FINANCES PUBLIQUES

CONCOURS EXTERNE
DE CONTRÔLEUR DES FINANCES PUBLIQUES DE 2ÈME CLASSE
AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ DE PROGRAMMEUR

ANNÉE 2023

_____

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 1

Durée : 3 heures – Coefficient : 4

_____

Réponses à des questions et/ou cas pratique
à partir d'un dossier composé de documents à caractère économique et financier

_____

Toute note inférieure à 5/20 est éliminatoire.

_____

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

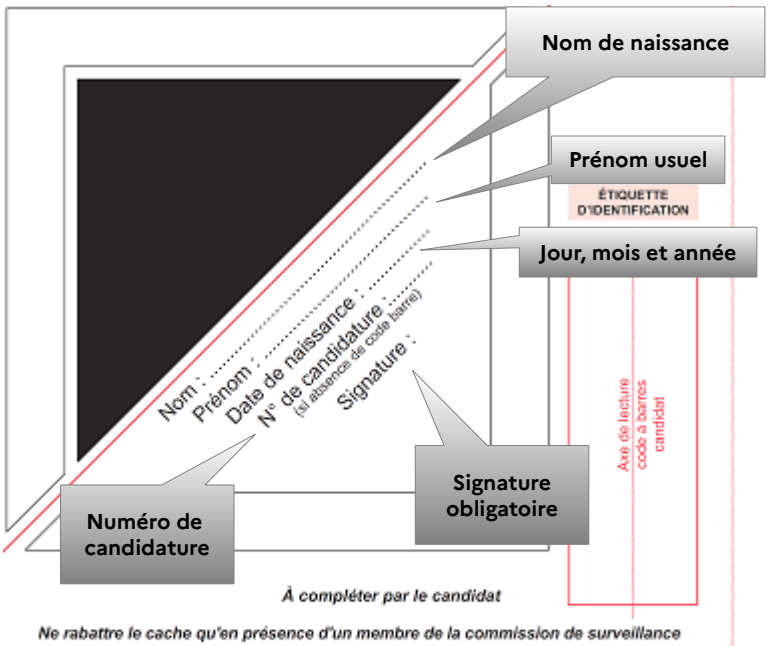
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

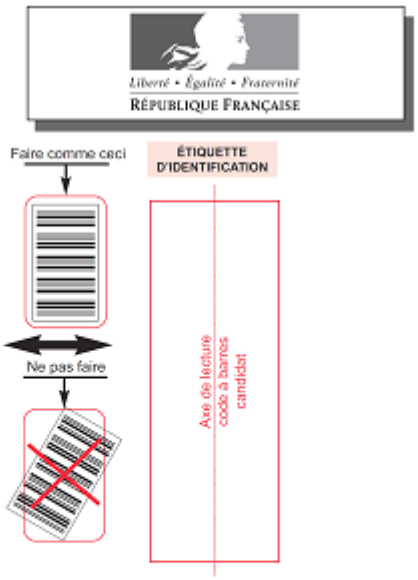
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





Concours externe - interne - professionnel - ou examen professionnel (1)
(1) Rayer les mentions inutiles

Externe

Pour l'emploi de : **Contrôleur Programmeur des Finances Publiques**

Épreuve n° : 1

Matière : ....**101- Analyse de dossier**.....

Date : 1 1 0 4 2 0 2 3

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones **NOTE / 20** et dans le cadre **A**

En cas d'erreur de codification dans le report des notes cochez la case **erreur** et reportez la note dans le cadre **B**.

Cadre A réservé à la notation		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75

Cadre B réservé à la notation rectificative		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75
Erreur		

NOTE / 20 ,

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

ANALYSE DE DOSSIER

Code matière : 101

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

À partir des seuls documents joints, vous traiterez chacune des questions suivantes.

Question 1

Vous présenterez la Stratégie nationale de cybersécurité mise en place en 2021.

Question 2

Selon vous, pourquoi la Stratégie nationale de cybersécurité a été intégrée au plan d'investissement France 2030 ? Votre réponse devra être synthétique (maximum 10 lignes).

Question 3

Quelles actions sont mises en place par les pouvoirs publics pour protéger et sensibiliser les citoyens à la cybersécurité ?

Tournez la page S.V.P.

Liste des documents

Document 1	Article « Stratégie nationale d'accélération pour la cybersécurité : les premières réalisations », issu du site economie.gouv.fr, du 16 février 2022 (3 pages)
Document 2	Communiqué de presse n°2030 « France 2030 : Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, inaugure le Campus cyber à la Défense et est revenu sur les premières réalisations de la stratégie nationale cyber », du 15 février 2022 (5 pages)
Document 3	Plaquette de présentation « Ensemble au service d'une grande nation cyber », issu du site campuscyber.fr (4 pages)
Document 4	Communiqué de presse « L'ANSSI, le Campus Cyber et le CCA s'associent pour organiser l'exercice REMPAR22 », issu du site ssi.gouv.fr, du 1er décembre 2022 (2 pages)
Document 5	Article « Cybersécurité : le gouvernement mise sur un filtre anti-arnaque et un cyberscore dès 2023 », issu du site bercynumérique.finances.gouv.fr, du 8 novembre 2022 (mise à jour le 16 janvier 2023) (1 page)
Document 6	Article « Cybersécurité : Pix, l'ANSSI et Cybermalveillance.gouv.fr s'associent pour développer les compétences du grand public », issu du site pix.fr, du 24 mars 2022 (2 pages)

Le fonds documentaire comporte 17 pages.

