01 · INFRASTRUCTURE SECURITY

Critical Server Hardening

Exposure diagnostic and remediation plan in 3 weeks, including the servers that can't be shut down.

THE PROBLEM

When a critical vulnerability hits, many companies discover they don't know how many servers are exposed. Many are old, run unsupported operating systems, and sit in production. The team fights fires without a plan and the risk stays open.

WHAT WE DELIVER

1. Inventory and classification: operating system, versions, end of support, and internet exposure.
2. Security coverage: which servers lack endpoint protection (EDR), patching, or monitoring.
3. Prioritized risk matrix: what to address this week, this month, and this quarter.
4. A plan for what can't be shut down: compensating controls, segmentation, maintenance windows, and a migration path.
5. Executive briefing with the risk, the cost of inaction, and the 90-day plan.

HOW IT WORKS

Week 1	Week 2	Week 3
Inventory and team interviews	Exposure and coverage analysis	Remediation plan and briefing

BaezLabs designs the plan and guides the decisions; your team executes. We don't sell licenses, cloud, or hardware.

NEXT STEP

A 30-minute call to understand your situation. Within 48 hours you receive a tailored proposal with scope, dates, and a fixed price.

FORMAT

Duration	**3 weeks**
Scope	**Based on server count**
Deliverable	**90-day plan for leadership**

Every proposal is built after a call, based on your company's size and needs.

WHO IT'S FOR

Head of Infrastructure, CISO, or CIO at companies with their own data center or a hybrid cloud setup.

WHO DELIVERS IT

20+ years leading global infrastructure at large enterprises

$50M+ USD in cloud and AI spend governed

$2.5M+ USD in annual savings delivered

Xavier Báez, Principal Architect. AWS Solutions Architect Professional.

Hidalia Román · CEO, BaezLabs
hidalia@baezlabs.com · solutions@baezlabs.com

Views expressed are personal and do not represent any organization. No proprietary systems, data, or organizations are referenced.