

# 資通安全威脅偵測管理 (SOC)服務介紹



# 資通安全威脅偵測管理(SOC)服務

## ● 服務實績

- ◆ A級機關- 審計部、內政部資訊中心(外網)
- ◆ B級機關- 榮民總醫院新竹分院
- ◆ C級機關- 交通部鐵道局
- ◆ D級級關- 新北市立大觀國中
- ◆ 特殊非公務機關- 國家實驗研究院實驗動物中心
- ◆ 民間企業- 全國電子公司、凌羣電腦
- ◆ SOC系統維護- 台大醫院

## ● 解決方案- OPENTEXT ARCSIGHT SIEM

# 資通安全威脅偵測管理(SOC)服務

## 111 年共契資安服務廠商評鑑結果

序號	得標廠商	SOC 服務	資安健診	弱點檢測	滲透測試	社交工程演練	
1	三甲科技		B 級	A 級	A 級		100-
2	中芯數據		B 級	B 級	B 級		90-
3	中華資安	A 級	A 級	A 級	A 級	A 級	80-
4	白帽犀牛		B 級	B 級	B 級		70-
5	光盾資訊		B 級	B 級	B 級	B 級	60-
6	昕恩科技		B 級	B 級	B 級	B 級	0-
7	果核數位	B 級					
8	凌群電腦	B 級	B 級			B 級	
9	華電聯網			B 級	A 級		
10	漢昕科技	B 級	B 級	B 級	B 級	B 級	
11	精誠軟體		B 級				
12	網達先進		C 級		C 級		
13	德欣雲宇		B 級	B 級		B 級	
14	數聯資安	A 級	B 級	B 級	B 級	B 級	
15	關貿網路	B 級				B 級	
16	關鍵智慧			B 級	B 級		

( 依受評廠商名稱筆畫由少至多排序 )

# 資通安全威脅偵測管理(SOC)服務

## 國家資通安全研究院

### 聯防監控廠商連通測試通過名單

廠商名稱	聯絡方式	資通安全防護、目錄服務系統及核心資通系統
安碁資訊股份有限公司	地址：桃園縣龍潭鄉渴望園區 電話：0800-286009	通過 111/4/14
中華電信股份有限公司數據通信分公司	地址：台北市信義路一段 21 號數據通信大樓 電話：(02)2344-4639	通過 111/10/19
數聯資安股份有限公司	地址：台北市內湖區瑞光路 218 號 電話：(02)7721-1688	通過 111/9/19
關貿網路股份有限公司	地址：台北市南港區三重路 19-13 號 6 樓 電話：(02)2655-1188	通過 111/11/28
果核數位股份有限公司	地址：台北市內湖區瑞湖街 111 號 電話：(02)2658-2220	通過 111/7/29
漢昕科技股份有限公司	地址：台中市北屯區文心路三段 1023 號 電話：(04)2298-3968	通過 111/12/16
中華資安國際股份有限公司	地址：台北市中正區杭州南路一段 26 號 8 樓 電話：(02)2343-1628 #8	通過 111/11/12
凌群電腦股份有限公司	地址：台北市萬華區峨嵋街 115 號 7 樓 電話：(02)2343-1628 #8	通過 111/7/12
精誠科技整合股份有限公司	地址：台北市中正區台灣大道二段 660 號 0 樓之 1 電話：(04)2452-3928#301	通過 111/6/30
白帽犀牛有限公司	地址：高雄市鼓山區中華一路 352 號 11 樓 電話：0915516152	通過 111/11/28
捷睿智能股份有限公司	地址：新北市板橋區雙十路二段 79 號 8 樓之 1 電話：(02)2627-7996	通過 111/7/7
智慧資安科技股份有限公司	地址：臺北市內湖區瑞光路 318 號 電話：(02)8798-6088#5775	通過 111/5/13

更新日期：112 年 1 月 1 日

## 國家資通安全研究院

### EDR 連通測試通過名單(更新至 112.03.08)

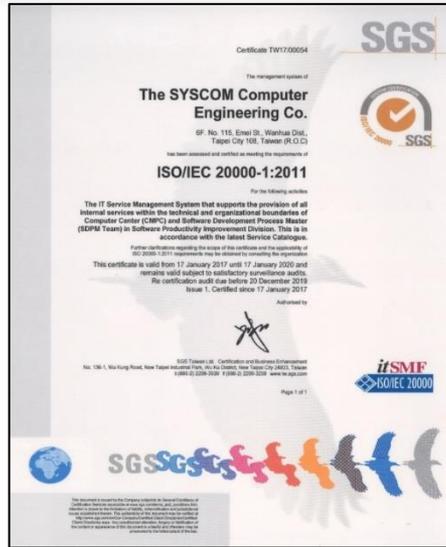
項次	通過連通測試之 SOC 廠商	該 SOC 進行連通測試時使用的 EDR 廠牌
1	智慧資安科技股份有限公司	智慧資安(uniXecure) Sophos
2	精誠科技整合股份有限公司	智慧資安(uniXecure)
3	凌群電腦股份有限公司	杜滿數位(TeamT5) 趨勢科技(TrendMicro) Fortinet Palo Alto Networks
4	數聯資安股份有限公司	杜滿數位(TeamT5) 中芯數據(CoreCloud) 趨勢科技(TrendMicro) 奧義智慧(CyCra) Carbon Black CrowdStrike
5	安碁資訊股份有限公司	Carbon Black

已完成T5、Forti、Paloalto、Trend Micro等四家EDR產品連通測試。

# 現有能量-資安相關認證



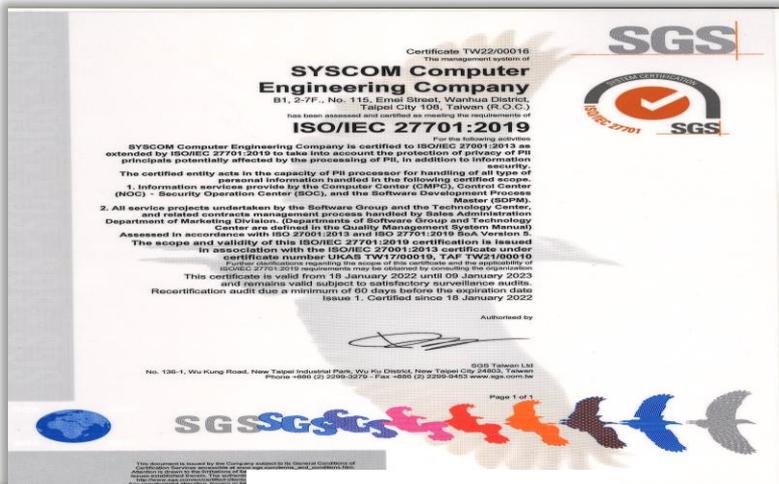
ISO27001:2013證書



ISO20000證書



BS 10012:2017證書



ISO27701證書



工業局能量登錄證書

# 資通安全威脅偵測管理(SOC)服務

監控部  
署建議

資安事  
件鑑識  
處理

威脅偵  
測與通  
報

預警情  
資蒐集  
與通報

# 資通安全威脅偵測管理(SOC)服務

監控部署建議：

- 客戶需求訪談(確認採購範圍)
- 監控網路環境與資安設備資訊收集
- 日誌收集器安裝
- 日誌收集與正規化
- 關聯規則與閾值調校
- 通報機制確認

# SOC服務-資安事件關聯規則偵測

ArcSight 控制台 7.6.0.14964.0 [esm01:admin.ast] Permanent license.

