GOUVERNEMENT
Liberté
Égalité
Fraternité

Communiqué de presse
Paris, le 15 juin 2021

INVESTISSEMENTS D'AVENIR : ANNONCE DES 27 LAUREATS DU GRAND DEFI CYBER – STARTUPS ET PME –

Le secrétaire général pour l'investissement, Guillaume Boudy et William Lecat, coordinateur nationale de la stratégie cybersécurité mise en œuvre dans le cadre du Programme d'investissements d'avenir (PIA) et de France Relance, présentent les 27 lauréats des appels à projets du Grand Défi cyber dédiés aux startups et aux PME. Les startups et les PME lauréates vont bénéficier d'un soutien financier allant de 200 000 euros à 1 400 000 euros.

L'évolution des technologies et des usages numériques transforme radicalement nos vies. L'exposition croissante au numérique nous rend cependant particulièrement vulnérables aux attaques informatiques. L'objectif de ces deux appels à projets était de répondre à cette problématique sécuritaire en investissant dans le développement de technologies de rupture et en favorisant l'émergence accélérée d'acteurs leaders dans leur domaine.

Suite aux appels à projets du Grand Défi cyber publiés les 31 juillet 2020 (dédiés aux PME) et 30 octobre 2020 (dédiés aux startups), visant à soutenir des projets d'innovation de rupture, **27 projets ont été retenus (16 PME et 11 startups) pour un total de 15,9 millions d'euros**. Les thématiques visées correspondent à la première tranche des axes verticaux de la feuille de route du Grand Défi cyber :

- Axe 1 : réseaux dynamiques
- Axe 2 : objets connectés
- Axe 3 : protection des petites structures contre la cybercriminalité

Les 27 lauréats seront éligibles à la seconde tranche des axes verticaux du Grand Défi cyber qui sera lancée début 2022.

bpifrance

LES 16 PROJETS LAUREATS DE L'AAP « PME »

PRESENTATION DES PROJETS LAUREATS DE L'AAP « PME »

iMRC par Tiempo Secure et le CEA Leti [Grenoble] : subvention de 1,41 M€

L'objectif du projet est de concevoir un « integrated Monitoring & Recovery Component » (iMRC), nouvelle génération de « Secure Element », capable de veiller sur le bon fonctionnement du « System-on-Chip » (SoC) dans lequel il est intégré, de garantir l'établissement régulier d'une connexion sécurisée avec une application de monitorage pilotée par un module de sécurité matérielle (*HSM*) géré dans le *cloud,* et de réparer le SoC en cas d'attaque identifiée sur le processeur applicatif.

Massena par Cyberwatch [Paris] : subvention de 0,49 M€

MASSENA (Moteur d'Audit des Systèmes SENsibles et de leur Analyse) est un projet visant à permettre d'automatiser les audits et analyses de vulnérabilités des systèmes sensibles, notamment les systèmes industriels ou classifiés, avec une prise en compte des particularités technologiques de ces derniers (contraintes de scans liées au milieu de la Défense, technologies web modernes durcies, protocoles industriels, environnements mono/multi-Cloud, technologies européennes spécifiques).

O SCAR par Wallix [Paris / Rennes] : subvention de 0,9 M€

Le projet O(Open) SCAR (Services Communs pour l'Administration et le Reporting) propose de fédérer différentes briques de sécurité, permettant l'automatisation de la détection et la prévention des risques Cybersécurité et offrant ainsi une meilleure résilience aux cyber-attaques.

Positionné entre le SIEM et le SOAR, OSCAR permettra de s'assurer (au sens souverain du terme) que les différentes briques utilisées, souveraines ou pas, se comportent conformément à ce qu'elles annoncent.

Proxy SaaS par Olféo [Paris] : subvention de 0,79 M€

Olfeo, leader français des solutions de filtrage de contenus Web pour les administrations et les ETI, a engagé le développement de la première plateforme européenne SaaS pour le filtrage des flux Web.

Le Grand Défi permet de renforcer notre offre ETI et d'élargir notre cible aux PME et TPE, de rendre notre plateforme exploitable par des FAIs qui pourraient ainsi en être distributeurs, et de réaliser des intégrations avec d'autres éditeurs de Cyber sécurité français afin d'augmenter les capacités de défense.

