RFC 2350 – CSIRT cybeReponse

TLP:CLEAR – This document is public by nature and may be freely redistributed.

This document is the reference version. It is written in English, which is the language of record for this profile in the CSIRT/CERT ecosystem. An informative French translation is available at rfc2350-fr.txt; in case of any discrepancy, this English version prevails.

1. Document Information

This document describes the CSIRT cybeReponse in accordance with RFC 2350. It provides basic information about the team, its channels of communication, its responsibilities, and the services it offers.

1.1 Date of Last Update

Version 1.0 – 2026-07-28

1.2 Distribution List for Notifications

There is no mailing list to notify changes to this document. Updates are published at the location indicated in section 1.3.

1.3 Locations where this Document May Be Found

The current version of this document is available at:

- https://cybereponse.fr/rfc2350.txt (English, authoritative)
- https://cybereponse.fr/rfc2350-fr.txt (French, informative)
- https://cybereponse.fr/rfc2350.pdf (PDF rendering)
- https://cybereponse.fr/rfc2350 (HTML rendering)

1.4 Authenticating this Document

This document is signed with the PGP key of the CSIRT cybeReponse (see section 2.8). The detached signature is available at:

- https://cybereponse.fr/rfc2350.txt.asc

1.5 Document Identification

Title:	RFC 2350 – CSIRT cybeReponse
Version:	1.0
Publication date:	2026-07-28
Expiration:	This document is valid until a new version is published, and no later than one year after its publication date (annual review), i.e. 2027-07-28 at the latest.

2. Contact Information

2.1 Name of the Team

Full name: CSIRT cybeReponse – territorial CSIRT for the Centre-Val de Loire region (France)
Short name: cybeReponse

2.2 Address

GIP cybeReponse
3 avenue Claude Guillemin - Batiment F2
BP 36009
45060 Orleans Cedex 02
FRANCE

2.3 Time Zone

Europe/Paris – CET (UTC+1), CEST (UTC+2) during daylight saving time.

2.4 Telephone Number

Emergency line (toll-free, France only, staffed 24/7):
0 805 69 15 05

General / office-hours line (internationally dialable):
+33 2 19 23 04 66

2.5 Facsimile Number

None.

2.6 Other Telecommunication

Secure messaging channels, selected according to the sensitivity of the information exchanged (see section 4.3):

- Mattermost (InterCERT-FR community) – routine coordination, TLP:CLEAR/GREEN only
- Tchap (Matrix – French State) – institutional government contacts, federated inter-CSIRT coordination
- Signal – incident coordination at TLP:AMBER/RED, on explicit request
- FIRST (Matrix) – international coordination via federated Matrix account

2.7 Electronic Mail Address

Incident reporting: csirt@cybereponse.fr (team functional mailbox, not a named individual's mailbox)
General enquiries: contact@cybereponse.fr

2.8 Public Keys and Encryption Information

The CSIRT cybeReponse uses PGP for encrypted and signed communications.

Key ID (long):	0xA6E46B70161273F0
Fingerprint:	26FA 319E 4026 C6AE D83B 03E5 A6E4 6B70 1612 73F0
UID:	CSIRT cybeReponse (RFC2350-2026) <csirt@cybereponse.fr>
Algorithm:	Ed25519 (primary, certification); dedicated Ed25519/Cv25519 subkeys for signing, encryption and authentication, each expiring 2027-12-31 (subject to renewal)
Available at:	https://cybereponse.fr/pgp/cert-cybereponse.asc and keys.openpgp.org (lookup by fingerprint or by <csirt@cybereponse.fr>)

The use of PGP is strongly recommended for any report containing sensitive data (TLP:AMBER and above).

2.9 Team Members

The identity of the CSIRT team lead is not published. It is communicated to authenticated parties on request.

The full list of team members is not public. Members identify themselves to the reporting party during incident handling.

2.10 Other Information

Website: https://cybereponse.fr

The CSIRT cybeReponse is recognised as a territorial CSIRT by ANSSI (the French national cybersecurity agency) under its national programme for regional CSIRT deployment, and is a member of the CERT-FR network. It is not, at this date, a member of InterCERT France, nor listed with TF-CSIRT/Trusted Introducer.

2.11 Points of Customer Contact

Preferred channel:	e-mail to csirt@cybereponse.fr (mailbox monitored by the team).
Emergencies:	the toll-free phone line in section 2.4 is staffed 24 hours a day, 7 days a week.
Office hours:	Monday to Friday, 09:00-18:00 Europe/Paris, excluding French public holidays.

Outside office hours, e-mail reports are handled on the next business day, except for P1-priority incidents (see section 4.1), which are triaged as soon as they reach the team via the 24/7 emergency line.

3. Charter

3.1 Mission Statement

The CSIRT cybeReponse assists its constituency (defined in section

3.2) in the prevention, detection and handling of information security incidents. It favours a proportionate approach suited to small and medium-sized organisations: pragmatic response, actionable recommendations, and coordination with national actors (ANSSI, CERT-FR) when the situation requires it. It operates under strict confidentiality of the information it receives, classified according to the TLP protocol.

3.2 Constituency

The constituency served by the CSIRT cybeReponse consists of territorial local authorities, small and medium-sized enterprises (SMEs), mid-sized companies, and non-profit associations located in the Centre-Val de Loire region (France) that request the CSIRT's assistance or fall within its territorial scope of intervention.

Domains and IP ranges covered are not fixed in advance: they are communicated to trusted parties on request, on a case-by-case basis according to the organisations being assisted.

