MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

RFC – 2350

(DESCRIPTION OF SERVICES)

TLP	**TLP:CLEAR** TLP: CLEAR information may be shared without restriction.
Reference	CECYBER-GN-CCG-RFC2350-EN
Version	7.3
Date	March 31st, 2023

Commandement de la Gendarmerie dans le cyberespace
4 rue Claude-Bernard
CS 60003
92136 Issy-les-Moulineaux
www.gendarmerie.interieur.gouv.fr

Table of content

VERSION HISTORY

Version & Date	Author	Change description	Pages		
			Add.	Change	Remov.
1.0 18-Sep-22	AMARCHAND	Document creation	**X**		
2.0 22-Sept-22	AMARCHAND	Document update		**X**	
3.0 22-Sept-22	AMARCHAND	Document update		**X**	
4.0 04-Oct-22	AMARCHAND	Document update		**X**	
5.0 06-Oct-22	AMARCHAND	Document update		**X**	
6.0 06-Dec-22	GLEONE	Document update		**X**	
7.0 13-Dec-22	GLEONE	Document update		**X**	
7.1 08-Feb-23	GLEONE	Document update		**X**	
7.2 14-Mar-23	GLEONE	Document update		**X**	
7.3 31-Mar-23	GLEONE	Document update		**X**	

1 ABOUT THIS DOCUMENT

Foreword: This document describes the CECYBER services in compliance with the RFC 2350 document[1].

1.1 Date of Last Update

The current version of this document is version 7.2 and was released on March, 14th 2023.

1.2 Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism, to inform of changes made to this document.

1.3 Location where this Document May be Found

The current and latest version of this document is available from Gendarmerie Nationale's website. Its URL is:
https://www.gendarmerie.interieur.gouv.fr/contact/cert/CECYBER-GN-CCG-RFC2350-EN.pdf

1.4 Authenticating this Document

This document has been signed with the CECYBER PGP key and the signature file is available at the same location as the document itself.

CECYBER public PGP key is given at chapter 2.7 below.

2 CONTACT INFORMATION

2.1 Name of the Team

Short name: CECYBER
Full name: "**Ce**ntre d'analyse et de regroupement des **cyber**menaces"

2.2 Address

ComCyberGend – CECyber
4 rue Claude Bernard
92130 Issy-les-Moulineaux
France

1 RFC 2350 is an IETF Best Current Practice available at: https://www.ietf.org/rfc/rfc2350.txt

2.3 Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4 Telephone Number

+33 (0)788 021 077

2.5 Other Telecommunication

None available

2.6 Electronic Email Address

cecyber@gendarmerie.interieur.gouv.fr

2.7 Public Keys and Other encryption Information

CECYBER PGP public key information are:

- KeyID: 0x9A869AD7
- Fingerprint: B636EDB70E3286B04B1D6F3B442A512A9A869AD7

CECYBER public PGP key is available at the following location:
https://www.gendarmerie.interieur.gouv.fr/contact/cert

2.8 Team Members

The team is composed of security experts who work full-time on CECYBER activities.
The list of the team members is not publicly available.

2.9 Operating Hours

CECYBER can be joined on business hours: Monday to Friday, 9:00AM to 6:00PM.
CECYBER is closed on French public holidays.

2.10 Additional Contact Info

General information about CECYBER can be found at the following URL:
https://www.gendarmerie.interieur.gouv.fr/contact/cert

The section "Contact" on the Gendarmerie nationale public website provides advice to contact us:
https://www.gendarmerie.interieur.gouv.fr/contact

3 CHARTER

3.1 Mission statement

CECYBER is a department part of the Gendarmerie Nationale's cyberspace command (ComCyberGend).

CECYBER monitor clear, underground and dark web in order to identify any new major cyber threats or emerging threat actors, their structuration, TTP, etc... that would represent a danger towards the French cyberspace. An analysis is performed on the collected information which is turned into cyber intelligence reports made available to the French Cyber ecosystem and judicial police investigators on a need to know basis.

CECYBER missions are to:

- Monitor open and underground sources in order to identify any new major cyber threats and attacks within the French Cyberespace;
- Gather information, analyse and provide cyber intelligence, thematic reports and synthesis;
- Inform French Gendarmerie Nationale Cyber Units, at central and local levels of significant events in this field, and enhance their level of knowledge about the threats, authors and types of attacks;
- Share cyber threat intelligence with other Public Actors and Private Companies and conduct actions to sensitize this ecosystem on Cyber threats;
- Be the go-between between the Gendarmerie Nationale's cyberspace command and cyber security teams in France and around the world;
- Act as an interface between the digital forensics and investigative high-level experts of the Gendarmerie Nationale's cyberspace command and the French CERT/CSIRT community;
- Provide information and anticipation on threats, to proactively reduce the threat risk, and provide assistance, tools and know-how to assist in crisis management

3.2 Constituency

The CECYBER constituency is Gendarmerie Nationale investigation units.

