CYBER CORSICA CSIRT

CSIRT CYBERCORSICA
À FIANC'À VOI

Veille, réponse à incident, sensibilisation

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

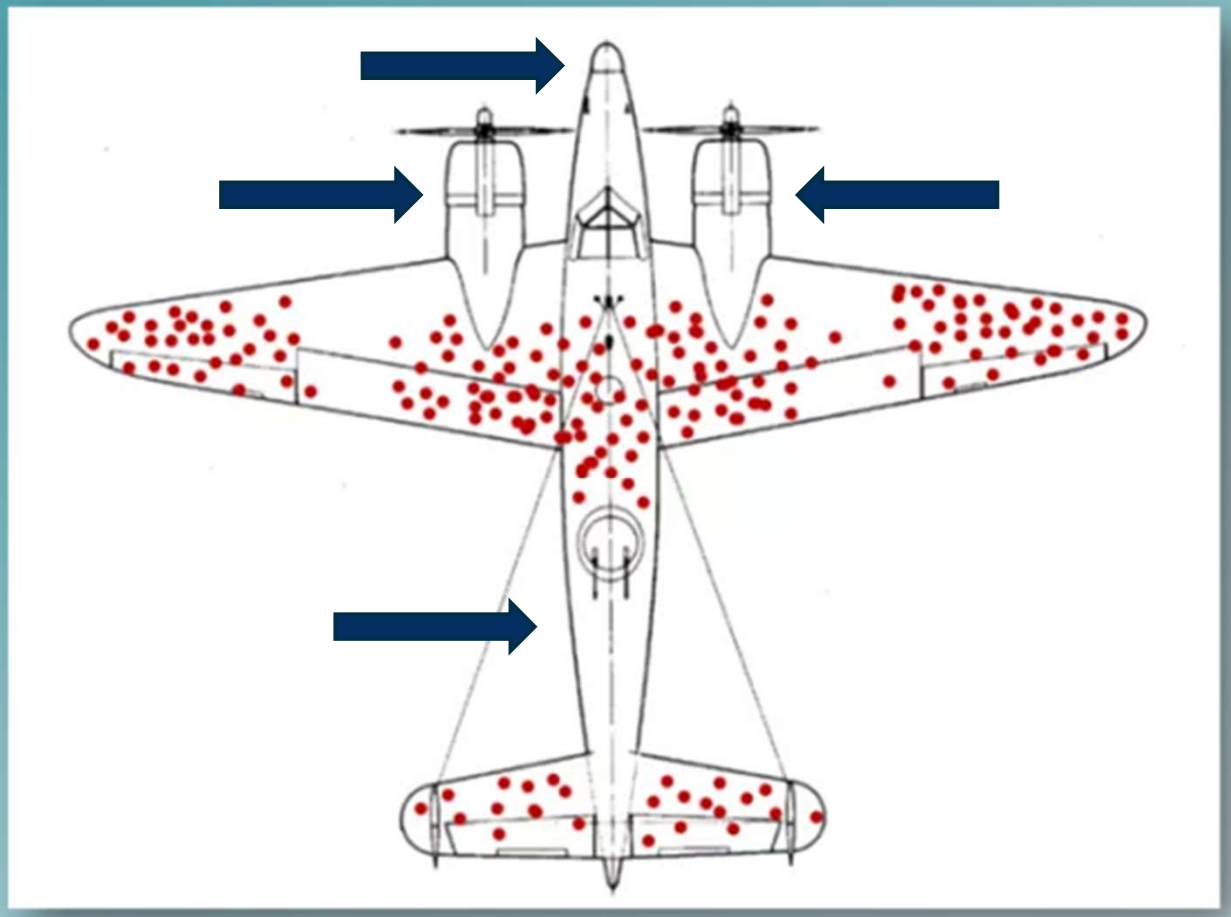
PARLONS AVIATION …

1943 : Abraham Wald, statisticien, étudie les bombardiers revenant de mission.

Les avions montraient beaucoup d'impacts sur les ailes et la carlingue.

L'armée a décidé de renforcer ces zones abîmées.

