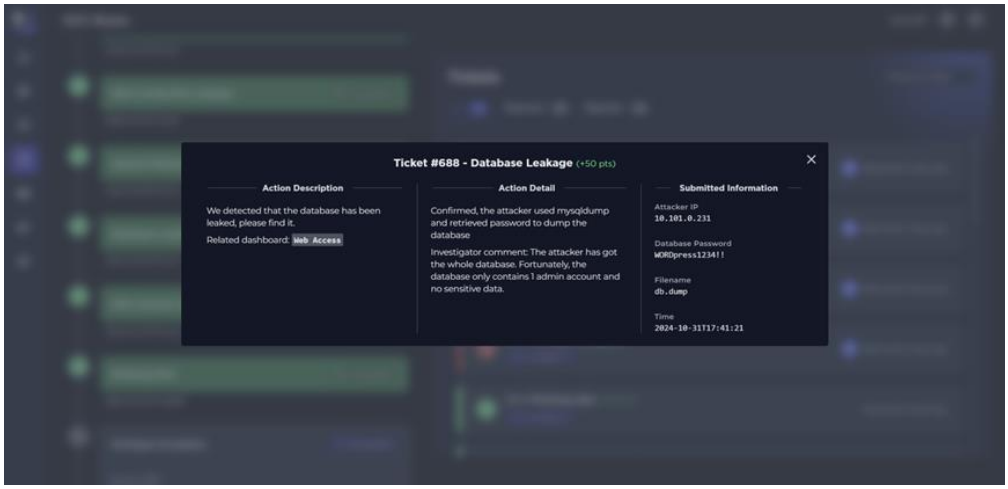


圖 24、資料庫洩漏(Database Leakage)題組內容

9. DMZ 至內部網路的網路掃描(DMZ-Intranet Network Scan)

- 行動描述：我們偵測到從 DMZ 到內部網路的異常流量，請調查相關情況。
- SIEM 相關儀表板：Firewall Status
- 行動細節：已確認，受感染的主機 Portal 向內部網路發起了連接埠掃描。
- 調查員評論：通常在掃描之後，攻擊者會嘗試通過受感染的主機進一步攻擊內部網路。目前尚未發現任何後續攻擊行為。
- 答題所提交之資訊：
  - 最大掃描連接埠：3389
  - 最小掃描連接埠：22
  - 掃描來源 IP：192.168.0.80
  - 目標子網路：192.168.1.0/24
  - 上述題組原始說明內容如圖 25 所示。

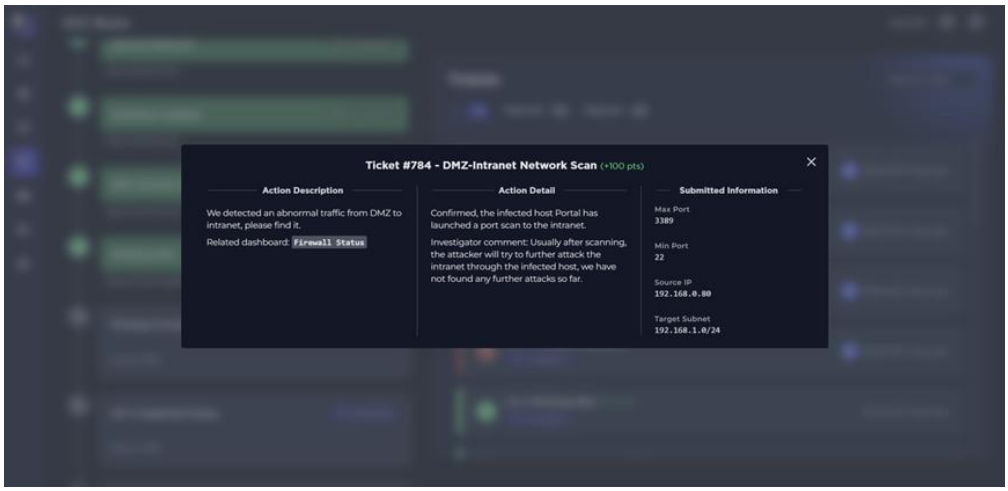


圖 25、DMZ 至內部網路的網路掃描(DMZ-Intranet Network Scan)題組內容

10. 網路釣魚郵件(Phishing Mail)

- 行動描述：我們發現有使用者打開了可疑檔案，且主機 HR-1 與互聯網建立了奇怪的連線。請調查以下事項：
- 建立回呼(callback)連線的程序
- 父程序和可疑檔案
- 產生可疑檔案的程序
- 哪封郵件包含了可疑檔案
- SIME 相關儀表板:Firewall Status、Windows Host Monitor、Mail Log from Snort
- 行動細節：已確認，該檔案包含利用 CVE-2017-0262 漏洞的封包(payload)，當使用者用 Word 軟體打開文件時，將會與回呼 IP 和連接埠建立後門連線。
- 調查員評論：當駭客成功進入內部網路後，極有可能會繼續嘗試提權和橫向移動，或嘗試竊取有價值的資料。因此，有必要仔細檢查受害主機，了解駭客在主機上所做的行為，並調查該主機的所有連線。
- 答題所提交之資訊：

- 附件名稱：gbcPfYJFeX.rar
- 回呼完整網域名稱(fully qualified domain name, FQDN)：webshop.xyz.com
- 回呼連接埠：37880
- 郵件收件人：hruser@enterprise.com
- 郵件 ID：20241031174414.001804@Attacker
- 打開郵件檔案之使用者：hruser
- 上述題組原始說明內容如圖 26 所示。

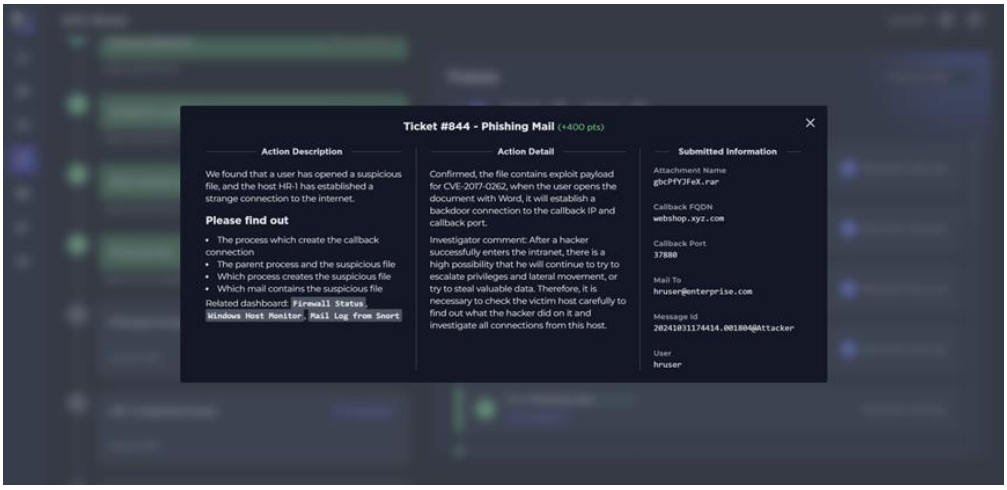


圖 26、網路釣魚郵件(Phishing Mail)題組內容

11. 特權提升(Privilege Escalation)

