SOFTWARE & SECURITY PRODUCT MAKERS

Software & Security Product Assessment

Penetration testing, post-quantum readiness and AI security for software publishers and security vendors — delivered as test evidence a notified body, lab or auditor can review.

Annex I
CRA-MAPPED FINDINGS

Build to install
SIGNING CHAIN TRACED

CycloneDX
CBOM & ML-BOM OUTPUT

Senior
PRACTITIONER-LED

What we assess

AI security
Copilots and agents in your product, AI-integrated browsers and IDEs, AI triage in security tools, and the models they inherit.

Post-quantum readiness
Code- and update-signing keys, PKI and certificate issuance, VPN and TLS stacks, and the key management your customers rely on.

Product & pipeline testing
Desktop clients, installers and updaters, endpoint agents, APIs and cloud back ends, and the build pipeline that signs each release.

What you get

- ✓ Findings mapped to CRA Annex I requirements
- ✓ Evidence a notified body, lab or CA auditor can review
- ✓ Signing and update chain tested from build to install
- ✓ Each finding rated by the trust boundary it crosses
- ✓ CBOM and a post-quantum roadmap for signing and PKI
- ✓ AI-BOM and test results for in-product AI and agents
- ✓ One round of retesting to confirm the fixes landed

How it works

1. Scope the product, its core function and target markets
2. Agree test builds, test keys and a test repository
3. Test clients, update path, APIs and pipeline hands-on
4. Deliver findings and evidence, then retest the fixes

A good fit if

- ✓ You sell installable software in the EU, where CRA reporting has applied since September 2026.
- ✓ You make IAM, VPN, SIEM, PKI, firewall or hypervisor products the CRA lists as important.
- ✓ You face Common Criteria, EUCC or FIPS 140-3 lab testing and want the problems found first.
- ✓ You run a publicly trusted CA, and the CA/B Forum NCSSR calls for annual penetration tests.

Probably not, if

- × You need a certificate or audit opinion — we are not a notified body, evaluation lab or CA auditor.
- × You want pipeline attacks proven in production — we validate only in a test repository.
- × You want source code reviewed on its own — our sister brand rouage delivers that.

How we engage

Scoped per release
A fixed-scope proposal for the build under test, priced before any work starts.

Senior-led
The practitioner who scopes the work does the work and writes the report.

Before the evaluation
Findings mapped to CRA Annex I, as evidence a notified body, lab or auditor can review.

Release path protected
Live pipeline reviewed read-only; attacks proven in a test repository, never shipped.