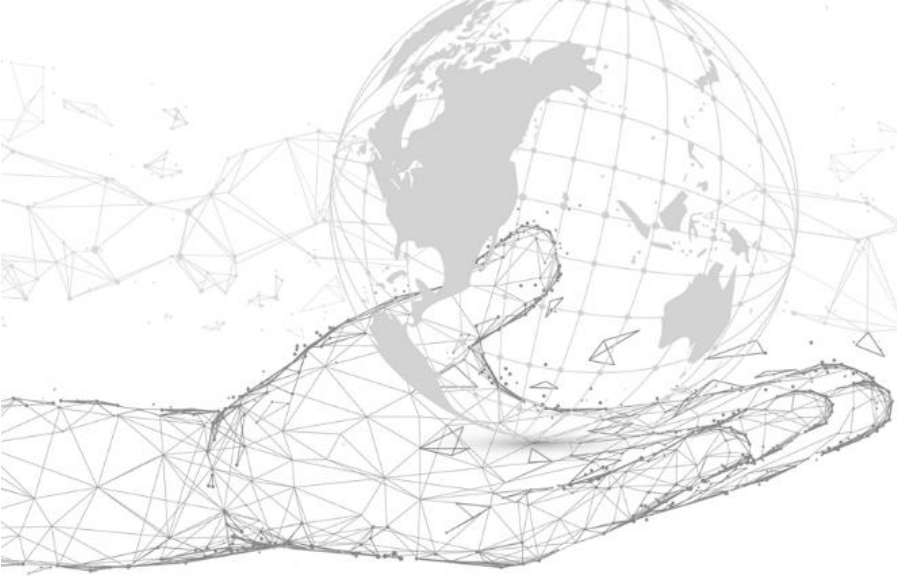


efcse.eu

PROGRAMMES EUROPEENS

Auteur : Secrétariat Général EFCSE
05/05/2019

Préambule

Il existe un grand nombre de programmes européens permettant aux entreprises de bénéficier de subventions, tant pour soutenir leur croissance, que pour un accompagnement dans les diverses phases de leur développement, y compris sur les axes d'innovation.

Le domaine du digital et de la sécurité numérique est plus qu'un sujet d'actualité, c'est un véritable challenge pour l'avenir économique de l'Europe et son positionnement sur la scène internationale.

Même s'il y a une certaine complexité dans le montage de dossier pour répondre aux appels à projets ou sur candidature à des programmes européens, il est intéressant de se pencher sur le sujet, cela pouvant se traduire par un apport financier substantiel et différenciant.

Les PME et TPE sont tout à fait concernées par ces programmes car leur croissance est une des priorités de l'UE.

EFCSE propose ici une extraction d'information sur certains programmes actuellement valides, sur les sujets tels que les TIC, la sécurité numérique, la confidentialité des données, la cybersécurité, etc…

Programme H2020

Rappel

Le programme Horizon 2020, entré en vigueur le 1er janvier 2014, regroupe les financements de l'Union européenne en matière de recherche et d'innovation et s'articule autour de trois grandes priorités : l'excellence scientifique, la primauté industrielle et les défis sociétaux.

Les enjeux majeurs du programme :

- Renfort de la position de l'Union européenne dans le monde sur les domaines de la recherche, de l'innovation et des technologies ;

- Assurance de compétitivité de l'Europe via un investissement dans les technologies et les métiers d'avenir, au service d'une croissance "intelligente, durable et inclusive" ;
- Renfort de l'attractivité de l'Europe de la recherche ;
- Prise en compte des préoccupations des citoyens (santé, environnement, énergies propres...) et apport d'éléments de réponse aux défis sociétaux.

Parmi les spécificités du programme, l'augmentation de participation des PME est un des points majeurs.

