Security testing is part of how we build and maintain our products

Deep InfoSec performs daily automated security scanning, annual penetration tests of its solutions, recurring security assessments combining human analysis with AI, and ongoing adversarial exercises intended to break assumptions before attackers exploit them. We use the findings to correct code, configuration, authentication, dependencies and operational controls, then verify the fixes in the affected environment.

Our security lifecycle

Deep InfoSec performs daily automated security scanning, annual penetration tests of its solutions, recurring security assessments combining human analysis with AI, and ongoing adversarial exercises intended to break assumptions before attackers exploit them. We use the findings to correct code, configuration, authentication, dependencies and operational controls, then verify the fixes in the affected environment.

Deep Advisor — attack paths

Deep Advisor explores attack-path hypotheses beyond known single-vulnerability patterns. It evaluates combinations of reachability, privileges and exposed services, proposes mitigations linked to each path, and helps analysts reduce the set of viable paths open to an attacker. These insights inform technical remediation and its verification.

What your team receives

The engagement outputs include test scope, classified findings, remediation ownership, retest evidence and improvement records. Product assurance and independent customer audits remain separately scoped activities.

Technical working notes

Daily security analysis

Automated checks evaluate dependencies, configuration drift, exposed endpoints and reachable components. Findings are routed for human review and remediation rather than left as unowned scanner tickets.

Annual penetration testing and adversarial exercises

Authorized penetration tests examine deployment boundaries and implementation behavior. Recurring expert-led and AI-assisted security evaluations challenge assumptions and try alternative routes through the system.

Deep Advisor prediction and mitigation

The model proposes attack-chain hypotheses from reachable assets, permissions and service dependencies. Each hypothesis links to a possible blocking control and validation test, so teams can narrow the available attack paths.

Engineering verification and handover

Every high-priority finding has technical evidence, a defined owner, remediation action and retest status. Product engineering, incident management and separately engaged assessors receive the material relevant to their roles.

sales.security@deepinfosec.com | https://deepinfosec.com