雲森數位有限公司

Cloud 3w Co. Ltd — Cyber Security & Intelligence Agency, Taiwan

---

數位發展部數位產業署　資訊安全服務機構登錄廠商

證書：113-IS-1-90619855-0040

證書：114-IS-1-90619855-0069

ISO 27001 Info認證通過

簡報目錄

本簡報依序介紹雲森數位有限公司之公司背景、服務範圍、資安技術與管理說明，以及加密勒索事件處理能力，協助政府機關及企業客戶全面了解本公司之資安服務。

CHAPTER 01

公司簡介

雲森數位有限公司成立於2022年1月，公司位於台北101大樓57樓。在「資安即國安」政策背景下，本公司以攻擊者視角提供公正第三方資訊安全管理顧問服務，協助政府機關與企業強化資安防禦體系。

公司緣起與核心理念

在政府積極推動「資安即國安」政策下，《資通安全管理法》與《資通安全責任等級分級辦法》明定政府機關（構）須導入資訊安全管理系統並通過公正第三方認證。雲森數位應運而生，以專業技術填補市場需求。

攻擊者視角

以駭客思維審視客戶資安漏洞，提供最貼近真實威脅的檢測服務

公正第三方

獨立於客戶資訊系統之外，提供客觀、中立的資安管理顧問評估

強化資安思維

針對人員進行資安意識培訓，從組織文化層面強化整體防禦縱深

絕對保密

對客戶資訊及檢測過程中獲取之敏感資料，嚴格執行保密協議

公司合規認證

雲森數位有限公司已完成數位發展部數位產業署之資訊安全服務機構登錄，並持有國際資訊安全管理標準認證，充分展現本公司符合政府採購規範及國際資安標準之資格。

數位服務機構能量登錄證書 113年

登錄類別：資訊安全服務機構

登錄之技術服務項目：

- 資訊安全防護能力分析評估
- 執行弱點掃描分析評估
- 資訊安全全風險評鑑服務
- 滲透測試服務
- 原始碼安全分析服務

證書：113-IS-1-90619855-0040

有效期間：2024/09/15 至 2026/09/15

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

數位服務機構能量登錄證書 114年

登錄類別：資訊安全服務機構

登錄之技術服務項目：

資訊安全服務項目 資訊安全或個人資料管理架構規劃與建置—

- 資訊安全管理系統建置輔導
- 個人資訊管理系統建置輔導

資訊安全防護能力分析與評估—

- 執行弱點掃描分析作業
- 提供資安事件分析服務

資訊系統安全防護服務—

- 滲透測試服務
- 程式源碼檢測服務

證書：114-IS-1-90619855-0069 有效期間：2025/09/01 至 2027/09/01

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
資訊安全或個人資料管理架構規劃與建置—
資訊安全管理系統建置輔導
個人資訊管理系統建置輔導
資訊安全防護能力分析與評估—
執行弱點掃描分析作業
提供資安事件分析服務
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114年09月01日
有效期限：中華民國116年09月01日

數位發展部數位產業署
署長 林俊秀

證號: 114-IS-1-90619855-0069

This is to certify that
Cloud3w Co., LTD.
has met the requirements of anInformation Security Service Organization in the following technical service items and sub-items.
Information Security Service Item
Planning and establishing ISMS or PIMS Services—
Consulting Services in Information Security Management System
Consulting Services in Personal Information Management System
Analysis and Assessment of Protection in Information Security—
Vulnerability Scanning and Assessment
Services in Analysis of Information Security Incident
System Security Protection Services —
Penetration Test Services
Source Code Security Analysis Services
This certificate is valid from September 01, 2025
to September 01, 2027

Director General
Administration for Digital Industries
Ministry of Digital Affairs

NO: 114-IS-1-90619855-0069

ISO 27001 國際資安認證

雲森數位持有由 AFNOR Certification 頒發之 **ISO 27001 資訊安全管理系統**國際認證，證明本公司在資訊安全管理制度上符合最嚴格的國際標準

AFNOR Certification 為國際認可之驗證組織，ISO 27001 認證代表雲森數位在資訊安全風險管理、資產保護及法遵合規上達到國際頂尖水準。

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

cofrac
CERTIFICATION DE SYSTÈMES

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 18 197 000 € - 479 076 002 RCS Bobigny - www.afnor.org

afnor
CERTIFICATION

公司負責人介紹

李智煒　創辦人暨顧問

具備公職經驗5年、資訊整合網服務逾10年。曾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。對公家機關作業流程嫻熟，並長期協助企業客戶進行資訊整合及資訊安全諮詢。

主要服務產業涵蓋公營事業及電信業，服務客戶包含：**電信公司、國家基礎建設、鐵道及機場、區域醫院、政府A級機關**等大型機構。現職主要負責資訊安全業務，透過多年資訊整合管理經驗，提供企業客戶網路及資安諮詢服務。