檔案 編輯 檢視 視窗 工具 系統 說明

導覽器 資源 套件 使用案例 規則 Ctrl+Alt+L

快捷徑

- 規則
- admin的規則
  - DEMO
    - YFN登入失敗
    - YFN登入成功
    - Windows登入失敗
    - Windows登入成功
    - 帳號提權事件
    - 建立新帳號
    - 收到可疑信件
    - 類似資料外洩
    - 駭客入侵事件
- 共用
  - 所有規則
    - ArcSight 基礎
    - ArcSight 管理
    - ArcSight 系統
    - ArcSight 解決方案
    - Personal
    - 下載
    - 停用
    - 啟用
  - 客戶
    - 全國電子
    - 共用
    - 凌群電腦公司
    - 實驗動物中心
  - 偵測
    - 觸發通報
  - 未指派

檢視器

觸發通報 關聯頻道 新增黑名單觀察三日 MISP 非技服黑名單連線 Kaspersky AWS\_WAF ELIFE\_WAF F-Secure 審計部 WAF

活動頻道: (16%)

開始時間: 12一月 2023 14:00:00 TST

結束時間: 19一月 2023 15:00:00 TST

過濾規則 (類型 = "Correlation" And 產生器名稱 StartsWith "通報")

內部過濾規則: 無過濾規則

雷達

管理員接收時間	結束時間	名稱	攻擊者位址	目
19一月 2023 14:18:52 TST	19一月 2023 06:17:36 TST	外部主機嘗試進行XSS攻擊V3	103.151.111.44	1
19一月 2023 14:06:14 TST	19一月 2023 14:04:56 TST	通報-IPS進入Bypass模式		1
19一月 2023 14:01:27 TST	19一月 2023 14:00:18 TST	黑名單連線(內對外)	10.10.10.108	1
19一月 2023 11:25:55 TST	19一月 2023 11:24:52 TST	黑名單連線(內對外)	10.0.3.42	1
19一月 2023 11:17:55 TST	19一月 2023 11:17:00 TST	黑名單連線(內對外)	192.168.20.14	1
19一月 2023 09:39:12 TST	19一月 2023 09:38:35 TST	通報-偵測到技服-DN-BK連線	10.1.152.220	1
19一月 2023 09:15:54 TST	19一月 2023 09:12:53 TST	通報-單一主機感染病毒(已刪除)-2023		1
19一月 2023 08:25:10 TST	19一月 2023 08:24:01 TST	黑名單連線(內對外)	10.27.63.127	1
19一月 2023 08:07:23 TST	19一月 2023 08:03:31 TST	通報-單一主機感染病毒(已刪除)-2023		1
19一月 2023 02:47:32 TST	19一月 2023 02:46:50 TST	黑名單連線(內對外)	192.168.54.2	1
19一月 2023 00:03:23 TST	19一月 2023 00:00:57 TST	通報-單一主機感染病毒(已刪除)-2023		1
18一月 2023 19:53:22 TST	18一月 2023 19:52:30 TST	通報-單一來源大量WAF事件	24.34.7.226	1

偵測及觸發通報關聯規則，透過ESM活動頻道即時監看觸發狀況

檢查/編輯

事件檢查器

詳細資料 評註 負載

事件檢查器

名稱	值
名稱	
事件	
名稱	
訊息	
類型	
結束時間	
應用程式通...	
傳輸通訊協定	
弱點資源	
接收位元組	
傳送位元組	
產生器資源	
客戶資源	
網域	
網域識別碼	
網域 URI	
網域外部識別碼	
網域資源	
網域名稱	
彙總的事件計數	
關聯事件計數	
類別	
類別意義	
類別行為	
類別技術	

搜尋:

# SOC服務-資安事件通報內容

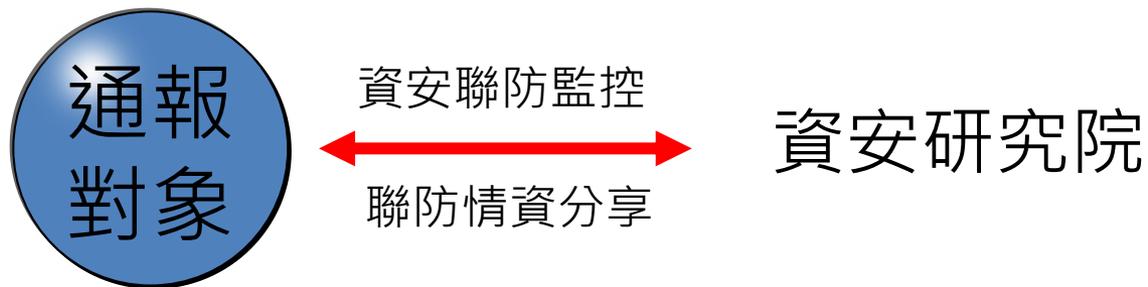
分類	事件行為
1. 違反安全政策之網路連線行為	1.1. 可能造成資料外洩或佔用鐵道局頻寬之連線行為 1.2. 不合法的來源IP、不合法的存取目的 1.3. 使用者的網路瀏覽行為，使用不合法的軟體連線或連線至高風險類別的網站
2. 不正常的網路連線行為	2.1. 短時間內被防火牆重複阻擋的連線 2.2. 短時間內大量對外或對內的允許連線，可能是蠕蟲爆發感染或木馬程式之連線行為 2.3. 行政院國家資通安全會報技服中心通報之惡意中繼站清單IP或是已知黑名單IP之連線行為 2.4. 個人主機之持續網路刺探掃描行為，疑似攻擊前兆，如Port_Scan、Port_Sweep等 2.5. 個人主機疑似遭到後門程式植入之連線行為 2.6. 不當的網路應用程式使用行為 2.7. 闖道端FTP、SMTP、HTTP、POP病毒等連線行為 2.8. 惡意程式連線行為及後門、穿隧程式
3. 蠕蟲擴散行為	3.1. 來源IP感染蠕蟲，正嘗試感染其他主機中
4. 感染病毒事件	4.1. 感染病毒事件
5. 內網異常網路行為	5.1. 伺服器間非正常的存取行為 5.2. 內部非法連線或Botnet運行軌跡 5.3. 非正常HTTP或HTTPS連線
6. 目錄伺服器異常行為	6.1. 單一來源IP帳號持續登入失敗 6.2. 帳號異動及非預期排程執行
7. 郵件收發異常行為	7.1. 多個IP使用同一帳號 7.2. 多個IP同時對特定目的端大量寄送信件
8. 其他	資安設備設定異動(防火牆)

