RAPPORT D'ACTIVITE DES CSIRT TERRITORIAUX

2025

CYBER CORSICA CSIRT

AGENCE CARIBÉENNE POUR LA CYBERSÉCURITÉ ACCYB

CSIRT BOURGOGNE-FRANCHE-COMTÉ

CYBER ASSISTANCE PAYS DE LA LOIRE

Urgence Cyber îledeFrance
Centre de réponse aux cyberattaques

CYBER'OCC
LE CENTRE CYBERSÉCURITÉ EN OCCITANIE

NORMANDIE CYBER

CRIC-NA
centre de réponse aux incidents cyber
Nouvelle-Aquitaine

CSIRT LA RÉUNION
COMPUTER SECURITY INCIDENT RESPONSE TEAM

LE CENTRE D'ASSISTANCE
Grand Est Cybersécurité

cybeRéponse
CENTRE-VAL DE LOIRE

Urgence Cyber
région Sud

CENTRE CYBER
DU PACIFIQUE

CSIRT
HAUTS-DE-FRANCE

Région Bretagne | Breizh Cyber

EDITO

VINCENT STRUBEL

DIRECTEUR GENERAL DE L'ANSSI

Les constats présentés lors du précédent rapport d'activité des CSIRT territoriaux se confirment : la menace cybercriminelle se maintient à un niveau élevé et touche une large variété de victimes. La plupart des attaques sont opportunistes, peu coûteuses en temps et ressources, avec une finalité lucrative.

Elles sont néanmoins capables d'ébranler TPE, PME, ETI, associations et collectivités dans les territoires. D'autres attaques peuvent avoir pour fin de déstabiliser ou d'espionner. Quelle que soit la finalité de l'attaque, les groupes malveillants s'adaptent constamment aux outils technologiques disponibles.

En ce sens, le panorama de la menace de l'ANSSI pour l'année 2025 relève entre autres évolutions que l'utilisation de capacités issues des technologies de l'intelligence artificielle permet également aux attaquants d'améliorer la quantité, la diversité et l'efficacité de leurs attaques. Si les acteurs malveillants s'adaptent, la communauté de la réponse à incident continue d'évoluer et de s'organiser pour faire face.

Présentée par le Gouvernement en janvier 2025, la Stratégie nationale de cybersécurité pour 2026-2030, dans son objectif n°6, vise à faciliter le parcours des organisations et des individus vers une meilleure cybersécurité.

Afin d'atteindre cet objectif, le rôle des CSIRT territoriaux est indispensable : ils sont le maillon local de la valorisation de l'offre de services et des produits de cybersécurité accessibles et adaptés aux acteurs dans les territoires.

Les CSIRT territoriaux participent à l'élévation du niveau général de cybersécurité au profit des entités les plus vulnérables aux cyberattaques.

Grâce à leurs actions de sensibilisation, de réponse à incident et de mise en relation avec des prestataires, ils concourent au renforcement du dispositif national d'accompagnement de proximité.

Cet accompagnement de terrain leur permet d'être un appui du CERT-FR, centre de réponse à incident de cybersécurité national porté par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), au plus près de plusieurs centaines de bénéficiaires, s'adaptant concrètement à leurs réalités. Par leur intermédiaire, l'accompagnement cyber de proximité devient encore plus tangible.

Afin de faciliter et de simplifier les parcours d'assistance, les CSIRT territoriaux s'intègrent également au dispositif 17Cyber porté par le groupement d'intérêt public Action contre la cybermalveillance.

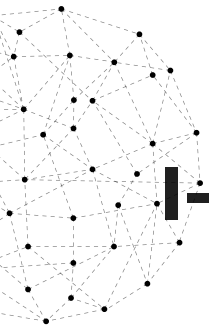
Aux côtés des forces de sécurité intérieure, du CERT-FR et de prestataires privés, cette plateforme d'assistance cyber permet de joindre les centres de réponse à incident de la majorité, et bientôt de la totalité, des territoires et régions de France.

Cette intégration souligne l'effort de cohérence des dispositifs nationaux et territoriaux de cybersécurité, afin de permettre un accompagnement fluide et adapté à la nature de chaque victime. Cet effort de cohérence est d'autant plus crucial dans la perspective du déploiement de la directive européenne sur la sécurité des réseaux et des systèmes d'information, dite « NIS 2 ».

Dans ce cadre, les CSIRT territoriaux demeurent des partenaires privilégiés de l'ANSSI et participent directement à la résilience numérique de notre Nation.

Table des matières

Table des matières



I- INTRODUCTION

Face à une menace cyber en forte progression, ciblant l'ensemble du tissu économique et social et profitant de la vulnérabilité des systèmes d'Informations (SI), l'ANSSI [1] soutient depuis 2021 la mise en place de CSIRT *(Computer Security Incident Response Team)* aux niveaux ministériel, sectoriel et territorial [2] afin d'apporter une réponse concrète et coordonnée aux organisations en cas d'incident. Elle facilite également leur montée en maturité cyber et les accompagnent dans la perspective du passage à l'échelle induit par la directive européenne NIS 2 *(Network and Information System Security)*.

Ces CSIRT participent à renforcer les actions de prévention, de détection et d'assistance dans les territoires, les secteurs et les ministères.

Les CSIRT territoriaux, se positionnent en acteurs centraux de la cybersécurité opérationnelle locale. Ils fournissent un service de réponse à incident de premier niveau et mettent en relation les victimes avec des partenaires de proximité tels que des prestataires de réponse à incident et des partenaires étatiques.

II -GOUVERNANCE ET COORDINATION

A- Présentation des CSIRT Territoriaux

1- Origine et Historique

Au sortir du confinement en 2020, la société française se retrouve confrontée à une explosion des cyberattaques, paralysant des hôpitaux et des villes. Tout le monde se souvient de la panne des services de la ville de Marseille qui avait entraîné un arrêt de la remontée des données d'état-civil à l'INSEE : en pleine crise du Covid, aucun mort n'était plus dénombré à Marseille, alimentant alors de folles rumeurs.[3]

L'État déploie alors le plan France Relance [4], doté d'une enveloppe de 100 milliards d'euros pour accélérer la reprise économique post-Covid. Ce plan comporte un volet cybersécurité, doté d'un fonds de 136 millions d'euros, dont le pilotage est confié à l'ANSSI pour renforcer la sécurité des administrations, des collectivités, des établissements de santé et des organismes publics tout en dynamisant l'écosystème industriel français. Un des projets est de soutenir la création de CSIRT territoriaux par les Régions en leur fournissant un accompagnement financier et méthodologique à la création d'équipes de réponse à des incidents cyber (CSIRT). Les Régions s'emparent du sujet, conscientes de l'urgence et du risque pour leur territoire.

Chacune y a répondu avec ses outils et en fonction de son écosystème.

En 2021, la France lance la stratégie nationale Cyber [5] qui s'inscrit désormais dans le plan France Relance 2030 : favoriser la relation entre les acteurs avec un focus sur le Campus Cyber national, favoriser l'innovation, renforcer la cybersécurité des administrations et des collectivités, former les talents cyber de demain.

2- Les missions des CSIRT Territoriaux

Issus d'un projet du plan France Relance de 2020, les CSIRT Territoriaux sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires [6].

Le cahier des charges des CSIRT prévoit une liste de missions essentielles [6] formant une base de services communs à chaque CSIRT.

Chaque CSIRT a développé d'autres services en fonction des besoins de son territoire et du développement de son écosystème cyber.

Les CSIRT portent des missions de **prévention**, d'**information**, de **sensibilisation** et d'**accompagnement** et de **conseil** dans la montée en maturité des acteurs de leurs régions, qu'il s'agisse de collectivités territoriales, d'associations, de TPE/PME ou d'ETI.

Ils offrent notamment une réponse de premier niveau aux incidents d'origine cyber et surtout une réponse humaine et de proximité.
Leurs objectifs sont de renforcer le niveau de résilience cyber au plus proche de leurs territoires et de favoriser la mise en relation entre les prestataires et les utilisateurs de cybersécurité. Ils ont un vrai rôle de relais à la fois auprès du secteur privé mais aussi auprès des partenaires étatiques.

Les CSIRT territoriaux sont tous construits au service de leurs bénéficiaires, en prenant en compte les spécificités de leurs territoires comme la volumétrie, les compétences et profils de leurs bénéficiaires et prestataires locaux.

Déroulement d'une assistance par un CSIRT territorial :

Mise en relation* entre le CSIRT et une victime (appel de la victime, mail...)**

Déclenchement :
Collecte des faits et des symptômes dont la victime a connaissance

Qualification :
Identification du type d'incident et définition de la réponse à apporter

Mise en oeuvre de la réponse :
- Information sur les premiers gestes de sécurité et investigations supplémentaires à mener
- Mise en relation avec des prestataires suivant le contexte
- Information sur les droits et obligations légales

Clôture de l'assistance :
- Constatation d'un retour à la normal
- Bilan et recommandations d'améliorations de la posture de sécurité

**Mise en relation plus difficile quand le déclenchement est à l'initiative du CSIRT suite à un signalement du CERT-FR*

***Les particuliers sont redirigés vers le 17Cyber*

3- Spécificité et Structuration par région

Chaque CSIRT s'est créé en fonction de son territoire, des projets déjà en place et des ressources régionales. Au vu de l'augmentation de la menace, la quasi totalité des Régions françaises ont inscrit la cybersécurité comme un axe fort dans leur stratégie numérique.

En plus des missions d'information, de sensibilisation et d'accompagnement en cas d'incident cyber, les CSIRT ont pu développer d'autres services, liés à leur territoire et à leur structuration. Ils peuvent être internes à un Campus Cyber Territorial ou indépendants et partenaires, intégrés dans un consortium national ou européen...

Présentation des CSIRT Territoriaux dans l'ordre chronologique d'ouverture :

16/05/2022

Campus Normandie Cyber [7]

NORMANDIE CYBER

Région Normandie
5 départements

Le CSIRT est interne au Campus Cyber territorial Normandie Cyber, lui-même désormais intégré dans l'association Normandie Numérique.

En 2022, la région Normandie projette de créer un campus cyber territorial et ouvre son centre de réponse à incident « CSIRT Normandie Cyber » porté par l'Agence de Développement AD Normandie [8]. En 2025, la Région a impulsé une restructuration de l'écosystème numérique en Normandie et a soutenu la création de l'association Normandie Numérique qui rassemble dorénavant les moyens et objectifs de la filière numérique, incluant le Campus Normandie Cyber et le CSIRT

Autres Services proposés par la structure :

- Accompagnement à la montée en maturité Cyber
- Analyse de vulnérabilité et alerte
- Sensibilisation
- Missions du campus (Opération, Innovation, Formation, Animation)

03/10/2022

CSIRT Bourgogne-Franche-Comté [9]

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

Région Bourgogne-Franche-Comté
8 départements

Le CSIRT EST un service au sein du GIP ARNIA.

La création du CSIRT est portée par l'Agence Régionale du Numérique et de l'Intelligence Artificielle (GIP ARNIA). Le CSIRT devient alors un service de cette agence [10].

