數位發展部數位產業署
資訊安全服務機構登錄
證書:113-IS-1-90619855-0040

Cloud 3w Co. Ltd

雲森數位有限公司

Cyber Security & Intelligency Agency

Taiwan

CONTENTS

公司緣起

「資通安全管理法」在政府積極推動「資安即國安」政策下，

「資通安全責任等級分級辦法」明定政府機關(構)資訊安全管理系統之導入及通過公正第三方認證

雲森數位成立於2022年1月

公司位於台北101的57樓

以攻擊者的角度提供公正第三方的資訊安全管理顧問服務

優化資訊環境的管理顧問服務

強化人員的資安思維

對客戶訊息絕對保密

公司負責人

李智煒

顧問

具備公職經驗5年、資訊整合網服務10餘年，曾擔任板橋市公所副市長秘書、台灣微型影像股份有限公司董事長特助、淮南寰宇股份有限公司業務副理，對於公家機關作業流程熟悉，並協助企業客戶於資訊整合及資訊安全諮詢服務。主要服務產業包含公營事業及電信產業，服務過的客戶包含：台灣大哥大、台灣之星、台灣電力(股)、中國石油(股)、桃園捷運(股)、機場捷運(股)、萬芳醫院等。另有深厚的系統及網路整合經驗，於服務台灣大哥大專案期間負責全省網路設備汰換專案及維運；服務台灣電力公司資訊系統整合、網路設計與大型專案管理；服務萬芳醫院的資訊安全檢測服務，建立起多面向豐富的網路與資訊安全經歷。

現職主要負責資訊安全的業務。透由多年資訊整合管理經驗，提供企業客戶網路及資訊安全諮詢服務，以及大型專案管理諮詢服務。

學歷：

2005 文化大學 景觀學士
2016 世新大學 資訊管理 碩士

專業證照：

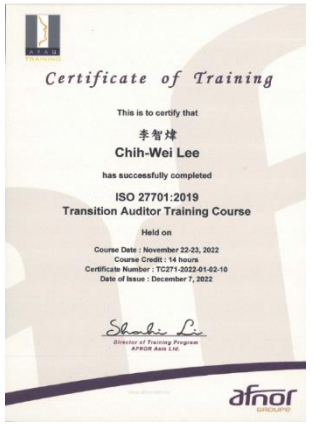
- TQC AutoCAD 2D/3D
- 環保署甲級廢棄物處理專責人員
- CISSP Training Certificate
- ISO 27701:2019
  IEC62443-2-1
- ISO 27001:2022
- AWS Certified Cloud
  Practitioner certificate
- NSPA-Class C封包分析技術
- Certified Ethical Hacker
- ISO 17025:2017

經歷：

- 板橋市公所
- 國防大學國防管理學院
- 台灣微型股份有限公司
- 淮南寰宇股份有限公司
- 中華民國網路封包分析協會理事
- 中華民國資通安全發展協會理事
- 網通科技安全檢測實驗室主管

主要負責服務之公司包括：

- 政府機關、公營事業
- 電信業
- 醫療業
- 連鎖超商
- 遊戲業



公司合規證明

數位發展部 數位產業署
Administration for Digital Industries, moda

數位服務機構能量登錄證書

Certificate of Registration as a Digital Service Organization

茲證明
雲森數位有限公司

登錄類別爲 資訊安全服務機構
通過登錄之技術服務項目及分項爲：

資訊安全服務項目
資訊安全防護能力分析與評估—
執行弱點掃描分析作業
資訊系統安全防護服務—
滲透測試服務
程式源碼檢測服務

登錄日期：中華民國113年09月15日
有效期限：中華民國115年09月15日

數位發展部數位產業署
署長 呂正華

證號: 113-IS-1-90619855-0040

This is to certify that
Cloud3w Co., LTD.

has met the requirements of an Information Security Service Organization in the following technical service items and sub-items.

Information Security Service Item
Analysis and Assessment of Protection in Information Security—
Vulnerability Scanning and Assessment
System Security Protection Services —
Penetration Test Services
Source Code Security Analysis Services

This certificate is valid from September 15, 2024
to September 15, 2026

Director General
Administration for Digital Industries
Ministry of Digital Affairs

NO: 113-IS-1-90619855-0040

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2024/111019.1

AFNOR Certification certifies that the management system implemented by:
AFNOR Certification certifie que le système de management mis en place par :

CLOUD3W CO. LTD.
雲森數位有限公司

for the following activities:
pour les activités suivantes :

INFORMATION AND COMMUNICATIONS SECURITY MANAGEMENT OF THE PROJECT AND SERVICE OPERATION PROCESSES.THIS IS IN ACCORDANCE WITH THE STATEMENT OF APPLICABILITY, VERSION: 1.0, DATED: JUNE 1, 2024.
本公司專案與服務作業流程之資通安全管理。
依據適用性聲明書，版次：1.0，發行日期：2024 年 06 月 01 日

has been assessed and found to meet the requirements of:
a été évalué et jugé conforme aux exigences requises par :

