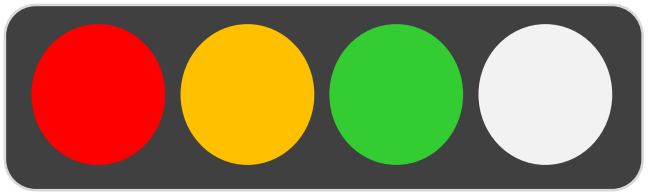
金融資安資訊分享與分析中心（F-ISAC）營運成果暨年度重點工作報告

Trust



TLP是信賴的處理原則

紅燈 TLP:RED

資訊僅限提供者指定之限定群組，通常透過口頭或面對面進行資訊交換。

黃燈 TLP:AMBER

接收者只可與自己組織的成員及需要了解這些資訊的廠商(進行必要之處理以防止傷害擴大)分享，但提供者仍可自由指定特定之資訊分享限制。

綠燈 TLP:GREEN

接收者可以與同屬單位或社群的人員或夥伴組織分享，但並非透過公開存取管道，且不可以在社群外散布。

白燈 TLP:WHITE

基於標準版權規則，此資訊可以無限制的散布。

簡報大綱

壹 營運成果

貳 年度重點工作

壹、營運成果

會員招募

374家金融機構會員

銀行、產壽險、證券期貨、投信投顧註

全數入會

註：開辦電子平台交易之投信投顧業者

壹、營運成果

情資分享與分析

- 提供偽冒我國金融機構網站及行動應用程式公告，以利民眾識別，避免遭受損失。

➢ 發布「**辦理偽冒金融機構網站及行動應用程式處置建議措施**」。

- 針對國際間重要資安攻擊事件、惡意程式等提供相關調研報告。

➢ 發布「**金融領域ATM與SWIFT資訊安全防護研究報告**」。

➢ 發布「**國際駭客組織針對我國金融機構發動DDoS勒索攻擊報告**」。

- 彙整國內外重大資安訊息與資安威脅趨勢預測，並提供FS-ISAC與SWIFT-ISAC之每週彙整資安情資。

➢ 發布「**馬來西亞金融機構CIMB遭勒索軟體攻擊之入侵威脅指標**」。

- 針對高風險（含有可利用之攻擊程式）以上漏洞，每日查找、分析及發布，以利會員即時評估及研擬因應對策。

➢ 發布「**VPN產品Pulse Secure高風險漏洞，且已有可利用之攻擊程式**」。

- 彙整前一週之弱點摘要、重要弱點修正程式、已被揭露攻擊程式碼之弱點、重要資安新聞、高風險惡意IP及網域等。

➢ 新增「**焦點議題，針對重要新聞事件進行分析，並提供偵測及防護建議**」。

- 彙整前一月之攻擊事件類型統計、攻擊來源分布統計、分散式阻絕服務攻擊(DDoS)攻擊流量統計、惡意軟體統計、資安威脅摘要等、重大政策、金融資安、共通資安及會員分享，並提供偵測及防護建議。

➢ 新增「**金融資安、共通資安及會員分享分析，並提供偵測及防護建議**」。

壹、營運成果

會員情資分享

108年度F-ISAC會員分享統計

未設定
0 個關注者

關注

Dec 18, 2019

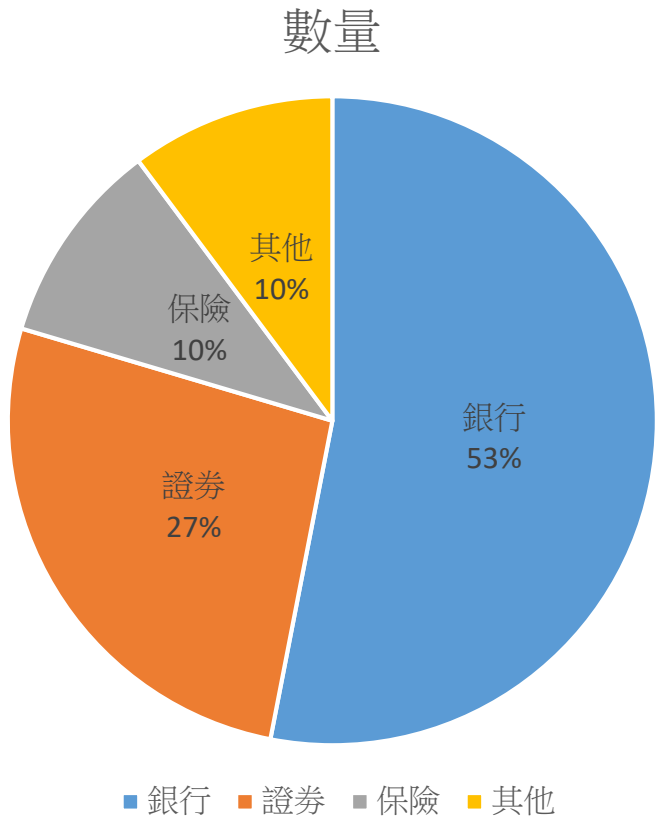
F-ISAC自今(108)年起規劃多項會員情資分享項目，迄今已有49家會員參與分享；分享情資數量亦達237則，另有26家會員定期分享其資安防護設備偵測或攔阻之統計資訊。F-ISAC感謝分享情資之會員，將持續於研討會、教育訓練及會員拜訪等活動加強推廣，期能與會員建立聯防體系，共同抵禦我國金融產業所面對之網際網路攻擊威脅，108年度F-ISAC會員分享統計如下:

