固若金湯 - 為何資料仍舊遭竊？

（eDetector 調查案例說明)

2017 July

鑒真數位 有限公司

黃敬博 資深鑑識顧問

service@iforensics.com.tw

www.iforensics.com.tw

簡報摘要

- 資料外洩主要管道及調查
- 從資料外洩案例談資安管理機制常見漏洞
- 資安管理與Log儲存機制建議
- 如何發現問題並解決(eDetector Demo)
- 資安鑑識服務說明

資料外洩主要管道說明

駭侵事件調查

	外洩管道	說　　明
1.	伺服器端遭駭客入侵將資料外洩	任何對外之伺服器均有可能遭駭客入侵，目標可能是應用程式、掛載之服務或作業系統之漏洞遭利用或設定疏忽所造成。
2.	擁有權限之使用者端電腦遭惡意程式感染或駭客入侵	擁有權限可存取敏感性資料之使用者端電腦遭感染或駭客入侵，導致敏感性資料遭外洩
3.	內部人員蓄意將資料外洩	為內賊利用各種管道蓄意將資料外洩

資安防護策略 / 資安緊急應變 / 數位鑑識 之關連

稽核及演練可定期進行
此步驟必需先做好!!

事件通報/各程序處理紀錄

緊急事件發生時

事先預防 → 事前證據保留 → 資安緊急應變 / 證據蒐證 → 數位鑑識分析 → 鑑識結果呈現

事先防範機制

- 採用EndPoint Agent
- 採用IDS/IPS/Firewall/NAC系統
- 採用側錄系統
- EnCrypt 保護
- CCTV 監控系統
- 門禁管制
- 可攜式設備管理
- 導入SOC

產品

- EndPoint Monitoring (EnCase ,FTK .. Agents)
- IDS/IPS/DLP/NAS
- Content Filter
- Encrypt and Authentication
- Access Control
- CCTV Monitoring
- Security Auditing

事前數位證據保留

- 使用紀錄、軌跡資料及證據保存
- 資料安全稽核機制
- 網路內容暨流量日誌
- 各種資料存取稽核Log
- 伺服器、應用程式、資料庫、網路設備、門禁日誌保存
- 人員異動主機硬碟封存
- 智慧手持裝置等軟硬體
- CCTV錄影內容

產品

- 日誌伺服器
- 大容量儲存設備
- Log 不可否認性摘要簽

事件發生時

- 系統回復營運
- 現場拍照/錄影及作業SOP
- 各種貯存裝置蒐證
- Email蒐證
- 網路蒐證
- 日誌蒐證
- Cloud Collection
- 手機及各式手持式蒐證
- 主機及伺服器蒐證

產品

- 各種數位證據封存不可否認性封存作業SOP
- SmartPhone Extraction module
- Memory Dump Tool
- FTK Imager
- 手持式硬碟複製機
- LiveSearch Tool
- Data Recovery Tool

舉證及分析究責原因

- Memory Analysis
- Process Analysis
- Registry Analysis
- HD Data Analysis
- Log Analysis
- Handset device Analysis
- Cloud Analysis

產品

- 機架型伺服器
- LogIndexing(Splunk)
- EnCase/FTK
- AccessData Insight
- VFC3/HBGary
- Netwitness
- Log Analysis

鑑識結果

- 調整SOC資訊安全事件標準作業流程
- 事件分類與分級
- 服務水準協議(SLA)

產品

- 文件處理軟體
- 各系統輸出資訊整合
- 數位證據擷取

資安緊急事件處理與資安鑑識之關係

- 資安緊急事件處理著重於當下的適當處置及系統的回復
- 資安鑑識著重於數位證據的保全及事情真相原因的調查

兩者並不衝突，可以同一組處理團隊來進行現場的處置，會有衝突主要在於事前的規劃不完備

共同必要:

