cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

Présentation du dispositif cybeRéponse

Version 3.3 a

le Centre de Réponse aux Incidents Cyber

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RESSOURCES NUMÉRIQUES PARTAGÉES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

28+

Expérience

Institutions Financières
Institutions Étatiques

10+

Finales DEFCON

Du Championnat du monde des Hackers

04

Vice-Champion du monde

Au CTF du DEFCON

X+

Cryptographie Appliquée

Guillaume Poupard

40+

Certifications

Sécurité | Cybersécurité

120+

Conférences

Sécurité des Systèmes d'information Sensibles et de l'usage de l'IA en cybersécurité

RAPPEL !

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

Risques Majeurs

- Naturels
- Technologiques
- Sanitaires
- Cyber
- Terroriste

Cybercriminalité
Déstabilisation
Sabotage
Espionnage

https://www.info.gouv.fr/risques | 12 MAI 2023

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

AXA Future Risks Report 2024

La cybersécurité reste perçue comme une menace majeure. Malgré un recul en troisième place, contre la deuxième l'an dernier, ce risque figure dans le top 5 de davantage d'experts. Une inquiétude probablement étroitement liée à l'instabilité géopolitique, aux avancées de l'intelligence artificielle et à la dépendance croissante à l'égard des grands fournisseurs.

https://www.axa.com/fr/actualites/2024-future-risks-report| 14 OCTOBRE 2023

Conséquences Majeures

- Financières
- Opérationnelles
- Politiques | Stratégiques
- Juridiques
- Sociales
- Réputation

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

inédite !

La France subit une vague de cyberattaques inédite !

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

40%

des ATTAQUES Cyber visaient des ENTREPRISES !

CERT-FR | InterCert France | Janvier 2023

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

Une avalanche de cyberattaques touche l'Europe

01Net · 1j

En France,

une cyberattaque a lieu toutes les minutes...!

Pascal Gautheron | Président de la CCI Côte-d'Or/Saône-et-Loire | Colloque cybersécurité | 2 MAI 2024

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

Un mystérieux nouveau ransomware menace les entreprises

01Net · 1j

Une attaque par RANSOMWARE toutes les 11 secondes dans le Monde !

Général de division Marc BOGET, ComCyberGend | Mai 2023

98%

des GRANDES entreprises françaises victimes de FUITES sur le web!

ACTU.fr | 4 Juillet 2023

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

SNCF

1'400'000 | lesnumeriques.com | 15 Juillet 2024
SNCF | lesnumeriques.com | 28 Juin 2023
SNCF | 20minutes.fr| 27 Juin 2017

INTER SPORT

52 Go de données sensibles | bfmtv.com | 4 avril 2024
InterSport | lemonde.fr | 6 Décembre 2022

dans 90%

de cas, ce sont leurs PRESTATAIRES qui ont été attaqués !

ACTU.fr | 4 Juillet 2023

ENGIE

100'000 | NUMERAMA.fr | 30 août 2023
Home Services | Clubic.fr | 5 mai 2024

almerys viamedis

33'000'000 | LEMONDE.fr | 8 février 2024

Sidaction ENSEMBLE CONTRE LE SIDA

20% donateurs | leparisien.fr | 28 février 2024

France Travail

43'000'000 | Figaro.fr | 13 Mars 2024

+50% des banques victimes d'une attaque « réussie » en 2024

https://www.lesechos.fr/finance-marches/banque-assurances/cybersecurite-plus-de-la-moitie-des-banques-victimes-dune-attaque-reussie-en-2024-2105640| 03 Juillet 2024

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

free

14'000'000 | zataz.com | 13 Septembre 2023

Free | commentcamarche.net | 09 février 2024

Free | commentcamarche.net | 03 octobre 2024

orange™

Orange | commentcamarche.net | Aout 2024

Orange | commentcamarche.net | Juillet 2024

Orange | commentcamarche.net | Décembre 2023

1 584 clients | zataz.com | 05 Septembre 022

1'300'000 | letemps.ch | 07 mai 2014

800'000 | letemps.ch | 02 février 2014

SFR

1'400'000 | lesnumeriques.com | 15 Juillet 2024

50'000 | ouest-france.fr | 3 Septembre 2024

100% des opérateurs !