學歷

- 2005　文化大學　景觀學士
- 2016　世新大學　資訊管理　碩士

主要經歷

- 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

負責人專業證照

李智煒顧問持有多張國際認可之資安專業證照，涵蓋倫理駭客、封包分析、雲端架構、資訊安全管理及工控安全等核心領域，充分展現全方位資安技術能力。

CEH
Certified Ethical Hacker

ISO 27001:2022
Lead Auditor

ISO 27701:2019
Transition Auditor

IEC 62443-2-1
Lead Auditor

AWS CCP
Cloud Practitioner

NSPA Class C
封包分析技術

CISSP Training
資訊系統安全認證

ISO 17025:2017
測試實驗室認證

主要服務產業

雲森數位長期深耕多個關鍵產業，累積豐富的資安服務實戰經驗，尤其在高度合規要求的政府機關、電信及醫療領域具備深厚專業底蘊。

政府機關與公營事業

熟悉政府採購法規與資安合規要求，協助機關通過資安認證

電信業

具備大型網路設備建置、汰換及維運經驗

醫療業

曾服務區域醫院，具備醫療資訊系統資安檢測及個資保護服務經驗

連鎖零售與遊戲業

提供連鎖超商及遊戲業者資安檢測與防護，保障消費者數據安全

CHAPTER 02

服務範圍

雲森數位提供涵蓋技術面與管理面的完整資訊安全服務，從合規檢測、ISMS輔導、教育訓練，到高階的攻防演練與加密勒索事件處理，一站式滿足客戶全方位資安需求。

六大核心服務項目

01　資訊安全檢測服務

涵蓋資安健診、弱點掃描、滲透測試、源碼掃描、社交工程演練等，依據數位發展部資通安全管理法規及共同供應契約規範執行。

02　ISMS輔導顧問服務

協助企業導入ISO/CNS 27001:2022資訊安全管理系統，提供三年完整輔導驗證循環，涵蓋文件制定、風險評估、內外稽陪同。

03　資訊安全意識教育訓練

提供全員資安意識宣導及資安主管專業課程，強化組織人員在面對社交工程、釣魚郵件等威脅時的識別與應對能力。

04　BAS入侵與攻擊演練

Breach and Attack Simulation，以最真實的方式模擬駭客入侵，驗證資安建設健全度、資安團隊可靠度及資安投資有效度。

05　加密勒索事件處理

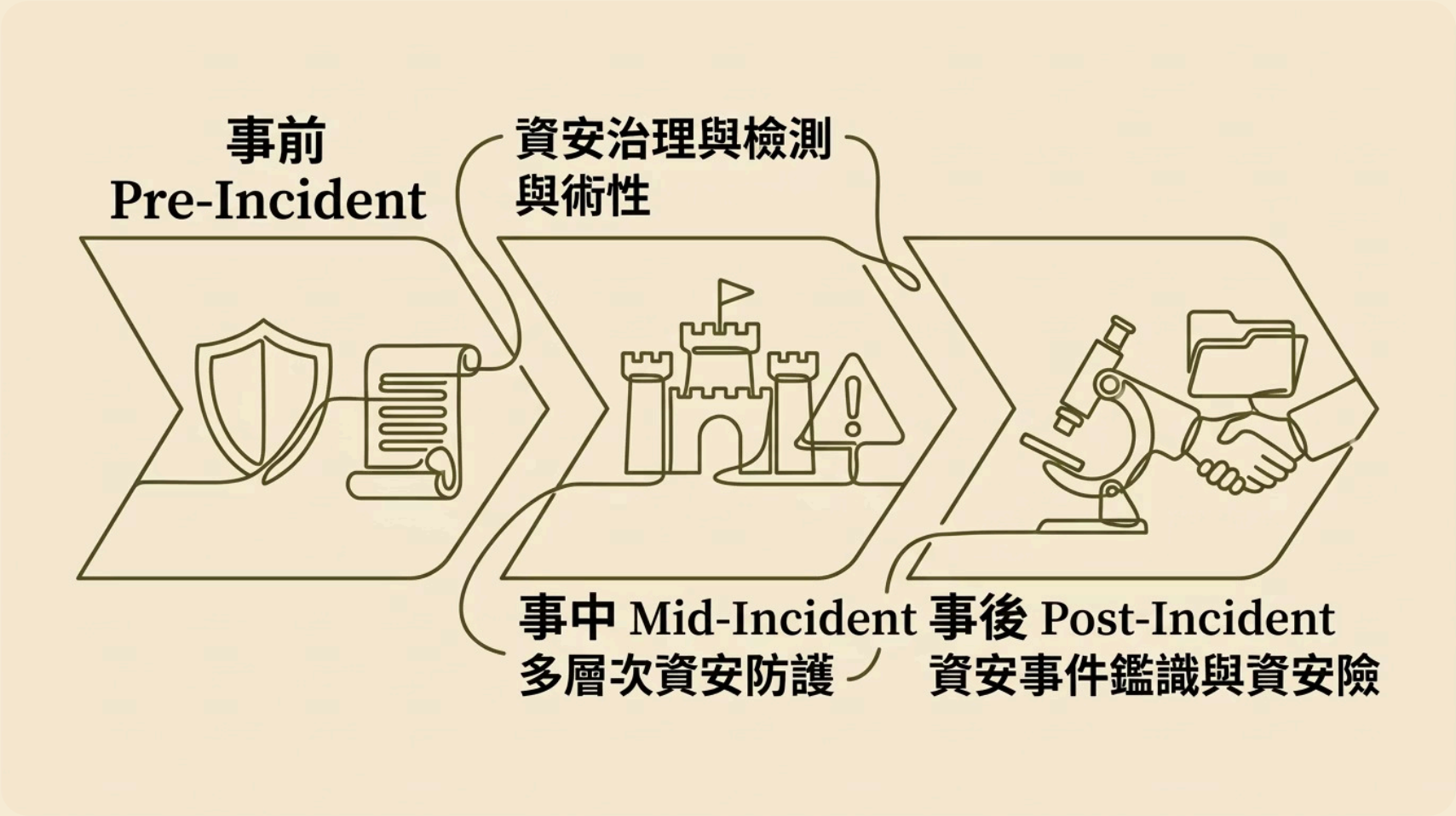
提供加密勒索攻擊數據還原、勒索談判斡旋、加密貨幣代付贖金等完整事件應變服務。

06　跨境商務情資調查

協助企業進行跨境商業情資蒐集與風險評估，掌握潛在威脅來源，強化供應鏈及商業合作夥伴的安全審查。

資安整合服務架構

雲森數位的資安服務以「事前預防、事中防護、事後復原」為主軸，技術面以資安檢測為核心，管理面以治理顧問與教育訓練為輔，形成完整的資安防護生態系。



資安服務合規依據

雲森數位所提供之資安檢測服務，嚴格遵循以下三大合規框架執行，確保服務品質符合政府採購規範及國際標準要求。

資通安全管理法

依據數位發展部推動之《資通安全管理法》及113年第五次電腦軟體共同供應契約採購規範（資通安全服務暨資訊服務）執行各項資安服務項目。

上市上櫃資安管控指引

