GOUVERNEMENT

Liberté
Égalité
Fraternité

Co-funded by the European Union

Stratégie Nationale de Cybersécurité

Appel à projets

« Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité »

Cahier des charges

L'appel à projets est ouvert jusqu'au **9 janvier 2025 à 12h00** (midi, heure de Paris), avec une relève intermédiaire au **13 novembre 2024** (midi, heure de Paris). Les projets peuvent être soumis à compter de la date de publication de cet appel à projets (ci-après « AAP ») et pendant toute la période d'ouverture.

Les porteurs de projets sont invités à déposer leur dossier de candidature en ligne sur la plateforme de Bpifrance : https://www.picxel.bpifrance.fr/accueil

Les candidatures seront relevées à la date de clôture de l'AAP.

Toute évolution du présent cahier des charges fera l'objet d'un arrêté du Premier ministre. Il peut, le cas échéant, être modifié, notamment pour tenir compte de l'évolution des cadres de régimes d'aides européens ou pour tenir compte du retour d'expérience des relèves précédentes et procéder à un ajustement du périmètre, des orientations ou du calendrier.

En cas d'épuisement des moyens financiers affectés à cet appel à projets, celui-ci peut être arrêté de manière anticipée par arrêté du Premier ministre pris sur avis du Secrétariat général pour l'investissement (SGPI).

APPEL À PROJETS
Juillet 2024

Sommaire

Contexte et objectifs de l'AAP

Le plan d'investissement France 2030

France 2030 a pour objectif de consolider et développer les positions françaises dans les domaines d'avenir, en cohérence avec les impératifs de la transition énergétique et écologique. France 2030 traduit une double ambition : transformer durablement des secteurs clés de notre économie (santé, énergie, automobile, aéronautique, espace) par l'innovation technologique, et positionner la France non pas seulement en acteur, mais bien en leader du monde de demain. France 2030 soutient l'ensemble du cycle de vie de l'innovation - de la recherche fondamentale à l'émergence d'une idée, la production d'un produit ou service nouveau, jusqu'à l'industrialisation de ce dernier.

Dans la continuité des programmes d'investissements d'avenir et de France Relance, France 2030 contribue à la préparation de l'avenir en intégrant les nouveaux enjeux révélés par la crise actuelle autour de trois objectifs communs qui guident les choix d'investissements de l'ensemble du programme :

- La compétitivité de notre économie ;
- La transition écologique et solidaire ;
- La résilience et la souveraineté de nos modèles d'organisation socio-économiques.

Plus d'informations sur : France 2030 : un plan d'investissement pour la France de demain | Gouvernement.fr

Dans le cadre de cet appel à projets, France 2030 apporte la moitié de l'enveloppe totale de soutien financier. La seconde moitié est apporté par l'Union Européenne au titre du projet NCC-FR, co-financé par le programme Digital Europe.

La stratégie nationale pour la cybersécurité

Le numérique est aujourd'hui présent dans tous les pans de la vie des Français. Support de nombreuses innovations qui bénéficient à chacun, il induit également de nouveaux risques en matière de sécurité et de souveraineté. En outre, le développement du télétravail durant la crise sanitaire a contribué à rendre plus ténue la frontière entre les outils informatiques professionnels et personnels, augmentant d'autant la vulnérabilité des systèmes. Les tensions internationales actuelles ont également entrainé une hausse du niveau des menaces dans le cyberespace. Dans ce cadre, le Gouvernement a souhaité, *via* la stratégie nationale pour la Cybersécurité, accompagner le développement de la filière française de la cybersécurité. La stratégie vise ainsi à faire émerger des champions français de la cybersécurité, tant pour accompagner le développement d'une filière au potentiel économique important que pour garantir à notre pays la maîtrise des technologies essentielles à la garantie de sa souveraineté.

À l'horizon 2025, l'objectif assigné à cette stratégie est l'atteinte d'un chiffre d'affaires de 25 milliards d'euros pour la filière, un total de 75 000 emplois et l'émergence de trois licornes françaises en cybersécurité. Pour cela, la stratégie s'articule autour de 5 axes :

1. Développer des solutions souveraines et innovantes de cybersécurité ;
2. Renforcer les liens et synergies entre les acteurs de la filière ;
3. Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales ;
4. Former plus de jeunes et professionnels aux métiers de la cybersécurité, actuellement fortement déséquilibrée ;
5. Soutenir le développement des entreprises *via* des investissements en fonds propres.

Pour en savoir plus : https://www.gouvernement.fr/cybersecurite.

Stratégie européenne en matière de cybersécurité

En application du règlement 2021/887, le Centre européen de compétences en matière de cybersécurité (ECCC) et le Réseau de centres nationaux de coordination (NCC) sont établis. Sous l'impulsion de la Commission européenne, les États membres de l'Union européenne se sont ainsi dotés d'un réseau de NCC en cybersécurité. Cet assemblage constitue le nouveau dispositif destiné à soutenir l'innovation et la politique industrielle en matière de cybersécurité à l'échelle européenne. Il doit permettre de renforcer les capacités de la communauté du secteur européen de la cybersécurité en permettant le déploiement et l'acquisition de solutions, en accompagnant la mise en œuvre des règlements européens visant la cybersécurité et en favorisant l'excellence et la valorisation de la recherche de l'Union européenne en la matière.

L'ECCC et le Réseau des NCC travaillent de concert pour mettre en commun et orienter les ressources de l'UE et de ses États membres vers les domaines où l'investissement est requis. A ce titre, l'ECCC et le Réseau des NCC ont construit et publié un agenda stratégique indiquant leurs priorités : les processus et l'outillage cyber, la transition vers la cryptographie post-quantique, le soutien à la certification harmonisée et la compétitivité de l'industrie, ainsi que le développement et renforcement des compétences en matière de cybersécurité via la formation.

Le « soutien financier à des tiers » (FSTP)[1] fait partie des dispositifs de financement vers l'écosystème. Également appelé « financement en cascade », il vise les projets d'innovation de plus courte durée et finance des activités de R&D, de prototypage (testing & qualification). Dans le cadre de ce dispositif, les NCC sont habilités à redistribuer des fonds européens via des appels à projets simplifiés ciblant des tiers, et en particulier des entreprises (PME et startups). Ces appels à projets financés par l'Union européenne sont généralement compétitifs pour :

- Sélectionner des startups ou des scale-ups technologiques à des fins d'accélération ou d'incubation ;
- Soutenir des pilotes, des démonstrations ou des expériences sur une technologie ou un cadre innovant spécifique ;
- Intégrer d'autres participants au projet afin d'en étendre la portée ou d'accomplir des tâches spécifiques.

L'appel à projets « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité » s'inscrit dans ce dispositif et intervient dans le cadre des missions portées par le NCC français (NCC-FR). A ce titre, il est financé à parts égales par le plan d'investissement France 2030 et par la Commission européenne sur les fonds du programme Digital Europe.

Plus d'informations sur : https://cybersecurity-centre.europa.eu/nccs_fr

Contexte et objectifs de l'appel à projets « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité »

En 2022, l'ANSSI a été désignée pour incarner le Centre National de Coordination français (NCC-FR). A ce titre l'agence assure :

- L'accompagnement au montage de projets européens dans le cadre des programmes Horizon Europe et Digital Europe ;
- L'animation de la communauté française de la cybersécurité et son insertion dans le réseau des centres nationaux (NCC) ;
- La contribution française à l'établissement du Centre Européen de Compétences pour l'industrie, les technologies et la recherche en matière de cybersécurité (ECCC) ;

[1] Terme anglais : Financial Support for Third Parties (FSTP)

- La redistribution de fonds européens pour la recherche et le développement et le déploiement de technologies en cybersécurité via des appels à projets nationaux de type « Soutien financier à des tiers » (FSTP).

