# SimplCyber Loss Exposure Report

hr4.com

Generated: 8/26/2025    Cyber Loss Snapshot

This report quantifies **financial losses driven by cybersecurity risks**. It translates technical vulnerabilities into dollar exposure, enabling boards and executives to prioritize remediation by business impact.

# Expected Annual Loss (EAL)

### CONSERVATIVE (P90)

**$0**

$0

High-confidence bound assuming partial exploitability.

### MOST LIKELY

**$0**

$0

Expected annual loss from current risk profile.
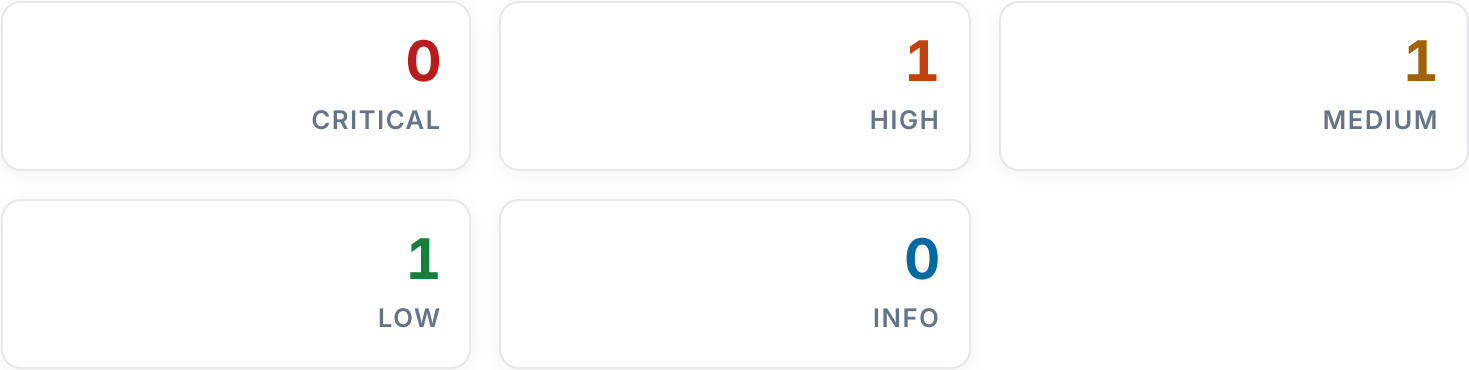
### WORST CASE

**$0**

$0

Upper bound under stacked adverse conditions.

## Executive Summary

3 total findings across 0 modules (runtime: 0s). Most likely loss: **$0**; worst case exposure: **$0**.

| | | |
|---|---|---|
| **0**<br>CRITICAL | **1**<br>HIGH | **1**<br>MEDIUM |
| **1**<br>LOW | **0**<br>INFO | |

## Risk Category Breakdown

## Security Findings

MEDIUM **Apache HTTP Server detected with confidence 100%**

Analysis for Apache HTTP Server v2.4.61. Supply chain score: 3.0/10.

> **Recommended Action:** Review and remediate this medium severity issue to reduce modeled loss.

HIGH **Ensure all links have descriptive text or aria-labels**

1 empty or unclear links (2 instances)

> **Recommended Action:** Review and remediate this high severity issue to reduce modeled loss.

**LOW**  **DMARC policy too weak**

DMARC policy is in monitoring mode (p=none) and provides no active protection.

**Recommended Action:** Review and remediate this low severity issue to reduce modeled loss.

## Methodology

EAL is computed from likelihood × impact across identified findings, adjusted for exposure windows, compensating controls, and industry prevalence. Values are point-in-time and should be re-baselined quarterly.

Report generated by **SimplCyber** on 8/26/2025.