資安事件通報單SOCC0000099				
單位名稱	資研電腦客戶部	事件等級	低	
標題	公用磁碟機 6B-RD6-SRV2 IP_172.16.200.207，遭入侵，Schelzer VPN 工具	事件分類	入侵或惡意事件	
事件編號	FBTC-DEV201900730	通報時間	2019-02-22 16:00	
處理方式	已通報	目的 IP	110.10.179.245	
通報內容	來源 IP	172.16.200.207	Web URL	
聯絡網址	6B-RD6-SRV2	事件說明	一、 20190222系統檢發現公司公用磁碟機 6B-RD6-SRV2 IP_172.16.200.207，遭入侵，Schelzer VPN 工具。 二、 經查，先於20180522日發現公司遭安裝Schelzer VPN 工具，係透過Google Chrome瀏覽器程式，連繫網頁api.adwords-google.com.tw，IP_110.10.179.245，該網頁於去年6月被DC09 遭入侵之IP_110.10.179.153的傳知相關。	
作業系統	WINDOWS	單位名稱	資研電腦客戶部	
業務負責人	CTAC	標題	--- 本公司MAIL_Servetion.ascom.com.tw 172.16.200.225遭向遭入侵「WEB Shell」一切跡不果。	
事件摘要	不會去連IP連線	事件編號	FBTC-DEV201900694	
事件說明	一、 本公司MAIL_Servetion.ascom.com.tw 172.16.200.225遭向遭入侵「WEB Shell」一切跡不果。 二、 經查，先於20180522日發現公司遭安裝Schelzer VPN 工具，係透過Google Chrome瀏覽器程式，連繫網頁api.adwords-google.com.tw，IP_110.10.179.245，該網頁於去年6月被DC09 遭入侵之IP_110.10.179.153的傳知相關。	處理時間	2019-02-13 16:00	
通報內容	來源 IP	172.16.200.232	目的 IP	172.16.200.225
聯絡網址	172.16.200.232	Web URL	https://mail.ascom.com.tw/home/web/mail/ver5.aspx	
作業系統	Microsoft Windows	事件說明	發現可疑的網路連線活動 --- 本公司MAIL_Servetion.ascom.com.tw 172.16.200.225遭向遭入侵「WEB Shell」一切跡不果。 二、 經查，先於20180522日發現公司遭安裝Schelzer VPN 工具，係透過Google Chrome瀏覽器程式，連繫網頁api.adwords-google.com.tw，IP_110.10.179.245，該網頁於去年6月被DC09 遭入侵之IP_110.10.179.153的傳知相關。	
業務負責人	張志豪	單位名稱	資研電腦客戶部	
事件摘要	發現可疑的網路連線活動	標題	--- 本公司MAIL_Servetion.ascom.com.tw 172.16.200.225遭向遭入侵「WEB Shell」一切跡不果。	
事件說明	一、 本公司MAIL_Servetion.ascom.com.tw 172.16.200.225遭向遭入侵「WEB Shell」一切跡不果。 二、 經查，先於20180522日發現公司遭安裝Schelzer VPN 工具，係透過Google Chrome瀏覽器程式，連繫網頁api.adwords-google.com.tw，IP_110.10.179.245，該網頁於去年6月被DC09 遭入侵之IP_110.10.179.153的傳知相關。	事件等級	低	
通報內容	來源 IP	192.168.99.101	事件分類	設備或服務異常
聯絡網址	192.168.99.101	標題	防火牆設定異動	
作業系統	SmartDashboard 7.0.0.2410.0	事件編號	RBTC-DEV201900722	
業務負責人	張志豪	處理方式	已通報	
事件摘要	設備設定異動	通報時間	2019-02-22 12:09:28	
事件說明	發現防火牆設備設定異動 來源：192.168.99.101 用戶名稱：admin 對象單位IP：192.168.99.119 進行設定異動			
單位名稱	資研電腦	事件編號	FBTC-DEV201900722	
標題	專門建立用以發售電腦 Trojan.Tinidebot.B 木馬程式訊息	處理方式	已通報	
事件分類	病毒或惡意事件	通報內容	事件主標 Trojan.Tinidebot.B !!! 使用駭客程式編譯，用於檢測 Trojan.Tinidebot.B 系列相關的威脅。 事件說明 Trojan.Tinidebot.B 是一種後門木馬，可以打開後門並可能在受感染的計算機上執行惡意活動。 1. 使用防火牆阻止從 Internet 到不信任的設備的所有傳入連接，對於傳入連接，您應拒絕所有傳入連接，並阻止所有需要從外界提供的服務。 2. 實施密碼策略，複雜的密碼應保存在受保護的計算機上並確保文件與密碼隔離，這有助於防止密碼受到攻擊時被盜取或攔截。 3. 確保計算機的程序利用戶使用或其所需的最低權限原則，當系統提示輸入 root 或 UAC 密碼時，請確保要求管理級別訪問的程序是合法程序。 4. 禁用自動播放以防止在網絡存儲設備上自動啟動可執行文件，並在不需要時關閉驅動器，如果不需要時關閉驅動器，則防止病毒利用時使用可移動式。 5. 如果不需要，請關閉文件共享，如果需要文件共享，請使用 ACL 和密碼保護來限制訪問，限制對共享文件夾的命名限制，確保不對必須共享的文件夾具有強密碼的用戶帳戶的訪問權限。 6. 關閉定期不信任的磁碟機，對於磁碟機，許多操作系統安裝不信任的磁碟機，這些磁碟機可能包含病毒，如果它們被發現，則防止病毒利用時使用可移動式。 7. 如果發現任何一個或多個磁碟機，請關閉磁碟機，如果發現磁碟機，則關閉磁碟機。 8. 始終保持最新的修補程序更新，尤其是在在載入公共服務及可連接的設備的計算機上，例如 HTTP、FTP、郵件和 DNS 服務。 9. 設置您的電子郵件服務以阻止或刪除包含常用於傳播威脅的文件附件的電子郵件，例如 vbs、bat、exe、pdf 和 azx 文件。 10. 快讀病毒感染的計算機，以阻止病毒進一步蔓延，執行分析並使用受信任的病毒掃描計算機。 11. 隨時更新您的防病毒引擎，除非他們斷掉他們。此外，除非已安裝進行病毒掃描，否則請勿執行 Internet 下載的軟件，如果無法從受感染源未掃描，則關閉受感染的網站即可導致感染。 12. 如果您無法更新您的防病毒引擎，則關閉磁碟機，如果您需要更新它，請確保您的防病毒引擎是最新的，以便您的磁碟機無法掃描，如果您無法更新防病毒引擎，請確保所有設備都設置為「未使用」需要對每個設備都執行病毒掃描，不要受感染或包含公共和私人的應用程序。 參考資料 <a href="http://www.symantec.com/blogs/computer/virus/2015-02/01-5-01010">http://www.symantec.com/blogs/computer/virus/2015-02/01-5-01010</a>	

# SOC服務-資安事件通報方式



# SOC服務-資安事件通報對象



單位承辦人  
機房維運人員

資訊(安)部門主管

陳先生 您好：

針對監控有效性部分，  
貴司 12 月份結果如下表格所示：

資安監控情資格式與回傳率	資安防護項目回傳率	網路攻防演練驗證	技服中心資安警訊驗證	機關通報資安事件驗證	資安監控情資內容正確性	有效情資回傳率
100.00%	100.00%	NA	NA	NA	100.00%	100.00%

NA 為期間未有相關之資安情資，  
以上資訊提供給貴司參考，  
如有任何問題歡迎提出。

# SOC服務-資安事件通報內容(客戶端)

您好，有新的資安事件通報單 SOC000010246 產生，煩請確認：

## 資安警訊通報單SOC000010246

單位名稱	凌群電腦	警訊分類	病毒/蠕蟲/木馬
警訊風險等級	低	通報時間	2023-03-19 23:44:34.24
標題	主機感染病毒(未刪除)		
警訊編號	SYSCO-VRS202310017		
處理方式	已通報		
日誌來源	APEXONE		
作業系統	Apex Central 2019		
業務負責人	CMPC		

