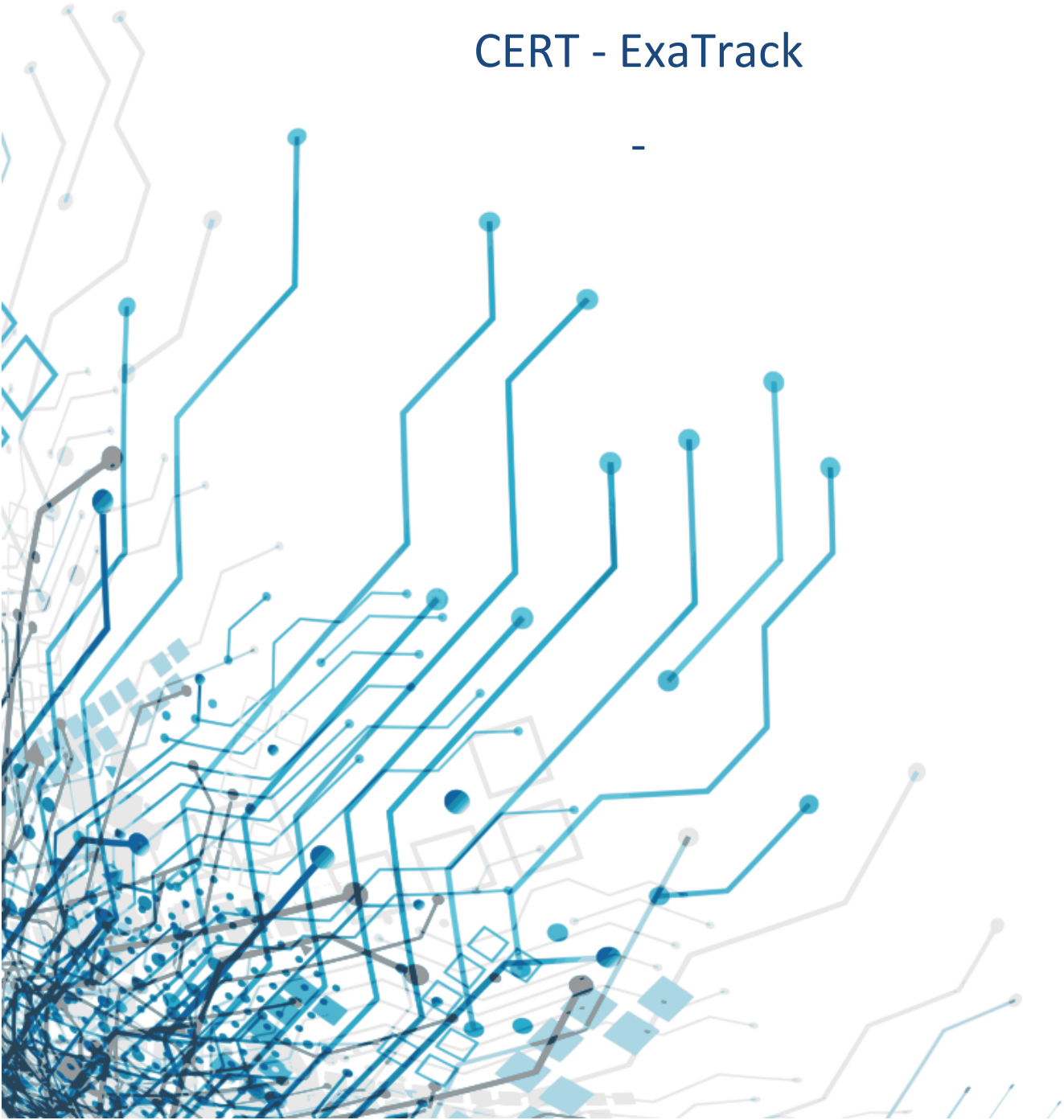
RFC 2350

-

CERT - ExaTrack

-



1. SUMMARY

2. Document Information

2.1. Revisions

Date	Version	Author	Comment
2022/05/10	0.0	TPO	Initial draft
2022/05/17	1.0	TPO/CRO	Administrative information

2.2. Distribution List for Notifications

There is no distribution list for notifications.

2.3. Locations where the Document May Be Found

The current and latest version of this document is available from CERT-ExaTrack's website at the following location:

https://exatrack.com/CERT-Exatrack-RFC2350.pdf

2.4. Authenticating this Document

This document has been signed with the PGP key of CERT-ExaTrack. The signature is available from CERT-ExaTrack's website at the following location:

https://exatrack.com/CERT-ExaTrack-RFC2350.pdf.sig

2.5. Document Identification

Title: CERT-ExaTrack – RFC 2350

Version: 1.0

Document Date: 2022-05-17

Expiration: this document is valid until superseded by a later version.

