RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

PRÉSENTATION DES APPELS À PROJETS CYBERSÉCURITÉ DES PROGRAMMES « *DIGITAL EUROPE* » ET « *HORIZON EUROPE* »

PAR LE CENTRE FRANÇAIS
DE COORDINATION CYBER (NCC-FR)

Les informations évoquées dans cette présentation sont à considérer comme un résumé. Veuillez vous référer aux programmes de travail officiels de Digital Europe Cyber et Horizon Europe pour le détail des appels à projets.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

1. INTRODUCTION

LE PROGRAMME *DIGITAL EUROPE*

L'UE s'efforce de **renforcer son leadership et son autonomie stratégique dans le domaine de la cybersécurité**.

Le programme de financements ***Digital Europe*** est conçu pour co-investir dans le déploiement de solutions de cybersécurité. Il intervient en complément du programme *Horizon Europe*, destiné à financer la recherche européenne, et permet d'avoir un effet multiplicateur sur les résultats de la recherche.

Le programme de travail *Digital Europe* 2025-2027 comprend, pour la première fois, un axe stratégique « **cybersécurité et confiance** » qui tient compte de toutes les obligations légales découlant des différentes réglementations européennes (NIS 2, CRA, Cybersecurity act, Cyber solidarity act).

390 millions d'euros vont être alloués à des projets de cybersécurité au cours de la période 2025-2027, via des appels à projets européens.

LE PROGRAMME *HORIZON EUROPE*

Objectifs de l'UE :

- Renforcer les bases scientifiques et technologiques de l'Union ;
- Stimuler sa compétitivité, y compris celle de son industrie ;
- Concrétiser les priorités politiques stratégiques de l'Union ;
- Contribuer à répondre aux problématiques mondiales, dont les objectifs de développement durable.

Le programme de financements ***Horizon Europe*** est conçu pour soutenir **la recherche et l'innovation.** Les activités d'Horizon Europe seront réalisées par le biais **d'appels à propositions ouverts et concurrentiels.**

Le programme de travail *Horizon Europe* 2025 comprend **90,5 millions d'euros qui vont être alloués à des projets de R&D en cybersécurité en 2025, via des appels à projets européens.**

LE CENTRE DE COORDINATION CYBER FRANÇAIS (NCC-FR)

Le **Centre européen de compétences en cybersécurité (ECCC)** et son **réseau de centres nationaux de coordination (NCC)** font partie des piliers de la stratégie cyber de l'UE.

Centre européen de compétences en cybersécurité (ECCC) :

- Elabore et met en œuvre un programme stratégique commun pour le développement et le déploiement de technologies cyber dans des domaines stratégiques.

Centre de coordination cyber français (NCC-FR) :

- Rend visible les dispositifs de soutien financiers européens.
- Développe des programmes nationaux de soutien financier.
- Anime la communauté cyber.
- Travaille les NCC des autres Etats membres.

Programmes de financements *Horizon Europe* et *Digital Europe*

→ Identifier des possibilités de consortiums.

→ Accompagnement aux candidatures, en collaboration avec Bpifrance.

2. APPELS À PROJETS CYBERSÉCURITÉ DU PROGRAMME *DIGITAL EUROPE*

Les informations qui suivent sont à considérer comme un résumé. Veuillez vous référer au programme de travail Digital Europe Cyber disponible sur le site de l'ECCC.

DIGITAL EUROPE CYBER 2025 - 2027

Sujets d'investissements

Soutien à l'adoption de nouvelles technologies pour la cybersécurité (IA et PQC) et sécurisation de leur mise en œuvre.

142 millions d'euros

Mise en œuvre du *Cyber Solidarity Act* en contribuant à la consolidation du système européen d'alerte en matière de cybersécurité.

121 millions d'euros

Mise en œuvre des politiques améliorant la résilience de l'UE (NIS2, *Cyber Security Act* et *Cyber Resilience Act*) tout en fournissant aux PME les outils nécessaires pour se conformer aux exigences réglementaires.

