Air Liquide CSIRT RFC 2350

Document information

This document contains a description of Air Liquide CSIRT according to RFC 2350. It provides basic information about the Air Liquide CSIRT, its responsibilities and services offered by Air Liquide CSIRT.

Date of the Last Update

This is the version 1.1 published on August 22th, 2022.

Distribution List for Notifications

Notification of document changes is not distributed by a mailing list or any other mechanisms outside of Air Liquide.

Location where this Document May be Found

The current and latest version of this document is provided on demand, a project to publish it on Air Liquide's website is ongoing.

Document authenticity

This document has been signed with the PGP Key of Air Liquide CSIRT. The PGP public key is available at: https://openpgp.circl.lu/pks/lookup?op=get&search=0xc1762a264c30ac7d.

Document identification

Title: 'RFC2350 - Air Liquide CSIRT'
Version: 1.1
Document Date: August 22th, 2022.
Expiration: this document is valid until superseded by a later version.

Contact information

Name of the team

Official name: CSIRT Air Liquide
Short name: AL CSIRT

Postal Address

Coeur Défense - Tour A - Défense 4
110 Esplanade du Général de Gaulle
92400 Courbevoie

Time Zone

CET/CEST

Telephone Number

Main number (duty office): none.

Facsimile Number

N/A

Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Air Liquide CSIRT, please contact us at: csirt@airliquide.com.

Public Keys and Encryption Information

Air Liquide CSIRT uses the following PGP key:
User ID: CSIRT Air Liquide <csirt@airliquide.com>
Key ID: 4C30AC7D
Fingerprint: 0E9B 47B4 C3A7 3FF9 7FE5 42FC C176 2A26 4C30 AC7D
The PGP key can be retrieved from applicable public key servers such as https://openpgp.circl.lu/.

Team Members

The list of the team members is not publicly available. The identity of Air Liquide CSIRT's team members might be disclosed on a case-by-case basis according to the need-to-know restrictions.

Other information

See our web site at https://airliquide.com for additional information about Air Liquide.

Points of Contact

The preferred method for contacting Air Liquide CSIRT is via e-mail at csirt@airliquide.com.
Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your email.
If it is not possible (or not advisable for security reasons) to use e-mail, Air Liquide CSIRT can be reached by telephone during regular business hours (local time).

Air Liquide CSIRT operates on a 24/5 basis (weekdays, from Monday to Friday) through a follow the sun organization.

Charter

Mission Statement

Air Liquide CSIRT assists Air Liquide group entities and affiliates (as defined hereafter) in managing all types and scales of cybersecurity incidents.

Air Liquide CSIRT is responsible for coordinating the incident response and detecting malicious activities across Air Liquide group entities and affiliates.

Constituency

The constituency of Air Liquide CSIRT is composed of Air Liquide group entities (Group branches, divisions, departments or other business segments) and affiliates (companies in which Air Liquide holds, directly or indirectly, the majority of the voting rights).

Sponsoring Organization / Affiliation

Air Liquide CSIRT is a private CSIRT set up and operated by Air Liquide, a world leader in gases, technologies and services for Industry and Health.
It maintains relationships with different national and international CSIRTs and CERTs.

Authority

Air Liquide CSIRT operates under the authority of the Air Liquide group CIO.

Policies

Types of Incidents and Level of Support

Air Liquide CSIRT’s assistance may be requested in all types of cybersecurity incidents that may occur within its constituencies, on premise or in the cloud, IT or OT, whenever Air Liquide group is impacted.

The level of support depends on the type and severity of the given security incident, the amount of affected entities, and our resources at the time.

Co-operation, Interaction and Disclosure of Information

Air Liquide CSIRT can collaborate with other CSIRTs and CERTs as well as with other affected third parties to the extent they are involved in the incident or incident response process.

Information received by Air Liquide CSIRT may be shared with Air Liquide group entities and affiliates, as well as to cybersecurity service providers, on a need to know basis in respect of the TLP of the information.

Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication Air Liquide CSIRT uses several encryption solutions. By default, all sensitive information should be encrypted with our public PGP key detailed in Section 2.7.
General non-restricted information can be transmitted by telephone, regular mail or unencrypted email.

Air Liquide CSIRT respects the Information Sharing Traffic Light Protocol (TLP[1]).

[1] https://www.first.org/tlp/

Services

1. Threat Intelligence

One of the main services provided by CSIRT to the Air Liquide group is the provision of Cyber Threat Intelligence.

Air Liquide receives global security watch, vulnerability watch and CTI feeds (IoCs) from various services.

CTI is then used for:

- Performing Threat Hunting campaigns.
- Providing IoC elements directly into detection tools.
- Improving detection rules to cover new threats.
- Informing the group about threats and vulnerabilities.

2. Intrusion Detection

Air Liquide CSIRT operates security monitoring on Air Liquide's on-premises infrastructure, Public cloud environments, Air Liquide’s critical digital assets and OT perimeter. Air Liquide CSIRT leverages tools, services and processes to detect potential intrusions.

3. Digital Forensics and Incident Response

Air Liquide’s Cyber incident management process: applies on all digital uses either for company purposes or any use involving company-procured IT / OT infrastructure, systems, devices or data; includes uses of all types of digital technologies, applications, and services: accessed and used permanently or occasionally; provided by the Group internally or through outsourcing arrangements; commercialized or accessible on the public internet; applies to all digital assets owned by the Group or contractually or legally placed under its responsibility; involves all employees and third-party personnel and any individual who has been granted authorized IT / OT access; and covers all areas of business operations, activities and support functions, including industrial operations, plant computing systems and connected devices.

The Cyber Incident management process rests on the following fundamental principles:

- Early detection and reporting of all incidents, using human (“first witness”) and technical detection abilities;
- Orchestrated, disciplined response adapted to the severity of potential incident;
- Central knowledge base of incidents to continuously broaden and refine Group’s knowledge, detection ability, and velocity of treatment;
- Involvement of Business, Communication, Digital Security and IT stakeholders with clear responsibilities and rules of engagement;
- Tracking and reporting of incident trends and process effectiveness through few simple and meaningful indicators;
- Capitalization plan implementation and tracking.

Incident Reporting Forms

There is no specific security incident reporting form. Incidents should be reported via encrypted email.

Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Air Liquide CSIRT shall not be responsible for any errors or omissions, or for any damages resulting from or arising out of the use of the information contained herein and therein.