Ci-après sont présentés 3 appels à projets qui entrent dans le cadre de H2020 dans un calendrier 2019 :

I - Cybersecurity H2020 / Éléments constitutifs de la résilience dans les systèmes TIC en évolution

Description

Type	Action de recherche et d'innovation		
Condition	Trois entités légales indépendantes l'une de l'autre et établies dans un pays membre de l'UE différent ou un pays associé à Horizon 2020 doivent participer au projet pour que la proposition remplisse les conditions d'éligibilité.		
	Modèle à stage unique		
Nom de l'appel	Cybersecurity 2020	Numéro de référence	SU-ICT-02-2020
Numéro de l'appel	H2020-SU-ICT-2018-2020		
Ouvert	25 juillet 2019	Deadline	19 novembre 2019 17 :00 :00 heure de Bruxelles

Sujet de l'appel d'offre

Les systèmes d'algorithmes, de logiciels et de hardware doivent être conçus en ayant à l'esprit dans leurs phases de design d'une manière mesurable : la sécurité, la confidentialité, la protection de la donnée et la responsabilité (accountability).

Les défis pertinents incluent :

- De développer des mécanismes qui mesureront la performance des systèmes TIC sur la cybersécurité et la confidentialité
- D'améliorer le contrôle et la confiance du consommateur de produits et de services numériques avec des outils innovants permettant d'assurer la responsabilité (accountability) des niveaux de sécurité et de confidentialité dans les algorithmes, dans les logiciels et finalement dans les systèmes IT, dans les produits et dans les services de la supply chain.

Sous-sujet

Cet appel comprend trois sous-sujets, en résultante du premier sujet, « Audit de cybersécurité/confidentialité, certification et standardisation ».

Mission

Approches innovatives pour :

- Designer et développer des validations et des tests de sécurité automatique, exploitant la connaissance de l'architecture, du code et des environnements de développement (par exemple white box)
- Designer et développer des contrôles automatiques de sécurité au niveau du code, se concentrer sur l'analyse évolutive des altérations, l'analyse des flux d'informations, l'intégrité des flux de contrôle, la politique de sécurité et la prise en compte de relation entre les cycles de vie sécurisés de développement.
- Développer des mécanismes, des indicateurs de performance clé et des mesures qui facilitent le processus de certifications au niveau des services
- Développer des mécanismes pour mieux auditer et analyses de l'open source et/ou des logiciels open license, et les systèmes ICT en respectant la cybersécurité et la confidentialité numérique.

L'aboutissement de la proposition doit mener au développement d'un niveau de maturité technologique (TRL) 5, ce qui correspond à une technologie validée dans son environnement.

Résultats attendus

Sur le court et moyen terme :

- Améliorer les opportunités du marché pour les vendeurs de composants de sécurité de l'UE
- Augmenter le niveau de confiance grâce aux développements intégrant les composants ICT et les utilisateurs finaux des systèmes SI et des services

- Protéger la vie privée des citoyens et la fiabilité des TIC
- Accélérer le développement et l'implémentation des processus de certification

Long terme :

Les produits et services de cybersécurité avancés seront développés améliorant ainsi la confiance dans le Digital Single Market.

- L'utilisation de systèmes de certification plus harmonisés augmenteront le potentiel d'affaires pour des services de cybersécurité devenant plus fiables.
- Les plateformes de validation fourniront des évaluations avec moins d'efforts par rapport à la situation actuelle et assureront une meilleure conformité aux règles et standards ainsi qu'une pertinence accrue.

Demande de contribution

La Commission juge apte de solliciter une contribution à hauteur de 4 à 5 millions d'euros mais d'autres sommes peuvent également être prises en considération.

Budget Indicatif

Le budget indicatif pour l'appel SU-ICT-02-2020 RIA est de 47 millions d'euros.

II - Digital Security 2019-2020 / Sécurité numérique et confidentialité pour les citoyens, PME et TPE

Description

Type	Action Innovante		
Condition	Trois entités légales indépendantes l'une de l'autre et établies dans un pays membre de l'UE différent ou d'un pays associé à Horizon 2020 doivent participer au projet pour que la proposition remplisse les conditions d'éligibilité.		
	Modèle à stage unique		
Nom de l'appel	Digital Security 2019-2020	Numéro de référence	SU-DS03-2019-2020
Numéro de l'appel	H2020-SU-DS-2018-2019-2020		
Ouvert	Depuis le 14 mars 2019	Deadline	22 août 2019 17 :00 :00 heure de Bruxelles

Sujet

Eliminer les vulnérabilités de cyber-attaques ou de violations de données et protéger/contrôler de manière appropriée les données sensibles. Considérant que les PMEs, compte tenu d'une carence de sensibilisation au sujet et de leurs ressources limitées (techniques et humaines) sont des proies faciles pour les attaques cyber, avec des risques plus importants.