118 millions d'euros

Note : pour l'ensemble des appels à projets Digital Europe Cyber, seules « les entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres » sont éligibles (art 12.5).

DIGITAL EUROPE : APPELS À PROJETS CYBER 2025 – 27

Co-funded by the European Union

NCC-FR FRANCE CYBERSECURITY COORDINATION CENTRE

Tableau synthétique des appels à projets Cybersécurité

Programme *Digital Europe*
Période
2025 – 2027

SUJETS ET ALLOCATIONS (EN MILLIONS D'EUROS)		2025	2026	2027	TOTAL
Nouvelles technologies : IA et transition PQC					**142 M€**
2.1	Outils de cybersécurité, technologies et services reposant sur l'IA	15 M€	15 M€	15 M€	45 M€
2.2	Renforcement des capacités cyber des PME européennes avec des solutions d'IA cybersécurisées		20 M€		20 M€
2.3	Déploiement d'une infrastructure européenne de test pour la transition PQC	25 M€			25 M€
2.4	Transition post-quantique des infrastructures de clés publiques	15 M€			15 M€
2.5	Migration des Cyber Hubs vers la PQC			7 M€	7 M€
2.6	Incitation à l'innovation en matière de cybersécurité pour les PME	15 M€		15 M€	30 M€
Implémentation du *Cyber Solidarity Act*					**121 M€**
2.7	Cyber Hubs nationaux	20 M€	15 M€		35 M€
2.8	Cyber Hubs transfrontaliers	20 M€		20 M€	40 M€
2.9	Renforcement de l'écosystème Cyber Hubs et développement du partage d'information		2 M€		2 M€
2.10	Tests de préparation coordonnés et autres actions de préparation	5 M€	15 M€	20 M€	40 M€
2.11	Assistance mutuelle		2 M€	2 M€	4 M€
Actions additionnelles pour améliorer la cyber résilience de l'UE					**118 M€**
2.12	Améliorer le réseau NCC	10 M€	16 M€	20 M€	46 M€
2.13	Renforcer les capacités et capabilités cyber européennes conformément aux exigences législatives		20 M€	12 M€	32 M€
2.14	Actions dédiées au renforcement cyber des hôpitaux et prestataires de soins	30 M€			30 M€
2.15	Technologies à double usage		10 M€		10 M€
Actions de support au programme		3	3	3	**9 M€**
TOTAL (EN MILLIONS D'EUROS)		**158 M€**	**118 M€**	**114 M€**	**390 M€**

3. APPELS À PROJETS CYBERSÉCURITÉ DU PROGRAMME *DIGITAL EUROPE* OUVERTS EN 2025

Note préalable :

- Les informations qui suivent sont à considérer comme un résumé. Veuillez vous référer au programme de travail Digital Europe Cyber disponible sur le site de l'ECCC.
- Pour l'ensemble des appels à projets Digital Europe Cyber, seules « les entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres » sont éligibles (art 12.5).

APPELS À PROJETS CYBER *DIGITAL EUROPE* 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Co-funded by the European Union

