「看不見的英雄」系列報導（二十二）

紙尿布變綠金

刁曼蓬

前言

吳倍任博士爲高分子化學專家，多年來致力開發紙尿布分解技術，將環保痛腳的廢棄尿布分解爲可再利用的再生紙漿或塑膠。其所參與成立的「益鈞環保科技股份有限公司」，新近完成建置商轉製程，使廢棄尿布回收且得以量產，並聯手紙尿布大廠與原料供應商（金百利、台塑、台橡、南寶樹脂）策略協同打造可回收產業供應鏈。扭轉形成污染廢棄物及有礙環境永續發展的傳統線性經濟「Make－Use－Waste」，成功打造循環經濟「Make－Use－Remake－Reuse」的營運模式，開啓環境永續的藍天。

初次接觸吳倍任博士開發的紙尿布回收專利技術，是在2017年環保署支持外貿協會協辦的國際綠色環保產業展覽會上。源自交大材料研究所的吳倍任博士，因其開發完成的紙尿布分解技術，受到爲紙尿布清理所困的新竹縣環保署舉薦，參與政府正積極推展的綠色永續產業計畫。

有別於大多數源自廢棄物回收的環保業者，專精於高分子化學的吳倍任博士，在交大材料研究所博士後，聚焦於「觸媒」及催化劑研究時，即因針對「世紀之毒」戴奧辛的分解研究嶄露頭角。其時新竹縣環保局受困於長照單位紙尿布回收的困擾（紙尿布含水高、焚化耗能，掩埋處理其塑膠成份無法分解），輾轉得知吳博士戴奧辛的研究成績，委託其協助處理惱人的紙尿布回收難題。

打造清淨家園的科技

全台灣每天至少產生三、四百萬片的廢棄尿布，長期來因為耗能（含水量高）以及無法掩埋（含塑膠），被環保署列名為不可回收項目，如何處理一直是個頭痛的問題。

吳倍任博士針對廢棄紙尿布的材質與特性，以生物技術開發出環境友善及清淨家園的紙尿布分解技術，將廢棄尿布變成再生紙漿、吸水高分子（聚丙烯酸鹽）以及塑膠片（PE&PP），並於中原大學成立新創「清倍華再源技公司」。此外在新竹縣政府、中華大學、台灣新竹綠色產業聯盟等團隊鼎力配合下，以「尿布加值」在2017年4月拿下環保署設計競賽冠軍，於600多件作品中脫穎而出。證明廢棄紙尿布可轉化為再生資源，成為氣候變遷、廢塑及減碳趨勢下全球產業競相爭取的項目。

由於廢棄尿布含水量高，若以焚化法處理，耗能大且會縮短焚化爐壽命，因此一直以來北部地區焚化爐是不收尿布廢棄物，但是若以掩埋法處理，專家估計至少400年才會分解，勢必造成掩埋場極大負荷。

「台灣一年約有13億片至15億片廢棄尿布，且逐年快速升高；再加上老年化的人口結構，2020年後成人紙尿布的產出量即大於嬰幼兒尿布。」吳倍任研發團隊起始即以長照事業單位的廢棄尿布為優先處理目標。

吳博士團隊於2017年開發的「尿布回收」技術，兼具快速、節能（不須加熱）分解廢棄尿布的特性，更重要的是不需要用到「超大型」分解設備，可以專門設置在特定的地點，做到現場回收、立即分解處理的效果，還可降低廢棄尿布放置過久產生細菌滋生及臭味的問題。其與中華大學黃思蓴教授合作的微生物分解技術，結合水處理系統可循環再利用；使用的能耗也極低（不必加熱處理），製程極具「環保」效益。

他以台灣為例，若能將回收尿布再利用，每年可產出7.5萬噸的再生紙漿，減少砍伐86.4萬棵樹木；回收過程的水資源可重複利用，平均製作每噸紙漿僅需2噸水，充分體現「循環經濟」及「環保」多重效益。

醉心科研，為地球盡一分力

在多數同學紛紛走向台積電等半導體高薪企業工作時，「醉心於材料技術研究、為地球盡一分力」的吳倍任卻不為所動，堅守其「有趣的紙尿布分解研究」，並努力走出Pilot run、小批次試營運的框架，朝商用量產製程邁進。

千里駒與伯樂

2019年是紙尿布回收技術關鍵年，是年益鈞環保科技總經理秦錫鈞自美國回台，接觸到吳博士尿布分解技術的獨特性，理解「國際正如火如荼進行中的循環經濟，乃勢不可擋的洪流。」說服父親秦嘉鴻，國內礦油業巨擘益州集團創辦人兼董事長，以技術換股的合作方式，成立益鈞環保科技，目標三年建置商用運轉。2021年在桃園工業區購置廠房與制定回收執行標準，由吳博士領軍機械設備製程的設計安裝。同時接續各機關執行計畫證照的取得。

▲益鈞環科董事長秦嘉鴻和總經理秦錫鈞父子

所建置的示範工廠，先以日處理2噸廢棄紙尿布的商轉能量，繼而增建日處理100噸的新建廠房。2022年上半年即通過經濟部工業局吸收性產品的再利用許可，開始處理紙尿布大廠金百利的NG（未使用）尿布，成為台灣第一家取得尿布再利用機構的廠商，並於同年第四季開始興建廢棄2,200噸/月處理中心廠房。預計2023年第三季即可建成全球第一座低碳廢棄紙尿布回收中心。

建立環境永續的循環經濟為經營目標

有別於目前廢棄尿布常見的焚化掩埋做法，益鈞環保科技所致力研發提出創新的尿布回收做法，可讓尿布在低耗能（無需加熱）下透過系統去分解；以物理分選（利用重力及外型的差異），經過初級分離槽、傾斜式圓桶篩、離心式分離機組、螺旋擠壓機以及氣浮式清洗分選機處理。完整有效分離出紙漿、吸水高分子（聚丙烯酸鹽）以及塑膠片（PE&PP）三種原料。並且還原至「原料」階段，可再次循環使用。目前已完成NG（未使用過）尿布分解回收系統開發，是台灣第一家提出完整解決目前廢棄尿布（未使用過）造成的垃圾問題的廠商。並取得我國兩項相關專利，掌握尿布「全分解」回收技術與門檻。並分別申請六項台灣、美國專利及全球優先權（PATENT COOPERATION TREATY）。

「垃圾減量 物質循環 企業經營環境永續」為益鈞環保科技的發展策略。秦錫鈞表示，該公司將針對目前國內尚無有效解決辦法的尿布垃圾問題導入關鍵技術製程及專利技術，於無害環境條件下，還原取得製造紙尿布所投入的原料，重新應用於產業上。秦錫鈞指出，益鈞現有技術不但符合市場趨勢，且解決大量廢棄尿布造成的垃圾問題，非其它現有國外尿布回收競爭對手可輕易仿效，也是國內目前僅有的一家公司具有研發實績。

「目前各國已開始制定相關法規，包含生產尿布的企業及環保業者均已著手進行相關技術研究以因應新環保法規的制定，預計將會迎來一波相關技術投入的研發高峰期。」秦錫鈞表示，益鈞正積極與中央、地方政府相關行政機關展開密切配合與協調並陸續取得相關許可。致力於相關法案的推動與落實，規劃陸續投入資源建立四條生產線，成為本領域的先行與開拓者。

紙尿布分解回收，循環經濟開拓者

2022年四月份益鈞開始處理世界紙尿布大廠金百利NG（未使用過）的紙尿布，連續半年，運行順利。10月、11月分別向經濟部提出無形資產融資、中堅企業實質審查。並於2022年10月於興櫃之戰略新板掛牌交易。

猶有甚者，在秦錫鈞富衝勁、國際觀的帶領下，益鈞連結我國吸水材料最大製造商台塑企業以及相關材料供應廠家如南寶樹脂、台橡等，與母公司益州集團有深厚往來的日本豐田等國際大廠加入協作，齊步邁向「循環經濟」、回收材料產業的建立。

行政院2018年12月20日通過「循環經濟推動方案」將循環經濟理念及永續創新的思維融入各項經濟活動，以期創造經濟與環保雙贏並接軌國際。益鈞環保科技總經理秦錫鈞指出，該公司所致力研發廢棄尿布問題的解決方案，對於當前廢棄尿布常見的焚化掩埋做法提出創新的尿布回收做法，不但符合政府的政策，且掌握尿布「全分解」回收技術與門檻，踏出循環經濟最難的一步。

益鈞環科使原先令人頭痛的紙尿布回收難題，藉由新的科技應用，開創新局。扭轉產業發展劣勢、從「Make Use Waste，開採製造 使用 丟棄」的線性經濟，轉型為資源永續的循環經濟「Make Use Remake Reuse」。以期創造經濟與環保雙贏並接軌國際。今後將積極持續投入系統優化，保持市場領先地位，希冀能成為台灣循環經濟的典範。

彰銀觀點

益鈞環科為彰銀中山北路分行重要客戶益州集團的子公司，益州集團成立於民國64年，自65年開始即與本行往來且是以本行為主力銀行，往來超過46年。彰銀提供該集團包括存款、員工薪資轉帳、外匯及授信業務等多項金融服務，彼此往來關係密切。益州集團多年來默默耕耘各項循環經濟相關事業，成立益鈞環科第一家想到要往來的銀行即是彰銀。

