RFC 2350

CERT Capgemini

@capgeminicert ♠ cert.global@capgemini.com

Date of publication	2022-05-24
Version	1.1
Author	Antonin HILY
Updated by	Nicolas TICHTINSKY

TABLE OF CONTENTS

Diffusion 3
Document Information 4
Date of Last Update 4
Distribution List for Notifications 4
Locations where this Document May Be Found 4
Authenticating this Document 4
Document Identification 4
Contact Information 5
Name of the Team 5
Address 5
Time Zone 5
Telephone Number 5
Electronic Mail Address 5
Other Telecommunications 5
Public Keys and Encryption Information 5
Team Members 5
Other Information 5
Points of Contact 5
Charter 6
Mission Statement 6
Constituency 6
Affiliation 6
Authority 6
Policies 7
Types of Incidents and Level of Support 7
Co-operation, Interaction and Disclosure of Information 7
Operations 7
Communication and Authentication 7
Services 7
Announcements 7
Alerts and Warnings 7
Pre-emptive Security Controls 8
Development of Security Tools for CERT-C own needs 8
Intrusion Detection 8
Digital Forensics and Incident Response 8
Incident Reporting Forms 8
Disclaimers 8

Diffusion

TLP:WHITE

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:WHITE information may be distributed without restriction, subject to copyright controls.

TLP:WHITE
Information may be distributed without restriction. Subject to copyright controls.

Document Information

This document contains a description of CERT Capgemini (CERT-C) as implemented by RFC 2350. It provides basic information about CERT-C, its communication channels, its roles and responsibilities.

Date of Last Update

Version 1.1 from May 24, 2022.

Distribution List for Notifications

There is no distribution list for notifications.

Locations where this Document May Be Found

The current and latest version of this document is available from CERT-C's website at:
https://www.capgemini.com/about-us/management-and-governance/a-responsible-business/cybersecurity/

Authenticating this Document

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

https://www.capgemini.com/about-us/management-and-governance/a-responsible-business/cybersecurity/

Document Identification

- **Title**: CERT CAPGEMINI - RFC2350
- **Version**: 1.1
- **Document Date**: 2022-05-24
- **Expiration**: this document is valid until superseded by a later version

Contact Information

Name of the Team

CERT-C aka CERT Capgemini

Address

CERT Capgemini
Capgemini
147 Quai du Président Roosevelt
92130 Issy-les-Moulineaux
FRANCE

Time Zone

CET/CEST

Telephone Number

+33 764 542 453 (24/7)

Electronic Mail Address

To report an information security incident or a cyber-threat targeting or involving Capgemini Group entities, please contact us at the following address:

cert.global@capgemini.com

Other Telecommunications

N/A

Public Keys and Encryption Information

CERT-C uses the following PGP key:

- ID: 0x2D581804
- Fingerprint: 7A27 A8E7 97FE D453 DB29 956E 29C0 BFD9 2D58 1804

The key can be retrieved at any time from applicable public key servers such as https://keyserver.ubuntu.com/ . The key shall be used whenever information must be sent to CERT-C in a secure manner.

Team Members

The team consists of IT, Cyber and Threat security analysts.

Other Information

Additional applicable information about CERT-C can be found at the following address:
https://www.capgemini.com/our-company/cybersecurity-and-data-protection/

Points of Contact

The preferred method to contact CERT-C is by sending an email to the following address:
cert.global@capgemini.com

An incident response analyst on duty can be contacted at this email address during hours of operation.

Urgent cases can be reported by phone, +33 764 542 453 on a 24/7/365 basis.

Charter

Mission Statement

Within Group Capgemini, the "Group Cyber Security" Department (GCS) defines and translates the security strategy in actionable plans, oversees the level of implemented security controls, responds to incidents and establishes operational security baseline.

As part of the "Group Cyber Security" Department, CERT-C is the global unit in charge of:

- incident response, (severe and critical incidents. The handling of these incidents can be managed with the support of the "Major Incident Management" unit),
- digital forensics,
- malware analysis,
- threat intelligence,
- threat hunting & vulnerability assessment,
- Red Teaming & Pentest activities.

CERT-C's main mission, in collaboration with SOC and C&C IM teams, is to support Capgemini Group's ability to deliver on business goals while protecting it from cyberattacks that would hamper the integrity of its informational and infrastructural assets or damage its reputation.

CERT-C's activities cover threat intelligence (collection, analysis, feeds…) prevention (vulnerability evaluation, exposure…), detection (new threat, campaign, malware, etc.), response, containment, eradication, recovery and post-incident activities as depicted in the incident response cycle.