Wald a montré qu'il fallait renforcer les zones **sans impacts** : moteurs, cockpit, réservoirs… car les avions touchés là ne revenaient pas.



INGÉNIERIE SOCIALE : LE HACK DU CERVEAU

⏳ L'Urgence
"Alerte : Votre compte sera supprimé dans 2h !"
En mode stress, le cerveau court-circuite le cortex préfrontal (logique) au profit de l'amygdale (réaction). On agit avant de réfléchir.

🛡️ Contre-mesure : Respirer, fermer l'onglet, vérifier via un autre canal.

👩‍🏫 L'Autorité
"Message de l'Administrateur ENT ou du Rectorat"
L'humain a une tendance innée à obéir aux ordres d'une figure perçue comme légitime. On vérifie rarement l'expéditeur réel.

🛡️ Contre-mesure : Analyser l'en-tête du mail, ne jamais donner de MDP.

💎 La Rareté / FOMO
"Seulement 100 codes gratuits pour GTA VI"
La peur de rater une opportunité unique (Fear Of Missing Out) pousse à l'imprudence. La valeur perçue occulte le danger.

🛡️ Contre-mesure : Si c'est trop beau pour être vrai, c'est un piège.

🏝️ Biais du Survivant
"Mon cousin le fait et il n'a jamais eu de soucis"
On base son jugement sur les exemples visibles (ceux qui n'ont pas encore été piratés) plutôt que sur les statistiques réelles d'infection.

🛡️ Contre-mesure : Comprendre que l'infection est silencieuse.

ET EN CORSE?

« L'ÎLE NOUS PROTÈGE, MAIS LE RÉSEAU NOUS EXPOSE »

« ICI ON SE CONNAÎT TOUS. SUR INTERNET ON NE CONNAIT PLUS PERSONNE »

LE *BIAIS D'OPTIMISME* EST UN PHÉNOMÈNE BIEN CONNU DES CHERCHEURS EN PSYCHOLOGIE DU RISQUE

IL A ÉTÉ DÉCRIT NOTAMMENT PAR DANIEL KAHNEMAN, AMOS TVERSKY ET PAUL SLOVIC, ET CONFIRMÉ PAR DE NOMBREUSES ÉTUDES EN CYBERSÉCURITÉ.

LA MENACE CYBER : ET LES COLLECTIVITÉS ?

1/3

des victimes de rançongiciel
sont des collectivités
(ANSSI 2024)

72h

délai moyen avant
détection d'une intrusion
(les dégâts sont déjà faits)

500k€

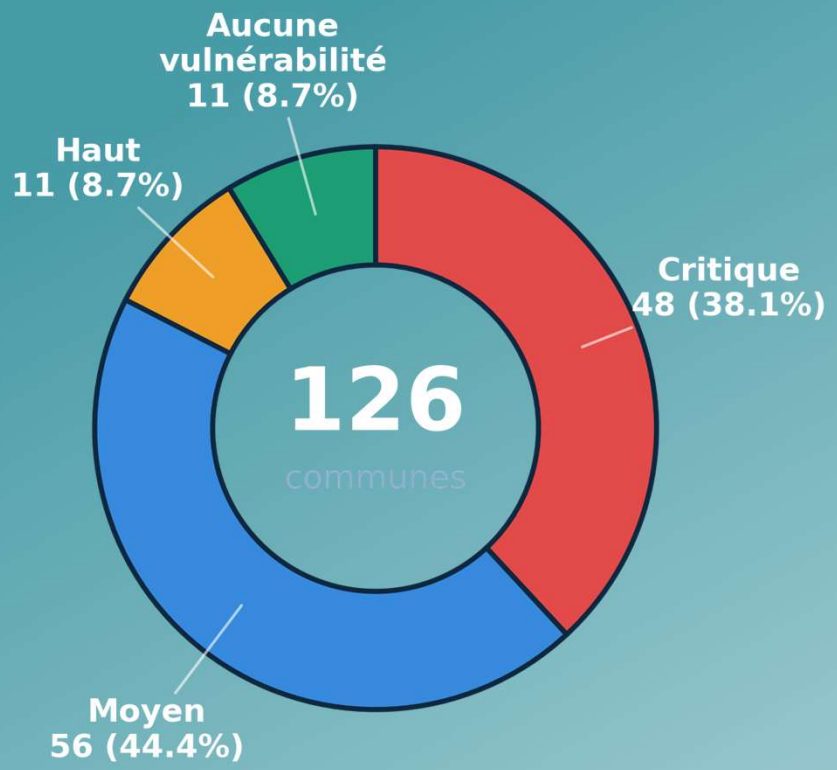
coût moyen d'une
cyberattaque réussie
pour une commune