- 忠實記錄工具及狀況
- 人員有事前的完備訓練及演練

駭客入侵或惡意程式感染之主要管道

一.人為的疏失造成:

a.設定或管理疏失

b.下載及執行被偽裝的程式或檔案

二.駭客入侵：

a.大多利用系統漏洞或設定疏失

作業系統漏洞 / 服務漏洞(Ftp,Http,Dns,Mail / 網站漏洞/應用軟體漏洞...等路徑)

b.若漏洞被駭客發現早於系統修補時間:

零時差攻擊

無法主動防禦，只能靠被動偵測

Signature Based Malware Detection is Dead

February 2017

ICIT 最新研究
現有的資安防禦普遍無法偵測！！

Author
James Scott, Sr. Fellow, ICIT

Figure 2 displays a Fully Un-detectable (FUD) Remote Access Trojan (RAT) sold on Hansa Market. Buyers look for the FUD keyword because it signifies that the malware will not be detected by signature or behavior based anti-malware applications.

從資料外洩案例談資安管理機制常見漏洞

案例一說明:電商公司遭駭客入侵並外洩交易個資給詐騙集團

一. 某日電商客服遭投訴，交易不久後即有詐騙集團來電進行相關詐騙

二.檢查Log未發現任何異常

請求鑑識是如何流出? 何人所為? 駭客入侵手法?

使用 eDetector 快篩分析掃描130多台電腦，發現有近30台遭惡意程式感染但未被公司防毒軟體所查覺-進一步確認主要遭感染為電話通訊主機及確認手法!!

本案主要資安管理問題及改善之建議:

1. 內部防禦完善，但主要疏忽了一台對外的電話主機(没有在防護範圍內)
2. 此台主機是委外管理：

   委外管理不當導致維護安裝時，即已安裝未驗證之軟體而有後門之惡意程式(但未觸發)
3. 電話主機Windows系統過舊，被駭客發現此後門而觸發執行

案例二說明:公司帳務及客戶系統資料遭勒索病毒加密

一. 某跨國貿易公司之重要帳務及客戶系統遭勒索病毒加密，但未能找出原因？

二. 持續資安攻擊將造成大量損失及公司營運威脅

內部無人下載觸發勒索病毒，請求找出感染源頭?
駭客入侵手法? 改善方式?

使用 eDetector 快篩掃描40多台電腦並委鑑伺服器一台，找出攻擊手法並建議如何防堵!!

發現之問題及改善之建議:

1. 防火牆設定不當，遠端登入協定並無限制Source IP
2. MIS為管理方便，設定可允許遠端登入，但密碼設定太簡單，駭客經由不斷的嘗試之後總算破入，由此植入勒索病毒
3. 防火牆設定不當，重要客服帳管伺服器沒有放在DMZ 區，導致入侵成功後可直接存取並加密資料

案例三說明:某知名電玩公司遭投訴玩家購買虛擬寶物後資料遭竊

一. 某日電玩客服遭投訴，許多玩家購買虛擬寶物，即有詐騙集團來電進行相關詐騙。

二. 此電玩公司所有伺服器均租用電信機房雲端伺服器群，查交易紀錄未發現任何異常

請求鑑識是如何流出? 何人所為? 駭客入侵手法?

使用 eDetector 快篩分析掃描50多台電腦，進一步確認主要並非駭客所為而是內賊外洩!!

發現之問題及改善之建議:

1. 發現主要維護關鍵系統的帳戶共用一組帳密,導致此內賊片面得知後即可登入
2. 此萬用帳戶為root權限，因此可刪除自已的相關登入痕跡，因此關鍵時段無發現任何Log
3. 利用快篩分析使用者端電腦發現可疑痕跡後，進行全硬碟鑑識才確認內賊所為

資安管理與Log儲存機制建議

Log 基本要素 及 稽核管理重點

基本要素:

- 必需要有時間(Time Stamp) =>必需對時
- 必需要有ID (對應出來源: IP/User Name/User ID/ Program Name/Machine Name...)
- 必需要有事件描述（能反應事實）

管理重點:

- 避免遭竄改 (異地備援及不可否認)
- 留存多久 (太短將無意義)
- 異常能否查覺

資安管理需注意之問題

檢視所有對外主機:

- 是否有對外伺服器疏忽？(CCTV/測試機...)
- 重要伺服器均放置DMZ → 設定允許協定及方向
- 帳密管理
- Log 稽核(常發現Log不全或無法反應事實...)

