SHADOWTWIN SECURITY REPORT

Executive Summary
Generated: 12/17/2025 | Target: sbsinformatique.com

0 /100
Security Score

Total Vulnerabilities: 9
Critical: 2
High: 4
Medium: 2
Low: 1

FINANCIAL RISK EXPOSURE

Estimated Loss Range: $660,000 - $1,787,500

This represents potential financial impact including incident response, legal fees, regulatory fines, and reputation damage.

- SQL Injection Vulnerability - $187,500 to $500,000
- Remote Code Execution (Log4j) - $187,500 to $500,000
- Cross-Site Scripting (XSS) - $100,000 to $250,000
- Broken Authentication - Session Fixation - $40,000 to $100,000
- Server-Side Request Forgery (SSRF) - $40,000 to $100,000

INDUSTRY BENCHMARKING

Industry: Technology Sector
Your Percentile: 0th
Industry Average Score: 72/100
Top Performer Score: 95/100

Compliance Standards: SOC 2 Type II, ISO 27001, PCI DSS, GDPR

LIABILITY STATUS

Last Full Scan: 12/17/2025
Pending Remediations: 9
Confirmed Remediations: 0

AGENT 7 ORCHESTRATOR - EXECUTIVE SUMMARY

Autonomous Defense Orchestration

Vulnerabilities Protected: 6
Protection Coverage: 100.0%
Estimated Risk Reduction: 63.3%
Hotfixes Deployed: 3
Integrations Used: Cloudflare WAF, AWS WAF, Palo Alto Firewall, CrowdStrike Falcon, Splunk SIEM

Manual Review Required: 4 hotfix rules provided for manual deployment

Agent 7 coordinates with Agent 3 (Exploitation) and Agent 5 (Causal Prophet) to deliver automated defense recommendations and ROI-justified remediation priorities.

RECOMMENDATIONS

1. URGENT: Address all critical vulnerabilities immediately. These pose immediate risk of compromise.
2. Schedule remediation of high-severity vulnerabilities within the next sprint cycle.
3. Implement parameterized queries and input validation to prevent SQL injection attacks.
4. Sanitize all user inputs and implement Content Security Policy headers.
5. Update Log4j to version 2.17.1 or later and remove JNDI lookup functionality.