Bootstrap and improve your SDLC with OpenSAMM

by Bart De Win and Sebastien Deleersnyder

Duration: 1 day

Building security into the software development and management practices of a company can be a daunting task.

There are many elements to the equation: company structure, different stakeholders, technology stacks, tools and processes, and so forth.

Implementing software assurance can have a significant impact on the organisation. Yet, trying to achieve this without a good framework is most likely leading to just marginal and unsustainable improvements.

OWASP OpenSAMM gives you a structural and measurable framework to do just that.

It enables you to formulate and implement a strategy for software security that is tailored to the risk profile of your organisation.

The goal of this one-day training, which is conceived as a mix of training and workshop, is for the participants to get a more in-depth view on and practical feeling of the OpenSAMM model.

The training is setup in three different parts.

In a first part, an overview is presented of the OpenSAMM model and similarities and differences with other similar models are explained.

The different domains (governance, construction, verification, and deployment), their activities and relations are explained.

Furthermore, different constituent elements (e.g., metrics) are discussed and the overall usage scenarios of the model are explained.

Next, approx. half a day will be spent on doing an actual OpenSAMM evaluation of your own organisation (or one that you have worked for).

We will go through an evaluation of all the OpenSAMM domains and discuss the results in group. This will give all participants a good indication of the organisation’s maturity with regards to software assurance.

In the same effort, we will define a target model for your organisation and identify the most important challenges in getting there.

The final part of the training will be dedicated to specific questions or challenges that you are facing with regards to secure development in your organisation. In this group discussion, experience between the different participants will be shared to address these questions.

In case you haven’t started a secure software initiative in your organisation yet, this training should provide you with the necessary foundations and ideas to do so. Be prepared for a highly effective and applicable treatment of this large domain! And in case you would be concerned about confidentiality issues, we adhere to the Chatham House Rule.