Advanced White-box

AEC

Check the security of the applications you develop

Advanced white-box is a product combining penetration testing and secure code review or other assessment services. The advanced white-box comprehensively examines the security of applications under development by simulating hacker attacks, making use of automated code analysis, manual code reviews and audits. The service's advantage is that it combines the strengths of experts in several security disciplines, which means the analyses give the maximum benefit and reveal a greater number of vulnerabilities, including detecting hidden threats and potential weaknesses in the application being audited. The resulting report from the advanced white-box testing includes a description of the vulnerabilities with specific recommendations to fix them that are built so they best suit the technologies used.

aec-security.eu

Advanced White-box involves:

- Penetration testing

Penetration testing is a simulation of hacker attacks at the network and application level to test the ability of an organization's systems to withstand real cyber-attacks from the external environment, but also its ability to withstand unauthorized interference by employees, regardless of whether they act knowingly or simply make a mistake.

- Secure code review

This consists of checking the source code of applications. It takes the form of manual source code reviews and automated analyses using SAST tools.

Advanced White-box

Penetration testing

- It simulates hacker attacks on applications, systems and entire infrastructures.
- It uses globally recognized methodologies such as the OWASP Web Security Testing Guide (WSTG) or Penetration Testing Standard (PTES).
- Penetration testing is done by certified penetration testers in line with required standards.
- It involves manual tests to scan your security combined with advanced commercial automated scanning tools, as well as custom tools from the AEC toolkit portfolio.
- Penetration testing detects vulnerabilities, configuration flaws or reveals undersized system elements at all layers of the application or system under test.

Code review

- A review of applications in many popular languages (Java, C#, PHP, ...).
- An internal methodology based on experience from security development and penetration testing, based on the recognized standards of the OWASP project.
- Reveals development errors, backdoors, design flaws, non-compliance with best practices, use of weak cryptography and many other vulnerabilities in the application.
- The code review consists of two main analysis 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 subparts as chosen by the client or a security specialist
- The vulnerabilities uncovered are described in detail and tailored recommendations are provided that take into account the technology stack used

Our advantages

- We are a successfully established Czech security company that has been on the market for over 30 years.
- We listen to our clients and adapt our tests to their needs and time constraints.
- Our team is made up of specialists with a wealth of experience in development and ethical hacking
- We follow the latest trends in social engineering.
- We combine penetration testing, automated source code analysis, manual reviews and audits to uncover a wide range of vulnerabilities.
- The resulting reports from the tests we conduct contain detailed descriptions of the vulnerabilities found and specific recommendations to fix them that are tailored to the technologies used.
- We build our services on many years of experience and time-tested standards.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283