NF EN ISO/IEC 27001:2023 / ISO/IEC 27001:2022

and is developed on the following locations:
et est déployé sur les sites suivants :

57F-1, NO. 7, SEC. 5, XINYI RD., XINYI DIST., TAIPEI CITY 110615, TAIWAN (R.O.C.)
110615 台北市信義區信義路五段 7 號 57 樓之 1

This certificate is valid from (year/month/day)
Ce certificat est valable à compter du (année/mois/jour)
2024-10-12 Until *jusqu'au* 2027-10-11

Julien NIZRI
Managing Director of AFNOR Certification
Directeur Général d'AFNOR Certification

Scan this QR code to check the validity of the certificate.
Flashez ce QR Code pour vérifier la validité du certificat.

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org

afnor CERTIFICATION

服務範圍

1. 資訊安全檢測服務。

   (資安健診、弱點掃描、滲透測試、源碼掃描、社交工程演練、資安曝險評估等)
2. 攻防演練。
3. 加密勒索攻擊數據還原、勒索談判、代付贖金。
4. 跨境商務情資調查。

雲森數位的資訊安全服務範疇

雲森數位的資訊安全服務項目，在整體資安整合服務架構中，以資安檢測的項目為主。(技術面)

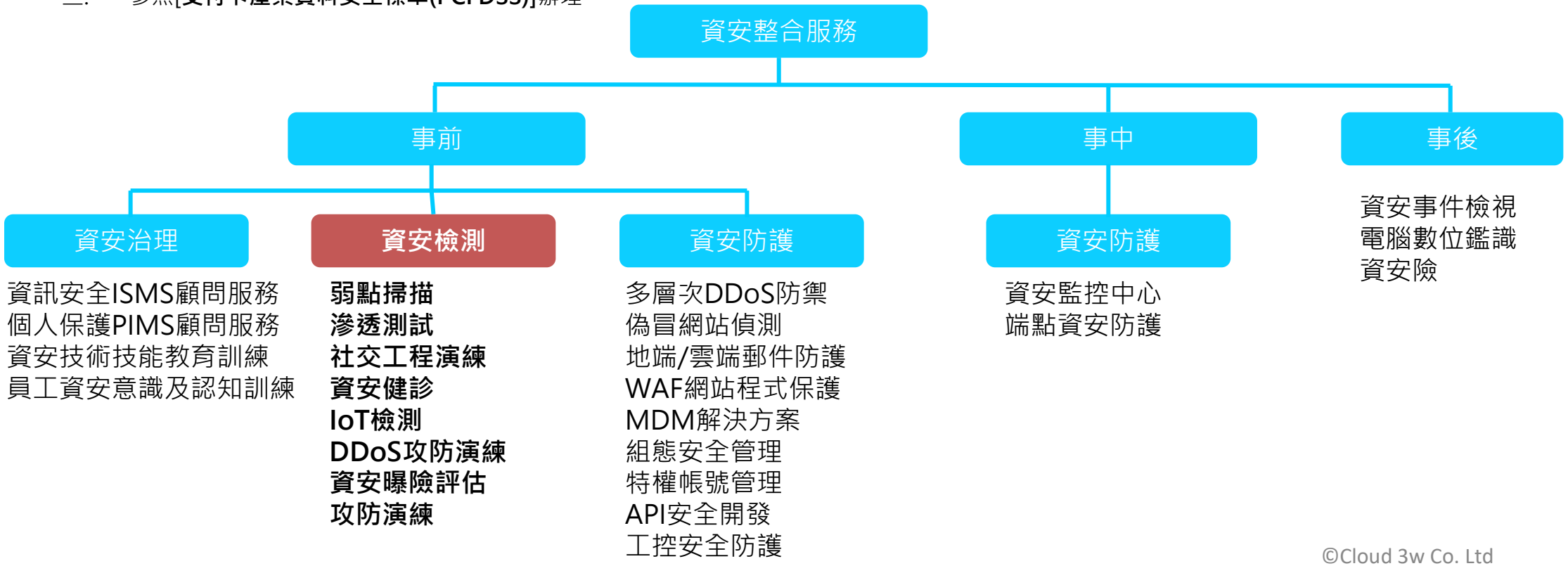
以及協助資安治理顧問服務、教育訓練為輔。(管理面)

資訊安全檢測項目依據方式:

一. 係參照數位發展部**資通安全管理法**推動及宣導事項，及[**113年第五次電腦軟體共同供應契約採購 - 資通安全服務暨資訊服務**]定義之[**113年共同供應契約資通安全服務品項採購規範**]辦理。

二. 參照110年頒布之[**上市上櫃公司資通安全管控指引**]辦理。

三. 參照[**支付卡產業資料安全標準(PCI DSS)**]辦理。



執行資安合規事務次數之基本建議

	資安項目規劃	說明
管理面	建立ISMS制度及輔導取得認證	三年一個循環
	員工資訊安全宣導	年度例行工作
	資安主管及人員專業課程	
技術面	弱點掃描	年度例行工作，每年至少一次
	滲透測試	
	原始碼檢測(系統上線前)	
	資安健診	
	社交工程演練	
系統整合	資訊安全軟硬體產品規畫導入	依合規需求規畫、設計