3.3 Sponsorship and/or Affiliation

The CSIRT cybeReponse is operated by GIP cybeReponse, a "Groupement d'Interet Public" (public interest grouping) under French law, founded by the Prefecture of the Centre-Val de Loire region, the Centre-Val de Loire Region, GIP RECIA, and Dev'UP Centre-Val de Loire (SIREN 938 088 465).

It is recognised as a territorial CSIRT by ANSSI under its national programme for regional CSIRT deployment, and is a member of the CERT-FR network. It is not, at this date, a member of InterCERT France, nor listed with TF-CSIRT/Trusted Introducer.

3.4 Authority

The CSIRT cybeReponse operates under the authority of the management of GIP cybeReponse. It acts towards its constituency in an advisory capacity only: it has no authority to impose measures on the organisations it assists. Implementation of recommendations remains the responsibility of each organisation. In the event of a major incident, the CSIRT may coordinate with, and escalate to, CERT-FR.

4. Policies

4.1 Types of Incidents and Level of Support

The CSIRT cybeReponse handles all types of information security incidents affecting its constituency, notably:

- account or system compromise;
- ransomware and malware;
- phishing and social engineering;
- data leakage or exposure;
- denial of service;
- vulnerabilities reported as affecting the constituency.

The level of support depends on severity, impact on the constituency, and resources available at the time of the report. Indicative prioritisation:

Priority	Situation	Response target
P1	Active incident, major impact (ongoing ransomware, confirmed compromise)	4 business hours
P2	Confirmed incident, no active propagation	1 business day
P3	Suspicion, vulnerability report, advisory request	3 business days

End-to-end support (full forensic investigation, on-site remediation) is provided within the scope of a service agreement (membership); outside such an agreement, the CSIRT provides advice and guidance only.

4.2 Co-operation, Interaction and Disclosure of Information

The CSIRT cybeReponse co-operates with other CSIRT/CERT teams, in particular CERT-FR, and with other relevant partner organisations as appropriate.

All information received is handled according to the Traffic Light Protocol (TLP), version 2.0 (FIRST):

- Information received without a TLP marking is treated by default as TLP:AMBER.
- No personal or technically identifying information is shared outside the constituency without the reporting party's consent, except where required by law.
- Data strictly necessary for incident handling may be shared with other response teams, under the applicable TLP level.

The CSIRT complies with the GDPR in processing personal data related to incidents.

4.3 Communication and Authentication

Channel matrix by TLP level:

Level	Authorised channel	Guarantee
TLP:CLEAR / TLP:WHITE	Unencrypted e-mail, Mattermost (InterCERT-FR)	TLS in transit
TLP:GREEN	Unencrypted or PGP e-mail, Mattermost	TLS; bounded trusted community
TLP:AMBER	PGP e-mail mandatory (csirt@, see 2.8) or Signal	End-to-end encryption
TLP:RED	Signal only, out-of-band, bilateral	E2E + no server-side trace

Instant-messaging channels:

- Mattermost (Community): TLP:WHITE/GREEN only — no E2E, TLS only
- Tchap (French State Matrix instance): native E2E — government

contacts and federated inter-CSIRT coordination
- Signal: emergencies and TLP:AMBER/RED content – E2E, no server-side metadata
- FIRST / international CSIRTs: federated Matrix account (matrix.org, or Tchap where federation is available)

Policy on incident content over Mattermost: no IOC, no technical incident detail, and no constituency data is exchanged over Mattermost Community. These elements are exchanged exclusively by PGP e-mail or Signal.

Correspondent authentication: verification of PGP signature, call-back on a known number, or introduction through a trusted community (InterCERT France, Trusted Introducer / FIRST).

5. Services

5.1 Incident Response

5.1.1 Incident Triage

- Assessment of the authenticity and scope of the report;
- Prioritisation according to the grid in section 4.1;
- Correlation with other known reports.

5.1.2 Incident Coordination

- Identification of the organisations involved;
- Contact with relevant parties (reporting party, hosting providers, ISPs, other CERTs);
- Escalation to CERT-FR where necessary;
- Reports to stakeholders and, in support of the beneficiary, assistance with applicable regulatory notifications (CNIL notification within 72 hours for a personal data breach, NIS2 obligations where applicable).

5.1.3 Incident Resolution

- Remote advice for containment, eradication and recovery;
- Direct technical assistance, within the scope of a service agreement (membership);
- Collection and preservation of evidence, within the scope of a service agreement;
- Post-incident lessons-learned report.

5.2 Proactive Activities

- Distribution of security advisories and alerts to the constituency;
- Vulnerability monitoring for technologies used within the constituency;
- Awareness-raising and training;
- Security hardening support and first-level audits, within the scope of the CSIRT's service offering;
- Secure, traceable document distribution via the SDOP platform (TLP-classified documents).

6. Incident Reporting Forms

There is no dedicated reporting form. Reports are sent by e-mail to csirt@cybereponse.fr (PGP encryption recommended), including as much of the following as possible: dates and times (with time zone), description of the facts, affected systems, observed IP addresses/domains, relevant logs, desired TLP marking, and call-back contact details.

7. Disclaimers

While every precaution is taken in the preparation of the information, notifications and alerts it distributes, the CSIRT cybeReponse accepts no liability for errors, omissions, or damages resulting from the use of the information it provides. Recommendations are provided as-is, without warranty; their implementation is the responsibility of their recipients.

-- End of RFC 2350 profile — CSIRT cybeReponse --