PCI DSS Assessment / Technical Audit

Customer：Canlead International Co., Ltd.

Date: 2025-05-12

v1.0

1. 環境檢視

掃描使用主機 (共 2 台)

Server 1 IP: 210.71.170.246

Server 1 User: securevectors

Server 2 IP: 54.178.41.188

Server 2 User: pcidss

主機規格:

OS: Ubuntu 24

Spec: 2 core, 8G RAM, 50G Disk

防火牆規則：

|  |  |  |  |
| --- | --- | --- | --- |
| From | To | Service ports | 用途 |
| 安律辦公室 | 掃描使用主機 | port 22/ssh | For 機器連線使用 |
| 掃描使用主機 | internet | port 80, 443 | For 機器設定安裝使用 |
| 所有內部網段 | 掃描使用主機 | port 22/sftp | For收集主機檢查結果使用 |
| 掃描使用主機 | 所有內部網段 | port ALL | For執行掃描使用 |

\*\*\* 連線白名單 IP (安律辦公室): 122.116.225.155, 60.250.130.225, 13.228.126.249

1. 參考資料

現行主機資訊參考「機器\_網段清單.xlsx」一張含有 文字, 字型, 螢幕擷取畫面, Rectangle 的圖片

AI 產生的內容可能不正確。以及下述各主機掃描結果進行比對。

|  |  |  |
| --- | --- | --- |
| 掃描 Server 1 | 掃描 Server 2 | 手動回傳 Report.zip |
| 一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片  AI 產生的內容可能不正確。 | 一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片  AI 產生的內容可能不正確。 | 一張含有 文字, 螢幕擷取畫面, 功能表, 文件 的圖片  AI 產生的內容可能不正確。 |

主機掃描摘要參考「consolidated\_system\_check\_report\_20250425\_121411.html」。一張含有 文字, 字型, 螢幕擷取畫面, 圖形 的圖片

AI 產生的內容可能不正確。

1. 掃描結果

3.1 雲端主機 (AWS)

|  |  |  |  |
| --- | --- | --- | --- |
| 雲端 (AWS) | | | |
| 10.0.0.0/24 | 10.0.9.0/24 | 10.0.3.0/24 | 10.0.1.0/24 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項目名稱 | IP | 所屬機房 | 網段/Zone | 狀態 |
| Web Server | 10.0.0.111 | AWS | 10.0.0.0/24 | 已檢查設置 |
| Web Server | 10.0.0.112 | AWS | 10.0.0.0/24 | 已檢查設置 |
| Web Server | 10.0.0.113 | AWS | 10.0.0.0/24 | 已檢查設置 |
| Web Server | 10.0.0.114 | AWS | 10.0.0.0/24 | 已檢查設置 |
| Active Directory | 10.0.0.100 | AWS | 10.0.0.0/24 | 已檢查設置 |
| 2FA Server | 10.0.0.10 | AWS | 10.0.0.0/24 | 排除檢查 (OS 不可控) |
| JUMP Server | 10.0.9.100 | AWS | 10.0.9.0/24 | 已檢查設置 |
| FTP Server | 10.0.0.200 | AWS | 10.0.0.0/24 | 已檢查設置 |
| FTP Server | 10.0.0.4 | AWS | 10.0.0.0/24 | 已檢查設置 |
| Mail Server | 10.0.0.6 | AWS | 10.0.0.0/24 | 已檢查設置 |
| FIM Server (ip-10-0-0-12) | 10.0.0.12 | AWS | 10.0.0.0/24 | 已檢查設置 |
| API Server | 10.0.3.120 | AWS | 10.0.0.0/24 | 已檢查設置 |
| API Server | 10.0.3.121 | AWS | 10.0.3.0/24 | 已檢查設置 |
| API Server | 10.0.3.122 | AWS | 10.0.3.0/24 | 已檢查設置 |
| MS SQL Server | 10.0.1.204 | AWS | 10.0.1.0/24 | 已檢查設置 |
| EIP Server | 10.0.0.98 | AWS | 10.0.0.0/24 | 已檢查設置 |

