TWAREN 威脅感知系統之即時攻擊資訊系統部署與比較

黃文源　李柏毅
財團法人國家實驗研究院國家高速網路與計算中心
{wunyuan, 1203007}@narlabs.org.tw

摘要

本論文探討了 TWAREN 威脅感知系統中兩種即時攻擊資訊系統的部署與比較，旨在提升網路攻擊監控與反應效率。隨著雲端計算、物聯網與人工智慧技術的發展，資安威脅日趨嚴峻，促使研究人員設計更有效的攻擊資訊系統。文中介紹了 Honeynet 的概念，並部署了 HoneyMap 與 SecKC Honeypot Dashboard 兩個系統。HoneyMap 與 MHN 集成，部署簡單但資訊有限；SecKC Honeypot Dashboard 提供更多統計資料與視覺化效果，但部署較為複雜。比較結果顯示，HoneyMap 適合快速部署，而 SecKC Honeypot Dashboard 更適合深入分析。研究提供了系統比較與選擇依據，未來將探索更多即時攻擊資訊系統，以提升資安防護能力。

關鍵詞：HoneyMap、Honeynet、Honeypot、TWAREN

Abstract

This paper examines the deployment and comparison of two real-time attack information systems in the TWAREN threat awareness system to improve network monitoring and response. With advances in cloud computing, IoT, and AI, cybersecurity threats have intensified, requiring more effective systems. The paper introduces Honeynet and presents the deployment of HoneyMap and SecKC Honeypot Dashboard. HoneyMap, integrated with MHN, is easy to deploy but provides limited data, while SecKC Honeypot Dashboard offers richer statistics and visualization but requires more complex setup. The comparison results show HoneyMap suitable for quick deployment, while SecKC is better for in-depth analysis. In the Future, we will focus on exploring additional real-time systems to further enhance cybersecurity defense capabilities.

Keywords: HoneyMap, Honeynet, Honeypot, TWAREN

1. 前言

在過去的幾十年裡，網際網路的普及速度驚人。從1990年代初期的少數科研機構和大學使用，到如今全球數十億人每天依賴網際網路進行溝通、娛樂和工作，網際網路已經成為現代社會的基礎設施。這種快速發展得益於多種技術的進步，包括光纖通訊、無線網路和資料壓縮技術。

隨著網際網路的快速發展，我們的生活方式和工作模式發生了翻天覆地的變化。從早期的電子郵件和簡單的網頁瀏覽，到如今的社交媒體、電子商務、與遠端工作，網路技術已經滲透到我們生活的方方面面，也推動了技術的進一步發展，例如雲端計算、物聯網(IoT)與人工智慧(AI)。

雲端計算是指透過網際網路提供計算資源和服務的技術。這些資源和服務包括伺服器、存儲、資料庫、網路、軟體等，並且可以根據需要擴增，用戶只需為實際使用的部分付費。雲端計算的核心理念是將計算資源集中在遠端資料中心，並透過網際網路提供給用戶。這種模式不僅降低了企業的 IT 成本，還提高了資源的利用效率。

物聯網是指透過網際網路將各種設備連接起來，使它們能夠相互通訊和協作。這些設備包括智慧家居設備、工業自動化設備、醫療設備等。藉由雲端平台，這些設備可以即時收集和分析資料，以提供更聰明和高效率的服務。例如，智慧家居系統可以根據用戶的習慣自動調整溫度和照明，工業物聯網可以實現設備的預測性維護，降低故障率和維護成本。

人工智慧是指透過機器學習和資料分析技術，使電腦能夠模仿人類的行為。AI 可以從大量資料中獲取有價值的資訊，並做出智慧決策。AI 的應用範圍非常廣泛，包括語音辨識、圖像辨識、自動駕駛等。雲端計算、物聯網和人工智慧的發展，都離不開網際網路的支持。網際網路提供了高速、可靠的資料傳輸通道，使得各種設備和服務能夠隨時隨地連接和通訊。總之，網際網路是這些技術的基礎設施，推動了它們的普及和進步。