一、資安檢測

技術面-執行方式

操作人員：

- 由受訓專業課程結業及認証Certified Ethical Hacker–認證道德駭客訓班證書、Computer Hacking Forensic Investigator–駭客偵防班證書、NSPA網路安全封包分析認證課程、TCCF 電腦鑑識實務班證書、 Certified Information Systems Security Professional 資訊系統安全認證專家實務班證書的專責人員操作。
- 執行安全檢測前會參與測式人員均會簽定保密協定文件，確保執行過程中獲得之重要資料及文件等，不會經由檢測過程中外洩。

資料保護：

- 執行中所暫時文件將存於授權保護主機中並加上RMS資料保護機制，確保資料的安全性。
- 專案結案後將檢測所有產生文件、檔案、記錄，檢測完成後主機重灌，確免資料外漏 。

技術面說明-資安健診

服務項目	
1.網路架構檢視	
2.網路惡意活動檢視(有線)	2.1封包監聽與分析
	2.2網路設備紀錄檔分析
3.使用者端電腦惡意活動檢視	3.1使用者端電腦惡意程式或檔案檢視
	3.2使用者端電腦更新檢視
4.伺服器主機惡意活動檢視	4.1伺服器主機惡意程式或檔案檢視
	4.2伺服器主機更新檢視
5.目錄伺服器設定檢視	
6.防火牆連線設定檢視	
7. 政府組態基準(GCB)檢視	
8.資料庫安全檢視	

技術面說明-弱點掃瞄

(一)系統弱點掃描(VA)

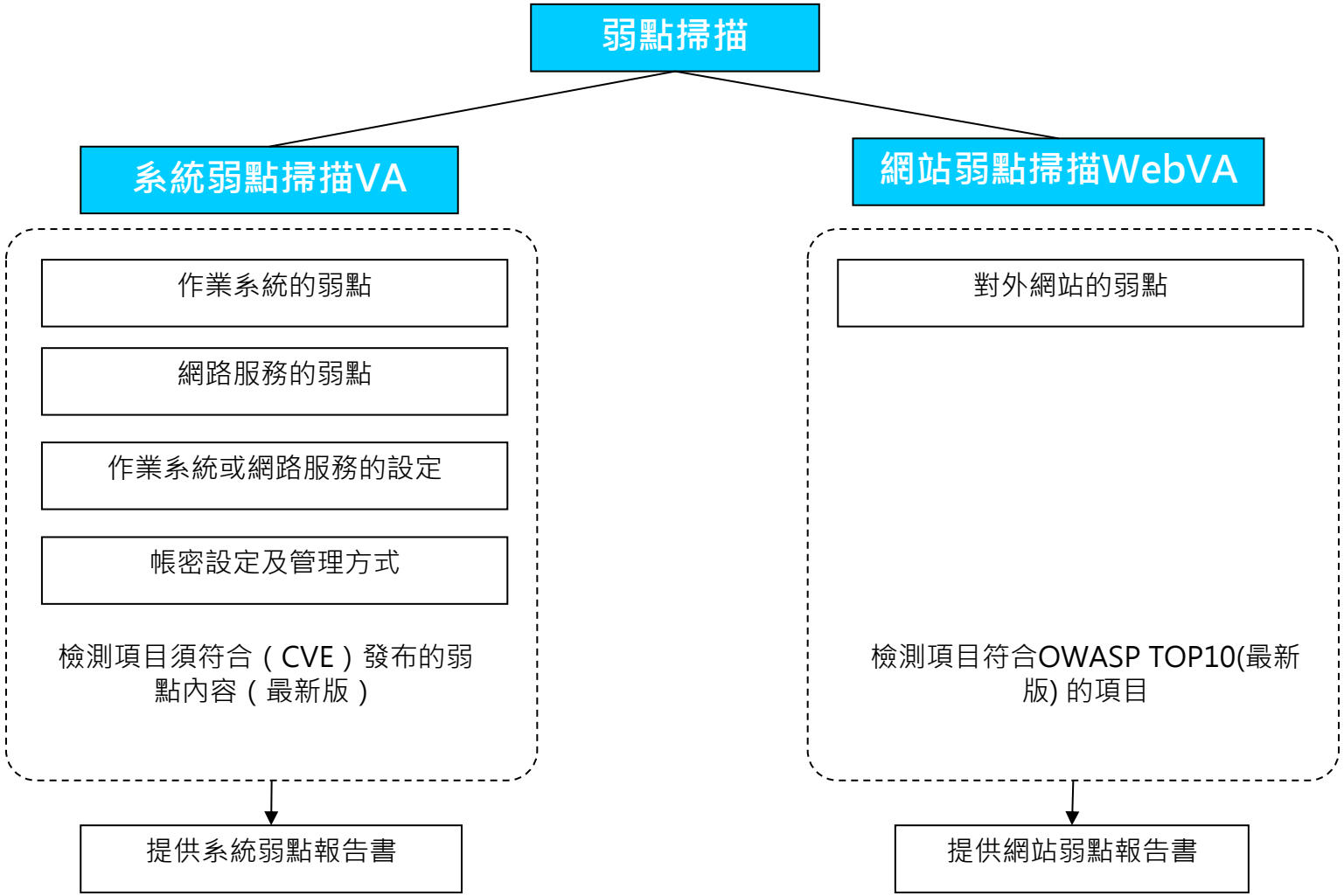
針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目，須符合Common Vulnerabilities and Exposures (CVE)發布的弱點內容(最新版)，至少包含以下項目：

