Local Network Security Monitoring System (LoNSeMonSy)

By Tim/TJ Smith

Small companies face **prohibitively high costs for enterprise security**, with solutions like SentinelOne costing approximately **$44,997.50** annually for 250 endpoints.

This project provides a **low-cost, on-premises alternative** for **basic attack detection** and alerting, eliminating all per-endpoint subscription fees.

Who / What does the project interface with?

Users

- Network and security admins
- Instructors and students in a lab environment
- People that want to secure their home network

Systems

- Proxmox VE (or VMware ESXI) hosting VMs
- PostgreSQL for event storage
- Grafana dashboard for visualization
- Optional Ollama local AI for explanations

Hardware

- Raspberry Pi as a network sensor
- Mini PC or server running Proxmox VE
- Managed switch supporting VLAN changes

What are the inputs?

Data Sources

- Network traffic events from the lab network
- System logs from servers and VMs (SSH logins, authentication failures)
- Security sensor data from the Raspberry Pi (packet capture, device discovery)

Configuration & AI

- Admin-defined rules and thresholds (example, 10 failed logins in 1 minute)
- Optional AI prompt input for plain-English alert explanations

What are the outputs?

Alert: “SSH brute-force from 10.0.0.25”

AI output: “A device is repeatedly guessing passwords. Quarantine the source IP.

PostgreSQL

Real-time alerts stored in PostgreSQL

Grafana Dashboard

Grafana dashboard showing incidents and trends

VLAN Quarantine

Automatic VLAN quarantine action for suspicious devices

AI Explanation

Plain-English AI explanation of alerts, optional and local only

Notifications

Notification messages for admins, optional

5 Steps to go from input to output

1. Collect logs and events.

2. Analyze events for attacks.

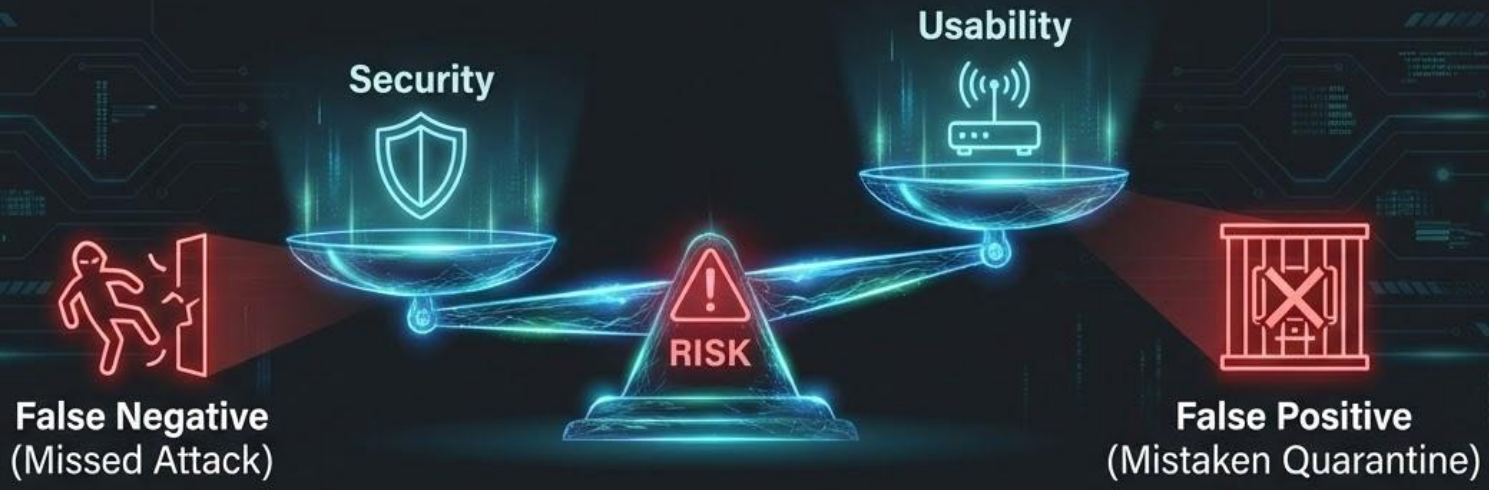
3. Store incidents in PostgreSQL.

4. Trigger quarantine (VLAN).

5. Display alerts in Grafana with AI.

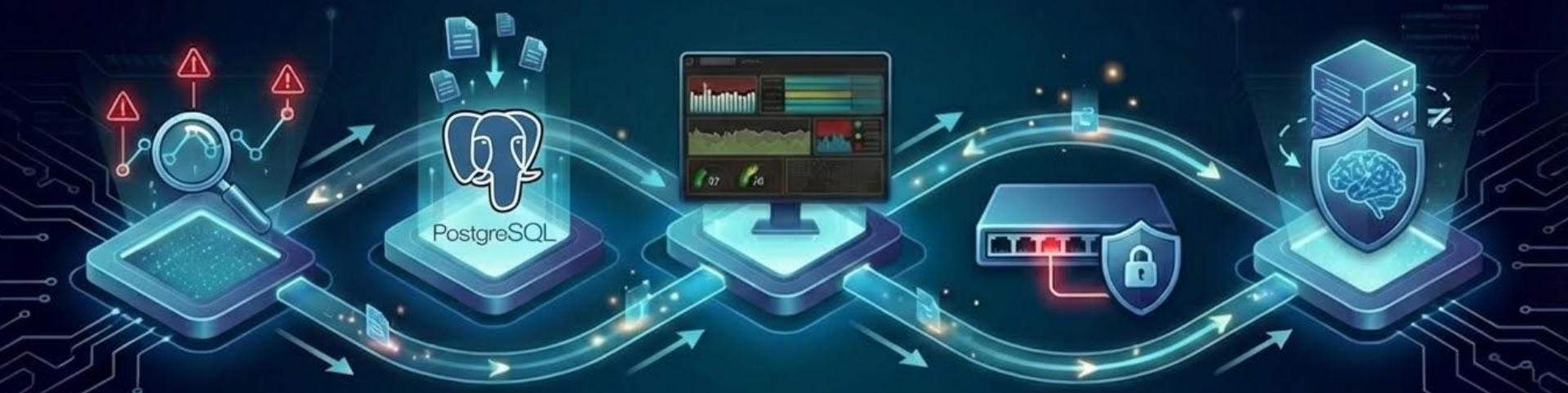
What’s the biggest risk?

The biggest risk is false positives and false negatives.



The system could quarantine a normal device by mistake,
or miss a real attack if detection rules are too simple.

How do you know you're successful?



Detect at least 3 attack scenarios in the lab environment

Correctly log all events into PostgreSQL

Dashboard updates in near real time

Quarantine VLAN action works during a live demo

System runs fully offline with AI explanations staying local