Article « Stratégie nationale d'accélération pour la cybersécurité : les premières réalisations », issu du site economie.gouv.fr, du 16 février 2022

Stratégie nationale d'accélération pour la cybersécurité : les premières réalisations

Lancée en février 2021, la stratégie nationale cyber s'inscrit désormais dans le plan d'investissement France 2030. Détails de cette stratégie et des premières réalisations.

Tripler le chiffre d'affaires du secteur cyber et créer 37 000 emplois d'ici 2025. C'est l'ambition de la stratégie nationale d'accélération pour la cybersécurité, dotée d'un **plan de plus d'un milliard d'euros**.

Cette stratégie s'articule autour de quatre axes :

- développer des solutions souveraines et innovantes de cybersécurité
- renforcer les liens et synergies entre les acteurs de la filière
- soutenir la demande (individus, entreprises, collectivités et État), notamment en la sensibilisant mieux les Français sur la cybersécurité, tout en faisant la promotion des offres nationales
- former plus de jeunes et de professionnels aux métiers de la cybersécurité.

Un an après sa présentation le 18 février 2021, puis son rattachement au plan France 2030, de nombreuses actions ont été lancées.

1 039 000 000 D'EUROS
Financement total de la stratégie d'accélération cybersécurité, dont 720 millions d'euros d'argent public.

Favoriser la collaboration entre acteurs : le Campus cyber

Le 15 février 2022, le **Campus cyber a été inauguré**. Celui-ci sera le fer de lance de la France en matière de politique cyber.

Focus : le Campus cyber
Le Campus cyber est l'incarnation de la politique française en matière de cybersécurité. Il rassemble plus de 160 acteurs nationaux et internationaux de la sécurité numérique, soit 1 800 experts. Le Campus dirigé par Michel Van Den Berghe doit permettre de favoriser la réalisation de projets de recherche et de développement ainsi que l'éclosion des licornes (start-up valorisée à plus d'un milliard de dollars) cyber de demain.

Ce campus accueillera et favorisera la collaboration entre les entreprises (grands groupes, PME et start-ups), les services de l'État (agence nationale de la sécurité des systèmes d'information, ministères de l'Intérieur et des Armées, etc.), les acteurs de la recherche, les organismes de formation et les associations.

L'objectif, renverser le rapport de force avec les cyber-attaquants ou cybercriminels. Lieu d'expérimentation et de partage, le Campus est fortement soutenu par la stratégie d'accélération cyber, avec près de **100 millions d'euros directs et indirects**.

Tournez la page S.V.P.

Soutenir l'innovation

Des appels à projets pour développer la filière française
Le soutien au développement de technologies cyber innovantes et critiques est au centre de la stratégie cyber. Financé à hauteur de 150 millions d'euros par France 2030, trois appels à projets ont déjà été ouverts.

Le start-up studio cyber booster
De nombreuses actions de soutien à l'entreprenariat ont aussi été mises en place, comme le start-up studio cyber booster, financé par le PIA4. Ce dispositif, unique en Europe, accompagne la création et l'amorçage dans le domaine de la cybersécurité. Trois start-ups sont déjà incubées et près de 50 dossiers sont en cours d'instruction.

Vers la mise en place d'un accélérateur de start-ups
Dans le prolongement, un appel à manifestation d'intérêt « Stratégie Nationale Cyber – Projets d'accélérateur cyber » a été lancé. Celui-ci vise la mise en place d'un accélérateur en lien avec la création du Campus cyber. Il doit se concentrer sur l'accélération de structures déjà créées et à la maturité supérieure à celles visées par le start-up studio cyber.

Exploiter tout le potentiel de la recherche

La stratégie ambitionne également de soutenir la recherche. À cet effet, un programme équipement prioritaire de recherche (PEPR), doté de 65 millions d'euros est en cours. Celui-ci doit permettre d'exploiter le fort potentiel de recherche et de croissance de la filière française.

Pour accompagner et favoriser le transfert de compétences et de technologies issues de la recherche publique, un programme de transfert sur le Campus cyber, opéré par l'institut national de recherche en sciences et technologies du numérique (INRIA), permettra de se concentrer sur l'identification et la mise en œuvre de projets de recherche et développement à forte valeur ajoutée.

Renforcer la cybersécurité des administrations et des collectivités

Le volet cybersécurité du plan France Relance, mobilisant 136 millions d'euros sous pilotage de l'agence nationale de la sécurité des systèmes d'information (ANSSI), a pour vocation d'élever significativement le niveau de sécurité numérique de l'État et des services publics.

Ce dispositif est orienté en priorité vers les collectivités territoriales et les entités impliquées dans la vie quotidienne des citoyens. Près de 600 bénéficiaires ont déjà été retenus.