一、銀行:臺灣銀行、土地銀行、合作金庫銀行、第一銀行、兆豐商銀、國泰世華銀行、高雄銀行、台中銀行、板信商銀、淡水一信、臺灣中小企銀行、京城銀行、日盛金控、聯邦銀行、玉山銀行、凱基商銀、安泰銀行、中國信託商業銀行、三信商業銀行、中國輸出入銀行、台新銀行、花旗銀行、富邦金控、華南銀行、新光銀行、彰化銀行。

二、證券投信:金管會證券期貨局、臺灣證券交易所、臺灣集中保管結算所、兆豐證券、凱基證券、中國信託證券、統一綜合證券、元大證券、元富證券、國泰投信、野村投信、群益金鼎證券、德意志證券。

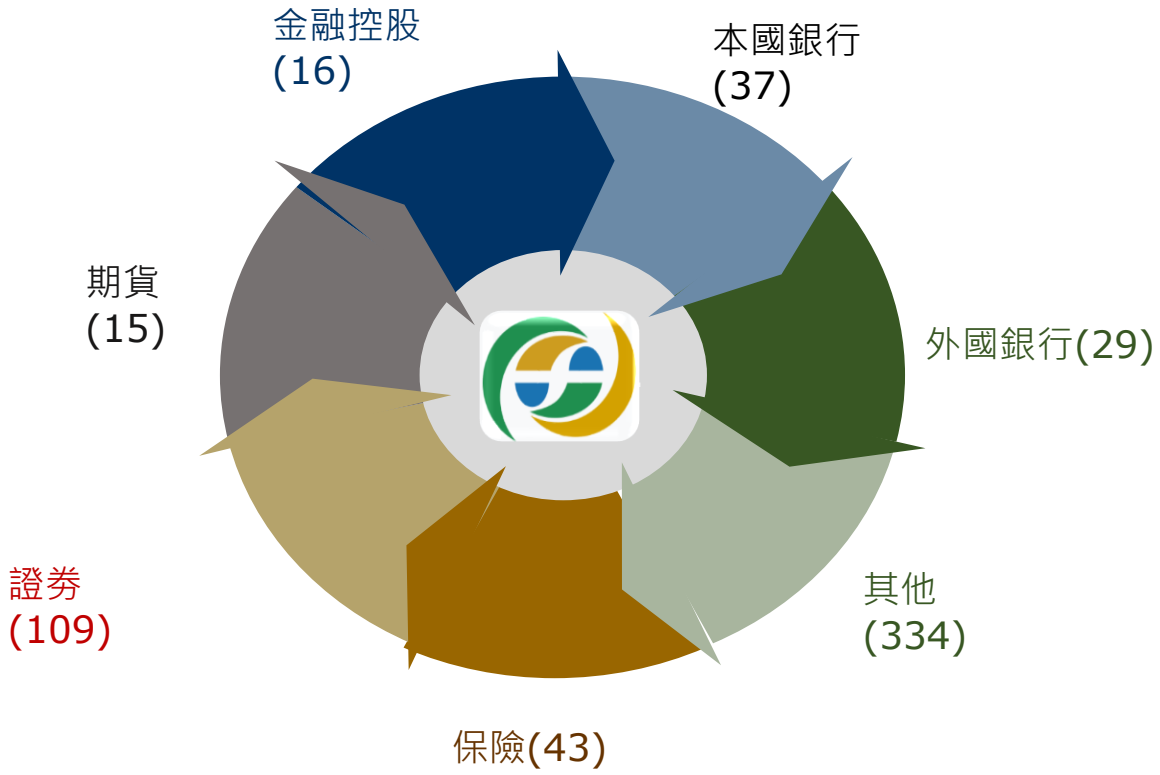
三、保險:南山人壽、新光人壽、明台產物保險、宏泰人壽、新安東京海上產險。

四、其他:中央銀行、台灣票據交換所、財團法人金融聯合徵信中心、農業金庫、財金公司。



壹、營運成果

重大警訊發布（1/2）



F-ISAC於 2019年10月28日接獲多家會員分享，接獲以駭客組織Cozy Bear名義，寄送主旨為「DDoS attack」之勒索信件，依據內文顯示其將於預告日期發動DDoS攻擊，並勒索2比特幣，若未於期限內付款，除將每日增加贖金，並將針對所屬網站於本週四進行大規模DDoS攻擊，請會員提高警覺。

依據MITRE ATT&CK[1]，駭客組織Cozy Bear（又稱APT29、YTTRIUM、The Dukes及CozyDuke）與俄羅斯政府有關，並自2008年起開始活動，該駭客組織亦被報導與2015年入侵美國民主黨全國委員會 (Democratic National Committee) 事件相關。

勒索信件內容說明如下：

1. 寄件人：Cozy Bear <sencastsciswac1975@protonmail[.]com>
2. 主旨：DDoS attack
3. 信件內容：

我們是「Cozy Bear」，我們選擇了(國內金融機構)作為下一次DDoS攻擊的目標。
請在Google搜尋「Cozy Bear」，以了解我們的背景資訊。
從周四上午開始，你的網路將受到DDoS攻擊。
（這不是一個騙局，現在為了證明這一點，我們將對(國內金融機構) 進行一次持續30分鐘的小型攻擊，這不會是嚴重的攻擊，也不會給你造成任何損害，因此請暫時不用擔心。）

