

RFC-2350

Expectations for Computer
Security Incident Response

FORENSIC



DOCUMENT IDENTIFICATION

Page Number	11
CLASSIFICATION & DIFFUSION	TLP CLEAR

DOCUMENT VERSION

VERSION	DATE	AUTHOR	DESCRIPTION	APPROVED BY
1.0	02/08/2024	Thomas BOURTHOUMIEUX	First release	N/A
2.0	24/07/2026	Kévin MARTIN	Second version	Thomas BOURTHOUMIEUX



Table of contents

1. Document information.....	5
1.1. Date of last update	5
1.2. Distribution List for Notifications.....	5
1.3. Locations where this document may be found.....	5
1.4. Authenticating this document.....	5
1.5. Document identification.....	5
2. Contact Information.....	5
2.1. Name of the Team	5
2.2. Address.....	5
2.3. Timezone	6
2.4. Telephone Number.....	6
2.5. Facsimile Number	6
2.6. Other Telecommunications	6
2.7. Electronic mail address	6
2.8. Public Keys and Encryption Information.....	6
2.9. Team Members	6
2.10. Other Information	7
2.11. Points of Customer Contact.....	7
3. Charter.....	7
3.1. Mission Statement.....	7
3.2. Constituency	8
3.3. Sponsorship and/or Affiliation	8
3.4. Authority	8
4. Policies	8
4.1. Types of incidents and Level of support	8
4.2. Co-operation, Interaction and Disclosure of Information.....	9
4.3. Communication and authentication.....	9
5. Services.....	9
5.1. Incident Response	9
5.1.1. Incident triage	9



5.1.2.	Incident Coordination.....	10
5.1.3.	Incident Resolution	10
5.2.	Proactive activities.....	11
6.	<i>Incident reporting forms</i>	<i>11</i>
7.	<i>Disclaimer.....</i>	<i>11</i>



1. Document information

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

1.1. Date of last update

The current version of this document is version 2.0 and was released on 24/07/2026.

1.2. Distribution List for Notifications

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

1.3. Locations where this document may be found

The current and latest version of this document is publicly available at ITrust's website at: https://www.itrust.fr/cert_itrust_rfc-2350.

1.4. Authenticating this document

This document has been signed with the PGP key of CERT ITrust. The signature and our public PGP key (ID and fingerprint) are available on our website: <https://www.itrust.fr/cert/>. This document's integrity can be checked using the `[CERT_ITrust]_RFC-2350.pdf.asc` file available at the same URL.

1.5. Document identification

Title : « [CERT_ITrust]_RFC-2350.pdf »

Version :2.0

Document Date : 24/07/2026

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

2. Contact Information

2.1. Name of the Team

CERT ITrust

2.2. Address



ITrust company has different premises in France. The CERT team is physically located in the company's office in Labège at the following address:

CERT ITrust, 1000 L'Occitane, 31670 Labège, France

2.3. Timezone

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

2.4. Telephone Number

+33(0)5.67.34.67.83 (Ask for the CERT Itrust)

2.5. Facsimile Number

Not Applicable (N/A)

2.6. Other Telecommunications

Not Applicable (N/A)

2.7. Electronic mail address

If you need to contact us about an information security incident or a cyber-threat targeting or involving CERT ITrust, one of its customers or your entity, please contact us at: cert@itrust.fr.

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT ITrust.

User ID	CERT ITrust <cert@itrust.fr>
Key ID	0x77BBBD67E7BF3529
Fingerprint	9632 7558 67C8 D356 7237 6327 77BB BD67 E7BF 3529

The public PGP key is available at the following location: <https://www.itrust.fr/cert>

2.9. Team Members

The CERT ITrust team consists of IT security experts.

Name	Role	Contact information
Thomas BOURTHOUMIEUX	SOC Operational Director	Not disclosed



Kévin MARTIN

CERT Team Technical Manager

Not disclosed

The list of the other team members is not publicly disclosed. The identities of team members may be revealed on a case-by-case basis, depending on need-to-know requirements.

