# Technical Security Audit Report

**Client:** Canlead International Co., Ltd.  
**Date:** 2025-05-16  
**Version:** 1.0  
**Assessment Period:** 2025-04-25 to 2025-05-12

## Executive Summary

### Key Security Findings

| Security Category | Critical | High | Medium | Low |
| --- | --- | --- | --- | --- |
| Network Exposure | 2 | 3 | 1 | 0 |
| Access Control | 1 | 1 | 2 | 0 |
| Authentication | 1 | 2 | 1 | 0 |
| Encryption | 0 | 1 | 0 | 0 |
| Configuration | 0 | 2 | 3 | 1 |
| Patching/Updates | 0 | 1 | 8 | 0 |
| Logging/Monitoring | 1 | 0 | 0 | 0 |
| **TOTAL** | **5** | **10** | **15** | **1** |

### Most Critical Security Issues

1. **Widespread unrestricted internet access**
   * 64 security groups with 0.0.0.0/0 access rules identified
   * 3 security groups allowing ALL TRAFFIC from any source
   * Critical services (databases, admin interfaces) directly exposed to the internet
2. **Extensive insecure protocol exposure**
   * 51 security groups allowing insecure protocols from the public internet
   * FTP, Telnet, unencrypted database access (MySQL, MSSQL) publicly accessible
   * Remote administration protocols (SSH, RDP) open to the internet
3. **Inadequate authentication security**
   * 11 IAM users without MFA enabled (2 with console access)
   * Non-compliant password policies on multiple systems
   * Missing account lockout controls on 11 cloud systems
4. **Insufficient logging retention**
   * CloudTrail logs without retention policies
   * Application logs with as little as 14 days retention
   * Missing centralized log management

### Prioritized Security Improvements

| Priority | Critical Actions |
| --- | --- |
| Critical | • Remove ALL TRAFFIC rules from sg-0fa30e9feec49f425, sg-ac1ad1cb, and sg-6fdb1208• Restrict database access (port 3306, 1433) to specific IP ranges• Enable MFA for Johnny\_howcool and mgc.paul.dev@gmail.com users |
| High | • Configure AWS CloudTrail and S3 log retention for 365+ days• Implement proper network segmentation using jump server at 10.0.9.100• Update load balancer “canlead” SSL policy to remove weak ciphers• Disable SMBv1 on all customer service workstations |
| Medium | • Replace FTP servers with SFTP• Implement centralized log management• Deploy uniform password and account lockout policies• Update Windows systems with critical security patches |

## 1. Assessment Scope and Methodology

### 1.1 Environments Assessed

**Cloud Environment:** - AWS Account: 366205796862 (ap-northeast-1 region) - 4 VPCs (10.0.0.0/24, 10.0.1.0/24, 10.0.3.0/24, 10.0.9.0/24) - 15 cloud servers including web, API, database, and infrastructure servers

**On-premises Environments:** - Core Network: 192.168.4.0/24, 192.168.9.0/24, 192.168.8.0/24 - Customer Service Network: 192.168.3.0/24 - 80+ systems including customer service workstations and accounting systems

### 1.2 Assessment Systems

**Scanning System Details:** | System | IP Address | User | Specifications | |——–|————|——|—————-| | Scanner 1 | 210.71.170.246 | securevectors | Ubuntu 24, 2 cores, 8GB RAM, 50GB disk | | Scanner 2 | 54.178.41.188 | pcidss | Ubuntu 24, 2 cores, 8GB RAM, 50GB disk |

**Firewall Rules for Scanners:** | From | To | Service Ports | Purpose | |——|—|—-|———| | Office IPs (122.116.225.155, 60.250.130.225, 13.228.126.249) | Scanners | 22/SSH | For system connection | | Scanners | Internet | 80, 443 | For system setup and installation | | Internal Networks | Scanners | 22/SFTP | For collecting scan results | | Scanners | Internal Networks | ALL PORTS | For scanning execution |

## 2. Critical Network Security Issues

### 2.1 Unrestricted Internet Access

#### 2.1.1 Issue Details

**Security Impact: CRITICAL**

A large number of security groups have been configured to allow unrestricted access from the internet (0.0.0.0/0), creating a substantial attack surface. Most concerning are several security groups that allow ALL TRAFFIC from any source, essentially providing no network-level protection.