- 調查行動：特權提升
- 題組說明:我們發現主機 HR-1 上啟動了一個具有特殊權限的奇怪程序，請調查此程序。
- SIEM 相關儀表板：Windows Host Monitor、Windows Event Viewer
- 答題所需提交之資訊：
  - 可執行檔名稱：用來提升特權的可執行檔名稱
  - 原始使用者：原本的使用者名稱

- 特權執行檔案：特權提升後執行的檔案
- 特權使用者：具有特權的使用者名稱
- 上述題組原始說明內容如圖 27 所示。

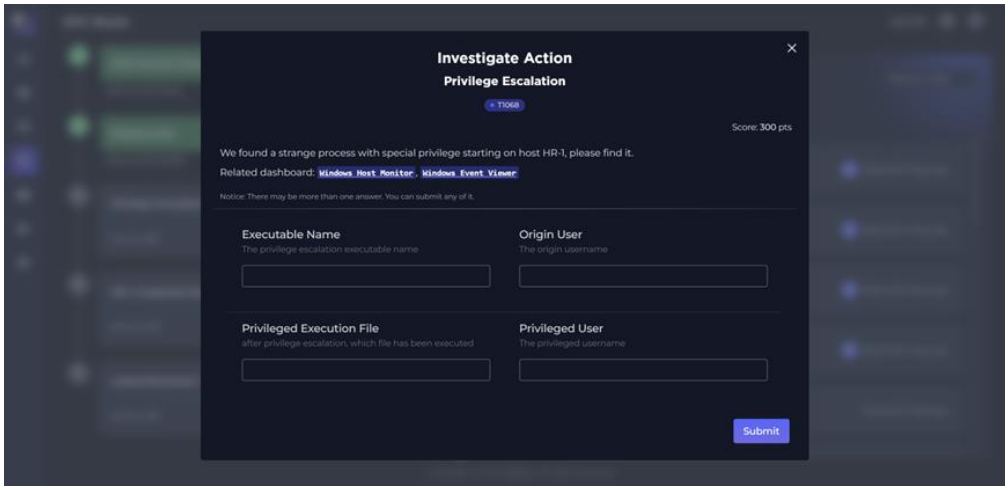


圖 27、特權提升(Privilege Escalation)題組內容

12. HR-1 憑證轉儲(HR-1 Credential Dump)

- 調查行動：HR-1 主機憑證轉儲
- 題組說明：我們偵測到 Windows 客戶端上有憑證轉儲的嘗試，請調查此情況。
- SIEM 相關儀表板：Windows Host Monitor
- 答題所需提交之資訊：
  - 程序 ID
  - 程序名稱
  - 事件發生時間
  - 該程序的使用者名稱
  - 上述題組原始說明內容如圖 28 所示。

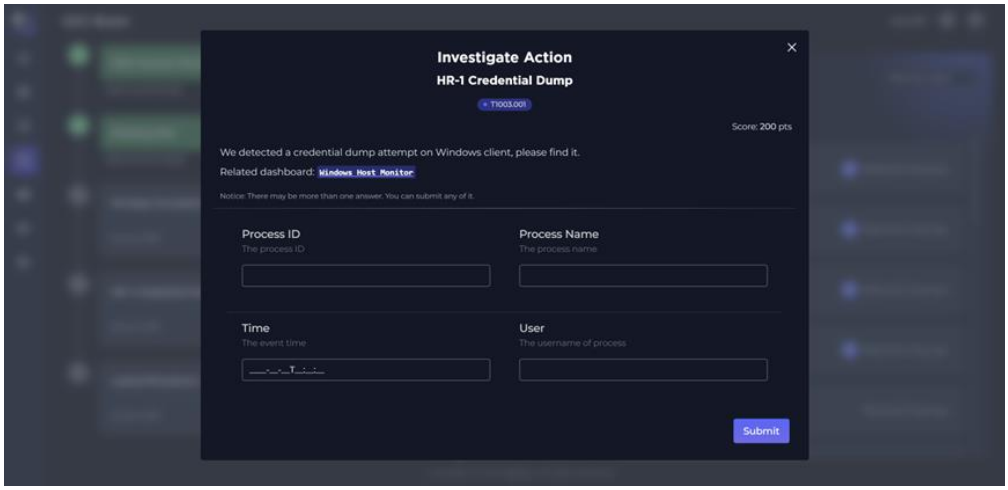


圖 28、HR-1 憑證轉儲(HR-1 Credential Dump)題組內容

13. 橫向移動-傳遞雜湊值(Lateral Movement – Pass the Hash)

- 調查行動：橫向移動 – 傳遞雜湊值
- 題組說明：受感染的主機已成功登入另一台主機，請調查此情況。
- SIEM 相關儀表板：Windows Host Monitor、Windows Event Viewer
- 答題所需提交之資訊：
  - 登入之目標主機(Host)
  - 登入的類型
  - 來源 IP
  - 事件發生的時間
  - 登入的使用者名稱
  - 上述題組原始說明內容如圖 29 所示。

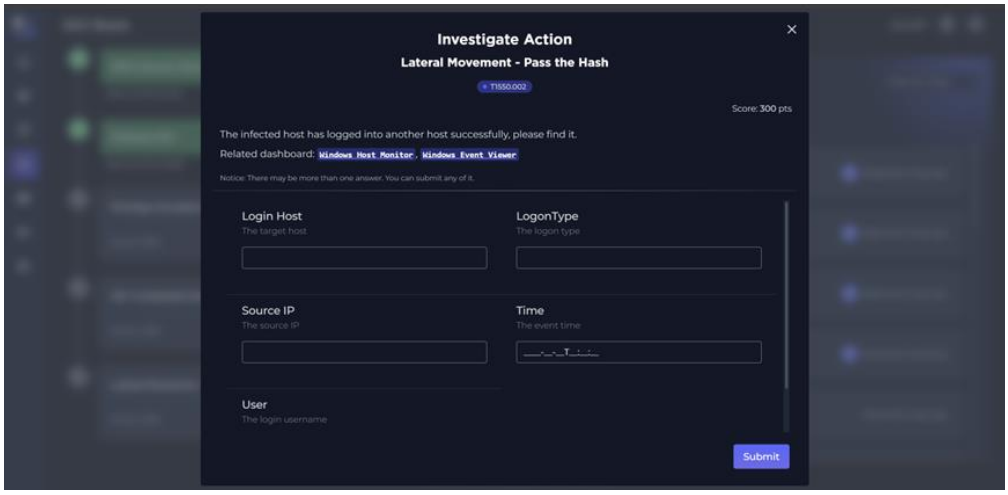


圖 29、橫向移動-傳遞雜湊值(Lateral Movement－Pass the Hash)題組內容

總體來看，這次攻擊可能之主要目的為，竊取公司內部資料，包括使用者密碼和敏感資料，利用網站和內部網路中的漏洞進行擴散，並維持對受害主機的控制，探索和滲透內部系統，進行權限提升和橫向移動，進一步侵入公司的內部基礎設施。