Les collectivités corses face aux 3 principales menaces

🎯 Menace	💥 Impact concret	⚡ Vitesse
🔒 Rançongiciel	Mairie paralysée, données chiffrées, rançon exigée	Quelques heures
📧 Phishing / fraude fournisseur	Virement frauduleux, fuite de données RH	Immédiat
🌐 Site web vulnérable	Défacement, vol de données citoyens, DDoS, intrusion	En continu

126 SITES DES COMMUNES CORSES SCANNÉS

Niveau de vulnérabilité, par commune (audit Tenable CSIRT CyberCorsica)



91,3 %

des communes corses présentent au moins une vulnérabilité exposée sur Internet

48 communes

présentent une vulnérabilité critique, exploitable immédiatement par un attaquant

Seulement 11 communes (8,7 %) ne présentent aucune vulnérabilité détectée à ce jour.

VOS ADRESSES EMAIL ONT-ELLES FUITÉ ?

Chaque jour, des bases de données piratées sont revendues sur le darkweb. Des outils permettent de tester votre adresse :

IntelBase

Mozilla Monitor

DeHashed

Have I Been Pwned

Si votre adresse est compromise :

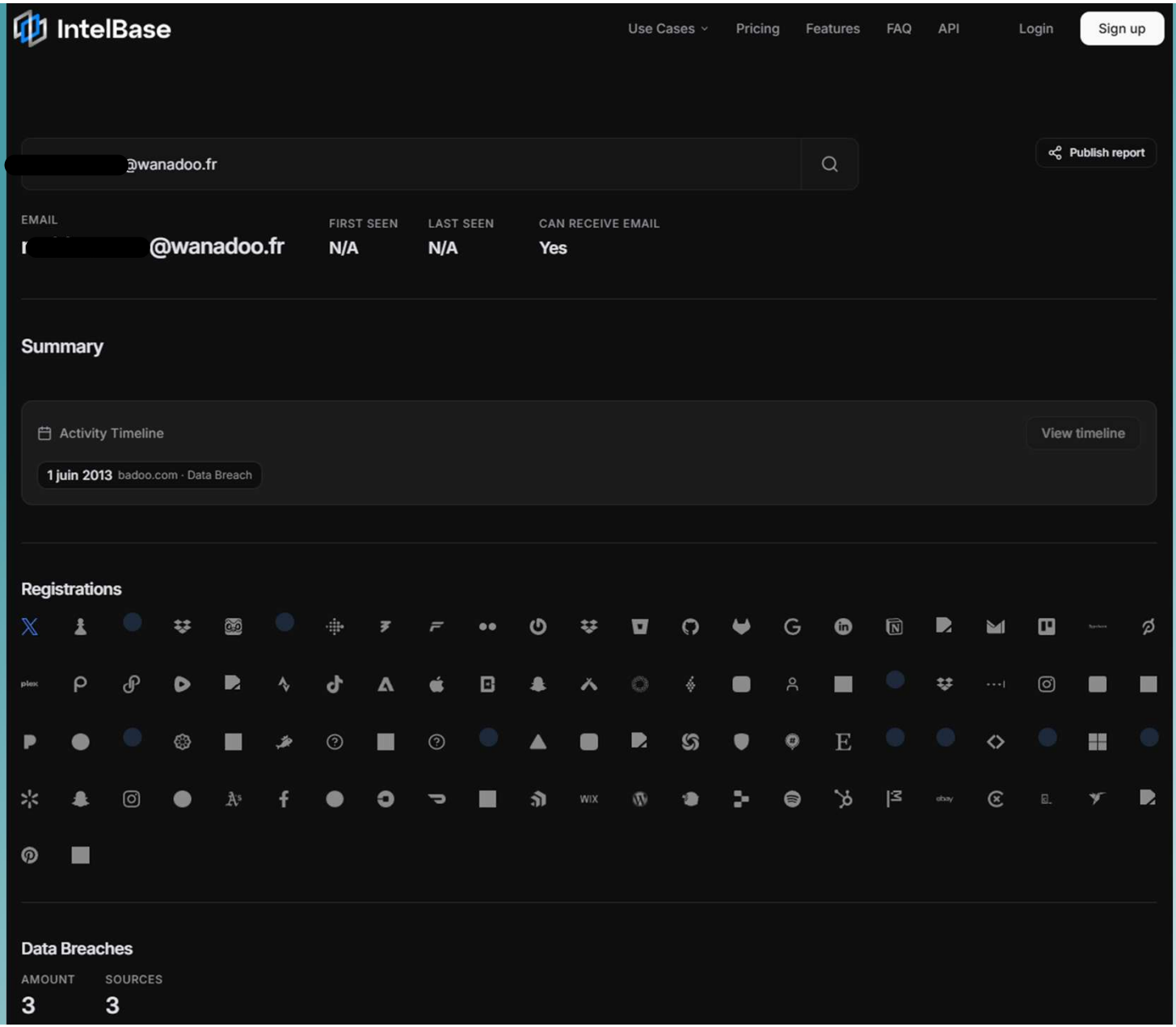
1. Changer le mot de passe immédiatement

