出國報告（出國類別：訓練）

「Cyber Defence Singapore 2019」出國受訓報告

服務機關：法務部調查局

姓名職稱：簡調查官稚軒及游調查官騰葦

派赴國家：新加坡

出國期間：108年7月7日至14日

報告日期：108年10月7日

摘要

為因應國內重要關鍵基礎設施發生重大資安事件，影響社會秩序，於資安鑑識作業時發現諸多技術亟待強化精進；另美國SANS Technology Institute為全球知名之網路安全及數位鑑識訓練機構，於全球已培育諸多資安專業人員，提供許多實務經驗及最新技術訓練課程，此次於108年7月8日至13日在新加坡舉辦之「Cyber Defence Singapore 2019」，課程計有「ICS515：ICS Active Defense and Incident Response」單元，內容包含網駭威脅情資整合、記憶體分析、網路流量監控、惡意程式分析及主動防禦等，對於強化本局資安事件調查及鑑識極有助益。

目次

壹、受訓目的

駭客攻擊手法日新月異,且針對關鍵基礎設施或工業控制系統實施客製化特殊攻擊,往往造成巨大傷害,為因應攻擊手法不斷翻新,強化資安鑑識及資安維護技術,特別針對網駭威脅情資整合、記憶體分析、網路流量監控、惡意程式分析及主動防禦等方面加強學習,故參加由美國SANS公司於新加坡舉辦之「Cyber Defence Singapore 2019」課程強化技能,此次課程包含「ICS515:ICS Active Defense and Incident Response」單元,簡述如下:

(一) ICS515:ICS Active Defense and Incident Response:

此項課程講授人Kai Thomsen先生,其主要專長為電腦入侵鑑識及資安事件調查,實務經驗約15年,曾經於奧迪(AUDI汽車)建立網路防禦團隊扮演重要角色,目前是奧迪首席數位鑑識分析師,以保護企業、工業控制系統(Industrial Control System ,ICS)及互聯汽車基礎設施。課程內容係針對工業控制系統或關鍵基礎設施發生資安事件時之預警措施及通報流程、威脅狩獵(threat hunting)、入侵鑑識、記憶體分析、時序分析及反鑑識分析等,講師照片如下:

鑑識主機軟硬體需求:

(1)CPU: 64-bit system.

(2)Laptop with Windows 10 installed on the host or in a Virtual Machine.

(3)Laptop with at least two USB ports.

(4)Ability to update BIOS configuration settings to enable

virtualization (VT) support.

(5)Latest VMware Player (7 or higher), VMware Workstation (11 or higher), or VWware Fusion installed.

(6)Ability to disable all security software on your laptop, including antivirus and/or firewalls.

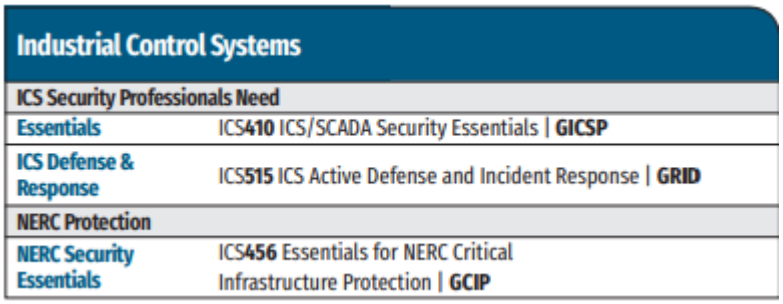
(7)At least 100 GB of hard-drive space.

(8)At least 8 GB of RAM.

(9)Local Administrator Access within the host operating system and BIOS settings.

(10) Wireless Ethernet 802.11 B/G/N/AC.