Dans sa mission de redistribution de fonds européens, le NCC-FR a pour mission de soutenir l'offre nationale en cybersécurité, à ses différents stades de maturité, en cohérence avec la stratégie nationale. L'écosystème de la cybersécurité français a atteint un premier palier de maturité caractérisé par un vivier enrichi de PME et startups innovantes. Dans ce contexte, il existe toujours des segments d'intérêt stratégique où le soutien de l'État permettra de renforcer l'offre française.

L'appel à projets « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité » vise à soutenir le développement de solutions innovantes de confiance par les PME et startups. Les objectifs poursuivis sont l'émergence de prototypes et démonstrateurs sur des verrous techniques, la montée en maturité de l'offre de prestations cyber et l'amélioration de la capacité de projection dans les activités de normalisation :

- Axe 1 – Solutions cyber et développements techniques
- Axe 2 – Soutien aux prestataires préfigurant une démarche de qualification PAMS
- Axe 3 – Soutien aux PME et startups dans le champ de la normalisation

Projets attendus

Les porteurs de projet attendus sont des Très Petites Entreprises (TPE) et Petites et Moyennes Entreprises (PME). Seuls des projets mono-partenaire sont éligibles à cet appel à projets.

La réalisation de ces projets doit porter sur des travaux innovants de recherche et développement en cybersécurité réalisés en France, et non engagés avant la date de relève et s'inscrire dans un axe précis.

Les projets auront une durée indicative comprise entre 6 et 8 mois. Ils devront s'achever au plus tard le 31 août 2025. Aucun report de fin de programme ne pourra être octroyé.

Les projets doivent présenter une assiette minimum de 30 000 euros. L'aide maximum apportée sera de 150 000 euros par porteur de projet. Les modalités de financement et de régimes applicables sont détaillées ci-dessous.

L'appel à projets étant structuré selon 3 axes, les candidats sont encouragés à déposer des projets multithématiques (pour illustration : un projet sur l'axe n°1 – Solutions cyber et développements techniques et un projet sur l'axe n°3 – Soutien aux PME et startups dans le champ de la normalisation).

Axe 1 - Solutions cyber et développements techniques

L'axe « Solutions cyber et développements techniques » vise au prototypage et à la démonstration de briques ou solutions techniques visant à répondre à des enjeux de doctrine technique ou règlementaire. Il comporte 7 thématiques de développement détaillées en annexe 1 :

- Déploiement d'*infrastructure as Code* (*IaC*) de confiance
- Passerelle de contrôle d'intégrité OT de données transmises depuis un réseau IT
- Gestion automatisée de certificats d'authentification service Web conformes RGS/eIDAS
- USB de confiance
- Développement de support amovible d'authentification et services cryptographiques
- Système de filtrage des ordres d'un SOC (Centre d'Opération de Sécurité) vers un système d'information (SI) supervisé
- Évaluation d'une extension de sécurité pour architectures matérielles

Au cours des projets, des échanges pourront être organisés avec l'ANSSI afin de supporter au mieux les lauréats dans leur réflexion technique.

Axe 2 - Soutien aux prestataires préfigurant une démarche de qualification PAMS

Le NCC-FR souhaite soutenir le développement capacitaire des prestataires d'administration et de maintenance sécurisées (PAMS). Si l'ANSSI constate la bonne disponibilité des prestations d'infogérance, elle identifie également un nombre de candidats à la qualification PAMS encore trop limité pour garantir à terme la disponibilité de prestations d'administrations et de maintenance qualifiées auprès des utilisateurs.

Le référentiel d'exigences PAMS permet d'attester que le service d'administration à distance proposé aux bénéficiaires est à l'état de l'art, d'offrir des garanties face au risque de malveillance interne ainsi que de se prémunir d'un scénario d'attaque pouvant conduire à la compromission du système d'information administré à travers les moyens d'administration mis en œuvre. Conscient de la complexité du référentiel PAMS, le NCC-FR propose d'accompagner à la montée en compétences en vue de la qualification PAMS.

Au cours des projets, des échanges pourront être organisés avec l'ANSSI afin de supporter au mieux les lauréats dans leur réflexion technique.

Les projets de l'axe 2 devront :

- Développer les compétences du porteur de projet vis-à-vis du référentiel PAMS, en coopération avec le prestataire accompagnateur[2]:
  - En complétant un audit d'écart complet du prestataire, sur la base de la trame d'évaluation du référentiel PAMS ;
  - En permettant d'identifier l'intégralité des exigences sur lesquelles le prestataire doit monter en compétences avant de pouvoir déposer un dossier de qualification.
- Développer un projet de montée en compétences pour pouvoir aboutir au dépôt d'une candidature PAMS, en coopération avec le prestataire accompagnateur :
  - En produisant un rapport (en annexe de l'audit d'écart) décrivant le projet de montée en compétences post-audit du prestataire et précisant les actions à prendre, y compris en termes d'investissements en ressources matérielles ou humaines ;
  - Permettant d'aboutir au dépôt d'une candidature PAMS, à une échéance précise, auprès de l'ANSSI.

De manière transverse, les projets attendus sont encouragés à présenter :

- Un socle de connaissances de base sur les exigences du référentiel PAMS et ses grands principes techniques et architecturaux ;
- Un recueil documentaire concernant l'architecture du ou des systèmes d'information utilisés par la société, ou que la société envisage d'utiliser, dans le cadre de ses prestations actuelles ;
- L'existence et les compétences du pilote et des contributeurs internes permettant la montée en compétences de la société en matière de sécurité de ses prestations d'infogérance, ainsi que de coordination avec le prestataire accompagnateur ;
- L'intégration des prestations d'administration et de maintenance sécurisées dans la stratégie ainsi que l'historique et l'expérience de la société dans la commercialisation de ces dernières ;
- La cohérence du besoin de qualification de la société : existence d'un marché, types de clients visés ;
- Les retombées économiques attendues en cas d'obtention de la qualification PAMS.

[2] Les lauréats de l'appel à projets choisiront leur prestataire accompagnateur parmi les prestataires qualifiés de l'ANSSI.

Axe 3 - Soutien aux PME et startups dans le champ de la normalisation

Les activités de normalisation sont un des leviers de renforcement de l'autonomie européenne en cybersécurité. A ce titre, elles permettent l'expression des positions des acteurs privés et publics du secteur, en coopération avec les parties prenantes internationales.

Constatant une représentation et une implication encore limitée des PME et startups dans le champ de la normalisation, le NCC-FR donne l'opportunité à ces dernières de présenter un projet présentant leur engagement en la matière. Les candidats sont ainsi invités à présenter un projet articulant plusieurs des options décrites dans l'axe 3.

Les projets de l'axe 3 devront :
Développer et accroître la représentation des PME et start-ups, dans les structures de normalisation, renforcer leur efficacité dès lors qu'ils participent aux travaux de normalisation, et favoriser des contributions françaises de qualité, prenant en compte les enjeux et les spécificités des PME et start-ups. Cela en :

- Réalisant des contributions à la montée en compétences cyber et à la maîtrise du risque cyber :
  1. Participer à des formations à la normalisation conférant les connaissances essentielles[3] permettant d'accroître ses capacités de projection dans les instances dédiées.
  2. Créer un mécanisme de parrainage eou d'accompagnement pour les PME et startups au sein des structures de normalisation cyber.
  3. Elaborer des formations[4] aux normes cyber pour en favoriser l'implémentation.
- Permettant la représentation et la contribution des PME et start-ups, aux travaux de normalisation notamment en appui des règlements européens (eIDAS, RED, CRA, etc.) et des technologies émergentes :
  1. Financer le temps de participation aux travaux de normalisation, de manière individuelle ou groupée, au travers d'un véhicule approprié (e.g. fédération).
  2. Défrayer les experts pour leur participation aux travaux de normalisation (e.g. frais de déplacement).