如何發現問題並解決

資安健診、快篩分析及鑑識服務 之服務差異及順序說明

資安健診：適用於未出事前之預防性服務（主要在於事先偵測可疑之惡意程式及資安漏洞問題）

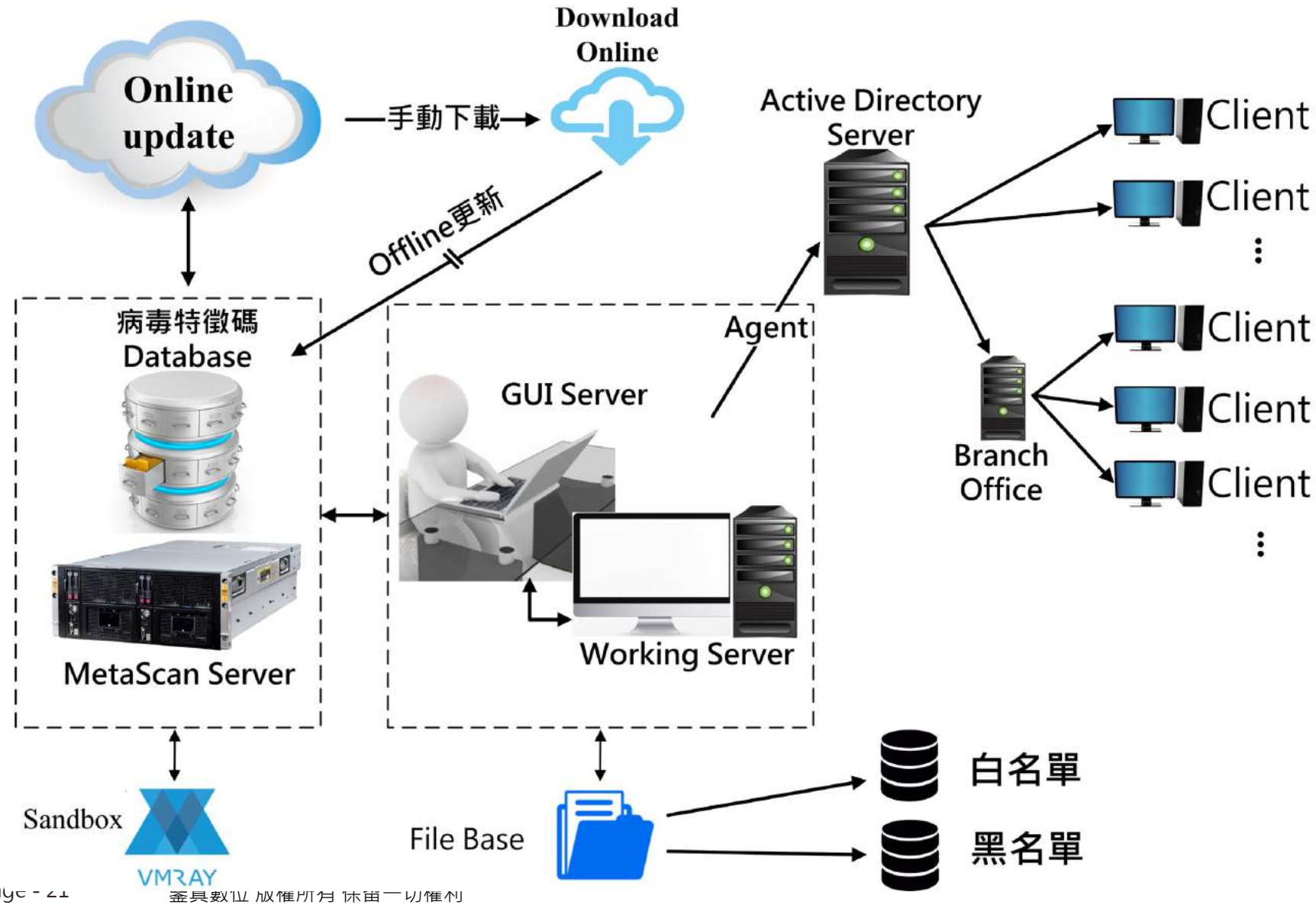
資安快篩分析：主要用於已確定遭遇資安事件，但不清楚感染範圍及主要遭感染之程式及主機

