

## Tool Box by Pôle Mer Bretagne Atlantique

## Ingénierie Cybersécurité pour les projets



### Publics

- ▶ Équipes des projets collaboratifs des adhérents
- ▶ Équipes des projets des adhérents



### Durée

- ▶ Évaluation des enjeux de cybersécurité : **2 semaines, dont 1 journée d'entretiens**
- ▶ Analyse des risques de cybersécurité : **selon projet (nous contacter)**



### Tarifs

- ▶ Kit d'évaluation de la criticité : **mis à disposition à titre gracieux**
- ▶ Évaluation des enjeux de cybersécurité : *sur demande*
- ▶ Analyse des risques de cybersécurité : *sur demande*



### Intervenants

- ▶ Consultant Senior ou Manager spécialisé en Cybersécurité
- ▶ **Nous contacter : pole-mer-BA@wavestone.com**



### Objectifs

**Wavestone propose d'apporter aux projets l'ingénierie Cybersécurité permettant d'identifier, d'évaluer et de réduire les risques de cybersécurité auxquels les produits et services cibles seront exposés.**

Face à la multiplication des incidents et à la professionnalisation des attaques informatiques, la cybersécurité est aujourd'hui devenue un enjeu majeur : en 2015, une hydrolienne Sabella à Ouessant stoppait sa production d'électricité pendant deux semaines à la suite d'une infection par un rançongiciel. Mi-2017, l'attaque destructrice NotPetya coûtait au transporteur Maersk 300 millions de dollars.

La prise en compte de la cybersécurité dans les projets est aujourd'hui devenue indispensable afin de maîtriser ces risques. Elle représente de plus un élément différenciant face à des clients de plus en plus exigeants sur le sujet.



### Contenu

L'accompagnement s'adresse à la fois aux **projets collaboratifs et aux projets des adhérents.**

Il repose sur un catalogue dans lequel adhérents ou projets peuvent choisir la ou les offres les plus adaptées :

- Wavestone met à disposition du Pôle Mer **un kit d'évaluation de la criticité d'un projet** : ce kit peut être utilisé directement par le Pôle Mer ou ses adhérents pour obtenir une première évaluation de la criticité d'un projet en matière de cybersécurité. Une fois complété, le kit recommande la démarche cybersécurité la plus adaptée au projet.
- Wavestone propose d'**évaluer les enjeux de cybersécurité d'un projet** et de fournir des recommandations sur les études cybersécurité conseillées lors du projet (exemple : analyse de risques, étude d'impact sur la vie privée, test d'intrusion...).
- Wavestone propose de **réaliser une analyse des risques de cybersécurité sur un projet et de déterminer des mesures de sécurité pour les réduire**. Cette démarche permet d'évaluer l'ensemble des risques de cybersécurité, de distinguer les risques acceptables de ceux devant être réduits et de proposer des mesures (organisationnelles et techniques) adaptées et proportionnées au projet. L'étude peut être suivie d'un accompagnement visant à apporter une expertise cybersécurité au projet, contrôler la mise en œuvre effective des mesures ou vérifier l'absence de failles de sécurité dans le produit ou le service finalisé.