隨著雲端計算、物聯網和人工智慧的廣泛應用，資訊安全問題變得尤為重要。這些技術依賴於大量資料的傳輸和存儲，因此，保護資料的機密性、完整性和可用性至關重要。雲端計算需要確保資料在傳輸和存儲過程中的加密，防止未經授權的訪問。物聯網設備需要強化身份驗證和授權機制，確保只有授權用戶才能存取設備和資料。人工智慧系統則需要防範資料篡改和惡意攻擊，確保分析結果的準確性和可靠性。

為了應對這些挑戰，企業和個人需要採取多種

資安防護措施。這包括資料加密、身份驗證和授權、網路防火牆和入侵檢測系統、定期更新和 Patch 管理，以及安全教育和培訓。這些措施能夠有效保護資料和系統免受各種攻擊，如惡意軟體、DDoS 攻擊、中間人攻擊、釣魚攻擊和勒索軟體攻擊。

在如此多的攻擊手法之下，要有好的資安防護，網路威脅情資（Cyber Threat Intelligence, CTI）扮演著關鍵角色。它透過收集來分析和解釋各種來源的威脅資料，幫助企業預測和防範潛在的攻擊。有效的資安情資可以識別最新的攻擊手法、惡意軟體和攻擊者的行為模式，從而幫助企業及時採取防護措施。網路威脅情資獲取方式除了藉由 OSINT、社群資訊外，也能透過誘捕系統網路獲得。

誘捕系統網路（Honeynet）是一種設置誘餌系統或網路，模擬真實環境以吸引攻擊者，從而收集有價值的攻擊資料。這些誘餌系統是專門設計來觀察和記錄攻擊者的行為，其旨為了解攻擊者的技術和策略，並收集有關攻擊的詳細訊息，以改進企業的安全防護措施。要提高 Honeynet 情資的獲取，就必須得提高其偽裝率，減少被識破率，現今已經有研究人員提出結合軟體定義網路(Software Defined Network, SDN)[1]的方式，以提高 Honeynet 的偽裝率與支援動態誘捕系統(Honeypot)的部署[2][3][4]。

在台灣，國家高速網路與計算中心擁有台灣高品質學術研究網路(TWAREN)，提供高達 100Gbps 的網路頻寬。TWAREN 是由五個骨幹核心主節點以及12個區網中心(GigaPOP)建構而成的，如圖1所示，詳情參見 TWAREN 官網[5]。

圖 1 TWAREN 網路架構[5]

由於 TWAREN 的高速頻寬與穩定性，其上提供了許多平台與服務，例如計算與儲存服務(TWCC)[6]和 SDN。此外，還有與資安防護相關的服務，包括雲端資安攻防平台(CDX)[7]、OWL 惡意程式知識庫[8]和 Honeynet 等。這些服務不僅提升了學術研究的效率，還為資安防護提供了堅實的基礎，確保資料傳輸的安全性和穩定性。

去年我們計畫於 TWAREN 上設計與部署一套基於軟體定義網路技術之響應式網路威脅感知與欺敵系統[9]，以獲取網路威脅情資。原先部署的系統即時攻擊資訊呈現不足，而為了能提高識別各種攻擊的效率，因此我們將額外部署其他的即時攻擊資訊系統，並比較此兩種資訊系統，來呈現各自的優缺點。

本篇論文中，首先會介紹 Honeynet，然後介紹兩種即時攻擊資訊系統的架構，以及說明他們的部署方式，最後展示這兩種即時攻擊資訊系統並比較優缺點。

2. 相關知識

本章中，我們將探討 Honeynet 及其相關軟體。首先，我們將介紹 Honeynet 的基本概念和架構，並說明與之相關軟體與系統，包括 SIEM、IDS/IPS、流量分析工具、威脅情報平台和 syslog 日誌系統，了解它們如何協同工作以提升整體安全防護能力。接著，我們會介紹 MHN（Modern Honey Network），了解其功能與特點，以便知道如何部署和管理，以提升整體安全防護能力。

