CYBER RÉUNION

CSIRT LA RÉUNION | COMPUTER SECURITY INCIDENT RESPONSE TEAM

EDIH LA RÉUNION | EUROPEAN DIGITAL INNOVATION HUB

Dossier de presse

Lancement de CYBER RÉUNION

CSIRT La Réunion
EDIH La Réunion

Version 1.1

Immeuble Emile Hugot
1 rue Emile Hugot
97490 Sainte-Clotilde - La Réunion

SOMMAIRE

Le mot du président

Normane Omarjee

Chères Réunionnaises, chers Réunionnais,

Dans un monde de plus en plus interconnecté, dont dépend grandement La Réunion, la cybersécurité est devenue un enjeu majeur pour les entreprises, les institutions et les familles. Face à la montée des menaces sur les réseaux, du simple phishing à des attaques plus poussées contre notre hôpital ou nos grandes entreprises, il est aujourd'hui essentiel de protéger nos infrastructures et nos données. Il en va de notre confiance face à une digitalisation croissante des services.

C'est dans ce contexte que nous avons l'honneur de lancer CYBER RÉUNION, portée par Réunion THD.

CYBER RÉUNION est avant tout une innovation collective adaptée à nos spécificités. Ce partenariat entre l'État et la Région rassemble les compétences et les ressources de notre territoire réunionnais. C'est une marque gage de qualité et de fiabilité qui vise à sécuriser l'ensemble des acteurs de notre écosystème numérique. Elle s'inscrit dans notre ambition régionale de sécuriser notre désenclavement numérique.

Nous sommes convaincus que la souveraineté numérique passe par la maîtrise et la protection de nos infrastructures et de nos données. CYBER RÉUNION offrira des services et des outils adaptés aux réalités locales, celle d'une île aux usages numériques poussés mais que nous voulons inscrits dans la durabilité de notre île. À travers cette initiative, nous souhaitons développer une culture locale de la cybersécurité, alignée avec les standards internationaux les plus rigoureux en sensibilisant et en formant nos concitoyens, dont notre jeunesse, et nos entreprises aux bonnes pratiques.

Enfin, CYBER RÉUNION pourra s'appuyer sur un tissu local riche et pluriel où chaque acteur, public comme privé, peut jouer un rôle pour protéger notre territoire. En unissant nos forces et nos expertises, nous pouvons continuer à construire un écosystème numérique résilient, au service des Réunionnaises et Réunionnais.

Je vous remercie de soutenir cette initiative qui marquera un tournant pour la sécurité et l'inclusion numérique de notre île.

Ensemble, faisons de La Réunion ce territoire numérique d'avenir et de confiance pour toutes et tous.

Normane OMARJEE
Président de Réunion THD
3e Vice-Président de la Région Réunion

INTRODUCTION :

Une Stratégie Nationale pour Renforcer la Cybersécurité Régionale

Lancée en février 2021, la stratégie française de cybersécurité vise à tripler le chiffre d'affaires de la filière cyber et à créer 37 000 emplois d'ici 2025, renforçant ainsi la souveraineté numérique nationale. En son cœur, la création de centres régionaux de réponse aux incidents informatiques (CSIRT) apporte des solutions locales face aux cybermenaces croissantes, notamment pour les PME, collectivités, et associations qui composent le tissu économique régional. Soutenus par l'ANSSI dans le cadre de France Relance, les CSIRT offrent une assistance en cas d'attaques et promeuvent les bonnes pratiques de cybersécurité.

En 2022, douze CSIRT hexagonaux ont été opérationnalisés, formant un réseau essentiel pour encourager la coopération locale, soutenir l'innovation cyber et former les talents de demain. Ces actions s'inscrivent dans un objectif global : faire de la France un leader européen de la cybersécurité, en réponse aux défis numériques d'aujourd'hui et de demain.

Cybersécurité à La Réunion : une mobilisation nécessaire pour un territoire résilient

Face à l'explosion des cyberattaques mondiales, La Réunion se trouve particulièrement exposée, notamment en raison de son statut économique attractif dans l'océan Indien. Les entreprises, associations et administrations locales sont de plus en plus ciblées par des cybercriminels cherchant à voler des données ou à paralyser les activités via des rançongiciels. La dématérialisation rapide des services, accentuée par la crise sanitaire, a parfois laissé la cybersécurité en retrait, augmentant, comme partout, la vulnérabilité de l'île face aux menaces.