（二） SANS Industrial Control System (ICS) courses road map：



此次受訓行程如下所示：

日期	內容	地點
07月07日（星期日）	桃園中正機場搭機－抵達新加坡樟宜機場	臺北-新加坡
07月08日（星期一）	ICS515.1-Threat Intelligence	新加坡
07月09日（星期二）	ICS515.2-Asset identification and Network Security Monitoring	新加坡
07月10日（星期三）	ICS515.3-Incident Response	新加坡
07月11日（星期四）	ICS515.4-Threat and Environment Manipulation	新加坡
07月12日（星期五）	ICS515.5-Active Defense and Incident Response Challenge	新加坡
07月13日（星期六）	會晤新加坡警方，交換網安情資及討論雙邊	新加坡

日期	內容	地點
	合作電信詐欺案件	
07月14日（星期日）	新加坡樟宜機場搭機－抵達桃園中正機場	新加坡-臺北

貳、行程記述

一、7月7日（星期日）抵達新加坡樟宜國際機場，前往飯店辦理入住手續，整備行李後準備次日受訓相關事宜。

二、7月8日(星期一) ICS515.1-Threat Intelligence：

安裝並設定課程所需之虛擬環境,並說明目前實務上針對工業控制系統及關鍵基礎設施遭遇資安事件時的通報回應及處理流程,強調資安事件事前防護及事後分析檢討應該相輔相成，另外工業控制系統（ICS）安全專業人員必須能夠利用內部和外部威脅情資來分析威脅，擷取危害指標(IOC）並指導安全團隊在環境中發現威脅，並於課程中講解實務上案例，包括2011年發生於美國伊利諾伊州的水公司遭駭(Illinois Water Utility)及2010年發生於伊朗核電廠遭Stuxnet病毒駭侵，皆造成重大影響。再者，由於現今企業組織規模逐漸擴大，動輒跨越不同國家領域，然而網路世界沒有國界,各企業應該建立完整的資安防護架構,選用適合企業組織的遠端監控系統,針對特定資安攻擊作防護及過濾,方能有效萃取出數位資料進行分析。

實作練習：

(1)CYBATIworks Kit - Build a PLC：Build the CybatiWorks™(PLC) and Load the Traffic Light Project File onto the PLC.

(2)ICS Information Attack Surface Mapping with Shodan：Familiarization with Shodan and Google Hacking Queries. Identify Information About Your Organization.

(3)ICS Honeypots and Analysis of Competing Hypotheses：Analyze Data from System Events and Alerts. Choose the Most likely Scenario.

(4)Consuming ICS Threat Intelligence：Generate Alerts for New ICS Appearing in Shodan. Create an ICS Heatmap in Maltego with Shodan.

三、7月9日(星期二) ICS515.2-Asset identification and Network Security Monitoring：

徹底瞭解網路架構及環境是企業主動防禦重要的一環，為對未知的風險進行防禦，此時收集數據、檢測並分析威脅及利用威脅情資進行主動防禦，所使用的技術包括Wireshark、TCPdump、SGUIL、ELSA、CyberLens、Bro、NetworkMiner和Snort等開源(Open Source)軟體，另外針對實務案例進行討論，包括Water Distribution System及Oil Rig Ballast Control System，並針對ICS特殊網路通訊協定進行解析。

實作練習：

(1)Asset Discovery：List the connected assets on the network by Ethernet and IP address. Identify what ICS protocols are used on the network.

(2)Collecting the Right Data from ICS Assets：Analyze Network Traffic to Identify the Network Behavior. Load the New Project File to the PLC.

(3)Detecting Potentially Malicious Activity：Test the Environment with a Basic Snort Rule. Apply the Snort Rules from the Threat Intelligence Consumption Personnel.

(4)ICS Network Visualization：Visualize the ICS Network.

(5)Analyzing the Detections：Analyze the Suspect Traffic to Determine Any New Communications. Determine if the Process was Attacked.