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

Ouverts de juin à octobre 2025	**IA et transition PQC**	**Transition post-quantique des infrastructures de clés publiques**	50%	Subvention	15 M€	Tous les acteurs de la chaine des infrastructures de clés publiques (Public Key Infrastructure)
	Implémentation du *Cyber Solidarity Act*	**Tests de préparation coordonnés et autres actions de préparation** [reconduit en 2027]	50%	Subvention	5 M€ pour 2025	Autorités nationales chargées de la cybersécurité, CSIRTs, acteurs publics (NIS2/CRA/CSA/CySol/DORA)
	Cyber résilience de l'UE	**Actions dédiées au renforcement cyber des hôpitaux et prestataires de soins**	50%	Subvention	30 M€	Acteurs publics et privés de toutes tailles
Ouverts de septembre 2025 à janvier 2026	**IA et transition PQC**	**Outils de cybersécurité, technologies et services reposant sur l'IA** [reconduit en 2026 et 2027]	50%	Subvention	15 M€ pour 2025	Fournisseurs de technologies, opérateurs de cyberhubs, centres de recherche, entités de cybersécurité, secteur public, entités soumises à directive NIS 2, autres parties prenantes concernées soutenant le déploiement de solutions d'IA cybersécurisées.
		Incitation à l'innovation en matière de cybersécurité pour les PME [reconduit en 2027]	50% et 75% pour PME	Subvention	15 M€ pour 2025	PME, entités privées et publiques mettant en œuvre la directive NIS 2, la Cyber Resilience Act, centres de recherche, etc.
	Implémentation du *Cyber Solidarity Act*	**Cyber Hubs nationaux** [ouvert de septembre 2025 à janvier 2026 + reconduit en 2026]	50% 50%	Subvention, Commande publique	20 M€ pour 2025	Acteurs publics agissant comme cyber hubs, identifiés par l'état membre
		Cyber Hubs transfrontaliers [ouvert de septembre 2025 à janvier 2026 + reconduit en 2027]	50% 75%	Subvention, Commande publique	20 M€	Acteurs publics agissant comme cyber hubs, identifiés par l'état membre
Date inconnue	**IA et transition PQC**	**Appel d'offres : Déploiement d'une infrastructure européenne de test pour la transition PQC** [2025 uniquement]	100%	Commande publique	25 M€	PME, startups, centres de recherche, entités publiques

Nouvelles technologies : IA et transition vers la PQC

Appel à projets « Transition post-quantique des infrastructures de clés publiques »
Ouverture : juin à octobre 2025

Objectifs :

- Une intégration effective des algorithmes de PQC au sein des infrastructures de clés publiques (PKI) en garantissant la rétrocompatibilité avec les PKI actuelles.
- Cette intégration doit offrir des stratégies de migration efficientes et de solides garanties de continuité des activités.
- L'appel s'adresse aux différents acteurs impliqués dans les écosystèmes PKI et les chaînes d'approvisionnement et de valeur, tels que les autorités de certification (AC), les AC intermédiaires, les chercheurs, les utilisateurs finaux dans différents domaines et les fournisseurs.

Typologie	Subvention
Durée	36 mois
Taux	50%
Montant	15 M€ (Projets de 4 à 5 mil)
Entités cibles	Tous les acteurs de la chaine des infrastructures de clés publiques (Public Key Infrastructure)

Périmètre :

- Développer des solutions hybrides et des outils : Concevoir des "combineurs" pour les signatures numériques et les mécanismes d'encapsulation de clés, et développer de nouveaux protocoles
- Assurer une transition sécurisée et compatible : La migration doit garantir la compatibilité avec les systèmes existants (pré-quantiques) tout en intégrant des solutions PQC. L'accent est mis sur des combinaisons hybrides.
- Prendre en compte les contraintes des secteurs critiques : Les solutions doivent répondre aux exigences de sécurité, performance et continuité des activités dans des domaines sensibles (gouvernement, télécoms, e-Santé, etc.), et s'adapter aux spécificités de l'IoT et des cartes à puce.
- Favoriser la collaboration et la sensibilisation (Consortiums diversifiés). Des activités de formation et de sensibilisation sont essentielles pour guider les parties prenantes dans cette transition complexe.

Mise en œuvre du *Cyber Solidarity Act*

Appel à projets « Tests de préparation coordonnés et autres actions de préparation »
Ouverture : juin à octobre 2025

Objectifs :

- Compléter les actions des Etats membres pour améliorer le niveau de protection et de résilience aux cyberattaques.
- Coordonner les tests de préparation des entités appartenant aux secteurs critiques dans l'ensemble de l'Union, prendre en compte les TIC et autres systèmes de contrôle opérationnel, technologique ou industriel.