益鈞環科透過其專利技術處理，可將廢棄尿布還原成塑膠、紙漿纖維與高吸水分子等再生原料，在全球重視永續發展的時代，益鈞環科的技術得以解決多年來廢棄尿布的痛點。有別於其他國家企業在處理廢棄尿布採用降階回收的方式，益鈞環科的技術不僅對環境友善，且可使資源永續再利用，結合綠能科技與循環經濟，實踐ESG的優秀新創企業。

日前益鈞環科參與經濟部工業局111年度智慧財產價值躍升計畫，針對「吸收性物品回收方法之發明專利」進行無形資產評價，獲得財團法人工業技術研究院諮詢委員一致肯定，並已由專業鑑價公司對該發明專利做成無形資產價格。雖目前仍處於設備建置、乙級廢棄物處理及再利用相關執照申請階段，但已於桃園縣大園鄉建置一座示範場進行相關回收製程研究，並完成相關可行性試驗評估，如能順利商轉，當具有相當大的業務發展潛力及經濟價值。

彰銀本於一貫對中小企業的支持，特別是循環經濟有關議題更是不遺餘力，未來彰銀中山北路分行將持續提供各項業務協助，與客戶一同成長，共創雙贏。

益鈞環科於2019年成立，即在彰銀土城分行開戶。彰銀土城分行羅偉碩經理指出，益鈞環科董事長秦嘉鴻先生為益州集團主要決策者，目前為總統府國策顧問及桃園市政府市政顧問，近年集團朝著多角化經營發展，除聚焦產業上下游整合，且在風電、環保等產業投資不遺餘力。益鈞環科近期即登錄興櫃戰略新板，掌握尿布回收技術與專利，對尿布汙染環境問題提出有效對策；為台灣循環經濟重大成就。尤其是益鈞環科總經理秦錫鈞與團隊展現對尿布回收與資源再生的使命感與熱情，對環境永續的責任堅持；與彰銀業務與ESG並重的精神相互輝映，攜手協同為環境保護與循環經濟貢獻心力。

▲彰銀土城分行同仁跟益鈞環保科技同仁合照

銀行業導入網路威脅情資（Cyber Threat Intelligence）機制之探討 - 下

王宏敦

第三節、網路威脅情資交換協定

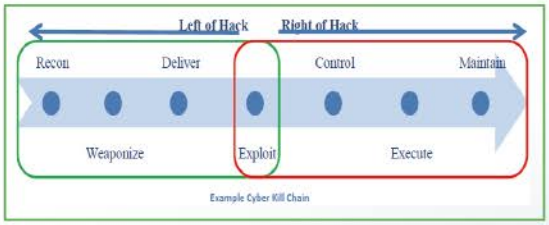
網路威脅情資（Cyber Threat Intelligence, CTI）內容用來識別攻擊者的手法、戰略等，再經過分析處理後，透過威脅情資平台分享給信任組織，提供企業組織內部資安團隊參考使用，並及早進行預防與改進資安措施，以防止相同攻擊事件重複發生。

依據美國系統與網路安全協會（SANS Institute）在2015年報告顯示，統計已有百分之三十八的企業組織使用網路威脅情資（CTI）強化企業本身之資訊安全，其中STIX（Structured Threat Information eXpression）結構化語言是企業組織中最普遍常見的情資交換標準格式。

STIX最初由美國電腦緊急應變小組（US-CERT）成員於2010年建立，用於討論網路事件的自動化數據交換格式，後來由MITRE公司（The MITRE Corporation）進行維護與後續發展，STIX語言能夠用來快速顯示資安事件的相關性與涵蓋性，藉以表達出具備架構性的網路威脅資訊，並具備彈性化、延展性、自動化以及容易解讀等特性。

透過網路攻擊鏈（Cyber Kill Chain）流程，如下圖，可知道一次網路攻擊可能分成好幾個步驟，也可從中了解最新的攻擊行為與如何防範因應。

圖 壹-36 攻擊鏈（Cyber Kill Chain）



資料來源：STIX Whitepaper v1.1, 2014

如上圖所示，在攻擊事件已經發生之後，企業組織所進行的因應措施成本非常高，無論是在有效阻擋駭客的攻擊或是清除駭客已建立的立足點，都須付出相當大的資源。

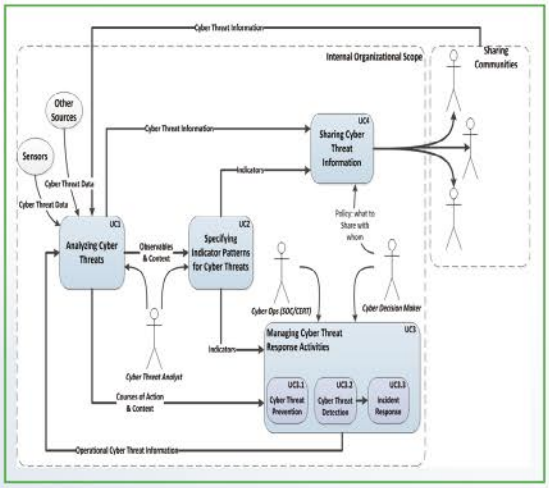
對防禦者而言，最好策略即是在攻擊鏈中盡可能在駭客發動攻擊之前，就已經採取行動，透過網路威脅情資的利用，可讓企業組織由事後補救的被動策略，轉變為主動防禦策略。

壹、STIX核心使用案例

STIX提供了一種統一的架構，將各種不同類型的網路威脅情資建立其關聯，主要區分以下項目：網路觀察、威脅指標、事件、攻擊者的策略、技術方法和程序（包括攻擊模式、惡意軟體、漏洞利用、攻擊鏈等）、利用目標（例如，漏洞、弱點或配置）、預防策略（例如，事件應變、漏洞及弱點補救或緩解措施）、網路攻擊活動及網路威脅參與者。

為使資安研究人員更快瞭解STIX，在STIX白皮書內容中提供了STIX網路威脅管理的核心使用案例（Use Cases, UC），如下圖為STIX核心使用案例示意圖，本文針對使用案例逐一進行說明。

圖 壹-37 STIX核心使用案例示意圖



資料來源：STIX Whitepaper v1.1, 2014

一、（UC1）分析網路威脅

網路威脅分析師可從各種透過手動或自動化的方式蒐集情資，以分析有關網路威脅活動之結構化和非結構化資訊，其內容包含了企業組織內部與外部的網路威脅情資。

藉由資安分析人員收集、分析並整理相關資安威脅情資後，識別這些威脅情資並記錄，再依據這些紀錄和特徵，分析師可以指定相關的威脅指標，提出因應處理措施與行動方案，並共享威脅情資給其他受信任方。例如，在潛在的網路釣魚攻擊（Phishing Email）情況下，網路威脅分析師可能會分析釣魚信件的附件或連結，以確認是否有惡意行為，調查使用者是否已經點選連結或開啟檔案，並且留存所有分析紀錄。

二、（UC2）指定網路威脅的指標模式

網路威脅分析師對於網路威脅資訊指定可衡量的模式，藉由可觀察的數據資料，透過手動或自動化工具完成。例如，在確認網路釣魚攻擊的情況下，網路威脅分析師可能會從以下資訊，收集相關的可觀察數據，例如，郵件地址、實際來源IP、信件主題、嵌入的 URL、附件類型等，並對釣魚郵件進行分析，藉由識別釣魚攻擊中表現出相關資安威脅手法（Tactics, Techniques, and Procedures, TTP），進行攻擊鏈的關聯比對，為指標分配適當的信度，並訂定的解決方案。

三、（UC3）管理網路威脅響應活動

組織決策者和內部資安團隊共同努力檢測網路威脅活動，並調查和因應任何檢測到的攻擊行為。資訊安全的預防性措施在本質上也是補救措施，對企業組織而言，能減少系統漏洞、弱點或錯誤配置的狀況，有助於提升資安上的防禦能力。例如，企業組織獲得有關網路釣魚攻擊事件的威脅指標後，決策者和內部資安團隊合作，全面瞭解網路釣魚攻擊在環境中的影響，包括安裝、執行的惡意軟體或點選惡意連結，以評估網路釣魚攻擊對組織的影響範圍與衝擊程度，再擬定因應策略，實施適當的預防機制或調查行動方案。

四、（UC4）分享網路威脅情資

組織內部資安團隊之決策者制定網路威脅情資分享政策，再依循政策進行威脅情資的分享，以確保資訊內容的一致與妥適性。例如，一個已經被證實的網路釣魚攻擊事件，由決策者預先定義好資訊分享政策，藉由相關指標能夠以自動或手動與信任單位進行分享，使信任單位可以利用所獲得的網路威脅情資強化資訊安全防禦能力。