Dans ce cadre, les computers security incident response team (CSIRT), des centres d'alerte et de réaction aux attaques informatiques destinés aux entreprises ou aux administrations de plusieurs régions (Bourgogne Franche-Comté, Centre-Val-de-Loire, Corse, Grand-Est, Normandie, Nouvelle Aquitaine et Sud-Provence-Alpes-Côte-d'Azur) participent au programme d'incubation de quatre mois mis en place par l'ANSSI dès février 2022.

Cette incubation doit permettre aux CSIRT régionaux d'être rapidement opérationnels pour répondre de manière pertinente et efficace aux besoins identifiés, tout en s'intégrant

pleinement à l'écosystème territorial et national. Un nouveau programme d'incubation sera proposé au second semestre 2022 pour les régions volontaires.

Former les talents cyber de demain

L'appel à manifestation « Compétences et métiers d'avenir »
Pour répondre aux besoins en formation, ce volet de la stratégie cyber est doté de 140 millions d'euros via l'appel à manifestation « Compétences et métiers d'avenir » (CMA) de France 2030. Deux vagues de relèves sont prévues les 24 février et 5 juillet 2022.

Former des étudiants à la cybersécurité
L'objectif de créer 37 000 emplois dans la filière ne sera atteignable que si des moyens de formation importants sont déployés. Environ 9 250 personnes seront formées afin de devenir des spécialistes du domaine à tous les niveaux de bac+2 à bac+8. La recherche doit également être soutenue via le financement de 100 thèses.

3 050 000
Nombre d'étudiants qui seront formés sur cinq ans (610 000 par an) afin de leur donner un socle indispensable sur la cybersécurité et augmenter le niveau de conscience cyber de la population

Tournez la page S.V.P.

Communiqué de presse n°2030 « France 2030 : Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, inaugure le Campus cyber à la Défense et est revenu sur les premières réalisations de la stratégie nationale cyber », du 15 février 2022

GOUVERNEMENT

Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

FRANCE 2030 : Bruno Le Maire, ministre de l'Economie, des Finances et de la Relance, inaugure le Campus cyber à la Défense et est revenu sur les premières réalisations de la stratégie nationale cyber

Paris-La Défense, le 15 février 2022
N°2030

Un an après l'annonce de la Stratégie Nationale Cyber, le Campus Cyber a été inauguré par Bruno Le Maire, ministre de l'Economie, des Finances et de la Relance, Frédérique Vidal, ministre de l'Enseignement supérieur et de la recherche et de l'innovation, et Cédric O, secrétaire d'Etat de la Transition numérique et des Communications électroniques. Ce campus sera le fer de lance de la France en matière de politique cyber.

Annoncé par le président de la République à l'été 2019, le Campus Cyber est l'incarnation de la politique française en matière de cybersécurité menée par la France. **Rassemblant plus de 160 acteurs nationaux et internationaux de la sécurité numérique - soit 1 800 experts - le Campus dirigé par Michel Van Den Berghe permettra de favoriser la réalisation de projets de recherche et de développement ainsi que l'éclosion des licornes cyber de demain.**

Ce campus accueillera et favorisera la collaboration entre les entreprises (grands groupes, PME et startups), les services de l'État (ANSSI, Ministère de l'Intérieur, Ministère des Armées...), les acteurs de la recherche (INRIA, CEA, CNRS...) les organismes de formation et les associations. Le regroupement de l'ensemble de ces acteurs, métiers et compétences est la clé du succès pour innover et pour renverser le rapport de force avec les cyber-attaquants ou cybercriminels. Lieu d'expérimentation et de partage, le Campus est fortement soutenu par la stratégie d'accélération cyber, avec près de 100 millions d'euros directs et indirects.

La stratégie cyber française a plus largement pour ambition de tripler le chiffre d'affaires du secteur cyber et de créer 37 000 emplois d'ici 2025. Le déploiement de ce plan doté de plus d'un milliard d'euros est dynamique. De nombreuses actions ont été lancées depuis un an parmi lesquelles :

Soutenir l'innovation et la recherche

Le soutien au développement de technologies cyber innovantes et critiques, au centre de la stratégie, est lancé. **Financés à hauteur de 150 M€ par France 2030 sur la durée du plan, trois appels à projets ont déjà été ouverts (dont 2 en cours).** Plus de cinq startups, PME et grandes entreprises sont déjà soutenues parmi les premiers lauréats (voir la liste en annexe).

De nombreuses actions de soutien à l'entreprenariat ont aussi été mises en place, comme le start-up studio Cyber Booster, co-localisé entre Rennes et le Campus cyber et financé par le PIA4. Ce dispositif unique en Europe accompagne la création, et l'amorçage dans le domaine de la cybersécurité. Trois startups sont déjà incubées et près de 50 dossiers sont en cours d'instruction.

La prochaine étape sera la mise en place d'un accélérateur de start-ups.

La stratégie ambitionne également de soutenir la recherche sur le sujet. A cet effet, un **Programme et Equipement Prioritaires de Recherche (PEPR), doté de 65M€ et piloté par le CEA, CNRS, INRIA est en cours.** Il permettra d'exploiter le fort potentiel de recherche et de croissance de la filière française afin de garantir les conditions de sécurité nécessaires au développement des usages.

Pour accompagner et favoriser le transfert de compétences et de technologies issues de la recherche publique, un **Programme de transfert sur le Campus opéré par l'Inria** permettra de se concentrer sur le sourcing et la mise en œuvre de projets de R&D à forte valeur ajoutée, en partenariat avec le CEA, le CNRS, l'IMT et les grandes universités de recherche actives en cybersécurité, l'ANSSI et des entreprises.