2.10. Other Information

See our web site at itrust.fr for additional information about CERT ITrust.

2.11. Points of Customer Contact

The preferred method for contacting the CERT ITrust is via email at cert@itrust.fr. If possible, use our PGP cryptographic key to ensure integrity and confidentiality of communications.

In case of emergency, please use the [URGENT] tag in the subject field in your email to smoothen the processing of your query. For better understanding, please include in your contact query some context elements about the incident and your expectations regarding the CERT ITrust support.

The CERT ITrust can be contacted during its hours of operation between 9 AM and 6 PM CET or CEST based on the year's period. Requests outside this period are only proceeded for clients that subscribe to an on-call service.

3. Charter

3.1. Mission Statement

ITrust's CERT provides cybersecurity services to ITrust, its partners, and its customers. It's a team used for internal purposes by ITrust that also offers services to external entities. The CERT analysts aim to provide guidance during cyber crisis, investigate security incidents, keep track and manage vulnerabilities and build general and detailed knowledge of the cyber threat landscape

- **Incident Response:** provide an efficient and quick reaction to ongoing or emerging cybersecurity incidents within its perimeter by offering technical support.
- **Analysis and Reporting:** analyze and investigate security incidents to produce detailed reports for the stakeholders.
- **Monitoring and Prevention:** monitor and keep track of threats, vulnerabilities and indicators for advising purposes.
- **Coordinate and Collaborate:** collaborate with other teams, internal or external to ITrust such as other CSIRT, security teams, organisms and national authority entities.



ITrust's CERT team is under the authority of Thomas BOURTHOUMIEUX, ITrust's Cyber Defense Director that defined its mission statement.

3.2. Constituency

CERT ITrust primary constituents are all the entities affiliated with ITrust or that already benefit from a managed service from ITrust. This includes public entities such as government entities, administrations, agencies, private companies, and Iliad internal groups.

ITrust's CERT can also provide exceptionally its services to entities that are not engaged commercially with ITrust if they require assistance to handle an IT security incident.

3.3. Sponsorship and/or Affiliation

CERT ITrust is a private CERT in the cybersecurity sector. It is owned, operated, and financed by ITrust and its shareholders.

3.4. Authority

CERT ITrust operates under the authority of ITrust's Cyber Defense Director and CEO.

The CERT team handles incident responses for customers and advises local security teams without having the authority to enforce specific actions. For engaged customers that benefit from Managed Services, a set of technical actions and activities allowed to be performed freely by the analysts is defined contractually. This authority depends on the service provided. Any usage of authority or recommendations made by CERT ITrust will be carried out according to the customer's direction.

Entities that engage with the CERT ITrust in an incident response can delegate for the duration of the incident more authority to the analysts based on their needs and the situation.

4. Policies

4.1. Types of incidents and Level of support

CERT ITrust is generally mandated by its customers to handle any type of incident occurring on their perimeter. The services include:

- 24/7 on-call duty for contractualized customers
- Alerts and warnings
- Incident analysis & Computer Forensics
- Incident response assistance
- Incident containment and remediation



- Vulnerability and malware analysis
- Threat Intelligence analysis and sharing
- On-site operations

4.2. Co-operation, Interaction and Disclosure of Information

CERT ITrust operates under the restrictions imposed by French laws. The CERT Team will cooperate with other Organizations in the field of Computer Security, which may help to deliver its services, especially incident resolution. CERT ITrust uses the Traffic Light Protocol (TLP) and Permissible Action Protocol (PAP) in accordance with ANSSI recommendations.

Incident-related information, such as names and technical details, is not published without the agreement of the stakeholders involved. If not agreed otherwise, supplied information is kept confidential. CERT ITrust will never pass information to third parties unless required by law. For educational purposes and cooperation, the CERT ITrust can publish publicly, or present tools and procedures used by an attacker during an incident. Presented elements can only consist of technical tactics, tools, and procedures used by attackers and cannot contain any customer-related information.