而根據上述所有題組的描述內容，可以歸納並推測這次活動體驗所開放網路攻擊腳本的手法和過程如下：

1. 初步入侵與暴力破解攻擊

攻擊者可能通過暴力破解或弱密碼攻擊進行了初步的入侵。根據 Ticket #516 的描述，攻擊者使用暴力破解的方式，從管理頁面登入並獲得了 admin 帳號的控制權。這可能是通過常見的預設密碼或弱密碼完成的。

2. 惡意程式上傳

一旦攻擊者成功登入管理後，根據 Ticket #685，攻擊者將 Webshell 上傳到受害網站的 Portal 上。Webshell 是一種植入於網站伺服器的惡意腳本，它允許攻擊者透過網頁

介面控制受感染的伺服器，並進行後續的攻擊操作。

3. 網路掃描與內部網路滲透

攻擊者利用受感染主機進行了網路掃描，這在 Ticket #784 中有描述，攻擊者從 DMZ 發起了對內部網路的連接埠掃描，這表示攻擊者試圖利用受感染的主機尋找內部網路中的其他漏洞，進一步滲透內部系統。

4. 資料庫滲透與洩漏

根據 Ticket #549 和#688，攻擊者透過 SQL 注入攻擊或其他漏洞(如 CVE-2017-0262)成功滲透並導出了資料庫密碼，並進一步獲得了/etc/passwd 和資料庫的憑證資料，這表示攻擊者不僅掌握了管理員帳號的密碼，還試圖竊取更多內部資料。

5. 利用惡意郵件釣魚攻擊

在 Ticket #844 中，攻擊者使用了釣魚郵件進行進一步的滲透，該郵件包含了利用漏洞代碼的檔案，表示攻擊者可能已經使用社交工程手段，將受害者誘騙打開了含有 Webshell 的附件，進而建立了回呼連線，使得攻擊者能夠與受害主機進行遠端通訊並控制它。

6. 憑證轉儲與特權提升

根據 Ticket #1003 和#1550.002，攻擊者在攻破內部網路後，進行了憑證轉儲動作，並利用轉儲的憑證進行特權提升和橫向移動，這表示攻擊者在成功登入一台主機後，利用從其他系統或主機獲取的憑證繼續提升其訪問權限，並利用這些權限來進一步滲透網路內部，控制更多的資源和伺服器。

7. 資料外洩與回連

在此過程中，攻擊者可能已經從受感染的主機導出了敏感

資料，例如資料庫憑證、使用者帳號、密碼等。在 Ticket #610 和#618 中提到的資料洩漏問題，顯示攻擊者在利用權限控制之後，進一步導出包含敏感資訊的檔案，並建立回呼連線來盡可能地獲取更多資料。

本次 TRAPA Cyber Range™訓練平台的體驗雖無法完成所有題組解題，但藉由該平台之環境與題組設計，可感受到該公司團隊對於培訓藍隊資安鑑識人員所需平台開發之用心，特別是在 SIEM 各項 log 之紀錄具有嚴謹之前後連貫性，而非僅是為了解題而設計具有強烈目的性之 log,非常貼近真實之網路場景，讓使用(訓練)人員不會有為了解題而解題的感受，評估相當適合作為訓練單位人員資安鑑識能力之優秀平台。

(三)會場專區展覽：

1. MS&AD インターリスク総研：

AttackIQ 是一個安全控制驗證和攻擊模擬產品的供應商。參考 MITRE ATT&CK 框架，模擬對手的策略、技術和程序，並透過資料分析和緩解指南提供對應的安全計畫。該公司於本次大會中展示其研發的一款同名滲透測試服務整合平台 ATTACKIQ READY，主要功能包括：

(1)入侵與攻擊模擬即服務(Breach and Attack Simulation-as-a-Service，BAS)：自動化、持續的安全驗證。由 ATTACKIQ 的專家策劃測試內容，尋找並修復防禦中的漏洞以及不恰當的安全控制設定。

(2)彈性化的測試：隨時隨地可自訂測試。依照假想攻擊組織模擬攻擊場景，以了解現有的安全控制設定與實際上的差距。

(3)及時偵測：及時回報安全控制設定的成效，並持續提供可精進的解決方案。

(4)MITRE ATT&CK 框架：與 MITRE ATT&CK 框架深度整合，所有的建議以及引導都循框架，使使用者能夠與稽核人員、保險公司或高階主管溝通安全狀況。