Périmètre :

- Développer des scénarios de tests d'intrusion (réseaux, applications, cloud, systèmes industriels, IoT) et soutenir leur exécution sur les infrastructures critiques.
- Déployer des outils numériques et des infrastructures tel que des "cyber-ranges" standardisés capables de simuler des environnements de secteurs critiques pour faciliter les exercices, notamment transfrontaliers.
- Évaluation et amélioration des capacités cyber : Tester les capacités des entités et des secteurs à prévenir, détecter et répondre aux incidents (y compris les tests de résistance sectoriels), et fournir des services de conseil pour l'amélioration de la sécurité.
- Soutenir l'implémentation de processus d'évaluation des menaces et l'analyse de scénarios de risque personnalisés.

Typologie	Subvention
Durée	36 mois
Taux	50 %
Montant	5 M€ en 2025 [Un AaP similaire de 15M€ ouvrira en 2026, un autre de 20M€ en 2027. Au total, 40M€ sur 2025-27]
Entités cibles	Les autorités publiques compétentes en matière de cybersécurité, les CSIRTs, les autorités publiques sujettes à la directive NIS 2 (CSA, CRA, CSoA, DORA, etc), les industriels, autres entités publiques ou privées qui peuvent soutenir la mise en œuvre de la directive NIS 2.

Cyber résilience de l'UE

Appel à projets « Actions dédiées au renforcement cyber des hôpitaux et prestataires de soins »
Ouverture : juin à octobre 2025

Objectifs :

- Soutenir le renforcement de la cybersécurité des hôpitaux et des prestataires de soins de santé.
- S'assurer que les hôpitaux et les prestataires de soins peuvent détecter, surveiller et répondre aux cyberattaques (ransomware).

Typologie	Subvention
Durée	18 – 24 mois
Taux	50 %
Montant	30 M€
Entités cibles	Acteurs publics et privés (clusters régionaux ou nationaux)

Périmètre :

Développer les capacités de surveillance des SI et de réponse aux incidents. L'initiative soutiendra des projets pilotes regroupant des clusters régionaux et nationaux.

Projets pilotes :

- Etablir l'état de l'art des produits et ressources de cybersécurité de pointe nécessaires (incluant SOC ou SIEM, CTI)
- Développer des plans techniques adaptés aux besoins (Recommandations de mise en œuvre et estimations de coûts)
- Réaliser des test physique pour prouver efficacité opérationnelle (Deux Etats membres)
- Former et sensibiliser le personnel à la cybersécurité
- Entreprendre de vastes activités de diffusion des bonnes pratiques à travers l'UE, dans le but d'aider à répliquer aussi largement que possible.
- Les projets pilotes soutiendront les établissements de santé dans leur conformité avec la Directive NIS2.

Nouvelles technologies : IA et transition vers la PQC

Appel à projets « Outils de cybersécurité, technologies et services reposant sur l'IA »
Ouverture : septembre 2025 à janvier 2026

Objectifs :

- Développer et déployer des technologies basées sur l'IA à destination des autorités de cybersécurité (Cyber Hubs nationaux et transfrontaliers, CSIRT, NCC, entités NIS2, etc.) pour renforcer leurs capacités d'analyse, de partage, de détection et de prévention des menaces et incidents cyber, ou encore de récupération.
- Production d'analyses plus efficaces pour les renseignements sur la menace cyber (CTI), automatisation de processus à grande échelle, traitement plus rapide et plus évolutif de la CTI.
- Promouvoir la sécurité de l'IA (des systèmes d'IA sûrs et éthiques).

Périmètre :

Les solutions IA proposées doivent être cyber-sécurisées.
Les activités doivent intégrer au moins l'une des fonctions suivantes :

- *Détection continue des MOA*
- *Création de flux de renseignements cyber*
- *Accroissement de la vitesse de réponse à incidents*
- *Reverse engineering de malware*
- *Gestion et triage des vulnérabilités*
- *Prévention par pentest et scan de vulnérabilité*
- *Protection des accès anormaux (ZTNA)*
- *Anonymisation et partage de renseignements d'intérêt*
- *Contribution à l'évaluation en vue de certification des modèles d'IA*

→ Voir liste complète pour détails.

Dans certains cas, un accès à l'infrastructure EuroHPC pourra être accordé.

Typologie	Subvention
Durée	36 mois
Taux	50%
Montant	15 M€ en 2025 [Reconduit en 2026 et 2027. Au total, 45M€ alloués à ce sujet sur 2025-27]
Entités cibles	Fournisseurs de technologies, opérateurs de cyberhubs, centres de recherches, entités de cybersécurité, secteur public, entités soumises à la directive NIS 2, secteur privé, autres parties prenantes concernées soutenant le déploiement de solutions d'IA cybersécurisées.

Nouvelles technologies IA et transition vers la PQC

Appel à projets « Incitation à l'innovation en matière de cybersécurité pour les PME »
Ouverture : septembre 2025 à janvier 2026

Objectif

Améliorer la préparation de l'industrie et du marché aux exigences en matière de cybersécurité pour les PME, telles que spécifiées dans la législation européenne (e.g. Cyber Resilience Act).

Périmètre

Les propositions doivent contribuer à la réalisation d'au moins un de ces objectifs :

- Outils et services innovants qui soutiennent les PME pour se mettre en conformité avec la législation européenne.
- Outils et services innovants qui soutiennent les PME pour la notification d'un incident, la récupération, et l'échange avec les autorités compétentes (CSIRT, Cyberhubs, ISAC).
- Améliorer la sécurité et les processus et notifications dans l'UE.
- Améliorer la sécurité des réseaux et systèmes d'informations dans l'UE.
- Préparation du marché et de l'industrie pour l'implémentation du Cyber Resilience Act.
- Soutien à la certification, conformément au Cybersecurity Act.
- Soutien aux prestataires de la chaîne d'approvisionnement pour leurs auto-évaluations et leurs certifications.
- Surmonter le défi de trouver les compétences techniques nécessaires pour faire face à un paysage technologique complexe.
- Boîte à outils de cybersécurité soutenant les PME dans la gestion de cyberisques, la définition et mise en œuvre de leur stratégie de cybersécurité.
- Capacités de soutien et de réponses aux incidents pour les PME.

Typologie	Subvention
Durée	36 mois
Taux	50 % et 75% pour les PME
Montant	15 M€ en 2025. [Reconduit en 2027. Au total, 30M€ alloués sur 2025-27]
Entités cibles	PME, entités privées et publiques mettant en œuvre la directive NIS 2, le Cyber Resilience Act, centres de recherche, etc.

Mise en œuvre du *Cyber Solidarity Act*

Appel à projets « Cyber Hubs nationaux »
Ouverture : septembre 2025 à janvier 2026

Un Cyber Hub est un centre national d'alerte mis en place par un Etat membre pour participer au système européen d'alerte pour la cybersécurité.

Typologie	Subvention, Commande publique
Durée	36 mois
Taux	50 % pour subvention
Montant	20 M€ en 2025 [Reconduit pour 15M€ en 2026. Au total, 35M€ sur 2025-27]
Entités cibles	Institutions publiques agissant comme cyber hubs, identifié par l'Etat membre.

Objectifs :

- Créer ou renforcer les Cyber Hubs nationaux, en les dotant d'outils pour surveiller, comprendre et gérer de manière proactive les événements cyber, en collaboration avec les entités concernées telles que les CSIRT, les ISAC, etc.
- Bénéficier d'informations et de flux provenant d'autres Cyber Hubs et utiliser les données et analyses agrégées pour émettre des alertes précoces aux infrastructures critiques ciblées.
- Surveiller les infrastructures sous-marines, telles que les câbles sous-marins.

Périmètre :

- Capacités de création d'un nouveau Cyber Hub ou de renforcement d'un Cyber Hub national existant e.g. via outils d'automatisation, d'analyse et de corrélation et de flux de données couvrant le renseignement sur les cybermenaces (CTI) à différents niveaux.
- Transfert et partage de connaissances avec d'autres Cyber Hubs, formation. Les Cyber Hubs doivent s'engager à participer, sous 2 ans, à un Cyber Hub transfrontalier.
- Transformation de résultats de recherche en outils opérationnels pour l'IA avancée, l'analyse des données et d'autres outils de cybersécurité pertinents, ainsi que la poursuite des essais et la validation de ces outils dans des conditions réelles, en combinaison avec l'accès à des installations de supercalcul.
- Déploiement de solutions pour la surveillance et la protection des infrastructures sous-marines critiques.