參照110年頒布之《上市上櫃公司資通安全管控指引》，協助上市櫃企業落實資安治理義務，強化對股東與主管機關的資安透明度。

PCI DSS 支付卡安全標準

參照《支付卡產業資料安全標準（PCI DSS）》，為金融支付相關業者提供符合國際支付安全合規要求的資安檢測服務。

資安服務執行建議頻率

針對不同資安項目，雲森數位建議客戶依循以下執行頻率規劃，以確保資安合規的持續性與有效性，形成系統化的資安管理循環。

資安項目	說明	建議頻率
建立ISMS制度及輔導取得認證	管理面合規建制	三年一個循環
員工資訊安全宣導	全員資安意識培訓	每年至少一次
資安主管及人員專業課程	技術人員進階培訓	年度例行工作
弱點掃描（VA）	系統及網站弱點偵測	每年至少一次
滲透測試（PT）	模擬駭客實際攻擊手法	年度例行工作
原始碼檢測（SAST）	系統上線前靜態分析	系統上線前執行
資安健診	全面網路環境健康檢查	年度例行工作
社交工程演練	模擬釣魚郵件測試	年度例行工作
資訊安全軟硬體規畫導入	系統整合建置	依合規需求規劃設計

CHAPTER 03

資安技術面及管理面說明

本章節詳細說明雲森數位各項資安技術服務的執行方式與操作規範，以及管理面ISMS輔導服務內容，讓客戶充分了解服務品質保障機制。

技術面執行規範

操作人員資格

所有資安檢測由持有以下國際認證之專責人員執行：

- Certified Ethical Hacker (CEH) — 認證道德駭客
- Computer Hacking Forensic Investigator (CHFI) — 駭客偵防
- NSPA 網路安全封包分析認證
- TCCF 電腦鑑識實務班
- CISSP 資訊系統安全認證專家

執行前所有測試人員均須簽署**保密協定文件**，確保檢測過程中獲取之重要資料不外洩。

資料保護機制

執行過程中產生之暫存文件，存於授權保護主機並加上**RMS資料保護機制**，確保資料安全性。

專案結案後，檢測所產生之所有文件、檔案、記錄均予銷毀，並對執行主機進行**重灌還原**，徹底防止資料外洩風險。

雙重保障：執行中 RMS 加密保護 + 結案後主機完整重灌，確保零資料殘留。

技術面說明：資安健診

資安健診是對客戶資訊環境進行全面性健康檢查，涵蓋網路架構、惡意活動偵測、主機安全及系統設定等八大面向，快速識別潛在安全風險。

1

網路架構檢視

審視整體網路拓樸架構，識別設計缺陷

2

網路惡意活動檢視

封包監聽分析與網路設備紀錄檔審查

3

使用者端電腦檢視

惡意程式或檔案偵測及系統更新狀態確認

4

伺服器主機檢視

主機惡意活動分析及更新狀態審查

5

目錄伺服器設定檢視

AD/LDAP目錄服務安全設定稽核

6

防火牆與GCB檢視

防火牆連線設定及政府組態基準（GCB）符合性稽核，含資料庫安全檢視

技術面說明：弱點掃描

（一）系統弱點掃描（VA）

針對作業系統、網路服務、帳號密碼管理等進行弱點檢測，須符合 **CVE 最新版**發布之弱點內容，至少涵蓋：

- 作業系統未修正漏洞掃描
- 常用應用程式漏洞掃描
- 網路服務程式掃描
- 木馬、後門程式掃描
- 帳號密碼破解測試
- 不安全與錯誤設定檢測
- 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 10:2025**，包含：