1.作業系統未修正的漏洞掃描
2.常用應用程式漏洞掃描
3.網路服務程式掃描
4.木馬、後門程式掃描
5.帳號密碼破解測試
6.系統之不安全與錯誤設定檢測
7.網路通訊埠掃描。

(二)網站弱點掃描(WebVA)

針對機關對外主機網頁安全弱點進行掃描，檢測項目須符合OWASP TOP 10 最新項目。

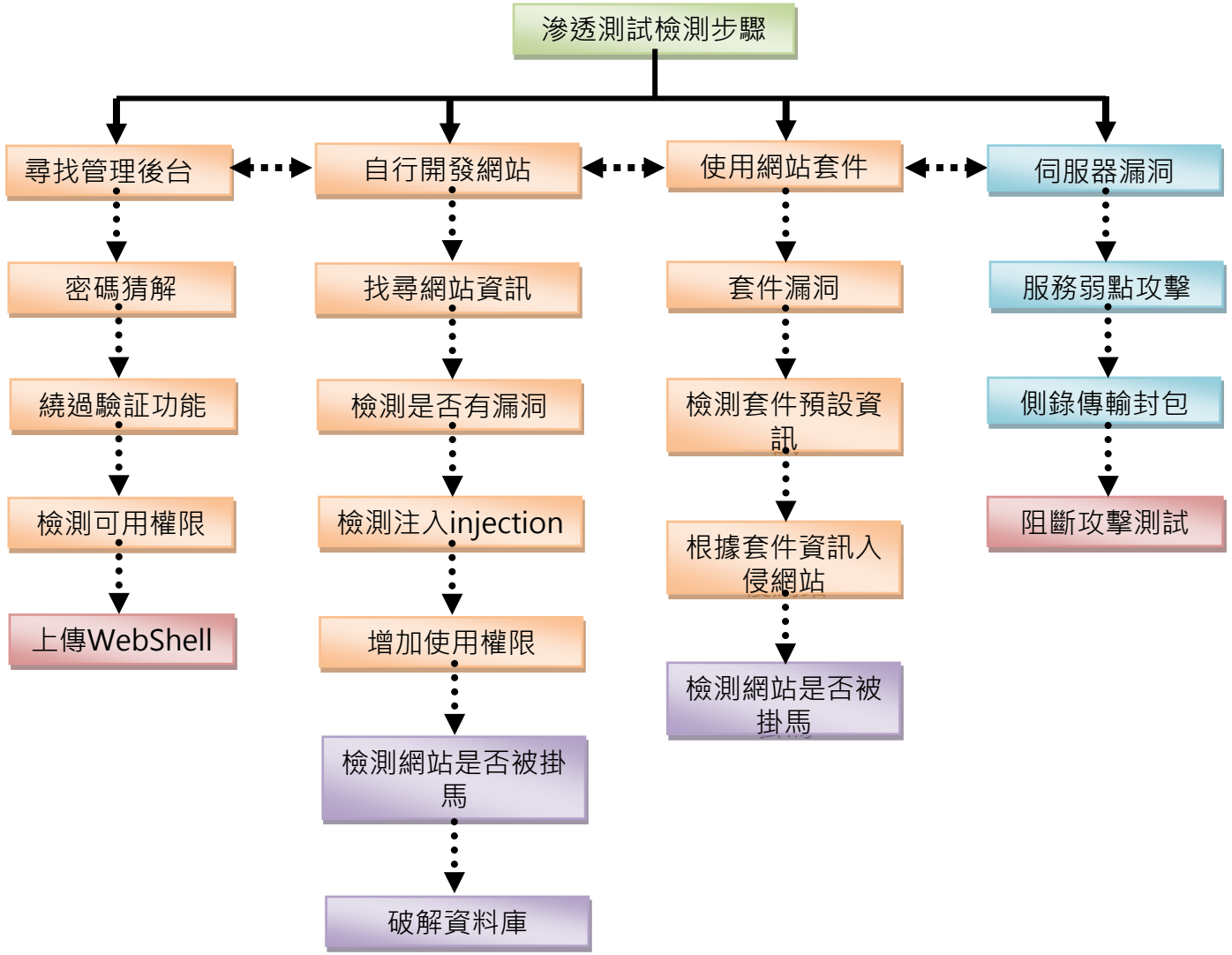
技術面說明-弱點掃瞄



技術面說明-滲透測試(PT)

