TLP:CLEAR

○○○

SUEZ GROUP CSIRT

RFC 2350

SUEZ - Information Systems Department – IS Security

MODIFICATION CHANGELOGS			
Date	**Modification**	**Author**	**Version**
01/01/2020	Creation of document	Acher ELGRABLY – CSIRT Manager	V1.0
31/03/2023	Review & update of document	Amine MADDAH – CSIRT Team Leader	V2.0
31/03/2023	Approval of the V2.0	Thibaud BINETRUY – CSIRT Manager	V2.0
02/11/2023	Update v2.1 – Renewal of CSIRT PGP Key	Amine MADDAH – CSIRT Team Leader	V2.1

CONTENTS

1 About this document 4

1.1 Document version and Date of Last Update 4

1.2 Distribution List for Notifications 4

1.3 Location where this document may be found 4

1.4 Authenticating this document 4

2 Contact Information 4

2.1 Name of the Team 4

2.2 Address 4

2.3 Creation date 4

2.4 Time zone 4

2.5 Telephone Number 5

2.6 Facsimile Number 5

2.7 Other Telecommunication 5

2.8 Electronic Email Address 5

2.9 Public Keys and Other encryption information 5

2.10 Team Members 5

2.11 Operating Hours 5

2.12 Additional Contact Information 5

3 Charter 6

3.1 Mission statement 6

3.2 Constituency 6

3.3 Sponsorship / Affiliation 6

3.4 Authority 6

3.5 Responsibility 7

4 Policies 7

4.1 Types of Incidents and Level of Support 7

4.2 Co-operation, Interaction and Disclosure of Information 7

4.3 Communication 7

5 Services 7

5.1 Incident Response 7

5.2 Proactive Activities 8

5.3 Alerts, Warnings and cyberthreat 8

6 Incident Reporting 8

7 Disclaimers 9

1 About this document

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

1.1 Document version and Date of Last Update

The version of this document is 2.1, published on 02/11/2023.

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 located in the CSIRT work directories.

1.4 Authenticating this document

The English version of this document is signed with the PGP key of the CSIRT of the SUEZ Group.

2 Contact Information

This section describes the means of communication of the SUEZ Group CSIRT.

2.1 Name of the Team

The registered name is the CSIRT of the SUEZ Group and its acronym CSIRT SUEZ.

2.2 Address

CSIRT of the SUEZ Group
Tour CB 21
16, place de l'Iris
92040 Paris La Défense Cedex
France

2.3 Creation date

The CSIRT of the Suez Group was set up in 01/01/2020.

2.4 Time zone

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

2.5 Telephone Number

+33 6 72 72 30 30

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

The CSIRT of the Suez Group has a PGP public key including:

- The KeyID is **0x57a92fa3;**
- The Fingerprint is: **B45C 3B0E 75EA 39C0 4D17 4C5A ED54 7D64 57A9 2FA3**

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

(e.g. https://keyserver.ubuntu.com/pks/lookup?search=0x57a92fa3&fingerprint=on&op=index)

2.10 Team Members

The team is made up of cyber security analysts. No personal information relating to members of the Suez Group CSIRT is published in this document.

2.11 Operating Hours

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

If it is impossible to send an email, it is possible to contact the CSIRT of the SUEZ Group by telephone at any time. SUEZ CSIRT organization type is "follow of the sun". Some L3 experts work from 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 the CSIRT of the SUEZ Group are not-for-profit and are financed by the SUEZ Group. The mandate for the SUEZ Group CSIRT is as follows:

- Control and monitor cybersecurity risks through a recurring monitoring activity on cyber threats and cybersecurity for the entire 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

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

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

3.3 Sponsorship / Affiliation

The CSIRT of the SUEZ Group is a private CSIRT in the energy sector. It is operated, financed by and owned by SUEZ SA.

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

Each year, CSIRT management assesses the opportunity to have its analysts participate in cybersecurity-related or CSIRT-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

The CSIRT of the SUEZ Group acts under the authority of SEHQ – SUEZ GROUP IT Security service.

3.5 Responsibility

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

4 Policies

4.1 Types of Incidents and Level of Support

The SUEZ Group CSIRT coordinates, analyses and handles IT security 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 security 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 the SUEZ Group CSIRT 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, the CSIRT co-operates with regional and local SUEZ security teams to manage incidents, vulnerabilities and recoveries. Processes are formalized to set the perimeters and interactions of each stakeholder.

At a groupwide level, the SUEZ Group CSIRT 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

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

SUEZ CSIRT 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 the exchange of non-sensitive information.

5 Services

5.1 Incident Response

CSIRT SUEZ, supported by other SUEZ security teams, has for activity:

- Incident management:

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

5.2 Proactive Activities

The team has for activity:

- Monitoring of threats and vulnerabilities;
- Artifact processing and analysis;
- The realization or the follow-up of intrusion tests;
- Analysis of attack scenarios and the security 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

The team has for activity:

- 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, the CSIRT of the SUEZ Group 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.