Renforcer la résilience

Pour ce qui est de notre protection collective, le volet cybersécurité de France Relance, mobilisant 136 M€ sous pilotage de l'ANSSI, a pour vocation d'élever significativement le niveau de sécurité numérique de l'État et des services publics. Ce dispositif est orienté en priorité vers les collectivités territoriales et les entités impliquées dans la vie quotidienne des citoyens. Au 1er décembre 2021, 590 bénéficiaires ont déjà été retenus pour 45 M€ d'accompagnement, dont 438 collectivités territoriales, 109 établissements de santé et 43 établissements publics sur toute la France.

Par ailleurs, les Computer Security Incident Response Team (CSIRT) de Bourgogne Franche-Comté, du Centre Val de Loire, de Corse, du Grand Est, de Normandie, de Nouvelle Aquitaine et du Sud -Provence Alpes Côte d'Azur participeront au programme d'incubation de 4 mois mis en place par l'ANSSI dès février 2022. Cette incubation permettra aux CSIRT régionaux d'être rapidement opérationnels pour répondre de manière pertinente et efficace aux besoins

Tournez la page S.V.P.

identifiés, tout en s'intégrant pleinement à l'écosystème territorial et national. Un nouveau programme d'incubation sera proposé au second semestre 2022 pour les régions volontaires.

Former les talents cyber de demain

Pour répondre aux besoins en formation, la stratégie est dotée de 140 M€ via l'appel à manifestation « Compétences et métiers d'avenir » (CMA) de France 2030, dont deux vagues de relèves sont prévues les 24 février et 5 juillet 2022.

L'objectif de créer 37 000 emplois dans la filière ne sera atteignable que si des moyens de formation importants sont déployés. Environ 9250 personnes seront formées afin de devenir des spécialistes du domaine à tous les niveaux de bac+2 à bac+8. La recherche sera également soutenue via le financement de 100 thèses.

La formation massive des non spécialistes, 3 050 000 étudiants sur 5 ans, permettra enfin de donner un socle indispensable sur la cybersécurité à de nombreux jeunes Françaises et Français afin d'augmenter considérablement le niveau de conscience cyber de la population.

Sur ces sujets, la stratégie s'appuiera de manière importante sur les synergies apportées par le Campus cyber qui regroupe déjà plusieurs organismes de recherche, des acteurs de la formation et des employeurs à la recherche de profils cyber qualifiés.

Le Ministre de l'Economie, des Finances et de la Relance Bruno Le Maire a déclaré «*Le numérique est porteur d'avenir et d'espoir, mais il est aussi porteur de menaces. Face à ces menaces, l'Etat lève les boucliers, pour protéger ses citoyens, ses entreprises et ses services publics. En ce sens, l'inauguration de ce campus cyber est une étape majeure dans la mise en œuvre de la stratégie nationale de cybersécurité décidée par le président de la République. C'est un enjeu vital pour notre souveraineté et une opportunité économique majeure pour nos entrepreneurs et nos start-ups. Il faut donc continuer à déployer cette stratégie et investir aux côtés des acteurs privés de l'écosystème cyber français dans les compétences, la formation et les entreprises du secteur*».

Cédric O, secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques déclare *« Après un an de mise en œuvre au pas de charge, la stratégie nationale cyber accélère et prend une nouvelle dimension avec l'inauguration du campus cyber. Nous sommes fiers de ce lieu emblématique public-privé, qui est une première en Europe.*

La stratégie nationale cyber allie une grande ambition technologique et une action résolue pour élever notre niveau de résilience face aux cyber-menaces.

La protection de nos concitoyens, de nos entreprises et des collectivités publiques passe par la mobilisation des talents, des énergies, des moyens et des intelligences de chacun : start-ups, grands groupes, filières industrielles, collectivités territoriales, organismes de recherche, forces et agences de sécurité. Les acteurs sont pleinement au rendez-vous. ».

Contacts presse

Cabinet du secrétaire d'Etat chargé de la Transformation numérique et des Communications électroniques
presse@numerique.gouv.fr

Secrétariat général pour l'investissement
01 42 75 64 58
presse.sgpi@pm.gouv.fr

Direction générale des entreprises
01 44 97 04 49
presse.dge@finances.gouv.fr

A propos de France 2030

Le plan d'investissement France 2030 :

- ✓ **Traduit une double ambition** : transformer durablement des secteurs clefs de notre économie (énergie, automobile, aéronautique ou encore espace) par l'innovation technologique, et positionner la France non pas seulement en acteur, mais bien en leader du monde de demain. De la recherche fondamentale, à l'émergence d'une idée jusqu'à la production d'un produit ou service nouveau, France 2030 soutient tout le cycle de vie de l'innovation jusqu'à son industrialisation.
- ✓ **Est inédit par son ampleur** : 54 Md€ seront investis pour que nos entreprises, nos universités, nos organismes de recherche, réussissent pleinement leurs transitions dans ces filières stratégiques. L'enjeu : leur permettre de répondre de manière compétitive aux défis écologiques et d'attractivité du monde qui vient, et faire émerger les futurs champions de nos filières d'excellence.
- ✓ **Sera mis en œuvre collectivement :** pensé en concertation avec les acteurs économiques, académiques, locaux et européens pour en déterminer les orientations stratégiques. Les porteurs de projets sont invités à déposer leur dossier via une procédure ouverte, exigeante et sélective pour bénéficier de l'accompagnement de l'Etat, dans la continuité des Programmes d'investissements d'avenir et du plan France Relance.
- ✓ **Est piloté par le Secrétariat général pour l'investissement** pour le compte du Premier ministre.

