

# Introduction to the Dialogue Tool

In recent years, cybersecurity has moved up the agenda in many companies, and focus on cybersecurity increases as we see both SMEs and high-profile companies being compromised by cyberattacks. Hence, security should be a key priority when designing digital solutions.

On the other hand, cybersecurity is a complex topic; the threat landscape is constantly evolving, it is a technically complex area, and security is often seen as both expensive and cumbersome.

When developing new digital solutions for your various customers, it may therefore be challenging to start the dialogue on security in the solution, especially if they lack awareness and knowledge about security.

## Dialogue Tool that supports the dialogue on cybersecurity

We have developed a *Dialogue Tool* designed to support the dialogue on security in the development of digital solutions based on the OWASP-SAMM framework. The aim is to enable you and your customers to determine the level of security that is relevant to them.

The dialogue can take place in many ways, which is why the *Dialogue Tool* consists of three documents: *01 Preparation*, *02 Presentation* and *03 Checklist*, as well as suggestions for how to use them. These three documents can be combined and utilised in different orders and ways, depending on your working methods and the customer. Below, we provide an overview of the different documents and how they can be utilised.

### CUSTOMISE THE DIALOGUE FOR EACH CUSTOMER

Perhaps you recognise that there can be substantial differences in your customers' technical knowledge and awareness of security. Therefore, it is important to customise the dialogue for each individual customer. One way of adapting the explanations to those who are less familiar with security terminology is to utilise some of the comparisons and examples included in the documents. Additionally, the *Checklist* can serve as a useful starting point for clearly illustrating various security aspects. Conversely, if your customers are more technically proficient, you may consider sending some of the documents to them in advance. Thus, they will have a chance to reflect on some of the topics in advance, providing a solid starting point for the dialogue.

### WHO SHOULD BE INVOLVED?

To gain the necessary insight into the security of the customer, it's essential to involve the right individuals. As a rule of thumb, it's a good idea for the customer to involve at least two employees:

- 1) Someone with the authority to make (financial) decisions.
- 2) A technical specialist who can answer the technical questions referred to in the tool.

## 01 PREPARATION

The *Preparation* document presents a number of security topics that a digital solution/software should include. The document is particularly useful as an internal resource for preparations before a client meeting or as part of instructing new employees in how to approach discussions about security. Using the *Preparation* document enables you to dive deeper into each of the topics. If your customers are technically skilled and have an understanding of security, the document can be sent to them before the meeting, if you think it's relevant and can contribute to your dialogue.

## 02 PRESENTATION

The *Presentation* is a slide deck that can serve as a brief overview of key questions to address during a meeting, which will form the basis for defining future security tasks relating to the solution. It can easily be integrated into a customer-facing presentation, allowing you to address security alongside new potential features. Alternatively, you can also use the presentation internally to prepare for a meeting. It provides a quick overview, so you have the questions in mind, and it can be supplemented with the *Checklist*.

## 03 CHECKLIST

The *Checklist* is a spreadsheet that provides a list of questions to guide the conversation with a customer. The *Checklist* is intended as a customisable resource, as not all questions may be equally relevant to all customers. First of all, the *Checklist* help prioritise the security topics by means of rating the questions from “Not important” to “Very important”. On this basis, each topic can then be investigated as appropriate. If the target customer has an understanding of security, the *Checklist* can be shared with them before the meeting. This will help initiate discussions about security needs – as perceived by the customer – and what you, as experts, would recommend them to do. Based on that dialogue, you can reach a common understanding of how to secure their solution.

### USING THE CHECKLIST AS SUPPORT

If you primarily use a whiteboard, Jira, or any other tool when discussing security with your customers, the *Checklist* can be used as inspiration for the dialogue. Alternatively, you can print it out and give it to the customer to focus on while you draw and explain.

*The Dialogue Tool has been developed by the Sb3D project  
in collaboration with the following companies:*



*Partners in the Sb3D project.  
The project is funded by the Danish Industry Foundation:*