3. Contact Information

3.1. Name of the Team

CERT-ExaTrack

3.2. Address

ExaTrack SAS

19 RUE DES PETITS CARREAUX

75002 PARIS

FRANCE

3.3. Timezone

CET/CEST

3.4. Telephone Number

Available on request.

3.5. Facsimile Number

Not available.

3.6. Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving your company, please contact us at

cert@exatrack.com

3.7. Other Telecommunication

Not available.

3.8. Public Keys and Encryption Information

CERT-ExaTrack uses the following PGP Key:

- ID: 0x2D834B73A24DAE94
- Fingerprint: 6F 2F BB 6D FD B7 28 4D 14 98 DF C2 2D 83 4B 73 A2 4D AE 94

The public key can be obtained on https://exatrack.com/public.asc

The key can be retrieved at any time from applicable public key servers such as https://pgp.circl.lu/ .

The key shall be used whenever information must be sent to CERT-ExaTrack in a secure manner.

3.9. Team Members

CERT-ExaTrack's team leaders are Stéfan Le Berre and Clément Rouault.

The team consists of IT Security Analysts.

3.10. Other Information

General information about CERT-ExaTrack services can be found at the following URL:

https://www.exatrack.com

3.11. Points of Contact

The preferred method to contact CERT-ExaTrack is by sending an email to the following address:

cert@exatrack.com .

A security analyst can be contacted at this email address during hours of operation.

CERT-ExaTrack's hours of operation are usually restricted to regular French business hours

(Monday to Friday 10:00 to 18:30).

Out of office hours operations in case of emergency.

4. Charter

4.1. Mission Statement

CERT-ExaTrack is a private CERT team delivering Security services, mainly in France and Europe.

4.2. Constituency

CERT-ExaTrack primary constituency is composed of all the elements of ExaTrack Information System: its users, its systems, its applications and its networks.

However, notwithstanding the above, CERT- ExaTrack's services are also delivered to a secondary constituency.

As a commercial CERT, the CERT- ExaTrack also provides services to its Customers Community.

4.3. Sponsorship and/or Affiliation

CERT-ExaTrack is part of ExaTrack: https://exatrack.com/

CERT-ExaTrack maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis

4.4. Authority

For internal matters, CERT- ExaTrack operates under the authority of the CEO of Exatrack.

For external incidents, CERT- ExaTrack coordinates security incidents on behalf of its constituency, and only at its constituents' request.

5. POLICIES

5.1. Types of Incidents and Level of Support

CERT-ExaTrack addresses all types of computer security incidents impacting the confidentiality, integrity, availability of its constituency IT assets.

Depending on the security incident, CERT-ExaTrack's expertise may cover - but is not limited to the areas of incident response – digital forensics, malware analysis, strategical, tactical and operational threat intelligence.

The level of support given by CERT-ExaTrack will vary depending on the severity of the security incident or issue, its potential or assessed impact, the type of constituent, and the available CERT-ExaTrack resources at the time of the incident.

5.2. Co-operation, Interaction and Disclosure of Information

CERT-ExaTrack supports the Information Sharing Traffic Light Protocol version 1.1 (ISTLP, see https://www.trustedintroducer.org/ISTLPv11.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

5.3. Communication and Authentication

CERT-ExaTrack protects sensitive information in accordance with relevant regulations and policies within France and the EU.

CERT-ExaTrack respects the sensitivity markings allocated by originators of information communicated to CERT-ExaTrack.

CERT-ExaTrack also recognises and supports the ISTLP version 1.1.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

6. Services

6.1. Digital Forensics and Incident Response (DFIR)

CERT-ExaTrack performs digital forensics activities whenever necessary, including but not limited to log analysis, memory forensics, physical/virtual drive forensics and network forensics along with the malware analysis activities, which may result from identified forensic needs.

CERT-ExaTrack performs incident response for its constituency and customers. The incident response service as developed by CERT-ExaTrack covers the following phases of the Incident Response process:

- Preparation,

- Identification

- Containment

Incident resolution is left to the responsible administrators within the constituency.

However, CERT-ExaTrack may offer support and advice on request.

6.2. Development of Security Tools

CERT-ExaTrack develops security tools for its own use, to improve its services and support its activities as needed. These security tools can be used by other members of its constituency or by members of the larger CERT, CSIRT, SOC and broader information security community.

6.3. Proactive activities

CERT-ExaTrack provides proactive services such as :

- Threat Intelligence
- Research and Development
- Training services

7. Incident Reporting Forms

No local form has been developed to report incidents to CERT-ExaTrack.

If possible, please provide the following information:

- Contact details and organizational information, such as person or organization's name, address and contact information
- Email address, phone number, PGP key if available
- Date and time when the incident was detected
- Incident description
- Affected assets, impact
- IP address(es), FQDN(s), and any other relevant technical element or comment
- Actions taken so far

8. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-ExaTrack assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.