資安鑑識服務：清楚目標並依委鑑目標進行完整鑑識分析

資安健診：使用eDetector找出三類型之惡意程式

- 未知型惡意程式
  - APT攻擊、零時差攻擊、新型態...等
- 已知型惡意程式
  - 文件檔案型、執行程式型、 Kernel/Driver RootKit、系統啟動區...等
- 駭客工具
  - 各種打包、傳檔、加密、搜尋、破壞...等

eDetector 大規模偵測及快篩蒐證分析 示意圖



一般防毒軟體無法偵測惡意程式: 新技術多由記憶體 進行

對外連線

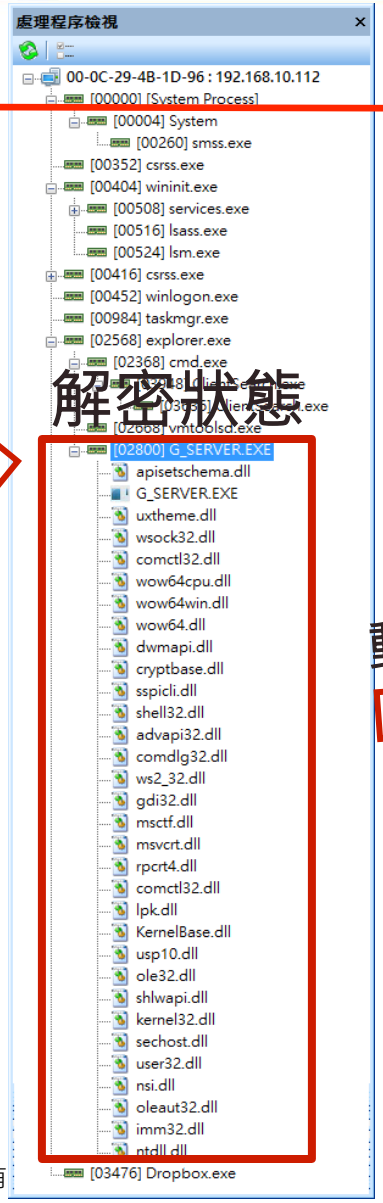
63.128.9.23 上海

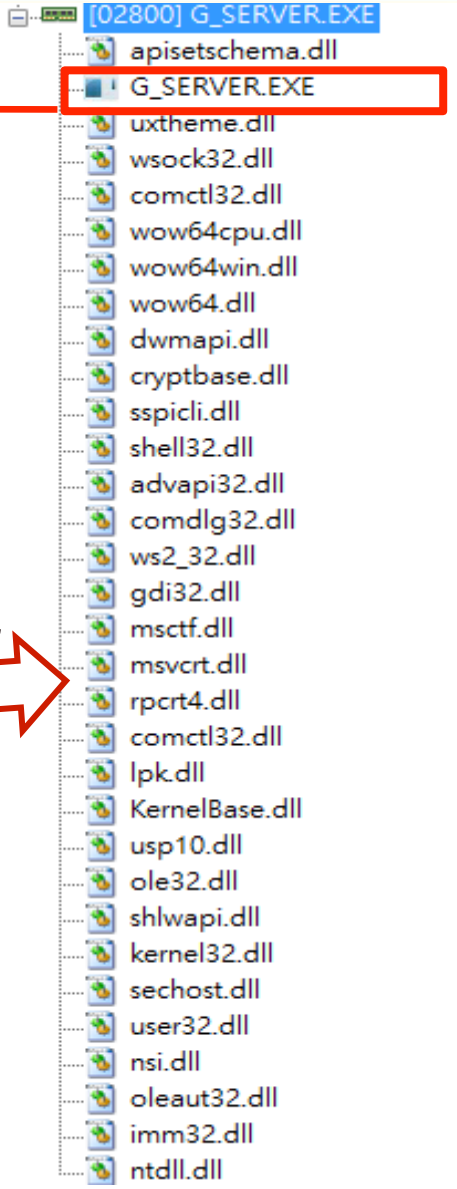
Virus exe

加密狀態

解密狀態

動態注入惡意程式

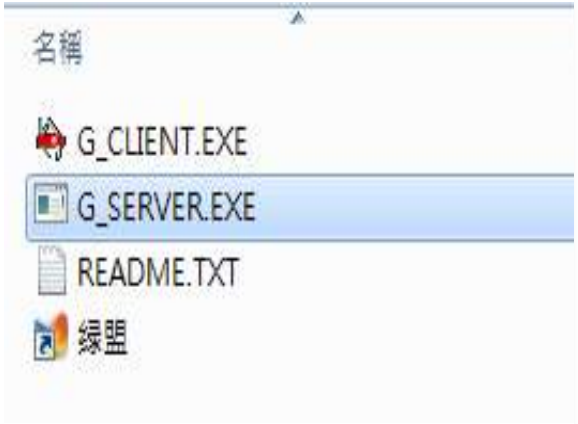




eDetector 特色: 記憶體程式及函式 惡意行為掃描

■記憶體掃描

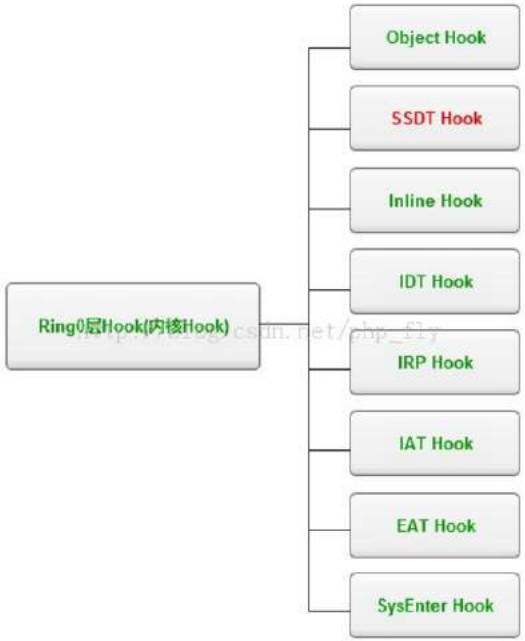
第一級:掃描程式本體



第二級:掃描所有程式動態載入函式庫

名稱	修改日期	類型	大小
advapi32.dll	2016/9/20 下午 0...	應用程式擴充	640 KB
apisetschema.dll	2016/9/20 下午 0...	應用程式擴充	4 KB
comctl32.dll	2016/9/20 下午 0...	應用程式擴充	528 KB
comdlg32.dll	2016/9/20 下午 0...	應用程式擴充	492 KB