## 通報內容

來源 IP	172.16.40.9	目的 IP	172.16.40.9
網際網路位址	172.16.40.9	Web URL	
摘要	單一主機感染病毒(未刪除)		
警訊說明	APEX偵測主機感染病毒(未刪除) IP : 172.16.40.9 設備名稱 : L5-275203-NB-01 病毒名稱 : Cryp_Xed-12 設備動作 : No action 第一動作 : No action 第二動作 : N/A 檔案路徑 : E:/Study Resources/eCRE - Reverse Engineer Professional 2022/[السيبرانيو لابنك] - شهادة لارسمو المقرر - الامتد الحكيو المهندسد - 2022/[@CyberBankSa] - eCRE - eLearnSecurity Course (REpV1) - 2022/[@CyberBankSa] - SECTION 2 - TECHNICAL PART/[@CyberBankSa] - 檔名 : UnPackMe_WinUpack0.39.exe		
建議處理措施	經檢測發現內部電腦(主機)受病毒感染(狀況如事件說明)，建議立即檢測該電腦(主機)受感染情況，以確認為單一事件。並將未刪除的感染檔案予以清除。		

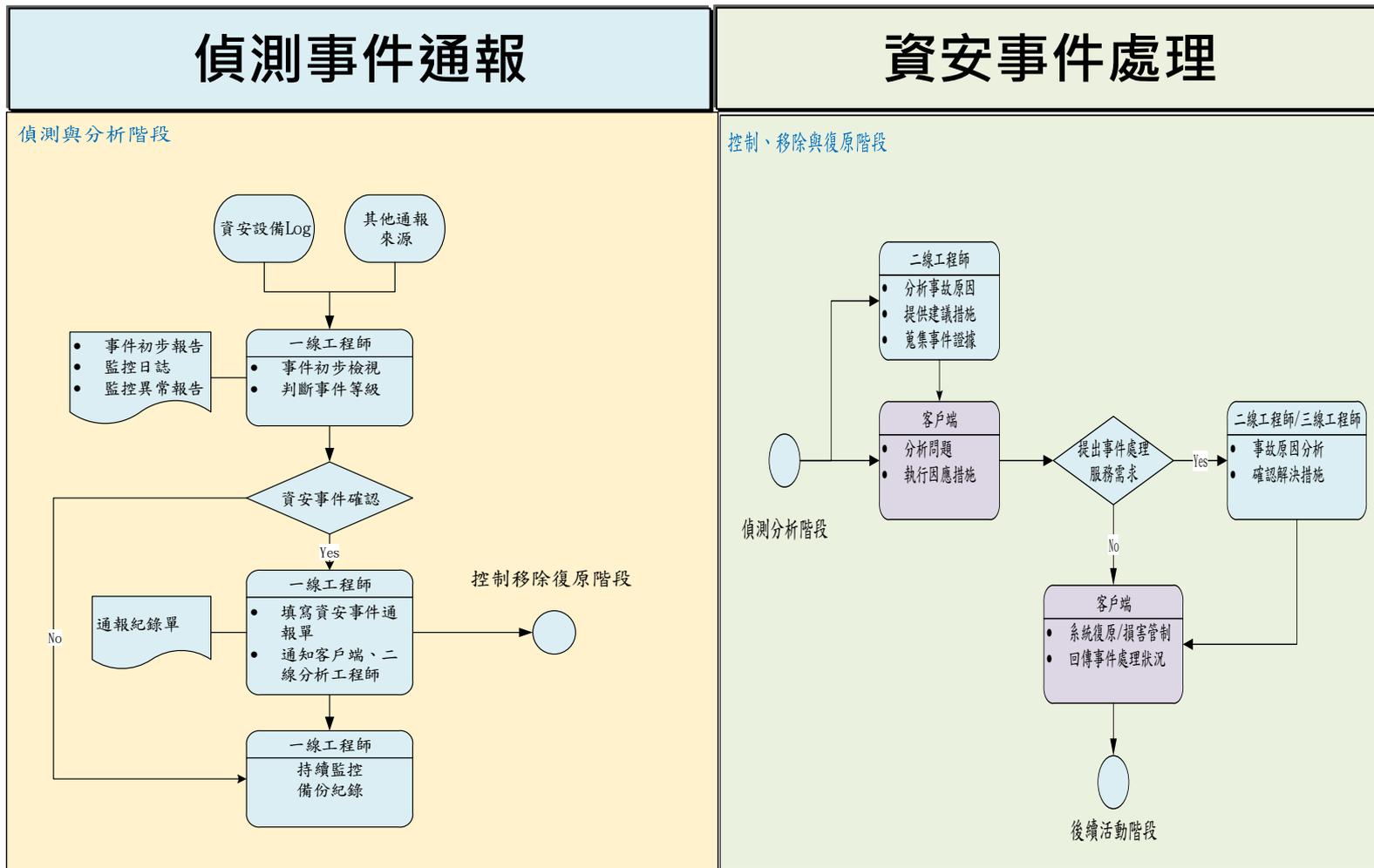
# SOC服務-通報資安事件追蹤管制

編號	日期	表單編號	標題	事件分類	風險等級	數量	處理情形回覆	追蹤處置狀況		
1	5月3日	SOC000010458	短時間大量WAF攻擊事件	入侵攻擊事件	低	2	進一步清查程式及資料庫，結果無異常	結案		
2		SOC000010459	訂購系統產出多筆錯誤資訊	系統服務類	低					
3	5月7日	SOC000010471	短時間大量WAF攻擊事件	入侵攻擊事件	低	4	已於5/8當天將來源IP：167.99.64.25封鎖	結案		
4		SOC000010473	短時間大量WAF攻擊事件	入侵攻擊事件	低					
5		SOC000010474	短時間大量WAF攻擊事件	入侵攻擊事件	低				已於5/8當天將來源IP：103.251.89.204封鎖	結案
6		SOC000010475	短時間大量WAF攻擊事件	入侵攻擊事件	低				已於5/8當天將來源IP：45.152.66.151封鎖	結案
7	5月8日	SOC000010476	短時間大量WAF攻擊事件	入侵攻擊事件	低	6	已於5/8當天將來源IP：167.99.64.25封鎖	結案		
8		SOC000010477	短時間大量WAF攻擊事件	入侵攻擊事件	低				已於5/8當天將來源IP：45.152.66.151封鎖	結案
9		SOC000010482	短時間大量WAF攻擊事件	入侵攻擊事件	低				已於5/8當天將來源IP：103.251.89.204封鎖	結案
10		SOC000010483	訂購系統產出多筆錯誤資訊	系統服務類	低				攻擊IP皆為103.251.89.204，建議封鎖此IP	結案
11		SOC000010484	訂購系統產出多筆錯誤資訊	系統服務類	低				攻擊IP皆為103.251.89.205，建議封鎖此IP	結案
12		SOC000010485	訂購系統產出多筆錯誤資訊	系統服務類	低				攻擊IP皆為103.251.89.205，建議封鎖此IP	結案
13	5月9日	SOC000010490	短時間大量WAF攻擊事件	入侵攻擊事件	低	2	已於5/9當天將來源IP：167.99.64.25封鎖	結案		
14		SOC000010491	短時間大量WAF攻擊事件	入侵攻擊事件	低					
15	5月10日	SOC000010530	AD帳號	系統服務類	低	1	已於5/10當天將來源IP：167.99.64.25封鎖	結案		
16	5月11日	SOC000010536	短時間大量WAF攻擊事件	入侵攻擊事件	低	1	已於5/11當天將來源IP：167.99.64.25封鎖	結案		
17	5月12日	SOC000010538	短時間大量WAF攻擊事件	入侵攻擊事件	低	2	已於5/12當天將來源IP：167.99.64.25封鎖	結案		
18		SOC000010540	短時間大量WAF攻擊事件	入侵攻擊事件	低					
19	5月14日	SOC000010541	短時間大量WAF攻擊事件	入侵攻擊事件	低	1	已於5/14當天將來源IP：167.99.64.25封鎖	結案		
20	5月15日	SOC000010544	短時間大量WAF攻擊事件	入侵攻擊事件	低	2	已於5/15當天將來源IP：167.99.64.25封鎖	結案		
21		SOC000010548	短時間大量WAF攻擊事件	入侵攻擊事件	低					
22		SOC000010559	短時間大量WAF攻擊事件	入侵攻擊事件	低	1	已於5/16當天將來源IP：20.214.205.72封鎖	結案		