Dans les territoires ultramarins, il est crucial d'adopter une approche adaptée aux spécificités locales. Les écosystèmes numériques y sont souvent moins structurés, moins sensibilisés aux risques et disposent de moins de prestataires spécialisés en cybersécurité. Ces défis imposent de mettre en place des solutions sur mesure pour renforcer la protection des systèmes d'information et accroître la résilience face aux menaces numériques.

Les méthodes d'attaque évoluent constamment, avec une intensification du vol de données et de la pression exercée sur les entreprises. La démocratisation des outils de cyberattaque permet même à des acteurs novices de lancer des offensives, accentuant le risque.

Pour contrer cette menace, il est essentiel de renforcer les mesures de protection et de sensibilisation. Réunion THD joue un rôle central dans cette dynamique, allant au-delà de la réponse aux incidents en accompagnant les acteurs locaux, en favorisant les bonnes pratiques et en soutenant l'innovation cyber. Ces efforts visent à construire un écosystème numérique résilient, contribuant à la sécurité et au développement économique de La Réunion.

Réunion THD, qui sommes-nous ?

Établissement public de la Région Réunion en charge des projets d'aménagement et de développement **numérique**.

Réunion THD a été créée en 2018 par la Région Réunion pour accélérer le déploiement de la fibre optique sur l'île, notamment dans les zones non couvertes par les opérateurs privés. Une mission dont l'objectif était de répondre aux enjeux de désenclavement numérique de La Réunion, par une équité d'accès au très haut débit, et en favorisant le développement des meilleurs services numériques partout et pour tous les réunionnais.

Sous l'impulsion de son Président Normane Omarjee, Réunion THD déploie non seulement les infrastructures numériques permettant à chaque réunionnais de bénéficier d'un service de qualité, mais participe également au développement des évolutions technologiques nécessaires au développement du territoire.

Traduction de la volonté politique régionale, Réunion THD porte des missions relatives à **l'aménagement** et au **développement numérique** de notre territoire, et à sa résilience, avec pour ambition :

- **De favoriser l'inclusion numérique de l'île** en permettant une égalité d'accès à tous les réunionnais, et une qualité de prestation identique à celle de la métropole ;

  A ce titre La Réunion peut s'enorgueillir de faire partie des trois régions les mieux fibrées de France *Source ARCEP T2 2024*.

- Gestion du **Réseau Gazelle**, l'autoroute locale créée à l'initiative de la Région Réunion dès 2008 afin de desservir les 24 communes de l'île.
- Construction du RIP – **Réseaux d'Initiative Publique** – de la fibre optique sur les zones non couvertes par les opérateurs privés, afin d'assurer une équité et une même qualité d'accès au numérique pour tous les réunionnais.

- **D'accompagner l'élévation régionale du niveau de maturité cyber et de proposer des services adaptés aux enjeux du territoire**

- Création d'un **CSIRT La Réunion** – Computer Security Incident Response Team-, centre de réponses aux incidents cyber.
- Coordination de l' **EDIH La Réunion** – European Digital Innovation Hub -, un parcours de cyber-sécurisation opéré par un consortium de 6 partenaires locaux.

CYBER RÉUNION

La marque régionale de cybersécurité.

Une marque régionale comme repère pour une identification forte

Naviguer dans l'offre de cybersécurité peut s'avérer complexe, en particulier pour les néophytes, car il s'agit d'un domaine technique souvent difficile à appréhender. En cas de cyberattaque, il est crucial de connaître les premiers gestes à adopter et de savoir vers qui se tourner pour une résolution rapide et efficace.

Pour répondre à ce besoin, Réunion THD a lancé "CYBER RÉUNION", la marque régionale dédiée à la cybersécurité. Cette initiative vise à fournir un point de contact et de référence fiable pour les acteurs locaux, leur permettant de trouver les bonnes ressources et les services adaptés à leurs besoins en matière de cybersécurité.