ZATAZ a repéré une vente de 4 millions de comptes Orange (ID + Mots de passe) ; 3 millions de Free ou encore 800.000 SFR

zataz.fr | 17 Juillet 2024

« «Ce qui est inédit ce sont 800 points administratifs qui sont attaqués d'un coup»»

800

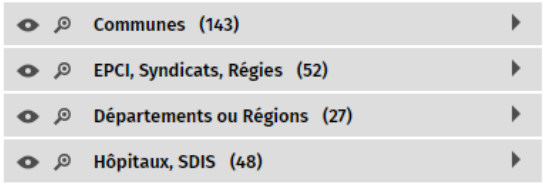
sites ADMINISTRATIFS ont été ciblés !

Stanislas Guerini | Ministre de la Transformation et de la Fonction publiques | 12 Mars 2024

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

“Nous avons découvert cette déclaration de guerre, mercredi matin.”

David Samzun | Maire de Saint-Nazaire | 9 Avril 2024



https://umap.openstreetmap.fr/fr/map/attaques-cybersecurite-aupres-dorganismes-publics_821557#6/46.890/-1.835

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

```
Domain Name: APPREDICAUP.COM
Registry Domain ID:
Registrar WHOIS Server: whois.fastdomain.com
Registrar URL: http://www.fastdomain.com
Updated Date: 2024-04-24T10:04:40Z
Creation Date: 2024-04-24T10:02:33Z
Registrar Registration Expiration Date: 2025-04-24T10:02:33Z
Registrar: FastDomain Inc.
Registrar IANA ID: 1154
```

DGFIP

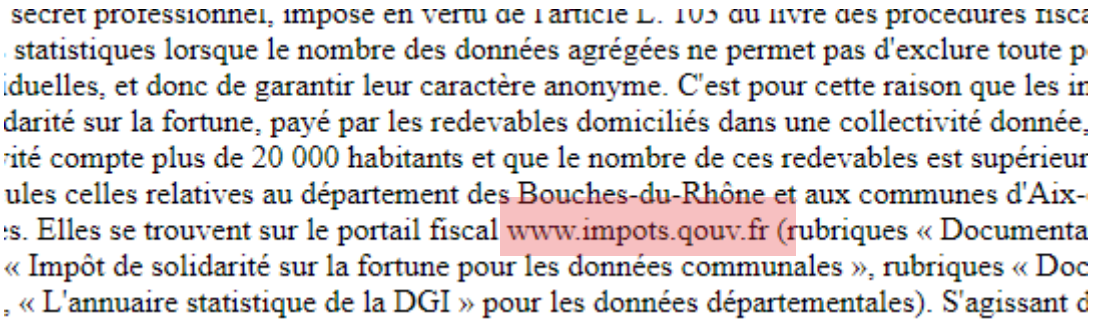
Usurpation du site de la Direction Générale des Finances Publiques