所有通報案件由SOC中心一線人員逐案列管，每週定期追蹤各單位完成處理結案並於月報中提列未處理案件。

# SOC服務-資安事件處理

## SOC中心資安事件通報及處理流程



# SOC服務-資安事件處理

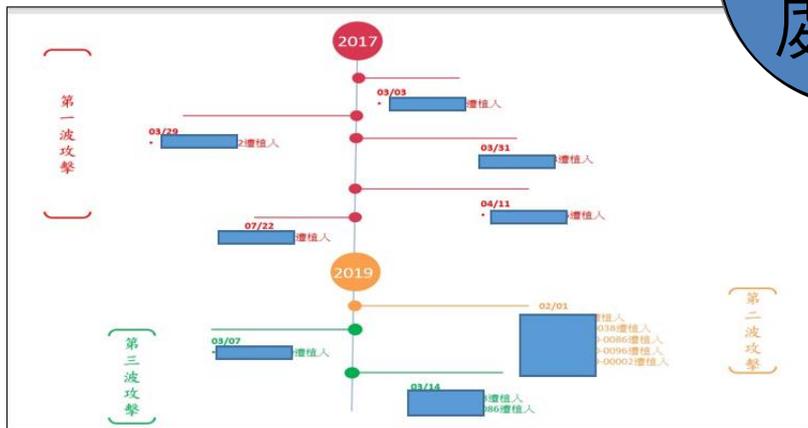


資安技術諮詢

id	version	id2	timestamp	ns5:Title	ns5:
example:Package-ecel096f-4138-4352-a18a-8eeac3e5cdd	1.2	example:incident-3a22c018-e2be-44cc-a1fd-66409596114d	2018-11-16T03:34:41.750565+00:00	事件主旨	事件
example:Package-ecel096f-4138-4352-a18a-8eeac3e5cdd	1.2	example:incident-3a22c018-e2be-44cc-a1fd-66409596114d	2018-11-16T03:34:41.750565+00:00	事件主旨	事件
example:Package-ecel096f-4138-4352-a18a-8eeac3e5cdd	1.2	example:incident-3a22c018-e2be-44cc-a1fd-66409596114d	2018-11-16T03:34:41.750565+00:00	事件主旨	事件
example:Package-ecel096f-4138-4352-a18a-8eeac3e5cdd	1.2	example:incident-3a22c018-e2be-44cc-a1fd-66409596114d	2018-11-16T03:34:41.750565+00:00	事件主旨	事件
example:Package-ecel096f-4138-4352-a18a-8eeac3e5cdd	1.2	example:incident-3a22c018-e2be-44cc-a1fd-66409596114d	2018-11-16T03:34:41.750565+00:00	事件主旨	事件

導出LOG協助分析

事件處理



資安事件處理

目標位址	目標連接埠	設備動作	目標城市	目標國家	連線起	訖
10.27.63.66	168.95.1.1	53 drop		Taiwan	20212 2019/12/23 上午 12:00:22	2019/12/29 上午 04:59:59
10.27.62.21	47.246.5.196	80 drop	San Mateo	United States	3031 2019/12/24 上午 12:00:09	2019/12/24 上午 04:59:43
10.27.63.120	118.214.244.152	443 drop		Singapore	2403 2019/12/23 上午 12:19:55	2019/12/29 上午 04:59:18
10.27.62.21	118.214.244.152	443 drop		Singapore	1966 2019/12/25 上午 12:00:37	2019/12/27 上午 04:59:30
10.27.54.31	119.161.16.11	443 drop		Korea, Republic of	1804 2019/12/24 上午 12:02:24	2019/12/29 上午 04:58:22
10.27.54.31	119.161.14.18	443 drop		Korea, Republic of	1804 2019/12/24 上午 12:02:45	2019/12/29 上午 04:58:01
10.27.54.31	119.161.16.12	443 drop		Korea, Republic of	1803 2019/12/24 上午 12:01:42	2019/12/29 上午 04:59:04
10.27.54.31	119.161.14.17	443 drop		Korea, Republic of	1803 2019/12/24 上午 12:02:03	2019/12/29 上午 04:58:43
10.27.64.41	172.217.27.142	443 drop	Mountain View	United States	1712 2019/12/24 上午 12:02:24	2019/12/26 上午 04:29:46
10.27.64.41	216.58.200.46	443 drop	Mountain View	United States	1442 2019/12/24 上午 12:01:04	2019/12/26 上午 04:59:53
10.27.64.41	172.217.160.78	443 drop	Mountain View	United States	1328 2019/12/24 上午 12:06:43	2019/12/29 上午 04:59:59
10.27.64.41	162.125.82.3	443 drop		Hong Kong	1209 2019/12/24 上午 12:13:06	2019/12/26 上午 04:59:54
10.27.64.41	172.217.160.110	443 drop	Mountain View	United States	1182 2019/12/24 上午 12:42:35	2019/12/26 上午 04:58:58
10.27.64.41	162.125.82.7	443 drop		Hong Kong	1110 2019/12/24 上午 12:23:30	2019/12/26 上午 04:58:59
10.27.63.66	216.58.200.234	443 drop	Mountain View	United States	1078 2019/12/23 上午 12:00:15	2019/12/28 上午 04:59:52
10.27.54.203	96.7.252.90	443 drop	Cambridge	United States	965 2019/12/23 上午 12:29:16	2019/12/29 上午 04:56:39
10.27.62.21	172.217.160.78	443 drop	Mountain View	United States	924 2019/12/25 上午 12:05:23	2019/12/29 上午 04:44:26
10.27.62.21	172.217.24.14	443 drop	Mountain View	United States	852 2019/12/25 上午 12:05:44	2019/12/29 上午 04:59:07
10.27.64.41	172.217.24.14	443 drop	Mountain View	United States	843 2019/12/24 上午 12:01:14	2019/12/26 上午 04:49:48
10.27.62.21	216.58.200.46	443 drop	Mountain View	United States	825 2019/12/25 上午 12:00:24	2019/12/28 上午 04:59:47