2.1 Honeynet

Honeynet[10][11][12]是一種由多個 Honeypot 組成的網路安全環境，旨是吸引並監控惡意攻擊者的行為。這些 Honeypot 是故意設置的虛假目標，模擬真實的網路服務，以誘使攻擊者進行攻擊。Honeypot 的主要目的是收集有關攻擊技術、工具和策略（Tactics, Techniques, and Procedures, TTPs）的資訊，從而幫助資安相關人員更好地理解和防禦潛在威脅。

Honeynet 通常由多個不同類型的 Honeypot 組成，包括低互動和高互動 Honeypot。低互動 Honeypot 模擬基本的網路服務和操作系統，主要用於捕獲自動化攻擊，如蠕蟲和機器人網路（botnet）。高互動 Honeypot 則提供更真實的操作環境，允許攻擊者進行更深入的攻擊行為，從而收集更詳細的攻擊數據。

Honeynet 的設計需要考慮多種因素，包括網路拓撲、流量監控和資料分析。為了確保所收集資料的準確性和完整性，Honeynet 通常會部署在隔離的網路環境中，並使用專門的監控工具來記錄攻擊者的每一步操作。這些資料不僅可以用於即時的威脅分析，還可以用於長期的安全研究和防禦策略的制定。

常見的 Honeynet 架構包括以下幾種：

- 分散式 Honeynet：這種架構將多個 Honeypot

分佈在不同的地理位置，以模擬分散的網路環境。這樣可以吸引來自不同地區的攻擊者，並收集更廣泛的攻擊資料。

- 集中式 Honeynet：所有 Honeypot 集中在一個實體或虛擬網路中，便於集中管理和監控。此架構適合於需要高效率資料收集和分析的環境。
- 混合式 Honeynet：結合分散式和集中式架構的優點，既能吸引多樣化的攻擊，又能集中管理和分析資料。
- 結合 SDN 的 Honeynet：結合 SDN 的 Honeynet 可以實現更精細的流量控制和監控，並且能夠快速回應和適應攻擊行為，能在 Honeypot 之間動態轉換，以便收集更詳細的攻擊資料，例如：HoneyProxy[13]。

Honeynet 架構中，可能結合以下類型的系統：

- SIEM（Security Information and Event Management）系統：這些系統能夠收集、分析和報告來自 Honeypot 的安全事件和資料，提供即時的威脅檢測和響應能力。
- IDS/IPS（Intrusion Detection/Prevention Systems）：這些系統可以與 Honeypot 協同工作，檢測並阻止潛在的攻擊行為，並提供詳細的攻擊分析報告。
- 流量分析工具：如 NetFlow 或 sFlow，這些工具可以監控和分析網路流量，幫助識別異常行為和潛在威脅。
- 威脅情報平台：這些平台可以整合來自 Honeypot 的資料，並與其他威脅情報來源進行比對，提供更全面的威脅分析和預警。
- syslog 日誌系統：此系統在 Honeynet 中扮演著重要角色，主要用於收集和存儲來自不同設備和應用程序的日誌資料。它能夠集中管理和分析來自各個 Honeypot 的日誌，提供全面的攻擊行為記錄。

總結來說，Honeynet 透過結合多種技術和工具，如 SDN、SIEM、IDS/IPS、流量分析工具、威脅情報平台和 syslog 日誌系統，提供了一個強大的平台來監控和分析網路攻擊行為。這不僅有助於即時的威脅檢測和響應，還能為長期的安全研究和防禦策略提供寶貴的資料支援。

2.2 Honeypot 管控平台: MHN

Modern Honey Network(MHN)[14]是一款專為管理和收集 Honeypot 資料而設計的軟體，具備多項強大功能。

首先，MHN 提供了簡便的 Honeypot 部署功能。內建的部署腳本讓使用者只需執行簡單的命令即可輕鬆完成 Honeypot 的部署，無需繁瑣的手動配置。這大大降低了部署 Honeypot 的門檻，使得即使是沒有深厚技術背景的使用者也能快速上手。