|  |  |
| --- | --- |
| **合規調整相關** | |
| **符合密碼原則**  未密碼原則(長度需為十二碼以上且英數字混合、新密碼不得與前四次密碼相同、最長使用時間90天) | AWS-DB1  EC2AMAZ-3CUKPHR  EC2AMAZ-3CUKPHR\_121  EC2AMAZ-5RNE6MK  EC2AMAZ-C87353G  EC2AMAZ-FO9SBK8  EC2AMAZ-L5S1NDE  (ip-10-0-0-12)  WEB1  WEB2  WEB3  WEB4 |
| **符合帳戶的鎖定原則**  未符合帳戶的鎖定原則(錯誤不可超過 10 次、帳戶鎖定解除不少於 30 分鐘 或是手動解除) | EC2AMAZ-3CUKPHR  EC2AMAZ-3CUKPHR\_121  EC2AMAZ-5RNE6MK  EC2AMAZ-C87353G  EC2AMAZ-FO9SBK8  EC2AMAZ-L5S1NDE  EC2AMAZ-Q3KNMMR  (ip-10-0-0-12)  WEB1  WEB2  WEB3  WEB4 |
| **符合帳戶閒置自動登出**  未符合帳戶閒置自動登出或超過15分鐘 | EC2AMAZ-BEI6GLN |

|  |  |
| --- | --- |
| **建議確認事項** | |
| **預設帳號關閉**  如無使用, 建議可關閉預設帳號如 (Guest, DefaultAccount, etc.) | ADServer01 |
| **Windows Update 紀錄**  偵測到大於 90 天未更新，建議可定期檢視微軟 Windows Update 是否有 Critical Patch 可更新。 | AWS-DB1  EC2AMAZ-5RNE6MK  EC2AMAZ-BEI6GLN  EC2AMAZ-L5S1NDE  WEB1  WEB2  WEB3  WEB4 |

3.2 地端主機

|  |  |  |  |
| --- | --- | --- | --- |
| 地端 | | | |
| 192.168.4.0/24 | 192.168.9.0/24 | 192.168.8.0/24 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項目名稱 | IP | 所屬機房 | 網段/Zone | 狀態 |
| Batch Server | 192.168.9.195 | Local | 192.168.9.0/24 | 已檢查設置 |
| Firewall | 192.168.0.254 | Local | 192.168.0.0/24 | 排除檢查 (OS 不可控) |
| Firewall | 192.168.3.254 | Local | 192.168.3.0/24 | 排除檢查 (OS 不可控) |
| Firewall | 192.168.6.254 | Local | 192.168.6.0/24 | 排除檢查 (OS 不可控) |
| Log Server | 192.168.9.190 | Local | 192.168.9.0/24 | 排除檢查 (OS 不可控) |
| Accountant | 192.168.8.74 | Local | 192.168.8.0/24 | 已檢查設置 |
| Accountant | 192.168.8.78 | Local | 192.168.8.0/24 | 已檢查設置 |
| Accountant | 192.168.8.79 | Local | 192.168.8.0/24 | 已檢查設置 |
| Accountant | 192.168.8.80 | Local | 192.168.8.0/24 | 已檢查設置 |
| Accountant | 192.168.8.81 | Local | 192.168.8.0/24 | 已檢查設置 |
| Accountant | 192.168.8.88 | Local | 192.168.8.0/24 | 已檢查設置 |
| 語音交換機主機 | 192.168.4.10 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |
| 語音交換機主機(主) | 192.168.4.11 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |
| 語音交換機主機(備) | 192.168.4.12 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |
| 語音客服系統(主) | 192.168.4.13 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |
| 語音客服系統(備) | 192.168.4.14 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |
| WebCall | 192.168.4.15 | Local | 192.168.4.0/24 | 排除檢查 (OS 不可控) |

|  |
| --- |
| **合規調整相關** |
| **N/A** |

|  |  |
| --- | --- |
| **建議確認事項** | |
| **USER8088 (192.168.8.88)** | * SMBv1狀態為 '已啟用' (應為 '停用') * 發現風險接聽埠: 445 * 安全開機狀態為 '已停用' (應為 '啟用')   TPM狀態異常: 'False' (應為存在且運作正常) |

3.3 地端主機 (CS)

|  |  |  |  |
| --- | --- | --- | --- |
| 地端 | | | |
| 192.168.3.0/24 |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項目名稱 | IP | 所屬機房 | 網段/Zone | 狀態 |
| CustomerService | 192.168.3.100 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.101 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.102 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.103 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.104 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.105 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.106 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.137 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.174 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.176 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.178 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.179 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.181 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.183 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.186 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.187 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.189 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.193 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.201 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.21 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.22 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.221 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.223 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.24 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.25 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.26 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.27 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.29 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.30 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.32 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.34 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.35 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.36 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.37 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.39 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.40 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.41 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.42 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.43 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.44 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.45 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.46 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.47 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.48 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.49 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.51 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.54 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.55 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.56 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.57 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.58 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.59 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.6 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.60 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.62 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.63 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.64 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.65 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.66 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.68 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.69 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.70 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.71 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.72 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.73 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.74 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.75 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.76 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.77 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.78 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.79 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.82 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.84 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.85 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.88 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.89 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.92 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.93 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.94 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.96 | Local | 192.168.3.0/24 | 已檢查設置 |
| CustomerService | 192.168.3.98 | Local | 192.168.3.0/24 | 已檢查設置 |