Sous-sujet

Cet appel comprend deux sous-sujets, cette proposition est dédiée au second, « Petites et Moyennes Entreprises et Très Petites Entreprises (PME et TPE) : défenseurs de la protection des données de sécurité, privées et personnelles.

Mission

« Les propositions devront livrer des solutions innovantes pour augmenter le partage de connaissances dans la sécurité numérique des PME et TPE, entre-les PME/TPE et des fournisseurs plus larges. Les utilisateurs dans les PME/TPE devront être soutenus par la démocratisation de l'accès à des outils et à des solutions d'un niveau de sophistication varié, afin de permettre aux PME/TPE de bénéficier de solutions innovantes ciblées, adressant leurs besoins et leurs ressources

disponibles spécifiques (actuellement réservé aux organisations plus grandes, compte tenu de des coûts et des expertises internes disponibles).

La proposition devra développer des solutions ciblées, faciles d'utilisation et rentables permettant aux PME/TPE de :

- Contrôler, prévoir et évaluer de façon dynamique les risques de protection et de sécurisation de leurs données, privées et personnelles (des évaluations de l'impact de leur protection de données sont requises pour les situations énumérées dans l'article 35 du RGPD)
- Sensibiliser davantage aux vulnérabilités, attaques et risques qui influent sur leurs activités
- Gérer et prévoir les risques de protection et de sécurisation de leurs données, privées et personnelles d'une manière simple et rentable
- Construire une collaboration en ligne entre les associations de PME/TPE et les CERTs/CSIRTs, permettant ainsi à des PME/TPE individuelles de rapporter n'importe quel incident.

De plus, des outils et des procédées devront être proposés pour faciliter la participation d'utilisateurs dans les PME/TPE sur des gammes pour la cybersécurité.

L'aboutissement de la proposition doit mener au développement d'un niveau de maturité technologique (TRL) 7, ce qui correspond à la démonstration d'un système prototype dans un environnement opérationnel.

Les projets devront aussi présager des activités et envisager des ressources pour se regrouper avec d'autres projets financés sur le même sujet et avec d'autres projets pertinents dans les domaines financés par H2020.

Résultats attendus

- Une meilleure protection : les PME/TPE peuvent devenir des acteurs actifs dans le Marché Unique Numérique (DSM – Digital Single Market), exécutant la Directive NIS et suivant l'application du RGPD.
- La protection et la sécurisation de données privées et personnelles sont renforcées en tant que responsabilité partagée à tous niveaux de l'économie digitale.
- Dégâts réduits par suite de cyber-attaques, d'incidents de confidentialité ou de brèches de protection des données.
- Ouverture d'une voie pour un environnement numérique de l'UE digne de confiance, bénéficiant à tous les acteurs économiques et sociaux.

Demande de contribution

La Commission juge apte la sollicitation d'une contribution à hauteur de 3 ou 4 millions d'euros mais d'autres sommes peuvent également être prises en considération.

III - Digital Security 2019-2020 / Sécurité numérique, vie privée/confidentialité, protection des données et responsabilité (accountability) dans des secteurs critiques

Description

Type	Action de recherche et d'innovation		
Condition	Trois entités légales indépendantes l'une de l'autre et établies dans un pays membre de l'UE différent ou d'un pays associé à Horizon 2020 doivent participer au projet pour que la proposition remplisse les conditions d'éligibilité.		
	Modèle à stage unique		
Nom de l'appel	Digital Security 2019-2020	Numéro de référence	SU-DS05-2018-2019
Numéro de l'appel	H2020-SU-DS-2018-2019-2020		
Ouvert	Depuis le 14 mars 2019	Deadline	22 août 2019 17 :00 :00 heure de Bruxelles

Sujet de l'appel

Dans le contexte cyber/numérique, certains secteurs sont identifiés en tant que critiques en raison de leurs besoins en cybersecurité en ligne avec la directive NIS (Network and Information Systems).