- A01:2025 存取控制失效（Broken Access Control）
- A02:2025 安全設定錯誤（Security Misconfiguration）
- A03:2025 軟體供應鏈失效（Software Supply Chain Failures）
- A04:2025 加密機制失效（Cryptographic Failures）
- A05:2025 注入式攻擊（Injection）
- A06:2025 不安全設計（Insecure Design）
- A07:2025 身份驗證失效（Authentication Failures）
- A08:2025 軟體及資料完整性失效（Software or Data Integrity Failures）
- A09:2025 資安記錄及監控失效（Security Logging & Alerting Failures）
- A10:2025 例外條件處理不當（Mishandling of Exceptional Conditions）

CVSS 3.1 與 4.0 版本差異

CVSS（Common Vulnerability Scoring System）是全球通用的漏洞嚴重性評分系統，由 FIRST 組織維護。2023年11月正式發布的 CVSS 4.0 針對 3.1 版的多項限制進行了重大改進。

CVSS 3.1

- 三大評估基準：基本（Base）、現狀（Temporal）、環境（Environmental）
- Scope 指標用於評估影響範圍
- 機密性/完整性/可用性（C/I/A）為單一維度評估
- 評分粒度不足（實際僅約99個離散分數）
- 時間指標對最終分數影響有限
- 主要適用於 IT 系統
- 評分命名無法區分使用了哪些指標組

CVSS 4.0（2023年11月發布）

- 四大評估基準：基本（Base）、威脅（Threat，原Temporal改名）、環境（Environmental）、補充（Supplemental，新增）
- 移除 Scope 指標，改為「受影響系統」與「後續系統」分別評估 C/I/A
- 新增攻擊要求（Attack Requirements）指標，提升評估精度
- 使用者互動細分為：無（None）、主動（Active）、被動（Passive）
- 新增補充指標：自動化可能性、價值密度、回復力、供應商緊急度等
- 擴展支援 OT/ICS/IoT 工控環境
- 新命名規範：CVSS-B、CVSS-BT、CVSS-BE、CVSS-BTE，明確標示使用的指標組

CVSS 基礎分（CVSS-B）僅代表漏洞嚴重性（Severity），不應單獨用於風險評估。建議使用 CVSS-BTE 進行更全面的真實風險評估。

OWASP Top 10 檢測涵蓋範圍

雲森數位滲透測試全面涵蓋 **依據 OWASP Top 10:2025 最新版** 的網頁應用程式安全風險，確保客戶系統對抗當前主流攻擊手法的防護能力。

A01:2025 - Broken Access Control

存取控制失效：最常見的應用程式安全風險，攻擊者可繞過授權機制存取未授權資源。

A02:2025 - Security Misconfiguration

安全設定錯誤：系統、框架或雲端服務設定不當，導致安全漏洞暴露。

A03:2025 - Software Supply Chain Failures

軟體供應鏈失效：第三方元件、開源套件或 CI/CD 流程遭受攻擊或含有漏洞。

A04:2025 - Cryptographic Failures

加密機制失效：敏感資料傳輸或儲存時未使用適當加密，導致資料外洩。

A05:2025 - Injection

注入式攻擊：SQL、NoSQL、OS 指令等注入攻擊，使攻擊者可執行惡意指令。

A06:2025 - Insecure Design

不安全設計：系統設計階段缺乏安全考量，導致架構層面的根本性漏洞。

A07:2025 - Authentication Failures

身份驗證失效：身份驗證與會話管理機制不當，攻擊者可冒充合法使用者。

A08:2025 - Software or Data Integrity Failures

軟體及資料完整性失效：未驗證軟體更新、CI/CD 管線或序列化資料的完整性。

A09:2025 - Security Logging & Alerting Failures

資安記錄及監控失效：缺乏足夠的日誌記錄與監控，導致攻擊行為無法被及時偵測。

A10:2025 - Mishandling of Exceptional Conditions

例外條件處理不當：程式對錯誤、例外狀況處理不當，可能導致系統崩潰或資訊洩漏。

技術面說明：滲透測試（PT）

滲透測試依據國際標準 **OSSTMM（Open-Source Security Testing Methodology Manual）**制定標準程序，並依客戶實際環境量身選擇適用檢測模組，以已知資安漏洞及 OWASP Top 10 為測試基礎。

