TLP:CLEAR

CHEOPS TECHNOLOGY

The Cloud & Data Centric Company

CERT CHEOPS

RFC 2350

VERSION 1.1 – 2026-03-04

1. DOCUMENT INFORMATION

This document contains a description of CERT CHEOPS in accordance with RFC 23501 specification. It provides basic information about CERT CHEOPS, describes its responsibilities and services offered.

1.1. Date of last update

Version 1.1, published on 2026-03-04.

1.2. Distribution list for notifications

There is no distribution list for notifications

1.3. Location where this document may be found

The current and latest version of this document is available from CHEOPS TECHNOLOGY website at:

https://cheops-technology.com/csirt-cyberpatriot

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT CHEOPS. The signature and our public PGP key (ID and fingerprint) are available on our website:
https://cheops-technology.com/csirt-cyberpatriot

1.5. Document Identification

Title: “CERT-CHEOPS-RFC2350_EN”
Version: 1.1
Document Date: 2026-03-04
Expiration: this document is valid until superseded by a later version

2. CONTACT INFORMATIONS

2.1. Name of the team

Official name:
CERT CHEOPS CYBERDEFENSE
Short name:
CERT-CHEOPS

2.2. Address

CHEOPS TECHNOLOGY
37, Rue Thomas Edison
33610 CANEJAN

2.3. Time zone

The time zone associated to the CERT-CHEOPS operations is: **CET/CEST**

2.4. Telephone number

Main number (24/7): +33 (0)7.57.08.77.82

2.5. Facsimile number

Not applicable

2.6. Mailing Address

To report any cybersecurity incident or a cyber-threat targeting, please contact us at the following address: **cert@cheops.fr**

2.7. Public keys and encryption information

PGP is used for secure dialog with CERT CHEOPS.
- **User ID:** cert@cheops.fr
- **Key ID:** 0xF5619CC8
- Fingerprint: 0A6C1808C634AC65D7C13188409C253DF5619CC8

The public PGP key is available at the following location:
https://cheops-technology.com/csirt-cyberpatriot

2.8. Team members

CERT CHEOPS team is composed of IT security experts. The list of CERT CHEOPS team's members is not publicly available. The identity of CERT CHEOPS team's members might be divulged on a case-by-case basis according to the need-to-know restriction.

2.9. Other information

See our web site at https://cheops-technology.com/csirt-cyberpatriot for additional information about CERT CHEOPS.

2.10. Points of customer contact

CERT-CHEOPS prefers to receive incident reports via e-mail at **cert@cheops.fr**.
Please use our cryptographic key to ensure integrity and confidentiality.

CERT-CHEOPS's hours of operation are 24/7.

3. CHARTER

3.1. Mission statement

CERT-CHEOPS is a part of CHEOPS Cybersecurity Division. CERT-CHEOPS's mission is to support its customer community in implementing proactive measures to reduce the risk of cybersecurity incidents, and to provide effective assistance in responding to such incidents when they occur.

The primaries missions of CERT-CHEOPS's are:

- **Prevention** – by delivering awareness programs, best practice guidelines, risk assessments, and proactive security recommendations tailored to customers' environments.
- **Detection** – by deploying and maintaining threat monitoring tools, establishing detection rules, and providing early warning on vulnerabilities or active campaigns.
- **Response** – by coordinating incident response efforts, conducting forensic analysis, containing threats, and supporting stakeholders during security events.
- **Recovery** – by assisting in system restoration, post-incident analysis, and advising on corrective actions to prevent recurrence and strengthen resilience.

3.2. Constituency

The primary beneficiaries of CERT-CHEOPS's services include **Cheops customers** and **Cheops itself**, with services primarily offered in **France** but also internationally for certain customers.

3.3. Sponsoring Organization / Affiliation

CERT-CHEOPS is affiliated to the CHEOPS TECHNOLOGY GROUP.

3.4. Authority

CERT-CHEOPS operates under the authority of Yoann BARILLON, Head of CERT of Cheops Technology Group.

4. POLICIES

4.1. Types of incidents and level of support

CERT-CHEOPS is generally mandated by its clients to manage any type of security incident occurring within their perimeter, whether it involves technical incidents or targeted attacks.
Depending on the nature and severity of the incident, CERT-CHEOPS deploys its services progressively and appropriately, offering solutions ranging from in-depth analysis to full remediation. Its activities cover the entire incident management lifecycle, from detection to resolution.