Autres Services proposés par la structure :

- Services en ligne : quiz, liste des formations, annuaire prestataires, informations, ressources, ...
- Sensibilisation
- Avis sur un courriel douteux
- Détecteur de site douteux
- Alerte fin de support logiciel
- Alerte de vulnérabilité

Membre d'autres programmes et adhésions :

- Membre interCERT-France

15/02/2023

Grand Est Cybersécurité [11]

LE CENTRE D'ASSISTANCE
Grand Est Cybersécurité

Région Grand Est
10 départements

Le CSIRT est interne au Hub Grand Est Cybersécurité qui a été labellisé Campus Cyber Territorial fin 2025. Le Hub est porté par l'agence Grand Est Développement.
Le hub est une association.

La création du CSIRT a été portée par l'Agence Régionale d'Innovation Grand Enov+ [12], devenue l'Agence Grand Est Développement en Janvier 2025.
Le CSIRT est intégré dans le Hub Campus Régional Grand Est Cybersécurité.

Opéré par Grand Est Développement, et mandaté par la Région Grand Est, le Centre d'Assistance intervient pour protéger, diagnostiquer et accompagner face aux cyber-incidents, en coordination avec un réseau d'experts qualifiés.

Autres Services proposés par la structure :

- Services en ligne : Informations, Agenda, Ressources
- Sensibilisation
- Scan de vulnérabilité
- Enregistrement IP

15/03/2023

Cyber'Occ [13]

En juin 2022, la Région Occitanie, l'agence de développement économique AD'OCC et l'association Ekitia créent le centre de cybersécurité d'Occitanie, Cyber'Occ, dont une des missions est la mise en place du CSIRT [14]. Le Service d'Urgence Cyber ouvre huit mois plus tard. Cyber'Occ est labellisé Campus Cyber territorial et installé au Data Valley à Labège.

Autres Services proposés par la structure :

- Services en ligne : informations, ressources, annuaire de la filière Cybersécurité, diagnostic de maturité cyber…
- Sensibilisation, ateliers thématiques
- Ateliers Collectifs : intelligence collective pour répondre à un besoin cyber d'un groupe (fédération, secteur…)
- Audit de maturité cyber
- Missions du Campus : Opération, Innovation, Formation, Animation

Membre d'autres programmes et adhésions :

- Membre du consortium OccitanIA – EDIH Occitanie *(voir partie IV, chapitre C)*
- Membre du consortium de l'AMI Compétences et Métiers d'Avenir Cyber : Osmose
- Membre du Comité exécutif de l'Institut Cybersécurité de l'Occitanie ICO
- Membre de l'association européenne ECSO

CYBER'OCC
LE CENTRE CYBERSÉCURITÉ EN OCCITANIE

Région Occitanie
13 départements

Le CSIRT est interne au Campus Cyber Territorial Cyber'Occ.
Le centre Cyber'Occ est une association.

16/03/2023

CSIRT Hauts-de-France [15]

CSIRT HAUTS-DE-FRANCE

Région Hauts-de-France
5 départements

Le CSIRT est partenaire du Campus Cyber Territorial Hauts-de-France.
Le CSIRT est une association.

En 2022, le CITC (Centre d'Innovation des Technologies sans Contact) a mis en place le CSIRT de la Région Hauts-de-France. Le CSIRT a ouvert en avril 2023 et il est hébergé au sein du Campus Cyber Hauts de France Lille Métropole.[16]

Autres Services proposés par la structure :

- Services en ligne : informations, actualités
- Le CSIRT Hauts de France accompagne le CITC dans deux projets France 2030 Métier et Compétence d'Avenir : Défi TL (la cybersécurité pour les métiers du transport et de la logistique) et le projet RECI (Réponse aux Enjeux Cyber pour l'industrie).

01/04/2023

Campus Régional de Cybersécurité et de Confiance Numérique [17]

CRIC-NA
centre de réponse aux incidents cyber
Nouvelle-Aquitaine

Région Nouvelle-Aquitaine
12 départements

Le CSIRT est interne au Campus Cyber Territorial Nouvelle-Aquitaine.
Le Campus est une association.

La mission d'opérer le CSIRT territorial est confiée au Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine créé par la Région Nouvelle Aquitaine, l'agence de développement ADI-NA, le CLUSIR et le GIP Acyma, en 2022.[18]
Le Campus est installé au sein du parc Ampéris à Pessac. Il anime également un réseau de structures locales sur les départements, les Centres de Ressources cyber dont neuf sont déjà déployés.

Autres Services proposés par la structure :

- Services en ligne : annuaire des prestataires Cyber, conseils, ressources
- Formation cybersécurité pour les dirigeants
- Vérification de la compromission d'un email
- Test de l'exposition aux risques
- Actions du campus : Opération, Innovation, Formation, Animation
- Sensibilisation CyberDépart
- OSINT et recherche d'informations sur le Darkweb
- Surveillance défacement des sites internet des collectvités, surveillance noms de domaine
- Recherche compromission, cartographie

Campus Cyber Nouvelle-Aquitaine

14/09/2023

Pays de la Loire Cyber Assistance [19]

Région Pays de la Loire
5 départements

Le CSIRT est un service du GIP Gigalis.

Le CSIRT est un service mis en place au sein du conseil régional. Depuis le 1er mars 2025, le CSIRT est porté par le GIP Gigalis.

Autres Services proposés par la structure :

- Diagnostic
- Sensibilisation

21/11/2023

Breizh Cyber [20]

Le CSIRT est porté par le conseil régional de Bretagne.

Autres Services proposés par la structure :

- Services en ligne : annuaire prestataires, informations, ressources
- Sensibilisation
- Analyse de la surface d'attaque externe
- Risques humains
- Veille en cybersécurité
- Protection de la messagerie M365
- Détection des vulnérabilités sur les domaines .bzh

Membre d'autres programmes et adhésions :

- Membre interCERT-France

Région Bretagne
4 départements

Le CSIRT est partenaire du Campus Cyber Territorial : Bretagne Cyber Alliance.
Le CSIRT est un service de la Région Bretagne.

27/11/2023

Urgence Cyber Île-de-France [21]

Urgence Cyber Île-de-France a été mis en place par la Région Île-de-France.

Au-delà de la gestion d'incidents, le dispositif agit en prévention grâce à des actions de sensibilisation et de formation à la cybersécurité. Il s'inscrit dans un écosystème régional dynamique, soutenu par des aides financières et des outils gratuits comme MonServiceSécurisé,

Autres Services proposés par la structure :

- Accompagnement à la maturité Cyber des communes franciliennes
- Mise en place de la gestion mutualisée du risque fournisseurs
- Formation, Sensibilisation, Conférence

Membre d'autres programmes et adhésions :

- Membre interCERT-France

Région Île-de-France
8 départements

Le CSIRT est partenaire au Campus Cyber National.
Le CSIRT est un service de la Région Île-de-France.

20/03/2024

Le CSIRT est porté par le GIP CybeRéponse créé à cet occasion par le GIP RECIA, le centre régional de ressources numériques et Dev'Up Centre-Val de Loire [23].

Autres Services proposés par la structure :

- Sensibilisation
- CyberCrise : exercice de crise
- CybeReveal : analyse de l'exposition aux risques Cyber
- CybeRanger : détection de vulnérabilité
- CybeRang : simulation d'attaque
- CyberSpear : système de continuïté d'activité en cas de crise majeure.

Ce Cyber Campus avec un pôle d'innovation qui a vocation a rejoindre le réseau des campus cyber territoriaux.

CybeRéponse [22]

Région Centre-Val de Loire *6 départements*

Le CSIRT est un service du GIP CybeRéponse.

03/04/2024

CSIRT CyberCorsica [24]

Collectivité de Corse

Le CSIRT est un service de la collectivité de Corse.

Le CSIRT CyberCorsica est porté par la Collectivité de Corse. Il a été inauguré le 3 avril 2024 [25]. Au-delà de la gestion et l'accompagnement en cas d'incident de cybersécurité, il contribue à la prévention et la sensibilisation à la cybersécurité de ses bénéficiaires. Il s'inscrit et anime l'écosystème insulaire et propose divers services destinés à accroître la maturité numérique des entités du territoire.

Autres Services proposés par la structure :

- Services en ligne :
  - Actualité, Veille
- Sensibilisation et prévention à la cybersécurité
- Diagnostics en cybersécurité
- Analyse de la surface d'exposition
- Suivi de la maturité cyber des bénéficiaires
- Veille et communication autour de la cybersécurité
- Animation du réseau des acteurs cyber du territoire

17/04/2024

Urgence Cyber région Sud [26]

Le CSIRT de la région Provence-Alpes-Côte d'Azur est porté par l'association loi 1901 « Urgence Cyber CSIRT région Sud ».

Autres Services proposés par la structure :

- Services en ligne :
  - informations, annuaire, actualités
- Sensibilisation
- Diagnostic
- Veille et alerte

Région Provence-Alpes-Côte d'Azur *6 départements*

Le CSIRT est partenaire du Campus Cyber Territorial.
Le CSIRT est une association.

30/07/2024

CSIRT Atlantic [27]

Le CSIRT-ATLANTIC est le centre d'assistance cyber unique pour les bénéficiaires de taille intermédiaire des territoires français d'Amérique. Il est au cœur du dispositif national de CSIRT régionaux soutenu par l'ANSSI, engagé dans des actions de prévention, protection et partage d'information communautaire cyber.

Autres Services proposés par la structure :

- Services en ligne :
  - Informations, ressources, actualités
- Sensibilisation
- Exercice de Cyber-crise
- Diagnostic
- Suivi de maturité Cyber
- Observatoire Cyber

Territoires français d'Amérique
Guadeloupe, Guyane, Martinique, Saint-Barthélémy, Saint-Martin, Saint-Pierre-et-Miquelon

Le CSIRT est un service de l'ACCYB (Agence Caribéenne pour la CYBersécurité).

24/10/2024

Centre Cyber du Pacifique [28]

Le CSIRT de Nouvelle-Calédonie est porté par l'association loi 1901 « Centre Cyber du Pacifique ». Le Centre Cyber du Pacifique structure et anime l'écosystème de la cybersécurité et accompagne la montée en maturité des acteurs économiques et institutionnels de la région [29].

Autres Services proposés par la structure :

- Services en ligne :
  - Informations
  - Annuaire
  - Ressources, actualités
- Sensibilisation

Nouvelle-Calédonie
3 Provinces

Le CSIRT est une association.

04/11/2024

CSIRT La Réunion [30] [30]

La Réunion

Le CSIRT est opéré par CYBER REUNION, la marque du Pôle Cybersécurité de l'établissement public Réunion THD.

Le 4 novembre 2024, La Réunion a lancé CYBER RÉUNION, la marque régionale de cybersécurité portée par Réunion THD, établissement public de la Région Réunion, avec une ambition claire : renforcer durablement le niveau de cybersécurité et de cyber-résilience du territoire. CYBER RÉUNION opère le CSIRT La Réunion, avec le soutien de la Région Réunion et de l'ANSSI, et coordonne l'EDIH La Réunion (European Digital Innovation Hub), cofinancé par l'Europe et la Région Réunion [31].