- 網站安全檢測程序是依照國際標準「Open-Source Security Testing Methodology Manual (OSSTMM)」之所參考制定的標準程序，並且依客戶訪談後之實際環境不同分別選擇檢測模組中適用於客戶環境的可執行之程序。
- 測試方式採用已知的資安漏洞及 OWASP Top 10
  - A01:2021-權限控制失效
  - A02:2021-加密機制失效
  - A03:2021-注入式攻擊
  - A04:2021-不安全設計
  - A05:2021-安全設定缺陷
  - A06:2021-危險或過舊的元件
  - A07:2021-認證及驗證機制失效
  - A08:2021-軟體及資料完整性失效
  - A09:2021-資安記錄及監控失效
  - A10:2021-伺服端請求偽造

技術面說明-滲透測試(PT)



技術面說明-BAS入侵與攻擊演練

實現一場真正的攻擊演練，用最真實的方式演練駭客入侵的情況。

1. 適用於驗證資安建設健全度
    - 檢視資安建設是否不夠健全
    - 檢視建設是否如預期的正常運作
2. 適用於驗證資安團隊可靠度
    - 熟練資安建設應變操作
    - 提升資安威脅應變經驗
3. 適用於驗證資安投資有效度
    - 資安投資是否能有效降低負擔&提升效率
    - 資安投資規劃是否切合企業與團隊需求

技術面說明-原始碼檢測

源碼檢測（靜態應用程式檢測）

源碼檢測又稱原始碼檢測、SAST、白箱測試、靜態應用程式檢測，是針對應用程式的原始碼進行測試與分析，找出潛在的漏洞與弱點並進行修補作業，並非檢查已完成的程式。所以建議在開發階段導入，才能大幅節省修復成本與時間。

動態應用程式檢測

而動態應用程式檢測又稱為黑箱測試、DAST，是透過模擬駭客攻擊的手法，由外而內搜索正在運行中的應用程式漏洞，當發現有漏洞時會自動發送警訊，因此可檢測出靜態應用程式安全測試工具無法識別的缺陷。

技術面說明-社交工程演練

服務項目/內容	電子郵件測試服務
測試次數與規格	1. 1年內，提供機關電子郵件帳號x次的測試。 2. 各帳號進行x封社交工程郵件測試，包含本文、附件、可連結資訊。
測試內容	1. 社交工程郵件設計應涵蓋x種以上不同類型的內容，例如：八卦、休閒、保健、財經、情色、新奇、時事等資訊。 2. 記錄「社交工程郵件開啟」及「社交工程郵件點閱」等受測者行為。

技術面說明-特殊測試

行動裝置攻擊：

- 針對移動設備（例如智慧手機、平板電腦）的攻擊行為進行描述和分類。
- 主要用於描述和整理在移動設備上的攻擊行為，包括iOS和Android等操作系統。

IoT攻擊：

- 物聯網（IoT）攻擊是指針對物聯網設備和網絡基礎設施的攻擊行為。
- 由於物聯網裝置的普及，攻擊者有機會利用這些裝置的弱點和漏洞來入侵、竊取數據、進行拒絕服務攻擊或者對網絡進行其他形式的攻擊。

OT攻擊：

- OT（Operational Technology）是指用於管理和監控現實世界物理過程的技術，例如工業控制系統（Industrial Control Systems，ICS）、自動化系統、智能電網等。
- OT環境通常與傳統的IT（Information Technology）環境有所不同，其主要特點是實時性、可靠性和安全性要求非常高。

二、攻防演練

攻防演練（也稱為**紅藍對抗**或**滲透測試**）是一種模擬網路安全威脅的測試方法，目的是檢測組織的安全防護能力，並通過模擬真實的攻擊行為來強化防禦措施。這種演練通常涉及攻擊方和防守方之間的對抗，透過模擬現實中的攻擊和防禦場景，來幫助組織了解其網路系統的安全漏洞，並改善整體的安全防禦能力。

攻防演練的主要角色：

1.紅隊（攻擊方）：

1. 紅隊模擬黑客或其他惡意攻擊者的行為，主動尋找並利用系統、網路或應用中的漏洞進行滲透。目標是突破防線，達成攻擊任務，例如竊取敏感信息、進行數據破壞或獲取系統控制權。紅隊通常使用多種攻擊技術，如社交工程、漏洞利用、網路釣魚等。

2.藍隊（防守方）：

1. 藍隊負責保護系統、偵測並應對來自紅隊的攻擊行為。他們的任務是通過監控網絡流量、分析日誌、管理安全策略來阻止攻擊，並即時做出反應。藍隊會運用防火牆、入侵檢測系統、殺毒軟體等工具進行防禦，並根據紅隊的行動及時調整防禦策略。

