Programme de Transfert au Campus Cyber

opéré par

Appel à Propositions de création de scénarios et de formations sur cyber range
V1.0

- Ouverture des candidatures : juin 2026
- Format de dépôt : en continu, avec une levée le dernier mardi de chaque mois
- Adresse de dépôt et point de contact : ptcc.formation@inria.fr

Table des matières

1 Contexte et objectifs de l'appel à propositions

1.1 Contexte général

Dans le cadre du plan « France 2030 » et du Programme d'investissements d'avenir, le Gouvernement a défini une stratégie d'accélération pour la Cybersécurité. Pour mémoire, la cybersécurité concerne les mécanismes logiciels ou matériels visant à assurer la confidentialité, l'intégrité et la disponibilité des systèmes, des logiciels et des données.

Construite en pleine collaboration entre les administrations compétentes sur les sujets cyber et les acteurs de l'écosystème (industriels, organismes de recherche, collectivités…), cette stratégie se décline selon cinq axes :

- renforcer les liens et synergies entre les acteurs de la filière ;
- développer des solutions souveraines et innovantes de cybersécurité ;
- former plus de jeunes et de professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- soutenir le développement des entreprises de la filière via un abondement en fonds propres ;
- soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales.

1.2 Le Programme de Transfert au Campus Cyber

Dans ce cadre, Inria a été mandaté pour assurer la mise en œuvre d'un programme de transfert de compétences et de technologies issues de la recherche publique vers l'ensemble des écosystèmes territoriaux de la cybersécurité. Le Programme de Transfert au Campus Cyber (PTCC), dont l'équipe est basée au Campus Cyber de Paris La Défense, est en charge de cette mission.

Les objectifs du PTCC sont :

- de renforcer les efforts de recherche en cybersécurité, en particulier en favorisant les projets conjoints entre acteurs académiques, industriels et gouvernementaux ;
- de favoriser le transfert de compétences et de technologies issues de la recherche publique vers l'ensemble des acteurs de l'écosystème, avec un rôle affirmé de tiers de confiance neutre garant d'un cadre souverain ;
- d'accélérer la mise sur le marché de produits de cybersécurité correspondant à une vraie barrière technologique en renforçant les logiques partenariales ;
- d'accélérer la dynamique de formation initiale et de formation continue à la cybersécurité, répondant au besoin des entreprises, en lien avec les établissements de formation concernés, en premier lieu les grandes universités de recherche franciliennes ;
- de s'articuler avec les dispositifs de soutien à l'entreprenariat technologique afin de soutenir la création et le développement d'entreprises innovantes.

1.3 Objectifs de l'appel à propositions de scénarios et de formations sur cyber range

Cet appel à propositions s'inscrit dans le cadre du soutien au transfert de compétences et de savoirs issus de la recherche académique. La mise en œuvre d'un cyber range Airbus au sein du PTCC répond aux besoins de mise à disposition d'environnements virtuels et de mise

en situation, de tests et d'évaluations de solutions pour les équipes de recherche ou les porteurs de projets, ou encore pour certaines entreprises (startup, PME) ou organismes publics. Cet appel a pour objectifs :

- d'aider à la production de nouveaux contenus pédagogiques pour des scénarios ou formations de pointe dédiés aux enjeux de souveraineté numérique et plus spécifiquement de cybersécurité ;
- de mettre en place, en lien avec la communauté académique, des actions de formation continue dans le domaine de la cybersécurité à destination des entreprises et des organismes publics ;
- de permettre le partage des ressources pédagogiques développées dans le cadre du programme avec les établissements d'enseignement supérieur et de recherche publics ;
- de renforcer l'attractivité et les actions de formation du secteur sur un marché d'emploi en forte tension.

L'offre de formation issue des chercheurs et enseignants-chercheurs vise à :

- couvrir un ensemble de thématiques prioritaires du domaine de la cybersécurité, en lien avec les technologies et savoirs issus de la recherche publique qui ont été identifiés comme présentant un intérêt pour les entreprises et les organismes publics ;
- considérer de façon complémentaire des thématiques autres que les thématiques prioritaires mentionnées ci-dessous pouvant relever de besoins très spécifiques ;

Les thématiques traitées (prioritaires ou non) sont rapportés au référentiel ECT/JRC ([1] et [2]). Les *cyber ranges* et CTF sont définis au sein de ce référentiel par la thématique (primaire) "*Education and Training*". Les propositions de scénarios et de formations sur *cyber range* pourront cibler des thématiques (secondaires) prioritaires ou non sous l'angle de la recherche, des technologies, des secteurs d'activités et des cas d'usage, conformément à ce référentiel.