Autres Services proposés par la structure :

Au-delà de la réponse aux incidents, le CSIRT La Réunion déploie un ensemble de services proactifs visant à anticiper les menaces et à élever le niveau de maturité des organisations, notamment :

- Services en ligne :
  - Informations, conseils, ressources, actualités
- Service de notification de risques et de vulnérabilités
- Service d'évaluation continue de la maturité cyber
- Publication d'alertes et l'organisation de webinaires mensuels
- Sensibilisation dont une immersive avec l'escape game cyber « TecTec Drone »
- Organisation d'exercices de gestion de crise ;
- Veille sur les noms de domaine en ".re"
- Production d'un rapport sur l'état de la menace cyber dans l'océan Indien

Membre d'autres programmes et adhésions :

- Membre de l'InterCERT-France
- Membre de TrustBroker Africa
- Coordonne l'EDIH La Réunion *(voir partie IV, chapitre C)*

B- Accompagnement et Coordination de l'ANSSI

1- Incubation et accompagnement par l'ANSSI

Depuis 2021 et à travers le plan France Relance, l'Agence accompagne le déploiement et la structuration des CSIRT territoriaux. Le dispositif est aujourd'hui constitué de 15 CSIRT dont 3 ultramarins. Ils sont complémentaires des autres acteurs cyber : le CERT-FR (intégré à l'ANSSI), Cybermalveillance.gouv.fr, les CSIRT sectoriels, les prestataires privés, etc...

Les responsables de projet des CSIRT territoriaux ont constitué dès le départ un groupe de partage, d'échange et de solidarité qui s'est développé et constitue aujourd'hui un groupe organisé et actif incluant tous les CSIRT territoriaux.

Une partie des CSIRT territoriaux ont pu suivre l'incubation proposée par l'ANSSI, leur permettant d'acquérir des bases méthodologiques et organisationnelles. Pour d'autres, le parcours d'incubation et d'accompagnement suivi auprès de l'association InterCERT France a joué ce rôle. Elle est présentée partie II, chapitre F. Ces parcours ont permis de structurer leur gouvernance, de formaliser leur processus de gestion d'incident et de préparer les équipes aux exigences opérationnelles d'un centre de réponse territorial.

2- Relations avec le CERT-FR

Le CERT-FR [32] (French Computer Emergency Response Team) est l'entité gouvernementale et nationale assurant la mise en œuvre opérationnelle de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la nation dévolue à l'ANSSI [33]. Il est armé par la sous-direction Opérations de l'ANSSI.

Il intervient prioritairement sur des incidents survenant au sein des ministères et services de l'Etat, des opérateurs d'importance vitale et opérateurs de services essentiels mais peut être amené à avoir une action sur l'ensemble du territoire national.

Relations opérationnelles

L 'équipe du CERT-FR est en relation étroite avec les CSIRT Territoriaux. Régulièrement, chaque CSIRT territorial fait le point avec les équipes du CERT-FR : incidents, signalement de victimes potentielles, suivi post incident, échanges d'information, précision sur une démarche ...

Lorsque le CERT-FR a connaissance d'un incident concernant une victime qui n'est pas dans son périmètre, il peut demander au CSIRT territorial de prendre le relais.

Coordination et régulation

L'équipe du CERT-FR coordonne également les échanges entre les écosystèmes cyber. Dans le cas des CSIRT territoriaux, leur naissance, leur montée en maturité et leurs activités sont quotidiennement suivies par l'équipe du CERT-FR. L'équipe anime aussi le réseau des CSIRT territoriaux. Un comité technique est organisé tous les mois et des points bilatéraux réguliers permettent de centraliser les incidents et assurer leur suivi au niveau national.

Les CSIRT territoriaux sont invités chaque année à participer à la journée du CERT-FR en présence de nombreux autres CSIRT et CERT nationaux, publics et privés.

C- Intégration au dispositif 17Cyber

Lancée le 17 décembre 2024, la plateforme **17Cyber.gouv.fr** [34] est le résultat d'une collaboration entre **Cybermalveillance.gouv.fr** (GIP Acyma) [35], la gendarmerie nationale et la police nationale.

Destiné aux particuliers, aux collectivités et aux professionnels, cet outil permet aux victimes d'une cyberattaque de qualifier la menace, d'obtenir des conseils personnalisés et si besoin, de bénéficier d'un accompagnement par un policier ou un gendarme 24/7 pour l'aide à la judiciarisation ou une mise en contact avec des prestataires pour de la remédiation technique.

En avril 2025, 17Cyber.gouv.fr a étendu ses collaborations avec des acteurs de l'écosystème tels que les CSIRT territoriaux pour renforcer la prise en charge des victimes de cybermalveillance. Les victimes professionnelles du 17Cyber.gouv.fr (entreprises, associations, collectivités) peuvent désormais **bénéficier de l'assistance téléphonique de l'équipe du CSIRT de leur région**. Les CSIRT de Nouvelle Aquitaine et d'Occitanie ont été les premiers à intégrer la plateforme avec une ouverture du service en octobre 2025 [36]. Le 25 novembre, le CSIRT La Réunion est également arrimé au dispositif suivi de près par 5 autres régions (Région SUD, ...).

Cette collaboration avec le 17Cyber contribue à renforcer l'accès des victimes quel que soit leur territoire et à apporter une réponse coordonnée et structurée à l'échelle nationale pour l'assistance Cyber en France.

D- Relations avec les Forces de Sécurité Intérieure

Pour assurer leurs missions, la relation avec les forces de l'ordre sur chaque territoire est essentielle pour les CSIRT territoriaux. Chaque CSIRT a à cœur de construire et d'enrichir ses relations.

Tous les CSIRT territoriaux ont des échanges avec leur préfecture de Région, les responsables police et gendarmerie de leur territoire et toutes les instances qui peuvent améliorer le service rendu aux victimes.

Certains CSIRT ont même mis en place des conventions comme Nouvelle-Aquitaine avec la préfecture de Région, PACA avec la gendarmerie…

Les CSIRT collaborent de manière continue avec les services de l'OFAC et de la Gendarmerie (C3N) dans le cadre des actions d'investigations.

Cellule d'anticipation organisée par le CSIRT Nouvelle-Aquitaine avec la gendarmerie et le CERT aviation

E- Coordination avec les CSIRT sectoriels

Le projet de l'ANSSI dans le cadre du plan France Relance 2030 contient également la volonté de créer des CSIRT ou CERT sectoriels [37]. Ces derniers sont des centres de réponse aux incidents cyber, associés à un secteur d'activité spécifique. Le CERT aviation pour le secteur de l'aéronautique, le CERT ED pour le secteur des entreprises de la défense, M-CERT pour le secteur du maritime et le CERT Santé dédié aux établissements de santé.

Ils disposent de relations privilégiées avec les CSIRT territoriaux qui ont dans leurs territoires, une forte imprégnation de secteurs particuliers (santé, portuaire, maritime, aéronautique, défense). Ils traitent les demandes d'assistance des acteurs de leur secteur et sont en capacité de traiter les événements de sécurité numérique.

En cas de cyber-incident concernant un acteur d'un de ces secteurs, le CSIRT territorial se met en relation avec le CSIRT sectoriel pour coordonner l'accompagnement. Les CSIRT sectoriels peuvent compter sur les CSIRT territoriaux pour connaître les prestataires locaux capables de répondre aux besoins de leurs victimes bénéficiaires.

F- L'InterCERT France

L'interCERT France (Computer Emergency Response Team) [38], première communauté française de CERT, est une association loi 1901 fédérant plus d'une centaine de membres. Son objectif est de renforcer la capacité de chaque membre **à détecter** et **à répondre aux incidents de sécurité** impactant son périmètre. Le partage d'expériences et l'échange d'informations contribuent à la réalisation de cet objectif. L'association constitue et pérennise un réseau d'organisations ayant des activités de réponse à incident d'origine cyber (CERT et CSIRT privés, sectoriels ou institutionnels) sur le territoire français.

Dans une logique de coopération et d'échange entre pairs, les CSIRT territoriaux ont pour projet de rejoindre l'InterCERT France, afin de consolider leurs capacités, partager les bonnes pratiques et contribuer aux dynamiques de sécurité à l'échelle nationale et régionale.

Certains d'entre eux l'ont déjà fait. En septembre 2024, le **CSIRT Bourgogne Franche-Comté** est le premier CSIRT territorial à intégrer l'interCERT France[55], suivi de la **Bretagne**, **Urgence Cyber d'Ile de France**, **Urgence Cyber Sud** et **La Réunion** en octobre 2025.

De plus, l'interCERT France a lancé en 2024 [39] son incubateur pour accompagner les équipes en émergence, leurs membres et les faire gagner en maturité. Les CSIRT La Réunion, Urgence Cyber Île-de-France, Normandie et Urgence Cyber Sud ont bénéficié de ce dispositif. Les CSIRT auront également la possibilité de l'utiliser pour faire monter en compétence leur nouvelle recrue.

G- La communauté des CSIRT Territoriaux

Les CSIRT territoriaux se sont construits en créant une communauté forte, en partageant leurs visions, leurs besoins, leurs interrogations, leurs bonnes pratiques et leurs outils ainsi qu'en intégrant les nouveaux CSIRT au fur et à mesure. Les premières phases d'incubation accompagnées par l'ANSSI ont contribué à créer des liens entre les CSIRT qui se sont consolidés au fil des rencontres lors d'événements (journée CERT-FR, salons Cyber…), des comités techniques organisés régulièrement par l'ANSSI et des journées inter-CSIRT organisées par les CSIRT eux-mêmes.

Les objectifs de la communauté des CSIRT sont notamment le partage (incidentologies territoriales, outils, process…), l'entraide, la mutualisation…

L'animation et les groupes de travail vont se renforcer pendant l'année 2026, qui sera jalonnée par des journées inter-CSIRT régulières.

La journée inter-CSIRT de novembre 2025 s'est déroulée à Toulouse, la veille de la Convention Business Cybersécurité (CBC), salon professionnel dédié à la Cybersécurité. Au programme : groupe de travail, rencontre avec des acteurs locaux (Airbus protect, Predicta Lab), échange avec les représentants des Campus Cyber Territoriaux venus pour le CBC et visite du Commandement de l'Espace.

Visite du commandement de l'espace en novembre 2025, à Toulouse

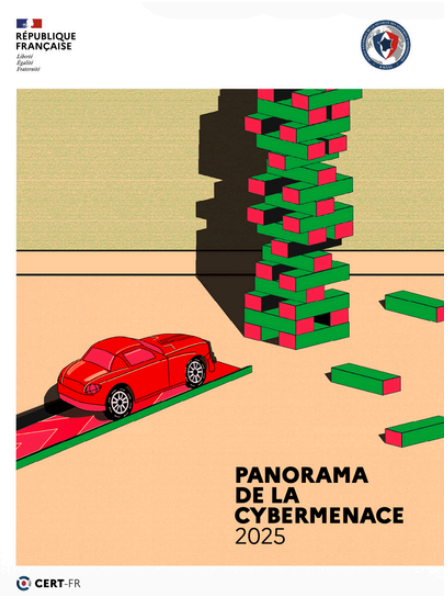
Dans la continuité de la journée inter-CSIRT, une table ronde dédiée aux CSIRT territoriaux et à l'ANSSI a été organisée pendant le salon CBC, le 27 novembre 2025, avec pour thématique :
ANSSI et CSIRT territoriaux, quelles réponses coordonnées face aux menaces ?
Participants : ANSSI, CSIRT Bourgogne-Franche-Comté, CSIRT Corse (CyberCorsica), CSIRT Atlantic et CSIRT Occitanie (Cyber'Occ)

III- BILAN 2025 ET PERCEPTION DE LA MENACE

En Cybersécurité, en France, l'ANSSI et Cybermalveillance.gouv.fr sont les acteurs incontournables sur le sujet. Chaque année, ils publient leurs synthèses de la menace au regard de leurs périmètres.