De manière transverse, les projets attendus sont encouragés à :

- Accroître le nombre de normes cyber, notamment celles harmonisées en soutien des règlements NIS2, CRA, DORA, RED, ou eIDAS) ; ainsi que la dissémination de nouvelles technologies telles que la cryptographie post-quantique.
- Respecter les bonnes pratiques de sécurité à l'état de l'art (langages de développement sécurisés, analyses statiques et dynamiques du code produit, guides ANSSI).
- Contribuer aux travaux de normalisation sur des technologies stratégiques (PQC, IA…) ou à des projets de normalisation utiles à la pérennisation ou à l'industrialisation des développements techniques de l'axe 1 du présent appel à projets.
- Faire valoir les positions et technologies françaises et européennes.

Le projet devra expliciter le socle de connaissances de la structure porteuse :

Le projet devra présenter les travaux de normalisation courants ou futurs couvrant un besoin spécifique de la structure candidate ou favorisant l'adoption ou l'usage de son produit ou de sa technologie (commentaires et orientations à porter dans les instances, nouveau projet de normes à proposer, etc.) ainsi que l'implication prévue dans ces travaux (participation active en tant qu'expert, rédacteur, ou au titre de la présidence ou de l'animation de l'instance productrice).

Le projet devra également mettre en lumière les moyens disponibles pour assurer la pérennité de l'engagement

[4] Formations visant à l'acquisition de connaissances sur le fonctionnement de la normalisation française, européenne et internationale et connaissances spécifiques de normes relatives à la maîtrise du risque cyber, aux compétences en cybersécurité, utiles à la mise en œuvre de la réglementation européenne (CRA, NIS2, REC, DORA, RED, etc.) ou appuyant l'adoption/interopérabilité de technologies d'intérêt pour la cybersécurité (par exemple, cryptographie post-quantique, la sécurité des systèmes d'intelligence artificielle).

en normalisation dans le domaine cyber, au-delà du présent appel à projets.

- les moyens engagés sur une thématique présentant des enjeux pour l'industrie française ou européenne ;
- Via ses capacités pédagogiques (transfert des savoirs techniques et comportementaux) et opérationnelles (création, mise en œuvre et conduite pérenne de la formation).
- En cas de proposition de parrainage, la structure candidate précisera sur quels projets et de quelle façon elle réalisera l'accompagnement de PME et startups concernées.

Nature des porteurs de projets

Le projet est porté par une entreprise unique (TPE ou PME au sens de la réglementation européenne), immatriculée en France au registre du commerce et des sociétés (RCS) à la date de dépôt du dossier.

Les aides s'adressent aux entreprises (à l'exception des entreprises unipersonnelles). Les établissements de recherche n'y sont pas éligibles.

Critères et processus de sélection

Critères d'éligibilité

Pour être éligible, un projet doit remplir l'ensemble des conditions suivantes :

- être complet au sens administratif lors du dépôt du dossier ;
- satisfaire les contraintes indiquées, notamment en termes de montant d'assiette de dépenses ;
- avoir pour objet le développement d'un ou plusieurs produits, procédés, solutions ou services, non-disponible(s) sur le marché et à fort contenu innovant ;
- être éligible à recevoir des aides publiques (en particulier, le porteur doit être à jour de ses obligations fiscales et sociales, ne pas faire l'objet d'une injonction de restitution d'aides, et ne pas avoir le statut d'« entreprise en difficulté » au sens de la réglementation européenne des aides d'Etat) ; sauf en cas de fourniture d'éléments jugés satisfaisants par Bpifrance justifiant sa sortie du statut « d'entreprise en difficulté » avant la décision de financement du projet ;
- proposer une assiette éligible de travaux qui ne fait pas ou n'a pas fait l'objet de financements publics hors du cadre du présent appel à projets : par l'État, les collectivités territoriales, l'Union européenne ou leurs agences ;
- lister l'ensemble des aides accordées ou sollicitées sur les trois dernières années pour les projets de R&D menés par le porteur de projet et soutenus par la puissance publique (européenne, nationale, territoriale), en précisant les montants des programmes de R&D et les montants des aides accordées, afin d'apprécier la capacité financière du porteur de projet à mener à bien le projet ;
- présenter les éléments d'évaluation de la performance environnementale du projet avec la grille d'impact fournie dans le dossier de candidature.

Les projets ne respectant pas l'un des critères d'éligibilité sont écartés du processus de sélection.

NB : Les dépenses liées au projet déposé dans le cadre du présent AAP sont éligibles à une aide seulement à compter de la date à laquelle le dossier est considéré comme complet par Bpifrance après la relève et jusqu'au 31 août 2025.

Critères de sélection

Pour être sélectionnés, les projets éligibles sont instruits notamment sur la base des critères suivants :

- adéquation avec les thématiques détaillées dans le cahier des charges ;
- caractère innovant et valeur ajoutée du projet ;
- niveau de maturité préexistant et faisabilité technique du projet ;
- insertion du projet dans l'écosystème de la cybersécurité ;
- cohérence entre la situation financière de l'entreprise et l'importance des travaux proposés dans le cadre du ou des projets présentés ;
- caractère stratégique à l'échelle nationale, régionale, ou européenne, existence d'une collaboration structurée ou d'un effet de diffusion au sein d'une filière ou d'un écosystème, en particulier pour les entreprises impliquées ;
- adéquation avec les priorités de politique publique ;
- prise en compte des menaces cyber dans les phases de conception et de développement du projet ;
- performance environnementale.

Description des attendus par axe

Dans le cadre de cet appel à projets, le NCC-FR souhaite sélectionner des projets qui répondent aux thématiques détaillées et ciblées dans les 3 différents axes. L'adéquation avec les axes visés est partie prenante des critères de sélection.

- Axe 1 - Solutions cyber et développements techniques
- Axe 2 – Soutien aux prestataires d'infogérance intéressés par la qualification PAMS
- Axe 3 – Soutien aux PME dans le champ de la normalisation

Critères de performance environnementale et impact socio-économique

Le présent appel à projets vise à sélectionner des projets démontrant une réelle prise en compte de la transition écologique. Les effets positifs attendus et démontrés du projet à cet égard, de même que les risques d'impacts négatifs, sont utilisés afin de sélectionner les meilleurs projets parmi ceux présentés et peuvent amener à moduler le niveau d'intervention publique accordé au projet.

Chaque projet doit expliciter sa contribution à la transition écologique, en présentant les effets, quantifiés autant que faire se peut, directs ou indirects, positifs ou négatifs, estimés pour les objectifs ci-dessous (cf. Annexe 2) :

- atténuation du changement climatique (à travers, notamment, l'impact relatif en termes de consommation énergétique et d'émissions de gaz à effet de serre) ;
- adaptation au changement climatique ;
- écoconception, avec en particulier, la prise en compte de l'empreinte carbone sur l'ensemble du cycle de vie des systèmes ou services développés ;
- transition vers une économie circulaire, en prenant mieux en compte les ressources naturelles ;

- prévention et réduction de la pollution ;
- protection et restauration de la biodiversité et des écosystèmes.

Les efforts des porteurs de projets en matière d'écoconception, de maitrise des émissions de CO2, des consommations énergétiques et de ressources, ainsi que de lutte contre l'obsolescence pourront être plus particulièrement considérés dans l'évaluation.

