Secure Code Review

AEC

Develop secure, high-quality and sustainable code

A secure code review is a form of analysing applications' source code to find flaws that pose or could pose security threats in the future. The code review process consists of automated and manual code review by specialists focused on secure development. Source code analysis can also reveal hidden threats and potential weak spots in an application that would not be easily detected by ordinary penetration tests. The code review results in a detailed description of the vulnerabilities with specific recommendations to remedy them.

aec-security.eu

Secure development and source code review:

Code review
We check the security of the given source code in the form of manual and automated analysis and give customized recommendations for the application and technology.

Advanced white-box
We carry out comprehensive application security reviews by combining security code reviews, penetration testing and audits of the target applications.

Checkmarx
We help clients implement advanced solutions from Checkmarx for automated source code analysis (CxSAST), application composition analysis (CxSCA) and developer training (Codebashing).

Training and consulting activities
We provide secure development training in the process (SSDLC) and technical (secure web application development) areas.

Code review

- Applications reviews in many popular languages (Java, C#, PHP, ...).
- An internal methodology based on experience from security development and penetration testing, leaning on recognized standards from the OWASP project.
- It can detect developer bugs, backdoors, design errors, not keeping to best practices, use of weak cryptography, and many other vulnerabilities in the application.
- Code review consists of two main analytical parts:
  – An automated review of the entire code using open-source and proprietary tools and a review of the results by a security specialist.
  – A manual review of the entire code or its sub-parts selected by the client or a security specialist.
- The vulnerabilities uncovered are described in detail and customized recommendations are provided, which take into account the technology stack used.

Advanced white-box

- An advanced form of white-box testing
- A combination of penetration testing, code review and other optional disciplines.
- It achieves better quality and efficiency by joining the forces of ethical hackers with experts in secure development.
- It maximizes the benefits of multiple security disciplines.

Checkmarx

- CxSAST - a tool for automated static analysis of source codes that can be integrated into a wide range of technologies.
- CxSCA - a tool for analysing software composition that aims to find vulnerable software dependencies and licencing conflicts.
- Codebashing – a platform for educating developers in the area of writing secure code.

Training and consulting activities

- Technical and procedural training.
- Consultation in the area of secure development.

Our strengths

- We are an established Czech security company that has been successfully operating on the market for over 30 years.
- We listen to our clients and adapt our tests to their needs and the time they have available.
- Our team is made up of specialists with extensive experience in the area of development and ethical hacking.
- We follow modern trends in development, security and technology.
- When analysing source code, we put an emphasis on manual reviews that lead to the discovery of a greater number of errors than ordinary automated solutions.
- We allow comprehensive security audits to be made by combining several security disciplines.
- We build our services on many years of experience and tried and tested standards.

Bezpečnost v SDLC a DEV-OPS prostředí

CxSAST a Codebashing
Tréning v správním čase

CxSAST a úroveň řízení/orchestrace
Snížení celkových nákladů

CxSAST a CxSCA
Lepší zabezpečení vlastního i open source kódu

CxSAST a CxIAST
Přesnější výsledky bezpečnostní analýzy