En tant que marque publique, CYBER RÉUNION opère en toute légitimité et en étroite collaboration avec les institutions, garantissant ainsi une approche neutre et impartiale pour l'ensemble des bénéficiaires de ses services.

Sa mission : élever les niveaux de cybersécurité et de cyber résilience du territoire.

Les valeurs qui nous animent et se traduisent dans chacune de nos actions :

- **PROXIMITE** : Offrir une réponse personnalisée aux besoins en cybersécurité de nos bénéficiaires, en collaboration étroite avec toutes les parties prenantes pour assurer un accompagnement adapté ;
- **CO-CONSTRUCTION** : Travailler de manière concertée avec nos partenaires pour renforcer le niveau de maturité de l'écosystème local et promouvoir des solutions de cybersécurité efficaces et durables ;
- **RESILIENCE** : en déployant des capacités techniques et organisationnelles visant à renforcer les défenses du territoire.
- **EXCELLENCE** : par le développement des compétences permettant d'atteindre les meilleurs standards de sécurité dans toutes les initiatives cyber.

Faire de La Réunion un pôle de référence en cybersécurité et en confiance numérique dans l'Océan Indien, tout en constituant une véritable opportunité pour le développement du territoire.

NOS MISSIONS

Informer
Sur les risques et les menaces

Sécuriser
Les entreprises et organisations

Répondre
Aux incidents d'origine cyber

1. Le CSIRT La Réunion (Computer Security Incident Response Team) a pour mission de renforcer activement la sécurité numérique du territoire. Il offre une réponse de proximité et un accompagnement humain en cas de crise, en répondant aux demandes d'assistance des acteurs locaux grâce à une compréhension approfondie du tissu régional. C'est un projet ambitieux, mais essentiel, pour bâtir une Réunion plus forte et résiliente.

CSIRT LA RÉUNION | COMPUTER SECURITY INCIDENT RESPONSE TEAM

2. En parallèle de cette initiative, Réunion THD coordonne l'EDIH (European Digital Innovation Hub) La Réunion. Ce pôle européen d'innovation numérique représente une démarche innovante permettant de financer la mise en place de dispositifs de sécurisation des systèmes d'information des TPE, PME et organismes publics réunionnais. Il favorise la mise en commun des ressources et des expertises de six partenaires : Réunion THD, DIGITAL REUNION, la Chambre de Commerce et d'Industrie de La Réunion (CCIR), le Club de la Sécurité de l'Information en Réseau – Réunion Océan Indien (CLUSIR ROI), La Réunion Développement, et la Technopole de La Réunion.

EDIH LA RÉUNION | EUROPEAN DIGITAL INNOVATION HUB

CYBER RÉUNION

CSIRT LA RÉUNION | COMPUTER SECURITY INCIDENT RESPONSE TEAM

Opéré par CYBER RÉUNION

Soutenu par l'ANSSI

Le centre de réponse aux incidents reçoit les demandes d'assistance provenant des TPE/PME, ETI, organismes publics et associations victime d'une crise d'origine cyber.

Premiers Conseils | Accompagnement pour les formalités réglementaire et la judiciarisation | Mise en relation avec des prestataires référencés | Veille sur les failles de sécurité Production de rapports sur l'état de la menace

Financé par l'État et la Région Réunion.

EDIH LA RÉUNION | EUROPEAN DIGITAL INNOVATION HUB

Coordonné par CYBER RÉUNION

Opéré par un consortium

Accompagne et cofinance les entreprises et administrations publiques dans l'adoption des technologies numériques avancées.

Conseils | Formations | Tests de nouvelles technologies pour stimuler l'innovation et la compétitivité | Accompagnement dans la recherche de financement.

Financé par l'Europe et la Région Réunion

Le centre de réponse aux incidents cyber

CSIRT La Réunion

Le **CSIRT La Réunion** a pour mission réactive d'apporter une réponse rapide et adaptée face aux incidents de sécurité informatique. Il doit également contribuer activement à l'élévation de maturité du territoire au travers d'actions de sensibilisation et de soutien aux projets locaux de cybersécurité.