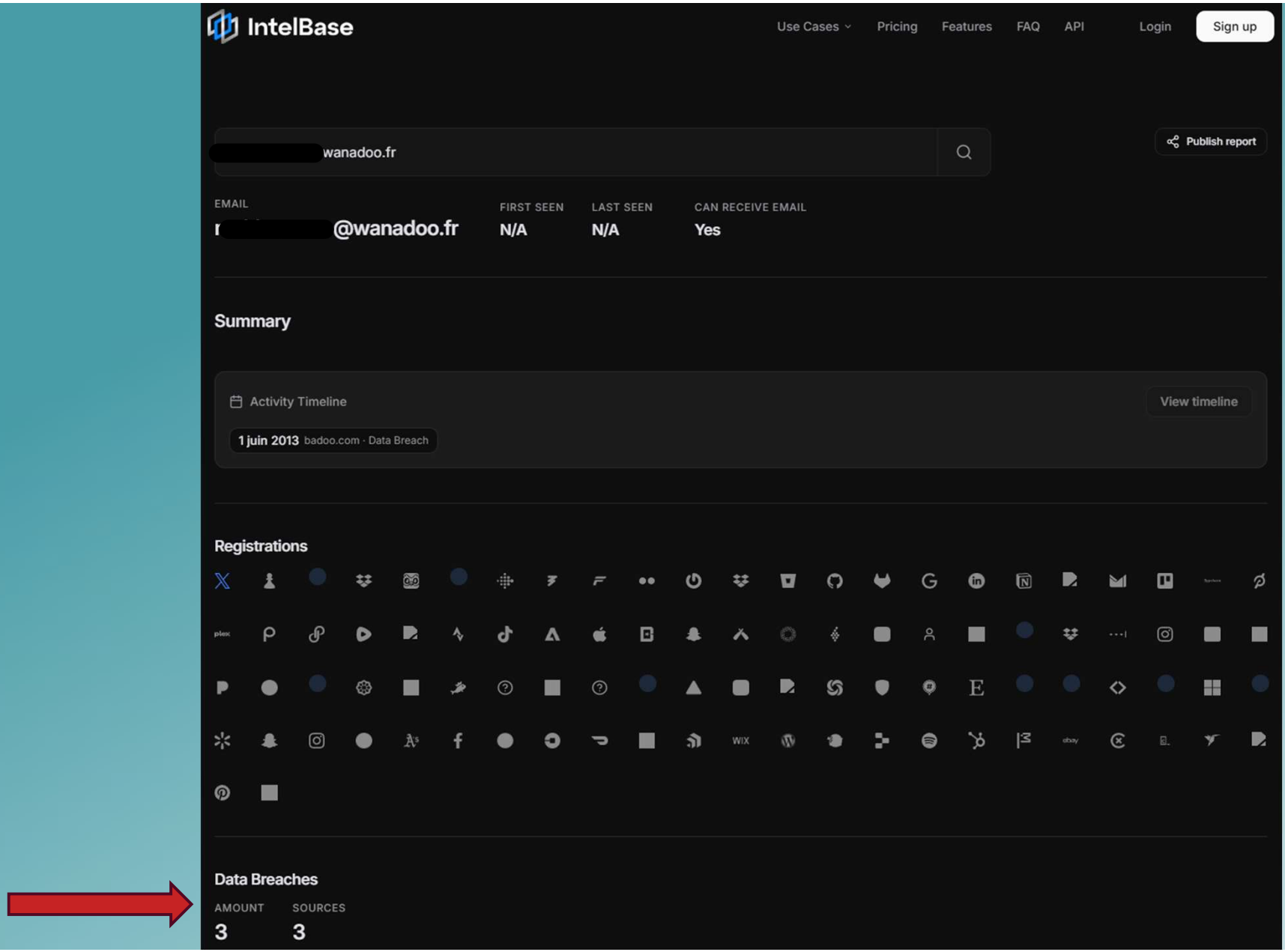
2. Activer le MFA sur ce compte

3. Vérifier les autres comptes utilisant le même mot de passe

4. Contacter le CSIRT si besoin d'aide

⚠ *Attention : ne jamais tester une adresse sans accord préalable du titulaire.*


IntelBase
Use Cases
Pricing
Features
FAQ
API
Login
Sign up
[redacted]@wanadoo.fr
Publish report
EMAIL
[redacted]@wanadoo.fr
FIRST SEEN
N/A
LAST SEEN
N/A
CAN RECEIVE EMAIL
Yes
Summary
Activity Timeline
View timeline
1 juin 2013 badoo.com · Data Breach
Registrations
Data Breaches
AMOUNT
3
SOURCES
3


IntelBase
Use Cases
Pricing
Features
FAQ
API
Login
Sign up
[redacted]wanadoo.fr
Publish report
EMAIL
[redacted]@wanadoo.fr
FIRST SEEN
N/A
LAST SEEN
N/A
CAN RECEIVE EMAIL
Yes
Summary
Activity Timeline
View timeline
1 juin 2013 badoo.com · Data Breach
Registrations
Data Breaches
AMOUNT
3
SOURCES
3

Data Breaches

Showing 1–3 of 3 data breaches

Source	Name	Username	Password	IP Address	Phone Number	Hash
antipublic	-	-	**beatrice2a**	-	-	-
badoo.com 2013-06	-	-	**168470408.0168470408**	-	-	-
collection-2	-	-	**beatrice2a**	-	-	-