Secteurs critiques : transport, infrastructures du marché financier, secteur de la santé (cadre des soins de santé, incluant les hôpitaux et les cliniques privées), etc. Il y a une importance particulière à définir et fournir des exigences communes spécifiques à chaque secteur, et à construire une protection By Design et By Default de la sécurité numérique et des données privées et personnelles, avec des principes et des standards clairement tournés vers les infrastructures critiques de ces secteurs pour assurer l'intégrité et la confidentialité de la donnée.

Les services de soins de la santé sont améliorés à travers les TIC (technologies de l'information et de la communication) qui permettent à des infrastructures, systèmes, entités et personnes variés d'être interconnectés.

Avec la complexité grandissante de la Supply chain pharmaceutique, la cybersécurité est critique pour la sûreté/sécurité et des approches nouvelles sont nécessaires pour assurer la traçabilité et les échanges/livraisons à zéro erreur. De plus,

les exigences liées aux législations de la protection de la donnée doivent aussi être prises en considération, car la santé est un secteur très sensible de ce point de vue.

Les cyber-attaques et les brèches causées aux données menacent les systèmes de gestion de documents de patients vulnérables.

« L'utilisation de dispositifs médicaux connectés sont en augmentation, en particulier les portables et les dispositifs de contrôle de la santé à domicile qui transmettent souvent des données sensibles sur des réseaux sans fils non sécurisés depuis le domicile du patient jusqu'aux hôpitaux, exposant la vie privée et les données personnelles des patients et la résilience des infrastructures de soins de santé. »

La participation de PME à ce projet est fortement encouragée mais pas obligatoire.

Sous-sujet

Cet appel comprend trois sous-sujets.

Cette proposition est dédiée au secteur de la santé, « La sécurité numérique, la protection des données privées et personnelles dans l'écosystème de la santé » et devra traiter d'au moins deux des aspects génériques suivants, en identifiant menaces et attaques communes, en développant des preuves de concepts pour gérer les risques de cybersécurité et de confidentialité, en identifiant des vulnérabilités spécifiques, des effets de propagation et des contre-mesures pour le secteur de la santé, en développant et en testant des solutions cyber basées sur l'innovation et en les validant via des pilotes/démonstrations.

Pendant les étapes de conception et de développement, les spécificités des domaines/secteurs critiques, telle que la complexité d'infrastructure et leur grande échelle, doivent être prises en considération. Ces pilotes/démonstrations sont encouragés à faire appel à des infrastructures cyber transversales pertinentes et à des capacités développées dans d'autres projets.

« Les propositions devront aussi inclure (mais ne devront pas être limitées à) la livraison d'aspects sociaux spécifiques à la sécurité numérique, en rapport avec la formation, tout particulièrement la formation pratique et opérationnelle incluant :

- L'augmentation des dynamiques de formation et des méthodes de sensibilisation, pour égaler/dépasser le même taux d'évolution des cyber attaquants ; c'est-à-dire de nouvelles méthodes de sensibilisation/formation offrant plus de pistes de qualification, afin d'intégrer efficacement les travailleurs et employés de systèmes de sécurité TIC dans les e-compétences du marché Européens
- L'Intégration de la sensibilisation dans des écosystèmes humains, de compétences, de services et de solutions qui sont rapidement capables de s'adapter aux évolutions de cyber attaquants voire même de les surpasser. »

Mission

« Les propositions répondant à ce sous-sujet devront contribuer à la mise en œuvre pratique de législation pertinente de l'UE (par exemple NIS, eIDAS ou RGPD) dans l'écosystème complexe de la santé, impliquant toutes parties prenantes (par exemple les responsables de sécurité, les administrateurs informatiques, les opérateurs, auditeurs, développeurs, fabricants, intégrateurs, responsables de la protection des données) de toutes les entités dans l'écosystème de la santé et considérant tous types de données traitées, avec une attention particulière sur les données sensibles telles que définies par le RGPD.