Les bénéficiaires cibles du CSIRT La Réunion

Les bénéficiaires cibles des services du CSIRT La Réunion sont les :

- Très petites entreprises (TPE) : Vulnérables, avec peu de ressources pour la cybersécurité ;
- Petites et moyennes entreprises (PME) : Plus structurées mais parfois limitées pour protéger leurs systèmes ;
- Entreprises de taille intermédiaire (ETI) : En croissance, avec des SI complexes à sécuriser ;
- Associations : Moins sensibilisées, souvent ciblées par les cybercriminels ;
- Organismes publics : Exposés aux enjeux de protection des données sensibles.

Activités du CSIRT La Réunion

Le CSIRT La Réunion offre un **service réactif** pour **accompagner les victimes de cyberattaques**, accessible au **0262 974 999**, du lundi au vendredi de 9h à 12h et de 13h à17h. Il accueille les victimes, recueille les informations clés, et leur prodigue des conseils pratiques pour réagir rapidement. L'incident est ensuite analysé pour en évaluer l'ampleur. Lorsque nécessaire, il aide les victimes à entamer des démarches judiciaires et réglementaires, notamment auprès de la CNIL, et les met en relation avec des experts qualifiés. Il assure un suivi régulier jusqu'à la résolution complète de l'incident, garantissant un soutien constant et sécurisé.

Le CSIRT La Réunion déploie également des **services proactifs** parmi lesquels :

- **Service de gestion de la surface d'attaque** : Surveille en continu les adresses IP et URLs réunionnaises pour détecter les vulnérabilités critiques. En cas de faille majeure, le propriétaire de l'actif reçoit une notification sécurisée avec les risques et les actions correctives à entreprendre, permettant une réduction proactive des risques pour les acteurs locaux ;

- **Service de diagnostic de cybersécurité** : Basé sur MonAideCyber, ce service évalue les vulnérabilités des systèmes d'information à l'aide d'un questionnaire adapté à chaque organisation. Un rapport personnalisé, incluant les principaux risques et recommandations, est ensuite remis aux acteurs locaux pour renforcer leur sécurité numérique.

- **Service de rapports sur l'état de la menace** : Fournit une vue actualisée des cyber-risques en analysant les tendances, menaces émergentes et incidents récents touchant La Réunion et à l'international.

Un parcours de sécurisation simple et efficace

EDIH La Réunion

Dans le cadre du programme européen DIGITAL EUROPE 2021-2027[1], la Commission européenne déploie un réseau de Pôles Européens d'Innovation Numérique (EDIH) pour accélérer la transformation numérique des économies locales et renforcer la résilience.

Sous l'impulsion de la Région Réunion, l'EDIH La Réunion a été conçu autour de la cybersécurité, complétant ainsi les services du CSIRT local pour offrir un parcours structuré et adapté de sécurisation numérique.

Cette initiative permet aux entreprises et administrations réunionnaises de tester des technologies de sécurisation avancées avant leur adoption, tout en facilitant leur accès à des financements.

Seul EDIH d'Outre-Mer français, il bénéficie de synergies étroites avec d'autres hubs européens, permettant un échange de savoir-faire et des collaborations transnationales pour répondre aux enjeux de souveraineté numérique, dans une approche durable et centrée sur l'humain.

Les bénéficiaires cibles de l'EDIH La Réunion

Les bénéficiaires de l'EDIH La Réunion sont les TPE, PME, ETI et organismes publics, particulièrement vulnérables aux risques cyber.

Tous les secteurs d'activité sont concernés, avec une attention accrue pour les sous-traitants des grands opérateurs portuaires et aéroportuaires ainsi que pour les collectivités territoriales n'ayant pas suivi le parcours de cybersécurité déployé par l'ANSSI.