每週提供異常連線清單



# SOC服務-資安事件處理

姓名	角色	專業證照/訓練證明	經歷
周彥甫	專案負責人	CCNA(訓練)	網路戰大隊長
夏伯倫	三線經理	CCNA(訓練)、BS10012(證照)、ISO27701(訓練)	陸軍通校主任教官
朱盈豪	工程師	CEH(證照)	陸軍通校教官
王鼎琪	工程師	CTIAI(證照)、MCSE(訓練)、UHE(訓練)、MCDDBA(微軟認證資料庫管理專家)、TCSE(證照)、物聯網資安(訓練)、醫療資安專業技術(訓練)、CHFI(證照)	軍情局資圖中心主管、TWCERT-CC
陳建仁	SOC組長	CPMS、CEH、ISO27001、ISO20000、ISO27701(訓練)、SOC分析師(證照)	國防部作計室資安官、TWCERT-CC
曾火生	工程師	CCNA(訓練)、安全維運中心分析(訓練)、ISO27001(訓練)、SOC分析師(證照)	電展室

資安事件處理團隊由軍方退役具網路、資安、攻防演練等相關技術人員編組，資訊、資安從業經驗均超過20年以上，另公司與T5及鑒真數位等兩家公司簽訂MOU，可協助客戶進行資安鑑識服務。

# 資安威脅預警情資

項目	說明	網站
資安聯防情資	行政院資通安全處不定時提供之惡意中繼站清單、高危險惡意特徵情資及其他情資通報。	資安相關訊息公告 國家資通安全通報應變網站 <a href="https://www.ncert.nat.gov.tw/">https://www.ncert.nat.gov.tw/</a> 行政院國家資通安全會報技術中心 <a href="https://www.nccst.nat.gov.tw/">https://www.nccst.nat.gov.tw/</a>

# 資安威脅預警情資

項目	說明	網站
病毒資訊警訊	如趨勢科技、Symantec 等防毒廠商中級以上病毒警訊	<p><b>趨勢科技</b> <a href="http://www.trendmicro.tw/vinfo/tw/threat-encyclopedia/">http://www.trendmicro.tw/vinfo/tw/threat-encyclopedia/</a></p> <p><b>賽門鐵克</b> <a href="https://www.symantec.com/zh/tw/security-center/threats">https://www.symantec.com/zh/tw/security-center/threats</a></p> <p><b>Avira</b> <a href="https://www.avira.com/en/threats-landscape">https://www.avira.com/en/threats-landscape</a></p> <p><b>McAfee</b> <a href="https://www.mcafee.com/enterprise/zh-tw/threat-center.html">https://www.mcafee.com/enterprise/zh-tw/threat-center.html</a></p>

# 資安威脅預警情資

項目	說明	網站
系統弱點公告	如 ICST、Microsoft、SecurityFocus 及各國 CERT 等國內外資安組織公告。	<b>US-CERT</b> <a href="https://www.us-cert.gov/ncas">https://www.us-cert.gov/ncas</a> <b>微軟</b> <a href="https://docs.microsoft.com/zh-tw/security-updates/securityadvisories/securityadvisories">https://docs.microsoft.com/zh-tw/security-updates/securityadvisories/securityadvisories</a> <b>cve</b> <a href="https://cve.mitre.org/cve/search_cve_list.html">https://cve.mitre.org/cve/search_cve_list.html</a> <b>securityfocus</b> <a href="https://www.securityfocus.com/">https://www.securityfocus.com/</a>

# 資安威脅預警情資

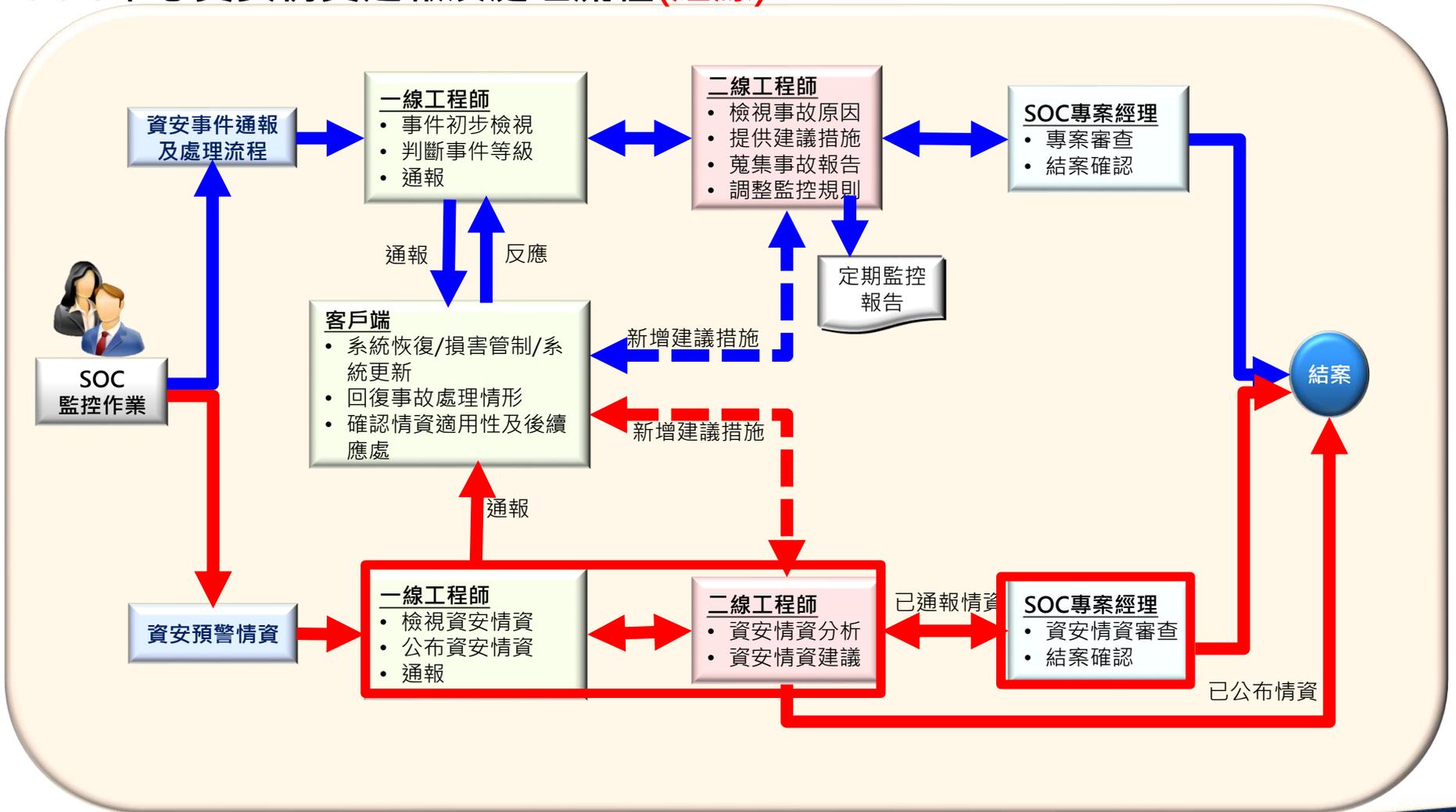
項目	說明	網站
新聞事件	如 CNN、Google 及 Yahoo 等資安新聞。	<p><b>IThome</b> <a href="https://www.ithome.com.tw/security">https://www.ithome.com.tw/security</a></p> <p><b>自由時報</b> <a href="http://news.ltn.com.tw/topic/%E8%B3%87%E5%AE%89">http://news.ltn.com.tw/topic/%E8%B3%87%E5%AE%89</a></p> <p><b>TechNews</b> <a href="http://technews.tw/category/internet/%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8">http://technews.tw/category/internet/%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8</a></p> <p><b>資安人</b> <a href="https://www.informationsecurity.com.tw/article/article_list.aspx?mod=2-1">https://www.informationsecurity.com.tw/article/article_list.aspx?mod=2-1</a></p> <p><b>infosecurity</b> <a href="https://www.infosecurity-magazine.com/news/">https://www.infosecurity-magazine.com/news/</a></p>