Plus d'informations sur : https://www.gouvernement.fr/secretariat-general-pour-l-investissement-sgpi
@SGPI_avenir

Tournez la page S.V.P.

ANNEXE

Les premiers lauréats retenus sont les suivants :

OLVID – WORKSPACE / OLVID

L'objectif du projet est de développer une solution de visioconférence, chat et partage de fichiers sécurisée qui offre une garantie sur la confidentialité et l'intégrité des données, l'assurance de l'identité des interlocuteurs, un anonymat complet vis-à-vis des tiers, tout cela sans avoir à faire confiance au moindre serveur, avec une simplicité d'usage, ouverte sur l'extérieur et sans aucune limite sur le nombre d'utilisateurs.

PARSEC EVENT HORIZON / SCILLE

Le projet consiste à réaliser, par hybridation avec des produits existants, une suite bureautique complète « Zero Trust » et « Zero Knowledge » (édition collaborative, messagerie instantanée, stockage de fichier, moteur d'indexation, couplage annuaire d'entreprise ...), permettant aux utilisateurs de collaborer et d'échanger sans latence des données sensibles chiffrées de bout-en-bout et signées en utilisant le Cloud Public comme pivot d'échange.

CYBERSAFE OS / PROVE & RUN

L'objectif du projet CyberSafeOS est de fournir aux architectes des systèmes cyber physique, une brique technologique essentielle sous la forme d'un système d'exploitation (OS) destiné à être utilisé et intégré comme un composant off-the-shelf (COTS) lors de la conception de ces systèmes pour répondre aux doubles exigences cybersécurité et sureté de fonctionnement.

CASES / CLEARSY

Le projet CASES vise à construire un calculateur générique sûr et sécuritaire souverain, permettant de contrôler et commander des infrastructures critiques au plus haut niveau d'intégrité. Il combine l'état de l'art en matière de calculateur et de logiciel, en ayant recourt de manière raisonnée aux méthodes formelles.

OVERSEC / STORMSHIELD

Le projet Oversec vise à concevoir une brique logicielle multiplateforme intégrable dans les différents actifs des infrastructures critiques, permettant de filtrer et chiffrer leurs communications. Durcie, elle sera conçue de façon à être très résiliente aux cyberattaques et aux pannes matérielles ou logicielles qui pourraient impacter la sûreté de fonctionnement et les processus pour la maintenir en conditions opérationnelles et de sécurité, dont les mises à jour, devront être transparents pour la production protégée. En outre, le déploiement et la configuration des différentes instances du logiciel se feront de façon globale, avec une approche accessible pour les métiers non experts en cybersécurité.

Plaquette de présentation « Ensemble au service d'une grande nation cyber », issu du site campuscyber.fr

CAMPUS CYBER

Tournez la page S.V.P.

FAIRE RAYONNER L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ.

SON CONCEPT

Projet initié par le président de République, le Campus Cyber est le lieu totem de la cybersécurité qui rassemblera les principaux acteurs nationaux et internationaux du domaine. Il permettra d'accueillir sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations.
Le Campus Cyber prévoit de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. Des partenariats entre le Campus national et des Campus territoriaux de cybersécurité seront développés dans les prochains mois. À ce jour, plus de 160 acteurs, issus d'une pluralité de secteurs d'activité, ont confirmé leur engagement.

SA MISSION

Réunir les acteurs de la sécurité numérique au sein d'un lieu totem pour protéger la société et faire rayonner l'excellence française du domaine.

SA VISION

L'écosystème cyber est le levier pour accélérer la création d'une société numérique de confiance.

SES VALEURS

EXCELLENCE | CONFIANCE | PARTAGE

UN MODÈLE FONDÉ SUR 4 PILIERS.

LES OPÉRATIONS

Partage des données pour renforcer la capacité de chacun à maîtriser le risque numérique

- Rassemblement d'experts de l'analyse cyber afin de renforcer les capacités de veille, de détection et de réponse à la menace.
- Création d'un observatoire de la cybermenace et d'une base commune de « Threat Intelligence » composée des indices de compromission assemblés par les différents partenaires publics et privés.

L'INNOVATION

Développement des synergies entre les acteurs publics et privés pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique

- Programmes communs qui rassembleront les industriels, start-up et centres de recherche.

LA FORMATION

Aide à la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiante(s), personnels en reconversion...) pour une montée en compétence globale de l'écosystème

- Programmes communs d'entraînement et de formation dispensés par des écoles ou des centres de formation.
- Partage de ressources matérielles et académiques.
- Sensibilisation et création de nouvelles vocations.

MOBILISATION

Un lieu vivant et ouvert dédié à la programmation d'événements innovants propice, aux échanges et à la découverte des évolutions de la société numérique de confiance

- L'équipe Campus Cyber accompagnera la réalisation de conférences, webinaires, podcasts, tables rondes, pitchs, job dating, création des communs de la cyber, expérimentations, learning expeditions, événements internationaux, speed dating investisseurs.

DES MOYENS UNIQUES :

17 000 M² d'espaces de travail privés ou partagés

6 000 M² de plateaux projets et d'innovation

3 000 M² consacrés à la formation

SHOWROOM // AUDITORIUM // STUDIO TV // « CAFÉ » PRIVÉ // ESPACES DE RÉCEPTION // PLATEFORME INTELLIGENCE ARTIFICIELLE (IA) // PLATEFORME DE FORMATION // CYBER RANGE

Tournez la page S.V.P.

CAMPUS CYBER

26 000 M² AU CŒUR DE LA DÉFENSE : LE CAMPUS CYBER

UNE CONNEXION IDÉALE

Transport en commun au pied de l'immeuble

Ⓜ1 Esplanade de la Défense

RER A La Défense *(Grande Arche)*

Accessibilité routière optimale

Quai de Dion Bouton à 200 mètres / Boulevard circulaire au pied de l'immeuble

NOUS CONTACTER :

contact@campuscyber.fr

@CampuscyberFR

Communiqué de presse « L'ANSSI, le Campus Cyber et le CCA s'associent pour organiser l'exercice REMPAR22 », issu du site ssi.gouv.fr, du 1er décembre 2022

COMMUNIQUÉ DE PRESSE

Paris, le 01/12/2022

L'ANSSI, le Campus Cyber et le CCA s'associent pour organiser l'exercice REMPAR22

Face à la menace cyber croissante et à un nombre d'attaques toujours plus important, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *le Campus Cyber et le Club de la continuité d'activité (CCA) s'unissent pour organiser REMPAR22, un exercice de simulation de crise cyber de grande ampleur, le jeudi 8 décembre 2022, autour d'un scénario unique créé pour l'occasion.*

Avec plus de 200 participants, issus de 100 organisations sur tout le territoire national, REMPAR22 fédère cet écosystème dans sa diversité autour d'un exercice cyber commun. Dispositif aujourd'hui inédit en France, la mise en place de cet exercice au sein du Campus Cyber, s'inscrit dans une stratégie d'entraînement cyber globale au profit d'acteurs publics, d'entreprises et d'associations, de niveau décisionnel et opérationnel.

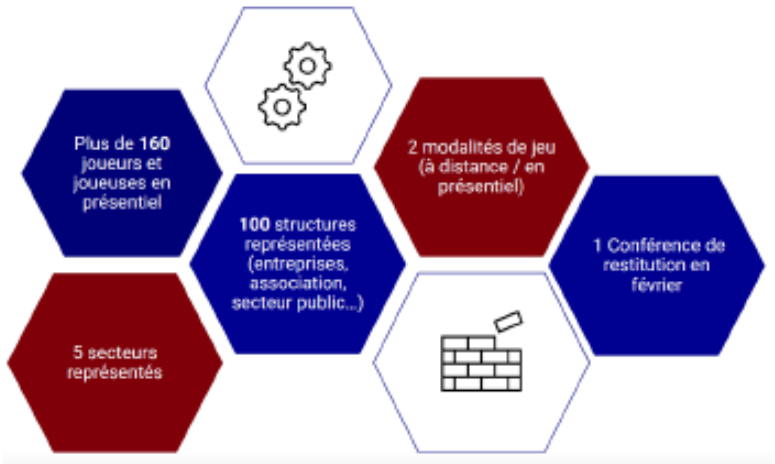
S'entraîner face à une menace hétérogène

Cet événement illustre une volonté forte de collaboration poussée afin d'améliorer le niveau global de cybersécurité en France. Face à des attaques qui se multiplient, il est essentiel de s'interroger sur les capacités des organisations françaises à répondre à une crise majeure sur leurs services. Les participants à l'exercice seront ainsi rassemblés dans une entreprise fictive en proie à une cyberattaque de grande ampleur et devront se coordonner afin de gérer la pression et d'opter pour les bons réflexes afin d'assurer une continuité d'activité.

L'exercice REMPAR22 est à l'initiative de trois instances, l'ANSSI, le Campus Cyber et le CCA, qui collaborent de façon rapprochée pour une organisation efficace. Tous ensemble, ils ont définis des objectifs pour cette séquence :

- Sensibiliser aux enjeux de continuité d'activité face au risque de « blackout » numérique ;
- Tester les dispositifs de gestion de crise afin de s'assurer de la prise en compte des spécificités des cyberattaques ;
- Entrainer la coordination des acteurs entre eux et au sein d'un même secteur ;
- Travailler les modalités de communication de crise en interne et en externe ;
- Créer des dynamiques de partage et d'échange entre les communautés et les secteurs.

Tournez la page S.V.P.



A propos de l'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale. L'ANSSI assure la mission d'autorité en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité de la Première ministre.
https://www.ssi.gouv.fr/

A propos du Campus Cyber

Projet initié par le président de République, le Campus Cyber est le lieu totem de la cybersécurité qui rassemble les principaux acteurs nationaux et internationaux du domaine. Il permet d'accueillir plus de 250 acteurs issus d'une pluralité de secteurs d'activité sur un même site : entreprises (grands groupes, PME), services de l'État, organismes de formation, acteurs de la recherche et associations.
https://campuscyber.fr/

A propos du CCA – Club de la continuité d'activité

Association régie par la loi de 1901, créée en 2007 pour échanger sur la Gestion de la Continuité d'Activité. Elle est ouverte à tous les praticiens de la Continuité d'Activité et réunit des entreprises de toutes tailles et de tous secteurs.
https://www.clubpca.eu/

Contacts presse :

ANSSI

Roxane ROSELL
Attachée de presse
roxane.rosell@ssi.gouv.fr
06 49 21 63 80
presse@ssi.gouv.fr

CAMPUS CYBER

Delphine Perez
Directrice de la communication
delphine@campuscyber.fr

Angèle Guilbert
Cheffe de projet
angele@campuscyber.fr

CCA

Monique Tinas
Présidente
monique.tinas@natixis.com
06 76 75 01 68

Article « Cybersécurité : le gouvernement mise sur un filtre anti-arnaque et un cyberscore dès 2023 », issu du site bercynumérique.finances.gouv.fr, du 8 novembre 2022 (mise à jour le 16 janvier 2023)

Cybersécurité : le gouvernement mise sur un filtre anti-arnaque et un cyberscore dès 2023

Dans le cadre du plan national pour la cybersécurité présenté par Emmanuel Macron en 2021, le gouvernement déploie des dispositifs pour protéger les Français des attaques en ligne. Promesse de campagne du chef de l'État, un filtre anti-arnaque sera testé l'an prochain.

La France affine sa stratégie en matière de cybersécurité. En visite le 27 octobre 2022 au Campus Cyber, érigé comme le « totem de la cybersécurité en France » par le gouvernement, Jean-Noël Barrot, ministre délégué au Numérique, a annoncé la mise en place de plusieurs dispositifs en 2023 pour protéger davantage les Français face à la multiplication et la sophistication des attaques en ligne. Le successeur de Cédric O souhaite ainsi développer une « cybersécurité du quotidien ».

Dans ce sens, Jean-Noël Barrot a fait savoir qu'un filtre anti-arnaque allait voir le jour. Promesse de campagne d'Emmanuel Macron, ce dispositif vise à filtrer de manière préventive les adresses internet qui correspondent à des sites malveillants, aussi bien sur ordinateur que sur smartphone. Ce filtre sera proposé en version bêta à l'été 2023, avant un déploiement auprès du grand public un an plus tard.

Un cyberscore sur le modèle du Nutri-Score

Par ailleurs, le ministre a rappelé qu'un cyberscore allait être lancé l'an prochain. À l'image du système d'étiquetage Nutri-Score pour les produits alimentaires, les sites internet, y compris les réseaux sociaux, devront ainsi afficher un « cyberscore » officiel, soit une note permettant de signaler aux internautes le niveau de sécurisation des données hébergées par les sites qu'ils utilisent. Si les modalités de ce dispositif restent encore à définir, son entrée en application est prévue pour le 1er octobre 2023.

L'arrivée de ces deux mécanismes pour se prémunir des attaques et des arnaques en ligne s'inscrit dans le cadre du plan national pour la cybersécurité présenté en 2021 par Emmanuel Macron. Celui-ci est doté d'une enveloppe d'un milliard d'euros pour accélérer le développement de la filière. Jean-Noël Barrot a indiqué que 100 millions d'euros avaient déjà été engagés. D'ici à 2025, le gouvernement ambitionne notamment de multiplier par trois le chiffre d'affaires du secteur (7,3 milliards d'euros actuellement), créer 37 000 emplois et faire émerger au moins trois licornes (start-up dont la valorisation dépasse le milliard de dollars).

Tournez la page S.V.P.

Article « Cybersécurité : Pix, l'ANSSI et Cybermalveillance.gouv.fr s'associent pour développer les compétences du grand public », issu du site pix.fr, du 24 mars 2022

Cybersécurité : Pix, l'ANSSI et Cybermalveillance.gouv.fr s'associent pour développer les compétences du grand public

La numérisation croissante de la société consacre la maîtrise des compétences en sécurité numérique comme un enjeu majeur, au niveau individuel comme collectif. Que ce soit par négligence ou ignorance, dans plus de 90 % des incidents de sécurité numérique, l'erreur humaine est impliquée. La crise sanitaire due au COVID-19 venant bouleverser d'autant plus les usages du numérique de chaque citoyen sur le plan professionnel comme personnel, la cybersécurité est plus que jamais d'actualité, comme en témoigne la crise de sécurité qui secoue l'Europe. Dès lors, la pédagogie aux risques cyber est un défi qu'il est nécessaire de relever sur les bancs de l'école, de l'université, dans le monde du travail ou encore dans le tissu associatif, et qui participe d'un effort global de renforcement de notre souveraineté numérique.

