RFC 2350

Document information

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

Date of Last Update

Version 3.0, published on 2025-02_26

Distribution List for Notifications

Notifications of updates are submitted to our mailing list when appropriate.

Locations where this Document May Be Found

The current and latest version of this document is available at Cyna's website at: https://www.cyna-it.fr/reponse-a-incident

Authenticating this Document

This document has been signed with the PGP key of CynaCERT. The signature and our public PGP key (ID and fingerprint) are available on our website: https://www.cyna-it.fr/reponse-a-incident

Document Identification

- Title: 'RFC2350 – Cyna CERT' Version: 3.0
- Document Date: 2025-02-26

Contact information

Name of the Team

Cyna CERT

Address

10 rue de Penthièvre, 75008 PARIS FRANCE

Time Zone

CET/CEST

Telephone Number

Main number on-call duty: +33 9 70 70 41 81 (24/7)

Facsimile Number

Not applicable.

Electronic Mail Address

cert@cyna-it.fr

Other Telecommunication

- Not applicable.
- Public Keys and Encryption Information
- PGP is used for functional exchanges with Cyna CERT.

- User ID: Cyna CERT (cert@cyna-it.fr)
- Key ID: 0x327487D6
- Fingerprint: F4EC 02C7 B808 28E0 AD10 6E86 56AA CB31 3274 87D6

The public PGP key is published in the following PGP directory: https://keys.openpgp.org/.

Team Members

The Cyna CERT team consists of IT security experts, whose specific members are not publicly disclosed. The identities of these team members could potentially be revealed on a case-by-case basis, adhering to need-to-know restrictions.

Points of Customer Contact

Cyna CERT encourages its customers to submit incident reports by phone at +33 9 70 70 41 81 Alternatively, for those who are not customers of Cyna CERT, the preferred method for submitting incident reports is through email at cert@cyna-it.fr.

We strongly recommend utilizing our cryptographic key to ensure the highest levels of confidentiality and communication integrity. In case of an emergency, kindly insert the [URGENT] tag in the email's subject line. Please note that while Cyna CERT operates 24/7, telephone support is not available during non-business hours.

Charter

Mission Statement

The primary objective of Cyna CERT is twofold: firstly, to aid Cyna's customers in proactively implementing measures that mitigate the risks of computer security incidents, and secondly, to support these customers in effectively responding to any such incidents as and when they arise.

Cyna CERT's mission encompasses prevention, response, and recovery through the following actions:

- Assisting in the prevention of security incidents by providing guidance on the implementation of essential protective measures.
- Disseminating information regarding cyber threats to its stakeholders and partners.
- Overseeing incident response, with the option of collaborating with trusted partners if required. Additionally, Cyna CERT engages in:
- Participation within reliable networks of Computer Security Incident Response Teams (CSIRTs).

Constituency

Cyna CERT's constituents consist of:

- Customers of Cyna.
- Users, networks, and systems affiliated with Cyna's services.

Affiliation

Cyna CERT is part of Cyna.

Authority

- For internal matters, Cyna CERT operates under the authority of the management of the Cyna company.
- For customer incidents, Cyna CERT coordinates security incidents on behalf of its constituency, and only at its constituents' request.

Policies

Types of Incidents and Level of Support

Cyna CERT is prepared to handle a broad range of security incidents affecting its constituency or posing potential threats.

Our level of support covers incidents such as email account compromises, network intrusions (e.g., ransomware), phishing attacks, data exfiltration, denial-of-service (DDoS) attacks, and critical vulnerabilities.

The level of assistance depends on the severity and urgency of the incident: - critical incidents receive 24/7 priority support, moderate incidents are handled during business hours, and emerging threats are monitored with preventive guidance. Whenever necessary, Cyna CERT coordinates with external stakeholders to enhance incident response and mitigation efforts.

Collaboration, Interaction, and Information Sharing

Cyna CERT prioritizes operational coordination and information sharing with CERTs, CSIRTs, SOCs, and other relevant entities to enhance its service delivery and strengthen the security posture of its constituency.

As needed, Cyna CERT collaborates with other CSIRTs, CERTs, and affected third parties within the incident response framework. Any information received is shared internally within Cyna and, where necessary, with cybersecurity service providers and law enforcement agencies, strictly on a need-to-know basis. No information that could identify a Cyna customer will be disclosed externally.

However, anonymized data—such as Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs)—may be shared within cybersecurity communities to improve threat intelligence, reinforce preventive measures, and support investigative efforts.

Communication and Authentication

It is recommended that all emails directed to Cyna CERT be signed using PGP. For emails containing sensitive information, encryption and PGP signing are imperative. Cyna CERT adheres to the Information Sharing Traffic Light Protocol, as established by the French national cybersecurity agency (FIRST TLP).

Services

Incident Response

Cyna CERT offers 24/7 incident response services to our constituents. We assess all incidents related to information and communication technologies. Our team of technical experts conducts thorough and in-depth analysis.

Incident Triage

- Severity Evaluation
- Expert Escalation
- Strategic Leadership

Incident Coordination

- Data Classification
- Selective Notification
- Real-time Channels
- Incident Playbooks
- Team Collaboration
- Communication Updates

Incident Resolution

- Forensic Analysis and Investigation
- Vulnerability Remediation
- Malware Eradication
- Recovery and Rebuilding
- Threat Hunting
- Lessons Learned and Analysis

- Continuous Monitoring and Threat Intelligence Integration
- Stakeholder Communication and Reporting
- Policy and Procedure Refinement
- Training and Awareness

Proactive Cybersecurity Measures

Cyna is committed to delivering proactive cybersecurity services to its clients, encompassing a range of strategic actions such as:

- Security Operation Center detection Services & Capabilities
- Asset Vulnerability Scans
- Active Directory Security Assessment
- Cloud Service Vulnerability Assessment
- Phishing Awareness Campaigns

These proactive measures underscore Cyna's commitment to staying ahead of emerging cyber threats and ensuring the utmost security for its clientele. For an up-to-date listing of services, please refer to the Cyna website at https://cyna-it.fr.

Incident Reporting Forum

- Cyna CERT's team members have access to an internal form designed to facilitate the systematic collection of essential information when responding to an incident call. However, parties reporting security incidents are not required to use specific forms. If feasible, kindly furnish the subsequent details:
- Contact Information: Please provide your contact details, including email address and phone number.
- Incident Timeline:
    - Start Time: Specify the date and time when the incident commenced.
    - Detection Time: Indicate the date and time when the incident was identified.
- Incident Description: Offer a concise yet comprehensive overview of the incident, including relevant contextual details.
- Affected Assets: Enumerate the systems, networks, or assets directly impacted by the incident.
- Impacts: Detail the consequences and potential ramifications resulting from the incident.
- Actions Taken: Outline any actions already undertaken in response to the incident, such as containment efforts or mitigation strategies.

While the internal form streamlines the process for Cyna CERT members, parties reporting incidents need not adhere to specific forms. Providing the aforementioned information will greatly aid in the efficient handling of the incident.

Disclaimers

While Cyna CERT is committed to ensuring accuracy and diligence in the creation of information, notifications, and alerts, it does not accept liability for any errors, omissions, or damages arising from the utilization of the provided information.