Les thématiques prioritaires (selon la terminologie ECT/JRC) sont les suivantes :

- aspects humains,
- *big data*, *cloud*, *edge* et virtualisation,
- *blockchain* et technologie des registres distribués,
- cryptologie (cryptographie et cryptanalyse),
- gestion des identités, des accès et des usages,
- ingénierie de la sécurité des logiciels et du matériel,
- intelligence artificielle et cybersécurité,
- internet des objets, systèmes embarqués et systèmes pervasifs,
- IoT industriel et systèmes de contrôle,
- méthodes formelles pour la cybersécurité,
- réseaux et systèmes distribués,
- sécurité des données et données personnelles,
- technologie matérielle,
- technologie quantique.

Il est possible de proposer d'autres thématiques issues du référentiel ECT/JRC en dehors des thématiques prioritaires listées ci-dessus.

Les propositions de formation qui ne visent pas exclusivement le *cyber range* sont du ressort de l'Appel à Propositions de modules de formation incluant la création de modules, de MOOC ou d'ePOC.

La création de scénarios ou de formations sur le *cyber range* du PTCC nécessite de préciser dans la demande de financement, les informations suivantes :

- une évaluation du volume horaire d'utilisation du *cyber range* nécessaire,
- une évaluation de la durée d'utilisation avec le volume horaire mentionné précédemment,
- une estimation des périodes d'utilisation du *cyber range*,
- la configuration attendue (nombre d'enclaves (*workzones*), RAM, disque),
- les éventuels besoins techniques additionnels.

Des informations comparables doivent aussi être précisées dans le cas où il serait prévu de dispenser la formation ou l'exécution des scénarios développés sur le *cyber range* du PTCC.

Un délai de prévenance d'un mois est attendu pour l'exécution des formations ou des scénarios sur le *cyber range* du PTCC. Les ressources du PTCC étant en outre limitées, il n'est pas impossible que le *cyber range* ne soit pas disponible sur certaines périodes car déjà utilisé par ailleurs.

2 Source, nature et résultats des propositions attendues

L'Appel À Propositions permanent : « AAP de création de scénarios et de formations sur *cyber range* » est piloté par la direction de programme du PTCC.

Il est diffusé au niveau national par la direction de programme, en étroite association avec les établissements d'enseignement supérieur et de recherche, les écoles et les organismes de recherche.

Les soumissions attendues proposeront la création de scénarios et de formations sur le cyber range du PTCC par un ou des chercheurs ou enseignants-chercheurs issus d'une ou plusieurs de ces entités. Dans le cas où la demande est issue de plusieurs entités, une seule demande de financement doit être soumise en indiquant la répartition de la charge entre ces entités.

Pour toute question relative à cet appel, vous pouvez envoyer un message à : ptcc.formation@inria.fr

2.1 Nature

La demande consiste en un document de demande de financement à remplir. Elle détaille notamment les scénarios proposés ou le contenu de la formation qui s'exécuteront sur le *cyber range*, sa durée, sa date de disponibilité ainsi que le montant du financement demandé.

En complément, et afin que les candidats positionnent le mieux possible leur proposition compte-tenu de la progression de la couverture de l'offre, la direction de programme fournira :

- la liste des scénarios et des formations sur cyber range déjà existantes au catalogue (https://ptcc.fr/formation/formations-financees/) et
- des informations mentionnant le contenu et/ou le type de propositions à privilégier.

Les propositions visent au développement de nouveaux contenus pédagogiques, pour des formations de pointe dédiées aux enjeux de cybersécurité :

- dans un cadre de formation continue, à destination des ingénieurs dans la R&D des entreprises et en particulier dans les PME et ETI, des développeurs des startups, des organismes publics et
- exploitant les compétences et savoirs issus de la communauté académique.

Les propositions peuvent se décliner sous différents formats :

- des scénarios ou des formations de courte durée sur une thématique donnée à destination des ingénieurs, des chercheurs ou des dirigeants des entreprises ou des organismes publiques ainsi que les enseignants et les étudiants ;
- des scénarios ou des formations sur mesure à la demande des entreprises ou des administrations dans le but de répondre à des besoins spécifiques.

On entend par courte durée, une formation ou des scénarios se déroulant sur une durée comprise entre un et trois jours. Des durées légèrement supérieures pourront être étudiées. Une journée représente 6 h d'exécution maximum.

