

DU NUMÉRIQUE

5 juillet 2024





par







Cofinancé par l'Union européenne



Agenda

- Les projets régionaux de cybersécurité ;
- II) Par où commencer?
- III) Que faire en cas d'attaque ?



Présentation de Réunion THD



Les projets régionaux de cybersécurité



La doctrine du « passage à l'échelle »









Le centre de ressources en cybersécurité

Soutenu par









AMI Centre de ressources en cybersécurité OM





Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information Dossier suivi par : 2 1 JUIL. 2022 /ANSSI/DIR/NP

NOTE

destinataires in fine

Objet

: Développement de centres de ressources en cybersécurité en Outre-Mer.

L'ANSSI pilote le volet cybersécurité de France Relance destiné à augmenter le niveau de sécurité numérique des services publics. Dans les territoires útra-marins, et après un travail initial exploratoire informel, le construit et partagé avec vos services de la nécessité de construire des solutions spécifiques, adaptées à l'écosystème local. Celui-ci est en effet souvent faiblement structuré, encore peu sersibilisé à ces problématiques et manquant netterment d'un tissu de

Des centres de ressources dédiés à la cybersécurité, en charge de promouvoir et de diffuser les bonnes pratiques de cybersécurité, de valoriser l'Offre de cybersécurité et de permettre aux utilisateurs d'accèder à des solutions adaptées et disponibles, pourraient répondre aux enjeux de l'écosystème local. Un soutien financier ponctuel via France Relance serait disponible pour la création de ces centres.

1. Le volet cybersécurité de France Relance : contexte et enjeux

France Relance, au travers de son volet cyberrécurité, a pour objectif de développer l'écosystème national de cybersécurité, tout en renforçant la capacité collective française à faire face à une menace cyber en forte croisance. Ces moyers alloués à la cyberrécurité interviennent dans un climat de hausser apide de la menace, pour toutes less eutretures, pobliques ou privées, de toute taille et quelle que soit leur secteur d'activité. La tendre la hausse des attaques, en particulier par rançongiciel, identifiée depois 2018 set confirmée en 2020 et en 2021, tant à l'échelle international que nationale. Les territoires ultra-mairin ne sont pai épagné; et les conséquences socioéconomiques y sont probablement encore plus marquées qu'en métropole, du fait notamment de la pénurie d'expertises locales, en mesure de prévenir et d'agir rapidement lors d'une cyberattaque.

Face à ce constat, l'ANSSI promeut la création d'entités chargées de :

- concentrer l'offre et la demande en matière de cybersécurité pour les stimuler ; fournir du contenu de sensibilisation adapté à l'écosystème ;
- réunir les besoins de formation
- offrir un lieu concentrant la compétence pour y faire émerger des services au profit de tous.

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01.71.75.84.06



13 exécutifs ultra-marins



- 1)Sensibilisation et la formation
- 2)Soutien de projet locaux visant à structurer et développer l'offre et la demande en cybersécurité ;
- 3)Réponse à incident de premier niveau



= 600 K€ / 3 ans pour La Réunion





Réponse à incident

Accompagner les victimes lors d'une cyberattaque et proposer la mise en relation avec des prestataires qualifiés « ExpertCyber »



Veille

Publier des rapports réguliers sur l'état des menaces. Diffuser de bulletins d'alertes sur les vulnérabilités.



Prévention

Identifier les vulnérabilités critiques de manière non intrusive et informer nos bénéficiaires (TPE, PME, ETI, CT et associations).



Coopération

Partager des informations avec le CERT-FR, les CSIRT régionaux et sectoriels, ainsi qu'avec les entreprises et les collectivités territoriales.



Diagnostic

Avec la communauté des aidants, Élaborer gratuitement un diagnostic cyber intégrant 6 recommandations prioritaires.



Evènements

Organiser des webinaires, de salons et de rencontres destinées à dynamiser l'écosystème local.



Sensibilisation

Diffuser les bonnes pratiques à travers des guides, des fiches réflexes, des mises en situation et, à termes, une plateforme de formation en ligne.