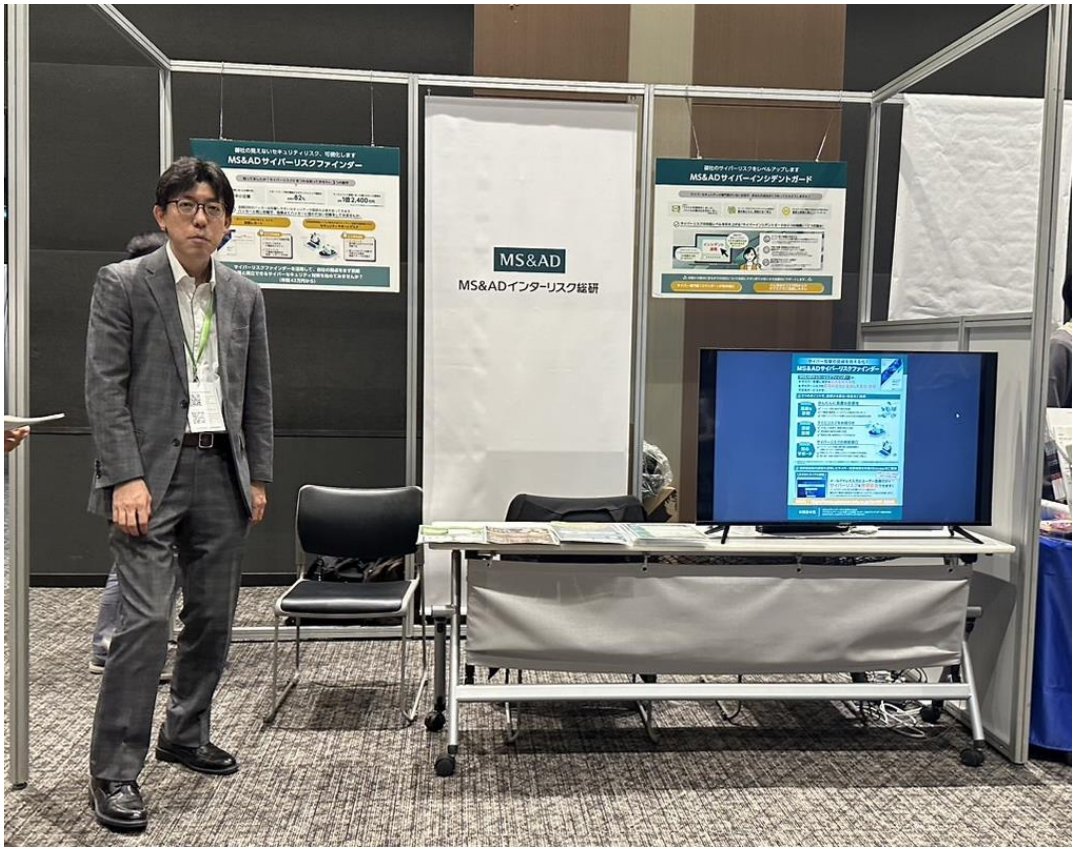


圖 30　MS&AD インターリスク總研提供服務介紹

2. NEC（日本電氣株式會社）：

NEC 是全球資訊技術和網絡解決方案的領導企業之一，在資訊安全 領域具有強大的專業能力與技術創新。以下是 NEC 在資訊安全領域的主要貢獻與服務；

(1)端到端的資訊安全解決方案:提供從基礎設施到應用層的完整安全解決方案，涵蓋以下領域：網絡安全（Network Security）、數據保護與隱私（Data Protection＆Privacy）、雲安全（Cloud Security）、

物聯網安全（IoT Security）。

(2)人工智慧驅動的威脅檢測:利用人工智慧和大數據技術進行威脅監測與分析，主動識別網絡異常和潛在威脅。提供實時的威脅情報和預警服務，幫助企業快速應對網絡攻擊。

(3)生物識別技術:領先世界的生物識別技術：臉部識別(Facial Recognition)、指紋識別 (Fingerprint Recognition)、虹膜識別(Iris Recognition)，用於提升身份驗證的安全性，應用於邊境安全、金融服務和智慧城市。

圖 31 NEC（日本電氣株式會社)服務介紹

3. SCSK 株式会社：

是日本一家領先的 IT 服務與解決方案公司，其子公司 SCSK セキュリティ株式会社 專注於 資訊安全 領域。以

下是 SCSK 在資訊安全領域的主要貢獻與服務：

(1)資訊安全諮詢與管理，風險評估，提供全面的企業資訊安全風險評估，幫助企業識別並減少安全漏洞。安全策略設計，協助企業制定資訊安全政策，涵蓋網絡架構、數據保護與應急計畫。法規合規支，確保企業符合 GDPR、ISO 27001、NIST 等國際與地方法規。

(2)網絡安全解決方案，提供高效的網絡安全服務，包括：入侵檢測與防禦系統(IDS/IPS)、防火牆管理、安全事件監控(SIEM)實時監控網絡威脅，主動防禦惡意攻擊。

(3)雲安全與數據保護，提供針對雲端架構的專業安全服務，包括：雲端存儲加密、訪問控制管理、數據洩露防護(DLP)，防止敏感數據洩露，確保數據傳輸和存儲的安全性。

(4)工業與 IoT 安全，為製造業和物聯網(IoT)提供定制化的安全解決方案，涵蓋工業控制系統(ICS)的安全保障、智能設備和連接環境的風險管理、確保關鍵基礎設施的運行安全。

圖 32 SCSK 株式会社服務介紹

4. NRI Secure Technologies（野村綜研資訊安全技術公司）

是日本領先的資訊安全服務提供商，專注於為企業和政府機構提供全面的資訊安全解決方案。公司在漏洞評估、風險管理和合規性支持方面擁有深厚的專業技術，協助企業滿足 GDPR、ISO 27001、PCI DSS 等國際標準。其 24/7 的安全運營中心(SOC)能即時監控網絡威脅，提供入侵檢測、防火牆管理和安全事件響應服務。

NRI Secure 還專注於雲安全與數據保護，幫助企業實施訪問控制、數據加密和數據洩露防護（DLP）。此外，通過高級威脅檢測和人工智慧技術，該公司能識別並應對高級持續性威脅（APT）。他們還提供資安培訓和模擬演練，提升員工安全意識和應變能力。

圖 33　NRI Secure Technologies 服務介紹

5. NTT DATA

在資訊安全領域具有廣泛的專業技術與解決方案。該公司專注於幫助企業應對複雜的網絡威脅，提供端到端的安全服務，包括風險管理、數據保護和事件響應。

NTT DATA 提供全面的安全評估與管理服務，包括漏洞掃描、滲透測試以及合規支持（如 GDPR、ISO 27001、PCI DSS）。他們的安全運營中心（SOC）能夠即時監控網絡威脅，並提供安全事件調查和快速應對。針對雲端和物聯網環境，NTT DATA 提供專業的安全解決方案，如雲存儲加密、身份驗證和 IoT 設備保護。

此外，NTT DATA 利用人工智慧和大數據技術進行威脅檢測與分析，有效應對高級持續性威脅（APT）。他們還提供資安教育和模擬演練，幫助企業提升內部安全意識。

圖 34　NTT DATA 攤位展示

6. TRAPA

提供創新的技術和解決方案，幫助企業應對現代化的網絡威脅與風險管理挑戰。TRAPA 利用人工智慧與機器學習技術，實現高效威脅檢測與防禦，並結合多層次防禦策略（如入侵檢測與防禦系統）降低攻擊風險。其漏洞管理服務幫助企業識別系統弱點並進行修補，全面提升資安能力。此外，TRAPA 在雲端安全與資料保護方面提供加密與資料洩露防護（DLP），確保敏感資訊的機密性。針對安全事件，TRAPA 提供快速響應與復原計劃，確保企業在遭遇攻擊後迅速恢復運營。公司同時專注於資安教育與合規支持，協助企業滿足 GDPR、ISO 27001 等法規要求。