cryptbase.dll	2016/9/20 下午 0...	應用程式擴充	48 KB
dwmapi.dll	2016/9/20 下午 0...	應用程式擴充	76 KB
G_SERVER.EXE	2016/		
gdi32.dll	2016/		
imm32.dll	2016/		
kernel32.dll	2016/		
KernelBase.dll	2016/		
lpk.dll	2016/		
msctf.dll	2016/		
msvcrt.dll	2016/		
nsi.dll	2016/		
ntdll.dll	2016/		
ole32.dll	2016/		
oleaut32.dll	2016/		
rpcrt4.dll	2016/		
sechost.dll	2016/		
shell32.dll	2016/		
shlwapi.dll	2016/		
sspicli.dll	2016/		
user32.dll	2016/		
usp10.dll	2016/		
uxtheme.dll	2016/		
wow64.dll	2016/		
wow64cpu.dll	2016/9/20 下午 0...	應用程式擴充	32 KB
wow64win.dll	2016/9/20 下午 0...	應用程式擴充	368 KB
ws2_32.dll	2016/9/20 下午 0...	應用程式擴充	212 KB
wsock32.dll	2016/9/20 下午 0...	應用程式擴充	28 KB

找出惡意 Hook 或注入行為



整合OPSWAT MetaDefender 各種偵測新技術

What is Metadefender Data Sanitization?