Matrice par Citalid [Paris] : subvention de 0,58M€

La MATRICE est un cockpit modulaire de pilotage du risque et des investissements cyber destiné à devenir l'outil n°1 du RSSI et des Risk Managers en Europe. Grâce à la MATRICE, ces derniers bénéficieront automatiquement d'une vision à 360° sur les contextes technique et business de leur entreprise, ainsi que sur son environnement de menaces. Cet état des lieux permettra également de générer et d'adapter en continu le plan d'investissement optimal de maîtrise du risque cyber, constitué du bon équilibre entre solutions de sécurité et d'assurance.

Virtual Browser par Oodrive [Paris] : subvention de 0,49M€

Le navigateur est le point d'entrée de la grande majorité des cyberattaques dans le réseau d'entreprise. Le projet permet de proposer aux TPE/PME d'isoler la navigation d'un ordinateur, d'un smartphone ou d'une tablette avec le principe du Remote Browser Isolation sur un serveur distant et sécurisé, hébergé en Europe et couplé à des outils de catégorisation d'URL.

Heracles par Egerie [Toulon] : subvention de 0,99M€

Le projet HERACLES (Heighten EGERIE Risk Analysis Concepts, Leveraging Environmental Solutions) ambitionne de développer une solution intégrée capable de produire des analyses de risque dynamiques, et de mettre à disposition leurs résultats de façon contextualisée auprès des acteurs et systèmes clés à même de décider et d'agir. Il élargit également la surface des risques pris en compte, ainsi que leur précision, grâce aux données environnementales obtenues par l'interconnexion de différentes sources.

MIB GD par Mail In Black [Marseille] : subvention de 0,64M€

Mailinblack a pour ambition d'être le leader cybersécurité 360° des organisations qui n'ont pas le temps. Les 2 objectifs de ce projet sont :

- Innover par l'IA, la neuroscience, l'éducation pour offrir les solutions Protect et Phishing Coach les plus simples, les moins chères, les plus « impactantes » du marché
- Interopérer avec l'écosystème des acteurs français clefs pour constituer ensemble un portefeuille de solutions de haute qualité

Open XDR Platform par HarfangLab [Paris] : subvention de 0,83M€

Le projet Grand Défi est complémentaire des travaux du PIA i-Nov qui apportent principalement des fonctions innovantes de détection et de blocage des cyberattaques complexes. A ce stade, Il s'agit de pousser plus loin l'automatisation et de trouver des applications opérationnelles à l'échelle d'une plateforme qui crée des connexions entre l'EDR (Endpoint Detection & Response) et d'autres produits. C'est l'objet de la solution XDR. La technologie EDR amorce un cycle vertueux en rassemblant les informations pertinentes sur le périmètre à défendre. Il permet d'y détecter les comportements suspects et les signaux précurseurs d'une attaque ciblée. L'EDR couvre l'intégralité du processus depuis la collecte jusqu'à l'enrichissement et l'analyse des informations. Il représente une brique essentielle dans le cycle de gestion de la donnée et donc la pierre angulaire d'une plateforme XDR.

0-SOC par Sekoia [Rennes] : subvention de 1,02M€

Le projet vise à mettre à disposition du marché une solution technologique qui repense les offres de SOC existantes, tant sur l'angle des services apportés que des briques technologiques. Ce projet s'appuie sur la plateforme SEKOIA, solution de SIEM *next generation* et de *threat intelligence*. 0-SOC permet de générer des alertes très fiables, contextualisées et disposant d'un plan d'action automatisable. Un seul but : permettre aux entreprises de réagir avant que les menaces ne soient graves.

SICOC par IoT.bzh [Lorient] : subvention de 0,47M€

Le cadre du projet est la cybersécurité des objets connectés industriels (trains, avions, bateaux, éoliennes etc). Notre ambition est de développer une solution pour sécuriser la technique d'isolation par conteneur, très populaire dans le secteur IT et désormais également en vogue dans le domaine embarqué, avec les risques cybersécurité importants qui en découlent.