Dans ce contexte, Pix s'associe à l'ANSSI et Cybermalveillance.gouv.fr, les références en France en matière de cybersécurité, pour expertiser et concevoir des défis pédagogiques accessibles à tous sur la plateforme pix.fr dans le domaine de la Sécurité numérique et pour produire un référentiel à destination des professionnels de l'enseignement et de la formation pour les appuyer dans l'accompagnement de leurs apprenants. Dans la continuité de cette démarche, et pour l'inscrire dans la durée, l'ANSSI rejoint officiellement le Groupement d'intérêt public Pix.

Un référentiel des compétences numériques de cybersécurité à destination des acteurs de l'enseignement et de la formation

Pix, en partenariat avec l'ANSSI et Cybermalveillance.gouv.fr et avec l'appui du ministère de l'Education nationale, de la Jeunesse et des Sports, a créé un référentiel des compétences numériques de cybersécurité dans le but de proposer une vision précise et structurée des compétences en sécurité numérique pour accompagner les acteurs de la formation (enseignants, formateurs…) dans leurs enseignements et pratiques d'évaluation.

Ce référentiel entend la sécurité numérique au sens large : bonnes pratiques, comportements de prudence, utilisation des outils de sécurité, mais aussi connaissance des menaces, compréhension des mécanismes de protection et de réaction, participation à l'effort collectif de sécurisation de l'espace numérique.

« *La cybersécurité est un défi collectif urgent et majeur. Grandement corrélées avec la numérisation de nos sociétés, les cybermenaces ont un impact croissant sur nos vies. Il est donc essentiel de former le plus grand nombre de citoyens à la sécurité du numérique et aux comportements responsables dans le cyberespace. En tant qu'autorité nationale de la sécurité des systèmes d'information, l'ANSSI a souhaité engager son expertise aux côtés de Pix et Cybermalveillance pour contribuer à l'élaboration de ce référentiel à destination des acteurs de la formation.* » Aurélie Bauer, Cheffe du Centre de Formation à la SSI à l'ANSSI

« *La sensibilisation est indispensable afin d'évoluer de manière sécurisée dans notre monde de plus en plus connecté. Pour donner aux citoyens les moyens de se protéger des*

cybermenaces en recrudescence, il est nécessaire de mettre en place des outils faciles d'accès pour les aider à se former aux bonnes pratiques et prendre connaissance des risques. Cybermalveillance.gouv.fr est fier de partager son expertise avec Pix et l'ANSSI, et ce référentiel saura certainement apporter les compétences nécessaires à chacun en cybersécurité. » Jérôme Notin, Directeur général de Cybermalveillance.gouv.fr

Des défis ludiques pour accompagner le développement des compétences nécessaires à la sécurité numérique de tout un chacun, accessibles à tous sur pix.fr

Pour sensibiliser aux enjeux de la cybersécurité et pour permettre à chacun de développer des compétences nécessaires à sa sécurité numérique personnelle et professionnelle, Pix permet à tout citoyen, qu'il soit débutant ou déjà à l'aise avec le numérique, de tester, développer et certifier ses compétences de façon ludique sur la plateforme pix.fr, dans le domaine « Protection et Sécurité ». Comme pour l'ensemble des domaines et compétences abordés sur Pix, l'utilisateur utilise le web, son environnement numérique et ses propres connaissances pour répondre à des défis ludiques inspirés de situations réelles d'utilisation comme : déjouer une tentative de phishing, reconnaître une URL suspecte, gérer des mots de passe, réagir en cas de fuites de données personnelles ou d'infection d'un ordinateur, etc. En partenariat avec l'ANSSI et Cybermalveillance.gouv.fr, Pix propose alors sur la compétence « Sécuriser l'environnement numérique » un contenu pédagogique expertisé et conçu conjointement avec ces acteurs.

« *Pix est fier de s'associer à l'ANSSI et Cybermalveillance.gouv.fr dans un partenariat de long terme qui vise à mettre en commun notre expertise et à concevoir des outils pédagogiques innovants au service de la sécurité numérique des élèves, étudiants, actifs, et plus généralement de tous les citoyens. In fine, le but est de les aider à se repérer et à progresser : à accroître leur autonomie, développer les bons réflexes et par conséquent, à être plus responsable face aux risques et menaces cyber, ce qui, de facto participe à notre souveraineté numérique à tous !* » Benjamin Marteau, Directeur de Pix

La cybersécurité : une compétence clé de la plateforme Pix propulsée auprès de l'ensemble des acteurs de la formation, de l'enseignement et de l'accompagnement

Parce que la cybersécurité est aussi l'affaire de tous dans le monde du travail, Pix met systématiquement à disposition des entreprises, collectivités, administrations, et organismes de formation utilisatrices de l'offre « Pix Pro », un parcours composé de tests Pix dédiés à la cybersécurité. Il permet aux acteurs de la formation, des RH, ou encore de la DSI de sensibiliser aux bonnes pratiques de façon ludique, de mesurer le niveau de maturité numérique à grande échelle et de cartographier et cibler les besoins de formation.

La pédagogie aux risques cyber étant nécessaire dès l'école et tout au long de la vie, des tests dédiés à la sécurité numérique sont également mis à disposition dans l'ensemble des cadres de déploiement de Pix : auprès des enseignants du second degré (la Certification Pix est obligatoire en 3e et Tle) et de l'enseignement supérieur, des médiateurs et aidants numériques ou encore auprès des conseillers du Service public de l'emploi.