在威脅情報收集方面，MHN 整合了 MongoDB 和 Hpfeeds 軟體[15]。Hpfeeds 是一個強大的資料傳輸工具，能讓 Honeypot 主動將收集到的資料傳送至 MHN，並記錄至 MongoDB 之內。這種自動化的資料傳輸方式，不僅提高了資料收集的效率，還確保了資料的完整性和即時性。透過 Hpfeeds，使用者能夠即時獲取最新的威脅情報，迅速做出反應，從而提升整體的安全防護能力。

MHN 還提供了直觀的威脅情報展示功能。使用者可以透過 MHN 提供的網頁介面，輕鬆檢視各種收集到的攻擊資訊。這些資訊包括攻擊的來源、攻擊的類型以及攻擊的時間等，幫助使用者全面了解當前的安全狀況。此外，MHN 還提供了即時攻擊資訊視覺化功能，也就是 HoneyMap[16]，使用者可以從地圖中直觀地看到攻擊者的地理位置，進一步提升了威脅情報的視覺化效果。

在資料分析方面，MHN 支援與 ELK 和 Splunk 的資料串接。這意味著使用者可以將收集到的威脅情報與這些強大的資料分析工具整合，進行更深入的分析。ELK（Elasticsearch, Logstash, Kibana）[17] 和 Splunk 是業界領先的資料分析平台，能夠提供強大的資料處理和視覺化功能。透過與這些工具的整合，MHN 能夠幫助使用者更好地理解和分析威脅情報，從而做出更明智的安全決策。

MHN 支援14種不同類型的 Honeypot 部署與資料收集，具體如下：

- Conpot：工業控制系統 Honeypot。
- Drupot：Drupal 內容管理平台的 Honeypot。
- Magenpot：Magento 電子商務平台的 Honeypot。
- Wordpot：WordPress 的 Honeypot。
- Shockpot：Web 應用程式 Honeypot，專門偵測利用 Bash 遠端程式碼漏洞（CVE-2014-6271）的攻擊者。
- P0f：用於檢測主機連接方式的工具。
- Suricata：開源入侵偵測系統。
- Glastopf：Web 應用程式的 Honeypot。
- ElasticHoney：Elastic 的 Honeypot。
- Amun：低互動性 Honeypot。
- Snort：知名的開源入侵偵測系統。
- Cowrie：SSH 和 Telnet 的 Honeypot。
- Dionaea：低互動性 Honeypot。
- Shockpot Sinkhole：用於偵測 Shellshock 和 Sinkholing。

儘管 MHN 支援多種 Honeypot 的部署，但由於其架構和部署腳本均採用 Python 2撰寫，因此需要進行設定修改才能順利部署。這意味著使用者在部

署過程中可能需要對腳本進行一些調整，以確保其能夠在現代環境中正常運行。

3. 即時攻擊資訊系統建置

本章中，我們將介紹兩套即時攻擊資訊系統，並說明各自的協作架構。接著，我們將描述此兩套系統的部署和設定方式，讓使用者能了解此如何有效地部署一個能夠即時顯示攻擊資訊的 Honeypot。

3.1 即時攻擊資訊系統介紹

即時攻擊資訊系統是能即時顯示 Honeypot 受攻擊的一套視覺化資訊系統。使用者能透過此系統立即得知包含 IP 與地理位置等攻擊者的資訊，以及受害的 Honeypot 與受到攻擊的時間等資訊，透過部署和管理一個即時攻擊資訊系統，能使資安從業人員立即查知可能的攻擊，從而更好地保護其網路資源。

MHN 安裝同時也將安裝 HoneyMap。HoneyMap 與 MHN 間的協作方式如圖2所示。NHN 安裝時也會安裝 Hpfeeds，透過此軟體來接收 Honeypot 傳送的即時攻擊資訊，而 MHN 於 HoneyMap 安裝階段時，會註冊一個專用頻道，使 Hpfeeds 收到攻擊資訊時，會根據註冊時設定接收的攻擊資訊類別，轉送至此頻道之上，而監聽此頻道的 HoneyMap 就能獲得即時攻擊資訊，待處理後便顯示於網頁介面之上。