3.白隊（觀察者/裁判）(選配條件)：

1. 白隊負責規劃、協調及評估整個攻防演練過程。白隊通常不直接參與攻擊或防禦行為，但他們會設定演練的規則和目標，並在演練結束後給出評估和建議。他們的工作包括確保演練的公平性和規範性，同時確保不對實際業務造成不必要的干擾。

攻防演練的目的

攻防演練的目的：

1. **評估安全狀況**：通過實際攻擊模擬來找出系統的潛在弱點和漏洞，了解組織在面對攻擊時的防禦能力。
2. **提升安全意識**：通過紅隊的攻擊行動，讓防守方了解真實攻擊的方式，提升全體員工的安全意識和應對能力。
3. **改進安全防禦措施**：根據演練結果，組織可以改進安全策略，部署更有效的防護技術，並加強防守團隊的技術能力。
4. **應急響應能力測試**：檢查組織的應急響應計劃是否有效，是否能在遭遇攻擊時迅速響應並最小化損失。
5. **合規性驗證**：攻防演練通常也是企業遵守安全法規、標準（如ISO 27001、NIST等）的方式之一，用於驗證安全系統的合規性。

攻防演練的選擇方案

在不影響企業營運的前提下，有五種選擇。

時間限制	紅隊可發動的模式	適用公司	演練標的 (客戶授權範圍)	目的與結果
演練時間：1~3個月 專案時間：4~16個月 複測時間：1~2個月	遠端攻擊 無限制任何方式	大型集團 上市櫃公司 特定公司	核心資產系統 客戶定義的重要系統	技術層面全方位最大化的找出最多可被入侵的方式及0-day攻擊。
演練時間：1~2個月 專案時間：3~10個月 複測時間：1個月	遠端攻擊或內網攻擊 使用已知的攻擊方式	大型企業 一般中小企業	核心資產系統 客戶定義的重要系統	測試出會可突破防線攻擊侵方式，演練被攻擊後會受損害的程度。
演練時間：1~3週 專案時間：2~6個月 複測時間：1週	遠端攻擊或內網攻擊 持續性攻擊劇本	一般中小企業	協助客戶建置測試標靶	考驗藍隊網路、系統防護成熟度與防護能力。
演練時間：1~5天 專案時間：1~2個月 複測時間：1天	遠端跳板攻擊 持續性特定劇本	一般中小企業	協助客戶建置測試標靶 客戶定義的重要系統	模擬被攻擊手法，考驗藍隊防護能力。
演練時間：1~5天 專案時間：1~2個月 複測時間：1天	內網或外網 針對加密勒索的方式進行攻擊	擔心遇到會被加密勒索過的單位	協助客戶建置測試標靶	模擬加密勒索攻擊，考驗藍隊的防護與應變能力。 協助撰寫入侵後的鑑識報告。