3.3 Sponsorship / affiliation

CECYBER is a public entity of the Law and Order sector. It is owned, operated and financed by the ComCyberGend (Gendarmerie nationale's cyberspace command).
It maintains relationships with different CSIRT-CERTs in France, Europe and beyond.

3.4. Authority

CECYBER operate under the auspices of, and with the authority delegated by, the Commander of the Gendarmerie nationale's cyberspace command. CECYBER strives to work cooperatively with IT Managers, System Administrators, SOC, law enforcement agencies at the European and international level, etc...

CECYBER services are performed by a technical team composed of Officers, NCOs and specialised staff of the French Gendarmerie.

4 POLICIES

4.1. Types of incidents and level of support

CECYBER may be involved in all types of cybersecurity incidents that may occur within its constituencies. The level of support depends on the type and severity of the given security incident, the amount of affected entities and available resources at the time.

CECYBER can then provide contextualised intelligence on threats, attacks and threat actors, incident coordination service and crisis management support.

On a permanent basis, CECYBER informs its constituencies about threats, modus operandi and vulnerabilities, especially new and emerging ones.
Anyone who is aware of a cyber-incident that might have a criminal purpose or origin may contact CECYBER to share information on this incident, its characteristics and, if applicable, authors.

4.2. Co-operation, interaction and disclosure of information

To fulfill their missions, CECYBER develop and maintain communication channels with other organisations and entities, among which other CERT or CSIRT teams, public administrations, private organisations, law enforcement agencies and anti-cybercrime units at the European and International level.

Information provided to CECYBER may be shared with Gendarmerie Nationale entities, as well as with other public or private interlocutors, in compliance with the TLP defined by the information source and national legislation.

A such CECYBER protect sensitive information in compliance with relevant law and regulations that may apply.

- CECYBER apply Traffic Light Protocol (TLP - as define by FIRST: https://www.first.org/tlp/) when sharing information.
- The Gendarmerie is a Law and Order force. As a result, some of the information processed by CECYBER is covered by various protective measures (National Defence Secret, Judicial Investigation Secret, etc...). These protection measures are imposed on the exchanges between CECYBER and their various interlocutors.

4.3. Communication and authentification

The preferred means of communication is email.
For exchanges within the Gendarmerie, CECYBER use the Gendarmerie's own secure messaging system. When sent on non-secure communication channels such as email, sensitive information is encrypted. Unencrypted email can only be used to submit non-sensitive information, and will not be considered as secure.

For the exchange of sensitive information and authenticated communication, CECYBER prefers the use of PGP to encrypt data. CECYBER public PGP key is detailed in Section 2.7.

In view of the types of information that CECYBER usually deal with, telephone will be considered sufficiently secure to be used even unencrypted. However, CECYBER will not exchange highly sensitive detailed information through telephone and ask counterparts to proceed with encrypted emails.

5 SERVICES

5.1. Incident Response

CECYBER are informed about all security incident that occurs in their different constituencies.

CECYBER will assist and liaise with Gendarmerie's entities and Gendarmerie's affiliates in:

- Artifact, incidents, threats and attacks monitoring and knowledge;
- Incident handling, analysis, response, response support and response coordination;
- Crisis management, preparation and training;
- Liaison with counterparts, association, other CERTs and legal, communication and operations for technical security investigation that are in progress.

The level of service provided by CECYBER depends on the ecosystem (SOC, operational entities, forensic team) needs.

However, CECYBER provides the collection, analysis and cross-checking of information on the threats and attacks and will ensure the relevant dissemination of the edited intelligence and related prevention tools.

5.2 Proactive Activities

CECYBER provide their interlocutors with a set of proactive Watch, Monitoring and Intelligence services on the basis of their right to know. This set can include:

- Annual reports on the threats landscape;
- Security advisories;
- Alerts;
- Attack/Threats/Authors datasheets;
- Prevention tools.

6 INCIDENT REPORTING FORMS

CECYBER provide its interlocutors and associated services with the tools, forms and contact points necessary for the most effective, rapid and secure communication.

There is no specific security incident reporting form. Incidents should be reported via encrypted email or deposited in the various relevant databases to which CECYBER has access.

7 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, CECYBER shall not be responsible for any errors or omissions, or for any damages resulting from or arising out of the use of the information contained herein and therein.

END OF DOCUMENT