ENTERPRISE NETWORK ASSURANCE REPORT

Sample — Kuzey Lojistik A.■. (fictional)

AUTHORIZED SCOPE: Corporate and production networks · illustrative sample report

2026-09-05 10:27 UTC

54	68	91
/ 100	/ 100	/ 100
NETWORK SECURITY SCORE	ANSWER COVERAGE	CONTROL COMPLETENESS

EXECUTIVE POSITION

This is a declared baseline based on organization-provided answers. It separates known weaknesses from unanswered evidence gaps; supporting evidence has not yet been independently reviewed. No attack was executed.

Declared baseline: Answers have not yet undergone independent evidence review.

TOPOLOGY AT A GLANCE

Sites	**3**
Network Devices	**84**

BUSINESS IMPACT

1 of 2 crown-jewel systems are reachable from an internet-exposed asset over 2 attack path(s); the single highest-leverage control closes 2 of them (100%).

• An attacker starting from 2 internet-exposed asset(s) reaches a crown-jewel system in as few as 2 hop(s).

• 1 of 2 crown-jewel systems (50%) are reachable from the internet today.

• One enforcement point closes 2 of 2 path(s) (100%) and removes 1 crown-jewel system(s) from reach.

• That single control fully severs every modeled internet-to-crown-jewel path.

PROVED ATTACK PATHS

Reachability proved deterministically over your declared topology — no exploitation, no scanning. Shows the worst path from an internet-exposed zone to a crown-jewel zone and the single control that breaks the most of them.

Worst proved path: dmz-web → app-tier → prod-db

Highest-leverage control: dmz-web → app-tier · on 2 path(s)

Put an enforcement point (stateful firewall / identity-aware proxy / deny) on 'dmz-web' → 'app-tier'. It sits on 2 of the discovered exposed-to-crown-jewel path(s), so hardening this one hop breaks the most attacker movement.

Enforce this one control and 2 of 2 path(s) close, protecting 1 crown jewel(s).

2 exposed zone(s) · 1 of 2 crown jewel(s) reachable · 2 path(s)

RISK & ARCHITECTURE REVIEW

ARCHITECTURE & ATTACK-PATH INTERPRETATION

CRITICAL - One control sits on the majority of exposed-to-crown-jewel paths

Potential impact: A single enforcement point closes most attacker movement.

Chain breaker: Prioritize the dmz-web → app-tier boundary first.

DECLARED CRITICAL CONTROL GAPS

Only critical controls declared missing are shown here. Unknown answers are kept in the separate evidence-gap section and are not vulnerability claims.

CRITICAL - Internet-facing DMZ has a flat path to the production database

Observed: dmz-web → app-tier → prod-db traverses allow rules only.

Still required: The declared allow rules are active.

Potential impact: A foothold on the web tier reaches the crown-jewel database.

Chain breaker: Insert an identity-aware default-deny control on dmz-web → app-tier.

Score deduction: -14

HIGH - User VLAN can reach the management jump host

Observed: user-vlan → mgmt-jump uses ACL-only enforcement.

Still required: A user-zone device is compromised.

Potential impact: A compromised endpoint approaches administrative systems.

Chain breaker: Require an identity-aware, MFA-gated management path.

Score deduction: -9

PRIORITIZED IMPROVEMENT ROADMAP

0–30 days —

No open action.

30–60 days —

No open action.

60–90 days —

No open action.

EXPLAINABLE CONTROL LEDGER

Control	State / evidence	Earned / max	Evidence reference

METHODOLOGY & LIMITATIONS

Evidence-adjusted point-in-time assessment based on an authorized abstract topology and referenced controls. No exploitation, credential testing, arbitrary command execution, or third-party scanning was performed. This report is not a certification and does not prove that every declared control is effective.

Assessment topology retention: not_persisted

Version: enterprise-network-score-v1