演練過程不會提供log，也不會進行通報，結束後統一撰寫報告書。

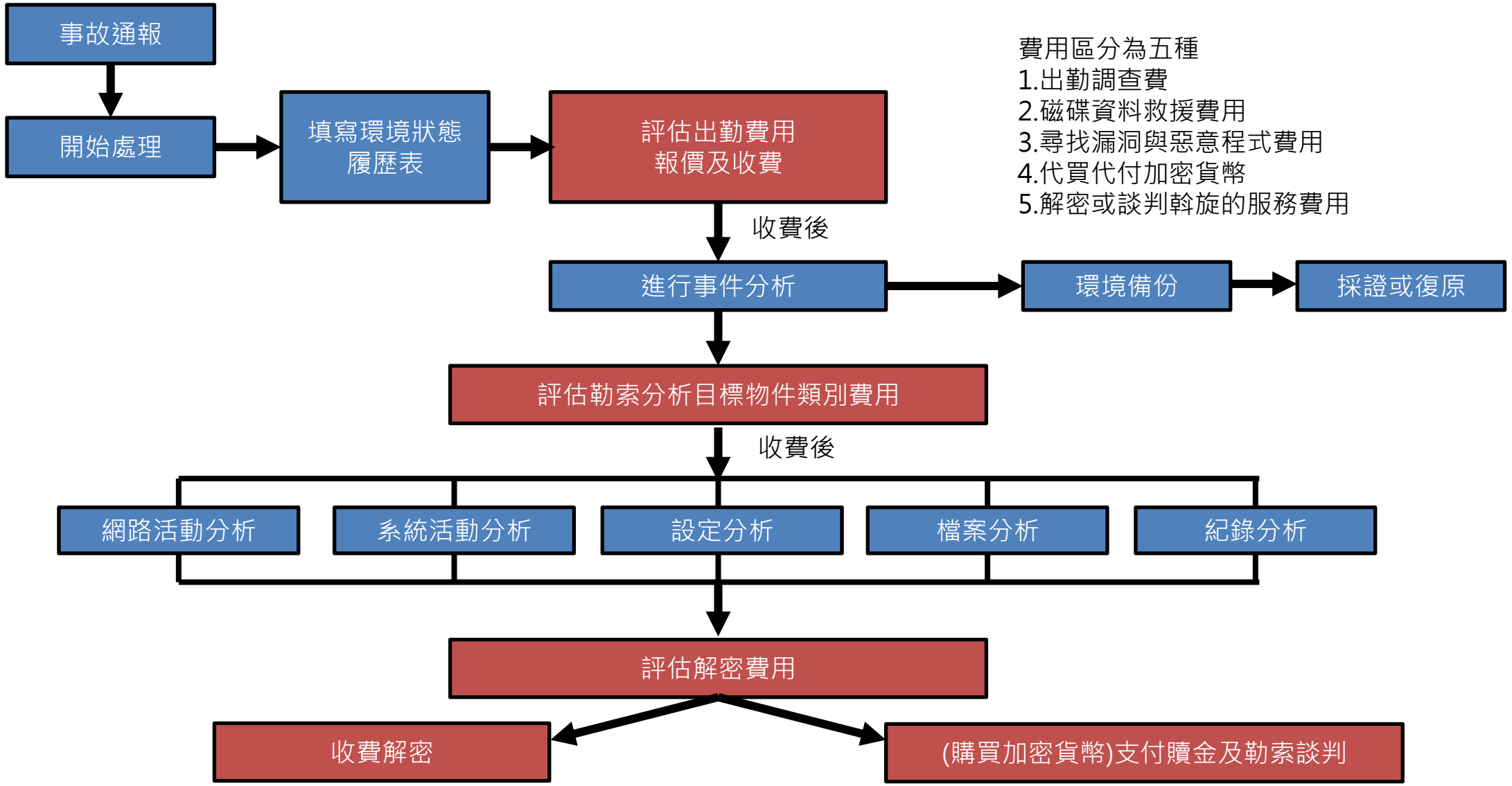
攻防演練的流程

1. **簽訂合約及保密協議。**
2. **規劃和準備**：
   設置演練目標、範圍和規則，確定演練的關鍵系統、資產及參與人員。
3. **信息收集**：
   紅隊進行偵查，收集目標系統的各種信息，為後續攻擊做準備。
4. **攻擊執行**：
   紅隊根據收集的信息發起攻擊。
5. **防禦與響應**：
   藍隊監測並嘗試阻止攻擊，根據攻擊行為做出防禦調整，並記錄攻擊過程。
6. **演練總結**：演練結束後，並提出改進建議。

加密勒索事後處理方案

尝試解密
談判
付款及復原

作業流程概觀



費用區分為五種
1.出勤調查費
2.磁碟資料救援費用
3.尋找漏洞與惡意程式費用
4.代買代付加密貨幣
5.解密或談判斡旋的服務費用

加密勒索事件

需要注意的事項

*如何增高解密救援恢復資料後的資料最高完整性

1.被勒索者需**提供任何被勒索加密資料夾內的 *.html 或 *.txt** 此為駭客聯繫資訊與任一個該資料內附檔名被加密的檔案。

2.被勒索者能否提供之前資料庫的舊備份檔案，例如資料庫複製檔，或Dbdump，或任何第三方備份工具曾經的歷史備份資料。

3.若無任何遭勒索加密的資料庫歷史檔案，Dbdump，或曾經的第三方備份工具的歷史備份資料，則可以提供乾淨的該資料庫的全新安裝的 "庫結構" 乾淨資料庫的意思

一、加密勒索解密

解勒索加密服務說明

可透過人工破解“已遭加密”檔案類型

1. 資料庫檔案格式:

For example: SQL,Oracle,mySQL,exchange,any database的檔案...etc

常見資料庫檔案格式的檔案...全部皆能解密

2.虛擬化主機檔案格式:

*.VMDK , *.vhd, ...etc 只有虛擬機檔案底層遭加密無法開機,但是虛擬機作業系統C: D: ..裡面的資料庫檔案實際上必須是沒有被加密的

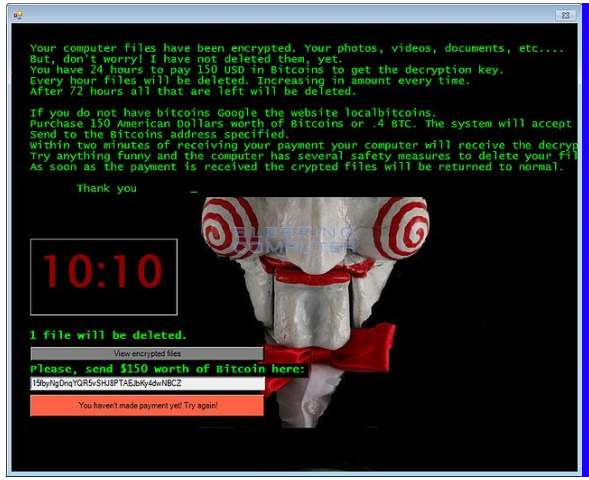
3.虛擬化檔案,for example *.VMDK , *.vhd, ...etc 虛擬機檔案底層遭加密無法開機,並且虛擬機作業系統C: D: ..也遭加密,但裡面的Database File 仍可以再做人工第二次解密