LEIA par le Systerel et le CEA List [Aix-en-Provence] : subvention de 0,89M€

LEIA vise à fournir une plateforme d'analyse de logiciels capable d'offrir des garanties fortes sur la sécurité des programmes analysés, tout en étant fortement automatisée et susceptible de s'intégrer dans des cycles de développement basés sur l'intégration continue. Le projet s'appuie sur des outils d'analyse déjà bien éprouvés et se propose d'étudier l'apport de techniques d'apprentissage pour en favoriser l'utilisation et améliorer l'efficacité et la précision de leurs résultats.

Loki par Sesame-IT [Paris] : subvention de 0,74M€

La validation du concept et les premières briques de la solution Loki de « deceptive technologie » - ou de leurrage des attaquants - ont été développés en 2019 et lauréats des concours i-Lab, DGA et iNov. Nous allons dans cette nouvelle phase de travaux apporter à Loki les modules complémentaires afin de présenter en 2022 une version commerciale de la solution. Celle-ci pourra déployer automatiquement une série adaptée de leurres réseau, et les superviser pour détecter, analyser et présenter les attaques en cours.

CrowdSec par CrowdSec [Paris] : subvention de 0,65M€

CrowdSec se positionne sur le marché de la cybersécurité avec une approche inédite : bloquer les tentatives de piratage, en temps réel, à n'importe étage du système d'information, via un outil Open-Source en SAAS. Les attaques bloquées sont ensuite envoyées à un serveur appartenant à l'entreprise pour être mutualisées pour l'ensemble de tous les utilisateurs. Le système cartographie ainsi, en temps réel et très précisément, les acteurs ayant un comportement malveillant sur Internet.

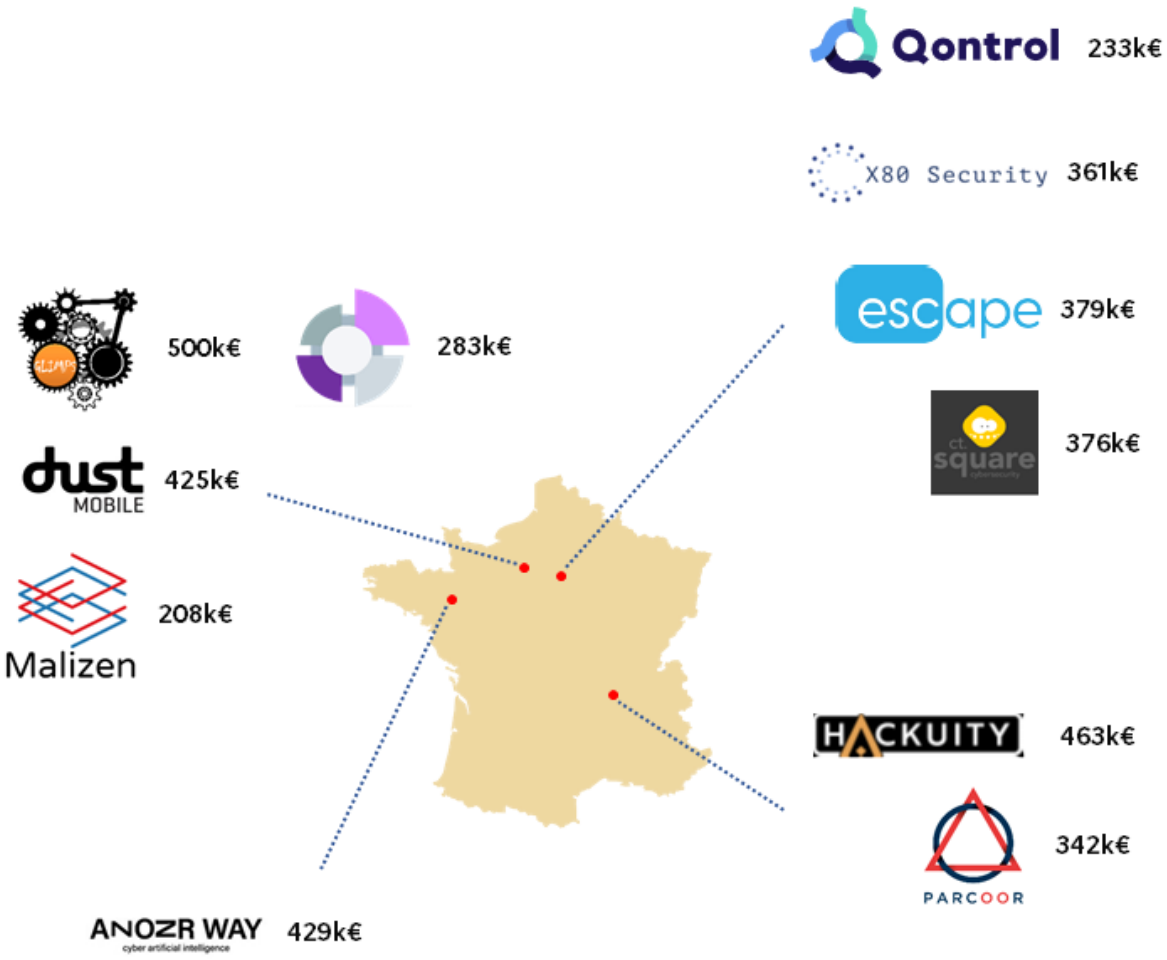
Nucleus par eShard [Aquitaine] : subvention de 0,56M€