一但我們展開攻擊，你的網站和其他對外服務將無法使用。

你必須要支付少量的費用來避免我們對你的服務進行攻擊，目前贖金費用為2比特幣（BTC），但如果你決定不付款，我們將在指定的日期開始攻擊，攻擊將會持續到你支付費用為止，沒有其他解決方法可以停止攻擊，如果尋求其他解決方案只會浪費你更多的錢（Cloudflare、Sucuri、Imperva及類似的服務是沒有用的，因為我們將直接攻擊你的IP）。我們將徹底破壞你的聲譽，並確保你的服務在付款之前將保持離線狀態。
不要回覆此電子郵件，並請勿嘗試協商，我們將不會閱讀任何回覆。支付費用後，我們將不會發起攻擊，你也永遠不會再收到我們的來信。

請注意，比特幣是匿名的，沒有人會發現你已經付贖金。

壹、營運成果

重大警訊發布（2/2）

全球性攻擊

本次事件為駭客組織「Cozy Bear」及「Fancy Bear」針對全球金融機構發動DDoS勒索攻擊，包含我國、新加坡、日本及紐西蘭等多個地區。

金融資安聯防

本次與證交所密切合作，除F-ISAC第一時間發布警訊提供預警，證交所並將F-ISAC警訊同步通知證券資訊主管，故本次會員均能有效因應及應處。

國內資安聯防

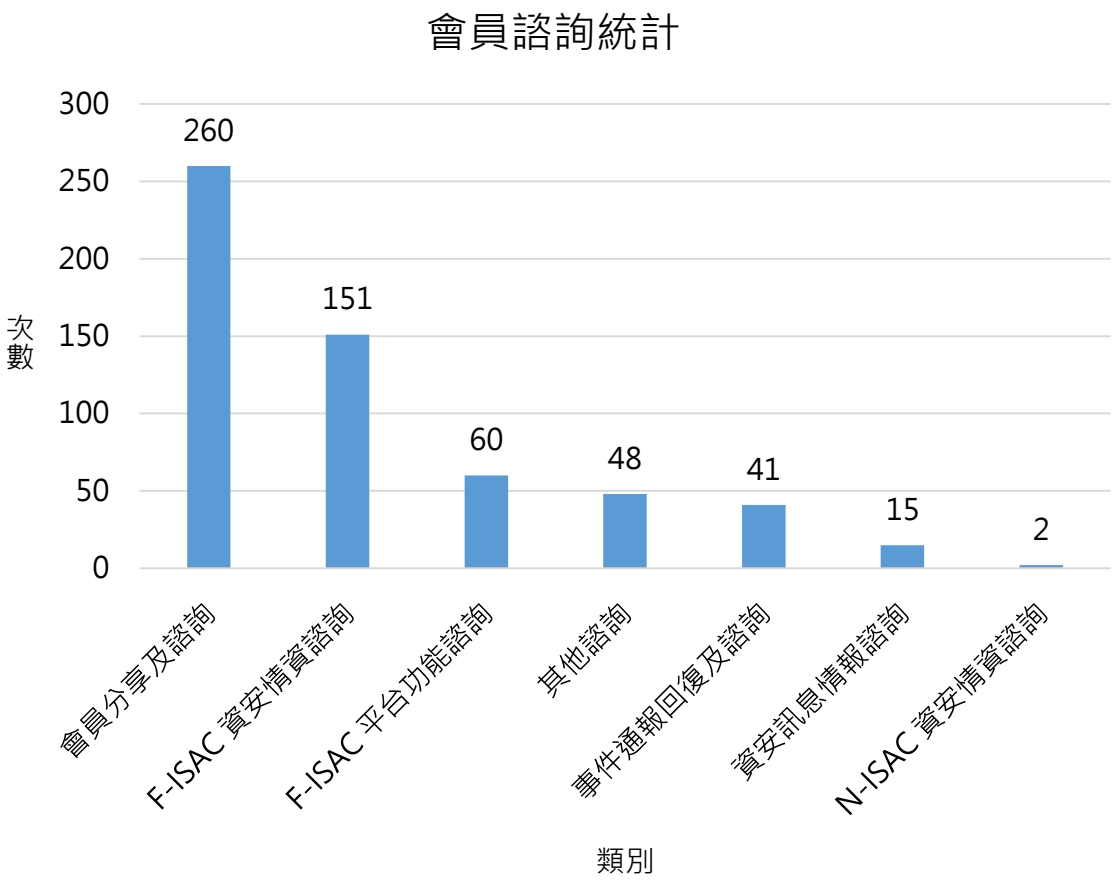
將攻擊IP分享給N-ISAC及TWCERT/CC進行國內及國外IP通報處理。同時協調國內通傳會C-ISAC協助監控攻擊IP，有效預警，達成領域聯防。

