Secure Software Development Lifecycle (SSDLC)

Secure Development Methodology Tailored to Your Needs

Whether you develop applications for internal or external customers, AEC has a solution to help you produce safer applications. The key to sound application security is not conducting as many penetration tests as you can. It is mainly about improving the whole development process, looking for weaknesses and addressing them continuously. Only a well-designed, risk-based, measurable, and repeatable process will ensure a sustainable and high-level security of your applications. A proven way to accomplish this is the implementation of a secure development methodology that will define security activities, requirements, roles, and responsibilities from the beginning to the end of the development lifecycle.

You may be considering implementing a SSDLC methodology, or you may have already taken specific steps towards this objective. In either case, AEC offers you a helping hand with the design and implementation of the methodology that will best suit the specifics of your organization.

Since its foundation, AEC professionals have carried out hundreds of penetration tests, training workshops and consultations on application security and software development. All the knowledge and experience of our team will be available to your benefit during the implementation of the methodology.

AEC

AEC SSDLC Services

- **Design of SSDLC Methodology**
  We will design a tailored SSDLC methodology addressing the security needs of your development teams.
- **Project Documentation**
  We will provide you with user-friendly templates of security artifacts you can use in your projects.
- **Application Audit Cycle**
  We will show you how to set up an audit cycle for your projects, which corresponds to the business and IT risk profile of each application.
- **Security Awareness Program**
  We will help you systematically educate your employees and increase their security awareness and skills using security training and e-learning courses.
- **Pilot Project**
  We will show you how to use the methodology on a real project.

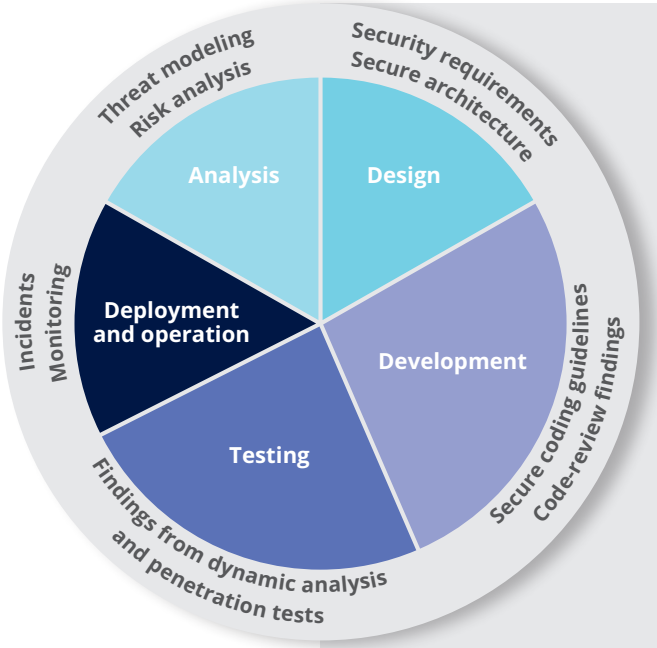
www.aec.cz

Secure Software Development Lifecycle (SSDLC)

AEC

Complete Coverage of the Development Cycle

Surely, you have heard that the costs of removing vulnerabilities in the early stages of development are lower than the costs of eliminating vulnerabilities found later in production.
Most organizations are in line with this principle, trying to integrate security into the development cycle as soon as possible. However, for many of them, it is not easy to work with security requirements in the same way as with functional requirements.
In particular, they are unable to implement them in accordance with the secure development standards and test them by using appropriate test scenarios.
Our methodology works with requirements from initial risk identification and requirements selection up to their final testing.



Focus on Fast Adaptation

Each organization has a unique culture and a way of managing and setting roles. For your employees to adopt the SSDLC methodology, it should respect the specifics of your organization as much as possible. Otherwise, there is a risk of gradual deviation from the methodology, or its rejection by the development teams.
Our methodology aims to integrate security principles and requirements seamlessly into your organization and project management. You do not have to go through a demanding reorganization of processes or roles. However, you will extend the competencies and knowledge of the respective teams, formalize activities, and give them new tools to manage security during application development. You will also get a better overview of the project's status due to the introduction of new metrics and consistent reporting.

Protect Yourself from Vulnerabilities

Unless your company is a rare exception, most of your application code is comprised of re-usable third-party code, libraries, frameworks, and code created by different vendors.
Your control over the creation of this code is limited, and any vulnerability in this code can endanger your application as well as a vulnerability in your own code. It is thus vitally important to always select secure components, monitor them for known vulnerabilities, and keep tight control over your suppliers.
Ask your suppliers for security certifications of their development cycle. AEC can also award you with a certificate of your SSDLC if you meet the necessary requirements, and you can use the certificate to prove the security of your development process to your partners without them having to do an audit.

Security Awareness and Education

An essential aspect of the SSDLC methodology is the continuous raising of security awareness. Your developers need to understand application vulnerabilities, common threats, and secure development methods. Remember to systematically improve your employees' skills using our training and interactive e-learning courses.

Secure Development Benefits

- Fewer findings from penetration tests.
- Less in-process security incidents.
- A sense of security for users.
- Lower risk of losing sensitive data.
- Lower reputation risk.
- Lower risk of sanctions for non-compliance with legislative requirements.
- Improvement of developed applications' quality.

Average Time Needed for Correction of the Finding, Based on its Severity

Critical
139 days

High
195 days

Medium
178 days

Low
216 days

WhiteHat Security Application Security Statistics (2018)

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