■ Security Audit Report

Organization Overview

- **Organization Name:** Sample Organization
- **Industry:** Finance
- **Audit Mode:** Offline AI-Assisted Audit
- **Date:** 2025-12-28

Executive Summary

This security audit identified **1 critical/high-risk vulnerabilities**. All findings were analyzed using a **context-aware, explainable risk engine** and prioritized based on real-world operational impact.

Key Highlights: - Offline analysis ensuring complete data sovereignty - Context-aware risk scoring based on organizational profile - AI-powered explanations with hallucination prevention - Full audit trail with explainable reasoning

Risk Summary

Priority	Vulnerability	Final Score	Risk Level
1	Unencrypted Database Connection	10.0	Critical

Detailed Findings

■ Priority 1: Unencrypted Database Connection

- **Vulnerability ID:** VULN-001
- **Affected Asset:** User DB Server
- **Base Score:** 9.8

- **Final Score:** 10.0

- **Risk Level:** Critical

Context Modifiers Applied:


```
{
 "org_type": "+1.0",
 "data_criticality": "+0.8",
 "internet_exposed": "+0.5",
 "patch_delay": "+0.3"
}
```


Evidence:
Port 3306 open without TLS encryption. Database credentials transmitted in plaintext.

AI Analyst Explanation:
This vulnerability is critical for a financial organization because unencrypted database connections expose sensitive customer data to interception. The Priority 1 ranking reflects the combination of a high base severity (9.8) and organizational context factors including financial sector requirements, high data criticality, and internet exposure.

Source: scan1.xml

Methodology

Data Ingestion (Module 1)

- Parsed XML/JSON vulnerability scan files

- Filtered for High and Critical severity findings only

- Normalized data into unified structure

Adaptive Risk Scoring (Module 2)

- Applied context-aware modifiers based on:

  - Organization type (Finance)

  - Data criticality

- Internet exposure
- Patch delay

- Implemented dampening logic to preserve prioritization
- Assigned priority rankings

Explainable Trace Matrix (Module 3)

- Built complete reasoning trails for each vulnerability
- Linked evidence to risk assessments
- Documented all modifier applications

AI Analyst Co-Pilot (Module 4)

- Generated human-readable explanations using local LLM (Ollama)
- Maintained offline operation (no cloud AI)
- Prevented hallucinations through constrained prompting

Recommendations

1. **Immediate Action Required:** Address Priority 1-3 vulnerabilities within 7 days

2. **Short-term:** Remediate remaining Critical findings within 30 days

3. **Long-term:** Implement continuous vulnerability scanning

4. **Process:** Review and update security policies quarterly

---

Disclaimer

This report was generated offline using deterministic logic and a local AI assistant. No customer data was transmitted externally. All risk calculations are based on provided scan data and organizational context.

Report Generated By: Synthetic Auditor v1.0
Technology Stack: Python + Ollama (Local LLM)
Data Sovereignty: 100% Offline