4.3. Communication and authentication

The preferred method of communication is through email. For the exchange of sensitive information and authenticated communication, CERT ITrust uses PGP for encrypting and/or signing messages if possible.

All sensitive communication to the CERT ITrust should be encrypted with our public PGP key as detailed in this document.

5. Services

CERT ITrust assists organizations in their incident and response workflows by providing technical assistance and councils.

5.1. Incident Response

CERT ITrust main field of expertise is to provide technical and operationnal support to entities to mitigate, understand and remediate cyber security incidents.

5.1.1. Incident triage



Incident triage activities intervene during the first steps of the incident. The elements and reports are transmitted to the CERT team through a communication channel and are then processed to define the perimeter, the scale, the nature, and the urgency of the incident.

- **Incident Assessment:** Assess the global context of the incident, link it, if possible, to the current or past threat landscape and plausible attack scenarios. Correlate it to current incidents or events occurring in the perimeter.
- **Verification:** Based on available data sources, logs, events and external research, determine if the behavior reported can be qualified as a security incident and its implications on the perimeter.

This service can include minor and quick technical verifications such as Open-Source research, log analysis and platform data review (EDR, SIEM, ...). However, the objective is not to fully investigate the events but to categorize them, to decide what kind of analysis to perform and the necessity of the study.

5.1.2. Incident Coordination

IT security incidents involve a variable amount of urgency, stress, and resource usage. Good coordination and organization during the incident handling improve response times and work efficiency. The CERT Itrust can provide its expertise on IT security incidents to customers to help them maintain a good organization and information centralization.

- **Characterize information:** Collect, process and provide information related to the incident whether they are used for logistics or technical activities. The artefact collection is performed to ensure optimal data integrity and prevent proof of alteration. The CERT ITrust will respect the information disclosure policy defined by the client and the TLP/PAP markings.
- **Coordination and governance:** Notify the different parties and stakeholders of the incident with context based on the urgency and the stakes of the incident. Based on the incident scale and the customer's internal organization, teams can be divided into different crisis cells that each handles an aspect of the incident: infrastructure operation, company management, technical analysis, communication, ...

5.1.3. Incident Resolution

All analysis is performed to gain comprehension of the incident to the best extent. They aim solely to mitigate and resolve the incident. Incident Resolution services constitute a cycle in incident response. Discoveries are followed by mitigations and recovery until no more traces of the attacker are found in the incident perimeter.

- **Technical assistance:** investigate, analyze and interpret incident related data. This includes forensic analysis of the compromised systems but also all logs available in monitoring systems. Threat hunting or external research to seek additional information can be performed based on the incident.



- **Eradication:** advise and provide recommendations to neutralize the attacker's influence on the comprised platforms. Based on the customer and its tools, authority to mitigate and respond to attacker activities can be delegated to the CERT team during the incident.
- **Recovery:** recommend and aid in restoring the affected systems and services into a fully operational state. Recovered system configuration and security shall be improved to limit and prevent incident resurgence. The CERT analysts support the customer technical teams, but administrative actions and implementation decisions are left to the customer.

5.2. Proactive activities

CERT ITrust coordinates and maintains the following services to the extent possible depending on its resources and availability:

- **Threat hunting:** perform proactive threat hunting search on available monitoring tools to discover potential threats and anormal behavior. Research may be conducted on customers' internal perimeters or on public-known threats.
- **Threat landscape surveillance:** overview, document and survey evolutions of the threat landscape. This includes surveying new vulnerabilities that are published, recent procedures and tools used by attackers and cybersecurity field for general news.
- **Improvement and development:** improve and enrich the CERT team tools and procedures to increase incident response efficiency and capabilities.
- **Education and training:** write technical articles and reports, deliver presentations and workshops to improve and document technical knowledge.

6. Incident reporting forms

CERT ITrust does not have a public incident reporting form.

7. Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, CERT ITrust assumes no responsibility for errors or omissions, or damage resulting from the use of the information contained within.