Pour l'évaluation technique de l'impact du projet vis-à-vis de chaque objectif environnemental exposé ci-dessus, le déposant doit renseigner les documents dédiés disponibles sur le site de l'appel à projets (cf. dossier de candidature – grille d'impact).

L'évaluation portera également sur les impacts socio-économiques anticipés et le caractère souverain de la solution, en particulier les retombées économiques pour le territoire national, chiffrées et étayées en termes d'emplois (accroissement, maintien de compétences, etc.), d'investissements (renforcement de sites, accroissement de la R&D, etc.), de valorisation d'acquis technologiques (brevet, propriété intellectuelle, etc.), de développement d'une filière ou d'anticipation de mutations économiques ou sociétales.

Les projets causant un préjudice important du point de vue de l'environnement seront exclus (application du principe DNSH – *Do No Significant Harm*[5] ou « absence de préjudice important »). Les projets devront, le cas échéant, justifier la neutralité pour l'environnement des applications de la solution proposée ou s'inscrire dans une démarche d'amélioration vis-à-vis d'une solution de référence pertinente (produits/procédés/services comparable). Cf. Annexe 2.

Processus de dépôt de candidature et de sélection des projets

Le canevas du dossier de candidature est disponible sur la page internet de l'appel à projets. Il doit être déposé de manière dématérialisée sur la plateforme de dépôt dédiée : https://www.picxel.bpifrance.fr/accueil.

Le dossier de candidature doit être complet au moment où il est déposé.

Une première phase de pré filtrage est réalisée par Bpifrance pour vérifier que chaque dossier de candidature soit complet. La deuxième phase est une instruction technique réalisée par l'ANSSI. La sélection des dossiers est réalisée selon les critères d'éligibilité et les critères de sélection (voir ci-dessus). Les dossiers sélectionnés font ensuite l'objet d'une instruction et d'une vérification de conformité approfondie réalisée par Bpifrance, qui pourra mobiliser des experts indépendants.

Un comité de pilotage composé de Bpifrance, de l'ANSSI et du Secrétariat général pour l'Investissement (SGPI) se prononce sur les projets retenus. La décision finale d'octroi de l'aide est prise par le Premier Ministre, sur avis du Secrétariat général pour l'Investissement (SGPI).

La liste des projets lauréats de cet appel à projets fera l'objet d'une publication sur les sites internet de l'ANSSI, de Bpifrance et de la plateforme européenne Funding & Tenders. Elle sera également transmise aux administrations participant à la stratégie nationale de cybersécurité du programme France 2030.

[5] Règlement (UE) 2020/852 sur l'établissement d'un cadre visant à favoriser les investissements durables, en mettant en place un système de classification (ou « taxonomie ») pour les activités économiques durables sur le plan environnemental, publié au journal officiel de l'UE le 22 juin 2020.

Conditions et nature du financement

Nature du financement

Les projets doivent présenter une assiette minimum de 30 000 euros. L'aide maximum apportée sera de 150 000 euros par porteur de projet. Le taux d'aide dépendra du régime applicable. L'appel à projets étant structuré selon 3 axes, les candidats sont encouragés à déposer des projets multithématiques (pour illustration : un projet sur l'axe n°1 – Solutions cyber et développements techniques et un projet sur l'axe n°3 – Soutien aux PME et startups dans le champ de la normalisation).

L'intervention publique s'effectue dans le respect de la réglementation de l'Union européenne applicable en matière d'aides d'État (articles 107 à 109 du Traité sur le Fonctionnement de l'Union européenne).

Il est notamment fait application des régimes d'aide suivants, adoptés sur la base du règlement général d'exemption par catégorie n° 651/2014 de la Commission européenne publié au JOUE du 26 juin 2014 et ses modifications :

- régime *de minimis* (règlement 2023/2831 du 13 décembre 2023) ;
- régime cadre exempté n° SA.111723 d'aides à la recherche, au développement et à l'innovation.

Les régimes d'aides sont disponibles sur le site : (https://www.europe-en-france.gouv.fr). Ils détaillent les conditions d'application du présent dispositif pour assurer sa compatibilité avec le droit de l'Union européenne.

La liste des présents régimes cadre peut être complétée selon l'évolution des cadres de régimes d'aides européens.

Aides proposées

L'aide apportée aux entreprises sera constituée d'une subvention d'un montant compris entre **30 000 euros et 150 000 euros** pouvant financer jusqu'à 100% des dépenses éligibles. Le taux de l'aide s'applique sur les dépenses éligibles et dans la limite des intensités maximales permises par les régimes d'aides évoqués ci-dessus : **100% pour le régime *de minimis*** et **45% pour le régime cadre exempté d'aides à la recherche, au développement et à l'innovation (RDI)**.

Le principe général est un versement unique et *in fine* sauf exception. Une avance à hauteur de 50% du montant de l'aide peut être versée lorsque les besoins en trésorerie du porteur de projet sont avérés, sur décision du comité de pilotage. Dans tous les cas, le solde est versé sur présentation d'un état récapitulatif des dépenses acquittées (ERDA) final et d'un rapport final. Les dépenses devront être justifiées par une attestation établie par un expert-comptable.

Travaux et dépenses éligibles

Les dépenses liées au projet sont à présenter hors taxe et selon la ventilation requise dans l'annexe financière du projet présente dans le dossier de candidature.

Les dépenses éligibles sont directement affectées au projet (hormis les frais connexes qui sont calculés par un forfait). La nature des dépenses éligibles est précisée ci-dessous :

Type de dépenses	Principes
Salaires et charges	Salaires chargés du personnel du projet (non environnés) appartenant aux catégories suivantes : chercheurs (post-doc inclus), ingénieurs, techniciens.
Frais connexes	Montant forfaitaire (20%,) des dépenses de personnel (salaires chargés non environnés)
Coûts de sous-traitance	Coûts de prestations utilisées exclusivement pour l'activité du projet (plafond à 30%). Les acteurs ou les projets développant la filière française seront privilégiés.
Contribution aux amortissements	Coûts d'amortissements comptables des instruments et du matériel de R&D au prorata de leur utilisation dans le projet. *Exemple : pour un équipement amorti de façon linéaire sur une durée de 10 ans, et utilisé durant 2 ans pour le projet, le montant éligible à une aide sera égal à 2/10e du montant total de l'investissement dans cet équipement.*
Coûts de refacturation interne	Sur la base de modalités de calcul détaillées et de la certification par un commissaire aux comptes ou expert-comptable. Pour des entreprises avec le même SIREN.
Frais de mission	Frais réels des déplacements liés à la réalisation du projet.
Autres coûts	Autres frais d'exploitation directement liés à l'activité du projet. (Consommables non amortis dans les comptes)

Mise en œuvre

Contractualisation

Chaque bénéficiaire signe une convention avec Bpifrance. Cette convention précise notamment les modalités d'utilisation des crédits, le contenu du projet, le calendrier de réalisation, les modalités de pilotage du projet, les prévisions de cofinancement des projets, les modalités de restitution des données nécessaires au suivi et à l'évaluation des investissements, et les modalités de communication.

Confidentialité et communication

Bpifrance s'assure que les documents transmis sont soumis à la plus stricte confidentialité et ne sont communiqués que dans le cadre des opérations du NCC-FR relatives à cet appel à projet et de la gouvernance de France 2030. L'ensemble des personnes ayant accès aux dossiers de candidature est tenu à la plus stricte confidentialité.

Une fois le projet sélectionné, chaque bénéficiaire soutenu par France 2030 est tenu de mentionner ce soutien dans ses actions de communication ou lors de la publication des résultats du projet, avec la mention unique : « Ce projet a été soutenu par le plan France 2030 », accompagnée du logo de France 2030.