Communication

Marquer la présence sur le territoire : Emissions économiques, spots publicitaires, réseaux sociaux, magazines



Le pôle européen d'innovation numérique en cybersécurité





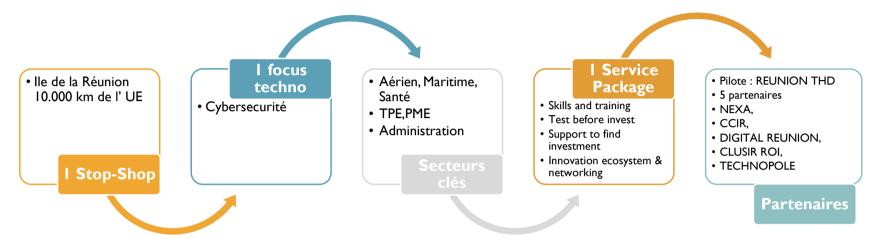


Cofinancé par l'Union européenne





Un pôle européeen d'innovation numérique en cyber



Objectifs principaux:

- I. Améliorer la cybersécurité et la résilience du territoire ;
- 2. Construire et mettre en œuvre des services adaptés aux bénéficiaires ;
- 3. Développer la coopération :
 - régionale avec Mayotte et les Etats voisins ;
 - française et européenne avec les autres EDIHs



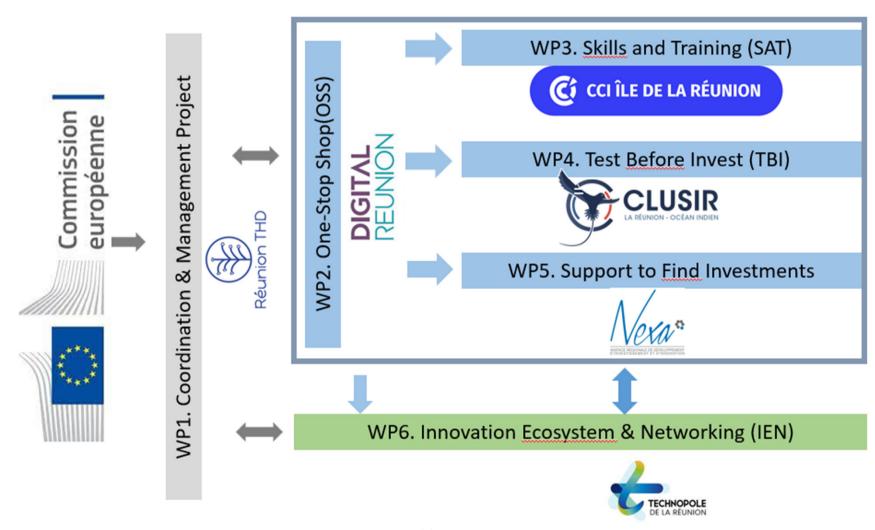
=1,5 M€ / 3 ans par la C.E. / I M€ de contrepartie régionale / 500 K€ Bénéficiaires



us (Le pôle européen d'innov

Structuration et répartition des services





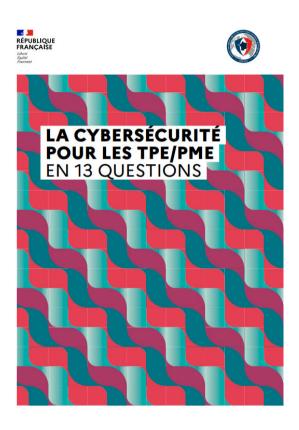
TLP:AMBER

Par où commencer?

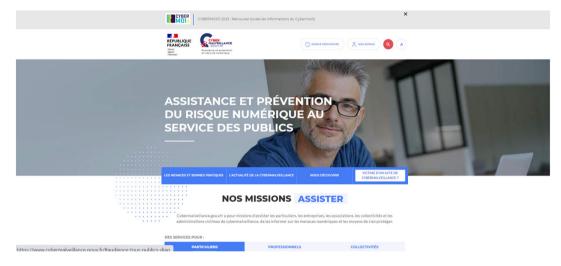


Quelques pistes pour aller plus loin





https://www.ssi.gouv.fr/guide/lacybersecurite-pour-les-tpepme-en-treizequestions/



https://www.cybermalveillance.gouv.fr/



https://secnumacademie.gouv.fr/



Par où commencer?





MonAideCyber met en relation les entités de faible maturité cyber avec des « Aidants » qui réalisent des diagnostics cyber de premier niveau et qui les aiguillent vers les dispositifs complémentaires existants.

Le diagnostic est **gratuit** et oriente sur **6 mesures de sécurité prioritaires** à mener sur les 6 prochains mois.









Que faire en cas d'attaque?



Que faire en cas d'attaque ?

Que faire en cas d'attaque?



CONTACTS UTILES 2



CONSEILS ET ASSISTANCE

Dispositif national de prévention et d'assistance aux victimes de cybermalveillance

www.cybermalveillance.gouv.fr

NOTIFICATION DE VIOLATION DE **DONNÉES PERSONNELLES**

Commission nationale informatique et liberté (CNIL)

www.cnil.fr/fr/notifier-une-violationde-donnees-personnelles

POLICE, **GENDARMERIE**

17











cyber@reunionthd.re







par







Cofinancé par l'Union européenne