1

訪談與範圍確認

與客戶進行技術訪談，確認測試目標環境、授權範圍及測試模式（黑箱/灰箱/白箱）

2

情資蒐集與偵查

針對目標系統進行開源情報蒐集（OSINT）、網路偵查及服務枚舉

3

弱點分析與驗證

依據 CVE 及 OWASP Top 10 進行漏洞識別，並手動驗證弱點可利用性

4

攻擊滲透執行

模擬真實駭客手法，嘗試突破防線、取得系統存取權限或敏感資料

5

報告撰寫與建議

提供完整滲透測試報告，包含風險等級評估、漏洞說明及具體修補建議

技術面說明：BAS 入侵與攻擊演練

Breach and Attack Simulation（BAS）透過最真實的方式模擬駭客入侵情境，協助組織全面驗證其資安防護能力的三個核心面向。

驗證資安建設健全度

檢視資安建設是否健全，確認各項防護措施是否如預期正常運作，識別防護盲點與設定缺陷。

驗證資安團隊可靠度

熟練資安建設應變操作流程，提升資安威脅應變實戰經驗，強化藍隊偵測與反應能力。

驗證資安投資有效度

評估資安投資是否有效降低風險、提升效率，驗證規劃是否切合企業與團隊實際需求。

滲透測試（PT）與 BAS 攻防演練的差異

滲透測試與 BAS 同屬主動式資安驗證手法，但兩者在執行方式、目的與適用情境上有明顯差異，企業可依需求搭配運用。

比較項目	滲透測試（PT）	BAS 入侵與攻擊演練
執行方式	由人工專業人員手動執行，模擬真實駭客攻擊	透過自動化平台持續模擬攻擊情境
執行頻率	定期執行（通常每年 1～2 次）	可持續、重複、自動化執行
測試範圍	針對特定系統、應用程式或網路進行深度測試	廣泛模擬多種攻擊手法與 Kill Chain 全流程
主要目的	找出可被利用的漏洞並提供修補建議	驗證現有資安防護工具與團隊的實際有效性
測試對象	系統漏洞、應用程式弱點	資安工具（EDR/SIEM/防火牆）、SOC 團隊應變能力
報告產出	詳細漏洞報告與修補建議	防禦覆蓋率分析、工具有效性評估報告
法規合規	符合資通安全管理法、共同供應契約規範	補充合規驗證，強化持續性安全監控
適用時機	系統上線前、重大變更後、年度合規要求	建立資安防護後的持續驗證與優化

雲森數位建議：滲透測試用於找出漏洞，BAS 用於驗證防護有效性，兩者相輔相成，建議搭配執行以達最佳資安防護效果。

技術面說明：原始碼檢測

靜態應用程式檢測（SAST）

又稱**源碼檢測**、**白箱測試**，針對應用程式的原始碼進行分析，在程式完成前找出潛在漏洞與弱點。

建議於開發階段導入，可大幅節省修復成本與時間。適用於自行開發系統、委外開發驗收前及系統上線前的安全把關。

動態應用程式檢測（DAST）

又稱**黑箱測試**，透過模擬駭客攻擊手法，由外而內搜索正在運行中的應用程式漏洞，發現弱點時自動發送警訊。

DAST 可**偵測出靜態測試工具無法識別的執行期缺陷**，兩者搭配使用可達到最完整的應用程式安全涵蓋率。

- 建議將 SAST（開發階段）與 DAST（上線後）結合，形成完整的應用程式安全生命週期防護策略（DevSecOps）。

技術面說明：社交工程演練

社交工程演練透過模擬真實釣魚郵件攻擊，測試員工面對惡意郵件時的識別與應對能力，是強化人員資安意識最有效的實戰訓練方式。

測試規格

- 在授權期間內對指定電子郵件帳號進行多次測試
- 每帳號接收多封社交工程郵件，涵蓋本文、附件及連結三種形式

測試內容與記錄

- 郵件設計涵蓋多種類型：八卦、休閒、保健、財經、情色、新奇、時事等
- 完整記錄「郵件開啟率」及「連結點閱率」，提供行為分析報告

技術面說明：特殊測試項目

除常規資安檢測外，雲森數位亦提供針對新興威脅領域的特殊安全檢測服務，涵蓋行動裝置、物聯網及工業控制系統三大高風險環境。

行動裝置攻擊測試（Mobile）

針對智慧手機、平板電腦等移動設備的攻擊行為進行描述、分類與測試。涵蓋 iOS 及 Android 作業系統的應用程式安全性、設備配置及資料洩漏風險評估。

IoT 攻擊測試

物聯網裝置的弱點與漏洞攻擊測試。由於 IoT 裝置普及，攻擊者易利用其安全缺陷進行入侵、資料竊取及拒絕服務攻擊，需要專業的檢測方法論。

OT 工業控制系統攻擊測試

針對工業控制系統（ICS）、自動化系統、智能電網等 OT 環境進行安全評估。OT 環境對實時性、可靠性要求極高，需專用測試方法確保不影響業務連續性。

攻防演練：概念與角色定義

攻防演練（紅藍對抗）是模擬真實網路安全威脅的測試方法，透過攻守雙方的實際對抗，協助組織全面了解資安防禦缺口，強化整體安全能力。

攻防演練的三大角色

🔴 紅隊（攻擊方）

模擬黑客及惡意攻擊者行為，主動尋找並利用系統、網路或應用程式漏洞進行滲透。目標為突破防線，達成攻擊任務（如竊取敏感資訊、取得系統控制權）。使用技術包含社交工程、漏洞利用、網路釣魚等。

🔵 藍隊（防守方）

負責保護系統、偵測並應對紅隊攻擊。透過監控網路流量、分析日誌、管理安全策略阻止攻擊，運用防火牆、IDS/IPS、EDR 等工具即時反應，並根據紅隊行動動態調整防禦策略。

⚪ 白隊（觀察者／裁判）

負責規劃、協調及評估整個演練過程（選配）。設定演練規則與目標，確保演練公平性與規範性，避免對實際業務造成不必要干擾，並於演練結束後給出專業評估與改善建議。

攻防演練的五大目的

評估安全狀況

透過實際攻擊模擬找出系統潛在弱點，了解組織在面對真實攻擊時的防禦能力與應變速度。

提升安全意識

讓防守方了解真實攻擊手法，提升全體員工的資安意識及面對社交工程等攻擊時的應對能力。

改進安全防禦措施

根據演練結果改進安全策略，部署更有效的防護技術，強化防守團隊的技術能力與應變流程。

應急響應能力測試

驗證組織應急響應計畫的有效性，確認在遭遇攻擊時能迅速響應並最小化業務損失。

合規性驗證

攻防演練是驗證安全系統符合 ISO 27001、NIST 等標準合規要求的重要手段之一。

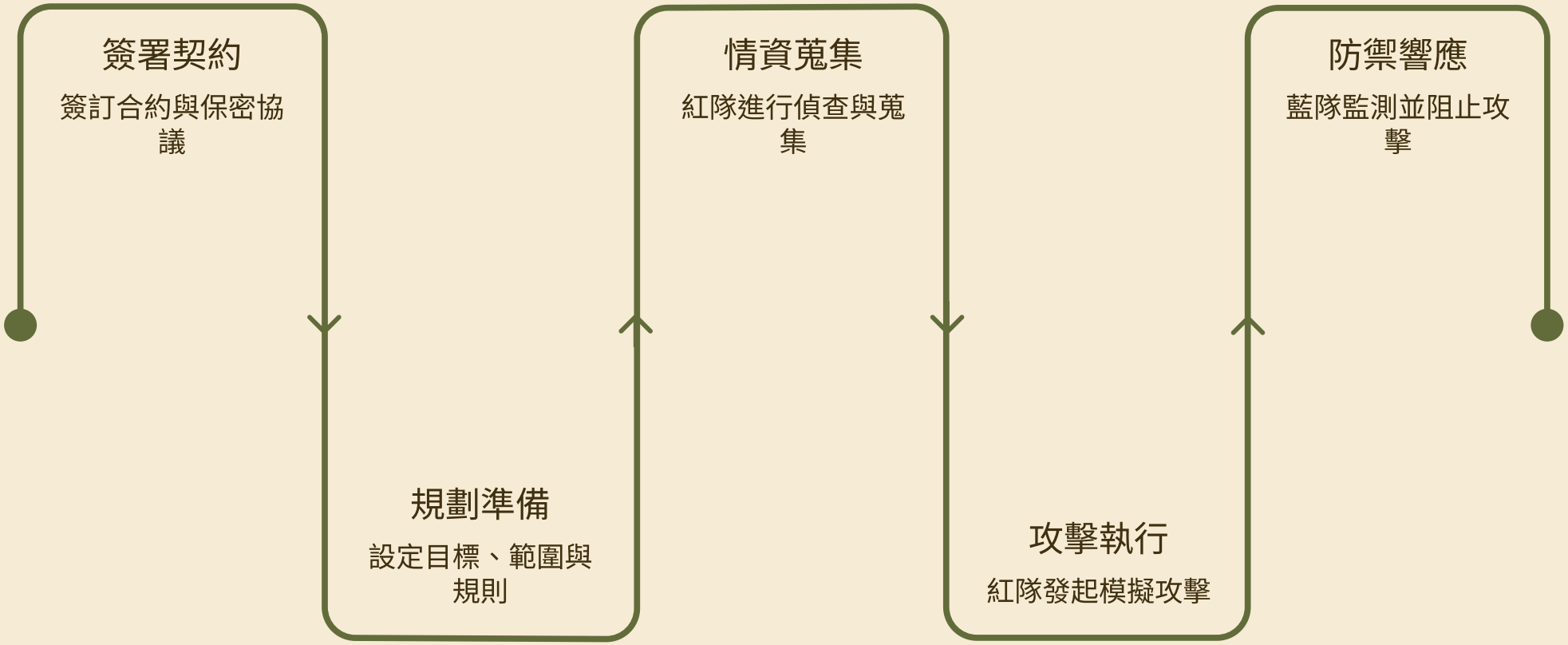
攻防演練的五種方案選擇

在不影響企業正常營運的前提下，雲森數位提供五種攻防演練方案，依客戶規模、需求及時間預算量身選擇最適合的演練模式。

紅隊模式	適用對象	演練目標	演練時間	目的與特點
遠端攻擊（無限制）	大型集團、上市櫃公司	核心資產系統	演練1~3月；專案4~16月	全方位找出最多可被入侵方式及0-day攻擊
遠端或內網（已知攻擊手法）	大型企業、一般中小企業	核心資產系統	演練1~2月；專案3~10月	測試突破防線方式及受損程度
持續性攻擊劇本	一般中小企業	協助建置測試標靶	演練1~3週；專案2~6月	考驗藍隊網路及系統防護成熟度
持續性特定劇本	一般中小企業	客戶定義的重要系統	演練1~5天；專案1~2月	模擬特定攻擊手法，考驗藍隊防護能力
加密勒索攻擊演練	擔心遭加密勒索的單位	協助建置測試標靶	演練1~5天；專案1~2月	模擬勒索攻擊，考驗藍隊防護與應變能力