四、7月10日(星期三) ICS515.3-Incident Response：

準備和執行ICS事件回應的能力對於控制系統的安全性和可靠性至關重要。ICS事件回應是ICS主動防禦中的核心概念，事件調查人員必須安全地擷取數位證據，同時確定環境的威脅及其對運營的影響。ICS事件回應需有效的策略和工具來收集和保存相關數據，並使用這些數據進行即時的分析並建立威脅指標(IOC)。另外針對數位證據解析，包括分析系統檔案輔助瞭解遭入侵時的軌跡，例如可以利用Prefetch檔案瞭解惡意程式觸發的時點、UserAssist資訊可以瞭解哪些帳號執行了哪些程式、分析系統Log檔案之事件代號可以瞭解哪些帳號透過什麼方式登入，判斷瞭解入侵方式，進一步推敲惡意程式是在何時入侵，以及還原遭惡意程式抹除的檔案。

實作練習：

(1)Acquisition in an Operational Environment：Install Redline and Create a Collector. Collect Vital Data for Initial Triage. Familiarize Yourself with Redline.

(2)Network Analysis During Incident Response：Analyze Network Traffic During the Incident Response Collection. Analyze the Data Historian Outputs.

(3)Memory Forensics：Familiarization with the Baseline Memory. Identify Malicious Activity in Suspect Memory.

(4)Incident Response Digging Deeper：Use Redline to Understand the Host Level Issues.

(5)IOCs in Action：Develop an IOC. Test the IOC Against the Infected Image.

五、7月11日(星期四) ICS515.4-Threat and Environment Manipulation：

瞭解威脅是發現其影響ICS的重要關鍵，利用惡意程式分析流程中，

獲取威脅情資，並對網路環境進行必要的調整以降低威脅的有效性，此類威脅情資對於ICS主動防禦至關重要，需由內部數據收集來創建和共享威脅情資。如何分析初始攻擊媒介（例如，魚叉式電子郵件），即時執行惡意程式分析技術，分析記憶體以及運用惡意程式特徵創建威脅指標為企業建立整體主動防禦關鍵。

實作練習：

(1)Analyzing Initial Attack Vectors：Familiarization with Good PSFs. Identifying Potentially Malicious PDFs.

(2)Timely Malware Analysis：Analyze the Malicious Logic File. Perform Automated Malware Analysis.

(3)YARA Development：Develop a Basic YARA Rule. Develop a YARA Rule for the Indicators. Upload the Good Project File and Validate.

六、7月12日(星期五) ICS515.5-Active Defense and Incident Response Challenge：

進行挑戰競賽，競賽項目為模擬化學石油廠網路遭受入侵，現場採集到的數位證據包括內外部網路封包及記憶體，透過分析這些數位證據釐清整體網路架構、特殊通訊協定、受駭主機及受駭範圍，並從中採擷惡意程式進行威脅情資分析。

七、7月13日(星期六)會晤新加坡警方：

當日中午1時許於受訓飯店大廳與新加坡警方見面，以非正式的案件討論形式，交換去年新加坡警方協請本局調查駭客架設釣魚網站之偵辦進度及偵查所得之線索。

八、7月14日(星期日) 從新加坡樟宜國際機場搭機回程，帶著滿滿的收穫回

到臺灣，此次受訓內容非常紮實，每一天的課程都充滿挑戰，也將此次成果帶回局裡與大家交流分享經驗。

參、心得與建議

此次受訓課程主要針對工業控制系統及關鍵基礎設施之資安事件調查及資安鑑識等議題，相較於一般企業發生資安事件時所造成的影響，更容易造成大規模的損害，嚴重影響社會秩序及國家安全，而工業控制系統及關鍵基礎設施資安防護較為薄弱，且網路系統也較為封閉，發生資安事件時應採取之措施也不同於一般企業，針對入侵者如何找尋系統漏洞伺機發動攻擊，而鑑識人員如何從系統稽核資料及相關檔案屬性找尋入侵軌跡，都是相當大的挑戰，唯有透過網路攻防不同角度觀察相同事件，始能激發各種無限可能，而資安觀念也並非僅只是相關技術人員需要瞭解，組織內部所有成員都該具備相關資安意識。另針對網駭威脅情資，可以透過網際網路公開資料，結合組織內部情資，加以分析整合，並利用大數據資料庫儲存案關重要證據或線索進行交叉比對，將可過濾出許多有用資訊，故情資蒐集應與案件偵辦結合運用，彼此交流情資線索，有助於建構完整情報網，達到主動防禦功能。