A- Synthèse de la menace observée par les acteurs institutionnels

1- L'ANSSI



L'ANSSI a publié le 11 mars son **Panorama de la cybermenace 2025** [40], dans lequel l'Agence constate que la menace cyber se maintient a un niveau élevé, Vincent Strubel parlant *"d'une marée haute qui perdure même si ce n'est pas un raz-de-marée"*.

Les secteurs les plus touchés sont la santé, l'éducation et la recherche. Néanmoins, une sur-représentation est possible dans la mesure où le service public déclare davantage ses incidents.

Du côté des cybercriminels, la tendance est aux fuites de données plutôt qu'aux rançongiciels plus complexes, car ce sont des attaques plus facile à mener. L'objectif est d'abord l'extorsion.

Les données peuvent aussi être revendues ou utilisées pour d'autres attaques. L'ANSSI précise que 58% des revendications sont de fausses revendications d'attaques déjà passées.

Au cours de l'année 2025, l'ANSSI a traité **3586 événements de sécurité** dont 1366 incidents, le nombre est stable par rapport à l'année dernière par contre les signalements ont un peu diminué.

Un incident est un événement de sécurité conduit par un acteur malveillant qui atteint le SI d'une victime. Les autres événements sont des signalements. En 2025, l'ANSSI a été confrontée à 128 incidents liés à des rançongiciels (contre 141 en 2024) et à **196 incidents liés à des fuites de données** (contre 130 en 2024).

Les acteurs étatiques poursuivent leurs opérations d'espionnage et de sabotages (attaques hybrides). Une campagne fin décembre a visé la Pologne avec l'objectif de couper le réseau électrique, même si le pire a pu être évité.

La frontière entre les cybercriminels et les acteurs étatiques est de plus en plus floue. L'ANSSI parle de brouillard technologique et organisationnel conséquence d'un partage de capacité, de l'adoption de pratiques initialement attribuées à certains, détournement d'outils et de services légitimes à des fins malveillantes comme les services d'IA. La France doit se préparer à une augmentation de ces attaques hybrides.

Les attaquants se concentrent aussi sur la recherche de vulnérabilités sur les équipements de sécurité de bordure qui sont largement répandus et peuvent leur fournir un accès initial. La chaîne de sous-traitance continue également a être fortement ciblée.

Enfin, l'IA générative représente un potentiel accélérateur des capacités offensives des attaquants, mais ne rend pas pour autant possible des attaques qui n'étaient pas possibles auparavant. Elle est cependant un outil pour les défenseurs.

L'ANSSI rappelle qu'elle travaille à renforcer le niveau de sécurité à travers la réglementation, la sensibilisation et en s'appuyant sur des acteurs relais dans les régions comme les CSIRT territoriaux.

2- Cybermalveillance.gouv

Chaque année, **Cybermalveillance.gouv.fr** publie son rapport d'activité [41], partage son état de la menace et revient sur les tendances et les faits marquants de l'année précédente.

En 2025, les sites cybermalveillance.gouv.fr et 17Cyber.gouv.fr (plateforme lancée en décembre 2024) ont enregistré, **504 000 demandes d'assistance** : 93% pour des particuliers et **7% pour des professionnels** (33 012 demandes) dont 6% d'entreprises et associations et 1% de collectivités et administrations.

Les premières menaces qui touchent **les particuliers** sont l'**hameçonnage** (**32,9%** des demandes) puis le **piratage de compte 11,6%** et les **violations de données 8%**.

La menace cyber continue de se diversifier et de s'intensifier. La professionnalisation et la spécialisation des cybercriminels se confirment. Les nombreuses fuites de données personnelles font craindre, pour l'avenir, d'importantes campagnes d'hameçonnage, de piratage de compte, d'usurpation d'identité.

Pour **les entreprises et les associations**, les demandes portent en priorité sur le **piratage de compte (21%)**, l'**hameçonnage** (**16%** - en baisse par rapport à 2024 où il représentait 20,7%) et les **faux ordre de virement** (**13,5 %** - en hausse par rapport à 2024 où il représentait 11,5%). Les rançongiciels enregistrent une légère baisse (8% contre 12,4% en 2024).

Pour **les collectivités** et **les administrations**, la menace principale et en hausse est le **piratage de compte** (**20,1%** contre 16% en 2024). Les 2 menaces suivantes sont l'**hameçonnage** (**19,2%** - en baisse par rapport à 2024 où il représentait 24,4%) et les **rançongiciels** (**13,1%** - en baisse aussi par rapport à 2024 où il représentait 18,7%). On note l'augmentation de la fraude au virement qui passe de 3,4% en 2024 à 8,5% en 2025 et arrive en 4e position.

Le **piratage de compte** et l'**hameçonnage** sont les premières raisons des demandes d'assistance. Les données personnelles, quelles qu'elles soient, suscitent l'intérêt des cybercriminels avec un **marché souterrain de la donnée volée structuré et très organisé**. Plus la donnée est récente, plus elle a de la valeur.

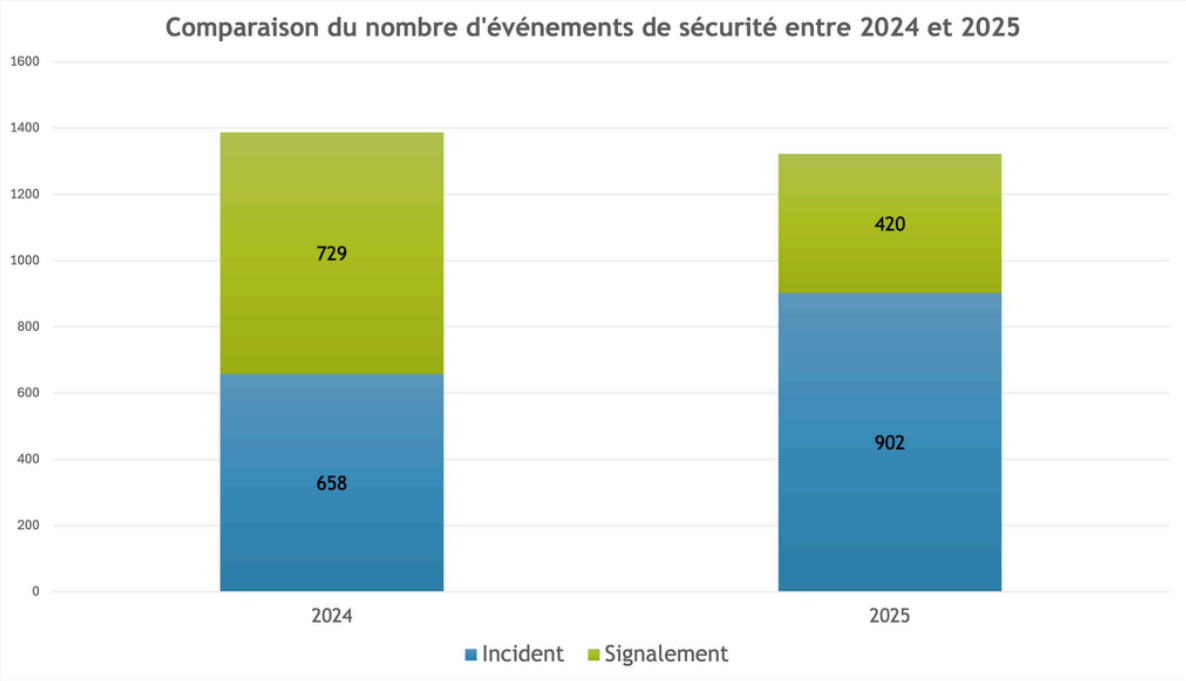
La **fraude au virement** ou **Faux Ordres de Virement** (FOVI) est en constante augmentation. Cette attaque fait souvent suite à la compromission d'un compte de messagerie (fournisseur, client...). Même si les **rançongiciels** affichent une légère baisse, la menace reste élevée. Ces attaques résultent le plus souvent d'une intrusion dans le système d'information, rendue possible par l'exploitation d'une faille de sécurité.

Enfin, la frontière entre Cyber et espace physique s'estompe avec, par exemple, le recours à des équipes "terrain" pour récupérer des cartes bancaires ou bien des cambriolages consécutifs à des fuites de données.

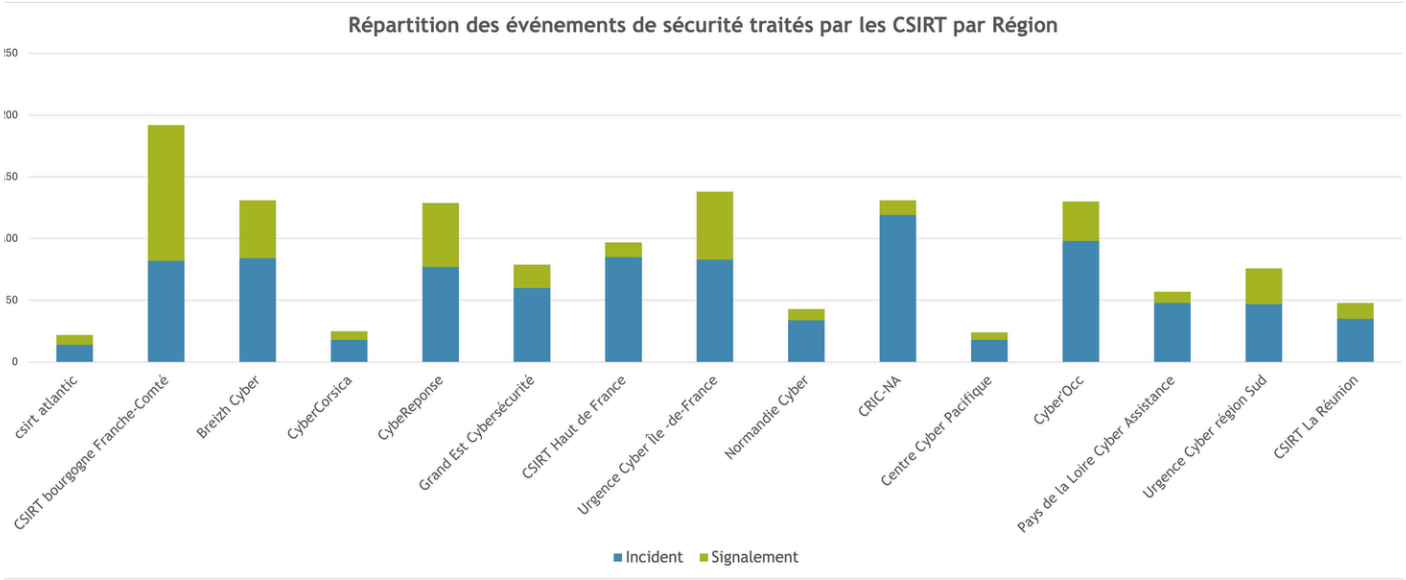
B- Synthèse de la menace observée par les CSIRT Territoriaux

En **2025**, les CSIRT territoriaux ont traité **1322 événements de sécurité** contre 1387 en 2024**.**

