solidlab

OFFENSIVE SECURITY

SECURITY ASSESSMENT FOR APPLICATIONS AND IT INFRASTRUCTURE

APPSEC

- AI/ML-powered applications
- Web applications & backend APIs
- Source code analysis
- Mobile apps (iOS / Android)

INFRASEC

- Internet-facing services
- Internal network & Wi-Fi
- Clouds
- Active Directory

Environments: Clouds, K8s & containers, etc.

WHAT SETS US APART

- **Quality control at every stage of the engagement**
  Mature project management and peer review of all findings
- **In-house tooling and assessment frameworks**
  Built on internal R&D and field-proven expertise
- **Expertise sharpened by ongoing security research**
  Our team regularly contributes to security research, CTF competitions, and bug bounty programs
- **Manual testing and real-world attack scenarios**
  We go beyond checklist-style testing to uncover business logic flaws and non-obvious attack paths
- **Adapted to the specifics of your project**
  Our approach and recommendations are shaped around how your application and infrastructure actually work
- **Visibility for your team throughout the project**
  Frequent check-ins, instant alerts on critical issues, and findings debriefs

ENGAGEMENT FORMATS TAILORED TO YOUR NEEDS

- Enterprise-wide security assessment
- Black-box, gray-box and white-box testing
- Red Team operations and adversary simulation
- Physical intrusion testing, badge and access control checks, social engineering campaigns

WHAT YOU GET

Critical vulnerabilities uncovered before attackers find them

Real-world validation of your existing security controls

Prioritized, actionable hardening guidance

A maturity boost for your security, IT, and SDLC practices

WHY RUN A SECURITY ASSESSMENT

To protect business processes, customers, and data

Business process automation and AI adoption expand your attack surface. A security assessment helps you identify and respond to risks before they escalate into unacceptable events.

To get a practical health check of your IT and security operations

To receive a sound, evidence-based evaluation of processes such as identity and access management, patch management, and network segmentation, as well as your monitoring and response capabilities.

To check software development and AI integration practices

With full access to source code and design, white-box testing goes beyond individual bugs to reveal systemic weaknesses across your architecture, development processes, third-party dependencies, and external integrations.

WHAT'S IN THE REPORT?

- Full list of discovered vulnerabilities
- Risk-based severity ratings backed by CVSS
- Technical appendices: PoCs, activity logs, screenshots, and more
- Executive summary
- Demo of attacks and attack chains
- Overview of confirmed defenses
- Detailed remediation guidance

WHY SOLIDLAB?

CVE credits
from Google, Apple, Microsoft, VMware and more

30+ skilled
offensive security experts holding OSWE, OSEP, OSCP, CRTP and more

700+ successful
security assessment projects delivered

15+ years
in offensive security

A track record that speaks for itself
– articles, conference talks, CTF wins and hall-of-fame mentions

98% of clients stay with us
after their first engagement

*NPS score of 80

47A Vavilova St., Moscow 117312, Russia

+7 499 705 76 57

info@solidlab.ru

For more than 15 years, SolidLab Group has been protecting organizations from cyber threats, preventing attacks and minimizing the risks of financial and reputational damage. SolidLab provides a full range of services: from pentesting to application protection, incident response and secure SDLC implementation.