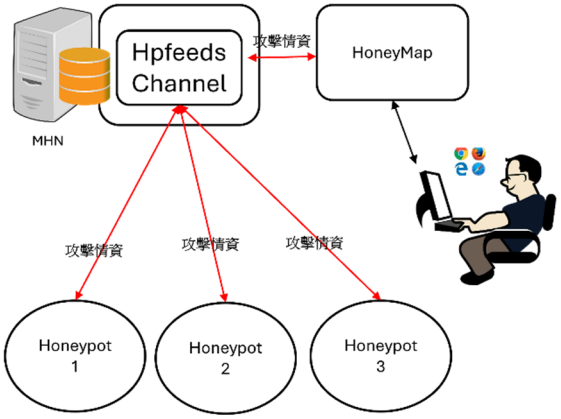

圖 2 MHN 與 HoneyMap 架構[本研究整理]

我們去年計畫於 TWAREN 上部署的基於軟體定義網路技術之響應式網路威脅感知與欺敵系統其架構包含 MHN，故此套欺敵系統也擁有 HoneyMap。然而 HoneyMap 其呈現的攻擊資訊較少，故我們便計畫額外部署另一套與 MHN 相容的即時攻擊資訊系統，此系統名為 SecKC Honeypot Dashboard[18]。

SecKC Honeypot Dashboard 系統是由 bwinchester 基於 arscan 開發的 Dashboard 調整與修改而成[19]。此系統不只包含即時攻擊地理位置顯示，還包含 MHN 本身的統計資訊，例如：24小時內攻擊次數排行等，其顯示的資訊量比 MHN HoneyMap 多。圖2為此系統與 MHN 之間的協作架構，SecKC Honeypot Dashboard 由 seckc-encom-boardroom[20]與 seckc-mhn-dashboard-api[21]所組成。前者為前端 Dashboard，當使用者透過瀏覽器拜訪 Dashboard 時，前端介面會執行統計資訊獲取與攻擊情資監聽兩個程序。統計資訊獲取程序會呼叫 seckc-mhn-dashboard-api 的 API 組件，透過它聯繫 MHN API 來獲取所需的統計資訊。攻擊情資監聽程序則是監聽 seckc-mhn-dashboard-api 中的 Hpfeeds Relay Websocket 組件來獲取及時攻擊資訊，而此組件同樣也須於 MHN 中註冊一個頻道，使 Hpfeeds 收到的即時攻擊資訊也能轉傳至註冊好的頻道之上，因此 Hpfeeds Relay Websocket 組件就能獲得 Honeypot 被攻擊的資訊。透過這兩道程序，使用者就能在 SecKC Dashbaord 上查看到即時攻擊資訊與 MHN 內部的統計資訊。

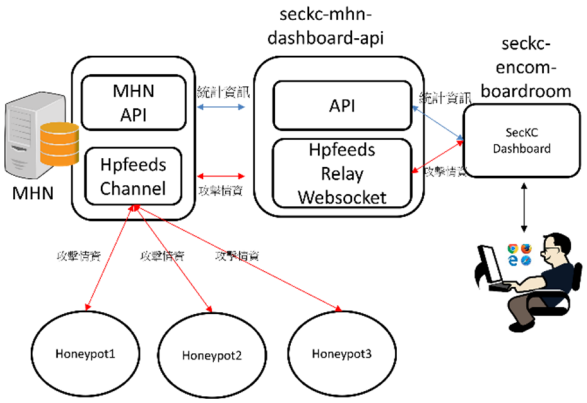

圖 3 SecKC Honeypot Dashboard 與 MHN 架構[本研究整理]

資安領域中，威脅情資的獲取一直是很重要的議題，而一套資訊豐富的即時攻擊資訊系統，不只能讓資安從業人員能更快查知可能威脅外，其紀錄的一些資訊也能提供研究人員來了解攻擊者的手法，從而強化組織內的資安技術與防護。