Activités de L'EDIH La Réunion :

L'EDIH La Réunion est un dispositif public opéré par un consortium et piloté par Réunion THD qui soutient ses bénéficiaires face aux cybermenaces et aux risques cyber. Il offre un parcours d'accompagnement complet, allant du diagnostic au cofinancement de mesures de sécurité techniques et organisationnelles adaptées. Il permet notamment :

- D'évaluer les risques grâce à un diagnostic dédié ;
- De préconiser des mesures adaptées ;
- De sélectionner des prestataires locaux compétents pour la mise en œuvre des mesures de sécurité ;
- De co-financer les mesures retenues à hauteur de 65% via les fonds de la Commission Européenne et de la Région Réunion ;
- De suivre et de mesurer l'impact des actions dans le temps ;
- De faciliter l'accès à d'autres aides pour consolider et pérenniser le niveau de cybersécurité des bénéficiaires.

[1] https://digital-strategy.ec.europa.eu/fr/activities/digital-programme

Les acteurs du consortium

- **Réunion THD :** Réunion THD[2] est un établissement public créé par la Région Réunion pour répondre aux enjeux de désenclavement numérique de La Réunion, permettre une équité d'accès au très haut débit, et favoriser le développement des meilleurs services numériques partout et pour tous les Réunionnais. Réunion THD a été mandaté par la Région Réunion pour porter les projets régionaux de cybersécurité. Réunion THD coordonne le consortium du projet EDIH La Réunion.

- **DIGITAL REUNION :** Le cluster DIGITAL REUNION[3], ex-association ARTIC, a été créée en 1997 à la demande des professionnels de la filière numérique réunionnaise. Elle réunit les principaux acteurs du marché intervenant directement et indirectement dans le secteur du numérique pour participer à la création de conditions économiques, législatives et concurrentielles indispensables au bon développement de la filière.

- **Chambre de Commerce et d'Industrie (CCI) de La Réunion :** La CCI de La Réunion[4] est un établissement public de l'Etat, placé sous la tutelle du ministère de l'économie et des finances. En sa qualité de corps intermédiaire de l'Etat, la CCI de La Réunion assure une fonction de représentation des intérêts du commerce, de l'industrie et des services auprès des pouvoirs publics. Elle contribue au développement économique, à l'attractivité, à l'aménagement du territoire et au soutien des entreprises. Gérée par des entrepreneurs, la CCI est en prise directe avec les besoins des entreprises.

- **Club de la Sécurité de l'Information en Réseau – La Réunion Océan Indien (CLUSIR ROI) :** Le CLUSIR - ROI[5] est une association régionale décentralisée liée au CLUSIF par une convention. Elle forme un réseau œuvrant pour promouvoir des bonnes pratiques afin d'améliorer la protection de l'information, aider les professionnels de la sécurité, leurs dirigeants et les entreprises elles-mêmes à améliorer leur niveau de protection et anticiper les nouvelles menaces qui pèsent sur leurs systèmes d'information.

- **La Réunion Développement :** Au service de l'économie réunionnaise, « La Réunion Développement » (anciennement Nexa[6]) insuffle un élan favorisant la transformation économique de La Réunion et accompagne l'ensemble du territoire dans cette évolution. Porte d'entrée de tous les projets à La Réunion, l'agence régionale de développement vous propose en une seule structure toute une palette de services transversaux, destinés à répondre aux besoins de publics diversifiés.

- **La Technopole de La Réunion :** La Technopole de La Réunion[7] est une association née en 2001, de la volonté commune des Institutions Publiques, des acteurs de la Recherche et de la Formation supérieure et du monde de l'Entreprise pour créer un outil de développement économique et social du territoire par l'innovation. Elle accompagne la création et l'accélération du développement des entreprises, soutient les acteurs économiques du territoire et promeut une Réunion technologique et innovante.

---

[2] https://reunionthd.re/
[3] https://digitalreunion.com/
[4] https://reunion.cci.fr/
[5] https://clusir-roi.org/
[6] http://www.nexa.re/accueil/
[7] https://www.technopole-reunion.com/

Financement et réseaux

A propos du CSIRT La Réunion

Le déploiement du **CSIRT La Réunion** s'inscrit dans le cadre :

- De la mise en œuvre de la réponse de La Région Réunion à l'appel à projet de l'ANSSI pour développer des centres de ressources en cybersécurité en Outre-Mer ;
- L'axe 3 « Un numérique pour un territoire résilient » de la Stratégie Régionale Numérique de la Région Réunion.