L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires. Toute autre communication est soumise à l'accord préalabledu bénéficiaire.

Les projets lauréats de cet appel à projets font l'objet d'une publication sur les sites internet, www.cyber.gouv.fr, www.entreprises.gouv.fr et www.bpifrance.fr. Une notification individuelle est également adressée aux porteurs

de projets.

Conditions de *reporting*

Le bénéficiaire est tenu de communiquer régulièrement à Bpifrance et l'ANSSI les éléments d'informations nécessaires à l'évaluation de l'avancement du projet (impact social, économique, sociétal, environnemental et numérique) ainsi qu'à l'évaluation *ex post* du projet. Ces éléments, et leurs évolutions, sont précisés dans conditions générales de la convention d'aide entre Bpifrance et le bénéficiaire.

Données

Le partage de données entre les acteurs d'une filière est un élément essentiel à sa structuration, axe fort de la stratégie nationale pour la cybersécurité. Dans le plein respect du droit de propriété des producteurs des données, cet appel à projets introduit certaines exigences qui doivent faciliter leur partage. Ces exigences seront valables pour tous les projets recevant des financements étatiques dans le cadre de la stratégie nationale pour la cybersécurité.

Protection et respect de la réglementation

Il est essentiel que les données produites ou manipulées dans le cadre des projets financés par la stratégie nationale, que ce soit lors de la phase de développement, d'expérimentation ou ultérieurement en production, soient protégées au bon niveau en fonction de leur sensibilité. Les objectifs sont à la fois de veiller à la protection de la propriété intellectuelle, d'éviter l'appauvrissement informationnel (typiquement contractuel) et de prévenir au mieux les fuites massives de données.

Dans cette optique, un travail d'analyse préalable est demandé aux porteurs de projets pour déterminer le niveau de sensibilité des différentes catégories de données du projet. Les mesures de sécurité qui en découleront (et qui devront être implémentées dans le cadre du projet) pourront faire intervenir la protection des communications de bout en bout (cryptographie) lors du transfert des données, un stockage sécurisé (chiffré et sauvegardé), un contrôle d'accès adéquat ainsi que des mesures juridiques ou contractuelles appropriées. Le cas échéant, le respect de la réglementation applicable (règlement général sur la protection des données, par exemple) sera le point de départ de cette analyse et de ces travaux.

Production, stockage et valorisation de données d'intérêt cyber

Dans le cadre des projets candidats, il est également demandé aux porteurs de capitaliser sur les opportunités de production de données d'intérêt cyber (de toutes natures). Cela implique de mettre en place les mécanismes *ad-hoc* de captation, de prétraitement (notamment de labélisation ou de normalisation) et de stockage de ces données, même s'il s'agit de données annexes non essentielles au projet.

Les réflexions sur un modèle économique autour de ces données sont fortement encouragées.

Dans le cas d'une abondance trop importante de données ou de contraintes spécifiques, une priorisation sur les données à stocker pourra être effectuée lors du suivi du projet. De même, la durée de stockage est à déterminer en fonction de la typologie des données concernées.

Le non-respect de cet aspect impactera négativement le dossier lors du processus de sélection et pourra *in fine* aboutir à une réduction du taux d'aide.

Accès aux données d'expérimentation

Les données générées dans le cadre du paragraphe précédent restent la propriété de leur producteur. Néanmoins, il est demandé aux porteurs bénéficiant d'une aide d'Etat dans le cadre de la stratégie nationale pour la cybersécurité de s'engager à mettre à disposition ces données gracieusement de manière ponctuelle dans le cadre d'expérimentations techniques non commerciales sous réserve de la compatibilité avec la réglementation et avec la non-concurrence des acteurs. Dans les deux cas d'exception, les données pourront éventuellement être mise à disposition si des traitements permettent de s'affranchir de ces contraintes (par exemple par de la cryptographie homomorphe, de l'anonymisation, de l'échantillonnage, etc.).

Mise à disposition des données

Les candidats autorisent Bpifrance à traiter leurs données pour mener l'évaluation de leur candidature, effectuer le suivi de leur dossier, répondre aux exigences réglementaires et de reporting, et pour toute autre finalité précisée dans la convention d'aide.

Les dossiers des projets lauréats de cet appel à projets seront transmis sur demande aux administrations participant à la stratégie nationale de cybersécurité du programme France 2030, les candidats y consentent expressément.

S'agissant des données à caractère personnel collectées et traitées par Bpifrance en tant que responsable de traitement :
Conformément à la réglementation applicable, notamment le Règlement européen 2016/679, dit règlement général sur la protection des données (RGPD) et les dispositions nationales relatives à l'informatique, aux fichiers et libertés, et sous réserve des conditions prévues par celles-ci, les personnes concernées bénéficient d'un droit d'accès, de rectification, d'effacement et à la portabilité des données et d'opposition, et de limitation du traitement. Ces droits peuvent notamment être exercés à l'adresse donneespersonnelles@bpifrance.fr. Elles disposent également du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Les informations relatives aux traitements de données à caractère personnel mis en œuvre par Bpifrance dans ce cadre sont disponibles dans notre Politique de protection des données accessible via ce lien.
Cette Politique peut être modifiée et actualisée périodiquement pour refléter une évolution législative ou réglementaire ou pour répondre à nos obligations d'information au titre de la réglementation applicable en matière de protection des données à caractère personnel. Nous vous invitons à vous y référer régulièrement sur notre site.

Contacts

Les renseignements concernant le processus administratif (constitution du dossier, démarches en ligne, précisions cahier des charges) pourront être obtenus auprès de Bpifrance par courriel en mentionnant en objet du message « AAP national NCC-FR » à l'adresse suivante :

strategies-acceleration@bpifrance.fr

Pour toute question technique relative aux thématiques attendues dans le cadre de cet appel à projets, des renseignements peuvent être obtenus auprès de l'ANSSI en mentionnant en objet du message « AAP national NCC-FR » à l'adresse suivante :

NCC-FR.ANSSI@ssi.gouv.fr

Pour toute question relative à la Stratégie Nationale cyber ou dépassant le cadre de cet appel à projets, le coordinateur de la Stratégie peut être contacté directement :

strategie.cyber@pm.gouv.fr

Annexe 1 : Thématiques des projets attendus pour l'Axe 1

Remarques préliminaires :

Pour l'ensemble des thématiques détaillées ci-après, les porteurs de projets sont invités à expliquer dans le dossier candidat les moyens et actions qui seront mis en place :

- Les porteurs de projets sont encouragés à se conformer aux guides de l'ANSSI[6] tels que :
  - Les recommandations relatives à l'administration sécurisée des systèmes d'information
  - Le guide d'hygiène informatique
  - Les recommandations relatives à l'interconnexion d'un système d'information à internet
  - Les recommandations sur le nomadisme numérique
  - Règles de programmation pour le développement sécurisé de logiciels en langage C

- Les porteurs de projets sont invités à respecter les bonnes pratiques de sécurité à l'état de l'art (langages de développement sécurisés si possible, analyses du code produit …)

- Les porteurs de projets sont invités à anticiper la compatibilité avec la délivrance d'un Visa de sécurité ANSSI sur le produit qui intègrera les développements.

- Les porteurs de projets sont invités à expliquer les moyens envisagés de pérennisation des développements, en particulier le degré d'internalisation, les réflexions sur leur stratégie open-source et la communauté d'experts mobilisable pour le maintien en condition opérationnelle et de sécurité s'il y a lieu.

- Les porteurs de projets sont invités à s'appuyer sur des logiciels déjà existants sur le marché ou disponibles en open-source.