# 資安威脅預警情資

項目	說明	網站
網頁攻擊 資訊	如 Gartner 、OWASP 資 安組織公告等	<b>Gartner</b> <a href="https://www.gartner.com/en">https://www.gartner.com/en</a> <b>OWASP</b> <a href="https://www.owasp.org/index.php/Main_Page">https://www.owasp.org/index.php/Main_Page</a>
廠商發現 之威脅	如 Zero-Day 事件。	<b>Hitcon Zeroday</b> <a href="https://zeroday.hitcon.org/">https://zeroday.hitcon.org/</a> <b>中華資安國際</b> <a href="https://www.chtsecurity.com/">https://www.chtsecurity.com/</a> <b>數聯資安</b> <a href="http://www.issdu.com.tw/contact.html">http://www.issdu.com.tw/contact.html</a> <b>安碁</b> <a href="https://www.acercsi.com/">https://www.acercsi.com/</a>

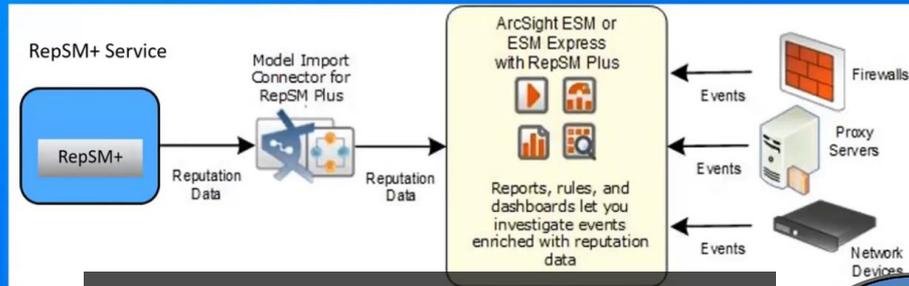
# SOC服務-資安情資分享方式

## SOC中心資安情資通報及處理流程(紅線)

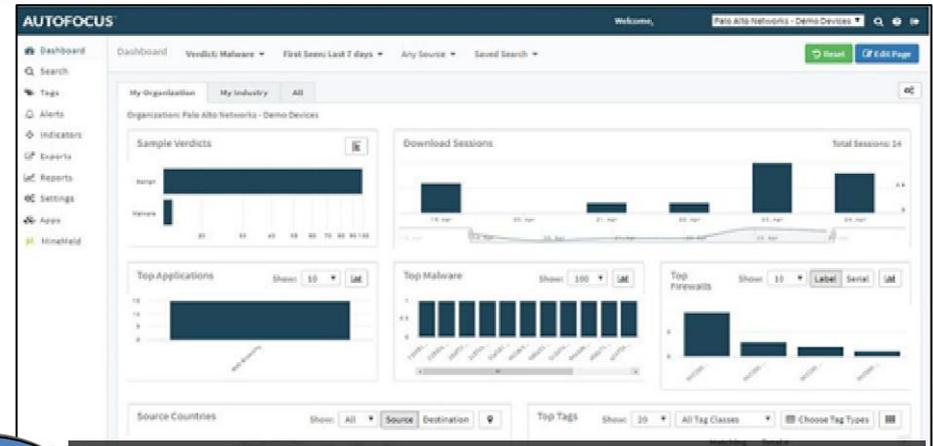


# SOC服務-資安情資分享方式

## RepSM+ Architecture



RepSM情資庫套件



PA-AUTOFOCUS情資庫

情資來源

項次	項目	說明
1	資安聯防情資	行政院資安處提供惡意中繼清單、惡意特徵情資通報
2	病毒資訊警訊	如趨勢科技、Symantec 等防毒廠商中級以上病毒警訊
3	系統弱點公告	如 ICST、Microsoft等國內外資安組織公告
4	新聞事件	如 CNN、Google等資安新聞
5	網頁攻擊資訊	如 Gartner 資安組織公告等
6	廠商發現之威脅	如 Zero-Day 事件

行政院資安處規範情蒐範圍



T5-ThreatSonar情資庫

# SOC服務-資安情資分享方式

## 網站分享

## 預警情報單



### 資安預警情報單EWA000000299

單位名稱	鐵道局
標題	藏有惡意程式之PDFReader，竊取使用者Facebook金融及廣告資訊
事件分類	病毒資訊警訊
事件編號	EWA-VIR-201900295
發布時間	2019-12-27 11:50
影響系統	Cookie

### 通報內容

事件主旨	近日發現有駭客透過含有惡意程式的PDFReader應用程式，竊取使用者Facebook Ads Manager以及Amazon的相關資訊，包含使用者的金融資訊、聯絡資訊、廣告發佈對象等，作為惡意行為之用。
事件說明	<p>1.資安團隊Malware Hunter Team發佈了一項資訊，指有駭客試圖透過惡意程式竊取使用者社群媒體的資料。首先，駭客製作了一款功能性高的PDF軟體「PDFReader」，並透過各種方式讓受害者連入該網站後下載安裝。然而，該軟體卻有木馬程式藏於其中，因此只要使用者進行安裝，該主機便會被木馬程式入侵，與駭客主機連線，接受駭客的指令和操縱。</p> <p>2.駭客在成功透過應用程式入侵後，會竊取使用者瀏覽器中Facebook的Cookie資料，並透過竊取到的使用者帳號密碼登入，觀察使用者使用Facebook中發佈廣告的Ads Manager系統的使用狀況。由於該系統主要為使用者付費以發佈相關廣告給特定群體，因此使用者便可透過該系統取得使用者付費時的信用卡資訊、金融資訊，以及發佈的對象、群體等，作為後續獲得不法利益之用。</p> <p>3.儘管在這件駭侵行為中，由於駭客開發之惡意PDFReader軟體除了功能強大且免付費之外，更因為該惡意程式具有合法的憑證，因此讓使用者得以信任並下載該軟體，但在經過針對該軟體之.exe檔案解析後，證實了其中的木馬程式，以及其竊取瀏覽器Cookie資訊等行為。然而，該駭侵行為在被發覺後，並未停止其攻擊行為，反而將其網站位址更動，以及將其程式進行版本之更新，企圖避過資安組織及檢測系統的偵測及阻擋，以進行更多的攻擊及獲取更多的資訊。</p>
建議處理措施	<ol style="list-style-type: none"> <li>勿隨意點擊下載或執行來源不明的檔案或軟體。</li> <li>使用防毒軟體進行定期性的掃描。</li> <li>進行作業系統或相關軟體的版本更新，並配合廠商修補相關的資安弱點。</li> </ol>
參考資料	<a href="https://www.twcert.org.tw/tw/cp-104-3191-7edbf-1.html">https://www.twcert.org.tw/tw/cp-104-3191-7edbf-1.html</a>

