Koniag TECH | Koniag CYBER | vervint. by Koniag Tech

PENETRATION TESTING

PEN TESTING THAT ENDS WITH FIXES

Most pen tests hand you a report and leave. Ours end with fixes, from the team that already helps run your environment.



SAME FINDING, DIFFERENT DAY TWO

The test is similar. What happens next is not.

MOST PEN TESTS

Finding 07 — Critical

Remote access portal reachable from the internet

Recommendation: restrict access and enforce MFA.

- The report gets forwarded to IT
- The fix waits on a change window and another vendor
- It shows up again in next year's test

WITH KONIAG TECH

Work item · Finding 07 — Critical

Remote access portal reachable from the internet

Owner	Your managed services engineer
Interim fix	Limited to known IPs within days
Permanent fix	Vendor access moved behind MFA
Change window	Scheduled with your IT lead
Retest	✓ Path closed

Illustrative example. Every critical and high finding comes to you as a work item like this.

One team, test to fix

We buy and harden your equipment, run your core systems and defend what we run. Testing closes the loop.

A team that knows you

The people who test and fix your environment already know your systems and your people.

No new MSA

Work with Vervint, Koniag Cyber or any Koniag Tech company? You're already covered.

WHAT YOU CAN TEST RIGHT AWAY

Three packages, one test-to-fix promise

Scope	FASTEST Attack Surface Profile	BROADER Breach Path Analysis	COMPLETE Full Compromise Evaluation
External and internet-facing systems	●	●	●
Internal network and Active Directory	○	●	●
Wireless networks	○	●	●
Cloud environments	○	○	●
Key web applications	○	○	●
Timeframe	72 hours	1 week	2 weeks

Operate in an OT/ICS environment? Our OT assessments and specialists work across energy, manufacturing, utilities and water treatment, and we plan every test around your production schedule.

EVERY PACKAGE INCLUDES

- ✓ Ranked findings in business terms
- ✓ Interim measures you can apply now
- ✓ Proved vs. not proved, clearly marked
- ✓ A work item for each critical and high finding
- ✓ A 30/60-day remediation plan
- ✓ Retesting

Multiple tests /year recommended if you

- Handle patient, payment or citizen data
- Sell to the DoD or are working toward CMMC
- Get asked for proof by insurers or auditors
- Added an ERP, a cloud move or an acquisition
- Run plant or building systems on your network
- Haven't tested since you were a smaller company

How to start

1. **Scope.** A 20-minute call with your account team to pick a package.
2. **Test.** The Koniag Threat Intelligence team runs the agreed scope.
3. **Fix.** A readout with work items and a remediation plan, then a retest.

Koniag TECH | Koniag CYBER | vervint. by Koniag Tech

Let's close the paths, not just the report

Already a client? It's covered under your current agreement. [CONFIRM koniagcyber.com URL]

Book a scoping call ↗