Signalement ANSSI | cybeRéponse | 25 AVRIL 2024

https://cfspart-idp-impots-gouv.appredicaup.com/oauth2/d8e33/

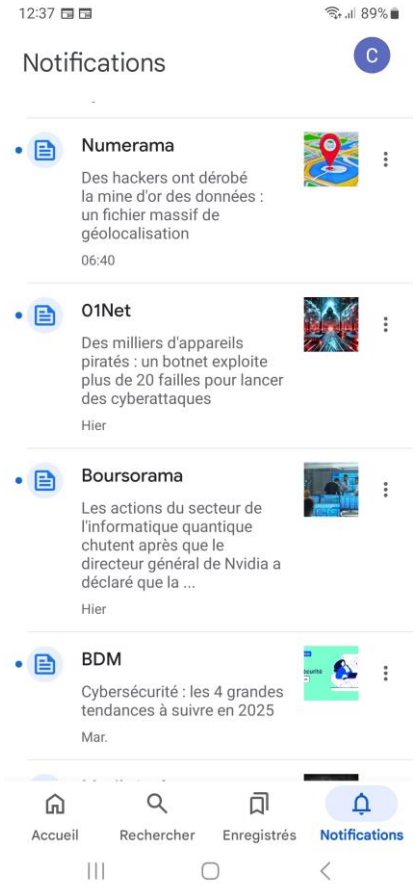
cybeRéponse

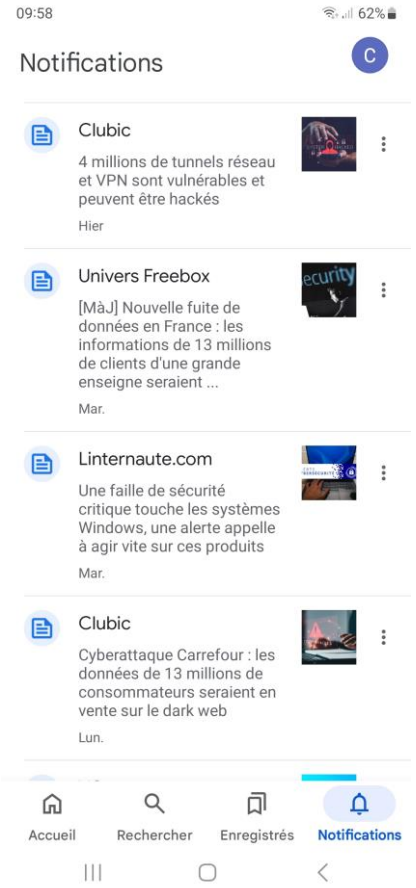
CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE


secret professionnel, impose en vertu de l'article L. 103 du livre des procédures fisca
statistiques lorsque le nombre des données agrégées ne permet pas d'exclure toute p
iduelles, et donc de garantir leur caractère anonyme. C'est pour cette raison que les in
darité sur la fortune, payé par les redevables domiciliés dans une collectivité donnée,
rité compte plus de 20 000 habitants et que le nombre de ces redevables est supérieur
ules celles relatives au département des Bouches-du-Rhône et aux communes d'Aix-
s. Elles se trouvent sur le portail fiscal www.impots.qouv.fr (rubriques « Documenta
« Impôt de solidarité sur la fortune pour les données communales », rubriques « Doc
, « L'annuaire statistique de la DGI » pour les données départementales). S'agissant d

Modification d'un site de l' Assemblée Nationale

https://****-impots-qouv.fr/ | https://questions.assemblee-nationale.fr/q12/12-113574QE.htm


12:37
89%
Notifications
C
Numerama
Des hackers ont dérobé la mine d'or des données : un fichier massif de géolocalisation
06:40
01Net
Des milliers d'appareils piratés : un botnet exploite plus de 20 failles pour lancer des cyberattaques
Hier
Boursorama
Les actions du secteur de l'informatique quantique chutent après que le directeur général de Nvidia a déclaré que la ...
Hier
BDM
Cybersécurité : les 4 grandes tendances à suivre en 2025
Mar.
Accueil
Rechercher
Enregistrés
Notifications


09:58
62%
Notifications
C
Clubic
4 millions de tunnels réseau et VPN sont vulnérables et peuvent être hackés
Hier
Univers Freebox
[MàJ] Nouvelle fuite de données en France : les informations de 13 millions de clients d'une grande enseigne seraient ...
Mar.
Linternaute.com
Une faille de sécurité critique touche les systèmes Windows, une alerte appelle à agir vite sur ces produits
Mar.
Clubic
Cyberattaque Carrefour : les données de 13 millions de consommateurs seraient en vente sur le dark web
Lun.
Accueil
Rechercher
Enregistrés
Notifications

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

100 %

des cyberattaqués avaient un ou plusieurs prestataires !

“Cela n’arrive qu’aux autres… jusqu'au jour où les autres c’est VOUS ! ”

Citation Anonyme

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

“La confiance n'exclut pas le contrôle ”

Vladimir Ilitch Lénine | 1870-1924

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

Mais ça continue encore et encore

C'est que le début d'accord, d'accord...

Francis Cabrel | Encore et Encore | 1985

Réponse

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RESSOURCES NUMÉRIQUES PUBLIQUES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

TIERS DE CONFIANCE

Le GIP-cybeRéponse COORDONNE et CENTRALISE la réponse aux incidents de cybersécurité de la région Centre-Val de Loire, FAVORISE la montée en compétence de son écosystème cyber par son ANIMATION, favorise le rayonnement des acteurs cyber locaux, CONTRIBUE à la diffusion et aux partages d'informations cyber et permet l'établissement et le suivi des STATISTIQUES d'Incidentologie cyber à l'échelle régionale.

Mission de service publique d'intérêt général - le centre de régulation cyber et des services spécifiques réservés aux bénéficiaires adhérents

PÉRIMÈTRE D'INTERVENTION PAR DISPOSITIF

	CYBER MALVEILLANCE .GOUV.FR	cybeRéponse CENTRE-VAL DE LOIRE	RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité / ANSSI
Particuliers	✓		
Entreprises	TPE ⟷	PME | PMI | ETI Associations Employeuses	
Collectivités		✓ Petites et Moyennes	Métropoles, Départements, Régions
Services publics locaux		✓	
Services étatiques			✓
OIV (opérateurs d'importance vitale) & OSE (opérateurs de services essentiels)			✓

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

PRINCIPAUX SERVICES

numéro d'information générale:

02 19 230 466

numéro d'urgence cyber

0 805 69 15 05

numéro d'information générale:

