

**Veilige Digitale Producten Bouwen**

 Letter of intent

**Project**

Verschillende factoren hebben ertoe geleid dat de laatste jaren het bewustzijn rond cyberveiligheid van digitale producten en platformen sterk is toegenomen (Europese wetgeving NIS2, groeiende media-aandacht voor incidenten, exponentieel groeiende hacking gemeenschap, oorlog in Oekraïne, …).

Bedrijven die er beter in slagen zich als veilige en betrouwbare partij te profileren, zullen dus een grotere kans hebben om hun diensten (internationaal) te verkopen dan concurrenten die dit minder doen.

Het collectieve onderzoeksproject 'Veilige Digitale Producten Bouwen' heeft als doel digitale productbouwers beter aansluiting te laten vinden met de uitgebreide wereld van cybersecurity, zodat ze gedurende de ganse levenscyclus van hun productontwikkeling de juiste keuzes kunnen maken als het gaat om investeringen in cybersecurity.

Het project wenst zo tegemoet te komen aan een aantal noden die we vaststellen bij bedrijven die digitale producten bouwen, zoals o.a. kennis over standaarden, differentiëren met veilige producten, …

**Begeleidingsgroep**

Geïnteresseerde bedrijven kunnen het project vanop de eerste rij opvolgen. De begeleidingsgroep fungeert als ‘klankbord’ voor de opvolging van de projectvooruitgang en rapportering, samenstelling en praktische werking, IPR en deontologische aspecten (confidentialiteit, gebruik van projectresultaten e.d.) en latere valorisatie van de projectresultaten. Deelname aan de begeleidingsgroep is kosteloos.

Ondergetekende verklaart kennis te hebben genomen van het COOCK-project
***Veilige Digitale Producten Bouwen***

|  |  |
| --- | --- |
| **Naam organisatie** |  |
| **Ondernemingsnummer** |  |
| **Naam van de contactpersoon en functie** |  |
| **Tel en e-mail** |  |  |
| **Vlaamse kmo?**(< 250 werknemers; < 50 mio EUR omzet of < 43 mio EUR balanstotaal) | Ja/nee (indien nee, aard organisatie toevoegen) |
| **Bereid tot deelname begeleidingsgroep** | Ja/nee |
| **Intentie ondernemingsspecifiek project** | Ja/nee |
| *Geef aan welke noden u herkent in de eigen organisatie met betrekking tot cybersecurity*[ ]  Nood aan kennis m.b.t. standaarden en wetgeving om rekening mee te houden (**vandaag** en in de **toekomst**, **geografisch**, …). [ ]  Nood aan een aanpak om tegemoet te komen aan security vereisten met een **minimale impact op innovatiesnelheid** (is onze applicatie veilig genoeg?) [ ]  Nood aan het integreren van CS (cyber security) in de **product roadmap**. Waarop inzetten & wanneer, waarop anticiperen?[ ]  Nood aan een aanpak om de **betrouwbaarheid van leveranciers** op vlak van CS te bepalen[ ]  Nood aan kennis hoe security aspecten te integreren in onze processen.[ ]  Nood aan **opleiding** en aan **kennis over het landschap** van CS aanbieders.[ ]  Nood aan een aanpak om **tijdig/zeer snel** te kunnen antwoorden op een security assessment[ ]  Nood aan methode om leads te **kwalificeren**. Kunnen we deze klant wel aan met ons huidig niveau van CS?[ ]  Nood aan methodes om aan te tonen dat ons product **veilig/betrouwbaar/ethisch genoeg is**?[ ]  Nood aan expertise om **CS risico’s in klantenovereenkomsten** op te nemen.[ ]  Nood aan manieren om CS in plannen voor investeerders op te nemen (fund raising)[ ]  Nood aan procedures voor **incident beheer**. Wat te doen bij een incident? Reputatie/Hoe detecteren…[ ]  Wat als een leverancier een incident meldt? (snel reageren ) |
| *Geef ook de kennissprong aan binnen de eigen onderneming die men verwacht te verwerven dankzij van het COOCK-project.* |
| *Geef toelichting bij de potentiële case(s)/toepassing(en) die u ziet binnen uw bedrijf om met de projectresultaten concreet aan de slag te gaan (welk probleem wilt u aanpakken, waarom, …)* |

**Handtekening en datum**