[6] Publications (cyber.gouv.fr)

Thème 1 : Déploiement d'Infrastructure as code de confiance

L'infrastructure as Code (IaC) est devenue un élément essentiel dans la gestion et le déploiement des infrastructures Cloud. L'IaC offre ainsi aux équipes les moyens de définir, provisionner et gérer les ressources via des scripts et des fichiers de configuration. Cette approche permet d'intégrer, dès le départ, des contrôles de sécurité et ainsi de détecter et de corriger rapidement les vulnérabilités ou les écarts avec les référentiels internes ou réglementaires. Les outils populaires comme Terraform, Ansible et CloudFormation automatisent ces processus et améliorent la réplicabilité et la scalabilité des environnements. Les pratiques modernes mettent également l'accent sur l'intégration et le déploiement continus (CI/CD), la gestion des secrets ainsi que l'adoption de standards de codage et de révision de code afin de garantir la qualité et la robustesse des infrastructures. Au-delà de cet état de l'art, l'IaC est l'occasion de capitaliser sur des modèles d'infrastructures déployables rapidement et prenant en compte les menaces et les bonnes pratiques cyber.

Le NCC-FR souhaite donc faire émerger des modèles de code de déploiement d'infrastructures conformes aux exigences et recommandations de l'ANSSI ainsi qu'une offre de service basée sur ces modèles, d'une maturité au moins de niveau démonstrateur afin de les rendre disponible à l'écosystème.

Le projet devra réaliser des développements innovants respectant tout ou partie des exigences suivantes et permettant de disposer :

- Des modèles d'Infrastructure as Code :
  - Déployables sur les offres qualifiées SecNumCloud ;
  - Permettant d'héberger des applications métier au sein d'un tenant, à terme :
    - Segmentation réseau (admin, données, métier, ...)
    - Gestion des identités
    - Filtrage réseau/applicatif
    - DMZ
  - Indépendants et pouvant être assemblés en fonction des contextes et besoins des projets. Les architectures proposées doivent être résilientes, sécurisées et réversibles vers d'autres infrastructures Cloud ;
  - Développés en langage Terraform/OpenTofu et utiliser une approche Cloud Native (cloud-init, gestionnaires de secrets, notamment).

De manière transverse, le projet attendu est encouragé à :

- Prioriser les modèles adressés au cours du projet, et maintenir à jour la liste priorisée (backlog priorisé) ;
- Accompagner les modèles d'une documentation d'architecture (plan d'architecture, matrice de flux, plan d'adressage) ;
- Fournir tout ou partie d'un démonstrateur illustrant le fonctionnement des modèles dans une offre qualifiée SecNumCloud.

Thème 2 : Passerelle de contrôle d'intégrité OT de données transmises depuis un réseau IT

L'interconnexion entre les réseaux IT (bureautique) et OT (Industriel) est généralement réalisée par des passerelles d'interconnexion traditionnelles (DMZ avec pare-feux) ou bien éventuellement avec des diodes unidirectionnelles. Si cette passerelle apporte aujourd'hui des fonctions de sécurité standards (filtrage réseau, contrôle antivirus, etc.), il manque dans l'écosystème des produits ou des modules intégrés à des produits permettant un contrôle métier de l'innocuité des données transmises vers le réseau industriel OT.

Cette fonction est très souvent proposée par les éditeurs de produits SCADA (gestion et supervision du procédé industriel) mais ces produits sont positionnés directement au sein du réseau OT et ont une surface d'attaque assez importante, ce qui présente un risque de sécurité en cas de compromission ou de contournement des contrôles métier réalisés par ces derniers.

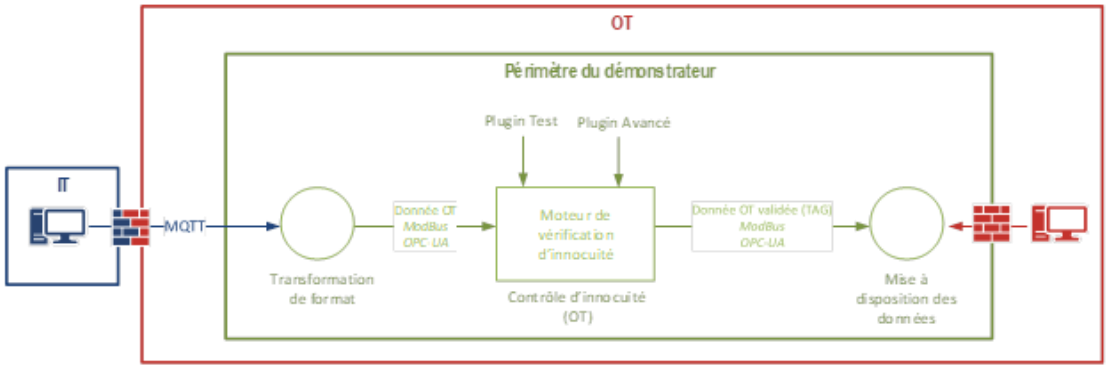
La montée en puissance de l'industrie 4.0, la multiplication des déploiements d'équipements IoT et l'émergence de solutions de supervision dans le Cloud impliquent d'améliorer la robustesse et la protection apportée par des passerelles d'interconnexions IT vers OT. Le développement d'une fonction de contrôle de l'innocuité métier des données transmises vers l'OT au sein d'une passerelle d'interconnexion permettrait ainsi d'améliorer la protection périmétrique et de ne plus reposer uniquement sur les contrôles réalisés par l'équipement de terminaison SCADA.

Le NCC-FR souhaite donc faire émerger une offre de passerelle d'interconnexion de l'IT vers l'OT en vue de protéger en intégrité les réseaux OT afin de la rendre disponible à l'écosystème.

Le projet devra réaliser des développements innovants respectant tout ou partie des exigences suivantes et permettant de disposer en fin de projet d'éléments de :

- Une fonction de contrôle d'intégrité OT ainsi que son démonstrateur, permettant de vérifier l'innocuité des données transmises depuis un réseau IT vers un réseau OT :

  - Comprenant les 3 composants suivants (cf schéma) :
    - Un composant « Transformation de format » permettant de récupérer des flux en provenance d'un réseau IT et de les mettre à disposition pour le composant « Contrôle d'innocuité (OT) » ;
    - Un composant « Contrôle d'innocuité (OT) » dont le rôle est précisé ci-après ;
    - Un composant « Mise à disposition des données » permettant de récupérer les fichiers validés par le composant « Contrôle d'innocuité (OT) » et de les mettre à disposition d'un réseau OT.



  - Le composant « Transformation de format » devant :
    - Récupérer en entrée des données transmises avec le protocole MQTT ;
    - Convertir les données reçues dans au moins un des 2 formats suivants : ModBus, OPC-UA ;
    - Envoyer en tant que client les données converties au composant serveur « Moteur de vérification d'innocuité ».
  - Le composant « Contrôle d'innocuité (OT) » est un moteur de traitement et d'analyse de flux OT dont l'objectif est de vérifier une conformité par rapport à des critères métier (ex : dépassement de seuils pour

des capteurs, incohérences entre plusieurs données transmises à la suite, etc.). Ce composant doit :

- Disposer d'un moteur de vérification d'innocuité générique pour s'adapter à différents cas d'usage et contextes métier OT ;
- Permettre de développer des plugins métiers venant se greffer au moteur de vérification d'innocuité, et qui seraient spécifiques à des cas d'usages ;
- Pouvoir annoter la donnée (ajout d'un tag) lorsque celle-ci est validée après le contrôle de conformité.