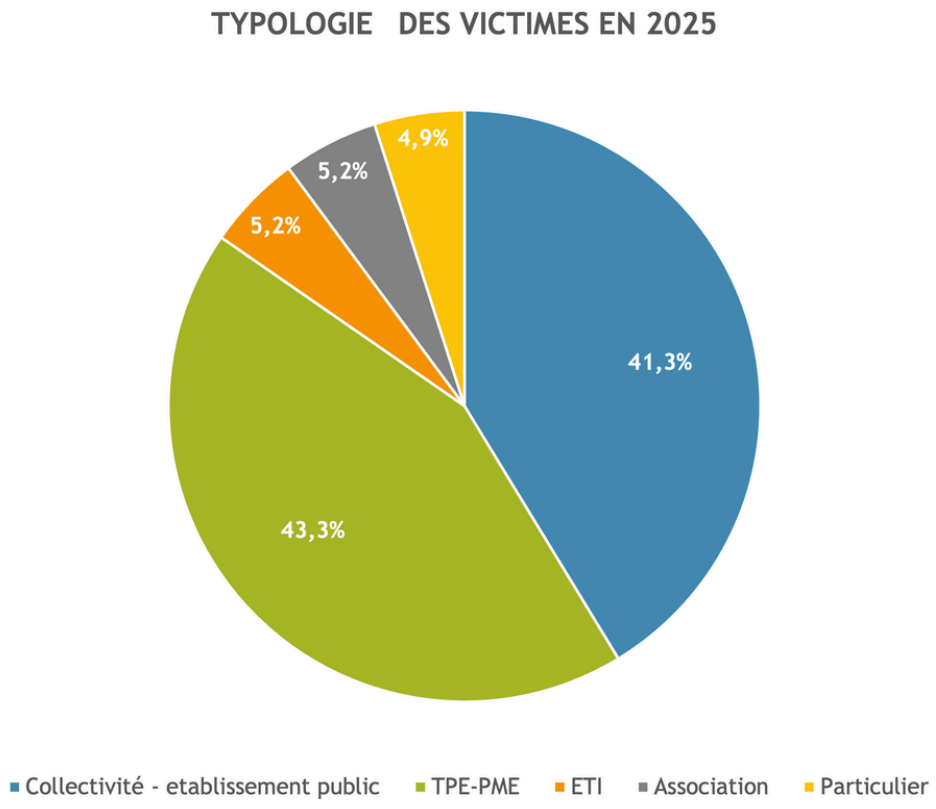
Les événements de sécurité sont constitués de deux familles : les incidents et les signalements. Un incident est un événement de sécurité conduit par un acteur malveillant qui a un impact sur le système d'information de la victime. Un signalement est un comportement anormal ou inattendu pouvant avoir un caractère malveillant ou ouvrir la voie à une autre action néfaste comme le déni de service, l'hameçonnage, la tentative de connexion, par exemple.



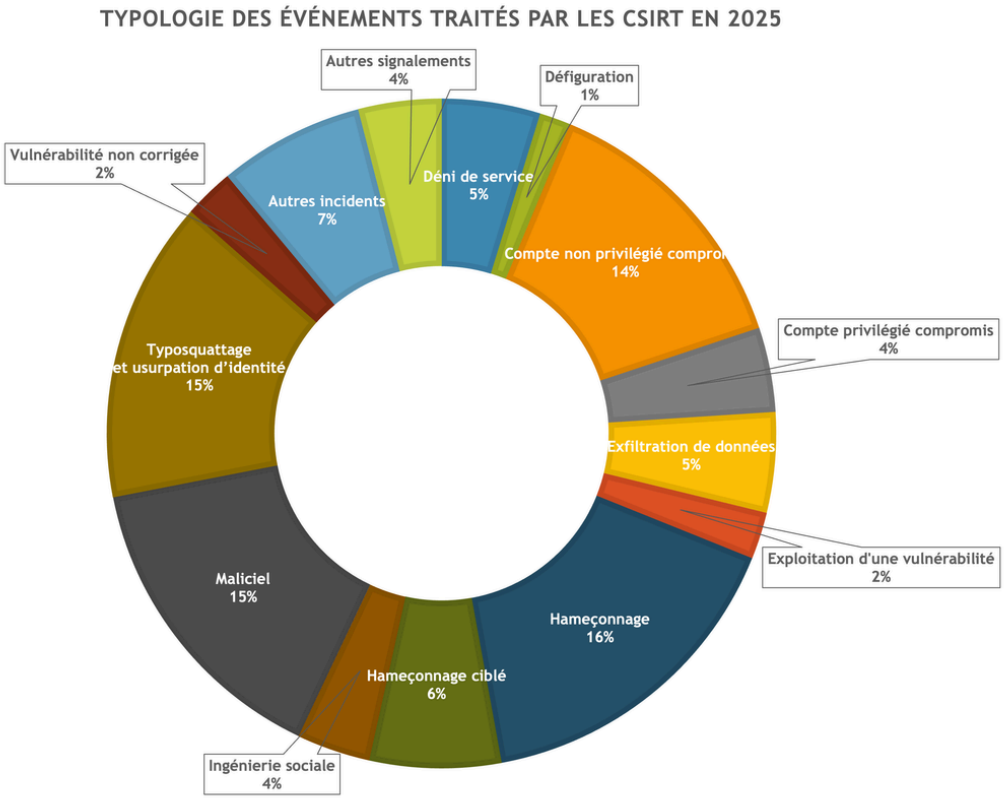
Le nombre d'incidents a fortement augmenté : **902 incidents** en 2025 contre 658 incidents en 2024. Par contre, le nombre de signalements a diminué : **420 signalements** en 2025 contre 729 en 2024. Cela peut s'expliquer par l'impact des Jeux Olympique de Paris 2024 et la constatation d'événements directement liés à cet événement. Par exemple, de nombreux dénis de service, visant souvent les mairies, ont eu lieu sur le passage de la flamme olympique.



La répartition des événements par régions est assez homogène au regard de la date d'ouverture du CSIRT, de la taille de son territoire, du nombre d'entreprises et de collectivités concernées.



48,5% des victimes qui contactent les CSIRT territoriaux sont des **entreprises** et **41,3%** sont des **collectivités**.

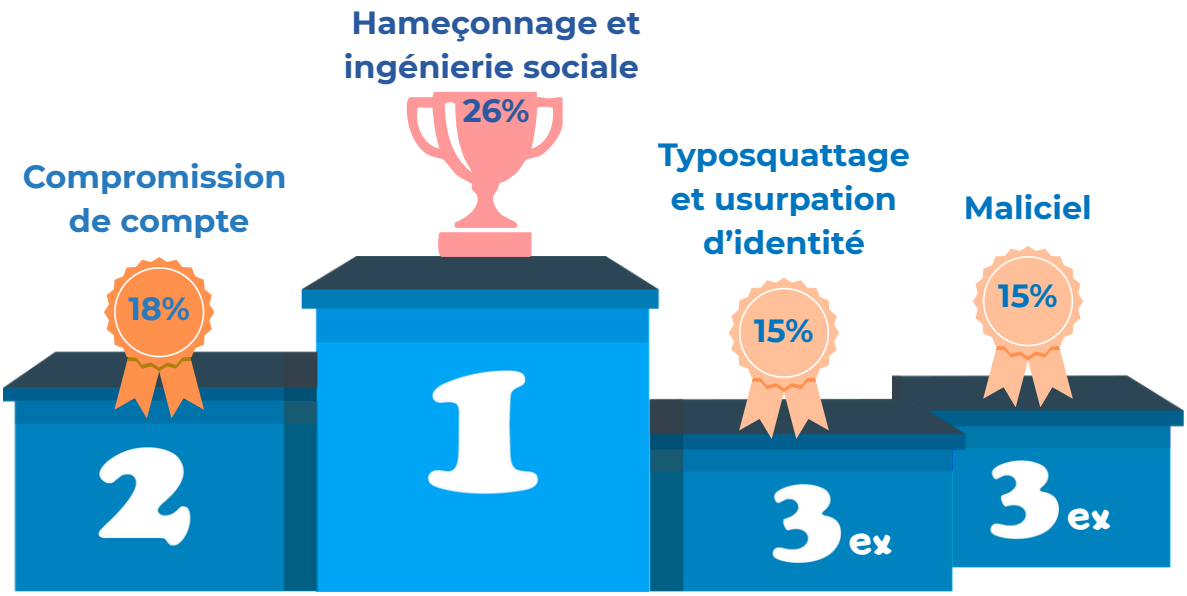


Les tentatives de manipulation sont en tête avec **22%** d'hameçonnage (ciblé ou non) et 4% d'autres techniques liées à de l'ingénierie sociale.

18% des événements concernent des compromissions de compte. Les attaquants cherchent de plus en plus à acquérir des accès légitimes ce qui leur permet ensuite de déployer d'autres attaques et surtout d'exfiltrer des données. Les incidents observés par les CSIRT, ne sont pas toujours requalifiés quand ils débouchent sur une exfiltration ce qui peut expliquer que le nombre d'exfiltration n'est que de 5%. D'ailleurs, l'actualité fin 2025 et début 2026, montre une recrudescence des fuites de données dont l'origine est une compromission de compte.

15% des événements concernent du **typosquattage** et de l'**usurpation d'identité** dont **49%** sont liés à du **FOVI** ou **fraude au virement**. Le typosquattage correspond le plus souvent à des créations de faux sites avec l'identité de la victime (Nom commercial, SIRET, etc..). L'objectif est d'amener des victimes à valider des paiements pour une marchandise ou un service qui ne seront jamais délivrés.

Les maliciels représentent **15%** des événements ; parmi eux, **82%** sont des rançongiciels.



3- Corrélation avec la synthèse de la menace et les alertes nationales et internationales

Les CSIRT observent comme l'ANSSI et cybermalveillance.gouv.fr une majorité d'**attaques par hameçonnage et ingénierie sociale**. De même, les **compromission de compte sont une part importante des événements** traités par les CSIRT. Les fuites de données personnelles récentes et l'usage de l'IA par les cybercriminels pour les exploiter, peuvent contribuer à alimenter ce type d'attaque.

Les **rançongiciels se maintiennent** avec de nouvelles formes très agressives comme celle du groupe criminel Qilin qui laissent nos entreprises désemparées quand l'attaque est réussie. Le facteur aggravant est l'absence de sauvegardes saines.

Le recours au typosquatting pour créer de faux sites aux couleurs d'une entreprise ou d'un service administratif augmente aussi, facilité par l'usage de l'IA. La fraude au virement est encore très présente. Elle est souvent permise par la compromission d'un compte de messagerie mais peut être contrée par des mesures organisationnelles.

Beaucoup d'entreprises hésitent encore à demander de l'aide et minimisent les conséquences de certains incidents de sécurité. Plusieurs de ces attaques auraient pu être évitées avec la mise en place des premiers gestes de sécurité.

Cela montre que les campagnes de sensibilisation menées par tous les acteurs et en particulier par les CSIRT territoriaux au plus proche de leur territoire, sont essentielles et doivent continuer pour faire prendre conscience de la menace, expliquer les premiers gestes de sécurité qui peuvent faire la différence et inciter les acteurs à entrer davantage dans une démarche de cybersécurité.

C- Actions de Prévention et d'Information

Au-delà du service d'assistance en cas d'incident, les CSIRT déploient différentes actions en fonction de leur territoire, pour la prévention, l'évaluation du niveau de sécurité, la montée en maturité, l'information sur les lois et réglementations à venir : NIS2, CRA..