Important : les supports pédagogiques produits dans le cadre du projet devront être accompagnés d'une licence qui en autorise au moins l'utilisation par les établissements d'enseignement supérieur publics français ans le cadre de la formation initiale.

2.2 Résultats attendus

Le contenu pédagogique produit suite au financement a pour objectifs de répondre aux attentes suivantes :

- garantir une démarche de transfert de savoirs ou de compétences en lien potentiellement avec les logiciels en source ouverte développés par les partenaires ;
- mettre en œuvre des outils facilitant le déploiement des scénarios et des formations à l'aide par exemple d'un langage de description de scénarios d'attaques comme le logiciel URSID [3] [4] ;
- produire des scénarios et des formations fonctionnels sur le cyber range Airbus du PTCC ;
- mettre à disposition des systèmes complets incluant potentiellement des émulateurs ;
- contribuer à la massification des formations adossées à la recherche, notamment en adhérant à la politique de partage des contenus entre les partenaires.

2.3 Diffusion des contenus produits

Le PTCC rend visible l'ensemble des contenus pédagogiques financés par le programme, plus spécifiquement, les scénarios et les formations sur cyber range Airbus du PTCC dans le cadre

de cet appel. Une promotion vis-à-vis des entreprises et des organismes publics sera effectuée par le PTCC notamment via :

- l'organisation ou la participation à des évènements tels que des salons professionnels ;
- la plateforme TAL-CYB du Campus Cyber national qui référence le PTCC et où les partenaires peuvent promouvoir leurs formations ;
- les outils de communication des différents campus du réseau des Campus Cyber.

Les partenaires s'engagent aussi à promouvoir ces contenus lors de leurs actions de communication.

3 Examen des propositions soumises

3.1 Procédure de qualification et de sélection

Le dossier de soumission doit être déposé complet. La direction de programme du PTCC validera sa recevabilité (voir ci-dessous). Un message de confirmation sera envoyé aux porteurs et la proposition sera alors présentée au Comité Technique du PTCC. Cette présentation permettra notamment d'apporter un regard critique destiné à consolider la proposition au regard de ses qualités techniques et scientifiques, des perspectives commerciales ainsi que de sa pertinence au regard des objectifs du programme.

La direction de programme et le comité technique sont susceptibles de faire appel à des experts externes en mesure de donner un avis éclairé sur la proposition, tout en évitant les conflits d'intérêt.

La sélection de la proposition et la caractérisation de son financement seront assurées par le Comité des Opérations du PTCC composé notamment d'un représentant de l'ANR, du SGPI, de l'ANSSI et de la DGA.

La direction de programme informera les porteurs de la proposition de la décision du Comité des Opérations du PTCC.

3.2 Critères de recevabilité et de sélection

La recevabilité administrative de la proposition est assurée par la direction de programme du PTCC avec l'assistance d'un groupe de travail dédié. Les conditions de recevabilité sont la complétude du dossier et l'éligibilité des partenaires.

Les principaux critères de sélection au financement des propositions sont :

- le lien avec la recherche ;
- le sujet (les aspects de sureté et de fiabilité ne sont pas considérés en tant que tels comme de la cybersécurité) ;
- la reconnaissance académique des auteurs dans leur domaine ;
- le positionnement (ECT/JRC) de cette production par rapport aux modules déjà financés en indiquant son apport spécifique ;
- la durée de la formation ;
- le budget demandé ;
- la date de disponibilité du support pédagogique.

Il est par ailleurs nécessaire que la proposition précise clairement :

- les objectifs des scénarios ou de la formation développés ;

- le public visé (formation continue et initiale) ;
- les prérequis à la compréhension des supports pédagogiques fournis (scénarios ou formations) ;
- les compétences acquises grâce aux supports pédagogiques (scénarios ou formations) (la taxonomie de Bloom pourra être utilisée dans ce cadre) ;
- les publications des auteurs en lien avec la proposition.

4 Modalités de financement

Le financement d'une proposition de création de scénarios ou de formations sur *cyber range* par le programme est évalué selon sa complexité. Il n'y a pas de prise en charge de coût d'environnement, ni d'achat de matériel. Les contributeurs devront présenter les éléments permettant de justifier le budget demandé.

Les propositions bénéficieront en plus, d'un kit de communication composé :

- d'une fiche de synthèse ;
- d'un post et visuel pour les réseaux sociaux ;
- d'une vidéo courte de présentation.