- Le composant « Mise à disposition des données » devant :
  - Être implémenté en tant que serveur en écoute sur deux interfaces réseaux, de manière à pouvoir répondre à la fois aux requêtes d'envois de la part du composant « Contrôle d'innocuité (OT) » et également aux requêtes de clients positionnés dans un réseau OT ;
  - Supporter au moins un des 2 protocoles industriels suivants : ModBus, OPC-UA ;
  - Être capable de contrôler l'annotation de la donnée reçue, et la rejeter en cas d'annotation invalide.
- Le démonstrateur (PoC) du projet doit :
  - Intégrer un plugin « test » permettant de valider le fonctionnement de l'ensemble de la chaîne de traitement : validation d'une seule valeur comprise entre deux bornes ;
  - Intégrer un plugin « avancé » permettant de valider un fonctionnement d'un cas d'usage « réel » reposant sur l'analyse statistique de données massives OT. Le scénario retenu est laissé au libre choix du porteur ;
  - Intégrer une possibilité d'interaction avec un utilisateur dans un but de paramétrage des plugins. Celle-ci doit être implémentée au minimum au moyen de scripts ou bien via une IHM sous la forme d'un site web ;
  - Il peut être implémenté dans n'importe quel environnement technique, incluant des environnements Cloud.

Thème 3 : Gestion automatisée de certificats d'authentification de service Web conformes RGS / eIDAS

La réduction de la durée de vie maximale des certificats d'authentification de service Web tolérée par les navigateurs web ajoutée aux obligations du RGS augmentent la complexité du renouvellement de ces certificats, gage de confiance dans les échanges électroniques entre administrations et citoyens.

Pour répondre à cette problématique de gestion de l'automatisation des certificats d'authentification de service Web, l'ANSSI a mené des études sur le protocole ACME (*Automated Certificate Management Environment*) qui est utilisé pour automatiser les échanges entre les autorités de certification et les propriétaires de certificats d'authentification de service Web.

L'automatisation de la gestion des certificats d'authentification de service Web implique notamment une plus grande exposition du service de délivrance de certificat à Internet (mise en œuvre d'un serveur ACME connecté à Internet et à l'Autorité de Certification (AC) et augmente la surface d'attaque côté demandeur de certificats avec la mise en œuvre d'un client ACME.

L'ANSSI travaille actuellement sur des référentiels d'exigences (applicables au serveur ACME et au client ACME) pour la mise en œuvre d'un service de gestion automatisée de certificats électroniques d'authentification de serveur web qui sera intégré dans la mise à jour du Référentiel Général de Sécurité (RGS). Ces référentiels d'exigences visent un niveau de sécurité équivalent à ce qui est prévu actuellement au niveau 1 étoile (*) du RGS.

Le NCC-FR souhaite donc faire émerger une offre de gestion automatisée de certificats d'authentification de service Web conformes RGS / eIDAS.

Le projet devra réaliser des développements innovants permettant de disposer en fin de projet :

- D'un serveur ACME conforme au RGS et aux référentiels d'exigences[7] et la RFC 8555
- D'un client ACME conforme au RGS et aux référentiels d'exigences [8]et la RFC 8555

Enfin, les porteurs de projet devront indiquer dans leur proposition dans quel délai ils seront en capacité d'assurer le renouvellement d'un certificat.

[7] Les référentiels d'exigences sont disponibles sur demande à l'adresse mail : supervision-eIDAS@ssi.gouv.fr
[8] Voir note précédente.

Thème 4 : USB de confiance

La littérature abonde de modes opératoires d'attaquants impliquant la connexion de supports amovibles USB malveillants sur des terminaux de confiance[9] et maîtriser la gestion des périphériques USB au sein des entités est devenu un enjeu majeur de sécurité.

Avec l'arrivée de l'USB Type C, l'USB-IF[10] a publié une spécification permettant l'authentification des périphériques USB lors de connexion à un système. Cette spécification n'a pour l'instant était que faiblement adoptée, seuls quelques microcontrôleurs la proposent et elle n'a pas été implémentée dans des systèmes d'exploitation grand public (Linux, Windows, notamment).

Le NCC-FR souhaite soutenir le développement d'une capacité d'authentification de périphériques USB afin de le rendre disponible à l'écosystème et permettre l'essor d'une gamme de périphériques USB de confiance.

En particulier, les projets devront adresser un ou plusieurs développements innovants, respectant les normes de l'USB-IF[11], respectant tout ou partie des exigences suivantes et permettant de disposer en fin de projet de :

- Une bibliothèque de fonctions d'authentification[12] des périphériques, d'une maturité au moins de niveau démonstrateur, intégrable à une pile USB 3.0 type C installée côté contrôleur :

  - Réalisant l'étape d'authentification avant l'étape d'énumération du périphérique USB ;

  - Permettant de valider :

    - a) si le périphérique a le droit d'être connecté à la plateforme ou non
    - b) quel type de périphérique (Device class) peut être rattaché au système

  - Paramétrable afin de pouvoir à terme :

    - a) configurer une infrastructure à clés publiques (PKI) utilisée pour la validation des certificats
    - b) autoriser un nouveau périphérique USB
    - c) renouveler les certificats des périphériques
    - d) révoquer des périphériques

- Un émulateur de périphérique USB 3.0 capable de s'authentifier via une bibliothèque d'authentification des périphériques USB.
- Un périphérique USB 3.0 implémentant l'authentification sur base d'une carte d'évaluation embarquant un composant USB type C.

De manière transverse, les projets sont encouragés à :

- Prioriser un développement sur système embarqué (priorité 1), linux/android (priorité 2), ou windows (priorité 3) ;
- Proposer autant que possible une architecture modulaire, indépendante du HW/FW ;
- Prévoir la possibilité d'isoler la pile USB via un hyperviseur, dans le cas d'un portage SoC/CPU.

[9] Par exemple : https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/
[10] Front Page | USB-IF
[11] "Universal Serial Bus Security Foundation Specification, Revision 1.0 with ECN and errata through January, 7 2019" et "Universal Serial Bus Type-C™ Authentication Specification, Revision 1.0 with ECN and errata through January, 7 2019" disponibles sur le lien *https://www.usb.org/document-library/usb-authentication-specification-rev-10-ecn-and-errata-through-january-7-2019*
[12] https://www.usb.org/authentication

Thème 5 : Développement de support amovible d'authentification et services cryptographiques

L'authentification d'un utilisateur sur un système est une étape cruciale pour la sécurisation de celui-ci. L'usage de deux facteurs d'authentification permet d'augmenter le niveau de sécurité de cette étape. Il existe des clés de sécurité permettant l'ajout d'un facteur « ce que je possède » (Yubikey, Nitrokey…). Cependant, elles nécessitent tout de même l'utilisation d'une interface utilisateur déportée sur le système ou ne sont utilisables que à distance.

Le projet devra réaliser des développements innovants permettant de disposer en fin de projet d'un support devant respecter tout ou partie des exigences suivantes :

- Être amovible et pouvoir être connecté physiquement à un pc ou un smartphone ;
- Être autonome pour réaliser l'authentification de l'utilisateur ;
- Embarquer un moyen d'authentification de l'utilisateur biométrique ou basé sur un code PIN ;
- Embarquer une applet customisable qui est déverrouillée sur authentification de l'utilisateur. Il doit être possible de charger une applet avec des services cryptographiques propriétaires ;
- Suivre la norme ISO 7816-12 USB-ICC[13] ;
- Suivre l'annexe B3 du référentiel général de sécurité (RGS) en vigueur édité par l'ANSSI et le guide sur l'authentification[14] .

De manière transverse, le projet attendu est encouragé à :

- Fournir un démonstrateur de type banc éclaté ;
- Baser les travaux sur un composant de sécurité évalué dans le cadre des critères communs[15] ;
- Suivre la conformité de dimensionnement cryptographique au RGS.