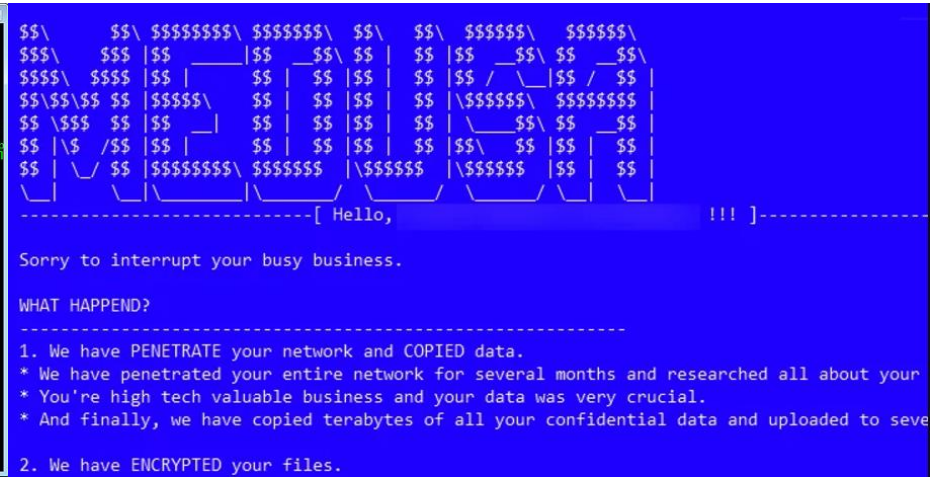
4.一般性檔案,for example *.pdf, *.doc, *.xls, *.ppt, *.mp4, *.bmp, *.一般任何檔案類型 .. PS:一般性各類檔案,需要是較舊款的勒索病毒,工程師可協助使用任何市面上可取得的勒索解密工具協助實施破解,取回原始檔案

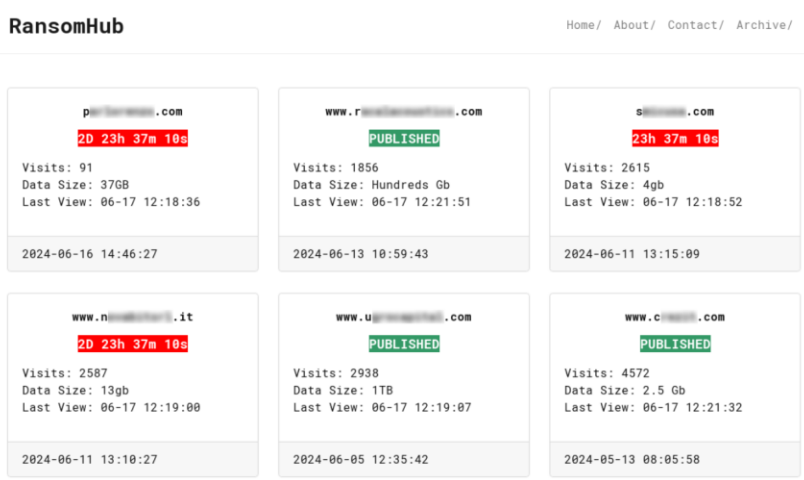
二、加密勒索斡旋與談判

需要透過我們與駭客聯絡，並協助談判斡旋降低金額，然後由我們提供的付款專用虛擬貨幣帳戶去暗網的冷錢包代為付款購買密鑰的方式

1.一般性檔案,for example *.pdf, *.doc, *.xls, *.ppt, *.mp4, *.bmp, *.一般任何檔案類型 .中的是 LockBit 3.0 加密破壞機制類型的病毒
2.資料庫檔案:for example SQL, Oracle, mySQL, exchange, any database的檔案.. 中的是 LockBit 3.0 加密破壞機制類型的病毒
3.RansomHub或其他新型態的加密勒索攻擊無法破解，只能夠進行斡旋談判。







三、加密貨幣代收代付服務

- 處理大筆現金或匯款購買加密貨幣服務，或是大筆加密貨幣換成新台幣的服務。
- 單次交易需超過300萬新台幣。

- 交易模式需先進行簽署商業服務合約、洗錢防制聲明、保密切結書。
- 適用於企業遇到加密勒索事件，需臨時購買大額加密貨幣，並代付給予特定加密貨幣地址的服務。
- 交易時間，限制於上班日上午9:00～14:00（需配合銀行作業時間）。
- 報價模式依照當日加密貨幣兌換匯率加上手續費。每筆服務費用依照購買的標的加密貨幣數量、或轉換成台幣的最終金額，依照相關美金匯率、加密貨幣匯率，以新台幣為基準進行服務報價。

- 開立全額三聯式商業發票。

以攻擊者的角度

協助做有效的資安方案!

數位發展部數位產業署
資訊安全服務機構登錄
證書:113-IS-1-90619855-0040

THANKS

雲森數位有限公司
Cloud 3w Co. Ltd