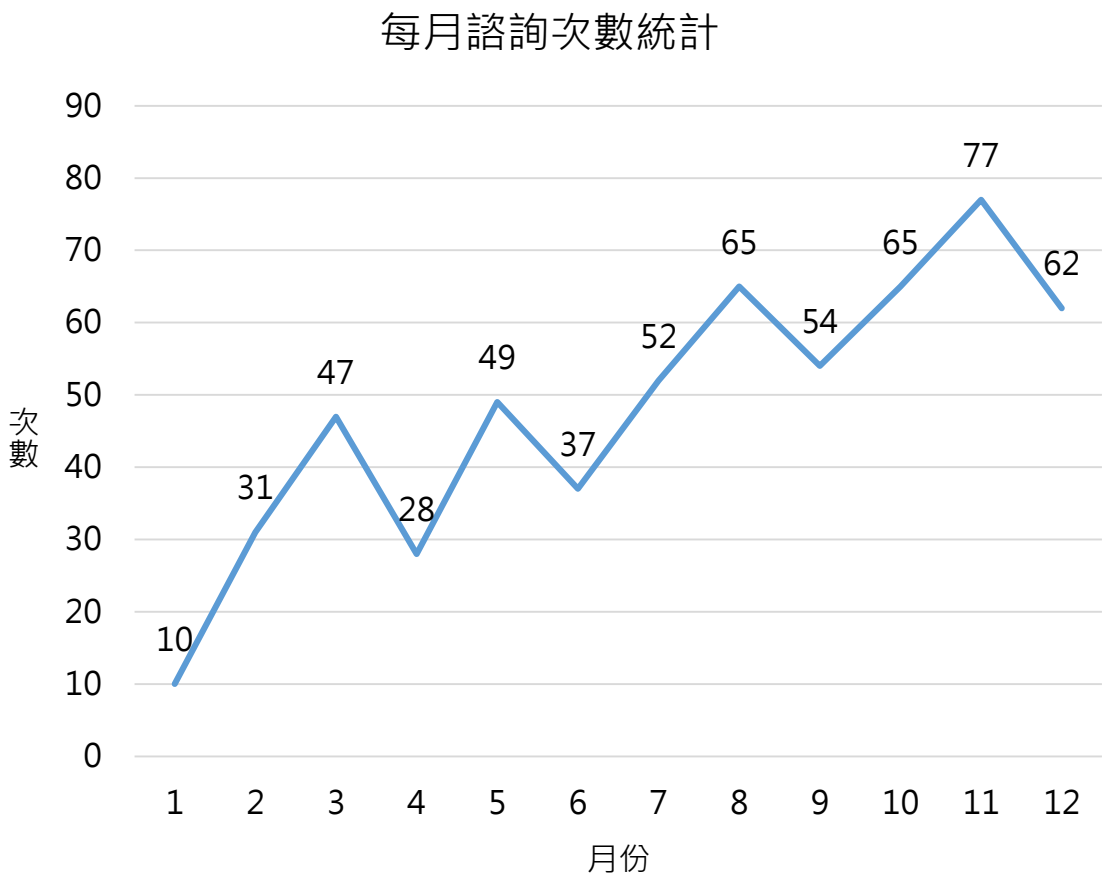
國際資安聯防

將攻擊IP及樣本分享給美國FS-ISAC、歐盟FI-ISAC、日本F-ISAC及韓國金融資安機構（FSI），共同打擊殭屍網路，提升我國資安能見度。

壹、營運成果

會員諮詢

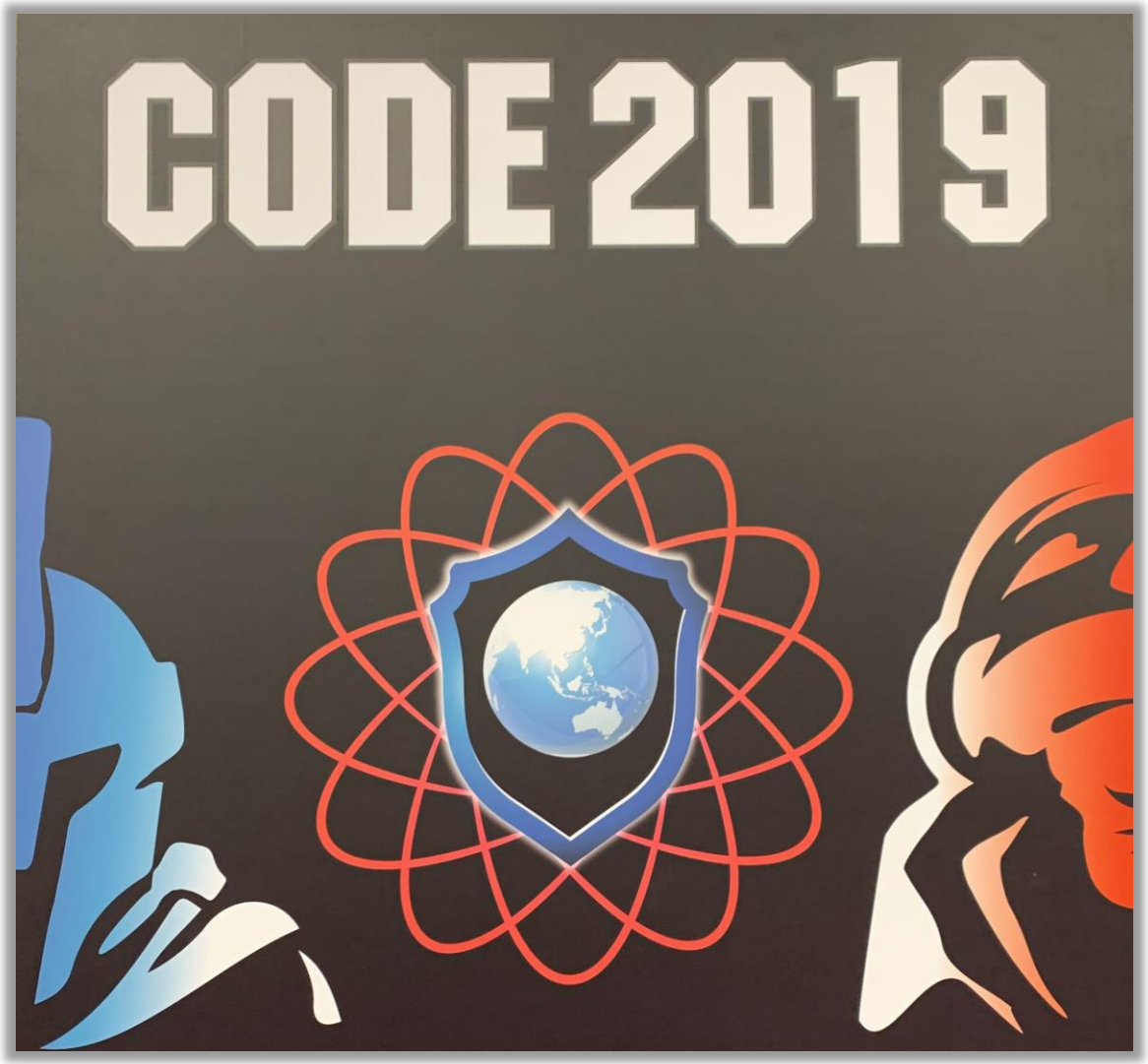

會員諮詢統計
300
250
200
150
100
50
0
次數
260
151
60
48
41
15
2
會員分享及諮詢
F-ISAC 資安情資諮詢
F-ISAC 平台功能諮詢
其他諮詢
事件通報回復及諮詢
資安訊息情報諮詢
N-ISAC 資安情資諮詢
類別


每月諮詢次數統計
90
80
70
60
50