02 19 230 466

INFORMATION

RÉACTION à l'URGENCE

ORIENTATION & SUIVI

RÉSILIENCE | RETEX

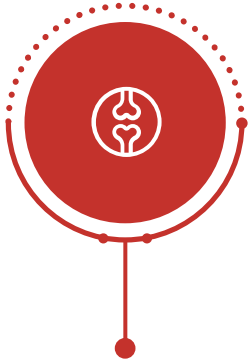
& STATISTIQUES

AMONT **ACTION** **AVAL**

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

ACCOMPAGNEMENT AUX PREMIERS SECOURS D'URGENCE CYBER

0 805 69 15 05



RÉPONSE à l'URGENCE

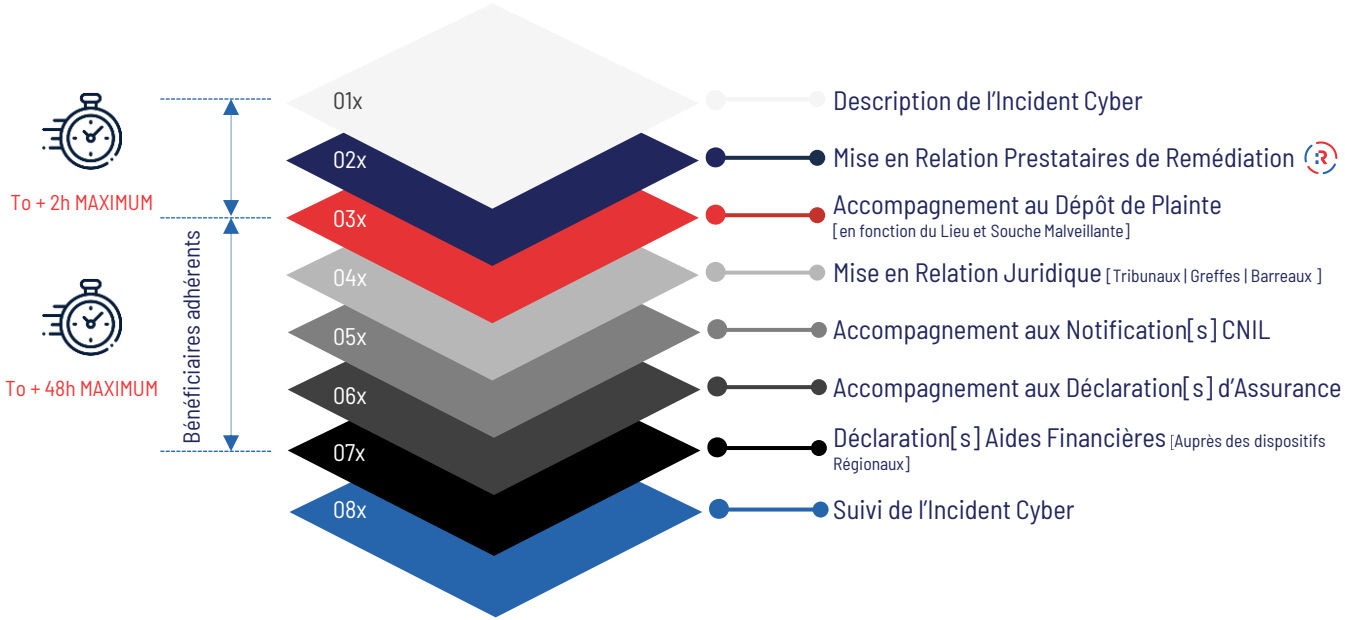
ORIENTATION & SUIVI

- Une QUALIFICATION de premier niveau, basée sur la TAXONOMIE OFFICIELLE de l'Agence Nationale de la Sécurité des Systèmes d'Information
- Une MISE en PLS CYBER et un accompagnement aux premiers secours d'urgence
- Une MISE EN RELATION avec des prestataires cyber de REMÉDIATION, de préférence régional, référencés et certifiés dans les deux heures suivant la déclaration de l'incident,
- Un ACCOMPAGNENT au dépôt de plainte
- Un SUIVI de l'incident jusqu'à sa complète résolution.

ACTION

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

DOSSIER INCIDENT CYBER | Confidentiel | en moins de 48h



cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

PRESTATAIRES

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RÉSIDENCES NUMÉRIQUES PUBLIQUES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

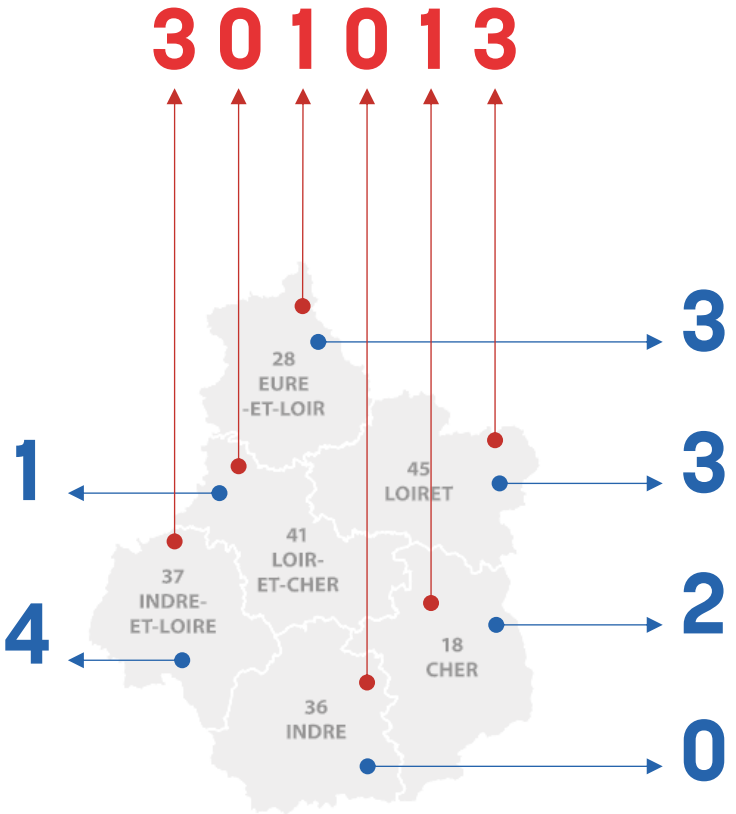
cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