Les CSIRTs ont réalisé en 2025 **637 actions de prévention** (interventions dans des événements, ateliers, conférences, exercices de gestion de crise ...) contribuant à amener les organisations de leur territoire (entreprises, collectivités...), à mettre en place des mesures de sécurité et à les renforcer.

Voici quelques exemples d'actions menées par les CSIRT :

- Plusieurs CSIRT étaient mobilisés avec l'ANSSI pour organiser l'**exercice de crise Rempar25** [42] (Occitanie, La Réunion...)

Cellules de crise REMPAR25 organisées par La Réunion

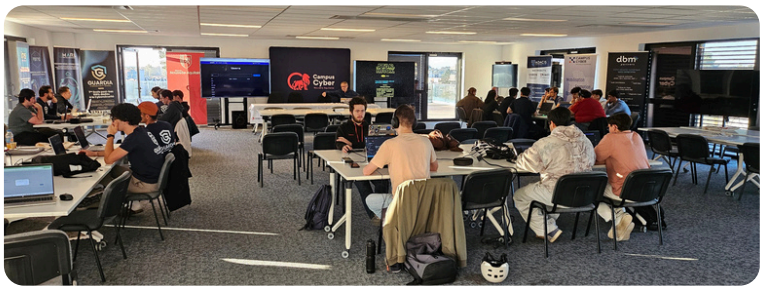
Lancement de l'événement REMPAR25 et Cellules de crise organisés par Cyber'Occ et l'ANSSI

- Certains CSIRT territoriaux comme celui de Bretagne et de La Réunion, mènent des campagnes de recherche de vulnérabilités aux profits des organisations de leurs territoires :
  - En Bretagne : **50 vulnérabilités signalées** (27 entreprises, 21 collectivités, 2 associations).
  - A La Réunion : **50 rapports de vulnérabilités** notifiés aux bénéficiaires.

- Les CSIRT proposent et réalisent des audits ou diagnostics de maturité Cyber (MonAideCyber, Diagnostic en ligne, autre diagnostic…) pour amener les responsables des organisations à avoir une vision organisationnelle de la sécurité de leur système d'information, avoir des premiers axes d'amélioration, trouver des partenaires de proximité pour mettre en place ses mesures de sécurité (PACA, Occitanie, Nouvelle-Aquitaine, La Réunion…)

1172 audits ou diagnostics de maturité Cyber en 2025

- Le **CSIRT Nouvelle Aquitaine** a mis en place un programme de **Bug Bounty "Star Hack"** [43] en partenariat avec une vingtaine d'écoles.



- Le **CSIRT Hauts de France** a organisé un **CTF** (Capture The Flag) dénommé **Vidocq**. Ce CTF met en compétition des équipes composées des prestataires cyber référencés au CSIRT, d'enquêteurs des services du Ministère de l'intérieur, du Ministère des Armées, de la Préfecture de Police de Paris et d'acteurs publics (CAUE, collectivités locales). Les participants ont dû résoudre une enquête cybercriminelle en utilisant les techniques forensiques et d'investigation numérique [44]. Le CSIRT a aussi participé à des exercices de *phishing* avec le CITC à destination des petites collectivités.

- La Région Île-de-France, avec l'appui de CSIRT Urgence Cyber Île-de-France, a mis en place **un observatoire de la performance cybersécurité** des communes d'Île-de-France, grâce à des évaluations non intrusives. C'est le CSIRT qui a ensuite pris contact avec les collectivités les plus à risque pour leur présenter leur rapport d'analyse et les aider à identifier les actions prioritaires.

- Certains CSIRT, comme celui des Hauts-de-France, sont également engagés, avec les services de l'État, dans la protection économique.

D- Spécificités territoriales

1- Côté Pacifique - La Nouvelle-Calédonie

Évoluant dans **une économie numérique peu développée et durement éprouvée par les émeutes de 2024**, le Centre Cyber du Pacifique doit accompagner des entreprises démunies dont la priorité est désormais la survie. L'insularité et l'éloignement de la métropole imposent une autonomie de réaction immédiate, malgré un partage complexe de compétences entre l'État et le Gouvernement local, qui peut brouiller la visibilité de ses missions. En recentrant ses activités sur la consolidation des partenariats de proximité et la sensibilisation, **le Centre Cyber du Pacifique peut transformer la cybersécurité en un levier de stabilité et de résilience** indispensable pour un territoire en quête de reconstruction économique.

2- Côté Océan indien - La Réunion

Territoire insulaire situé au cœur de l'océan Indien, La Réunion présente des spécificités qui, à l'instar de tout territoire insulaire éloigné de plusieurs milliers de kilomètres de la France hexagonale, renforcent la sensibilité des enjeux de cybersécurité. **L'éloignement, les contraintes de connectivité et la dépendance à des infrastructures clés** appellent une attention renforcée en matière de prévention, de réaction et d'accompagnement.

Dans ce cadre, le **CSIRT La Réunion développe une approche de proximité** visant à apporter un appui opérationnel aux acteurs du territoire, tout en participant à la diffusion d'une culture commune de vigilance et de résilience. Cette dynamique s'articule également avec le **projet européen EDIH La Réunion**, qui constitue un levier complémentaire pour accompagner la montée en maturité numérique et cyber des TPE et des PME. Au-delà de l'appui direct aux structures bénéficiaires, ce dispositif contribue également à structurer progressivement un écosystème local.

À terme, et pour en démultiplier l'effet, les corps intermédiaires ont naturellement vocation à jouer un rôle de têtes de réseau, ce qui suppose de développer à leur intention une offre de services adaptée.

Dans un marché encore en consolidation, l'ambition est également de favoriser l'émergence d'une offre plus lisible, plus accessible et mieux adaptée aux besoins

des petites structures, afin de contribuer, de manière pragmatique, au développement d'un véritable tissu économique de la cybersécurité à l'échelle réunionnaise.

Dans ce contexte, la situation particulière de La Réunion, à distance de l'Europe continentale mais au contact direct de son environnement régional, peut également ouvrir des perspectives de coopération utiles, dès lors qu'elles s'inscrivent en pleine cohérence avec les orientations régaliennes et au service du développement économique du territoire.

3- Côté Méditerranée - La Corse

Le CSIRT CyberCorsica : un relai de confiance face aux défis d'un territoire particulier

La mise en place d'un centre territorial de réponse à incident pour la Corse, le **CSIRT CyberCorsica** a marqué une étape décisive dans la résilience numérique du territoire. Peut-être plus qu'ailleurs en France, cette création a mis en lumière les besoins cruciaux de l'ensemble de la société insulaire face à l'accroissement des menaces pesant sur les réseaux. Pour comprendre l'impact et les enjeux de ce CSIRT territorial, il est indispensable de prendre en compte les spécificités géographiques, économiques et sociologiques propres à la Corse :

- **Le défi de l'insularité et de la topographie** : le statut d'île montagne de la Corse engendre des contraintes géographiques majeures. L'isolement inhérent à l'insularité, couplé à des temps de déplacement rallongés par le relief, complexifie l'accompagnement des victimes. Lors d'attaques ou de crises cyber, les entreprises isolées se retrouvent souvent démunies, éloignées des centres d'expertise continentaux.

- **Un tissu économique vulnérable** : l'économie corse repose en immense majorité sur des Très Petites Entreprises (TPE). Celles-ci n'ont malheureusement pas la taille critique nécessaire pour dégager des fonds suffisants et investir de manière proactive dans leur cybersécurité ou recruter des spécialistes dans ce domaine.

- **Le paradoxe de la « porte ouverte » :** la forte tradition de sécurité physique qui règne dans les villages corses – où il est encore courant de ne pas verrouiller la porte de sa maison – induit un biais cognitif dangereux. Ce sentiment d'immunité est souvent transposé à tort sur les systèmes d'information, les acteurs locaux oubliant qu'un objet connecté à Internet abolit instantanément toute frontière physique ou géographique.

Face à ces vulnérabilités croissantes, l'ancrage territorial du CSIRT CyberCorsica s'est avéré déterminant. L'implantation d'un relai local a permis d'instaurer la proximité et la légitimité nécessaires pour briser ce faux sentiment de sécurité et éveiller une véritable prise de conscience.

De plus, l'intervention du CSIRT au cœur même des territoires permet de lisser les inégalités d'accès à l'information et à l'assistance qui existaient historiquement entre les deux grands bassins de population à l'intérieur de l'île.

4- Les territoires français d'Amérique

Les territoires français d'Amérique — Guadeloupe, Martinique, Guyane, Saint-Martin, Saint-Barthélemy et Saint-Pierre-et-Miquelon — font face à une vulnérabilité cyber structurelle résultant d'un faisceau de fragilités économiques, sociales et géostratégiques. Avec plus de 90 % d'entreprises constituées de TPE de 0 à 2 salariés, une **forte dépendance aux importations** pour les équipements, les logiciels et la maintenance, ainsi qu'un **risque élevé d'illectronisme** identifié par l'INSEE, le tissu économique et social reste particulièrement exposé. La faiblesse persistante de la formation initiale et continue limite par ailleurs l'émergence d'un vivier local de compétences, ce que confirme l'**étude de maturité réalisée par l'ACCYB en 2023**, évaluant le niveau global à **D-** [40].

Cette vulnérabilité structurelle se manifeste concrètement : **plus de 50 % des collectivités territoriales des six territoires ont été touchées par une attaque majeure** ces dernières années. Face à cette pression opérationnelle, et anticipant les objectifs fixés par l'ANSSI en 2022, l'ACCYB a fait de la création du **CSIRT-ATLANTIC** une priorité stratégique, afin de doter les territoires d'un dispositif local de veille, d'assistance et de réponse à incident adapté à leur éloignement géographique et à leurs réalités spécifiques.
Dans ce contexte, l'ACCYB articule son action autour de **cinq domaines prioritaires** :

- la **représentation** des intérêts et des réalités ultramarines ;
- l'**acculturation**, incluant la sensibilisation et la formation, notamment via CyberEDAntilles et l'ACAI lauréat de l'AMI-CMA ;
- un **observatoire** assurant le suivi de la maturité ;
- la **souveraineté et la résilience**, notamment sur les enjeux de connectivité dans un contexte de dépendance aux câbles sous-marins étrangers ;
- et la **réponse à incident**, structurée autour du CSIRT-ATLANTIC.

L'ensemble de ces éléments fait de la cybersécurité un enjeu majeur de résilience économique, sociale et souveraine pour les territoires français d'Amérique.

IV - Coopération et structuration, actions dans les territoires

A- Coordination au sein des territoires

1- Synergie avec les Campus Cyber Territoriaux

Le développement des CSIRT s'accompagne de la dynamique de déploiement des **Campus Cyber Territoriaux** dans les régions. Certains Campus sont dans une structure commune avec leur CSIRT, d'autres sont séparés mais les synergies sont toujours présentes.

La **Région Haut de France** porte une politique publique Cyber engagée auprès des entreprises et des collectivités au travers de la mise en place d'un Pass Cyber en 2015 et bénéficie d'un écosystème régional important au travers du CITC, un Centre de Ressource Technologiques (CRT) dédié aux numériques qui va porter la mise en place du premier Campus Cyber Territorial, labellisé en juin 2022 [45]. Une Task Force, constituée du CITC, du Campus Cyber HDFLM, du CSIRT, du délégué de l'ANSSI, de la Gendarmerie, de l'OFAC et de Centres de Gestion, opère pour sensibiliser l'ensemble du territoire régional. Une gouvernance unique a été mise en oeuvre pour le pilotage du **Campus Cyber Hauts de France Lille Métropole**, du CSIRT et du CITC.

