RFC 2350 - CSIRT EXODATA Cyberdefense

Version 1.0 - 20-01-2023

1. Document Information

This document contains a description of the EXODATA Cyberdefense CSIRT as recommended by RFC2350. It presents information about the team, the services offered and how to contact the CSIRT EXODATA Cyberdefense.

1.1. Date of last update

This document is version 1.0 of the EXODATA Cyberdefense CSIRT RFC2350, published on January 17, 2023.

1.2. Mailing list for notifications

Any changes made to this document will be shared through the following channels:

- https://www.exodata.fr/cybersecurite/csirt-as-a-service/uploads/RFC2350
- InterCERT-FR / French network CSIRT - www.cert.ssi.gouv.fr/csirt/intercert-fr

Queries about the updated information in this document has to be sent to the CSIRT EXODATA Cyberdefense team's email address: incidents@exodata-csirt.fr. These exchanges can be secured by the use of PGP infrastructure.

1.3. Places where this document can be found

The latest version of this document can be found on the CSIRT EXODATA Cyberdefense website at the following location: https://www.exodata.fr/cybersecurite/csirt-as-a-service/uploads/

1.4. Authentication and integrity of this document

This document was signed with the PGP key of the CSIRT EXODATA Cyberdefense.
The signature and public key of the CSIRT EXODATA Cyberdefense (Identifier and fingerprint) are available on the CSIRT EXODATA Cyberdefense website: https://www.exodata.fr/cybersecurite/csirt-as-a-service/contact

1.5. Document identification

Title: RFC2350 of the CSIRT EXODATA Cyberdefense
Version: 1.0
Updated: 2023-01-20
Expiry: This document is valid until its next new version is available.

2. Contact Information

2.1. Team Name

Official name: CSIRT EXODATA Cyberdefense
Common name: CSIRT EXODATA

2.2. Address

EXODATA Cyberdefense
CSIRT Team
4 rue Emile Hugot
97490 Sainte-Clotilde

2.3. Time zone

RET / UTC+4 (Meeting Time)

2.4. Phone number

+33 (0)9 71 05 77 59

2.5. FAX Number

Not applicable

2.6. Other telecommunications

Not applicable

2.7. E-mail address

incidents@exodata-csirt.fr

2.8. Public keys and encryption information

CSIRT EXODATA Cyberdefense uses the following PGP key:
User ID: incidents@exodata-csirt.fr
Key ID: 0x81932F45B59FE677
Footprint: DCCA FC27 9CDB 3D71 9D98 6088 8193 2F45 B59F E677

The PGP key can be retrieved from public key servers such as https://keys.openpgp.org/search?q=incidents%40exodata-csirt.fr or directly from the CSIRT EXODATA Cyberdefense website: PGP Key.

2.9. Team Members

The CSIRT EXODATA Cyberdefense team is composed of IT security experts.

The list of CSIRT EXODATA Cyberdefense team members is not publicly available. The identity of its members may be disclosed on a case-by-case basis, on a need-to-know basis.

2.10. Other information

Visit the CSIRT EXODATA Cyberdefense website at https://www.exodata.fr/cybersecurite/csirt-as-a-service for more information.

2.11. Customer Contact Point

The CSIRT EXODATA Cyberdefense is available during business hours, from 8 a.m. to 7 p.m. from Monday to Friday (excluding public holidays).
To reach the CSIRT EXODATA Cyberdefense, the preferred means of communication is by email at the incidents@exodata-csirt.fr address. Please use the PGP cryptographic key of the CSIRT EXODATA Cyberdefense to guarantee the integrity and confidentiality of the information exchanged.
In case of emergency, please specify the [URGENT] tag in the subject field of your email.

3. Charter

3.1. Order of missions

3.2. Beneficiaries

The entities that can benefit from the support of the CSIRT EXODATA Cyberdefense are organizations located in metropolitan France, overseas territories and the rest of the world, belonging to the following categories:

- Multinationals.
- SMEs.
- Mid-caps.
- Local authorities and public institutions.
- Health facilities.