40
30
20
10
0
次數
10
31
47
28
49
37
52
65
54
65
77
62
1
2
3
4
5
6
7
8
9
10
11
12
月份

壹、營運成果

跨國演練

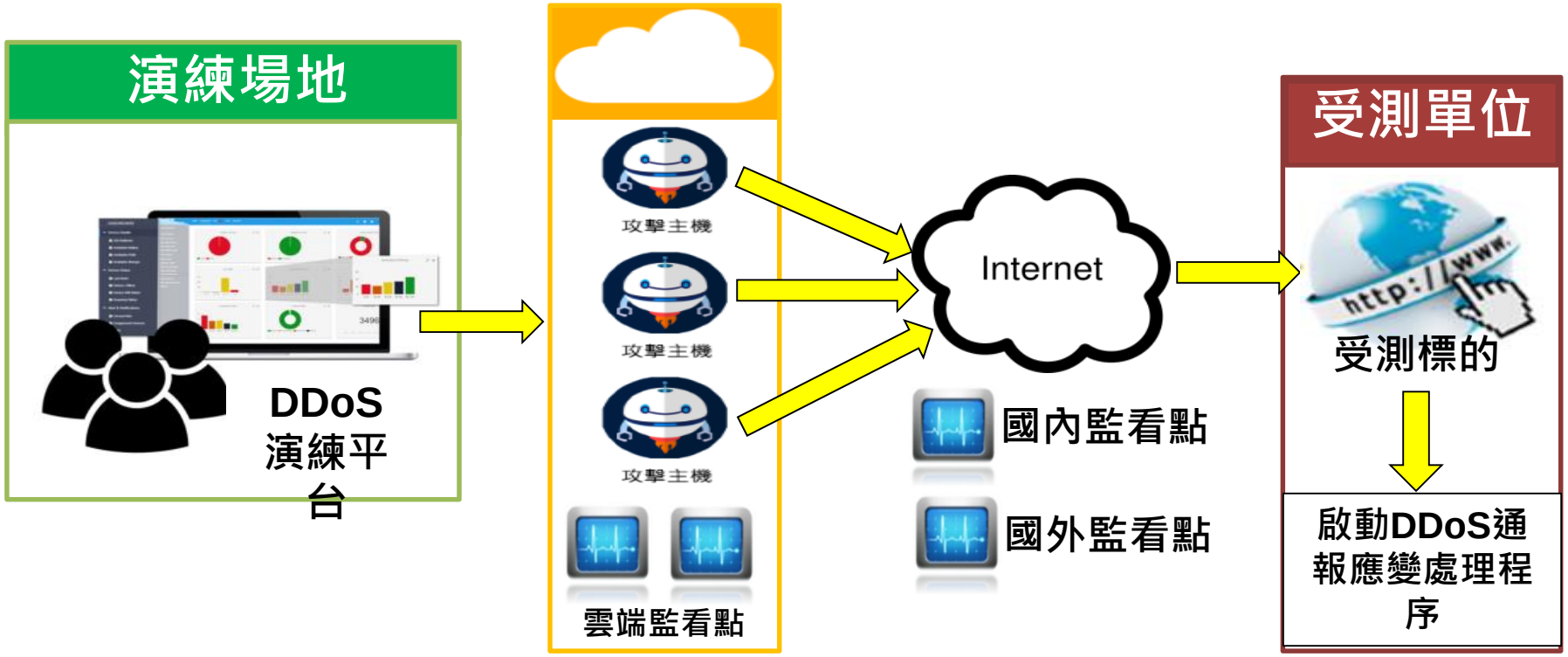
- 行政院自102年起每兩年舉辦一次跨國攻防演練，今(108)年首度以紅/藍軍實兵攻防對抗方式舉行。
- 以**金融服務為演練場域**，邀請藍軍2隊(14家銀行合組聯隊)，紅軍4隊(台灣2隊、國外2隊)參與為期3天演練，11月6日及7日為實兵演練，11月8日經驗分享。
- 於**11月7日向與會各國嘉賓及資安組織分享及介紹F-ISAC營運經驗**，並參與座談交流，提升我國金融領域資安能見度。