En octobre 2022, la **Région Nouvelle-Aquitaine**, l'Agence de développement et d'innovation de Nouvelle-Aquitaine (ADI-NA), le CLUSIR et le GIP Cybermalveillance créent le **Campus Régional de Cybersécurité et de Confiance Numérique**. Celui-ci a pour vocation d'être un Campus Cyber territorial et une de ses premières missions sera la mise en place du CSIRT territorial [18].

Dès 2022, la **Région Normandie** envisage de créer un Campus Cyber territorial. Le projet se développe au côté du CSIRT normand « Normandie Cyber ». Le campus **Normandie Cyber** est créé et labellisé en septembre 2024. En 2025, le Campus et le CSIRT Normandie Cyber sont intégrés à une nouvelle structure, Normandie Numérique, qui fédère l'ensemble des acteurs et actions de la filière numérique régionale.

En 2024, la **Région Bretagne** lance son Campus Cyber baptisé Bretagne Cyber Alliance [46]. L'ambition de ce campus cyber régional est de « faire rayonner l'écosystème cyber breton comme une référence en Europe pour un monde numérique plus sûr».

Le projet se veut collectif et implique six collectivités : la région Bretagne, Brest Métropole, Lannion Trégor Communauté, Lorient Agglomération, Rennes Métropole et Golfe du Morbihan – Vannes Agglomération.

Bretagne Cyber Alliance s'engage à travers quatre missions concrètes :

- Accompagner la croissance des acteurs économiques de la filière
- Conforter la performance de la recherche et de l'innovation
- Répondre aux besoins de compétences
- Diffuser la cybersécurité dans toute la société bretonne

C'est dans cette dernière mission que le CSIRT de Bretagne est engagé aux travers de différentes actions sur l'ensemble du territoire breton.

En **Région Provence-Alpes-Côte-d'Azur**, le **Campus Cyber Territorial Région Sud** [47], inauguré en novembre 2024, est structuré autour de quatre pôles territoriaux : Euromed Marseille, Sophia Antipolis, Salon-de-Provence et Toulon.

En **Région Grand Est**, le campus cyber Grand Est, **Hub Grand Est Cybersécurité**, structure son organisation autour d'un réseau de pôles d'excellence à Reims, Metz, Nancy et Mulhouse. Le Hub porte la politique régionale en cyber et coordonne les dispositifs existants tels que le CSIRT régional et l'EDIH *(European Digital Innovation Hub)*. Il a été labellisé en novembre 2025 [48].

Dès 2019, la **Région Occitanie Pyrénées - Méditerranée** lance un projet d'accompagnement des organisations du territoire en matière de cybersécurité et de fédération de la filière Cybersécurité, porté par son agence de développement économique AD'OCC : « Cyber'Occ ». Le **centre de cybersécurité d'Occitanie Cyber'Occ** [45] est créé en juin 2022 pour mettre en place ses actions. En plus d'être le CSIRT d'Occitanie, Cyber'Occ développe des missions qui par essence sont celles d'un campus cyber territorial. Cyber'Occ est labellisé Campus Cyber Territorial en novembre 2025 [48].

2- Régions, Métropoles et Communautés de communes et d'agglomération,

Chaque CSIRT est porté par sa Région et a créé des liens avec les collectivités les plus importantes de son territoire.
Le CSIRT Nouvelle-Aquitaine a créé des Centres de ressources Cyber dans 8 départements sur 12.
L'Occitanie a plusieurs collectivités importantes parmi ses adhérents.

B- Autres partenariats / coopérations

1- La filière Cybersécurité au niveau régional

Tous les CSIRT territoriaux ont identifié les acteurs de la réponse à incident présents sur leur territoire et en capacité d'aider les victimes professionnelles qui contactent les CSIRT. Une partie des CSIRT territoriaux a aussi construit des annuaires de tous les prestataires Cybersécurité, voire de la filière (écoles, avocats spécialisées, acteurs RGPD ...)

Certains CSIRT et leur Campus permettent à ces acteurs d'adhérer et de bénéficier d'accompagnement, de faire partie d'une animation locale dans leur domaine, d'avoir accès à des stands collectifs à des tarifs préférentiels lors de salons professionnels comme le FIC à Lille, le Cyber Show à Paris, le CBC à Toulouse... C'est le cas de la Nouvelle-Aquitaine, de l'Occitanie, de Grand-Est, de Hauts-de-France, de Bretagne, de Normandie, de la Réunion.

Le Campus Nouvelle-Aquitaine permet à des entreprises d'avoir une domiciliation de R&D.

2- Autres partenariats

Les CSIRT territoriaux développent des partenariats avec les réseaux de CCI, avec les fédérations d'entreprises CPME, Medef, différentes agences comme l'ARS (Agence Régionale de la Santé), les GRAdeS (Groupement régional d'appui à la e-santé), les syndicats mixtes énergie, eau, les OPSN (Opérateur Public de Service Numérique), les pôles de compétitivité, les agences de développement économique, les associations nationales comme Hexatrust, le CLUSIR, l'Afnor, les barreaux d'avocats, les conseils régionaux des experts comptables...

C- Participation à des projets européens ou bassins géographiques

Les Pôles européens d'innovation numérique (ou EDIH) [49] sont issus d'une **initiative de l'Union européenne en faveur de la numérisation des entreprises**. Chaque Pôle européen d'innovation numérique **regroupe sur un territoire donné des acteurs de la transformation numérique** des entreprises, notamment des TPE-PME et peut mettre en avant un axe cybersécurité.

Certains CSIRT sont associés à leur EDIH regional :

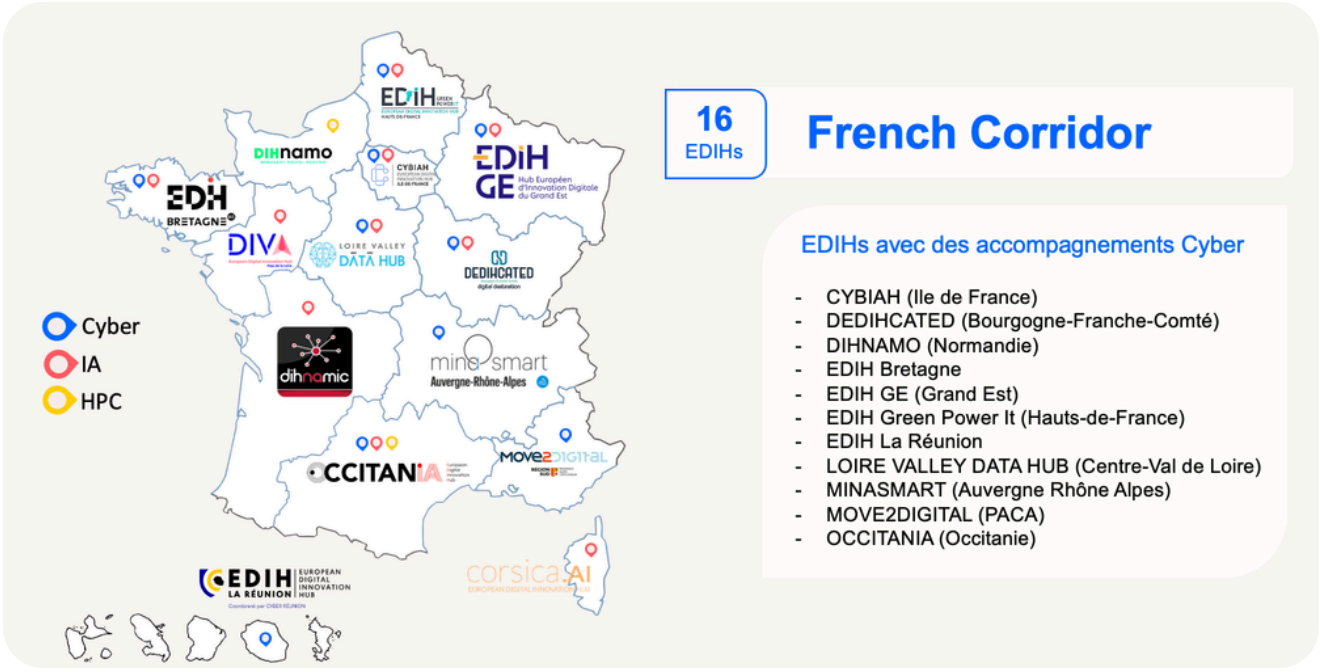
- Le CSIRT Occitanie, Cyber'Occ est membre du consortium **OccitanIA** [50] et réalise des audits de maturité cyber pour les entreprises.

- L'**EDIH La Réunion** [52] complète l'action du CSIRT en soutenant et en finançant la mise en œuvre de dispositifs concrets de sécurisation des systèmes d'information, à l'issue d'une phase de diagnostic réalisée à l'aide de l'outil Cyber Départ, au service de la transformation numérique et de la résilience des acteurs du territoire.

- Le CSIRT Hauts de France est engagé dans le European Digital Innovation Hub **GreenPowerIT** [51] piloté par le CITC. Il apporte son soutien dans les diagnostics Cyber pour l'ensemble des acteurs régionaux.

- Normandie Numérique coordonne l'EDIH **DIHNAMO**, dont fait partie Normandie Cyber [53]

- Grand Est Développement porte l'**EDIH GE** [54]



V- Axes de développement et perspectives

A- AMI RALEC : renforcement et enrichissement du réseau des CSIRT Territoriaux

Le 22 août 2025, l'ANSSI lance un appel à manifestation d'intérêt **« Renforcement de l'accompagnement local aux enjeux de cybersécurité »** [55] doté d'une enveloppe de 6,8 millions €. L'objectif est d'encourager au niveau territorial les initiatives permettant de renforcer le dispositif national de cyberdéfense, développé dans la Revue nationale stratégique 2025 [56], et ainsi d'élever le niveau général de cybersécurité au profit des entités les plus vulnérables aux cyberattaques par un accompagnement cybersécurité de proximité et un service d'assistance lors de la survenance d'une cyberattaque, autant sur les démarches réglementaires que techniques et opérationnelles.

Les **CSIRT territoriaux** ont candidaté et ont tous été lauréats [57], ce qui leur permet de continuer et de renforcer leurs actions. Cela permet aussi de compléter le dispositif avec le projet de création de deux nouveaux CSIRT Territoriaux : à **Mayotte** et en Région **Auvergne-Rhône-Alpes**.

B- Objectifs 2026 et feuille de route stratégique

La dynamique des communauté des CSIRT territoriaux va se renforcer en 2026 : organisation de groupes de travail thématiques, construction et déploiement de projets communs.

Les CSIRT vont poursuivre et intensifier leurs actions d'information et de sensibilisation et être un maillon essentiel du dispositif national de réponse aux incidents de sécurité. Ils sont d'ailleurs bien identifiés, dans la stratégie nationale de Cybersécurité 2026-2030 [58] comme acteurs de l'accompagnement aux victimes dans les territoires.
Comme précisé ci-dessus, **deux nouveaux CSIRT** doivent être créés et pourront s'appuyer sur la communauté des CSIRT territoriaux pour leur montée en maturité.

