



Agile Security Evaluation

What is Agile Security Evaluation?

Agile Security Evaluation (ASE) is the process we have adopted for undertaking a continuous security assessment throughout the lifetime of an Agile project.

It differs from the traditional approaches to evaluation by effectively evaluating and accrediting each and every security enforcing or security relevant change as and when each change is made.

Once a project is initiated we use the same approach to ensure that the business security requirements, which reflect the business risk appetite, remain current and are satisfied throughout the project's lifetime.

Why use it?

Current and emerging development methods mean that it is no longer acceptable, or practical, to constrain your development approach to a lengthy evaluation and accreditation process before a release goes into production.

If you are well on your way to continuous delivery or continuous deployment you will either have already adopted ASE – or you may be deploying systems about which you have only a limited understanding of the security risks that you and your customers are facing.

Data driven projects, especially those that use machine learning or other AI approaches and have a direct impact on real-world situations are not only in continuous deployment by default, but also inherently untestable in a classical sense.

What do we do?

We build an ASE panel that is embedded (virtually or physically) within the most appropriate part of the business that owns the project or function concerned. Using the panel, we analyse the business threats and risk appetite to establish the evaluation criteria that need to be applied throughout the project.

We facilitate the development of threat and adversary models for the business that can be kept current and determine any additional project specific items that must be considered.

We identify and document:

- the project vulnerability profile;
- the proposed security enforcing functions and mechanisms;
- the proposed security relevant functions and mechanisms;
- a proposed baseline configuration for ongoing evaluation.

At the earliest instance of:

- a project gateway, for example a sprint boundary, or;
- a project feature request or problem report (including data) that impacts security enforcing or security relevant functions or the vulnerability profile.

The ASE panel reviews the impact of the changes and determines the necessary updates to the evaluation criteria.

It is the responsibility of the relevant development teams to make the required engineering updates to their documentation, code, tests and processes to ensure that the evaluation criteria are being conformed to.

It is the responsibility of the ASE panel to assure that the evaluation criteria are fully incorporated within the engineering functions.

We would like to talk to you

If you would like to know more about ASE please call us. We will schedule a free-of charge initial exploratory teleconference between us so we can understand your requirements and learn more of your needs and objectives.

We use this initial discussion to draw up a short proposal in the form of a letter of engagement that lets us work together quickly on a series of short time and budget-bound sprints for your approval.

Contact us

We look forward to hearing from you:

t: +44 1403 599900

e: webfb@primarykey.co.uk

a: PO Box 2254, Pulborough, West Sussex, RH20 9AW, UK