One of Three Distinct Technologies in Metadefender

SIGNATURES & HEURISTICS

Signature and heuristic scanning with 30+ embedded anti-malware engines

AhnLab, ESET, SOPHOS, McAfee, Symantec, Bitdefender, Avira, nProtect, AVG, Emsisoft, NANO, KASPERSKY, LAVASOFT, TREND MICRO, IKARUS, Zillya!, TOTAL DEFENSE, K7, Quick Heal

DATA SANITIZATION

Removal of potentially harmful macros and scripts with 90+ data sanitization engines

VULNERABILITY ENGINE

The Vulnerability Engine supports over a million binaries and 15,000 applications with support for version checks and reported known vulnerabilities

Adobe, Java, Microsoft Office Word, Microsoft Excel, skype

and many more....

資安健診或快篩以不影響單位之日常運作為原則

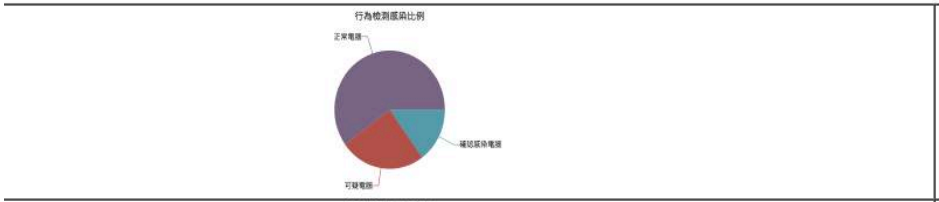
- 資安健診或快篩重點在於事前之預防及可疑目標之確認，主要之執行將以最小打擾方式，可不影響單位之日常運作
- 使用鑒真數位自行研發之動態記憶體偵測分析工具，可於隱藏輕量模式下執行，使用者工作不受影響且未能查覺。