# SOC服務-資安情資分享方式

## 【目錄】

壹、摘要說明.....	4
貳、本月份重大資安漏洞(TLP-White).....	5
一、漏洞資訊介紹.....	5
二、漏洞探勘技術.....	5
三、影響範圍.....	15
四、修補建議.....	15
參、本月份重要資安攻擊事件(TLP-White).....	16
一、攻擊事件說明.....	16

凌羣電腦  
112年6月份  
資安威脅

- ◎ 當月重大資安漏洞資訊介紹、漏洞技術探勘、影響範圍與修補建議。
- ◎ 當月重要資安攻擊事件，攻擊手法、IOC及防護建議。
- ◎ 監控資安事件攻擊態樣(含攻擊手法、惡意程式樣本分析)、IOC及防護建議。
- ◎ 每半年提供資安威脅趨勢分析。

# SOC服務-服務報告

表 1、防毒軟體偵測病毒及事件次數統計表

時間	目標位址	目標主機	病毒名稱	動作	檔案名稱	偵測次數
2019/11/25	10 [redacted]	AS [redacted]	TrojanSpy. Win32. EMOTET.SMD2.hp	Upload unsuccessful	fxdpp255dwpcl6161010wxpcizz.exe	1
2019/11/26	10 [redacted]	MS [redacted]	TROJ_GEN. US EFB25	Upload unsuccessful	ikudian_Leeeloo_s_Talent_Agency.rar	1
備註	1. 11/1-11/30 偵測到病毒類事件計 71 筆，其中未清除計 2 筆。 2. 建請 [redacted] 針對上述主機與檔案進行處理。					

表 2、防毒軟體偵測間諜軟體事件統計表

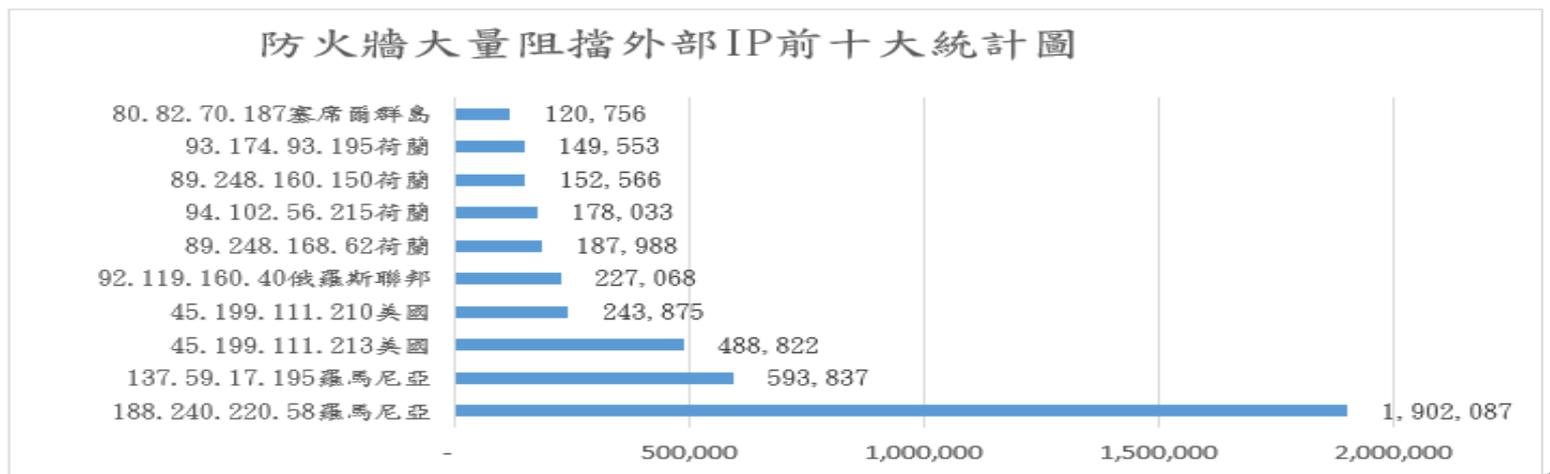
項次	間諜軟體名稱	感染主機	偵測次數
一	HackTool. VBS. InviBat. A	ACEE [redacted] ACEE [redacted] ASUS [redacted] DESH [redacted] DESH [redacted] HP60 [redacted] IPR2 [redacted] IPR3 [redacted] IPR3 [redacted] 0035 [redacted]	30

# SOC服務-服務報告

表 3、防火牆大量阻擋外部 IP 前十大統計表

項次	外部 IP	數量	來源地
1	188.240.220.58	1,902,087	羅馬尼亞
2	137.59.17.195	593,837	香港
3	45.199.111.213	488,822	美國
4	45.199.111.210	243,875	美國
5	92.119.160.40	227,068	俄羅斯聯邦
6	89.248.168.62	187,988	荷蘭
7	94.102.56.215	178,033	荷蘭
8	89.248.160.150	152,566	荷蘭
9	93.174.93.195	149,553	荷蘭
10	80.82.70.187	120,756	塞席爾群島

防火牆大量阻擋外部IP前十大統計圖



# SOC服務-服務報告

表 5、入侵防禦事件前十大統計

項次	事件類別名稱	設備動作/次數			
		alert	drop	Reset-both	sinkhole
1	SIPVicious Scanner Detection(54482)		88,128		
2	RPC Portmapper DUMP Request Detected(32796)		7,759		
3	HTTP SQL Injection Attempt(30514)	4,753			
4	HTTP SQL Injection Attempt(35827)	4,464			
5	HTTP Cross Site Scripting Attempt(32658)		1,903		
6	SMB: User Password Brute Force Attempt(40004)		864		
7	Windows Dynamic Link Library (DLL)(52019)	656			
8	PHP DIESCAN Information Disclosure Vulnerability(55834)		433		
9	Windows Mail UNC Navigation Request Code Execution Vulnerability(30224)		372		
10	HTTP SQL Injection Attempt(54608)	268			

# SOC服務-服務報告

參、執行建議：↵

(一)資安威脅預警建議：↵

11 月份預警情報單計 4 件，處置建議均已即時放在資安監控入口服務網站供 [ ] 查詢。↵

(二)資安威脅預警諮詢：↵

本月份接獲 [ ] 詢問有關病毒碼資訊計 1 件，建議 [ ] 可運用電話或電子郵件，針對資安威脅預警情資需處置建議提出諮詢，本司會派遣專業人員提供諮詢服務，此項諮詢亦可透過每月定期會議進行討論。↵

(三)資安監控防護建議(評估建議改善項目)：↵

1. SQL Injection 攻擊防護↵

本月 11 月 4 日凌晨發現「外部主機多次嘗試 SQL Injection 攻擊」事件，攻擊來源為新加坡，累積一小時超過 50 次；經持續監控，觀察到針對貴局 SQL Injection 短期大量攻擊有明顯增加之趨勢(較上月增加約 4,000 筆)，將納入持續監控重點，如短時間持續發生大量攻擊事件，將提高風險等級，並立即通報 [ ] 處理。↵

簡報完畢  
恭請指導