| Security Group | Service/Purpose | Critical Exposures | Risk |
| --- | --- | --- | --- |
| sg-1bd4787f (allOpen) | Unknown | ALL TCP ports (0-65535) open to 0.0.0.0/0 | Extreme exposure of all services |
| sg-0fa30e9feec49f425 | CentOS 7 | ALL TRAFFIC (ALL PORTS) to 0.0.0.0/0 | Complete system exposure |
| sg-ac1ad1cb | Windows Nano | ALL TRAFFIC (ALL PORTS) to 0.0.0.0/0 | Complete system exposure |
| sg-6fdb1208 (idanbean\_windows) | Windows | ALL TRAFFIC (ALL PORTS) to 0.0.0.0/0 | Complete system exposure |
| sg-36048f51 (launch-wizard-7) | Unknown | ALL TCP ports (0-65535) to 0.0.0.0/0 | Extreme exposure of all TCP services |
| sg-02da57be4258f2acb (launch-wizard-11) | Unknown | ALL TCP ports (0-65535) to 0.0.0.0/0 | Extreme exposure of all TCP services |

**Additional Findings:** - 58 additional security groups with more targeted but still concerning internet exposure - Multiple database access ports (3306, 1433) directly exposed to the internet - Administration interfaces publicly accessible

#### 2.1.2 Remediation Steps

1. **Priority Actions:**
   * Remove ALL TRAFFIC allow rules from sg-0fa30e9feec49f425, sg-ac1ad1cb, and sg-6fdb1208
   * Replace 0.0.0.0/0 with specific IP allow lists for all necessary external access
   * Restrict database ports (3306, 1433) to internal access only
2. **Additional Improvements:**
   * Utilize the existing jump server (10.0.9.100) for administrative access
   * Implement security group referencing instead of direct internet access
   * Document all required external access with business justification
3. **Technical Implementation:**

* # Example AWS CLI command to remove all traffic rule  
  aws ec2 revoke-security-group-ingress \  
   --group-id sg-0fa30e9feec49f425 \  
   --protocol all \  
   --cidr 0.0.0.0/0  
    
  # Example to add restricted access  
  aws ec2 authorize-security-group-ingress \  
   --group-id sg-0fa30e9feec49f425 \  
   --protocol tcp \  
   --port 443 \  
   --cidr 122.116.225.155/32

### 2.2 Insecure Protocols Exposed

#### 2.2.1 Issue Details

**Security Impact: CRITICAL**

51 security groups allow access to known insecure protocols directly from the internet. These protocols often transmit data in cleartext or have known vulnerabilities, creating significant security risks.

| Protocol | Exposure | Security Risk |
| --- | --- | --- |
| FTP (TCP/21) | 9 security groups | Plaintext authentication and data transfer |
| SSH (TCP/22) | 42 security groups | Common target for brute force attacks |
| Telnet (TCP/23) | 6 security groups | Plaintext transmission of credentials and data |
| SMTP (TCP/25) | 7 security groups | Potential mail relay abuse if not secured |
| MySQL (TCP/3306) | 11 security groups | Unencrypted database access |
| MSSQL (TCP/1433) | 8 security groups | Potential SQL injection and data exposure |
| RDP (TCP/3389) | 10 security groups | Target for brute force attacks |

**Most Concerning Examples:** - sg-0f1c8699dd4f51575 (SG-MailServer): Exposing POP3, SMTP, and IMAP directly to internet - sg-0545ed506b8930369: Exposing FTP (both TCP/UDP) to internet - sg-0ffddcd33ce3db48c (Canlead Mail Server): Multiple mail protocols exposed

#### 2.2.2 Remediation Steps

1. **Priority Actions:**
   * Restrict access to these protocols to specific IP ranges
   * For FTP servers (10.0.0.200, 10.0.0.4): Migrate to SFTP or implement TLS
2. **Additional Improvements:**
   * Replace FTP with SFTP/FTPS for all file transfers
   * Implement TLS for mail services
   * Configure SSH to use key-based authentication only
   * Deploy VPN or jump server architecture for administrative access
   * Implement just-in-time access for RDP connections
3. **Technical Guidance:**
   * For FTP servers: Configure vsftpd with TLS or migrate to SFTP
   * For mail servers: Configure TLS with proper certificates
   * For database access: Implement SSL/TLS connections, restrict to VPN access