Ce projet bénéficie d'un financement de 1,2 million d'euros réparti sur trois ans, financé à 50 % par l'ANSSI et à 50 % par la Région Réunion.

Soutenu par

Dans l'objectif de renforcer la résilience collective face aux cybermenaces, **le CSIRT La Réunion** travaille en étroite collaboration avec l'écosystème cyber territorial, incluant les offreurs et utilisateurs de solutions et prestations de cybersécurité, les associations et les forces de sécurité intérieure. Face à une menace mondiale et sans frontières, le **CSIRT La Réunion** collabore également activement avec le CERT-FR[8], le réseau des CSIRTs territoriaux[9] et les CSIRTs sectoriels.

A propos de l'EDIH La Réunion

Le déploiement de **l'EDIH La Réunion** s'inscrit dans le cadre de la réponse du consortium réunionnais porté par Région Réunion à l'appel à projets de la Commission européenne, qui visait à soutenir la transformation numérique des entreprises et des administrations publiques par l'adoption de technologies avancées telles que l'intelligence artificielle, la cybersécurité et le calcul haute performance.

Ce projet bénéficie d'un financement total de 2,5 millions d'euros sur trois ans, avec une contribution de 1,5 million d'euros de la Commission Européenne et 1 million d'euros de la Région Réunion.

Soutenu par

L'EDIH La Réunion collabore activement avec le réseau French Corridor des EDIH français, notamment au sein du groupe de travail dédié à la cybersécurité, et contribue aux initiatives de l'European Cyber Security Organisation[10] (ECSO). Il s'appuie également sur le réseau européen des European Digital Innovation Hubs (plus de 150 EDIH[11]) pour accompagner les entreprises et promouvoir les compétences de l'écosystème réunionnais à l'international.

---

[8] https://www.cert.ssi.gouv.fr/
[9] https://cyber.gouv.fr/csirt-territoriaux-un-reseau-essentiel-face-aux-cybermenaces
[10] https://ecs-org.eu/
[11] https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue

Lexique

Qu'est-ce que la Cybersécurité ?

La **Cybersécurité** c'est l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les systèmes d'information contre les accès non autorisés, les attaques, les pertes de données et les dommages. Elle englobe la prévention, la détection et la réponse aux incidents pour assurer la confidentialité, l'intégrité et la disponibilité des informations, tout en renforçant la résilience des infrastructures numériques face aux menaces.

Qu'est-ce que l'ANSSI ?

L'Agence Nationale de la Sécurité des Systèmes d'Information[12] (ANSSI) est l'autorité nationale en matière de cybersécurité. Placée sous l'autorité du Premier ministre et rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), elle bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle. Cette politique s'attache à défendre les infrastructures numériques publiques et privées les plus critiques. L'ANSSI s'adresse également à l'ensemble des acteurs de la transformation numérique du pays et favorise les conditions d'un dialogue de confiance avec ses homologues à l'échelle européenne et internationale.

Qu'est-ce que Cybermalveillance ?

Cybermalveillance.gouv.fr[13] est la plateforme du dispositif national de prévention et d'assistance aux victimes de cybermalveillance en France. Lancée en 2017, elle a pour mission d'informer, de sensibiliser et de guider les victimes potentielles ou avérées de cyberattaques, qu'il s'agisse de particuliers, de très petites entreprises (TPE), de petites et moyennes entreprises (PME), de collectivités, ou d'associations. La plateforme fournit des conseils pratiques, des ressources pédagogiques et des solutions concrètes pour faire face aux cybermenaces, en réduisant les risques et en limitant les dommages causés par des attaques comme le phishing, les rançongiciels ou les piratages de compte.

Le recours à la plateforme est entièrement automatisé : les utilisateurs y trouvent des informations et des outils en libre accès pour diagnostiquer leurs problèmes de cybersécurité et trouver des solutions, mais il n'est pas possible d'interagir de vive voix avec un conseiller humain.

Qu'est-ce que le CERT-FR ?