Pour soutenir les activités des Cyber Hubs, 2 volets d'activités sont prévus :

- **Action conjointe de commande avec l'État membre hébergeant le Cyber Hub** : couvrira l'acquisition de l'infrastructure, des outils et services nécessaires à la mise en place du Cyber Hub.
- **Subvention** pour les activités d'installation et d'opérationnalisation du Cyber Hub, ses interactions, la coopération, etc.

Mise en œuvre du *Cyber Solidarity Act*

Appel à projets « Cyber Hubs transfrontaliers »
Ouverture : septembre 2025 à janvier 2026

S'adresse principalement aux nouveaux Cyber Hubs transfrontaliers. Les activités de soutien aux SOC déjà lancées dans le cadre des précédents programmes de travail DIGITAL (2021-2022 et 2023-2024) pourraient également être incluses, le cas échéant, afin de garantir la collaboration avec les Cyber Hubs transfrontaliers.

Typologie	Subvention, Commande publique
Durée	36 mois
Taux	50 % pour subvention / 75% pour achat conjoint
Montant	20 M€ en 2025. [Reconduit en 2027. Au total, 40M€ sur 2025-27]
Entités cibles	Institutions publiques agissant comme Cyber Hubs, identifiées par l'Etat membre.

Objectifs :

- Mise en place de processus, d'outils et de services pour la prévention, la détection et l'analyse des cyberattaques émergentes.
- Acquisition et/ou adoption d'outils (d'automatisation), de processus et d'infrastructures de données partagées communs pour la gestion et le partage d'informations opérationnelles contextualisées et exploitables.

Périmètre :

- Les plateformes des Cyber Hubs transfrontaliers contribueront à améliorer et à consolider la connaissance de la situation et les capacités de détection et de CTI, en soutenant le développement d'outils d'analyse de données, de détection et de réponse, grâce à la mise en commun de grandes quantités de données, y compris de nouvelles données générées en interne par les membres des consortiums.
- Les Hubs pourraient également déployer des solutions pour la surveillance et la protection des infrastructures sous-marines essentielles, telles que les câbles sous-marins, et la détection des activités malveillantes autour d'elles, afin d'améliorer la résilience et la sécurité de ces infrastructures.

Pour soutenir les activités des Cyber Hubs, 2 volets d'activités sont prévus :

- **Action conjointe de commande avec l'État membre participant** : couvrira l'acquisition de l'infrastructure, des outils et services nécessaires à la mise en place.
- **Subvention** pour les activités préparatoires à la mise en place du Cyber Hub, son interaction et sa coopération avec d'autres parties prenantes, ainsi que les coûts de fonctionnement/exploitation, permettant le fonctionnement efficace, par exemple en utilisant l'infrastructure, les outils et les services achetés dans le cadre de la passation conjointe de marchés, le personnel. des outils et des services achetés dans le cadre de la passation conjointe de marchés, du personnel. Ils indiqueront également les étapes et les résultats attendus afin de suivre les progrès accomplis.

Nouvelles technologies : IA et transition vers la PQC

Appel d'offres « Déploiement d'une infrastructure européenne de test pour la transition PQC »
Date de lancement non connue

Objectifs :

- Créer une infrastructure de tests européenne pour la transition vers la PQC, qui deviendrait une référence mondiale, accessible à différents types d'acteurs pour des tests en conditions réelles.
- Identifier les défis dans la transition vers la PQC en se centrant sur la connectivité, l'interopérabilité et l'agilité. Les tests de sécurité devront également être envisagés (basés sur des résultats d'autres projets UE).
- Soutenir la conception des tests et les évaluations de résultats et faciliter les échanges avec les acteurs qui ont déjà débuté les tests (Infrastructure ouverte aux secteurs public et privé).
- Soutenir la transition des entités publiques et privées vers la PQC pour faciliter l'émergence d'un marché européen de produits, services et outils PQC.