Remédiation

PRESTATAIRES CYBER RÉGIONAUX

8 Prestataires cyber seulement
EN PURE REMÉDIATION

- 24 sont **pleinement RÉFÉRENCÉS**
  - 8 de Remédiation cyber
  - 11 prestataires cyber pour l'Amont | Aval
  - 5 prestataires Informatiques Sécurité
- 17 en **COURS** de **référencement**
- 4 **DEMANDES** de **référencement**



cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

Gendarmerie nationale

PARTIES PRENANTES | CONCERTATIONS | COLLABORATIONS

COMCYBER-MI

PRÉFÈTE DE LA RÉGION CENTRE-VAL DE LOIRE
Liberté Égalité Fraternité

RÉGION CENTRE VAL DE LOIRE

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

POLICE NATIONALE

CYBER MALVEILLANCE .GOUV.FR

OFAC
OFFICE ANTI-CYBERCRIMINALITÉ

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

2 minutes | 2 heures | 2 jours

servir l'efficacité de la réponse à tous ses bénéficiaires adhérents

0 805 69 15 05

du Lundi au Vendredi de 9h à 12h30 et de 14h à 17h30

Bilan

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

...en CHIFFRES | -2 Ans | Volet OPÉRATION | JAN. 2025

+417
DOSSIERS ouverts

36%
DEMANDES d'information

33%
redirections

22%
INCIDENTS MAJEURS

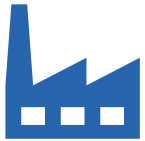
92
INCIDENTS MAJEURS

0.6'
TEMPS MOYEN D'ATTENTE

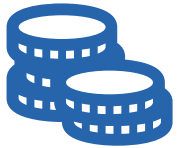
6'
TEMPS MOYEN de conversation

25.4'
TEMPS MAXIMUM de conversation

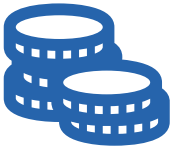
32%
COLLECTIVITÉS



68%
ENTREPRISES



0
DÉPÔT DE BILAN



1M°€
FOVI

85%
DÉPÔTS DE PLAINTE

+18
INCIDENTS Majeurs évitées

cybeRéponse
CENTRE DE RÉPONSE AUX INCIDENTS DE CYBERSÉCURITÉ CENTRE-VAL DE LOIRE

Pourcentage de tickets d'incident | par Type | TOP 3 | JAN. 2025

21%
Ingénierie sociale

14%
Maliciel - Ransomware

13%
Typosquattage

barque-populaire.fr
cdiscount.cm
ca-f.fr
parcourup.fr
education-gouv.fr
facebook.net

rnicrosoft.com
leboncoinn.fr
impots.qouv.fr

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

20 & 21 Mars 2025 | Vierzon

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
ASSOCIATION NUMÉRIQUES PUBLIQUES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

« Faire de la sécurité ce n'est pas faire de la cybersécurité » L.H.

RETENEZ

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RESSOURCES NUMÉRIQUES PARTAGÉES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

RETENEZ

0 805 69 15 05

Gendarmerie nationale

POLICE NATIONALE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

CONSIGNES EN CAS DE CYBERATTAQUE

1 DÉBRANCHEZ LA MACHINE D'INTERNET OU DU RÉSEAU INFORMATIQUE

Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.

2 N'ÉTEIGNEZ PAS L'APPAREIL

Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.

3 ALERTEZ AU PLUS VITE VOTRE SUPPORT INFORMATIQUE

Votre support pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.

4 N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS

Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.

5 PRÉVENEZ VOS COLLÈGUES DE L'ATTAQUE EN COURS

Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.

CYBERMAVEILLANCE.GOUV.FR | MAI 2023

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

Exercice[s] de CRISE

cybeRéponse | cybeCrise

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RÉSIDENCES NUMÉRIQUES PUBLIQUES en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu par
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE

“ Si tu veux la paix, prépare la guerre ”

Si vis pacem, para bellum | Origine inconnue

cybeRéponse

CENTRE DE RÉPONSE
AUX INCIDENTS
DE CYBERSÉCURITÉ
CENTRE-VAL DE LOIRE

CYBER

MERCI

PRÉFÈTE
DE LA RÉGION
CENTRE-VAL
DE LOIRE
Liberté
Égalité
Fraternité

Recia
RÉSIDENCES NUMÉRIQUES PUBLIQUES
en Centre-Val de Loire

devup
Centre-Val de Loire
Innovation et développement des entreprises

Soutenu
par

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION
CENTRE
VAL DE LOIRE