Les propositions de ce sous-sujet devront aborder au moins deux des éléments suivants :

- En collaboration avec toutes les parties prenantes dans l'écosystème de la santé et les CERTs/CSIRTS, développer des bases de données dynamiques sur les vulnérabilités, pour collecter, télécharger (upload), maintenir et disséminer les vulnérabilités de systèmes médicaux basés sur des TIC, de technologies, d'applications et de services (améliorant ceux des TIC générique, par exemple NIST, MITRE). Construire des taxonomies dynamiques pour des attaques en relation avec le domaine médical, pour devenir la base de construction de systèmes de gestion d'incidents de cybersécurité dans le secteur de la santé.
- Livrer des cadres et des outils dynamiques sophistiqués et fondés sur des preuves, sur l'évaluation de risques, sur la protection des données privées et personnelles et de sécurité, pouvant faire face à des effets en cascade de menaces et propager les vulnérabilités dans des infrastructures de santé interconnectées, dans des entités, des systèmes, des services de supply chain et des applications (conformes avec les standards de cybersécurité appropriés, par exemple ISO27001, ISO27005, ISO28000).
- Fournir des outils collaboratifs, tenant compte des problématiques de confidentialité (privacy-aware), permettant aux parties prenantes de la santé d'accéder à et de partager l'information (où son intégrité est garantie), conseiller sur et fournir les meilleurs/bonnes pratiques sur le traitement d'incident via des interactions en adéquation avec les bénéficiaires des systèmes de santé, dans le respect de la protection de leurs données privées et personnelles.

L'aboutissement de la proposition doit mener au développement d'un niveau de maturité technologique (TRL) 7, ce qui correspond à une démonstration d'un système prototype dans un environnement opérationnel. »

Résultats attendus

Tout ce qui suit devra être mis en perspective en considérant les secteurs/domaines critiques respectifs qui seront adressés (dans ce cas, le secteur de la santé).

Sur le court-terme :

- Les facilitateurs technologiques et opérationnels dans la Réponse et Récupération (Response and Recovery) contribueront au développement du Réseau CSIRT à travers l'UE (l'une des cibles clé de la directive NIS).
- L'identification d'aspects génériques et spécifiques pertinents en relation avec la confidentialité numérique et la cybersécurité.
- Des systèmes holistiques avancés et preuves de concepts (POC) innovants pour gérer la cybersecurité et les risques de confidentialité.
- Des avancées dans l'analyse de pointe d'aspects spécifiques, en relation avec des menaces, des attaques ou des vulnérabilités cyber.
- De bonnes analyses d'effets en cascade de menaces cyber spécifiques au sein de la supply chain.
- L'amélioration de la cybersécurité sur le partage d'information et la collaboration entre parties prenantes et parmi les CERTs/CSIRTs.
- Des solutions de gestion de la sécurité plus ciblées et acceptables adressant des spécificités.
- Déclencher l'adoption rapide des meilleurs pratiques en matière de cybersécurité/ confidentialité/ protection des données personnelles.

Sur le moyen-terme :

- Meilleures technologies et services de Réponse et Récupération qui aideront les organisations à réduire significativement l'impact de menaces, vulnérabilités et brèches propagées et en cascade.
- Améliorer la protection contre des menaces avancées, nouvelles et émergentes.
- Améliorer la gouvernance de la sécurité.
- Un marché de la cybersécurité meilleur et plus mature.
- Réduire l'impact de brèches avec des niveaux variables de succès à pénétrer les défenses.

Sur le long-terme :

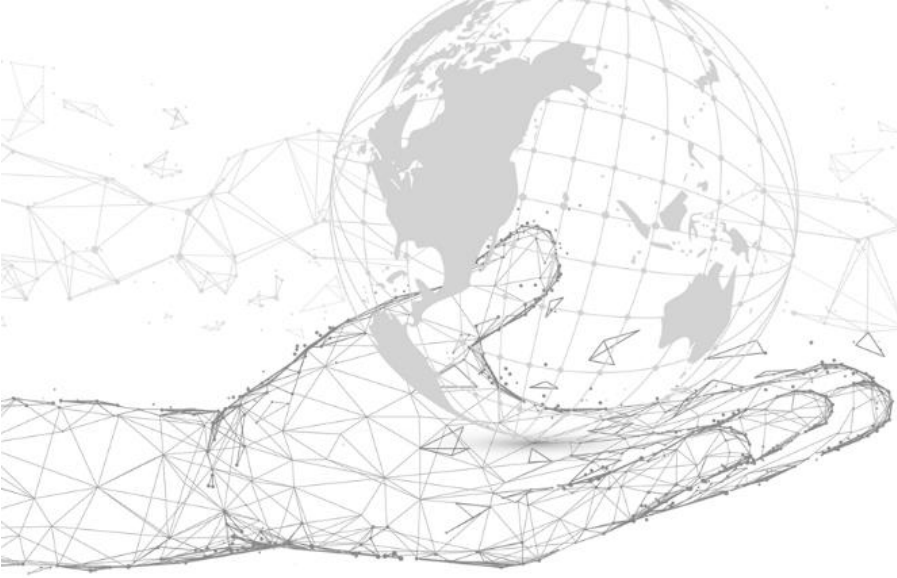
- Une meilleure cybersécurité pour des standards spécifiques, qui déclencheront une adoption rapide des meilleures pratiques dans les industries connexes.
- Etablir des chaines de confiance parmi les entités dans les écosystèmes.
- Une meilleure mise en œuvre des législations pertinentes de l'UE (par exemple NIS, eIDAS, RGPD).
- Des entreprises/organisations plus volontaires et impliquées dans la promotion de la cybersécurité, la protection des données privées et personnelles dans la totalité de l'écosystème spécifique de l'UE. »