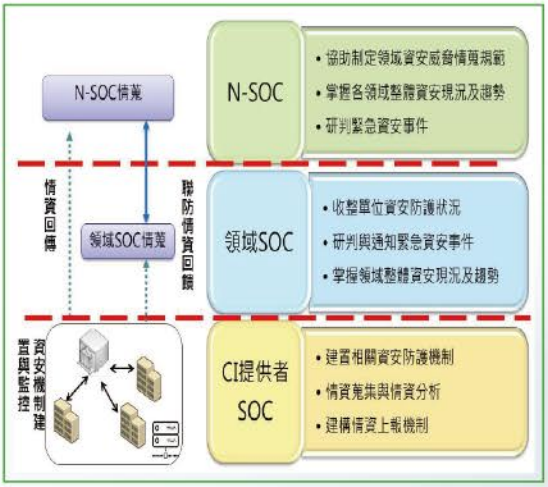
以上為STIX核心使用案例說明，透過組織內部決策者與資安團隊對於資安威脅情資分析整理後，藉由網路威脅情資的分享，達到聯合防禦的綜效，以本國金融機構而言，銀行、保險或券商等金融單位，可透過金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）推動的金融領域資訊安全防護（Financial Security Operation Center, F-SOC）平台，進行網路威脅情資分享，以達到金融資安聯防效果，提升本國金融體系之資訊安全。

貳、資訊安全監控中心（Security Operation Center）的應用

資訊安全監控中心（Security Operation Center, SOC）調查觸發告警事件所蒐集的情資，可能包含惡意中繼站黑名單IP、惡意網路連結URL、惡意程式之檔案雜湊值（Hash Value）、開放威脅指標（Open Indicator of Compromise, Open IOC）規則、資安漏洞與弱點情資以及相關郵件資訊等，依本國為例，領域層級 SOC需彙整相關情資，並以STIX標準格式封裝，回傳給國家層級N-SOC進行資安事件單關聯彙整。

行政院資通安全處在「國家資通安全防護整合服務計畫領域SOC實務建置指引」中指出，領域層級SOC需彙整該領域之相關情資，並採用STIX標準格式封裝回傳給國家層級的N-SOC，進行事件單關聯彙整，回傳機制示意圖如下：

圖 壹-38 國家層級N-SOC與領域層級SOC透過STIX格式進行資料交換示意圖

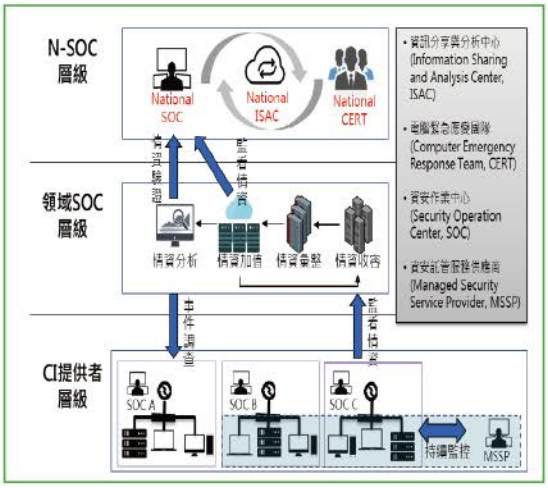


資料來源：行政院資通安全處，國家資通安全防護整合服務計畫領域SOC實務建置指引

CI-SOC、領域SOC及N-SOC彼此間運作架構及流程

行政院資通安全處在「國家資通安全防護整合服務計畫領域SOC實務建置指引」內容要求領域SOC收容CI-SOC事件情資進行情資彙整、加值與分析，並適時針對重大事件支援CI-SOC進行事件調查。同時，領域SOC及時回傳威脅情資予N-SOC，並固定回報真實威脅情資資訊予N-SOC，確保威脅情資之準確性。有關CI-SOC、領域SOC及N-SOC彼此間運作架構及流程如右圖：

圖 壹-39 CI-SOC、領域SOC及N-SOC彼此間運作架構及流程圖



資料來源：行政院資通安全處，國家資通安全防護整合服務計畫領域SOC實務建置指引

參、STIX格式介紹

領域SOC調查觸發事件所蒐集的情資可能包含惡意中繼站黑名單IP、惡意網路連結、惡意程式檔案雜湊值（Hash Value）、OpenIOC規則、資安漏洞與弱點情資及相關郵件資訊等，後續彙整相關威脅情資以STIX標準格式封裝，並回傳給N-SOC進行事件單關聯彙整。STIX官方網站包含相關資安威脅情資範例共計27類，本文整理常見之STIX威脅情資範例及類型供參考，如下表說明：

表 壹-2 STIX格式之威脅情資範例

STIX 官方範例名稱	STIX 類型	說明
Command and Control IP List	Observable、TTP	C2 黑名單情資
Indicator for Malicious URL	Indicator	惡意網路連結情資
Malware Indicator for File Hash	Indicator、TTP	惡意程式 / 檔案情資
OpenIOC Test Mechanism	Indicator、TTP	OpenIOC 情資
Identifying a Threat Actor Profile	Threat Actor	駭客資訊情資
Incident Essentials - Who, What, When	Incident	威脅事件描述
CVE in an Exploit Target	Exploit Target	資安漏洞 / 弱點情資
Assets Affected in an Incident	Incident	資安事件影響資產情資
Kill Chains in STIX	TTP	網際狙殺鍊階段情資
Malicious E-mail Indicator With Attachment	Indicator、TTP	惡意電子郵件附件情資

資料來源：行政院資通安全處，國家資通安全防護整合服務計畫領域SOC實務建置指引

一、STIX第一版九大模組介紹

STIX第一版發行的官方白皮書詳細敘述其架構與相關技術，其架構主要可分為九大模組，模組之間或模組本身可具有關聯性與上下關係，詳細模組逐一說明如下：

（一）資安威脅觀察資料（Observables）：敘述資安威脅事件中所觀察到的相關資料，內容可包含資料來源、資料名稱、內容敘述、資料真實性及相關資安威脅事件等。

（二）資安威脅模式（Indicator）：敘述資安威脅可能被觀察到的活動模式，內容可包含威脅模式名稱、模式描述、有效時間、攻擊手法、觀察資料及攻擊鏈Cyber Kill Chain）階段等。

（三）資安威脅事件（Incident）：敘述資安威脅事件，內容可包含事件名稱、事件描述、事件類型、受害者、影響範圍與影響資產等。

（四）資安威脅手法（Tactics,Techniques, and Procedures, TTP）：敘述資安威脅策略、技術與手法，內容可包含資安漏洞、攻擊模式、惡意程式、使用工具、受害者及攻擊鏈（Cyber Kill Chain）階段等。

（五）資安威脅活動（Campaign）：敘述資安威脅活動資訊，內容可包含一群駭客、攻擊手法、威脅模式與相關事件，甚至可推演關聯至其他相關資安威脅活動。

（六）資安威脅者（Threat Actors）：敘述資安威脅者的特徵與描述資訊，內容可包含相關基本描述、資安威脅活動、威脅手法、情資來源及動機等。

（七）資安威脅目標（Exploit Target）：敘述被惡意利用的資安漏洞、弱點及設定檔，內容可包含目標名稱、目標描述、資安漏洞、資安弱點、因應措施、處理狀況及相關資安威脅手法等。

（八）資安威脅防護措施（Course of Action）：敘述面對資安威脅所做的應變與預防措施，內容可包含防護措施名稱、描述、效用、使用成本、應用範圍及相關防護措施等。

（九）資安威脅報告（Reports）：綜整各模組資訊而成資安威脅報告，也可處理難以單一套用至其他模組的資安資訊，設計此模組以文字格式彈性封裝資安資訊。

二、STIX封裝架構介紹

STIX封裝架構分為三部分，說明如下：

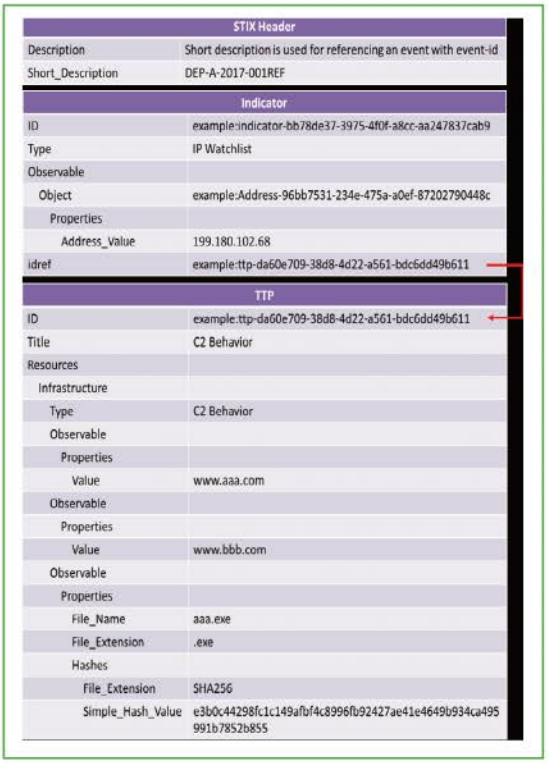
（一）STIX Header：分別利用STIX Header表示事件識別碼，方便與回傳之事件情資進行關聯。

（二）Incident：資訊安全威脅事件（Incident）表格內含事件之IP情資。

（三）TTP：資訊安全威脅手法（TTP）表格內含事件調查情資，例如，網路連線IP位址、惡意程式名稱、惡意程式檔案類型及SHA256雜湊值。

STIX封裝中繼站黑名單觸發事件調查情資範例，如下圖：

圖 壹-40 STIX封裝中繼站黑名單觸發事件調查情資範例



STIX Header	
Description	Short description is used for referencing an event with event-id
Short_Description	DEP-A-2017-001REF
Indicator	
ID	example:indicator-bb78de37-3975-4f0f-a8cc-aa247837cab9
Type	IP Watchlist
Observable	
Object	example:Address-96bb7531-234e-475a-a0ef-87202790448c
Properties	
Address_Value	199.180.102.68
idref	example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611
TTP	
ID	example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611
Title	C2 Behavior
Resources	
Infrastructure	
Type	C2 Behavior
Observable	
Properties	
Value	www.aaa.com
Observable	
Properties	
Value	www.bbb.com
Observable	
Properties	
File_Name	aaa.exe
File_Extension	.exe
Hashes	
File_Extension	SHA256
Simple_Hash_Value	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

資料來源：行政院資通安全處，國家資通安全防護整合服務計畫領域SOC實務建置指引

自2020年由「金融資安資訊分享與分析中心（F-ISAC） 」所推動的「金融領域資訊安全防護（F-SOC）」平台，包含本行在內，全國已有多家金融單位成功與F-SOC藉由STIX威脅情資標準格式完成介接，本文將於第肆章節，以彰化銀行為例，介紹本行資訊安全威脅傳輸平台X-SOC（eXtensible Security Operation Center, 資訊安全威脅情資傳輸平台）與金融領域F-SOC系統建置過程，並說明情資平台之資安強化措施。

第貳章 系統規劃與設計

本研究以「銀行業導入網路威脅情資」為研究目標，探討企業組織內部資安團隊透過網路威脅情資的蒐集、分析、利用以及分享，以有效利用資安威脅情資，協助組織決策者進行資安策略訂定與技術強化措施，在駭客發動攻擊之前，降低組織可能產生的破口、漏洞及弱點，以最低成本，獲得最大資安防禦能量目的。

自2017年總統蔡英文的「資安即國安」到2021年的「資安即國安2.0」宣示，近幾年將中央政府的資訊安全政策拉高到國家安全的層級，促使國家層級的N-SOC的快速發展，行政院資通安全處為建構國家資訊安全聯防體系，同步推動八大關鍵領域之資安威脅情資分享機制，並依據「國家資通安全防護整合服務計畫領域SOC實務建置指引」要求，領域層級 SOC需彙整該領域之相關情資，並採用 STIX標準格式封裝回傳給國家層級N-SOC。

本行依據「國家資通安全防護整合服務計畫領域SOC實務建置指引」內容要求，協同「金融資安資訊分享與分析中心（F-ISAC）」進行資訊安全威脅情資傳輸平台（X-SOC）建置，並於2021年成功與金融領域F-SOC完成介接，透過資安威脅情資的分享，提升本國金融機構之資訊安全。

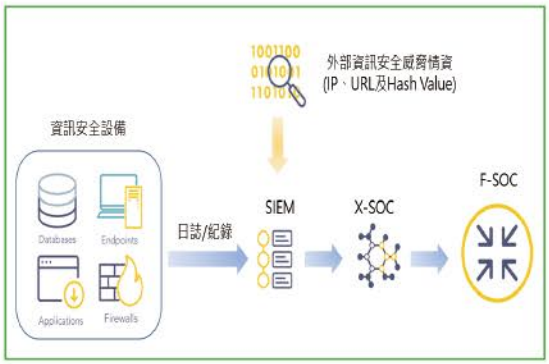
本行所建置之資訊安全威脅情資傳輸平台（X-SOC），透過STIX（Structured Threat Information eXpression）情資標準格式，提供本行資安相關威脅情資給F-SOC，再由F-SOC與N-SOC系統進行資安威脅情資的蒐集、交換與分享，以達到金融機構資安威脅情資之分享、監控及聯合防禦之綜效，強化本國金融體系之資訊安全。

第一節、基礎架構

壹、整體架構

本研究整體架構為企業組織內部之資安團隊，透過資安威脅情資資訊的蒐集彙整後，匯入資訊安全事件管理平台（Security Information Event Management, SIEM）系統，再經由SIEM系統之關聯規則，分析組織內部所收容的資訊系統日誌，進行關聯分析，以產出即時資安告警事件，並同時取得內部資安威脅情資，再透過資訊安全威脅情資傳輸平台（X-SOC）以STIX情資標準格式分享至金融領域資訊安全防護（F-SOC）平台，達到本國金融體系聯合防禦之綜效，整體架構示意圖如下：

圖 貳-1 威脅情資平台X-SOC情資傳輸示意圖



資料來源：本研究整理

由威脅情資平台X-SOC情資傳輸示意圖可以得知，組織內部資安管理者取得外部威脅情資後，將情資內容如，惡意中繼站IP、網址URL或惡意檔案Hash Value匯入SIEM系統，並進行規則設定，再透過組織內部資訊設備之日誌，進行關聯分析產生即時資安告警事件。

資安告警事件透過SIEM規則過濾後，傳輸至資安威脅情資平台X-SOC，再藉由系統的審核與放行機制，提供給F-SOC進行彙整、分析，達成國內金融體系之資安聯防效果。

貳、運作說明

一、外部資安威脅情資

本行主要的外部威脅情資來源以「金融資安資訊分享與分析中心（F-ISAC）」為主，另外也透過資安產品與服務供應商如，安碁資訊、FireEye等，取得惡意中繼站IP、惡意網址URL或網域，以及惡意檔案雜湊值（Hash Value）等資訊，經過彙整後匯入本行資訊安全事件管理平台（SIEM）系統，並訂定關聯規則與後續分析作業。

二、資安設備日誌與紀錄

本行SIEM系統收容重要主機、伺服器、資訊及資安設備之日誌與紀錄，再透過關聯規則分析後，產出即時異常告警事件，藉由資安威脅情資的匯入，如惡意中繼站IP、惡意網址URL或網域等資訊進行分析，揭露組織內部的資安威脅事件，並即時調整資訊與資安設備之相關參數，以強化本行資訊安全。

三、SIEM

SIEM收容大量資訊與資安設備之日誌與紀錄檔，並經由外部資安威脅情資的匯入，藉由關聯規則的制定，形成自動化分析功能，產出即時告警事件以供資安人員進行快速因應。

四、X-SOC

由SIEM建立資安威脅情資傳送規則，以自動化方式將告警事件格式轉換為STIX標準格式，再傳輸至資訊安全威脅情資平台X-SOC後，由X-SOC管理人員進行人工審核及放行作業，將可用之資安威脅情資傳送至F-SOC彙整分析。

第二節、威脅情資平台之安全機制

為確保資安威脅情資平台內容之可用性與機密性，針對資訊安全威脅情資傳輸平台（X-SOC）系統在資安的保護機制，以連線安全及系統安全兩大方向，提供以下安全強化措施：

壹、連線安全

一、連線安全保護機制

使用者透過瀏覽器登入資訊安全威脅情資傳輸平台X-SOC系統網站時，全程採用HTTPS通訊協定進行連線安全加密，以確保使用者資料傳輸過程之安全性與隱密性，降低遭受中間人攻擊（man in the middle, MITM）的機會。

二、身分驗證機制

使用者登入時除了必要的帳號密碼之外，另外採用圖形驗證碼，以保護網站減少遭受暴力密碼破解之風險，並輔以一次性密碼（One Time Password, OTP）強化身分驗證安全性。

三、存取管控機制

透過防火牆等資訊設備，進行存取管控（Access Control List, ACL）設定，限制可存取之來源IP位址，提升存取管控能力。

貳、系統安全

一、角色與權限設計：為符合最小授權原則，本系統設計時具備多種角色與權限設定功能，可針對使用者需求進行最小授權設定。

二、完整稽核軌跡：使用者登入系統後所進行的操作，均完整記錄，以利稽核作業執行與使用者行為調查。

三、採用Ubuntu作業系統，並於上線前完成弱點掃描及原始碼檢測作業，以確保系統安全。

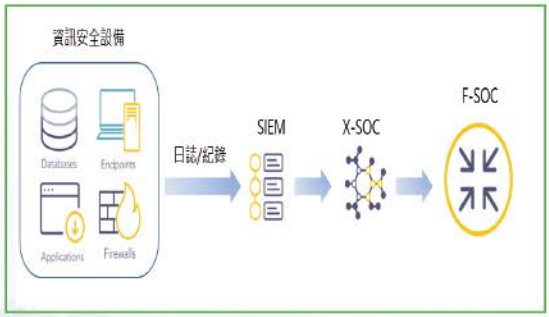
藉由上述針對本系統之資安防禦機制，可有效降低中間人攻擊（MITM）、帳號密碼的暴力密碼破解機會，並且有效抵禦未授權之存取行為，使資安威脅情資平台獲得完善保護，確保威脅情資之機密性、完整性與可用性。

第參章 系統架構實作-以彰化銀行為例

第一節、建置環境

本研究系統架構主要採用Docker技術，建構彰化銀行資訊安全威脅情資傳輸平台，命名為X-SOC，搭配本行資訊安全事件管理平台SIEM整合後，並透過STIX標準格式傳送威脅情資給F-SOC進行彙整與分析，以達到本國金融領域之資訊安全聯合防禦之綜效，示意圖如下：

圖 參-1 X-SOC威脅情資傳輸架構示意圖



資料來源：本研究整理

壹、Docker簡介

Docker 是一個開放原始碼軟體，用於開發、應用與執行程式，並提供使用者建置任何應用程式，並運行在任何地方。

透過Docker技術可以分離應用程式所運行的基礎設施（Infrastructure）限制，並且具備快速建立、發佈應用程式特性，可節省環境建置時間，更能讓使用者專注於應用程式的設計與開發。