3.2 即時攻擊資訊系統部署

HoneyMap 的部署與設定較為容易，安裝 MHN 時就會呼叫 HoneyMap 的安裝設定腳本。安裝 HoneyMap 的流程中會註冊 Hpfeeds 的頻道，預設會使用 port 10000接收即時攻擊事件，而預設接收的攻擊事件有 dionaea.connections、dionaea.capture、glastopf.events、beeswarm.hive、kippo.sessions、cowrie.sessions、conpot.events、snort.alerts、amun.events、wordpot.events、shockpot.events、p0f.events、suricata.events、elastichoney.events、drupot.events、agave.events，使用者可以根據需求自訂接收的事件。

SecKC Honeypot Dashboard 部署上分成 seckc-

mhn-dashboard-api 與 seckc-encom-boardroom 兩部分，兩者必須修改設定檔與程式碼，才能搭配 nginx 成功部署。前者下載至伺服器後，須將 encom-boardroom.min.js 檔案內連接 seckc-mhn-dashboard-api 的 URL 部分修改成正確的 IP 或網址。後者下載至伺服器上後，先根據 HoneyMap 註冊頻道的方式，註冊 SecKC Honeypot Dashboard 的專用頻道，並記下 user 與 token，接著將程式碼呼叫 MHN API 中的 URL 改成自己的 MHN IP，最後需要建立 setting.yaml 設定檔供此組件讀取，此設定檔的內容如圖4所示，此部分說明如下

- hpfeeds 選項
  - host：MHN 的 IP
  - port：MHN 的 Hpfeeds port
  - channels：自訂接收的事件
  - user：專屬頻道的 user。
  - token：專屬頻道的 token。
- mhn 選項
  - host：MHN 的 IP。
  - apikey：連接 MHN API 的 key，能於 MHN 的管理介面中找到。
- mnemosyne 選項
  - username：MHN 資料庫的使用者名稱。
  - password：MHN 資料庫的密碼。

```
#relay mhn hpfeeds
hpfeeds:
  host: your mhn ip
  port: your mhn hpfeeds port
  channels: [amun.events,dionaea.connections,dionaea.capture,glastopf.events,bee
swarm.hive,kippo.sessions,cowrie.sessions,conpot.events,snort.alerts,kippo.alert
s,cowrie.alerts,wordpot.events,shockpot.events,p0f.events,suricata.events,elasti
choney.events,drupot.events,agave.events]
  user: user_name
  token: 111111111111111111111111111111111111111111
#communication with mhn api
mhn:
  host: your mhn ip
  apikey: your mhn apikey
mnemosyne:
  username:
  password:
```

圖 4 seckc-mhn-dashboard-api 的設定檔內容

當我們完成部署後，仍必須根據所屬的環境來修正，例如:當部署的誘捕系統以安全考量，採用私有 IP 傳送攻擊資訊至 MHN 時，SecKC Honeypot Dashboard 因為無法辨識私有 IP，就會出錯，因此我們於設定檔中新增一個表格供 SecKC Honeypot Dashboard 查詢，以解決此問題。此外 Dashboard 並非完全支援 MHN 上所有 Honeypot 的資訊顯示，需修改前端介面的程式碼，才能讓非支援的 Honeypot 能在網頁上正確顯示即時受攻擊資訊。

當 MHN 與 SecKC Honeypot Dashboard 部署與修正完畢後，將擁有兩套即時攻擊資訊系統，如此一來便能根據需求切換適合的系統，以利資安研究與防護需求。