壹、營運成果

DDoS演練

邀請10家金融機構參與DDoS演練，驗證金融機構面對資安風險之應變程序、標準作業流程及金融領域資安聯防機制。



壹、營運成果

教育訓練

splunk> BOSS OF THE SOC

- 舉辦6梯次「Cyber Threat Hunting實作課程」，受訓人次約120人。
- 學員透過上機實作與分組競賽方式，學習Cyber Threat Hunting之方法理論與實作技術，讓會員得以運用與F-ISAC相同之情資分析方法，針對單位內外部情資進行統合分析，並與F-ISAC分享情資。

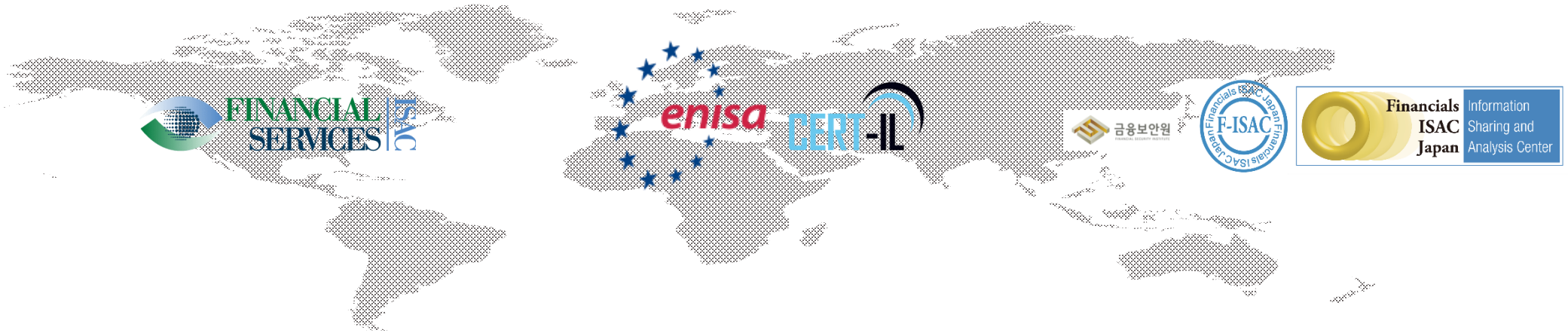
壹、營運成果

研討會

- 辦理**4場資安研討會**，約計**704人次**參與，並提供**線上直播服務**，平均在線觀看數約**35家**會員。
- 辦理**27次會員拜訪**，推廣**F-ISAC服務**、瞭解會員需求及鼓勵會員主動分享。

壹、營運成果

國際交流



- 美國FS-ISAC：107年4月取得試用會員資格，於108年成為FS-ISAC正式會員，得分享其TLP WHITE/GREEN/AMBER之情資，並參與2018、2019年FS-ISAC亞太區年會。
- 歐盟FI-ISAC：108年5月7日參加歐盟FI-ISAC會員會議，建立聯繫窗口，就雙方情資交換合作進行交流。
- 以色列CERT-IL： 108年5月25日參訪以色列網路安全局，並與FC3接洽及建立聯繫窗口，洽談雙方合作模式。
- 日本F-ISAC ：108年10月21日參與日本F-ISAC年會並簽署合作備忘錄，就雙方情資交換合作達成協議。
- N-ISAC ：108年12月2日參與N-ISAC年會，分享F-ISAC營運經驗，並邀請美國FS-ISAC、日本F-ISAC及泰國銀行電腦緊急應變中心(TB-CERT)假F-ISAC辦公室進行實質交流。
- 韓國 FSI ： 108年12月辦理合作備忘錄內容洽談作業。