Plateforme de surveillance continue des incidents cyber pour l'IoT avec détection automatique via intelligence artificielle.

Cyberia par Tehtris [Pessac] : subvention de 0,48M€

Un SOC in the box 2.0 pour développer une nouvelle technologie d'Intelligence Artificielle permettant d'optimiser les activités de détection et de remédiation des équipes de sécurité opérationnelle.

LES 11 PROJETS LAUREATS DE L'AAP « STARTUPS »



PRESENTATION DES PROJETS LAUREATS DE L'AAP « STARTUPS »

2AD&R par Hackuity [Lyon] : subvention de 463k€

Le projet « Automated Asset Discovery & Rating » (2AD&R) s'inscrit dans l'ambition d'Hackuity de doter sa plateforme de technologies de rupture visant à automatiser la gestion des vulnérabilités. En proposant la première solution qui cartographie les actifs et évalue dynamiquement leur criticité, sur la base d'informations de sources hétérogènes mais complémentaires (ex. scanners de vulnérabilités, CMDB, analyses de risques), Hackuity résout deux problèmes endémiques à la pratique de la Gestion des Vulnérabilités et plus largement à la Cybersécurité.

AADG par X80 [Paris] : subvention de 361k€

X80 Security développe la première solution de cybersécurité basée sur la génération combinée d'attaques et de menaces par intelligence artificielle. La solution est déployée sur cloud et protège le réseau ainsi que tous les terminaux. Elle permet une protection contre les menaces les plus sophistiquées et détecte les intrusions en temps réel, sans faux positifs et en préservant les ressources matérielles de l'infrastructure protégée (CPU et RAM).

DEMA par Parcoor [Lyon] : subvention de 342k€

Le but de ce projet et de développer un système de machine learning pour la détection de malwares. Ce système est destiné à tourner sur des objets connectés eux-mêmes pour les protéger contre la menace de logiciels malveillants. Il s'appuierait sur une approche innovante pour l'analyse de micro-évènements et le fonctionnement sur des environnements très contraints en ressources.

DROP par CT-Square [Paris] : subvention de 376k€

Le projet DROPE porte sur les travaux d'automatisation d'une plateforme de cybersécurité développée par CT-Square et destinée à améliorer sensiblement la protection des PME contre les cyberattaques. Ce projet est la première étape d'une roadmap qui ambitionne de fournir aux PME une solution intégrée, souveraine et adaptée à leurs contraintes spécifiques. Pour CT-Square ce niveau d'automatisation doit permettre de maîtriser les coûts d'exploitation afin de rendre accessible cette plateforme à un maximum d'entreprises.

EscapeTech par Escape Technologies [Paris] : subvention de 379k€

Escape Technologies développe une plateforme SaaS en B2B permettant de tester automatiquement les APIs http de ses clients dans l'optique de détecter et corriger des vulnérabilités ainsi que des failles de sécurité lors des phases de développement.

MalwareHunter par Glimps [Rennes] : subvention de 500k€

Le but du projet GLIMPS Malware-Hunter est de mettre au point une plateforme complète et performante d'analyse de fichiers par conceptualisation de code. GLIMPS Malware-Hunter automatise les différentes étapes de la détection, caractérisation des menaces présentes dans les fichiers ou directement en mémoire volatile. Un effort est mis sur la qualité de l'information présentée lors de la détection d'un évènement malveillant, afin de faciliter les opérations de remédiation. En tirant pleinement parti des possibilités offertes par la technologie de conceptualisation de code GLIMPS, nous adresserons aussi bien les spécificités des réseaux IT classique que des réseaux OT.

HyperMo par Dust Mobile [Evreux] : subvention de 425k€

DUST MOBILE est le 1er opérateur mobile international de cyberdéfense. Son objectif est de sécuriser les télécommunications pour tous les appareils connectés aux réseaux 2G/3G/4G LTE/5G. Le projet HyperMO vise à offrir une solution innovante d'analyse de l'environnement cellulaire, d'hypervision, et de détection de contre-mesures adaptées. Il permettra de générer 2,9 millions d'euros de chiffre d'affaires à horizon 2023, et de créer 58 nouveaux emplois sur le territoire

Moka35 par Anozrway [Rennes] : subvention de 429k€

ANOZR WAY développe depuis 2018, une solution de cyber sécurité « augmentée » afin de prévenir de toutes cybers attaques liées aux failles humaines. Les travaux de R&D menés impliquent des technologies de pointes de machine learning qui permettront à terme une automatisation totale du système de détection et de recommandations, condition indispensable au déploiement sur le marché des petites structures. L'objectif principal est d'être en mesure d'effectuer une analyse plus poussée que les attaquants afin d'anticiper les attaques cyber pour optimiser la défense et ses coûts.

Qontrol par Articule [Paris] : subvention de 233k€

Le projet Qontrol se fixe pour mission de transformer les petites structures (Startups, PME et collectivités territoriales) pour qu'elles maîtrisent leur risque numérique. C'est une plateforme SaaS qui détermine de manière automatisée un plan d'actions adapté à la structure, incluant outils à déployer (en priorité français et européens) et pratiques à mettre en place. La plateforme accompagne ensuite au quotidien les décideurs et employés de la structure pour mettre en place avec succès la stratégie de cybersécurité choisie.

SYRRHCé par Cy Mind [Rennes] : subvention de 283k€

SYRRHCé - Système de Renforcement de la Résilience Humaine contre la Cybercriminalité - proposera une solution simple afin de prévenir de toutes cyber-attaques liées aux failles du périmètre humain avec une automatisation impliquant de l'intelligence artificielle fédérative. L'ensemble des traitements est opéré localement en garantissant la confidentialité avec une "Tech for Good".

WARP par Malizen [Rennes] : subvention de 208k€
Notre objectif principal est d'augmenter les capacités de notre plateforme à destination des SOC et des CERT avec les toutes dernières avancées scientifiques en termes de machine learning, de statistiques et de systèmes de recommandation. Pour atteindre cet objectif nous devons dans un premier temps enrichir notre compréhension du fonctionnement des équipes de cybersécurité et du mode opératoire de leurs membres, d'abord par des études qualitatives puis par des mesures quantitatives automatisées. Dans un second temps ces systèmes automatiques vont nécessiter des données de qualité associé à des appréciations humaines afin d'apprendre et permettre de prendre le relai.

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

À propos du Programme d'investissements d'Avenir

Engagé depuis 10 ans et piloté par le Secrétariat général pour l'investissement auprès du Premier ministre, le PIA finance des projets innovants, contribuant à la transformation du pays, à une croissance durable et à la création des emplois de demain. De l'émergence d'une idée jusqu'à la diffusion d'un produit ou service nouveau, le PIA soutient tout le cycle de vie de l'innovation, entre secteurs publics et privés, aux côtés de partenaires économiques, académiques, territoriaux et européens. Ces investissements reposent sur une doctrine exigeante, des procédures sélectives ouvertes, et des principes de cofinancement ou de retours sur investissement pour l'Etat. Le quatrième PIA (PIA4) est doté de 20 Md€ d'engagements sur la période 2021-2025, dont 11 Md€ contribueront à soutenir des projets innovants dans le cadre du plan France Relance. Le PIA continuera d'accompagner dans la durée l'innovation, sous toutes ses formes, pour que notre pays renforce ses positions dans des secteurs d'avenir, au service de la compétitivité, de la transition écologique, et de l'indépendance de notre économie et de nos organisations. »

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