The services provided by CERT-CHEOPS include both reactive and proactive offerings, as detailed below:

- **Alerts and warnings**: Continuous monitoring and rapid notification of ongoing threats or incidents, with precise alerts to assist in real-time decision-making.
- **Incident analysis and investigation**: Expertise in understanding and analysing incidents, with a detailed approach to identifying the origin and impact on affected systems.
- **Assistance and support in incident management**: Crisis management support, with dedicated teams coordinating and resolving incidents quickly while minimizing operational impact.
- **Incident response and remediation**: Immediate action to contain incidents, restore compromised systems, and implement corrective measures to reduce future risks.
- **Threat analysis, hunting, and intelligence sharing**: Proactive monitoring of emerging threats, hunting for persistent threats, and sharing intelligence on ongoing attacks to enable the entire ecosystem to protect itself effectively.

4.2. Co-operation, Interaction and Disclosure of Information

CERT-CHEOPS acknowledges the importance of sharing information with third parties. The "**need to know**" principle is applied to share only the necessary information with the relevant people or organizations. Additionally, CERT-CHEOPS adheres to the **Information Sharing Traffic Light Protocol** (TLP).
CERT-CHEOPS can exchange information with other entities, such as external SOCs, CERTs, and other cybersecurity teams, to facilitate information sharing. CERT-CHEOPS maintains a privileged dialogue and cooperates closely with cybersecurity entities related to its activities.

4.3. Communication and authentication

Email is the preferred communication method. For exchanging sensitive information and authenticating communication, CERT-CHEOPS uses PGP to encrypt and/or sign messages. All sensitive communication to CERT-CHEOPS should be encrypted with our public PGP key as detailed in Chapter 2.7. If encryption is not necessary, a clear text email will be acceptable.

5. SERVICES

5.1. Incident Response

CERT-CHEOPS provides 24/7 incident response services for its customers. It handles incidents related to information technologies, conducts in-depth technical analyses, and supports its beneficiaries from the earliest warning signs by offering operational assistance to contain, analyze, and remediate incidents throughout their lifecycle.

5.1.1. Incident triage

The incident triage process enables a rapid assessment of the incident's criticality to prioritize its handling and allocate the appropriate resources by:

- Gathering information about the incident, with confirmation or assessment of its nature
- Evaluating the severity of the incident and its scope
- Categorizing the incident according to its type.

5.1.2. Incident coordination

Incident coordination includes the following activities:

- Organizing the resources mobilized during incident management.
- Facilitating communication with other potentially involved sites.
- Communicating with management to explain the situation and the incident's progress.
- Monitoring the actions taken throughout the incident.
- Identifying and assigning tasks to be completed.
- Producing reports to ensure proper follow-up of operations.

5.1.3. Incident resolution

- Conduct specialized expertise tasks, including forensic analysis and network traffic analysis.
- Provide support for eliminating identified vulnerabilities.
- Assist in securing systems to mitigate the impact of the incident and support their restoration.

5.2. Proactive activities

5.2.1. Vulnerability management

As part of its vulnerability management efforts, CERT-CHEOPS implements several actions to help its constituents anticipate and reduce their exposure to threats. These include:

- **Identifying the attack surface** through technical scans to detect exposed services and externally accessible vulnerabilities;
- **Open Source Intelligence (OSINT) monitoring**, aimed at detecting potential data leaks, published exploits, or known vulnerabilities affecting the beneficiaries' technical environment;
- **Issuing remediation recommendations** to support beneficiaries in mitigating identified risks.

5.3. Incident reporting forms

No public form is available on our website to report an incident to CERT-CHEOPS, but you can directly contact our team via email, providing the necessary information (using the PGP key for confidentiality). CHEOPS Technology customers can also use the CHEOPS internal tools to submit events and relevant information.

In case of an emergency or crisis, please provide CERT-CHEOPS with at least the following information, along with the appropriate TLP/PAP:

- Name of the contact, organization name, email address, and phone number
- IP address(es), FQDN(s), and any other relevant technical elements, along with any associated observations or analysis
- **Date and time of the event**: specify the exact date and time when the incident was detected or occurred

This information will enable our team to respond quickly and efficiently to the incident.

5.4. Disclaimers

CERT-CHEOPS will take all necessary precautions and apply its expertise and efforts when preparing, notifying, and alerting about an incident.
However, CERT-CHEOPS takes no responsibility for any errors, omissions, or damages resulting from the use of the information it provides.