



# CERT DEFANTS

## RFC 2350

Version 1.0 – 2024-04-24

DATE	VERSION	NOTE	AUTHOR
22/04/2024	1.0	Initial version	Defants

# 1. DOCUMENT INFORMATION

This document contains a description of the CERT DEFANTS in accordance with RFC 2350 specification. It provides basic information about our team, describes its responsibilities and services offered.

## 1.1. DATE OF LAST UPDATE

This is the version 1.0 released on 2024/04/24.

## 1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

## 1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available at:

[https://www.defants.com/app/uploads/2024/04/20240424\\_cert\\_defants\\_rfc2350v1-0.pdf](https://www.defants.com/app/uploads/2024/04/20240424_cert_defants_rfc2350v1-0.pdf)

## 1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of the CERT DEFANTS and can be found at this URL: [https://www.defants.com/app/uploads/2024/04/20240424\\_cert\\_defants\\_rfc2350v1-0.pdf](https://www.defants.com/app/uploads/2024/04/20240424_cert_defants_rfc2350v1-0.pdf)

## 1.5. DOCUMENT IDENTIFICATION

Title: CERT DEFANTS RFC 2350 Version: 1.0

Document Date: 2024/04/24

Expiration: this document is valid until superseded by a later version

# 2. CONTACT INFORMATION



TLP: CLEAR



## 2.1. NAME OF THE TEAM

Short name: CERT DEFANTS

Full name: CERT DEFANTS

## 2.2. ADDRESS

CERT DEFANTS

1137A avenue des Champs Blancs, 35510 CESSON-SEVIGNE

## 2.3. TIME ZONE

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

## 2.4. TELEPHONE NUMBER

+33-222-668-845

## 2.5. FACSIMILE NUMBER

None available

## 2.6. OTHER TELECOMMUNICATION

None available

## 2.7. ELECTRONIC MAIL ADDRESS

[cert@defants.com](mailto:cert@defants.com)

This is a mail monitored by the person(s) on duty for the CERT Defants.

## 2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP is used for functional exchanges with external CERT / CERT.

User ID: CERT DEFANTS <CERT@defants.com>

Key ID: 832D 87D3 7988 48E4

Fingerprint: DOBE5DF5F07F12C2D0CB1A6E832D87D3798848E4

It can be retrieved from one of the usual public key servers.



TLP: CLEAR



## 2.9. TEAM MEMBERS

The CERT DEFANTS representative is François Khourbiga (CEO) (substitute Maxime Lebreton).  
The full list of the team members is not publicly available.

## 2.10. OTHER INFORMATION

None

## 2.11. POINTS OF CUSTOMER CONTACT

CERT DEFANTS prefers to receive incident reports via e-mail through the email address mentioned in 2.7.

Please use our PGP key to ensure integrity and confidentiality.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail. CERT DEFANTS operates during regular business hours (9:00 AM-7:00 PM from Monday to Friday).

# 3. CHARTER

## 3.1. MISSION STATEMENT

The purpose of the CERT is, first, to assist the customer community in implementing proactive measures to reduce the risk of computer security incidents, and second, to assist the customer community in responding to such incidents when they occur.

CERT Defants will operate according to the following key values:

- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues.
- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of proper practices between constituents and peers
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis

## 3.2. CONSTITUENCY

Our constituency includes:



TLP: CLEAR



- DEFANTS digital assets
- DEFANTS vSIRT solutio
- Customers of DEFANTS product and professional services

### 3.3. SPONSORSHIP AND/OR AFFILIATION

CERT DEFANTS is a private CERT in the cybersecurity sector.  
It is owned, operated and financed by DEFANTS SAS.

### 3.4. AUTHORITY

The CERT DEFANTS operates with the authority delegated by the DEFANTS's CEO.

As CERT DEFANTS is aimed to handle incident responses on customers' perimeter, CERT DEFANTS has an advisory role with local security teams and has no specific authority to require any specific action. Any recommendation which CERT DEFANTS may provide will be implemented under the direction of the customer.

## 4. POLICIES

### 4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERT DEFANTS is generally mandated by its customers to handle any type of incident occurring within their own perimeter.

Depending on the type of security incident, CERT DEFANTS will gradually roll out its services, which include incident response and digital forensics.

CERT DEFANTS services include reactive and proactive services:

- Alerts and warnings;
- Incident analysis and forensics approach;
- Incident response assistance and support;
- Incident response and remediation;
- Threat intelligence analysis and sharing.

In addition, CERT DEFANTS liaises and can rely on the expertise and knowledge provided by other Advens services.



TLP: CLEAR



## 4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT DEFANTS exchanges all necessary non-restricted information with other CERTs / CERTs as well as with other affected parties involved in the incident or incident response process.

Incident or vulnerability related information would not be publicly disclosed without the agreement of all involved parties.

## 4.3. COMMUNICATION AND AUTHENTICATION

DEFANTS CERT recommends sending all information through encrypted email.

DEFANTS CERT supports the TLP (Traffic Light Protocol) in order to classify information sharing ability.

## 5. SERVICES

### 5.1. INCIDENT RESPONSE

The DEFANTS CERT provides the following incident response services:

- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response
- Crisis management
- Incident coordination
- Forensic analysis approach

#### 5.1.1. INCIDENT TRIAGE

When an incident is declared to DEFANTS CERT, triage is performed first to assess the seriousness of the impacted assets. Then the incident gets a criticality score. The score can be reviewed during the incident handling and defines the priority of the treatment.

#### 5.1.2. INCIDENT COORDINATION

The incident coordination involves the following services:

- Provide a quick treatment action plan after the incident's detection



- Collection of technical evidence
- Identification of the perimeter impacted by the incident
- Proposition of immediate corrective measures
- Determining the initial cause of the incident

### 5.1.3. INCIDENT RESOLUTION

At the end of an incident, DEFANTS CERT provides:

- Proposition of long-term corrective measures
- Informal feedback to the team concerned by the incident
- A forensic investigation report, when necessary

## 5.2. PROACTIVE ACTIVITIES

DEFANTS CERT offers the following proactive activities services:

- Cyber Threat Intelligence
- Threat Hunting
- Technology watch
- Cyber security alerts publication / blogposts
- Knowledge gathering on cyber threat actors

## 6. INCIDENT REPORTING FORMS

No public form is proposed on our web site to report incident to CERT DEFANTS, but you can directly use the contact e-mail with proper information when needed (using the PGP Key).

In case of an emergency or a crisis, please provide to CERT DEFANTS the following information at least:

- Contact details and organizational information (minimal): name of the person, organization name, email address and telephone number
- IP address(es), FQDN(s), and any other relevant technical element with the associated observations
- Scan results (if any) and/or any extract from the log showing the problem



TLP: CLEAR



## 7. DISCLAIMERS

N/A