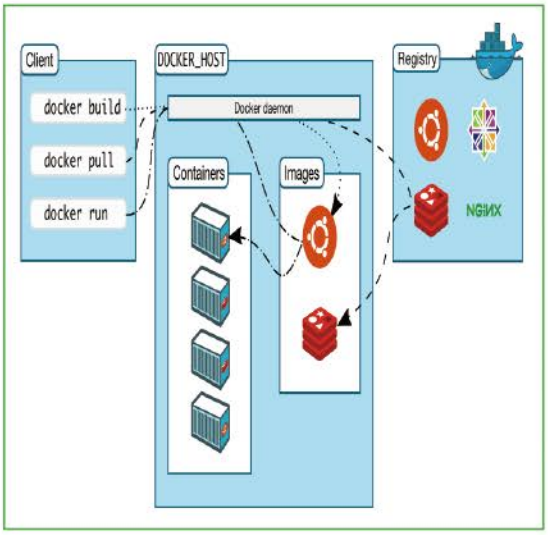
Docker 運行應用程式的環境被稱作容器（container），運行時不用要像虛擬機器（virtual machine）一樣，需要模擬出軟體、韌體或硬體，反而直接運行於主機的核心。以執行應用程式的運行而言，虛擬機器需要模擬出整套作業系統才能運行應用程式，而應用程式容器則是直接運行在主機上，因此，Docker比虛擬機器更輕量、執行啟動更為快速。

貳、Docker架構介紹

Docker 採用主從式（Client–Server model）服務架構。Docker Client端與Docker Daemon進行溝通對話，Docker Daemon負責構建、運行和分配 Docker Containers容器的繁重工作。

Docker Client和Docker Daemon可以在同一系統上運行，或者可以將 Docker Client連接到遠端的 Docker Daemon，並藉由REST API、UNIX Sockets或網路介面進行通訊。示意圖如下：

圖 參-2 Docker架構示意圖



資料來源：https://docs.docker.com/get-started/overview/

一、Docker daemon

Docker daemon監聽 Docker API的請求，並管理Docker對象，例如Images、Containers等。Docker daemon還可以與其他Docker daemon通信以管理 Docker服務。

二、Docker Client

Docker Client是與Docker溝通的主要方式。當使用命令時，例如，docker run，Docker Client會將這些命令發送到Dockerd，而執行指令。該docker命令使用 Docker API。Docker Client可以與多個Docker daemon通訊。

三、Docker registries

Docker Registry 類似倉庫的概念，存放著各式各樣的Docker Images。Docker官方有提供一個 Docker Hub Registry，在上面可以找到許多官方開源套件的Images。

四、Docker Hub

Docker Hub上有許多的專案，每個人都可以上傳自己的專案，也可以下載別人的專案，有時也可以在某些開源專案，提問或提交自己的程式碼，並提供免費帳號及私有的儲存庫空間。

五、Images

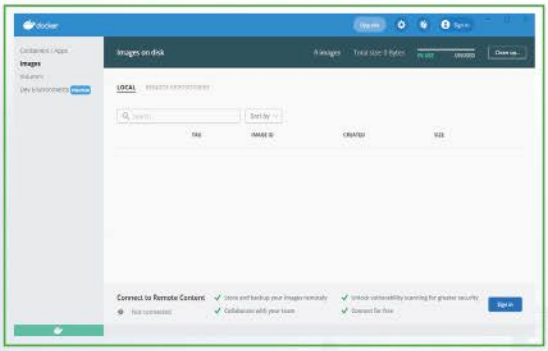
Images類似一個模板。通常，Images帶有一些額外的自定義。例如，在構建一個以ubuntu作業系統的image，其中會包含安裝Apache Web服務和使用者要加入的應用程序，以及應用程序運行所需的配置詳細資訊。使用者也可以創建自己的image，也可以僅使用其他人創建並在註冊表中發布的image。若要構建自己的image，只需要使用簡單的語法創建一個Docker file。

參、Docker實作

由於本研究系統架構主要採用Docker技術，以下針對Docker進行簡單實作，以更加了解Docker技術的實際使用方式。以下將使用Windows 10作業系統，透過Docker技術，利用滲透測試工具Kali Linux進行示範。

一、下載安裝Docker：至Docker官方網站進行下載，並安裝完成後如下圖：

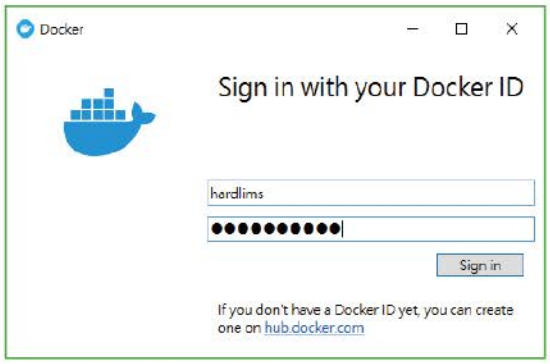
圖 參-3 Docker安裝完成畫面截圖



資料來源：本研究整理

二、註冊Docker帳號：首先至Docker官方網站https://hub.docker.com 進行註冊，完成後使用安裝好的Docker軟體進行登入，如下圖：

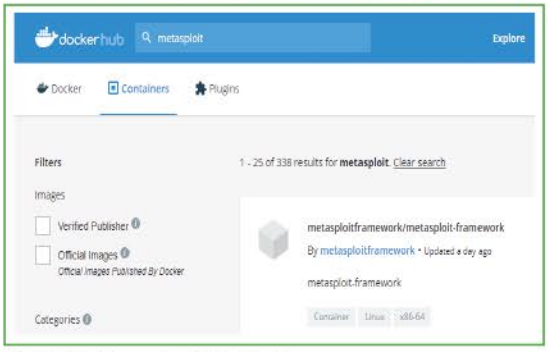
圖 參-4 Docker登入畫面截圖



資料來源：本研究整理

三、登入Docker並進行滲透測試工具Kali Linux相關套件搜尋，以下以Kali Linux常用的框架metasploit，工具進行示範，在搜尋欄位搜尋metasploit，如下圖：

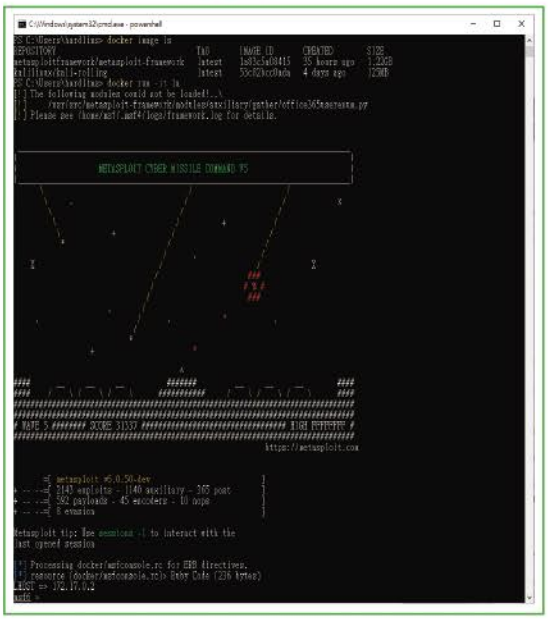
圖 參-5 Docker搜尋metasploit畫面截圖



資料來源：本研究整理

四、在Docker環境下啟動metasploit工具：透過Docker相關指令在Windows作業平台中的powershell執行Docker，並成功啟動metasploit工具，如下圖：

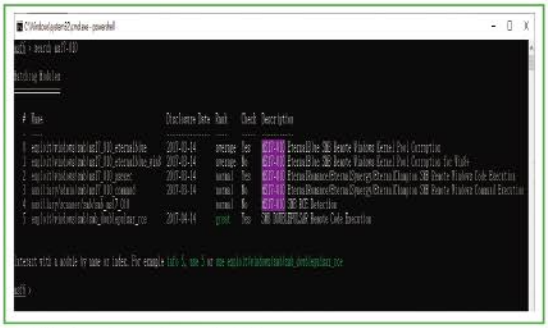
圖 參-6 滲透測試工具Metasploit在Docker容器中運行畫面截圖



資料來源：本研究整理

在metasploit中搜尋微軟系統相關漏洞資訊MS17-010，如下圖：

圖 參-7 滲透測試工具Metasploit在Docker容器中搜尋微軟系統漏洞（MS17-010）畫面截圖



資料來源：本研究整理

第二節、彰化銀行X-SOC架構說明

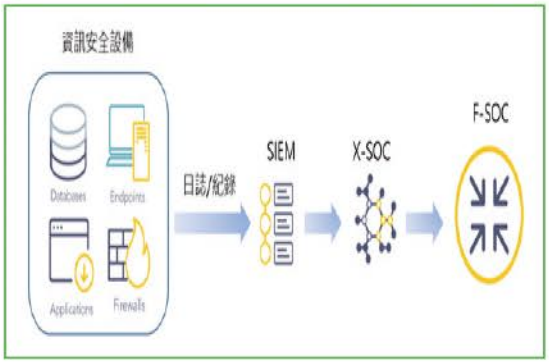
壹、平台架構圖

資訊安全威脅情資傳輸平台（X-SOC）具備網頁管理介面，提供管理者進行參數調整，與金融領域資訊安全防護（F-SOC）介接作業。

如下圖所示，資訊安全威脅情資傳輸平台X-SOC系統架構如下欄藍色框處，以本行而言，對外與金融領域資安監控F-SOC介接連線僅需開通單向 HTTPS協定。

硬體需求規格採用虛擬機架設，其規格為：CPU 4 Core、8G RAM、兩顆200GB Disk，資訊安全威脅情資傳輸平台X-SOC系統架構示意圖如下：

圖 參-8 X-SOC系統架構示意圖



資料來源：本研究整理

貳、平台功能說明

一、底層介接模組

（一）STIX JSON轉換模組：資安事件管理平台SIEM系統產出CEF格式事件單，透過syslog協定傳送至「STIX JSON 模組」進行 CEF to STIX JSON轉換。