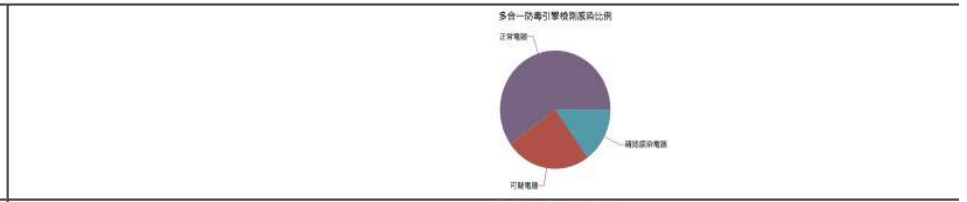
使用派送執行，支援所有Windows 平台之分析。

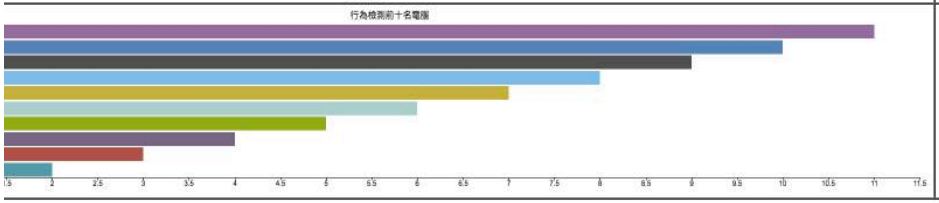
Mac 或 Linux平台，則需要登入分析

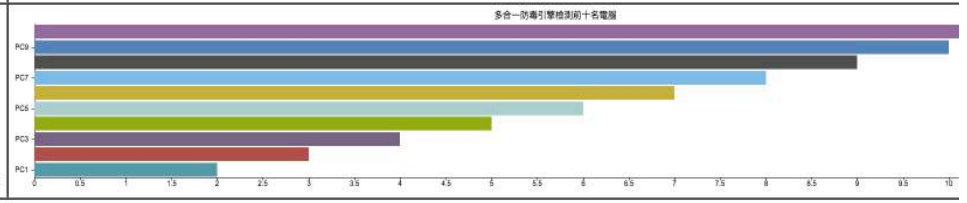
eDetector 健診/快篩 產出分析結果報告

eDetector 惡意程式檢測分析報告









受害電腦	惡意程式 (索引)	惡意分析指標						
		Hook	Code Inject	Hidden	Network	Anti Detect	No Digital Signature	Bad Signature
	svch0st.exe (#B001)		■		■	VM Debug	■	■
	ntdll1.exe (#B002)	SSDT		Process File	■	VM	■	

析

受害電腦	惡意程式 (索引)	防毒引擎分析指標						
		Kapasky	Symantec	McAfee	Sophos	TrendMicro	Avira	Ava
	svch0st.exe (#S001)	■	■	■	■	■	■	■
	ntdll1.exe (#S002)	■	■	■	■	■		

受害電腦	索引	惡意檔案存放路徑
	#B001	C:\Windows\System32\svch0st.exe
	#B002	C:\Windows\System32\ntd1l.dll

析

受害電腦	索引	惡意檔案存放路徑
	#S001	C:\Windows\System32\svch0st.exe
	#S002	C:\Windows\System32\ntd1l.dll