Typologie	**Commande publique**
Durée	48 mois
Taux	100%
Montant	25 M€
Entités cibles	PME, startups, centres de recherche, entités créées par la directive NIS 2, acteurs du secteur et acteurs de secteurs similaires

Périmètre :

- Aménagement d'un espace pour réaliser des tests physiques, accès pour des essais à distance.
- Conception et mise en œuvre de tests en situation réelle (focus connectivité, interopérabilité et agilité) pour la compréhension des conditions de fonctionnement des protocoles pour les applications.
- Identification de besoins pour la mise à jour du hardware/software et des services qui utilisent la PQC.
- Automatisation de tests de conformité et de sécurité.
- Développement et déploiement d'outils pour l'implémentation de la feuille de route européenne pour la transition vers la PQC.

4. APPELS À PROJETS CYBERSÉCURITÉ DU PROGRAMME *HORIZON EUROPE* OUVERTS EN 2025

Les informations qui suivent sont à considérer comme un résumé. Veuillez vous référer au programme de travail Horizon Europe - Cluster 3.

HORIZON EUROPE : APPELS À PROJETS CYBER 2025

Tableau synthétique des appels à projets touchant à la cybersécurité

Programme *Horizon Europe* pour l'année 2025

Ces appels à projets sont lancés par la Commission Européenne. L'ECCC se chargera d'évaluer.

Appel à projets	Type d'action	Contribution UE	Nombre de projets financés
Technologies d'amélioration de la protection de la vie privée	Recherche & innovation	3 à 4 M€	3 projets
L'IA générative pour les applications de cybersécurité	Recherche & innovation	12 à 14 M€	3 projets
Nouveaux outils et processus avancés pour la cybersécurité opérationnelle	Innovation	4.5 à 6 M€	4 projets
Évaluation de la sécurité des primitives de cryptographie post-quantique (PQC)	Recherche & innovation	2 à 3 M€	2 projets
Mise en œuvre de la sécurité des algorithmes de cryptographie post-quantique (PQC)	Recherche & innovation	2 à 3 M€	2 projets
Intégration d'algorithmes de cryptographie post-quantique (PQC) dans des protocoles de haut niveau	Recherche & innovation	2 à 3 M€	2 projets

4. LES BONNES PRATIQUES & LES ORGANISMES D'ACCOMPAGNEMENT

Etapes clés :

- **Prendre connaissance du programme de travail** (Digital Europe/Horizon Europe) et **contenus des appels à projets**. Une FàQ sera prochainement mise à disposition sur la page web.
- **Identifier son profil candidat** : coordinateur/partenaire/partenaire associé.
- **Monter un consortium : s**i besoin d'aide dans la recherche de partenaires européens, contacter le NCC-FR
- **Une fois les attendus et expertises internes identifiées, les entités sont invitées à contacter :**
  - Les pôles de compétitivité (adhésion nécessaire)
  - Les campus cyber régionaux
  - DIAG Europe/PTI de Bpifrance (Prestation d'accompagnement)

Informations pratiques :

- Le dépôt d'un projet européen se fait sur la plateforme **Funding & Tenders** qui nécessite de créer un compte et d'utiliser le numéro PIC de l'employeur.
- La rédaction d'un projet prend **minimum 3 mois**.
- Les différents services de l'entité doivent être impliqués (service juridique, financier, RH, etc.)
- Selon les appels à projets, il y a des parties clés qu'il faudra tout particulièrement soigner : implementation ; relevance ; impact.

A noter : il est recommandé de **se présenter en consortium européen** pour candidater à un appel à projet européen.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

Merci
pour votre écoute !

Un point de contact :

NCC-FR.ANSSI@SSI.GOUV.FR