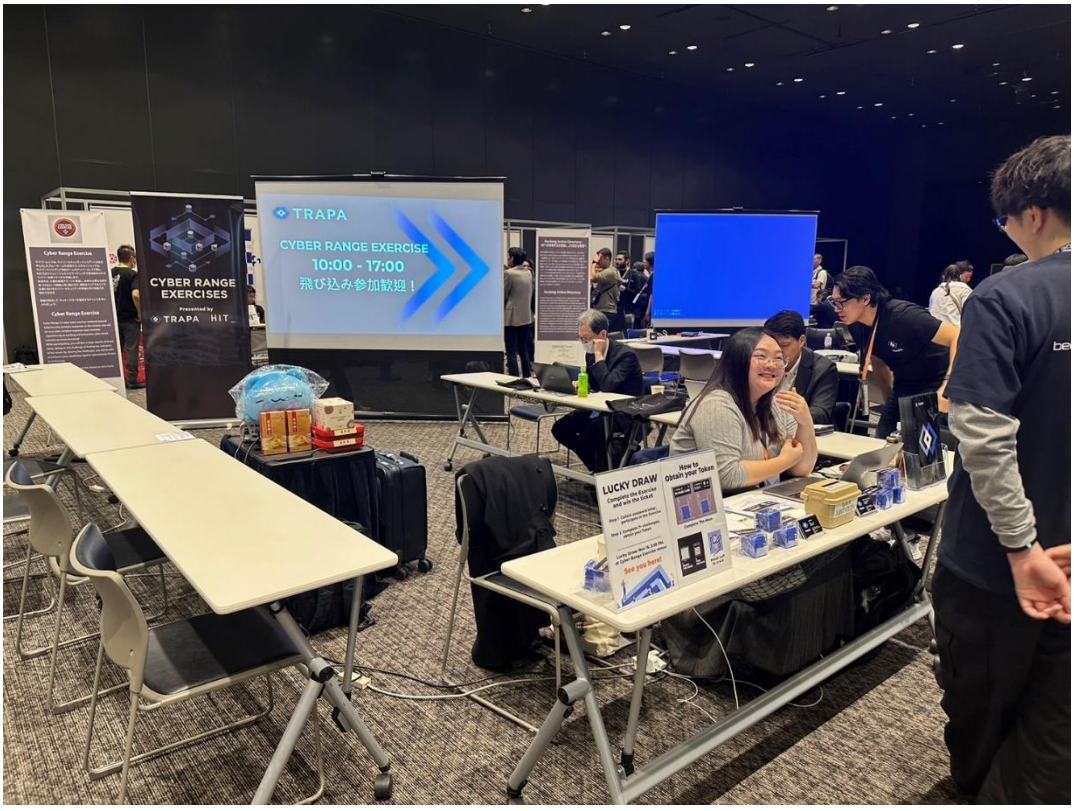


圖 35　TRAPA 攤位展示

肆、心得與建議：

一、 心得：

（一）AI 模型的安全性和隱私保護至關重要： 隨著 AI 技術的發展，AI 模型被廣泛應用於各個領域，但也帶來了新的安全風險。攻擊者可能利用 AI 模型的漏洞來竊取數據、操控模型行為，甚至發動攻擊。同時，AI 模型的訓練數據也可能洩露用户的隱私資訊。因此，確保 AI 模型的安全性、隱私性和可靠性至關重要。

（二）傳統鐵路信號系統存在安全漏洞：傳統的鐵路信號系統缺乏現代安全機制，容易受到駭客攻擊。例如，攻擊者可以偽造信號，導致列車停止或發生意外。因此，必須加強傳統基礎設施的安全性，並導入現代化的安全技術來防範攻擊。

（三）雲端安全防護面臨新的挑戰：雲端服務的普及也帶來了新的安全挑戰。攻擊者可以利用雲端服務的漏洞來竊取數據、發動 DDoS 攻擊，甚至入侵企業內部網路。因此，企業需要提升雲端安全的防禦能力，並採取適當的安全措施來保護雲端環境。

（四）軟體供應鏈安全需要持續關注： 軟體供應鏈攻擊日益猖獗，攻擊者可以透過入侵軟體供應商或植入惡意程式碼來攻擊目標系統。因此，確保軟體供應鏈的安全性至關重要，例如嚴格審查軟體供應商、使用軟體物料清單(SBOM)和軟體簽署技術等。

（五）模糊測試技術有助於提升軟體安全性：模糊測試是一種有效的漏洞挖掘技術，可以自動生成大量的測試案例來檢測軟體中的潛在漏洞。透過持續整合和持續交付(CI/CD)流程整合模糊測試工具，可以更早地發現和修復軟體漏洞。

（六）深度學習技術可以用於惡意軟體分析：深度學習技術可以幫助安全研究人員更有效地分析和偵測惡意軟體。例如，利用深度學習模型來分析 API 呼叫序列，可以識別惡意軟體的行為模式和特徵。

（七）駭客攻擊手法不斷演進：駭客組織持續發展新的攻擊技巧和策略，例如利用社群工程技巧、零時差漏洞和供應鏈攻擊等。安全研究人員需要持續關注最新的攻擊趨勢和技術，並更新防禦策略。

（八）資安人才培育需要多元化管道：全球面臨資安人才短缺的問題，需要透過多元化管道來培養資安人才，例如舉辦資安競賽、工作坊和訓練營等。同時，也需要鼓勵女性和年輕人參與資安領域。

（九）資安防禦需要結合人工智慧和專家知識：AI 技術可以幫助自動化部分資安工作，但仍然需要安全專家的知識和經驗來制定策略、分析威脅和應對攻擊。因此，AI 技術和專家知識的結合才能有效提升資安防禦能力。

（十）國際合作對於應對網路威脅至關重要：網路攻擊無國界，各國需要加強合作，分享威脅情報、最佳實務和應對策略，才能有效應對跨國網路攻擊

二、 建議：

（一）強化勒索軟體防禦，應建立完善的應變機制，包括定期備份重要資料並將其儲存在離線且安全的環境中，以防止勒索軟體加密或刪除備份資料；限制用戶權限，僅授予最低必要權限，降低攻擊影響範圍；及時更新系統和軟體，修補已知漏洞以減少攻擊成功率；部署防毒軟體與 EDR 解決方案，偵測並防範潛在威脅；提升員工資安意識，教育員工識別可疑郵件與網站並避免點擊危險連結；進行模擬攻擊演練，評估組織的應變能力並持續完善應變計劃；以及建立全面的事件應變流程，包括通報、隔離受感染系統、資料恢復與與執法機構合作等具體步驟，從而提升整體防禦與應變能力。

（二）積極監控子網域活動並利用威脅情報進行防禦，可採取以下措施：使用威脅情報平台和安全工具監控可疑的子網域註冊和解析活動，及時封鎖已知的惡意子網域並將其加入黑名單；研究和部署如 AADNS 等新型防禦技術，以有效偵測和防範子網域濫用攻擊；同時，與其他組織共享威脅情報，增強集體防禦能力並提升整體資安效益。

（三）加強防範釣魚攻擊，應多管齊下提升員工警覺性，包括部署反釣魚郵件閘道過濾可疑郵件，使用多因素驗證防止攻擊者竊取帳號密碼後登入系統；教育員工識別與報告可疑郵件和網站，並避免點擊可疑連結；定期進行釣魚攻擊模擬演練，以評估員工警覺性和組織防禦能力；利用反釣魚