Le CERT-FR[14] **(Computer Emergency Response Team – France)** est le Centre National de Réponse aux Incidents de Cybersécurité du gouvernement français, chargé de traiter techniquement les incidents de cybersécurité à l'échelle nationale. Placé sous la responsabilité de la Sous-Direction des Opérations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le CERT-FR coordonne les réponses aux incidents critiques et veille à la résilience des infrastructures essentielles du pays. Les principaux bénéficiaires des actions du CERT-FR sont :

- **Les organismes publics** : ministères, institutions, autorités indépendantes, juridictions et collectivités territoriales ;
- **Les opérateurs d'importance vitale (OIV)** : acteurs publics et privés exploitant des infrastructures indispensables à la sécurité et à la continuité de la nation ;

[12] https://cyber.gouv.fr/
[13] https://www.cybermalveillance.gouv.fr/
[14] https://www.cert.ssi.gouv.fr/

- **Les opérateurs de services essentiels (OSE)** : organisations dont les services, reposant sur des systèmes d'information, sont cruciaux pour l'économie ou la société et dont l'interruption aurait un impact significatif.

Bien que le CERT-FR partage via son site des informations utiles à tous, comme des listes de vulnérabilités et des rapports sur l'état des menaces, il n'a pas vocation à intervenir directement auprès des particuliers, des très petites entreprises (TPE) et des petites et moyennes entreprises (PME).

Qu'est-ce qu'un CSIRT sectoriel ?

Un **CSIRT (Computer Security Incident Response Team) sectoriel** est une équipe dédiée à la réponse aux incidents de sécurité informatique pour un secteur d'activité spécifique, tel que la santé, l'énergie, ou les transports. Sa mission consiste à traiter et à coordonner la réponse aux incidents de cybersécurité au sein de son secteur, à fournir des conseils sur les bonnes pratiques de sécurité, et à partager des informations sur les menaces avec les acteurs concernés.

Qu'est-ce qu'un CSIRT territorial/régional ?

Un **CSIRT (Computer Security Incident Response Team) territorial/régional**[15] est une équipe dédiée à la réponse aux incidents de cybersécurité pour une région spécifique. Leur mission inclut la préparation, la détection, et la réponse aux incidents, ainsi que la sensibilisation et le partage d'informations sur les menaces. En renforçant la résilience régionale, ces CSIRT contribuent à la sécurité globale face aux cybermenaces sur l'ensemble du territoire.

Qu'est-ce qu'un EDIH ?

Un **EDIH**[16] **(European Digital Innovation Hub)** est un pôle européen d'innovation numérique (EDIH) qui se matérialise par un guichet unique qui aide les entreprises et les organisations du secteur public à relever les défis numériques.
Un EDIH combine les avantages d'une présence régionale avec les possibilités offertes à un réseau paneuropéen. La couverture européenne du réseau facilite l'échange de bonnes pratiques entre les pôles de différents pays ainsi que la fourniture de services spécialisés entre les régions lorsque les compétences requises ne sont pas disponibles localement.

Qu'est-ce que « MonAideCyber » ?

MonAideCyber[17] est un dispositif national développé par l'ANSSI pour encourager les TPE, PME, associations et collectivités à agir face aux menaces cyber. Cet outil gratuit offre un diagnostic de vulnérabilité de leur système d'information, suivi de recommandations prioritaires pour renforcer leur sécurité. L'objectif est de sensibiliser ces entités aux risques et de les guider vers une maturité accrue en cybersécurité, en leur donnant les moyens de prendre les premières mesures essentielles pour protéger leurs données et systèmes contre les cyberattaques.

Qu'est-ce qu'une vulnérabilité ?

Une **vulnérabilité** est une faiblesse ou une faille dans un système informatique, un logiciel, ou une configuration, qui peut être exploitée par des cybercriminels pour accéder à des informations sensibles ou perturber le fonctionnement du système.

---

[15] https://www.cert.ssi.gouv.fr/csirt/csirt-territoriaux/
[16] https://digital-strategy.ec.europa.eu/fr/activities/edihs
[17] https://www.monaidecyber.ssi.gouv.fr/

Contacts Presse:

lfontaine@runconcept.com
06 92 61 22 62

muriel.thierry@reunionthd.re
06 92 64 36 81

www.cyber-reunion.fr

Un incident d'origine cyber ?
Contactez-nous

0262 974 999