3.3. Affiliation

The CSIRT EXODATA Cyberdefense is a member of the Cyber Campus of Nouvelle Aquitaine.

3.4. Authority

CSIRT EXODATA Cyberdefense operates under the authority of the Director of the Cybersecurity division of the EXODATA group.

4. Policies

4.1. Type of incidents and level of support

The scope of action of the CSIRT EXODATA Cyberdefense covers all IT security incidents affecting the organizations of the territories described in paragraph 3.2 Beneficiaries.
The level of support depends on the type and severity of the security incident in question, the number of entities affected, and the resources available at the time of the event.

4.2. Cooperation, interaction and disclosure of information

The publication of information relating to an incident such as the name of the structure and technical details is carried out only after obtaining the agreement of the named party.
The CSIRT EXODATA Cyberdefense may be required to communicate information to regional CSIRTs or CERT-FR when a structure requests their support. In the same way, information may be shared with a sectoral CSIRT for the purpose of capitalizing on incidents specific to the sector concerned, always with the prior agreement of the client.
All information is transmitted according to its classification and the principle of the need to know.
The CSIRT EXODATA Cyberdefense processes information in secure physical and logical environments in accordance with existing information protection regulations defined by the National Agency for the Security of Information Systems (ANSSI).

4.3. Communication and authentication

The preferred method of communication is e-mail.
For the exchange of sensitive information and authenticated communication CSIRT EXODATA Cyberdefense uses several encryption solutions.
By default, all sensitive communications must be encrypted with our PGP public key detailed in section 2.7.
Unrestricted general information may be transmitted by telephone, regular mail, or unencrypted e-mail.
The CERT EXODATA Cyberdefense respects the Traffic Light Protocol (TLP: https://www.first.org/tlp) which is in the form of WHITE, GREEN, AMBER or RED tags depending on the level of confidentiality of the data exchanged.

5. Services

5.1. Incident Response

The CSIRT EXODATA Cyberdefense will intervene for its beneficiary customers (which have subscribed to the service) as well as all entities experiencing a security incident opportunistically.
Here are the services offered by CSIRT EXODATA Cyberdefense to its customers:

- Crisis management (support & coordination of incident response)
- Communication during incident response
- Incident response (processing & analysis and management of the incident response)
- Forensics (technical analysis and response of artifacts)
- On-site and remote incident response management
- Cyber Threat Intelligence

5.1.1. Triage, incident qualification

- Support for authorities’ notification of the victim of the security incident;
- Collection of information from the reporter in order to qualify the nature of the incident.
- Determine the severity of the impact of the incident / its scope within the information system.
- Categorization of the security incident.

5.1.2. Incident Coordination

- Categorization of information related to the incident.
- Notification of other interested parties on a need-to-know basis.

5.1.3. Incident handling

- Analysis of compromised systems;
- Isolation of compromised machines
- Assistance in the eradication of the cause of a security incident and its impacts.
- Advice for the service restoration plan.
- Establishment of a RETEX

5.1.4. Proactive activities

CSIRT EXODATA Cyberdefense offers proactive services to its customers, including:

- Monitoring services.
- Cybersecurity threat analyses.
- An alert bulletin based on the news for its subscribed customers.

5.1.5. Vulnerability Management

- Analysis of vulnerabilities in the news.
- Writing vulnerability reports to its subscribed customers.

5.1.6. Cyber threat analysis (Cyber Threat Intelligence CTI)

- Collection of Indicators of Compromise (IOC) streams to help subscribed customers and partners detect and prevent threats and analyze incidents.

6. Incident Report Forms

A form to notify the CSIRT EXODATA Cyberdefense of an incident is available on the https://www.exodata.fr/cybersecurite/csirt-as-a-service website at the bottom of the page in the "Contact our CSIRT team" section.

7. Disclaimer

Although every precaution is taken in the preparation of information, notifications and alerts, CSIRT EXODATA Cyberdefense assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained in this document.

If you notice an error in this document, please report it to us by email. These will be corrected as soon as possible.