[13] https://www.usb.org/sites/default/files/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf
[14] https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe
[15] https://www.commoncriteriaportal.org/

Thème 6 : Système de filtrage des ordres d'un SOC vers un SI supervisé

L'automatisation des réactions d'un système de supervision en cas de détection et de qualification d'un incident se heurte à plusieurs difficultés. D'une part plusieurs fonctions doivent être adressées (orchestration des actions sur plusieurs équipements, validation de la légitimité des actions, intégration et mise en œuvre technique des actions), et d'autre part plusieurs problématiques apparaissent :

- Il faut adresser de nombreux objets techniques différents (ex. toutes les marques de firewall...) ;
- Il faut connaitre toutes les possibilités d'ordre légitime, et mettre à jour ce catalogue à chaque évolution ;
- Enfin, il faut émettre des ordres depuis le système de supervision (à basse intégrité) vers le SI d'administration (à haute intégrité), qui revient à créer une rétroaction entre périmètre de supervision et périmètre supervisé.

Dans le cas où il existe un lien technique entre le SI de supervision et le système de réaction automatique, il serait envisageable de proposer des dispositifs permettant de sécuriser ces ordres afin de faciliter cette automatisation.

Le NCC-FR souhaite donc soutenir le développement d'une capacité de filtrage d'ordres légitimes venant d'un système de détection vers le système d'information qu'il supervise, afin de la rendre disponible à l'écosystème.

Le projet devra réaliser des développements innovants respectant tout ou partie des exigences suivantes pour le développement :

- D'une API standard programmée pour maîtriser l'envoi d'ordres depuis un SOC vers certains dispositifs du SI qu'il supervise en vue de déclencher des mesures de réponse automatique. Le développement :
  - Réalise le filtrage des ordres légitimes d'un SOC vers un SI supervisé ;
  - Assure que les ordres descendants d'un SOC vers un SI supervisé sont légitimes. Ainsi, les capacités d'intervention sur un SI supervisé depuis un SOC seraient davantage sécurisées. Le bénéficiaire d'un SOC serait ainsi davantage enclin à accepter certaines capacités d'intervention d'un SOC moderne sur son SI supervisé, qu'elles soient automatiques ou manuelles ;
  - S'appuie sur une définition des ordres qu'un SOC serait légitime d'envoyer vers un SI supervisé. En particulier, ces ordres doivent légitimement inclure l'ajout de restrictions, mais jamais l'ajout de privilèges ou d'élargissement de droits, par exemples :
    - L'interdiction d'URL sur un Proxy, mais jamais d'autorisation de nouvelle URL
    - L'ajout de règles "deny" sur un pare-feu, mais jamais une règle "allow"
  - Prévoit le rétablissement d'une restriction par un autre canal pour éviter toute utilisation malveillante de ce dernier. Le dispositif pourrait par exemple inclure : proxy, pare-feu, EDR, NDR, antivirus, DNS … Cette liste est non exhaustive et le candidat a toute latitude pour l'enrichir en fonction de ce qu'il estime pertinent.
- Un module logiciel de contrôle adapté à cette API.

De manière transverse, les projets attendus sont encouragés à :

- Faciliter une mise en œuvre opérationnelle idéale en prévoyant que tous les dispositifs puissent s'intégrer à l'API standard, ou à minima en ajoutant au module de contrôle un module de translation : ce module de translation traduirait les ordres depuis l'API standard vers des API propriétaires pour chaque dispositif pilotable du SI supervisé.
- Développer une documentation technique :
  - Sur le module logiciel de contrôle et l'API ;
  - Expliquant leur intégration avec les choix de dispositifs pilotables du SI supervisé.
- Fournir tout ou partie d'un démonstrateur illustrant le fonctionnement du produit dans une offre qualifiée SecNumCloud.

Thème 7 : Évaluation d'une extension de sécurité pour architectures matérielles

Le monde académique développe des extensions de sécurité pour architectures matérielles comme le projet CHERI (Capability Hardware Enhanced RISC Instructions) pour les architectures ARM et RISC-V visant à faire disparaître les vulnérabilités mémoires qui forment à l'heure actuelle la majorité des vulnérabilités logicielles. Ces projets sont prometteurs, mais il n'y a eu relativement que peu d'évaluations poussées et d'études d'impact de ces solutions qui sont nécessaires à une montée en maturité et à une industrialisation ultérieure.

Le NCC-FR souhaite donc soutenir l'évaluation d'extensions matérielles de sécurité comme CHERI. Les résultats de l'étude devront à minima être mis à disposition de l'ANSSI pour son utilisation propre, la mise à disposition au public étant encouragée mais pas obligatoire.

Le projet devra réaliser des travaux innovants respectant tout ou partie des exigences suivantes et permettant de disposer en fin de projet d'éléments parmi :

- Une évaluation de l'usabilité (facilité d'utilisation, de modification et d'installation de logiciels) d'un processeur implémentant l'extension de sécurité dans plusieurs scénarii :
  - dans le cadre d'un système embarqué (utilisant par exemple CHERIoT pour l'extension CHERI) ;
  - dans le cadre d'un serveur ouvert sur Internet ;
  - dans le cadre d'une utilisation personnelle d'un ordinateur.
- Une validation de la sécurité apportée dans différents scénarii :
  - Exemples simples et illustrateurs de vulnérabilités liées à la mémoire ;
  - Applications complexes, par exemple, protection contre des vulnérabilités de type Heartbleed dans un serveur WEB, ou compartimentalisation d'applications dans un système de type Android.
- Un prototype et d'un exemple d'implémentation utilisant l'extension.

De manière transverse, les projets attendus sont encouragés à :

- Préciser les environnements de développement / test / validation etc. utilisés, voire les mettre à disposition avec l'étude ;
- S'assurer que les résultats soient reproductibles.

Annexe 2 : Critères de performance environnementale

Les projets causant un préjudice important du point de vue de l'environnement seront exclus (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie[16].

En créant un langage commun et une définition claire de ce qui est « durable », la taxonomie est destinée à limiter les risques d'écoblanchiment (ou "greenwashing") et de distorsion de concurrence, et à faciliter la transformation de l'économie vers une durabilité environnementale accrue.

Ainsi, la taxonomie définit la durabilité au regard des six objectifs environnementaux suivants :

- l'atténuation du changement climatique ;
- l'adaptation au changement climatique ;
- l'utilisation durable et la protection des ressources aquatiques et marines ;
- la transition vers une économie circulaire ;
- la prévention et la réduction de la pollution ;
- la protection et la restauration de la biodiversité et des écosystèmes.

Pour l'évaluation technique de l'impact du projet vis-à-vis de chaque objectif environnemental, le déposant doit renseigner le document dédié disponible sur le site de l'appel à projets (dossier de candidature) et le joindre au dossier de candidature.

Il s'agira d'autoévaluer les impacts prévisibles de la solution proposée (faisant l'objet de l'aide) par rapport à une solution de référence explicite, pertinente et argumentée. Cette analyse tient compte du cycle de vie des processus et du ou des produits ou livrables du projet, suivant les usages qui en sont faits. En tant que de besoin, ces estimations pourront être étayées par des analyses en cycle de vie plus complètes. La présentation au dossier d'éléments concrets sur la façon dont les porteurs de projet contribuent ou s'engagent à contribuer, dans le cadre du projet, voire dans l'ensemble de leurs activités, sera prise en compte positivement dans l'évaluation.

16 Règlement (UE) 2020/852 sur l'établissement d'un cadre visant à favoriser les investissements durables, en mettant en place un système de classification (ou « taxonomie ») pour les activités économiques durables sur le plan environnemental, publié au journal officiel de l'UE le 22 juin 2020