Au vu des typologies d'incidents observés touchant leurs bénéficiaires, les CSIRT travaillent à mettre en place des actions d'informations et des services spécifiques à ces incidents pour permettre aux organisations de leur région d'être mieux préparées et mieux protégées.

Les CSIRT territoriaux vont orienter leurs travaux autour de 3 axes :

- La **mutualisation** des outils et des actions
- La **construction de nouveaux services** pour répondre aux besoins des territoires au regard des menaces observées.
- La **co-construction** d'observatoires de la menace régionale

Les CSIRT territoriaux sont aussi concernés par le projet de **loi** relatif à la **« résilience des infrastructures critiques et au renforcement de la cybersécurité »** [59] qui entrera en application prochainement. Cette loi transpose la **directive européenne NIS2** (Network Information Security) [60] sur laquelle les CSIRT sont déjà mobilisés pour expliquer aux organisations de leur région la directive et ses objectifs.

VI- Annexes

A- CARTES D'IDENTITÉ DES CSIRT-TERRITORIAUX

CSIRT ATLANTIC

0970 260 801

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h30 - 13h30 à 17h00

En dehors des horaires et jours fériés : redirection vers le CERT-FR

CSIRT BOURGOGNE-FRANCE-COMTÉ

0 970 609 909

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h30 - 13h30 à 17h00

En dehors des horaires et jours fériés : redirection vers le CERT-FR

BREIZH CYBER

0 800 200 008

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 17h30

contact@breizhcyber.bzh

En dehors des horaires et jours fériés : redirection vers le CERT-FR

CSIRT CYBERCORSICA

04 20 97 00 97

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 8h30 à 12h30 - 14h00 à 17h00

En dehors des horaires et jours fériés : redirection vers le CERT-FR

Formulaire sur le site

CYBERÉPONSE

0 805 69 15 05

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 8h30 à 12h30 - 14h00 à 17h30

En dehors des horaires et jours fériés : redirection vers le CERT-FR

GRAND EST CYBERSÉCURITÉ

0 970 512 525

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 8h30 à 12h30 - 14h00 à 17h30

En dehors des horaires et jours fériés : redirection vers ses partenaires de réponses à incident (service payant)

CSIRT HAUTS-DE-FRANCE

0 806 700 111

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h30 - 14h00 à 17h30

En dehors des horaires et jours fériés : redirection vers le CERT-FR

URGENCE CYBER ÎLE-DE-FRANCE

0 800 730 647

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 8h à 18h00

urgencecyber@iledefrance.fr

Formulaire sur le site

En dehors des horaires et jours fériés : redirection vers le CERT-FR

NORMANDIE CYBER

0 808 800 001

Horaires d'ouverture : Du lundi au jeudi
De 8h00 à 17h00

Le vendredi (hors jours fériés)
De 8h00 à 16h00

contact@normandie-cyber.fr

En dehors des horaires et jours fériés : redirection vers le CERT-FR

CRIC-NA CENTRE DE RÉPONSE AUX INCIDENTS CYBER

0 805 2929 40

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h30 - 14h00 à 17h30

En dehors des horaires et jours fériés : redirection vers le 17Cyber

CENTRE CYBER DU PACIFIQUE

+ 687 505 300

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 8h00 à 16h00

En dehors des horaires et jours fériés : redirection vers le CERT-FR

Formulaire sur le site

CYBER'OCC

0 800 71 13 13

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h30 - 14h00 à 17h30

urgence@cyberocc.fr

En dehors des horaires et jours fériés : redirection vers le CERT-FR

PAYS DE LA LOIRE CYBER ASSISTANCE

0800 100 200

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 17h00

cyberassistance@paysdelaloire.fr

En dehors des horaires et jours fériés : redirection vers le CERT-FR

URGENCE CYBER RÉGION SUD

0 805 036 083

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 18h00

Formulaire sur le site

En dehors des horaires et jours fériés : redirection vers le CERT-FR

CSIRT LA RÉUNION

0262 974 999

Horaires d'ouverture : Du lundi au vendredi (hors jours fériés)
De 9h00 à 12h00 - 13h00 à 17h00

csirt@cyber-reunion.fr

Formulaire sur le site

ANSSI - CERT-FR

32 18

09 70 83 32 18

Horaires d'ouverture : Service disponible 24h/24 et 7j/7

cert-fr@ssi.gouv.fr

B- Taxonomie et Glossaire

2- Glossaire

ANSSI	**Agence Nationale de Sécurité des Systèmes d'Information**
CERT	**Computer Emergency Response Team**

CSIRT	**Computer Security Incident Response Team**
EDIH	**European Digital Innovation Hub**
SI	**Système d'Information**
SSI	**Sécurité du système d'Information**
Evénement de sécurité	**Evénement de sécurité qui a donné lieu à un traitement par un CSIRT ou un CERT**
Incident	**Evénement de sécurité conduit par un acteur malveillant qui a un impact sur le SI d'une victime**
Signalement	**Tout comportement anormal ou inattendu pouvant avoir un caractère malveillant ou ouvrir la voie à une nouvelle action malveillante**

2 - Taxonomie des événements de sécurité

Ingénierie sociale	Stratégie visant à manipuler des personnes afin d'obtenir une information ou la réalisation d'une action.
Compte compromis	Une compromission d'un compte désigne un accès non autorisé à un compte par un attaquant.
Défiguration	Modification de l'apparence d'un site web ou d'un service afin d'afficher des informations nuisant à la victime.
Déni de Service (Ddos)	Attaque informatique ayant pour but de rendre indisponible un service.
Divulgation	Action de dévoiler (sur les réseaux sociaux, dans la presse...), sans son accord, des informations appartenant à une organisation.
Exfiltration de données	Compromission d'un système engendrant l'accès non autorisé à ses informations et leur transfert vers l'extérieur.
Exposition de données	Peut résulter d'une action malveillante, d'une vulnérabilité ou d'une erreur de manipulation.
Hameçonnage	Attaque (ciblée ou non) d'ingénierie sociale destinée à leurrer la victime (par mail, sms...) pour l'inciter à communiquer des données personnelles ou réaliser une action.
Maliciel	Programme malveillant qui a pour objet d'endommager ou de mettre hors service un système, par exemple le rançongiciel.
Typosquattage et usurpation d'identité	Attaque qui consiste à imiter l'identité d'une entité de confiance (physique ou non) et qui utilise des sources légitimes ou non, afin de tromper les victimes.

*Seule la taxonomie des événements les plus rencontrés par les CSIRT est présentée.

VII-BIBLIOGRAPHIE

[1] https://ssi.gouv.fr

[2] - https://cyber.gouv.fr/actualites/le-dispositif-national-de-cybers%C3%A9curit%C3%A9-se-renforce-gr%C3%A2ce-aux-centres-de-r%C3%A9ponse-%C3%A0-incident-aux-niveaux-territorial-sectoriel-et-minist%C3%A9riel/

[3] - https://www.lemagit.fr/etude/Un-RSSI-face-au-stress-dune-cyberattaque-lexemple-de-la-Ville-de-Marseille

[4] - https://www.economie.gouv.fr/presentation-plan-relance

[5] - https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite

[6] - https://cyber.gouv.fr/csirt-territoriaux

[7] - https://adnormandie.fr/normandie-cyber/

[8] - https://adnormandie.fr/le-dispositif-de-reponse-a-incidents-de-cybersecurite-normandie-cyber-est-operationnel/

[9] - https://www.csirt-bfc.fr/

[10] https://www.ternum-bfc.fr/actualites/le-nouveau-pole-arnia-cybersecurite

[11] - https://cybersecurite.grandest.fr/

[12] - https://www.grandestdeveloppement.fr/wp-content/uploads/2023/02/02-14-23_CPresse_Lancement-GrandEstCybersecurite.pdf

[13] - https://www.cyberocc.com/en-cas-durgence/

[14] - https://www.laregion.fr/La-Region-Occitanie-lance-Cyber-Occ-un-centre-d-expertise-regional-dedie-a-la

[15] - http://csirt-hdf.fr/

[16] - https://www.hautsdefrance.fr/communique-de-presse-le-centre-de-reponse-aux-incidents-cyber-csirt-des-hauts-de-france-est-operationnel/

[17] - https://www.campuscyber-na.fr/
[18] - https://entreprises.nouvelle-aquitaine.fr/actualites/un-campus-regional-pour-la-cybersecurite-et-la-confiance-numerique
[19] - https://www.paysdelaloire.fr/economie-et-innovation/entreprise/mon-organisation-subit-une-cyberattaque

[20] https://www.breizhcyber.bzh/

[21] - https://urgencecyber.iledefrance.fr/
[22] - https://www.cybereponse.fr/
[23] - https://www.centre-valdeloire.fr/comprendre/numerique/cybereponse-le-centre-durgence-regional-dedie-aux-risques-cyber
[24] - https://cyber.corsica/
[25] - https://ambizionedigitale.isula.corsica/inauguration-du-csirt-cybercorsica/
[26] - https://www.urgencecyber-regionsud.fr/
[27] - https://www.accyb.org/fr/FindOutAtlantic
[28] - https://centrecyberpacifique.nc/
[29] - https://gouv.nc/actualites/28-10-2024/lancement-officiel-du-centre-cyber-du-pacifique

[30] https://www.cyber-reunion.fr/csirt/

[31] - https://www.cyber-reunion.fr/actualites/lancement-de-la-marque-regionale-cyber-reunion/
[32] - https://www.cert.ssi.gouv.fr/
[33] - https://cyber.gouv.fr/nous-connaitre/lagence/organisation/cert-fr/
[34] - https://17cyber.gouv.fr/
[35] - https://www.cybermalveillance.gouv.fr/
[36] - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/csirt-territoriaux-17cyber
[37] - https://cyber.gouv.fr/nous-connaitre/ecosysteme/csirt/csirt-sectoriels/
[38] - https://www.intercert-france.fr/
[39] - https://www.usine-digitale.fr/article/intercert-lance-son-incubateur-pour-faire-gagner-en-maturite-les-equipes-de-reponse-aux-cyberincidents.N2211398

[40] https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/

[41] - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025
[42] - https://cyber.gouv.fr/securisation/gestion-de-crise/entrainement-crise/rempar/rempar25/
[43] - https://star-hack.fr
[44] - https://csirt-hdf.fr/actualites/ctf-vidocq-2025/
[45] - https://hdf.campuscyber.fr
[46] - https://www.cyberalliance.bzh
[47] - https://campuscyber-regionsud.fr/
[48] - https://campuscyber.fr/le-grand-est-et-loccitanie-rejoignent-le-reseau-des-campus-cyber-territoriaux/
[49] - https://edih-hdf.eu/

[50] https://www.cyberocc.com

[51] - https://www.edih-occitania.fr/
[52] - https://www.cyber-reunion.fr/edih/
[53] - https://dihnamo.org/
[54] - https://www.grandestdeveloppement.fr/edihge/
[55] - https://cyber.gouv.fr/actualites/appel-%C3%A0-manifestation-dint%C3%A9r%C3%AAt-clos/
[56] - https://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_Actualisation_2025_RNS_FR.pdf
[57] - https://cyber.gouv.fr/actualites/r%C3%A9sultat-de-lappel-%C3%A0-manifestation-dint%C3%A9r%C3%AAt/
[58] - https://www.sgdsn.gouv.fr/publications/strategie-nationale-de-cybersecurite-2026-2030
[59] - https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/

[60] https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/