演練過程不提供即時 log，不進行通報，結束後統一撰寫完整報告書，確保演練的獨立性與客觀性。

攻防演練標準流程



完整的攻防演練涵蓋從合約簽署、目標設定、情資蒐集、攻擊執行、防禦響應到最終報告的全流程管理，確保演練結果具有實際參考價值與改善依據。

管理面說明

ISMS 資訊安全管理制度簡史

ISO/IEC 27001 是全球最廣泛採用的資訊安全管理系統國際標準，歷經近三十年演進，持續強化對現代資安威脅的應對能力。

1995

英國 BSI 訂定 BS7799 Part 1

2000

BS7799 Part 1 成為 ISO/IEC 17799 國際標準

2005

ISO/IEC 27001 正式發布成為國際標準

2013

控制措施重整為 114 項，新增密碼學與供應商管理

2022

ISO/IEC 27001:2022 及 27002:2022 最新版發布

2023

CNS 27001:2023 及 27002:2023 台灣國家標準同步發布

認可組織與驗證機構體系

認可組織（Accreditation Body）

負責授予驗證組織執行認證的資格與能力認可：

- **UKAS** — 英國認可服務機構
- **ANAB** — 美國國家認可局
- **TAF** — 台灣財團法人全國認證基金會

驗證組織（Certification Body）

經認可組織授權，執行 ISO 27001 等標準之稽核與認證：

- **BSI** — 英國標準協會
- **SGS** — 台灣檢驗科技
- **AFNOR** — 法國標準協會
- **TÜV** — 台灣德國萊因技術監護顧問
- **TCIC** — 環奧國際驗證
- **ARES** — 亞瑞士

ISO/CNS 27001:2022

ISMS 導入步驟

雲森數位依據 ISO/CNS 27001:2022 標準，提供系統化的八步驟 ISMS 導入服務，協助客戶從零開始建立完整資訊安全管理制度。

步驟一　制訂資安政策

確立最高管理層對資安的承諾與方向

步驟二　定義 ISMS 範圍

明確界定資訊安全管理系統適用的業務範圍與組織邊界

步驟三　進行風險評鑑

識別資訊資產、威脅與弱點，評估風險等級

步驟四　進行風險管理

選擇適當的風險處理方式：接受、降低、轉移或規避

步驟五　制訂程序與規範

建立資安相關程序文件、作業規範及參考相關法規要求

步驟六　資安設備建置

導入必要的資安技術控制措施及實體環境安全改善

步驟七　災害演練與 BCP 演練

執行業務持續計畫（BCP）及資安事件應變演練，驗證應急能力

步驟八　認證程序

由第三方公正單位到場進行正式稽核與認證頒發

管理面：ISMS 三年輔導驗證規劃

雲森數位提供完整的三年 ISMS 輔導服務，由受過 ISO/CNS 27001:2022 資格認可的專業人員每月赴客戶現場執行，確保管理制度的持續有效性。

第一年　建制與認證

- 優化資安政策、目標及安全管理組織
- ISO 27001 差異化分析作業
- 資訊資產盤點與風險評估
- ISMS 暨 PIMS 四階管理文件建立
- BCP 建立、測試及演練
- 執行 ISMS 內稽作業
- 協助召開 ISMS 管理審查會議
- ISMS 外稽陪同及缺失改善