|  |
| --- |
| **合規調整相關** |
| **N/A** |

|  |  |
| --- | --- |
| **建議確認事項** | |
| UAC 已停用 | USER3055 (192.168.3.55) |
| 防火牆未完全啟用 | USER3028 (192.168.3.28) |
| Windows更新不活躍 | USER3095 (192.168.3.95) |
| SMBv1協議未停用 | USER3021 (192.168.3.21)  USER3022 (192.168.3.22)  USER3025 (192.168.3.25)  USER3027 (192.168.3.27)  USER3028 (192.168.3.28)  USER3029-2 (192.168.3.29)  USER3032 (192.168.3.32)  USER3035 (192.168.3.35)  USER3036 (192.168.3.36)  USER3038 (192.168.3.38)  USER3041 (192.168.3.41)  USER3043 (192.168.3.43)  USER3048 (192.168.3.48)  USER3058 (192.168.3.58)  USER3060 (192.168.3.60)  USER3063 (192.168.3.63)  USER3065 (192.168.3.65)  USER3066 (192.168.3.66)  USER3070 (192.168.3.70)  USER3072 (192.168.3.72)  USER3077 (192.168.3.77)  USER3082 (192.168.3.82)  USER3084 (192.168.3.84)  USER3089 (192.168.3.89)  USER309 (192.168.3.137)  USER3095 (192.168.3.95)  USER3098 (192.168.3.98)  USER3101 (192.168.3.101) |

* 1. 雲端環境

**AWS Account:** 366205796862

**Report Generated:** 2025-05-08 09:36:30

**Regions Checked:** Current region (ap-northeast-1 only). Use --all-regions for a complete scan.

一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

AI 產生的內容可能不正確。

|  |
| --- |
| **合規調整相關** |
| **Requirement 1: Install and maintain network security controls**  **1.i Firewall Rules - Unrestricted Access**  ✗ FAIL: Found **64 non-compliant** security groups with unrestricted access  **1.ii Publicly Exposed Protocols**  ✗ FAIL: Found **51 non-compliant** security groups with publicly exposed protocols  **Requirement 4: Protect cardholder data with strong cryptography**  **4.ii Weak Ciphers**  ✗ FAIL: Found **1 non-compliant** load balancers using weak ciphers  **Requirement 8: Identify users and authenticate access**  **8.i Password Policy**  ✗ FAIL: Found **Some non-compliant** IAM password policies  **8.ii MFA Enforcement**  ✗ FAIL: Found **11 non-compliant** IAM users without MFA  **Requirement 10: Log and monitor all access**  **10.i Log Retention**  ✗ FAIL: Found **4 non-compliant** log buckets without 1-year retention |

|  |
| --- |
| **建議確認事項** |
| N/A |

雲端掃描摘要參考「pci\_dss\_v4\_compliance\_report.html」。一張含有 文字, 字型, 螢幕擷取畫面, 圖形 的圖片

AI 產生的內容可能不正確。

1. 總結摘要

|  |  |
| --- | --- |
| **目前範圍內是否有範圍外的主機出現** | **通過**  尚未發現未授權主機。 |
| **是否有「合規調整相關」內容須修正** | **需要修正/或確認**  雲端環境  部分Firewall Rules, Weak Ciphers, Password Policy, MFA Enforcement, Log Retention 需確認。  主機環境  部分主機可能不滿足以下需求。  未密碼原則(長度需為十二碼以上且英數字混合、新密碼不得與前四次密碼相同、最長使用時間90天)  未符合帳戶的鎖定原則(錯誤不可超過 10 次、帳戶鎖定解除不少於 30 分鐘 或是手動解除)  未符合帳戶閒置自動登出或超過15分鐘 |
| **是否有「建議確認事項」內容須確認** | **需要修正/或確認**  部分主機可能需確認以下事項。  SMBv1狀態為 '已啟用' (應為 '停用')  發現風險接聽埠: 445  UAC 已停用  防火牆未完全啟用  Windows更新不活躍  其他建議確認事項。  預設帳號關閉, 如無使用, 建議可關閉預設帳號如 (Guest, DefaultAccount, etc.)  Windows Update 紀錄, 偵測到大於 90 天未更新，建議可定期檢視微軟 Windows Update 是否有 Critical Patch 可更新。 |
|  |  |
|  |  |