4. 即時攻擊資訊系統展示與比較

此章中，我們將展示部署完成的兩套即時攻擊資訊系統，並比較它們各自的優缺點，以供資安相關人員於部署選擇上的參考。

4.1 即時攻擊資訊系統展示

HoneyMap 的介面如圖5所示，其介面分為地圖介面與資訊顯示介面。在地圖介面上，當接收到一個即時攻擊資訊時，地圖介面會以紅點顯示攻擊者的地理位置，而受攻擊的 Honeypot 則會在地圖中以黃點呈現。當發生一個攻擊事件時，紅點與黃點會產生出波紋，表示正發生攻擊，因此波紋一直持續出現時，就表示此攻擊者發動了許多次的攻擊。在資訊顯示介面上，其資訊顯示的格式會以”受攻擊時間點-即時攻擊事件種類-攻擊者地點(經緯度)-受害者地點(經緯度)”呈現，例如”15:46:22 <cowrie.sessions> New attack from Buffalo, USA (42.89, -78.88) to Taiwan (23.50, 121.00)”表示15:46分時部署在台灣的 cowrie 受到一個位於美國水牛城攻擊者的攻擊。資安人員透過地圖介面與資訊顯示介面，便能很快得知目前是否遭受攻擊。

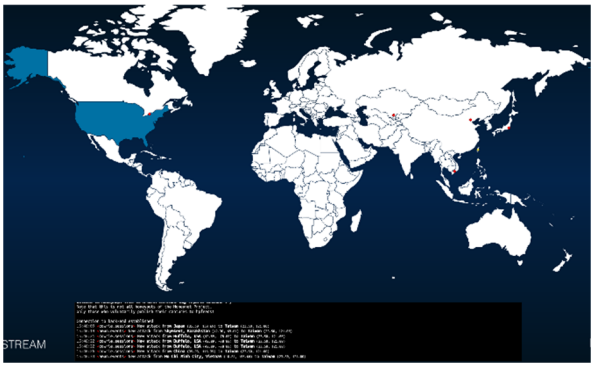

圖 5 HoneyMap 介面展示

SecKC Hoenypot Dashboard 前端介面如圖6所示。圖中，3D 地球是能得知攻擊者的地理位置，將會以直線的方式標示攻擊者的 IP 所在城市，而紫色衛星圖示表示 Honeypot 的數量，另外固定在台灣的黃色圓點則代表 Honeypot 部署的位置。另外，介面中的即時攻擊資訊顯示部分，能夠根據不同的 Honeypot 格式展示攻擊資訊。例如，Dionaea 的格式會顯示連接類型、攻擊者 IP、Port 和協定等；Cowrie 格式則主要用於監控 SSH 攻擊，並顯示帳戶密碼、攻擊者 IP、Port、協定與攻擊時間等資訊；Amun 則側重於連接類型及攻擊者 IP 和 Port 的展示。

除了即時攻擊資訊外，此 Dashboard 還提供了詳細的統計資訊，展示過去24小時內攻擊次數最多的攻擊者排名、攻擊者的地理位置，以及每小時的攻擊次數統計。介面也顯示了網頁運行時間及各城市的當前時間，讓使用者能夠全面了解攻擊趨勢與防護情況。

圖 6 SecKC Hoenypot Dashboard 介面展示

4.2 即時攻擊資訊系統比較

此兩套即時攻擊資訊系統有著各自的優缺點，我們分幾個面向來比較，圖7為比較結果。維護和部署上，HoneyMap 於安裝 MHN 完畢後，便已包含在內，而 SecKC Honeypot Dashboard 尚必須根據環境修正設定檔與程式碼，其門檻較高。安全性上，因為 HoneyMap 與 MHN 一體性程度較高，容易讓不良分子直接碰觸到 MHN，而 SecKC Honeypot Dashboard 有 seckc-mhn-dashboard-api 作為中間層，且易於部署於其他設備上，因此 MHN 的安全性較優。視覺化效果方面，SecKC Honeypot Dashboard 為 3D 地球且會轉動，整體介面比 HoneyMap 更有科技感。另外資料呈現上，HoneyMap 即時攻擊資料呈現較少，且無額外的統計資料，反之 SecKC Honeypot Dashboard 資料呈現多，對於資安從業人員而言，較能獲得更多資訊，然而 SecKC Honeypot Dashboard 呈現的3D 地球與攻擊者圖標呈現上較為繁雜，對於全球攻擊總數的判讀上，較不佳。