第二年　維護與優化

- 管理制度維護及優化服務
- ISMS 維護服務（含文件更新）
- 外部稽核陪同及缺失改善
- 年度監督稽核支援

第三年　續評與精進

- 管理制度維護及優化服務
- ISMS 維護服務（含制度精進）
- 外部稽核陪同及缺失改善
- 協助三年重新認證（Re-certification）

CHAPTER 04

特殊事件處理：加密勒索事件

當企業遭受加密勒索攻擊，雲森數位提供從事故通報、資料鑑識、解密嘗試、談判斡旋到贖金代付的完整事件應變服務，協助客戶在最短時間內恢復業務運營。

1

嘗試檔案復原

人工嘗試復原已遭加密的資料庫、虛擬機及一般性檔案

2

談判斡旋

代為與駭客聯繫，進行談判並協助降低贖金金額

3

付款及復原

加密貨幣代付購買解密金鑰，並協助系統環境復原

加密勒索事件作業流程

事故通報

填寫環境狀態履歷表

出勤評估

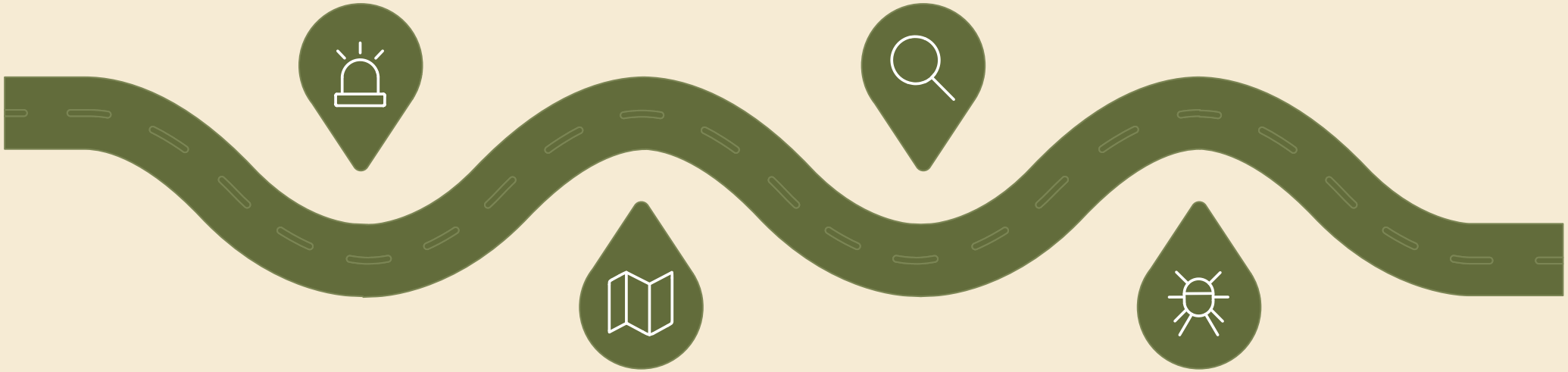
評估並收取出勤調查費

事件分析

環境備份與磁碟救援

漏洞與惡意程式

尋找漏洞與移除惡意程式



提升解密數據完整性的關鍵事項

在加密勒索事件發生後，被勒索者能否提供以下關鍵資訊，將直接影響資料救援後的完整性與復原率。請務必在聯繫我們前預先確認以下事項。

提供駭客聯繫資訊與加密樣本

提供被加密資料夾內的 ***.html 或 *.txt** 檔案（駭客聯繫資訊），以及任一個附檔名已被加密的檔案樣本，作為識別勒索病毒種類的依據。

提供舊版資料庫備份檔案

若能提供事發前的資料庫備份（**DB 複製檔、Dbdump** 或任何第三方備份工具的歷史備份），可大幅提升資料還原的完整性與準確性。

提供乾淨的資料庫庫結構

若無任何歷史備份，可提供該資料庫的**全新安裝「庫結構」**（無資料的乾淨結構），工程師可以此為基礎進行部分資料還原作業。

加密勒索檔案復原服務

提供人工破解各類型已遭加密檔案的專業服務，涵蓋四大主要檔案類別，協助企業在無需支付贖金的情況下嘗試恢復資料。

資料庫檔案格式

SQL、Oracle、MySQL、Exchange 及各類資料庫格式均可嘗試檔案復原，為資安事件中最高優先復原目標。

虛擬機底層加密

.VMDK、.VHD 等虛擬機底層遭加密導致無法開機，但虛擬機內部（C:/D:）資料庫實際未加密，可直接提取復原。

虛擬機雙層加密

虛擬機底層及內部作業系統均遭加密的情況，工程師可對底層檔案復原後，再對內部資料庫檔案進行第二次人工檔案復原。

一般性檔案

.pdf、.doc、*.xls、*.ppt、*.mp4 等一般類型檔案，較舊款勒索病毒加密者，工程師可協助使用市面檔案復原工具嘗試破解取回。

加密勒索斡旋與談判服務

當加密檔案無法透過技術手段直接解密時，雲森數位提供專業的駭客談判斡旋服務，協助降低贖金金額，並透過安全合規的渠道代付加密貨幣取得解密金鑰。

需透過談判處理的情境

- 一般性檔案（pdf/doc/xls/ppt/mp4等）遭 **LockBit 3.0** 加密破壞機制感染，無法直接破解
- 資料庫檔案（SQL/Oracle/MySQL/Exchange等）遭 **LockBit 3.0** 類型加密，破壞機制無法繞過
- 遭 **RansomHub 或其他新型態**加密勒索攻擊，目前技術上無法破解，只能透過斡旋談判支付贖金取得金鑰

加密貨幣代收代付服務

針對企業遭受加密勒索需緊急購買大額加密貨幣的情境，雲森數位提供合規、安全的加密貨幣代收代付服務，協助企業在最短時間內完成贖金支付流程。

服務條件與規範

- 交易必須文件：商業服務合約、洗錢防制聲明、保密切結書
- 交易時間限制：上班日 **上午9:00～14:00**（配合銀行作業）
- 開立全額**三聯式商業發票**，符合企業財務合規要求

報價模式

依照當日加密貨幣兌換匯率加上手續費進行報價。每筆服務費依據：

- 購買的目標加密貨幣數量
- 或轉換成台幣的最終金額
- 參照當日美金匯率及加密貨幣匯率
- 以新台幣為基準進行服務報價

加密貨幣代付流程

加密貨幣代收代付服務提供企業在緊急勒索事件中，一個合法、安全、可稽核的資金流動渠道，避免企業直接接觸高風險的暗網交易環境，同時確保整體交易過程符合台灣洗錢防制法規要求。

以攻擊者的角度，協助做有效的資安方案！

雲森數位以獨特的「攻擊者視角」為核心價值，跳脫傳統防守思維，主動識別客戶資安環境中最真實的威脅面，提供最具針對性、最有效的資安防護方案。

聯絡我們

雲森數位有限公司

Cloud 3w Co. Ltd

Cyber Security & Intelligence Agency, Taiwan

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

證書：114-IS-1-90619855-0069