壹、營運成果

F-CERT

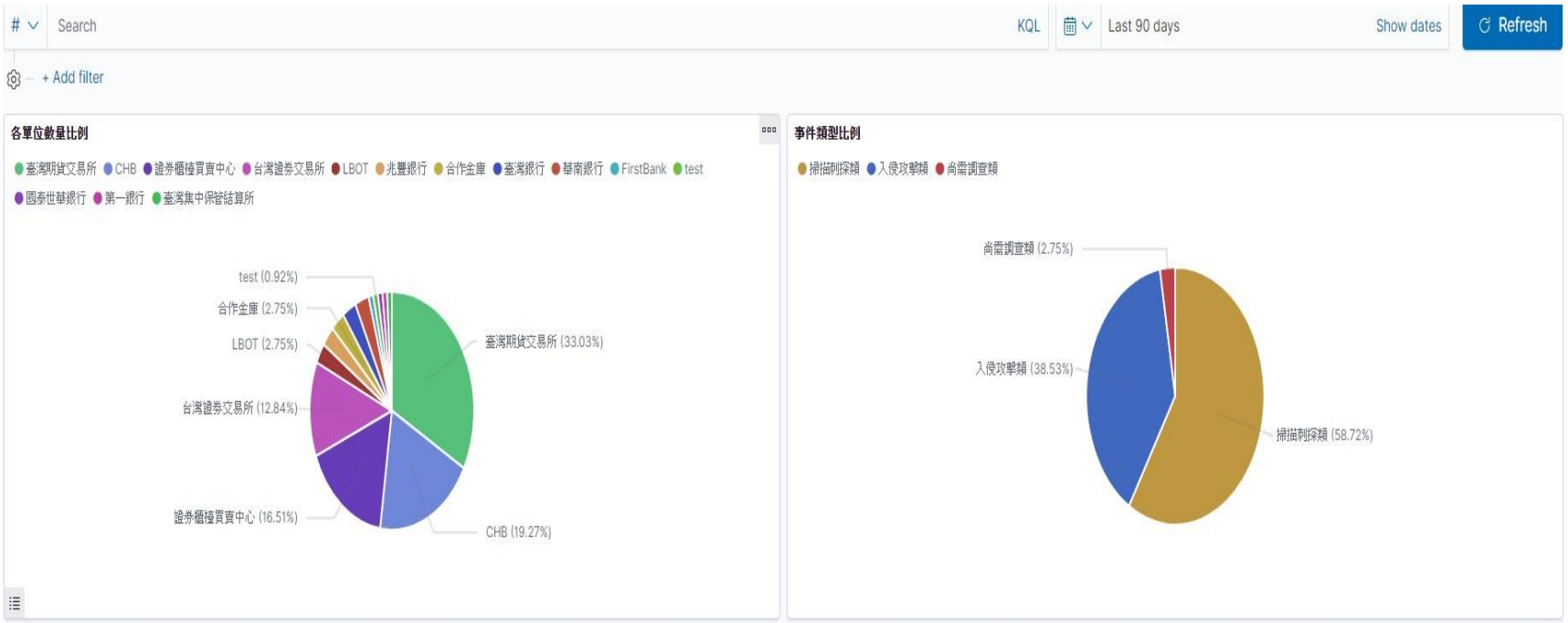
- F-CERT擔任金融領域第二線的應變協處，當金融機構第一線資安人員無法處理時，F-CERT偕同資安專業廠商提供所需支援服務，如：金融機構資安事件應變處理、事件調查及數位鑑識等。
- FCERT**舉辦資安攻防演練(如DDoS)**及**資安事件處理教育訓練**，協助提升金融機構驗證防護能量。
- F-CERT另與4家資安專業廠商簽署合作協議，提供金融機構「資安事件應變處理」服務。
  - 中華資安國際
  - 安碁資訊
  - 趨勢科技
  - 奧義智慧

工作項目	工作內容
SafeCove 資安事件監控及分析系統（2 個 Device 授權）	監控及分析2台資安設備之資安事件(365天)
Safecove AD 或是 DAM 監控及分析系統	監控及分析 AD 或是 DAM 設備之資安事件(365 天)
SafeCove 網頁安全弱點掃描作業 (2 URL)	執行網站弱點掃描之初掃、複掃作業(含報告)乙次
SafeCove 系統安全弱點掃描作業 (10 IP)	執行系統弱點掃描之初掃、複掃作業(含報告)乙次
Safecove 網路資安事件鑑識作業 (2 次)	執行網路資安事件調查分析之鑑識作業(含報告)二次
SafeCove 滲透測試作業 (2 URL)	執行網站滲透測試之初測、複測作業(含報告)乙次
SafeCove 網路架構及安全設定檢視作業	執行網路架構檢視、防火牆設定值檢視(含報告)乙次
Safecove 資安弱點管理-惡意程式檢測作業	執行標的物(伺服器、個人電腦)惡意程式檢測、分析作業(含報告)
SafeCove 行動裝置 APP 應用程式檢測作業 (含 iOS、Android)	執行 APP 應用程式檢測之初測、複測作業(含報告)乙次
SafeCove 資安日誌保存與稽核系統（2 個 Device 授權）	提供2個標的物資安日誌收集授權(365天)

壹、營運成果

F-SOC POC

邀請金融領域關鍵基礎設施（5)、公股行庫（8）及民營系統性銀行（3）等16家金融機構參與概念性驗證，規劃及建置金融相關機構F-SOC測試用途平台，研究分析回傳內容之可用性、關連性並評估F-SOC軟、硬體之營運規模。



貳、年度重點工作

強化會員互動及交流

持續透過**說明會、研討會、教育訓練或小規模的閉門情資分享會議**等，建立F-ISAC與會員資安人員間之信賴感，**讓F-ISAC成為金融資安人員充分交流的平台**。

項次	類別	會議(課程)名稱	頻率
1	說明會	F-SOC服務與資安治理成熟度評估	2梯次
2	研討會	會員資安防護技術研討會	2梯次
3	閉門會議	閉門情資分享會議	不定期召開
4	教育訓練	(1)駭客防護實作課程	4梯次
		(2)網路安全監控(SOC)分析師認證課程	2梯次