轉存STIX JSON後，為 JSON Document格式，有別於CEF全純文字格式，JSON Document已解析為key-value型態，有助於資訊讀取。並平時先以 JSON格式保存，無XML過多贅字造成儲存空間肥大問題。必要時再轉換為 STIX XML，提供後續上傳流程。

（二）STIX XML 轉換模組：STIX雖為情資描述標準，但呈現變化可依據需求不同。如同HTML為網頁語法標準，但可被設計出不同的網頁。為避免各單位STIX描述方式有所差異，行政院國家資通安全會報技術服務中心G-SOC有定義八大事件類別，作為聯防監控體系之STIX情資範本。

金融領域資訊安全防護（F-SOC）沿用行政院國家資通安全會報技術服務中心G-SOC定義之STIX事件單格式，作為金融領域情資範本。此階段「STIX XML模組」將來源STIX JSON，產生符合G-SOC定義STIX XML的格式結構，並可通過其XSD驗證，確保事件單收容流程正確無誤。

（三）TAXII Client：金融領域資訊安全防護（F-SOC）目前定義兩種上傳機制。一種為人工登入至金融領域資安監控F-SOC網頁進行上傳；另一種為透過TAXII，將事件單上傳至金融領域資安監控F-SOC TAXII Server。

二、網頁管理模組

（一）事件單網頁管理&上傳金融領域資安監控F-SOC：以網頁管理介面取代命令列介面，讓資安人員以易用介面，完成事件單辨識與上傳金融領域資安監控F-SOC。

（二）使用者管理：帳號管理功能，用於帳號之新增、修改、刪除與檢視。並可配置帳號對應權限，讓使用者帳號登入時，依權限限縮使用功能。

（三）事件單列表與搜尋：以網頁列表方式進行事件單呈現，並提供搜尋功能，過濾特定事件單。

（四）事件單檢視、編輯及刪除：提供事件單管理，並可透過 網頁管理介面新增關聯分析事件單。

（五）事件單操作日誌紀錄：紀錄使用者進行事件單管理相關資訊，包含刪除、上傳與編輯。紀錄使用者登入資訊包括：帳號、連線IP、登入及登出時間。

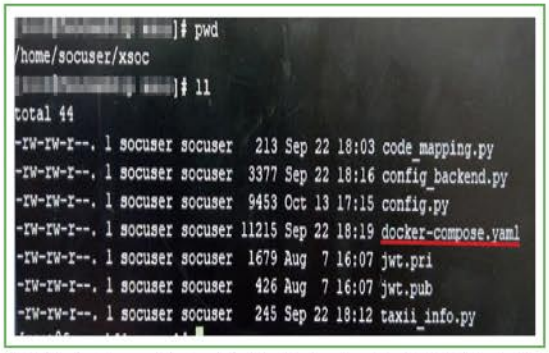
（六）平台資料備份功能：提供事件單資料庫備份功能。

參、應用軟體建置與管理

一、Docker-compose容器建置

金融領域資安監控F-SOC介接平台採用 Docker Compose機制建置，Docker Compose定義檔路徑如下：/home/socuser/xsoc/docker-compose.yaml。

圖 參-9 docker-compose.yaml檔案路徑畫面截圖



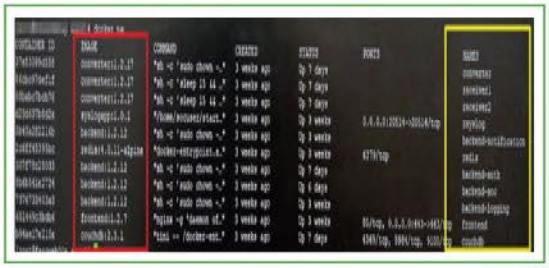
資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

執行Docker Compose定義檔，只需執行以下指令：

$ docker-compse up -d

相關的網路、應用服務與主機儲存（如建立資料夾）就會自動建立，並運作。金融領域資安監控F-SOC介接平台共建立11個容器服務，將於後續詳細說明用途。

圖 參-10 docker運行畫面截圖



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

二、Docker容器虛擬網路

虛擬網路部分，所有應用服務容器皆使用soc_app_net網路環境，其網段為XXX.XXX.XXX.0/24。所有容器皆於虛擬網路內通訊，除Web UI模組、Syslog模組外，其他容器服務外部皆無法存取。

而Web UI模組可被外部主機存取，主要透過docker port mapping機制，將容器的連接埠對應（mapping）到實體主機連接埠，Syslog模組也是同樣機制。

三、平台容器服務說明

金融領域資安監控F-SOC介接平台共建立11個容器服務，功能說明如下：

（一）rsyslog：Syslog Server負責接收來自資安事件管理平台SIEM傳送來的CEF Log，接收後將syslog message部分透過Web API機制，傳送至receiver1 或receiver2模組。

（二）receiver1：為 Web API Server，接收CEF Log並解析為key=value型態，解析完保存於Couchdb資料庫。即第壹章提及之 “STIX JSON轉換模組”。

（三）receiver2：同receiver1功能，與其組成高可用（HA） Web API Server。

（四）couchdb：保存receiver1 & receiver2轉換後的數據。

（五）converter：將STIX JSON轉換為 STIX XML，即第壹章提及之“STIX XML轉換模組”。

（六）frontend：網頁模組，即F-SOC介接模組Web 管理模組。

（七）backend-notification：為Web管理模組後端處理邏輯服務之一，主要負責發送郵件通知。

（八）backend-auth：為Web 管理模組後端處理邏輯服務之一，主要負責進行帳號驗證、權杖發放等相關帳號功能。

（九）baskend-soc：為Web 管理模組後端處理邏輯服務之一，主要負責事件單管理，包含 TAXII Client功能。

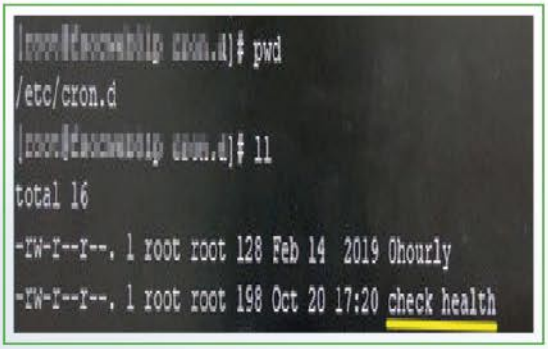
（十）backend-logging：為Web 管理模組後端處理邏輯服務之一，主要負責進行使用者模組操作紀錄。

（十一）redis：為Web 管理模組後端處理邏輯服務之一，主要負責進行登入時驗證碼（Captcha）與OTP保存。

肆、主機健康監控

金融領域資安監控F-SOC介接平台有健康監控排程，透過作業系統排程機制，觸發備份腳本。設定檔位置於下圖所示：

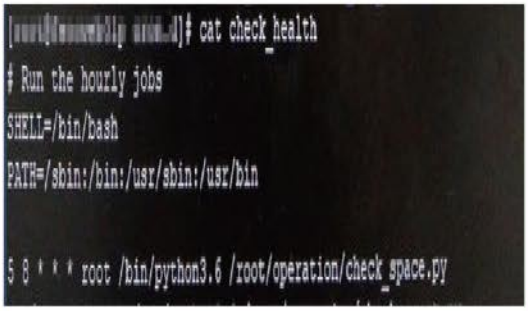
圖 參-11 F-SOC健康監控排程檔



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

Check health排程功能為檢查磁碟空間。當磁碟分割區使用率達80%時，會自動透過電子郵件寄送告警信件，如下圖：

圖 參-12 check health觸發時間與腳本位置



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

伍、維運處理程序

一、站台異動位址

站台IP更換時，需要編輯hosts設定檔案，路徑為/etc/hosts，透過編輯器進行IP修改，如下圖：

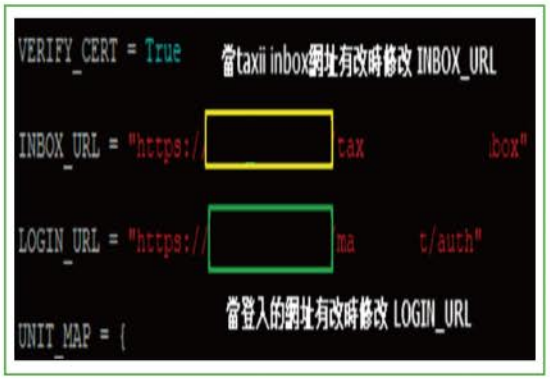
圖 參-13 修改IP畫面截圖

資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

二、若測試機或正式機網址有更換

若網址有更換時，需編輯taxii_info設定檔，其檔案路徑為：/root/xsoc/taxii_info.py，如下圖所示：

圖 參-14 修改網址畫面截圖



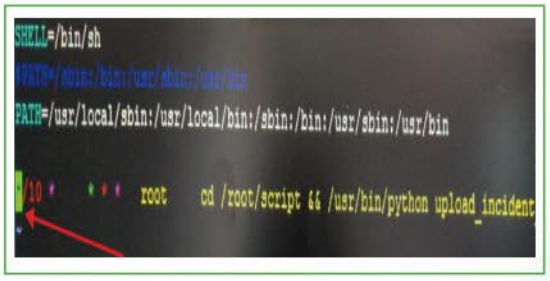
資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