## 3. Authentication and Access Control Issues

### 3.1 Missing Multi-Factor Authentication

#### 3.1.1 Issue Details

**Security Impact: CRITICAL**

11 AWS IAM users lack MFA protection, creating significant risk of account compromise. Two users have console access without MFA, presenting the highest risk.

| User | Access Type | Last Console Login | Active Access Keys | Risk Factors |
| --- | --- | --- | --- | --- |
| Johnny\_howcool | Console | 2024-12-10 | 1 (unused since Mar 2023) | • Console access without MFA• Unused access key |
| mgc.paul.dev@gmail.com | Console | 2024-05-30 | 2 (one used Oct 2024) | • Console access without MFA• Multiple access keys |
| callcarbar | API only | N/A | 1 (active, used Apr 2024) | • Long-term key since 2017• No key rotation |
| roamingbar | API only | N/A | 2 (both active) | • Multiple active keys• No key rotation since 2016 |
| s3 | API only | N/A | 1 (active, used May 2025) | • Long-term key since 2015• No key rotation |

**Additional Issues:** - 6 other service accounts without MFA - Multiple stale access keys that remain active - No clear access key rotation policy

#### 3.1.2 Remediation Steps

1. **Priority Actions:**
   * Enable MFA for Johnny\_howcool and mgc.paul.dev@gmail.com
   * Rotate or disable unused access keys
   * Validate necessity of all service accounts
2. **Technical Implementation:**

* # Check MFA status  
  aws iam list-virtual-mfa-devices  
    
  # Find inactive access keys  
  aws iam list-access-keys --user-name Johnny\_howcool  
  aws iam get-access-key-last-used --access-key-id AKIAVKQ4RAH7GYHPJBIZ  
    
  # Deactivate unused access key  
  aws iam update-access-key \  
   --access-key-id AKIAVKQ4RAH7GYHPJBIZ \  
   --status Inactive \  
   --user-name Johnny\_howcool

### 3.2 Insufficient Password Policies

#### 3.2.1 Issue Details

**Security Impact: HIGH**

Multiple systems have inadequate password policies that fail to enforce industry standard security practices. This increases the risk of password-based attacks.

**Cloud Systems with Non-Compliant Password Policies:** - AWS-DB1 - EC2AMAZ-3CUKPHR - EC2AMAZ-3CUKPHR\_121 - EC2AMAZ-5RNE6MK - EC2AMAZ-C87353G - EC2AMAZ-FO9SBK8 - EC2AMAZ-L5S1NDE - ip-10-0-0-12 - WEB1, WEB2, WEB3, WEB4

**Password Policy Deficiencies:** - Insufficient minimum length (less than 12 characters) - Missing complexity requirements (no alphanumeric mix) - No password history enforcement (allow reuse of recent passwords) - Maximum age exceeding 90 days

#### 3.2.2 Remediation Steps

1. **Priority Actions:**
   * Document current password policy settings across all systems
   * Prioritize policy updates for critical systems
2. **Technical Implementation:**

* # Example PowerShell command for Windows systems  
  Net Accounts /MINPWLEN:12 /MAXPWAGE:90 /UNIQUEPW:5  
    
  # For Active Directory  
  Set-ADDefaultDomainPasswordPolicy -Identity yourdomain.com `  
   -MinPasswordLength 12 `  
   -PasswordHistoryCount 5 `  
   -MaxPasswordAge 90.00:00:00 `  
   -ComplexityEnabled $true

### 3.3 Account Lockout Policy Issues

#### 3.3.1 Issue Details

**Security Impact: HIGH**

12 cloud systems lack proper account lockout policies, making them vulnerable to brute force password attacks.

**Affected Systems:** - EC2AMAZ-3CUKPHR - EC2AMAZ-3CUKPHR\_121 - EC2AMAZ-5RNE6MK - EC2AMAZ-C87353G - EC2AMAZ-FO9SBK8 - EC2AMAZ-L5S1NDE - EC2AMAZ-Q3KNMMR - ip-10-0-0-12 - WEB1, WEB2, WEB3, WEB4

**Policy Deficiencies:** - Missing account lockout after failed attempts - Lockout threshold higher than 10 attempts - Lockout duration less than 30 minutes

#### 3.3.2 Remediation Steps

1. **Priority Actions:**
   * Configure account lockout policies on all systems
   * Prioritize systems with internet-facing services
2. **Technical Implementation:**

* # Example PowerShell for Windows systems  
  Net Accounts /LOCKOUTTHRESHOLD:10 /LOCKOUTDURATION:30 /LOCKOUTWINDOW:30  
    
  # For Active Directory  
  Set-ADDefaultDomainPasswordPolicy -Identity yourdomain.com `  
   -LockoutThreshold 10 `  
   -LockoutDuration 0:30:0 `  
   -LockoutObservationWindow 0:30:0

## 4. System Configuration Issues

### 4.1 SMBv1 Protocol Enabled

#### 4.1.1 Issue Details

**Security Impact: HIGH**

SMBv1 is an outdated, insecure protocol vulnerable to various attacks, including the WannaCry ransomware. This protocol is enabled on multiple systems.

**Affected Systems:** - USER8088 (192.168.8.88): SMBv1 enabled with port 445 exposed - 28 customer service workstations in the 192.168.3.0/24 network, including: - USER3021 (192.168.3.21) - USER3022 (192.168.3.22) - USER3025 (192.168.3.25) - USER3027 (192.168.3.27) - [24 additional workstations listed in full report]

**Security Implications:** - Vulnerability to wormable malware (WannaCry/EternalBlue) - Lack of encryption and modern authentication - No protection against man-in-the-middle attacks

#### 4.1.2 Remediation Steps

1. **Priority Actions:**
   * Perform application compatibility testing for SMBv1 removal
   * Create group policy to disable SMBv1 on all workstations
2. **Technical Implementation:**

* # PowerShell command to disable SMBv1  
  Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

1. **Group Policy Implementation:**
   * Verify no applications require SMBv1
   * Deploy group policy to disable SMBv1
   * Monitor for attempted SMBv1 connections to identify any missed systems

### 4.2 Missing Windows Updates

#### 4.2.1 Issue Details

**Security Impact: HIGH**

Multiple systems have not received Windows updates for over 90 days, leaving them vulnerable to known security issues.

**Affected Cloud Systems:** - AWS-DB1 - EC2AMAZ-5RNE6MK - EC2AMAZ-BEI6GLN - EC2AMAZ-L5S1NDE - WEB1, WEB2, WEB3, WEB4

**Affected On-Premises Systems:** - USER3095 (192.168.3.95): Windows Update inactive

**Security Implications:** - Exposure to known vulnerabilities with available patches - Potential for exploit via unpatched security flaws - Non-compliance with security best practices

#### 4.2.2 Remediation Steps

1. **Priority Actions:**
   * Run Windows Update scan on all affected systems
   * Prioritize critical security updates for immediate installation
   * Document systems that require extended testing
2. **Technical Implementation:**

* # PowerShell commands to check for and install updates  
  Get-WindowsUpdate  
  Install-WindowsUpdate -AcceptAll

1. **Additional Improvements:**
   * Implement Windows Server Update Services (WSUS) or other patch management
   * Create maintenance windows for regular updates
   * Develop testing procedure for critical updates

### 4.3 Miscellaneous System Hardening Issues

#### 4.3.1 Issue Details

**Security Impact: MEDIUM**

Several workstations have security features disabled that should be enabled as part of standard system hardening.

**User Account Control (UAC) Disabled:** - USER3055 (192.168.3.55)

**Windows Firewall Not Fully Enabled:** - USER3028 (192.168.3.28)

**Default Accounts Not Disabled:** - ADServer01: Default accounts (Guest, DefaultAccount) not disabled

**Other Security Issues:** - USER8088 (192.168.8.88): - Secure boot disabled - TPM status abnormal - Port 445 exposed

#### 4.3.2 Remediation Steps

1. **User Account Control:**

* # Enable UAC via PowerShell  
  Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 1

1. **Windows Firewall:**

* # Enable Windows Firewall for all profiles  
  Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

1. **Default Accounts:**

* # Disable Guest account  
  Disable-LocalUser -Name "Guest"

## 5. Logging and Monitoring Issues

### 5.1 Insufficient Log Retention

#### 5.1.1 Issue Details

**Security Impact: CRITICAL**

Multiple log storage systems have insufficient retention periods, severely limiting security investigation capabilities and failing to meet industry standards.

| Log Storage | Current Retention | Required Retention | Gap |
| --- | --- | --- | --- |
| aws-cloudtrail-logs-366205796862-993f53a6 | No lifecycle policy | 365 days | Undefined retention |
| callcarbar-log | 30 days | 365 days | 335 days |
| canlead-ecs-log | 14 days | 365 days | 351 days |

**Security Implications:** - Limited ability to investigate past security incidents - Loss of valuable forensic data - Insufficient timeframe for threat detection - Non-compliance with security standards requiring 1-year retention

#### 5.1.2 Remediation Steps

1. **Priority Actions:**
   * Configure S3 lifecycle rules for CloudTrail logs bucket
   * Extend retention periods for application log buckets
2. **Technical Implementation:**

* // Example S3 lifecycle configuration  
  {  
   "Rules": [  
   {  
   "Status": "Enabled",  
   "ID": "CloudTrail-Logs-Retention",  
   "Filter": {  
   "Prefix": ""  
   },  
   "Transitions": [  
   {  
   "Days": 90,  
   "StorageClass": "STANDARD\_IA"  
   },  
   {  
   "Days": 180,  
   "StorageClass": "GLACIER"  
   }  
   ],  
   "Expiration": {  
   "Days": 365  
   }  
   }  
   ]  
  }

1. **Cost-Effective Implementation:**
   * Use S3 Intelligent-Tiering for cost optimization
   * Implement log compression for storage efficiency
   * Consider central log aggregation solution

## 6. Encryption and TLS Issues

### 6.1 Weak TLS Configuration

#### 6.1.1 Issue Details

**Security Impact: HIGH**

The “canlead” load balancer is using an outdated SSL policy (ELBSecurityPolicy-2016-08) with weak ciphers, potentially allowing downgrade attacks or use of cryptographically weak algorithms.

**Security Implications:** - Support for outdated TLS protocols - Potential for man-in-the-middle attacks - Non-compliance with current security standards

#### 6.1.2 Remediation Steps

1. **Priority Actions:**
   * Update load balancer SSL policy to ELBSecurityPolicy-TLS13-1-2-2021-06
2. **Technical Implementation:**

* # AWS CLI command to update SSL policy  
  aws elbv2 modify-listener \  
   --listener-arn <listener-arn> \  
   --ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06

1. **Verification Process:**
   * Use SSL testing tools to verify cipher strength
   * Document updated configuration
   * Implement regular checks for TLS configuration

## 7. Remediation Roadmap

### 7.1 Critical Security Improvements

| Issue | Action | Complexity | Resources |
| --- | --- | --- | --- |
| Unrestricted internet access | Remove ALL TRAFFIC rules, restrict to necessary IPs | Low | Cloud admin |
| Insecure protocols exposed | Restrict access to VPN or specific IPs | Medium | Cloud admin, network team |
| Missing MFA | Enable MFA for all users with console access | Low | Security team |
| Insufficient log retention | Configure proper log lifecycle policies | Low | Cloud admin |
| SMBv1 enabled | Disable SMBv1 on critical systems | Medium | Windows admin |

### 7.2 High Priority Improvements

| Issue | Action | Complexity | Resources |
| --- | --- | --- | --- |
| Weak TLS configuration | Update load balancer SSL policies | Low | Cloud admin |
| Account lockout policies | Implement consistent policies | Medium | Systems admin |
| Password policies | Deploy uniform password requirements | Medium | Systems admin |
| Windows updates | Apply critical security patches | Medium | Systems admin |
| Jump server implementation | Configure secure administrative access | Medium | Network team |

### 7.3 Medium Priority Improvements

| Issue | Action | Complexity | Resources |
| --- | --- | --- | --- |
| Migration to SFTP | Replace FTP with secure alternative | Medium | Systems admin |
| Windows firewall | Standardize firewall configurations | Medium | Security team |
| Default accounts | Disable or secure default accounts | Low | Systems admin |
| UAC/Secure boot | Enable security features on all systems | Medium | End-user support |
| Access key rotation | Implement key rotation policy | Medium | Cloud admin |

## 8. Appendices

### Appendix A: Detailed Security Group Findings

[Complete list of all 64 security groups with unrestricted access]

### Appendix B: Network Scan Results

[Raw scan output and technical details]

### Appendix C: Applicable Compliance Requirements

[Mapping of findings to relevant compliance standards including PCI DSS]

**Report Prepared By:**  
[Security Assessor]  
[Security Engineer]  
[Contact Information]

**Report Reviewed By:**  
[Security Team Lead]  
[Senior Security Architect]  
[Contact Information]