Demande de contribution

La Commission juge apte de solliciter une contribution à hauteur de 5 millions d'euros mais d'autres sommes peuvent également être prises en considération.

Budget indicatif

Le budget indicatif pour l'appel SU-DS05-2018-2019 RIA est de 10 millions d'euros.



Programme : « Connecting Europe Facility »

Le « Connecting Europe Facility - Telecom » [CEF] est un programme européen permettant de financer les projets d'intérêt commun, notamment pour l'interconnexion en Europe, il est un instrument central de « l'European Infrastructure Package » véritable train de mesures sur les infrastructures européennes.

Les CEF est destiné à stimuler la croissance économique, à soutenir l'achèvement et le fonctionnement du marché intérieur, à obtenir de réelles améliorations dans le quotidien des citoyens, des entreprises de toute taille (dont les PME) et des administrations, tout ceci via le déploiement d'une infrastructure transeuropéenne solide.

Les projets soutenus doivent contribuer à la création d'un écosystème européen de services numériques interopérables et interconnectés pour le soutien du marché unique numérique.

Un budget de 1,04 milliard d'euros a été affecté aux services numériques transeuropéens pour la période 2014-2020. L'INEA[1] est responsable de l'exécution d'environ 500 millions d'euros du budget de CEF Telecom sous forme de subventions au cours de la même période.

Les 33 propositions sélectionnées, reçoivent un financement de près de 11,4 millions d'euros, en provenance de l'appel 2018 CEF sur la cybersécurité, et incluent des candidats de 17 États membres de l'UE, pour augmenter les aptitudes d'acteurs de la cybersécurité.

Ce financement contribue à la mise en œuvre de la directive NIS[2], premier élément de la législation européenne qui vise à renforcer la préparation de l'Europe en matière de cybersécurité.

[1] Innovation and Networks Executive Agency INEA

2 Directive NIS : Network and Information Security – UE 2016-1148. Objectif : assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne

Un nouvel appel à la cybersécurité (2019-2 CEF Telecom) a été ouvert le 14 mai dernier, avec un budget de 10 millions d'euros (indicatif). Dans ce cadre sont programmés les appels à propositions listés ci-dessous :

Appel à proposition[3]	Ouverture	Date limite / réponse
CEF-TC-2019-2 Business Registers Interconnection System (Budget indicatif : €2 millions)	04-juil-19	14-nov-19
CEF-TC-2019-2 CYBERSECURITY (Budget indicatif : €10 millions)	04-juil-19	14-nov-19
CEF-TC-2019-2 eHealth (Budget indicatif : €5 millions)	04-juil-19	14-nov-19
CEF-TC-2019-2 eProcurement (Budget indicatif : €3 millions)	04-juil-19	14-nov-19
CEF-TC-2019-2 European e-Justice (Budget indicatif : €3 millions)	04-juil-19	14-nov-19
CEF-TC-2019-2 European Platform for Digital Skills and Jobs (Budget indicatif : €1 million)	04-juil-19	14-nov-19
CEF-TC-2019-2 Public Open Data (Budget indicatif : €5 millions)	04-juil-19	14-nov-19

[3] Date à titre indicatif