完成修改後進行系統重新啟動，指令為：sudo docker restart converter。

三、啟用或停用自動上傳

透過註解／反註解來啟用或停用自動上傳排程，上傳排程位址路徑為：/etc/cron.d/run_autoupload，如下圖所示：

圖 參-15 自動上傳排程設定畫面示意圖



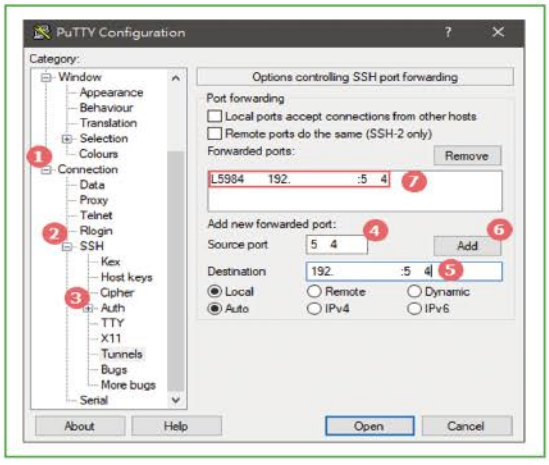
資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

四、手動清除資料庫

透過以下操作流程進行資料清除，詳細說明步驟如下：

（一）SSH Tunnel 連線設定：透過PuTTY連線工具，進入設定畫面後，由Category點選Tunnels，Soruce Port輸入5XX4，Destination輸入192.XXX.XXX.XXX:5XX4，點選【Add】新增設定，新增完成後設定出現於紅框處，既可登入Server，如下圖所示：

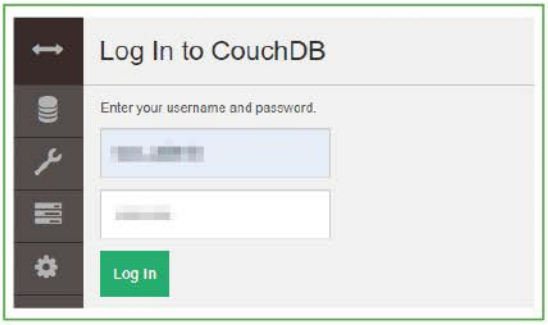
圖 參-16 SSH 連線Tunnel設定示意圖



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

（二）登入CouchDB並重新啟動服務：開啟瀏覽器，並於網址列輸入以下連結登入CouchDB5：http://127.XXX.XXX.1:5XX4/_utils/#login，輸入帳號及密碼後，點選【Log in】如下圖所示。

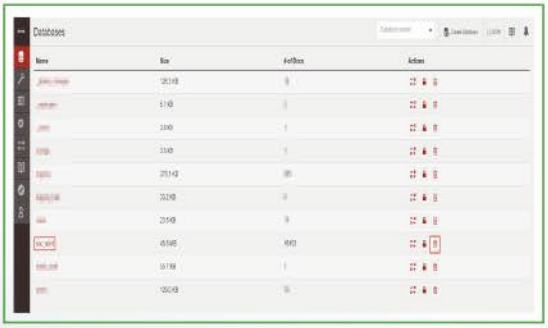
圖 參-17 CouchDB 登入示意圖



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

Databases選擇soc_alert點選刪除，如下圖所示。

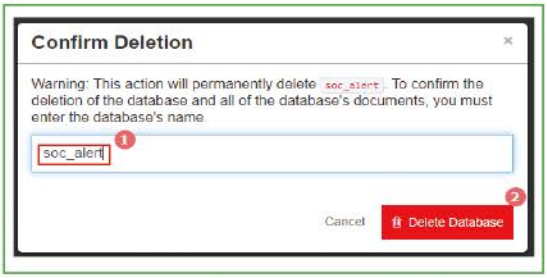
圖 參-18 Databases 列表示意圖



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

在Confirm 視窗輸入 database 名稱，點選【Delete Database】，如下圖所示，完成清除資料庫，如下圖：

圖 參-19 Database 清除示意圖



資料來源：彰化商業銀行金融領域資安監控F-SOC模組建置說明書

在指令列下輸入sudo docker restart converter receiver2，等待待receiver2重啟完成後，再輸入以下指令進行服務重啟sudo docker restart receiver1 backend-soc backend-logging backend-auth backend-notification，完成重啟服務作業

第三節、系統安全強化措施

本行資安事件管理平台SIEM彙整分析資訊集資安設備日誌後所產生的威脅情資，並透過資安威脅情資傳輸平台X-SOC，以STIX標準格式傳送至金融領域資安監控F-SOC，資安威脅情資傳輸平台X-SOC透過角色與權限，進行威脅情資管控，每一筆情資均需要管理者進行審核放行，才能傳送至金融領域資安監控F-SOC，由於資安威脅情資傳輸平台X-SOC存放本行相關資安威脅情資，透過系統安全強化措施提升系統安全性，本章節將針對系統安全強化措施進行詳細說明。

一、IP偽冒防禦強化措施（IP Spoofing protection）

透過調整Linux Kernel設定，避免來源路由攻擊（Source Routing Attack）。調整參數設定方式如下：

（一）編輯/etc/sysctl.conf：$sudo vi /etc/sysctl.conf。

（二）進行以下調整：

```
# IP Spoofing protection
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts=1
# Disable source packet routing
net.ipv4.conf.all.accept_source_route=0
net.ipv6.conf.all.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0
net.ipv6.conf.default.accept_source_route=0
# Ignore send redirects
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
# Block SYN attacks
net.ipv4.tcp_syncookies=1
net.ipv4.tcp_max_syn_backlog=2048
net.ipv4.tcp_synack_retries=2
net.ipv4.tcp_syn_retries=5
# Log Martians
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
net.ipv4.icmp_ignore_bogus_error_responses=1
# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
net.ipv4.conf.all.secure_redirects=0
net.ipv4.conf.default.secure_redirects=0
# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all=1
# disable tcp_timestamps
net.ipv4.tcp_timestamps=0
net.ipv4.conf.all.arp_notify=1
# Disable IPv6 auto config
net.ipv6.conf.default.accept_ra=0
net.ipv6.conf.default.autoconf=0
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.all.autoconf=0
# Disable Ipv4 forward
net.ipv4.ip_forward=0
# Disable IPv6
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

（三）重新載入設定