瀏覽器擴充功能協助識別釣魚網站；並與社交媒體平台合作，移除釣魚帳號與貼文，從多方面構建全方位的防禦策略。

（四）提升軟體供應鏈安全並落實安全開發流程，應嚴格審查軟體供應商的安全性，並要求提供安全證明文件；利用 SBOM 追蹤軟體組成成分，識別潛在漏洞和安全風險；實施軟體簽署驗證，確保軟體來源的可靠性；建立包含程式碼審查、安全測試與漏洞修補的安全開發流程；同時，採用容器化技術，如 Docker 和 Kubernetes，隔離應用程式運行環境，降低供應鏈攻擊的影響範圍，從而全方位保障軟體供應鏈的安全性。

（五）積極投入漏洞研究與利用，並與安全社群合作，應建立專門的漏洞研究團隊，負責研究與分析最新漏洞資訊；與外部安全研究機構合作，分享漏洞資訊與研究成果；推動漏洞回報獎勵計劃，獎勵安全研究人員發現並報告漏洞；基於最新漏洞資訊，開發創新的攻擊手法與防禦技術；同時，積極參與開源安全社群，貢獻程式碼與知識，促進社群合作並提升整體安全水平。

（六）推廣模糊測試技術的應用並將其整合到 CI/CD 流程中，應鼓勵在軟體開發過程中使用模糊測試工具，以早期發現和修復軟體漏洞；將模糊測試嵌入 CI/CD 流程中，自動化測試環節，提升效能與效率；研究並開發自動化模糊測試平台，降低技術應用門檻，讓更多團隊能輕鬆採用；同時，

採用基於覆蓋率的模糊測試技術，進一步提高測試效率與有效性，從而增強軟體的安全性與穩定性。

（七）建立多層次防禦架構並加強威脅情報與事件分析能力，應導入零信任架構，驗證每個使用者與裝置的身份並限制其存取權限；部署入侵偵測與防禦系統（IDS/IPS），以即時偵測並防範惡意網路流量；使用網路行為分析(NBA)和安全資訊與事件管理(SIEM)系統，分析網路活動日誌並識別可疑行為；加強端點安全防護，防止惡意軟體與勒索軟體攻擊；同時建立威脅情報分析團隊，負責收集、分析並分享威脅情報，從而構建全面的防禦能力，提升網路安全性和應變效率。

（八）加強資安意識培訓並提升員工對新興威脅的認知，應針對不同職位與權限等級設計客製化資安培訓課程，例如為開發人員提供安全程式碼培訓，為管理人員提供資安風險管理課程；定期進行資安演練和模擬攻擊，評估員工應變能力並增強他們的警覺性；推廣資安意識與最佳實務，包括使用強密碼、定期更新軟體及避免點擊可疑連結；透過內部網路、電子郵件和社交媒體等多種管道進行資安宣導；同時建立資安回報機制，鼓勵員工主動報告可疑活動與安全事件，從而形成全員參與的資安文化。

（九）積極參與國際合作，共同應對跨國網路犯罪，應積極參與國際資安組織和活動，例如 FIRST 和 INTERPOL 等，深化全球資安網絡的聯繫；與其他國家和地區的資安機構建立合

作關係，分享威脅情報與最佳實務，促進跨境資訊流通；參與國際資安演練與聯合行動，提升協同作戰的效率與應對能力；同時，與國際社群共同制定資安標準與規範，推動全球資安合作的統一性和有效性，應對日益嚴峻的跨國網路威脅。

（十）提升國家整體防禦能力，應持續投資於最新的資安技術與解決方案，例如 AI 驅動的資安工具和雲端安全服務；支持資安人才培育與發展計劃，提供獎學金、實習機會及專業認證，吸引並留住高素質資安人才；鼓勵資安研究與創新，促進學術界與產業界的合作，開發前沿資安技術和解決方案；同時，建立國家級資安研究機構，專責研究與分析最新網路威脅，並制定與實施國家資安戰略，從技術、人才與政策層面全面增強防禦能力。

附錄 1

DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
11/14	09:00	AI for formal verification; formal verification for AI 人工智慧用於形式化驗證；AI 的形式驗證		
	10:00	Piloting Edge Copilot 操控 Edge Copilot	〔PwC コンサルティング合同会社〕AI レッドチーム：生成 AI サービスにおけるセキュリティリスクに対する取り組み 〔PwC Consulting LLC〕AI 紅隊：針對生成式 AI 服務 PwC 咨詢股份有限公司-AI 紅隊：應對生成式 AI 服務中的安全風險	Automatically Detect and Support Against Anti-Debug with IDA/Ghidra to Streamline Debugging Process 使用 IDA/Ghidra 自動檢測並支援反調試機制，以簡化除錯流程
	10:45			
	10:50	Proxying to Kernel:Streaming vulnerabilities from Windows Kernel 代理到核心:從 Windows 核心流出的漏洞		
	10:55		〔日本電気株式会社〕AI エージェントを活用したサイバー脅威インテリジェンス生成 日本電氣股份有限公司 (NEC)-運用 AI 代理生成網路威脅情報	
	11:00			BullyRAG:A Multi-Perspective RAG Robustness Evaluation Framework BullyRAG：一個多視角的 RAG 健壯性評估框架
	11:25			
	11:40			
	12:50	Defeating		

DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
	13:00	PlayStation 5 network encryption 破解 PlayStation 5 網路加密		EchidnaTermApp:Penetration Test Assist & Learning Tool EchidnaTermApp：滲透測試輔助與學習工具
	13:15		〔株式会社 Flatt Security〕設定ミスによる情報漏洩だけじゃない。S3 等のオブジェクトストレージの脅威を包括的に理解する Flatt Security 股份有限公司-不只是設定錯誤導致的信息外洩——全面理解 S3 等物件儲存的威脅	
	13:40	Attention Is All You Need for Semantics Detection:A Novel Transformer on Neural-Symbolic Approach 語義檢測的全新方法：基於神經符號的新型轉換器模型		
	13:45			
	13:55		〔株式会社 CyCraft Japan〕次世代 EASM：外部攻撃パスシミュレーションのための AI コパイロット CyCraft Japan 股份有限公司-次世代 EASM：用於外部攻擊路徑模擬的 AI 副駕駛	
	14:00			Event Tracing for Windows Internals Windows 內部事件追蹤
	14:20			
	14:25			
	14:35		〔NTT データ先端技術株式会社〕AI 活用ルール策定とリスクについて NTT DATA 先端技術	
	14:50	SBOM and Security Transparency -		
	15:00			Modern SOC:Less Than One and More
	15:05			

DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
		How it all fits together 軟體物料清單（SBOM）與安全透明性：完整解析其相互關聯	股份有限公司-AI 活用規範的制定與風險探討	Than Infinity 現代化安全運營中心（SOC）：少於一，卻多於無限
	15:15		〔FutureVuls／株式会社ディアイティ〕脅威となるサイバー攻撃・ランサムウェアに備える脆弱性対策とは～インシデント発生現場の裏側から学ぶ～ FutureVuls / 株式會社迪艾提 (dit)- 如何防範威脅性網路攻擊與勒索軟體——從事故發生現場學習的脆弱性對策	
	15:30			
	15:40	Abusing legacy railroad signaling systems 濫用舊式鐵路信號系統		
	15:45			
	16:00		〔パナソニックホールディングス株式会社〕 Panasonic IoT Threat Intelligence "ASTIRA"とその活用事例：車載ソフトウェア脆弱性分析ソリューション VERZEUSE® for SIRTCorporation	NTLMv1 reversion to NTLM with hashcat and the NTLMv1-multi tool NTLMv1 降版至 NTLM，使用 hashcat 和 NTLMv1-multi 工具
	16:20			
	16:30	Hacking Google - Lessons learned running and growing an internal red team 入侵 Google：運營與強化內部紅隊的經驗教訓		
	16:40			
	16:45			
	17:10			
	17:20	An Inside Look at Pixel Security 深入探討 Pixel		
	18:00			

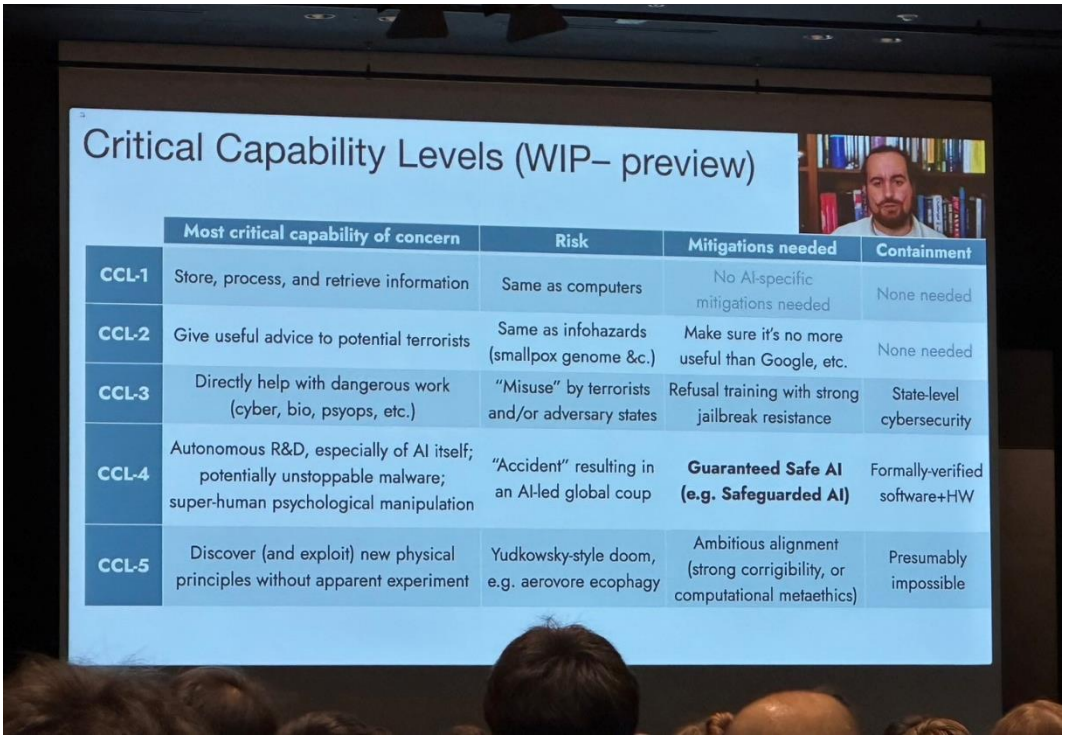
DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
		的安全機制		
11/15	09:00	Did Subdomain Abuse by BlackTech “Evolve”？ BlackTech 的子域名濫用是否已經“進化”？		
	09:50	PkgFuzz Project:Yet Another Continuous Fuzzing for Open Source Software PkgFuzz 專案：針對開源軟體的又一持續模糊測試工具		
	10:00		〔株式会社日立システムズ〕第 1 部：サイバー領域視点でのセキュリティ / 第 2 部：中国の全方位情報影響工作 日立系統公司 1.從網路領域視角探討安全性 2.中國的全方位資訊影響工作	
	10:30			
	10:40	APTs in APAC aerospace:when Dragons and Chollimas Reach for the Stars 亞太航空產業的進階持續性威脅(APT)：當巨龍與千里馬邁向星空		
	10:45			
	11:25		〔MS&AD インターリスク総研株式会社〕インシデントマネージメントの重要性 MS&AD 風險綜合研究公司 事件管理的重要性	
	11:30	China’s Evolving Playbook:The Combination of Hack-and-Leak and Influence Operations	〔三井物産セキュアディレクション株式会社〕大規模言語モデルを用いた ASM 運用の自動化 三井物產 Secure	
	12:10			

DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
		中國不斷演變的戰略手法：駭取洩密與影響力行動的結合	Directions 公司利用大規模語言模型（LLM）自動化 ASM 運營	
	13:00		1- Click-Fuzz：Systematically Fuzzing the Windows Kernel Driver with Symbolic Execution. 1-Click-Fuzz：使用符號執行系統化對 Windows 核心驅動進行模糊測試	
	13:20	Behind Enemy Lines:Engaging and Disrupting Ransomware Web Panels 深入敵營：接觸並破壞勒索軟體的網頁面板		
	13:40			
	13:50		WebAssembly Is All You Need:Exploiting Chrome and the V8 Sandbox 10+ times with WASM WebAssembly 就夠了：利用 WASM 在 Chrome 和 V8 沙箱中成功攻擊超過 10 次	
	14:00			
	14:10	V for Vendetta:Dissecting a Global Phishing Platform After Being Phished V 字仇殺隊：被釣魚後解剖全球網路釣魚平台		
	14:30			
	14:40		〔ＳＣＳＫセキュリティ株式会社〕日本における OSINT の 10 年：知見の拡大と業務での深化 SCSK 安全公司日本 OSINT 的 10 年：見解的擴展與業務應用的深化	
	14:50			
	15:10	NGate:Novel Android malware for unauthorized ATM withdrawals via NFC relay NGate：用於 NFC 中繼未授權提款		