🚨 RETEX : FRAUDE AU FAUX ORDRE DE VIREMENT

Cas réel — Mairie de Corse

Le mail arrive

Faux compte de messagerie usurpant l'adresse email du maire

La mise en scène

Demande de reglement d'une facture en attente, avec un caractère urgent

Le virement

8000€

La découverte

Une fois la facture reglée, le maire en est informé, sauf que… Il n'est pas à l'origine de la demande

Les conséquences

Impact financier, procédures, suites judiciaires …

✅ **Ce qui aurait évité la fraude ?**

U CSIRT CYBERCORSICA HE A FIANC'À VOI
VOUS N'ÊTES PLUS SEULS FACE À LA MENACE.

Réponse à incident

En cas de cyberattaque,
nous intervenons en appui
dans les 24h

Observatoire de la menace

Veille, relai des alertes du réseau cyber
corse, rapport des scans de vulnérabilité
fournis

Sensibilisation

Ateliers pour vos agents,
vos élus, adaptés
au contexte insulaire sur demande

04 20 97 00 97

Du lundi au vendredi, 8h30-12h30 / 14h00-17h30 ,
relai du CERT-FR en HNO

contact@cyber.corsica

CYBER CORSICA CSIRT

AVEZ-VOUS DES QUESTIONS?

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE