Scanity.ai

Pre-Insurance Security Assessment Report

TechStart Solutions Inc.

Domain: techstartsolutions.com | Scan Date: September 23, 2025 | Report ID: SAMPLE-2025-001

EXECUTIVE SUMMARY - CRITICAL ATTENTION REQUIRED

This security assessment has identified multiple critical vulnerabilities that will significantly impact your cyber insurance eligibility and premiums. Immediate remediation is required before applying for coverage. Based on our analysis, your current security posture would likely result in either coverage denial or premium increases of 300-500% above baseline rates.

SECURITY SCORE	CRITICAL ISSUES	EST. PREMIUM IMPACT
42	3	+450%
GRADE: F	IMMEDIATE ACTION	$45,000/year

CRITICAL FINDINGS - INSURANCE BLOCKERS

Remote Desktop Protocol (RDP) Exposed to Internet

CRITICAL

Port 3389 is accessible from the internet on IP 198.51.100.42. This is the #1 attack vector for ransomware and will result in immediate insurance denial or extreme premium increases.

Insurance Impact:
- Automatic denial from Coalition, At-Bay, and most carriers
- If approved: 300-500% premium increase
- May require $10M+ in ransomware coverage exclusions

Affected Systems:	198.51.100.42:3389 (DC-PROD-01)
First Detected:	Over 90 days ago (via internet-wide scan historical data)
Attack Surface:	Fully exposed, no geo-restrictions detected

Microsoft Exchange Server Vulnerable to ProxyLogon

CRITICAL

Exchange Server 2019 CU8 detected with multiple unpatched vulnerabilities including ProxyLogon (CVE-2021-26855) and ProxyShell variants. These are actively exploited in the wild.

Insurance Impact:
- Known CVEs = automatic premium increase of 200%+
- Must be patched before binding coverage
- Requires attestation of patch management program

HIGH RISK FINDINGS - PREMIUM IMPACTS

Database Ports Exposed (MySQL, PostgreSQL)

HIGH

MySQL (3306) and PostgreSQL (5432) ports are accessible from the internet. Database exposure indicates poor network segmentation and significantly increases data breach risk.

Insurance Impact:
- Premium increase of 150-200%
- May require database encryption attestation
- Increased data breach deductibles ($100K+)

Exposed Ports:	3306/tcp (MySQL), 5432/tcp (PostgreSQL)
Data Risk:	Potential PII/PCI exposure if compromised

SSL Certificate Expired

HIGH

Main domain SSL certificate expired 47 days ago. This breaks secure communications and indicates poor security hygiene and maintenance practices.

Insurance Impact:
- Shows negligent security practices
- 50-75% premium increase
- May require quarterly security attestations

MEDIUM RISK FINDINGS - COMPLIANCE ISSUES

Missing Email Security (No SPF/DMARC)

MEDIUM

No SPF or DMARC records detected. Email can be easily spoofed, increasing business email compromise (BEC) and phishing risks.

Insurance Impact:
- 25-50% premium increase for social engineering coverage
- May exclude BEC losses from coverage
- Required fix for many carriers

Outdated Web Server Software

MEDIUM

Apache 2.4.41 detected (3+ years old) with known vulnerabilities. Running outdated software demonstrates poor patch management.

TECHNICAL SCAN DETAILS

Total Open Ports **27**	Critical Ports Exposed **5**
Known CVEs **14**	Security Headers **2/8**

Port Scan Results:

22/tcp (SSH) - Open
80/tcp (HTTP) - Open
443/tcp (HTTPS) - Open
445/tcp (SMB) - Open [CRITICAL]
3306/tcp (MySQL) - Open [CRITICAL]
3389/tcp (RDP) - Open [CRITICAL]
5432/tcp (PostgreSQL) - Open [CRITICAL]
8080/tcp (HTTP-Alt) - Open
8443/tcp (HTTPS-Alt) - Open

Detected Technologies:

- Operating System: Windows Server 2019
- Web Server: Apache 2.4.41 (outdated)
- Database: MySQL 5.7.32, PostgreSQL 12.4
- Mail Server: Exchange 2019 CU8 (vulnerable)
- Framework: PHP 7.2 (end-of-life)
- CMS: WordPress 5.6 (outdated)

INSURANCE CARRIER REQUIREMENTS (2025)

Coalition: RDP must be disabled, MFA required, EDR deployment mandatory

At-Bay: No critical CVEs, email security required, 24-hour patch SLA

Corvus: Network segmentation proof, quarterly scans, incident response plan

Cowbell: Continuous monitoring required, API integration for real-time assessment

PRIORITY REMEDIATION ROADMAP

IMMEDIATE (24-48 hours):

1. Disable RDP on all internet-facing servers immediately
2. Apply critical Exchange Server security updates
3. Renew expired SSL certificates
4. Close or firewall database ports 3306, 5432

HIGH PRIORITY (1 week):

1. Implement SPF and DMARC records
2. Update Apache web server to latest version
3. Enable MFA on all administrator accounts
4. Deploy EDR solution on all endpoints

MEDIUM PRIORITY (30 days):

1. Implement network segmentation
2. Deploy security headers on all web properties
3. Establish patch management program
4. Create and test incident response plan

ESTIMATED INSURANCE IMPACT AFTER REMEDIATION

Current Premium Estimate **$45,000/yr**	After Critical Fixes **$18,000/yr**
After All Fixes **$10,000/yr**	Potential Savings **$35,000/yr**

IMPORTANT DISCLAIMERS

This is a SAMPLE REPORT showing PROFESSIONAL/COMPREHENSIVE TIER features including internet-wide vulnerability scanning. Basic tier ($49) includes external scans only (SSL, DNS, Headers). Professional ($79) and Comprehensive ($99) tiers include advanced port and vulnerability analysis shown in this sample.

This report is for informational purposes only and represents a point-in-time external security assessment. Scanity.ai is NOT an insurance company, broker, or agent. We do not sell, broker, or advise on insurance products. Insurance carriers mentioned are for reference only.

This assessment does not guarantee insurance approval or specific premium rates. Actual insurance decisions are made solely by insurance carriers based on their underwriting criteria. This scan covers only externally visible assets and does not assess internal security controls, policies, or procedures.

Findings are based on internet-wide vulnerability scanning and public sources. Data may be up to 30 days old. While we strive for accuracy, we make no warranties about completeness or accuracy. This is not a comprehensive security audit or penetration test. Organizations should conduct thorough security assessments before applying for cyber insurance. (Technical note: Port scanning powered by Shodan.io)