貳、年度重點工作

強化F-CERT運作

- **強化**F-CERT在處理資安事件之**角色與功能**，提供金融機構有感之服務。**偕同資安專業廠商協助金融機構**資安事件諮詢、應變處理、事件調查及協調專業人員執行鑑識等緊急事故通報及應變協處服務。

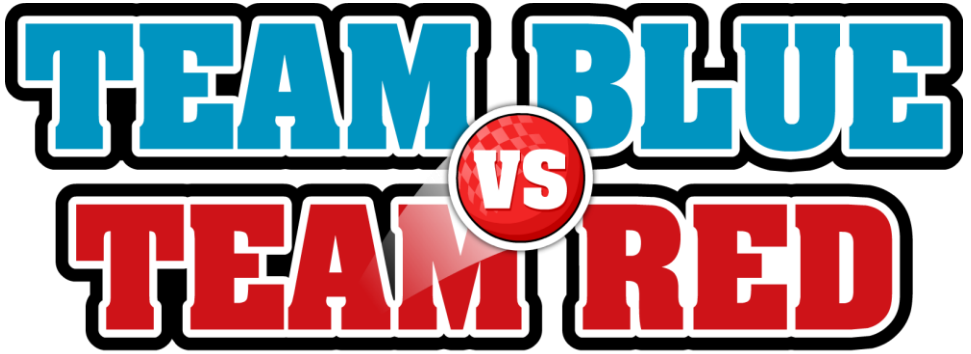
- F-CERT**洽談並支付資安專業廠商前述服務之基本費用**。倘若金融機構發生重大偶發資安事件，得向F-CERT申請前述服務基本人力(時數)，縮短恢復正常營運所需時間。

- 與國內資安應變組織(TWCERT/CC)協同合作，完善資安事件應處作為。

貳、年度重點工作

賡續辦理演練或舉辦競賽

協助金融機構驗證當面臨資安攻擊時，相關偵測與防護策略、人員專業技能、應變團隊組成、業務持續運作計畫、緊急應變程序等機制之有效性。F-CERT亦可依據演練結果提供金融機構資安防護改善建議，以精進金融機構資安防護作為。



- **辦理金融機構DDoS攻防演練(至少12家金融機構參與)**，演練攻防計畫於實施前1個月報鈞會核定，檢測金融機構系統服務之可用性防護能力，以及F-ISAC情資分享機制。
- **偕同資安專業廠商或團體辦理資安攻防競賽**，協助金融機構驗證其事件處理程序，擴大金融機構之電腦緊急事故人才培訓，組建跨金融機構之任務型資安應變團隊，培養金融領域資安專業人才。

貳、年度重點工作

促進交流及合作

促進與我國檢調單位、國內外資安組織及資安專業廠商交流合作，除強化資安應處能量，亦可提升國內金融機構資安防禦的專業技術，並藉由金融領域的資安防護市場，培植國內資安產業的發展。

- 配合行政院「國家資通安全發展方案」之規劃，與N-ISAC、N-CERT、N-SOC等單位交換與分享資安情資及事件通報，並辦理金融領域應辦事項。
- 參與國內外資安聯防活動或會議，促進資安情資交流與合作，強化資安應處能量。
- 配合專案推動需求，參加相關國際交流活動，規劃活動如下：
  - **ISAC：參加FS-ISAC亞太區高峰(年)會**。
  - **CERT：參加TWCERT/CC會員年會**。

貳、年度重點工作

建立金融資安監控中心

擬**建立金融資安監控中心**，並**邀請16家金融機構**執行回傳作業。

- **建立資料分析機制**，依據資安事件情資進行趨勢分析，並**分析會員資安事件間之關聯性**，可**即時向會員發布異常事件告警通知**，發揮資安聯防功能。
- **建立資安情資關聯機制**，蒐集綜整併分析跨金融關鍵基礎設施之事件資訊，交叉分析其遭受的資安威脅，了解各設施面對資安威脅的同異程度，可依據會員提交事件單內資訊，搜尋彙整相關資安威脅情資，提供會員評估利用。
- **彙整N-SOC情資及外部情資**，**關聯F-SOC收容之資安事件情資**，產製事件共通之攻擊手法、弱點及威脅等聯防情資，**並與N-SOC進行聯防**。

貳、年度重點工作

推動資安治理成熟度評估

為**有效評估國內金融機構資安治理成熟度現況**，俾各機構**掌握其所面臨之資安風險**，擬**建立可衡量之評估作業方法**，並**邀請十家金融機構**執行**試評**作業。

茲分述主要執行項目如下：

1. 規劃金融機構資安治理成熟度評估方法。
2. 確認資安治理成熟度評估框架。
3. 確認評估項目，再依國內金融機構特性進行客製化及中文化。
4. 完成國內金融資安治理成熟度評估作業方法。
5. 執行金融機構業務服務及資訊安全現況普查。
6. 選定成熟度試評項目及十家試評金融機構。
7. 針對試評會員辦理相關教育訓練。
8. 彙整及分析試評執行成果並產製報告。

Intelligence-Driven Defense

F-ISAC Taiwan

www.fisac.tw
service@fisac.tw
(02)2655-7077