While delivering on objectives, CERT-C is driven by the following values:

- CERT-C strives to act in accordance with the highest standards in terms of ethics, integrity, honesty and professionalism,
- CERT-C is committed to deliver high quality services to the Capgemini Group within its constituency and while responding to external parties,
- CERT-C does its best to respond to security incidents as efficiently as possible within the best possible delays,
- CERT-C facilitates information exchange between Capgemini Group entities and its peers on a need-to-know basis.

Constituency

The constituency of CERT-C is composed of all institutions and organizations belonging to the Capgemini Group. Please refer to the following resource for more details:

https://www.capgemini.com/our-company/

Affiliation

CERT-C is affiliated to the Capgemini Group.

CERT-C strives to maintain regular contacts with various national and international CSIRT, CERT, incident response and security teams whenever such communication follows Capgemini's needs and communication culture.

Authority

CERT-C operates under the authority of the Capgemini Group Chief Cybersecurity Officer.

Policies

Types of Incidents and Level of Support

CERT-C handles all types of incidents impacting the confidentiality, integrity or availability of Group Capgemini information systems and processes.

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

CERT-C will adjust the extent of provided support depending on the incident's severity, its potential impact and the available staff resources at the time of the incident.

Co-operation, Interaction and Disclosure of Information

CERT-C considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar internal and external bodies, since such cooperative actions are likely to improve CERT-C's efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when CERT-C's cooperation is likely to enable third-party CERTs, CSIRTs and other security teams to better perform their duties and resolve incidents.

Operations

CERT-C operates under the current French legal framework.

CERT-C is fully compliant with the latest approved version of CSIRT Code of Practice version 2.4 as featured at https://www.trusted-introducer.org/TI-CCoP.pdf

Communication and Authentication

CERT-C protects sensitive information in accordance with relevant French, European and Capgemini Group's regulations and policies for applicable jurisdictions.

Specifically, CERT-C enforces the sensitivity markings defined by originators of information communicated to CERT-C ("originator control").

CERT-C also recognizes and follows the FIRST TLP (Information Sharing Traffic Light Protocol) version 1.0.

Communication security, including both encryption and authentication, is achieved by using PGP or any other agreed and tested means, depending on sensitivity and context.

Services

Announcements

CERT-C provides announcements in the form of alerts and security briefings featuring threat intelligence of different sorts, which may include, but is not limited to detected vulnerabilities, new attack tools, techniques and processes as leveraged by the threat actors, indicators of compromise, and security measures needed to protect the Information Systems of Capgemini Group.

Alerts and Warnings

CERT-C disseminates information and intelligence on cyberattacks, technical disruptions, security vulnerabilities, intrusions, malware, and provides recommendations on how to tackle the resulting risk within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis. Alerts bulletins and Newsletter could be internal or external or both, in function of the information and their sensitivity.

Pre-emptive Security Controls

CERT-C performs pre-emptive security controls and technically lead offensive security missions (red teaming) drived by C&C Team to detect potential breaches, vulnerabilities and misconfigurations that may be leveraged by threat actors. These security controls tend to align the compliance level of various systems and applications with the existing security policies.

Development of Security Tools for CERT-C own needs

CERT-C 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, SOC, C&C and broader information security community.

Intrusion Detection

CERT-C challenge tools, services and processes to detect potential intrusions to allow SOC teams to be more effective in their mission.

Digital Forensics and Incident Response

CERT-C performs digital forensics activities whenever necessary, including but not limited to endpoint forensics, memory forensics, smartphone forensics, network forensics, cloud forensics, along with the malware analysis activities, which may result from identified forensic needs.

CERT-C performs incident response for its constituency. The incident response service as developed by Group Cyber Security [including the CERT-C] covers the 6 phases of the Incident Response process: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

Incident Reporting Forms

CERT-C, in collaboration with SOC team, specifically designed incident reporting forms and documents for internal needs, that have been developed to report constituency incidents to CERT-C.

To report an external incident from the outside, please provide the following details to CERT-C:

- contact details and organizational information such as person or organization's name, address and contact information,
- email address, phone number, PGP key if available,
- IP address(es), FQDN(s), and any other relevant technical element or comment,
- supporting technical elements such as logs to illustrate the issue.

Should you desire to forward any email message to CERT-C, please include all relevant email headers, bodies and attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

Disclaimers

CERT-C will take all necessary precautions and apply its best competence and effort while preparing, notifying and alerting about an incident.

However, CERT-C will take no responsibility for errors, omissions or damages resulting from the use of the information it provides.