Le versement du financement à l'entité académique (ou aux entités académiques) dont dépendent le ou les auteurs s'effectue en plusieurs versements sur une base annuelle. Le solde est versé à la livraison du support pédagogique après validation par le PTCC des support(s) produit(s) en termes de qualité et de conformité. Le soutien financier sera apporté dans le cadre d'un conventionnement entre Inria et chacun des partenaires.

La dispense de la formation n'est pas financée par le PTCC. Néanmoins, la direction de programme suivra la réalisation du nombre d'occurrences de sessions déroulées en assurant le suivi d'un ensemble d'indicateurs :

- nombre et types d'actions de promotion utilisant notamment le kit de communication ;
- nombre de sessions de formation dispensées ;
- nombre de personnes formées ;
- nombre de femmes formées.

À ce titre, la direction de programme collectera ces informations sur une base annuelle auprès des entités académiques.

5 Dossier de candidature

Le document de demande de financement doit être soumis sous forme électronique au format demandé, en utilisant le modèle [5].

6 Ordonnancement

Le processus d'instruction des propositions est le suivant :

- réception des propositions ;
- validation de la recevabilité des propositions par la direction de programme ;

- proposition de la direction de programme d'une évaluation des propositions ;
- organisation par la direction de programme d'une consultation du Comité Technique du PTCC concernant le classement proposé ;
- présentation des propositions au Comité des Opérations par la direction de programme ;
- notification aux auteurs par la direction de programme des décisions du Comité des Opérations.

Suite à la validation de la recevabilité des propositions par la direction de programme, celle-ci prendra contact avec les contributeurs afin d'obtenir une annexe financière décrivant les ressources correspondant à la demande d'aide et précisant la personne habilitée à engager juridiquement l'établissement. Ceci permettra la poursuite de l'instruction.

7 Suivi de la fourniture

La durée maximale de création de scénarios et de formations sur cyber range est fixée à 6 mois. A l'issue de cette durée, les supports devront être remis contractuellement à la direction de programme.

Les scénarios et formations sur *cyber range* sont réalisés en français ou en anglais.

Le kit de communication sera financé par le PTCC en lien avec les porteurs de la proposition. Il sera fourni au moment où le support pédagogique sera mis à disposition de la direction de programme.

8 Supports pédagogiques

Le partage des supports pédagogiques pour la formation initiale des établissements d'enseignement supérieur publics français est un élément important du programme. Dans le plein respect du droit de propriété des producteurs de contenus, cet appel à propositions introduit certaines exigences qui doivent faciliter leur partage, décrites dans cette section.

8.1 Formats

Les scénarios et formations sur cyber range doivent pouvoir s'exécuter sur le cyber range Airbus du PTCC. A ce titre, les livrables se présentent sous la forme de "bundles" Airbus. Ils doivent être déposés sur le hub d'Airbus (https://hub.cyberrange.cloud) en accès ouvert. Dans le cas où des scénarios seraient développés en utilisant des langages de description de scénarios d'attaques tels qu'URSID [3] [4], le code devra aussi être fourni et mis à disposition.

8.2 Protection et respect de la réglementation

Il est essentiel que les contenus produits ou manipulés dans le cadre des propositions financées par le programme, que ce soit lors de la phase de création, d'utilisation, de réutilisation ou ultérieurement de modification, soient protégés au bon niveau en fonction de leur sensibilité. Un travail d'analyse est ainsi demandé aux porteurs pour déterminer le niveau de sensibilité des contenus mis à disposition. Les porteurs doivent garantir que les images, les textes, les vidéos inclus dans les contenus n'entravent pas le droit à la propriété intellectuelle.

9 Annexe – Documents de référence

[1] NAI-FOVINO, I., NEISSE, R., HERNANDEZ-RAMOS, J. L., POLEMI, N., RUZZANTE, G., FIGWER, M., LAZARI, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089.

[2] European Commission, Joint Research Centre (JRC) (2021): JRC CYBERSECURITY TAXONOMY. European Commission, Joint Research Centre (JRC) [Dataset] PID: http://data.europa.eu/89h/d2f56334-a0df-485b-8dc8-2c0039d31122

[3] URSID: Automatically Refining a Single Attack Scenario into Multiple Cyber Range Architectures. Pierre-Victor Besson, Valérie Viet Triem Tong, Gilles Guette, Guillaume Piolle, Erwann Abgrall

[4] https://gitlab.inria.fr/pirat-public/ursid

[5] Demande de financement de scénarios ou de formations sur cyber range – AAP Cyber Range – V1.0