DEFCON 研討會議議程表				
日期	時間	場次 1	場次 2	場次 3
	15:20	的 Android 新型惡意軟體	〔ＮＲＩセキュアテクノロジーズ株式会社〕NRI セキュアにおける宇宙セキュリティに関する取組みについて NRI Secure Technologies 公司 NRI Secure 在太空安全領域的相關措施與實践	
	15:50			
	16:00	From Snowflake to Snowstorm:Navigating Breaches and Detections 從雪花到暴風雪：駕馭資安入侵與偵測	〔GMO インターネットグループ株式会社〕GMO イエラエ全員集合！！進化するサイバー攻撃への対策最前線 GMO 網際網路集團公司 GMO Ierae 全員集結！應對不斷進化的網路攻擊最前線	
	16:40			
	16:50	Panel Discussion：International Approaches to Cybersecurity Talent Development and Strategic Initiatives 小組討論：國際間網路安全人才培育與戰略舉措		
	17:50			

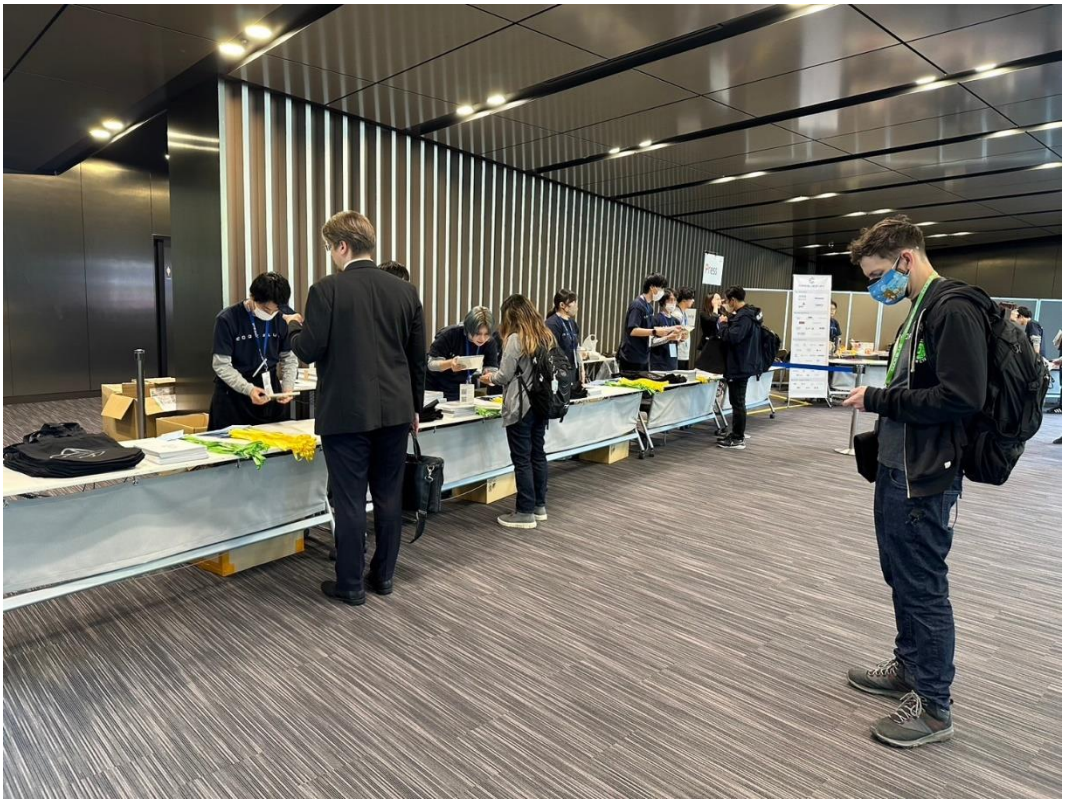
附錄 2

展場活動花絮



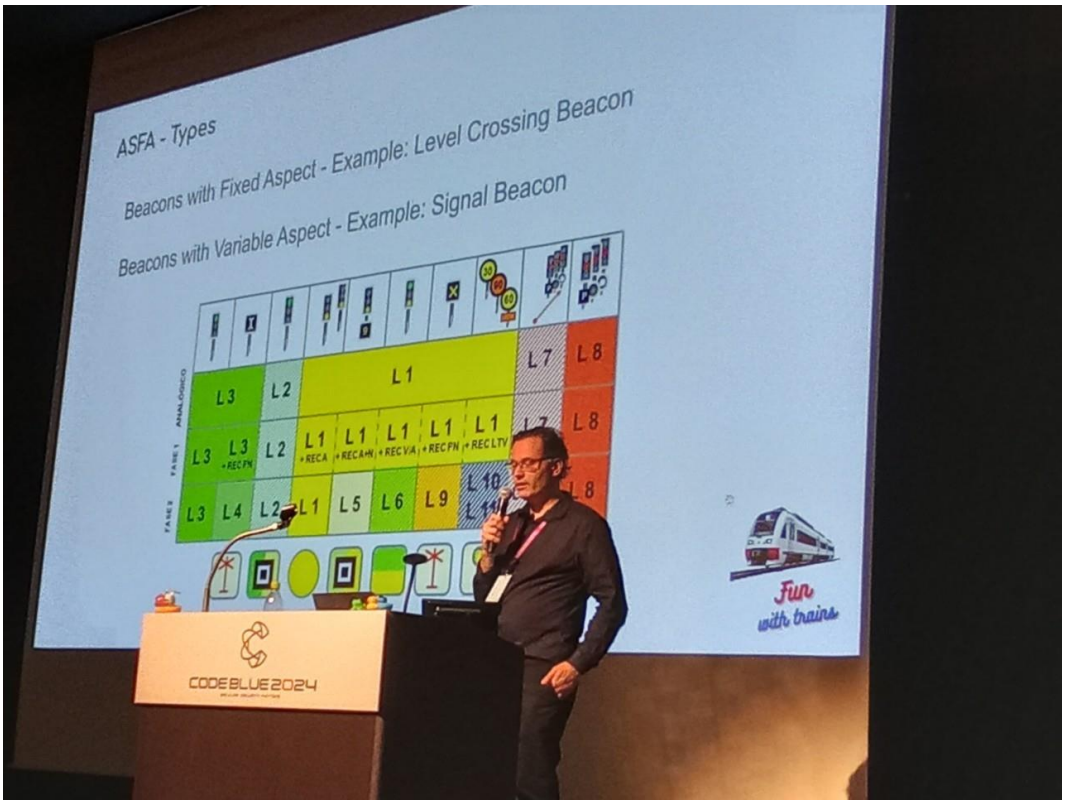
議程：人工智慧用於形式化驗證；AI 的形式驗證 講者：David A. Dalrymple

議程：破解 PlayStation 5 網路加密 講者：Aapo Oksman



CODE BLUE 會場入口

議程：操控 Edge Copilot 講者：Jun Kokatsu



議程：濫用舊式鐵路信號系統 講者：David Melendez

議程：代理到核心:從 Windows 核心流出的漏洞 講者：Angel boy