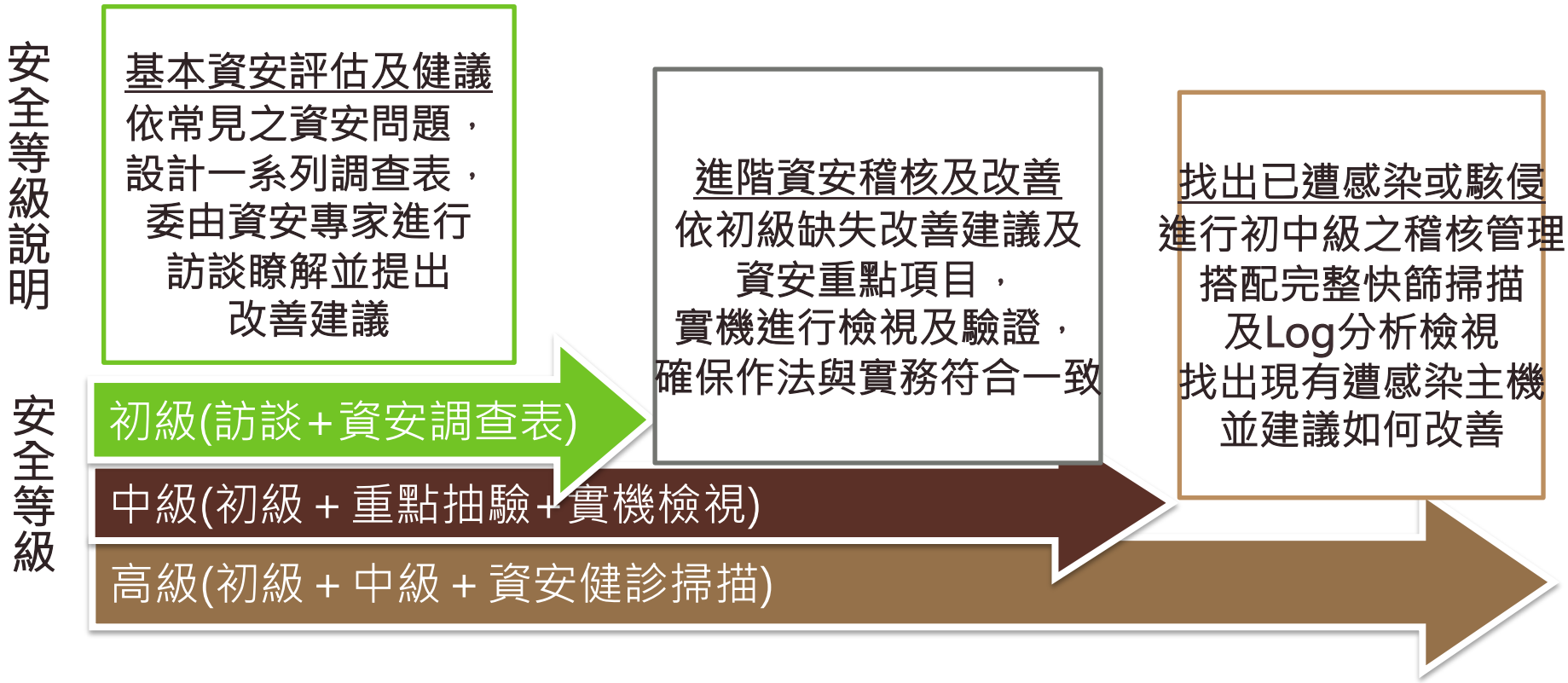
鑒真數位資安鑑識服務說明

鑒真數位-提供資安管理稽核服務說明

▲初級為資安風險評估之最基本要求

▲所有具交易及大量擁有個資之商用服務系統建議能進行中級稽核

▲等級越高表示資安風險評估愈準確且愈能有效改善資安現況



鑒真數位【規模最大】商用數位鑑識實驗室

最專業資安鑑識服務:

- 代理國際資安鑑識大廠

  OPSWAT / VMRay
- 自有研發APT偵測掃描軟體(eDetector)
- 定期惡意程式鑑識專業課程

本團隊擁有國內最多之資安鑑識證照及教學經驗 – 不定期提供數位鑑識課程

- 2017 教育訓練時程表
- Encase
- AccessData
- 電腦鑑識教育
- 智慧型手機鑑識
- 手機進階鑑識
- iPhone專業鑑識
- 硬碟修復暨資料救援訓練

鑒真數位2017年教育訓練時程表

早鳥優惠方案最多可享八五折

國際數位鑑識認證　資安鑑識　數位鑑識基礎
國際手機鑑識認證　手機資安鑑識　智慧型手機鑑識
現場蒐證　資料救援　影像鑑識

月份	日期	天數	課程名稱	類別	課程編號	定價	
1	12,13	2	資安緊急應變暨惡意程式蒐證分析教育訓練		NM02	$24,000	我要報名
2	20	1	智慧型手機破密		SP02	$12,000	我要報名
2	23,24	2	網路鑑識及惡意程式分析(含記憶體分析及Sandbox分析)		NM01	$24,000	我要報名
3	1,2,3	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)		AF01	$70,000	我要報名
3	7,8	2	數位(電腦)鑑識實務案例調查教育訓練		IF02	$26,000	我要報名
3	14,15	2	智慧型手機APP反組譯暨傳輸封包鑑識分析		PW01	$24,000	我要報名
3	20,21	2	駭客入侵暨惡意程式分析調查實務		NM02	$24,000	我要報名
3	21,22,23,24	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)		GE01	$75,000	我要報名
3	28,29,30,31	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)		GE02	$75,000	我要報名
4	5,6,7	3	專業手機暨硬碟資料救援教育訓練課程		ID01	$38,000	我要報名
4	12,13,14	3	AccessData Android Forensic認證		AF02	$75,000	我要報名
4	19	1	數位(電腦)鑑識現場處理教育訓練		IF01	$12,000	我要報名
4	24,25,26	3	AccessData原廠授權認證課程 FTK BootCamp (含ACE認證考試)		AF01	$70,000	我要報名
5	2,3,4,5	4	Guidance原廠授權認證課程EnCase Computer Forensic I (CF1)		GE01	$75,000	我要報名
5	9,10,11,12	4	Guidance原廠授權認證課程EnCase Computer Forensic II (CF2)		GE02	$75,000	我要報名
5	15,16	2	XRY Certification 教育訓練		XPA02	$72,000	我要報名
5	17,18,19	3	原廠認證Cellebrite Certified Physical Analyst (CCPA)		CCPA01	$75,000	我要報名

問題與討論