```
$ sudo sysctl –p
```

二、強化 Shared Memory避免未經授權的執行檔被執行

針對shared memory加入nodev,nosuid,noexec可避免未經授權的執行檔被執行。使用vi編輯 /etc/fstab，為tmpfs 加入nosuid,nodev,noexec後儲存，重新開機後生效。

三、限制 SSH人員存取之安全設定

指定特定使用者名稱與特定來源位址才能存取 SSH Service，先透過vi編輯vi /etc/ssh/sshd_config，再增加允許來源IP設定，可使用空白區隔，以便進行多筆不同來源IP位址設定，例如：Allow Users isac@192.XXX.XXX.XXX isac@192. .XXX.XXX.XXX ，完成後，使用指令$ sudo sytemctl restart ssh，重新啟動ssh服務後生效。

四、強化 SSH安全設定

系統預設帳戶root只能使用Private key登入，透過以下設定可完全禁止root登入，首先編輯編輯sshd_config，sudo vi /etc/ssh/sshd_config，調整PermitRootLogin 設定由yes變更為no，再重新啟動 sshd服務 sudo systemctl restart sshd。

五、取消無密碼用戶SSH連線請求

透過以下設定禁止沒有密碼的用戶使用SSH登入，首先編輯sshd_config，sudo vi /etc/ssh/sshd_config，再調整PermitEmptyPasswords設定由yes邊更為no，重新啟動 sshd服務sudo systemctl restart sshd。

六、修改SSH 協定版本

系統預設使用SSH-1協定，透過以下設定為SSH-2協定，提高安全性，首先編輯sshd_config，sudo vi /etc/ssh/sshd_config，新增以下設定Protocol 2，再重新啟動 sshd服務，sudo systemctl restart sshd。

七、SSH連線時間設置

透過以下設定，當閒置一定時間可自動中斷連線，首先編輯sshd_config，sudo vi /etc/ssh/sshd_config，然後調整ClientAliveInterval設定，從0變更為180秒，再重新啟動 sshd服務sudo systemctl restart sshd即可。

八、Log層級調整為Info等級

透過以下設定，設定Log Level 為Info層級，以詳細記載事件，首先編輯sshd_config，sudo vi /etc/ssh/sshd_config，然後再調整LogLevel設定，取消註解，將LogLevel調整為INFO，再重新啟動 sshd服務，sudo systemctl restart sshd即可。

九、強化SSH之 Ciphers

變更預設的加密演算法，首先編輯sshd_config，sudo vi /etc/ssh/sshd_config，設定檔最下方，增加 Ciphers、MACs、KexAlgorithms，Ciphers aes128-ctr,aes192-ctr,aes256-ctr MACs hmac-ripemd160,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160@openssh.com KexAlgorithms diffie-hellman-group-exchange-sha256，然後再重新啟動 ssh服務，sudo systemctl restart sshd即可。

十、停用 Ctrl+Alt+Del組合鍵盤輸入功能

執行以下指令systemctl mask ctrl-alt-del.target即可停用 Ctrl＋Alt＋Del組合鍵盤輸入功能。

十一、檢視不必要的服務埠，並關閉進行關閉

檢查目前的服務埠，sudo ss -anp | more，若發現有不必要的服務，可執行停用，sudo systemctl disable SERVICE_NAME，或直接進行移除，sudo apt remove package_name

十二、移除TTY（終端設備的統稱），限制root透過TTY方式登入

Limit root login to special devices，備份securetty，sudo cp /etc/securetty /etc/securetty_bak，執行以下指令，sudo cat /dev/null > /etc/securetty。

十三、調整特定目錄權限，設定為不可更改屬性

針對以下目錄增加不可更改屬性，防止資料更改、刪除。執行以下指令，注意：執行指令後，無法新增、刪除用戶，如需新增、刪除用戶需取消屬性，chattr＋i /etc/passwd、/etc/shadow、/etc/group、/etc/gshadow及/etc/services後，使用lsattr指令確認檔案屬性，取消檔案屬性chattr -i /etc/passwd、/etc/shadow、/etc/group、/etc/gshadow及/etc/services。

十四、調整使用者家目錄權限為 700

使用者家目錄權限為 700，先執行sudo ls –al /home查看使用者家目錄列表，再逐一執行sudo chmod -R 700 USERNAME。

十五、防止用戶使用 su 指令成為 root

首先編輯su檔案sudo vi /etc/pam.d/su，新增以下指令auth sufficient /lib/security/pam_rootok.so debug auth required /lib/security/pam_wheel.so group=wheel再將需要的使用者新增至wheel group即可使用su指令，usermod -aG wheel XXXXXXX，存檔後生效。

十六、強化密碼安全設定

透過變更passwd與pwquality.conf設定，進行密碼強度及其相關設定。編輯passwd，sudo vi /etc/pam.d/passwd，新增以下指令password required pam_pwquality.so retry=3，編輯 pwquality.conf，sudo vi /etc/security/pwquality.conf，新增以下指令，密碼長度（12字元）、密碼須有英文、符號及數字、禁止連續字元（3字元）如“abc”或“111”。

minimum length of 8 characters

minlen = 12

The minimum number of required classes of characters for the new password（digits, uppercase, lowercase, others）.

minclass = 4

To set a password strength-check for character sequences and same consecutive characters

maxsequence = 3

maxrepeat = 3

第肆章 結論

本研究以「銀行業導入網路威脅情資」為研究目標，探討企業組織內部資安團隊透過網路威脅情資的蒐集、分析、利用以及分享，以有效利用資安威脅情資，協助組織決策者進行資安策略訂定與技術強化措施，在駭客發動攻擊之前，降低組織可能產生的破口、漏洞及弱點，以達到企業耗費最低成本，獲得最大資安防禦能量目的。

在攻擊事件已經發生之後，企業組織所進行的因應措施成本非常高，無論是在有效阻擋駭客的攻擊或是清除駭客已建立的立足點，都須付出相當大的資源。對防禦者而言，最好策略即是在攻擊鏈中盡可能在駭客發動攻擊之前，就已經採取行動，藉由網路威脅情資的利用，可讓企業組織由事後補救的被動策略，轉變為主動防禦策略，以相對低的成本提升整體資訊安全。

近幾年中央政府的資訊安全政策已逐步拉高到國家安全的層級，促使國家層級的N-SOC的快速發展，行政院資通安全處為建構國家資訊安全聯防體系，同步推動八大關鍵領域之資安威脅情資分享機制，依據「國家資通安全防護整合服務計畫領域SOC實務建置指引」要求，領域層級 SOC需彙整該領域之相關情資，並採用 STIX標準格式封裝回傳給國家層級N-SOC，而金融領域F-SOC藉由各金融單位的資安威脅情資分享，提升本國金融機構之資訊安全。本行於2021年所建置之威脅情資傳輸平台X-SOC，透過情資交換STIX標準格式提供本行資安相關情資給F-SOC，再由F-SOC與N-SOC系統進行資安威脅情資的蒐集、交換與分享，以達到金融機構資安威脅情資之分享、監控及聯合防禦之綜效，強化本國金融體系之資訊安全。

伴隨著金融科技蓬勃發展，駭客攻擊手法戰略更加多元化，且難以掌握，而透過大量網路威脅情資的使用，將有助於企業組織對抗現行複雜網路攻擊趨勢，提升資訊安全防禦能量。

～完～

參考文獻

1. Google Trend。Cyber Threat Intelligence關鍵字統計（全球2004-2021），取自美商谷歌網路搜尋公司。https://trends.google.com.tw/trends/explore?date=all&q=Cyber%20Threat%20Intelligence。
2. 行政院資通安全處，2021，政府領域資安聯防監控作業規範。
3. Christopher S. Johnson, Mark L. Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150, October 2016, http://dx.doi.org/10.6028/NIST.SP.800-150.
4. Matt Bromiley. "Threat Intelligence: What It Is, and How to Use It Effectively," SANS Institute Information Security Reading Room, 2016, https://www.sans.org/reading-room/whitepapers/threathunting/threat-intelligence-is-effectively-37282
5. OSINT Framework, https://osintframework.com/
6. OpenPhish, https://openphish.com/
7. PhishTank, https://www.phishtank.com/
8. PhishStats, https://phishstats.info/
9. nQuest, https://inquest.net/
10. MITRE ATT & CK, https://attack.mitre.org/
11. 蘇柏鳴，2020，MITRE ATT&CK 框架概述，金融聯合徵信第三十七期，期刊。
12. FIND，2020，MITRE ATT&CK：一種從攻擊面探討的全新資安威脅模型，https://www.find.org.tw/index/wind/browse/352c42330a0ca7492f9df54d63f51417/
13. IBM X-Force Exchange, https://exchange.xforce.ibmcloud.com/
14. Project Honey Pot, https://www.projecthoneypot.org/index.php
15. HoneyDB, https://www.honeynet.org/
16. Mrlooquer, https://mrlooquer.com/
17. 蔡福隆，2018，推動我國金融資安聯防體系，財金資訊季刊。
18. iTHome，2019，IntSights彙整暗網與內部動態，打造企業專屬威脅情報，iThome online，https://www.ithome.com.tw/review/131827
19. Google Trend。Dark Web關鍵字統計（全球2004-2021），取自美商谷歌網路搜尋公司。https://trends.google.com.tw/trends/explore?date=all&q=Dark%20web
20. 0day.today, https://0day.today/
21. Common Vulnerabilities and Exposures, https://cve.mitre.org/
22. Exploit DB, https://www.exploit-db.com/
23. Dark Web, Haystack, http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/
24. Dark Web, Torch, http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/cgi-bin/omega/omega
25. Dark Web, Tor Onionland, http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/

26. Dark Web, Happy Blog, http://dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion
27. Dark Web, Dopple Leaks, http://hpoo4dosa3x4ognfxpqcrjwnsigvslm7kv6hvmhh2yqczaxy3j6qnwad.onion
28. 賴漢鍾，2016，應用STIX於網路威脅情資之研究，國防大學，碩士論文。
29. 林宛蔚，2020，基於STIX/TAXII標準格式建構資安威脅情資應用系統，樹德科技大學，碩士論文。
30. Sean Barnum., 2014, STIX Whitepaper v1.1, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression（STIX™）, MITRE.
31. 行政院資通安全處，2017，國家資通安全防護整合服務計畫領域SOC實務建置指引。
32. iTHome，2021，臺灣資安大會直擊蔡英文總統出席臺灣資安大會，首度公開「資安即國安2.0」戰略，iThome online ，https://www.ithome.com.tw/news/144172
33. 李金榜，2017，第一次用Docker就上手，碁峰出版。
34. 楊保華，2017，Docker入門與實戰，碁峰出版社。
35. Docker doc, 2021, https://docs.docker.com/get-started/overview/
36. 安碁資訊，2021，彰化商業銀行金融領域資安監控（F-SOC）模組建置說明書，專案建置說明書。
37. Shackleford, D., 2015, Who’s Using Cyberthreat Intelligence and How?, SANS Institute.
38. E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Proc. 6th Int’l Conf. Information Warfare and Security （ICIW 11）, Academic Conferences Ltd., 2010, pp. 113–125;
39. https://stixproject.github.io/getting-started/whitepaper/#ref-9
40. iTHome，2018， Structured Threat Information eXpression， iThome online， https://ithelp.ithome.com.tw/articles/10206720