TLP:WHITE

CSIRT SUEZ

RFC 2350

SUEZ IT - Cybersecurity

Contents

1 About this document

This document contains a description of CSIRT SUEZ according to RFC 2350 and provides essential information about CSIRT SUEZ, its role, responsibilities and means of communication.

1.1 Document version and Date of Last Update

The version of this document is 1.0, published on 7th December 2020.

1.2 Distribution List for Notifications

Changes to this document are not communicated by distribution list.

1.3 Location where this document may be found

The current version of this document has not yet been published. It is stored in CSIRT SUEZ work directories.

1.4 Authenticating this document

This document is signed with the PGP key of CSIRT SUEZ.

2 Contact Information

This section describes the means of communication of CSIRT SUEZ.

2.1 Name of the Team

The registered name is **CSIRT SUEZ**.

2.2 Address

SUEZ Groupe SA
DSI Groupe - Cybersécurité – CSIRT SUEZ
16, place de l'Iris
92040 Paris La Défense Cedex
FRANCE

2.3 France Creation date

CSIRT SUEZ was created on May 18th, 2020.

2.4 Time zone

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

2.5 Telephone Number

+33 1 58 81 29 13

2.6 Facsimile Number

NA.

2.7 Other Telecommunication

NA.

2.8 Electronic Email Address

The email address is: **csirt@suez.com.**

2.9 Public Keys and Other encryption information

CSIRT SUEZ has a PGP public key including:

- The KeyID is **0xE172F74A**
- The Fingerprint is: **96b6 901f 2240 c7b7 12c8 acdf 99da 818d**

The public key can be obtained by sending an email to CSIRT SUEZ (see address in section 2.8) or can be found on the usual key servers,

(e.g. https://keyserver.ubuntu.com/pks/lookup?search=0xE172F74A&fingerprint=on&op=index).

2.10 Team Members

The team is made up of cyber security analysts and expert security incident responders. No personal information relating to members of CSIRT SUEZ is published in this document.

2.11 Operating Hours

It is preferable to contact CSIRT SUEZ by email at the address in section 2.8.

If it is impossible to send an email, it is possible to contact CSIRT SUEZ by telephone at any time. CSIRT SUEZ organization type is “follow of the sun”. L3 experts work from France, United-States and Australia to cover all time zones. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail. Moreover, in the event of an emergency and outside working hours, the telephone is redirected to the on-call service (mobile number of one of the members).

2.12 Additional Contact Information

No additional contact information can be found for now.

3 Charter

3.1 Mission statement

The activities of CSIRT SUEZ are non-profit and are financed by the SUEZ Groupe SA. The mandate for CSIRT SUEZ is as follows:

- Control and monitor cybersecurity risks through a recurring monitoring activity on cyber threats and cybersecurity for the entire SUEZ Group and its subsidiaries;
- Prevent and anticipate cybersecurity incidents by providing solid expertise in vulnerability management, awareness and technical security auditing;
- Investigate, respond to and coordinate the cyber security incident that may affect the assets of the SUEZ Group, in accordance with the laws and regulations that may apply;
- Ensuring compliance with SUEZ Group safety rules.

3.2 Constituency

CSIRT SUEZ coordinates and processes the response to the incident. It also provides cybersecurity services for the entire SUEZ Group. More information about the SUEZ Group is available at the following address: www.suez.com.

3.3 Sponsorship / Affiliation

CSIRT SUEZ is a private CSIRT in the environment sector. It is operated, financed by and owned by SUEZ Groupe SA.

CSIRT SUEZ maintains relations with various CSIRTs in France and abroad. Some moments are dedicated to share about CERT/CSIRT activities and news.

Each year, CSIRT SUEZ management assesses the opportunity to have its analysts participate in cybersecurity related or CSIRTs related conferences or events. These events can be held in person or remotely. This time is allocated to the teams as part of their cyber watch.

CSIRT SUEZ is willing to share within the CSIRT/CERT networks and to join some communities.

3.4 Authority

CSIRT SUEZ acts under the authority of **SUEZ IT Group**.

3.5 Responsibility

CSIRT SUEZ is responsible for anticipating cyber threats and responding to major cybersecurity incidents throughout the Group. If necessary, the CSIRT SUEZ may help on and respond to more minor incidents.

4 Policies

4.1 Types of Incidents and Level of Support

CSIRT SUEZ coordinates, analyses and handles cybersecurity incidents, requiring its L3 expertise, which target or could target one of the entities or subsidiaries of the SUEZ Group. In this capacity, it also participates in the management of cybersecurity vulnerabilities by informing people who need to know about the vulnerabilities reported to it and helping them to eliminate them.

The level of support offered by CSIRT SUEZ may vary according to the type of incident, its criticality, and the resources available to handle it. Generally, support is provided on the same working day, or the next day, during operating hours.

4.2 Co-operation, Interaction and Disclosure of Information

At a group level, CSIRT SUEZ co-operates with regional and local SUEZ cybersecurity teams to manage incidents, vulnerabilities and recoveries. Processes are formalized to set the scope and interactions of each stakeholder.

At a groupwide level, CSIRT SUEZ will exchange all necessary information with other CERT/CSIRTs, in the same CERT/CSIRT communities or not, that may be concerned on a need-to-know basis.

No incident or vulnerability will be disclosed publicly without the agreement of all the parties concerned.

Legal requests will be evaluated by our legal department and an appropriate response will be given if the request is acceptable, within the limits of the court order, the related investigation and the information requested.

4.3 Communication

CSIRT SUEZ strongly encourages the use of a PGP key for email encryption. All emails containing confidential information must be encrypted using a PGP key.

CSIRT SUEZ respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED.

A telephone call, a postal service or an unencrypted email can be used for non-sensitive information sharing.

To make itself known from its constituency, CSIRT SUEZ organizes several different monthly meetings with SUEZ entities’ IT and cybersecurity teams to discuss incident response and detection. These meetings are also an opportunity for CSIRT SUEZ to share information from the group's point of view with these IT and cybersecurity teams. Moreover, CSIRT SUEZ sends them vulnerability bulletins to help them through vulnerability management.

5 Services

5.1 Incident Response

CSIRT SUEZ, supported by other SUEZ cybersecurity teams, has the following activities in charge:

- Incident management:
    - Consideration of the incident (false positive or true positive):
        - Gather information about the incident;
        - Confirm that the event described is a cybersecurity incident;
        - Determine/review the severity of the incident and its extent.
    - Incident analysis and investigation;
    - Coordination of incident response;
    - Aftermath and feedback on most critical incidents.

- Vulnerability management:
    - Coordination of responses to vulnerabilities.

5.2 Proactive Activities

CSIRT SUEZ is in charge of :

- Monitoring of threats and vulnerabilities;
- Artifact processing and analysis;

The realization or the follow-up of intrusion tests;

- Analysis of attack scenarios and the cybersecurity measures required to protect information systems.

This information may be exchanged with other CSIRTs if it proves useful, on a need-to-know basis.

5.3 Alerts, Warnings and cyberthreat

CSIRT SUEZ is in charge of:

- Identification and processing of IOCs and viral signatures;
- The improvement of its knowledge on the actors of the cyber threat;
- Communication about Cyber Threats;
- Cyber Threat Awareness.

6 Incident Reporting

To report an incident, please report the incident by encrypted email to the address in section 2.8.

Incident reports should contain the following information:

- Date and time of the incident (including time zone);
- Description of the incident;
- Source/destination IPs, ports and protocols or product concerned;
- Any other relevant information.

7 Disclaimers

Although the information provided in this document has been verified, CSIRT SUEZ declines all responsibility in the event of any error or omission or for any prejudice resulting from information contained in this document. If you notice any error in this document, please notify us by e-mail. We will try to rectify the information as soon as possible.