	HoneyMap	SecKC Honeypot Dashboard
維護和部署	易	難
安全性	普	優
視覺化效果	普	具科技感
資料呈現	少	多
地圖攻擊數判讀	易	難

圖 7 即時攻擊資訊系統比較表

從上述的比較中，我們能知道 HoneyMap 部署且維護簡單，可是資訊量不足，而 SecKC Honeypot Dashboard 有著更多的資訊量，但其部署門檻較高，因此使用者需考量自身條件，來選擇適合自己的系統。

5. 結論

本論文，為了強化原先於 TWAREN 上部署的欺敵系統，於擁有 HoneyMap 條件上，額外研究與建置 SecKC Honeypot Dashboard，並以五大面向來比較，從而了解到 HoneyMap 適合快速部署且維護簡單的場景，而 SecKC Honeypot Dashboard 則提供更時髦的視覺化呈現與即時攻擊資訊，但需考慮較高的部署門檻。文中的比較結果，供有相同部署需求的組織單位參考，使他們能依據實際需求來選擇。

未來方面，將研究與比較更多的即時攻擊資訊系統，提供更多的比較資訊，來挑選出更佳的即時攻擊資訊系統，以獲得豐富的資安情資，如此一來不只能更加完善中心的資安防護需求也能擁有較棒的使用者體驗。

參考文獻

[1] Open Networking Foundation. (n.d.). Software-Defined Networking (SDN). https://opennetworking.org/sdn-definition/

[2] 李宇哲、王偉齊、史碩三、黃柏勝、周立德. (2016, October). SDN 網路中針對惡意行為之智慧誘捕系統. TANet2016論文集，花蓮

[3] H. Wang, , B. Wu, “SDN-based hybrid honeypot for attack capture,” IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 1602–1606, March 2019.

[4] Z. Minjiao, M. Yufeng, W. Bo and Q. Zhang, “A Dynamic Deceptive Honeynet System with A Hybrid of Virtual and Real Devices,” 2022 5th International Conference on Computing and Big Data (ICCBD), Shanghai, China, pp. 113-117, December 2022.

[5] 台灣高品質學術研究網路. (n.d.). https://www.twaren.net/

[6] Taiwan Computing Cloud: TWCC. (n.d.). https://www.twcc.ai/

[7] Cyber Defense Exercise: CDX. (n.d.). https://cdx.nchc.org.tw/

[8] OWL 惡意程式知識庫. (n.d.). https://owl.nchc.org.tw/

[9] 黃文源、鍾旻哲、郭懿萱、鄭欣恬、黃連億、李柏毅. (2023, November). 基於軟體定義網路技術之響應式網路威脅感知與欺敵系統建置. TANet2023論文集，台北

[10] Honeynet Project. (n.d.). https://www.honeynet.org/

[11] L. Spitzner, “The Honeynet Project: trapping the hackers,” IEEE Security & Privacy, vol. 1(2), pp. 15–23, April 2003.

[12] D. Watson, J. Riden, ”The Honeynet Project: Data Collection Tools, Infrastructure, Archives and Analysis,” 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp. 24–30. September 2008.

[13] S. Kyung et al., “HoneyProxy: Design and implementation of next-generation honeynet via SDN,” 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 2017, pp. 1-9, October 2017.

[14] Modern Honey Network. (n.d.). https://github.com/pwnlandia/mhn

[15] Hpfeeds. (n.d.). https://github.com/hpfeeds/hpfeeds

[16] HoneyMap. (n.d.). https://www.honeynet.org/2012/10/01/honeymap-visualizing-worldwide-attacks-in-real-time/

[17] Elastic Stack. (n.d.). https://www.elastic.co/elastic-stack

[18] SecKC Honeypot Dashboard. (n.d.). https://mhn.h-i-r.net/dash/

[19] encom-boardroom. (n.d.). https://github.com/arscan/encom-boardroom

[20] seckc-encom-boardroom. (n.d.). https://github.com/bwinchester/seckc-encom-boardroom/

[21] seckc-mhn-dashboard-api. (n.d.). https://github.com/bwinchester/seckc-mhn-dashboard-api/